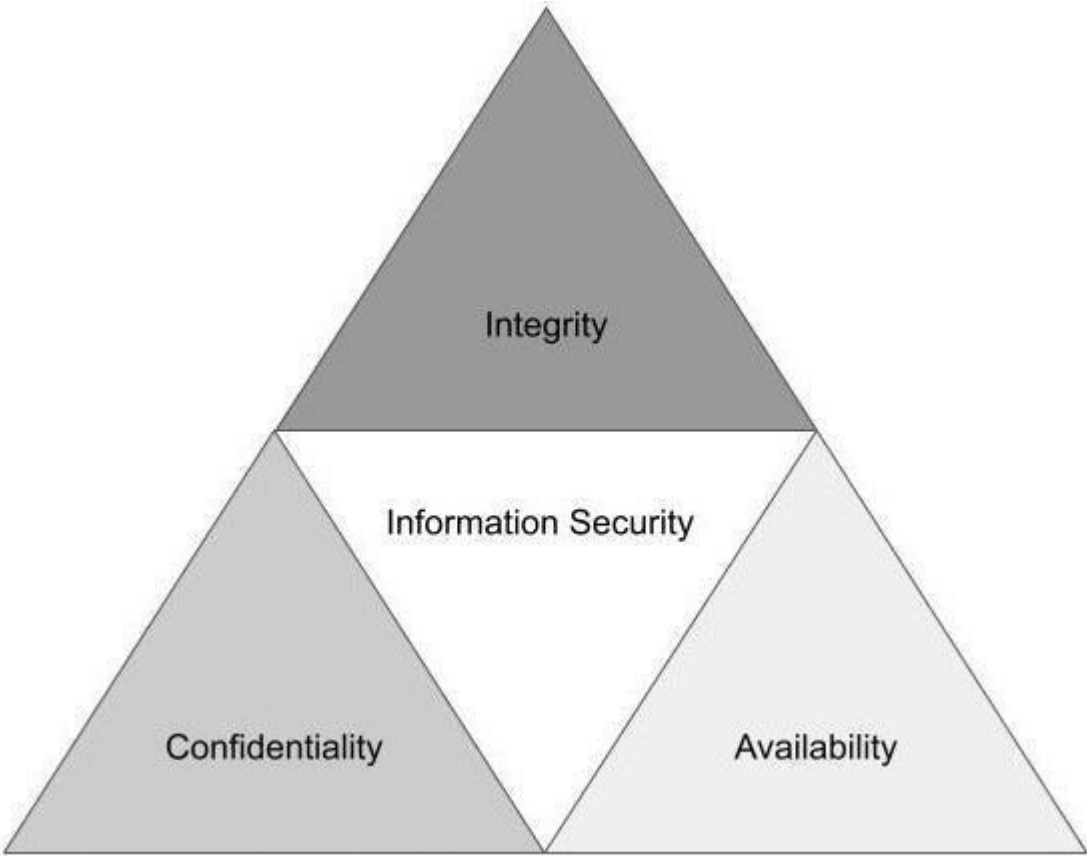
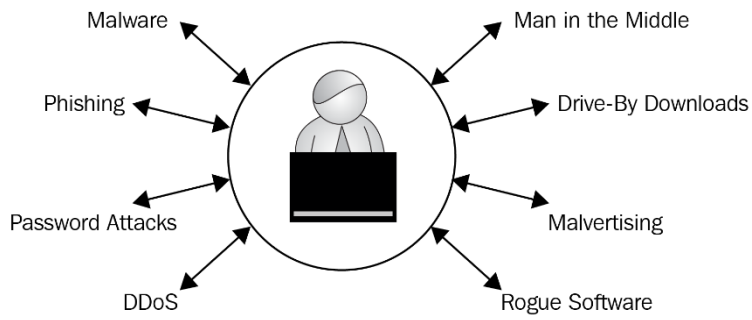
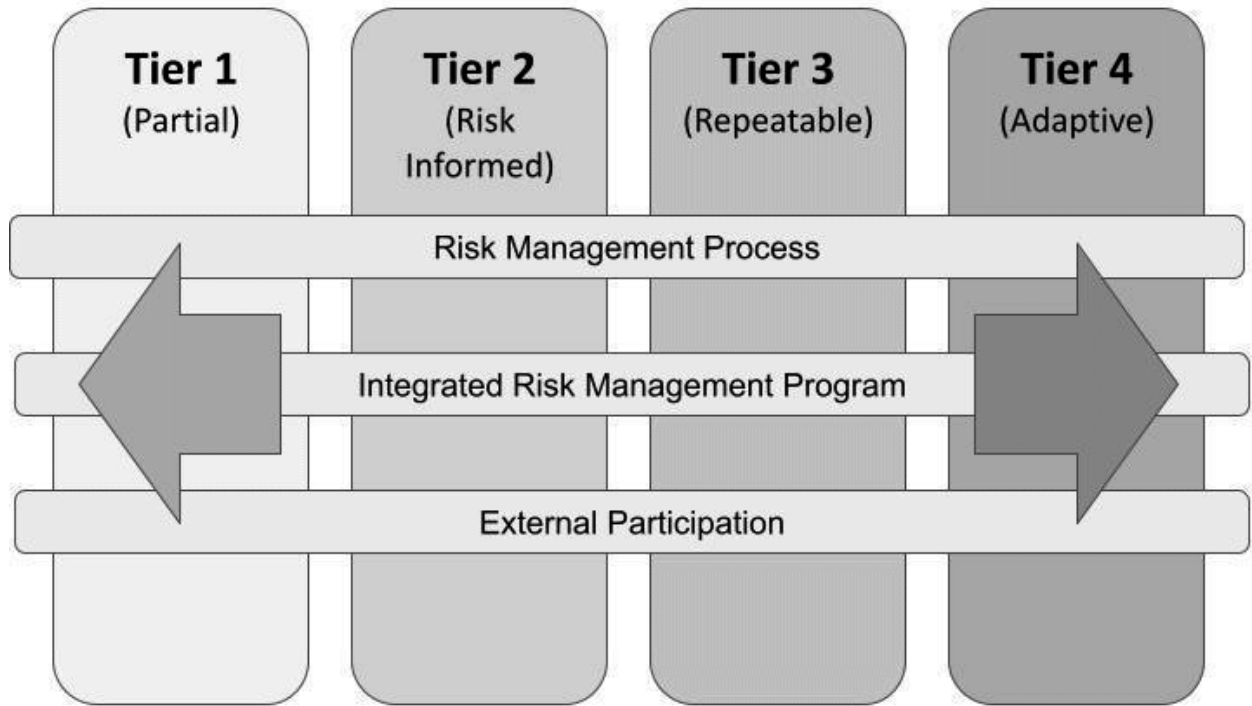
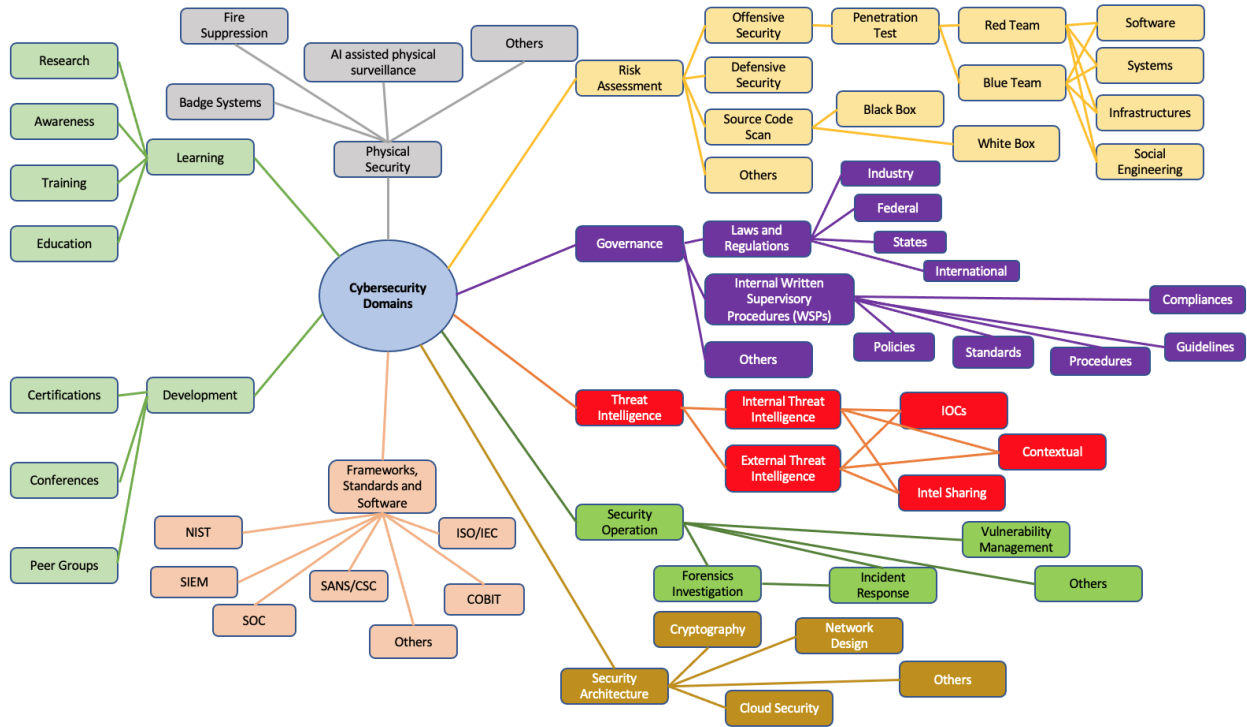


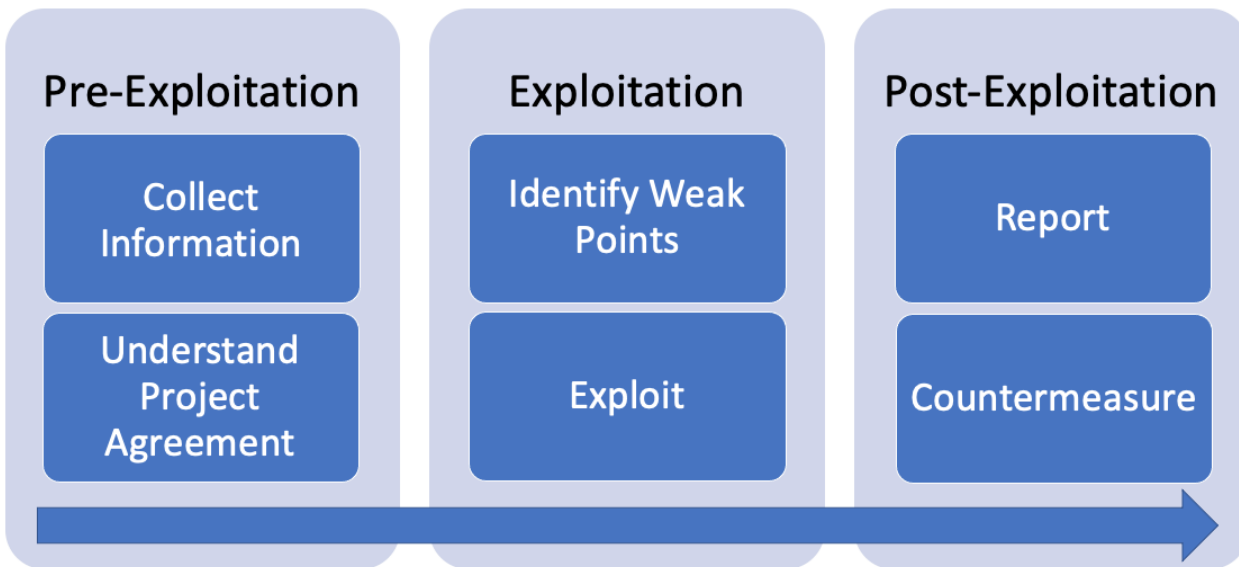
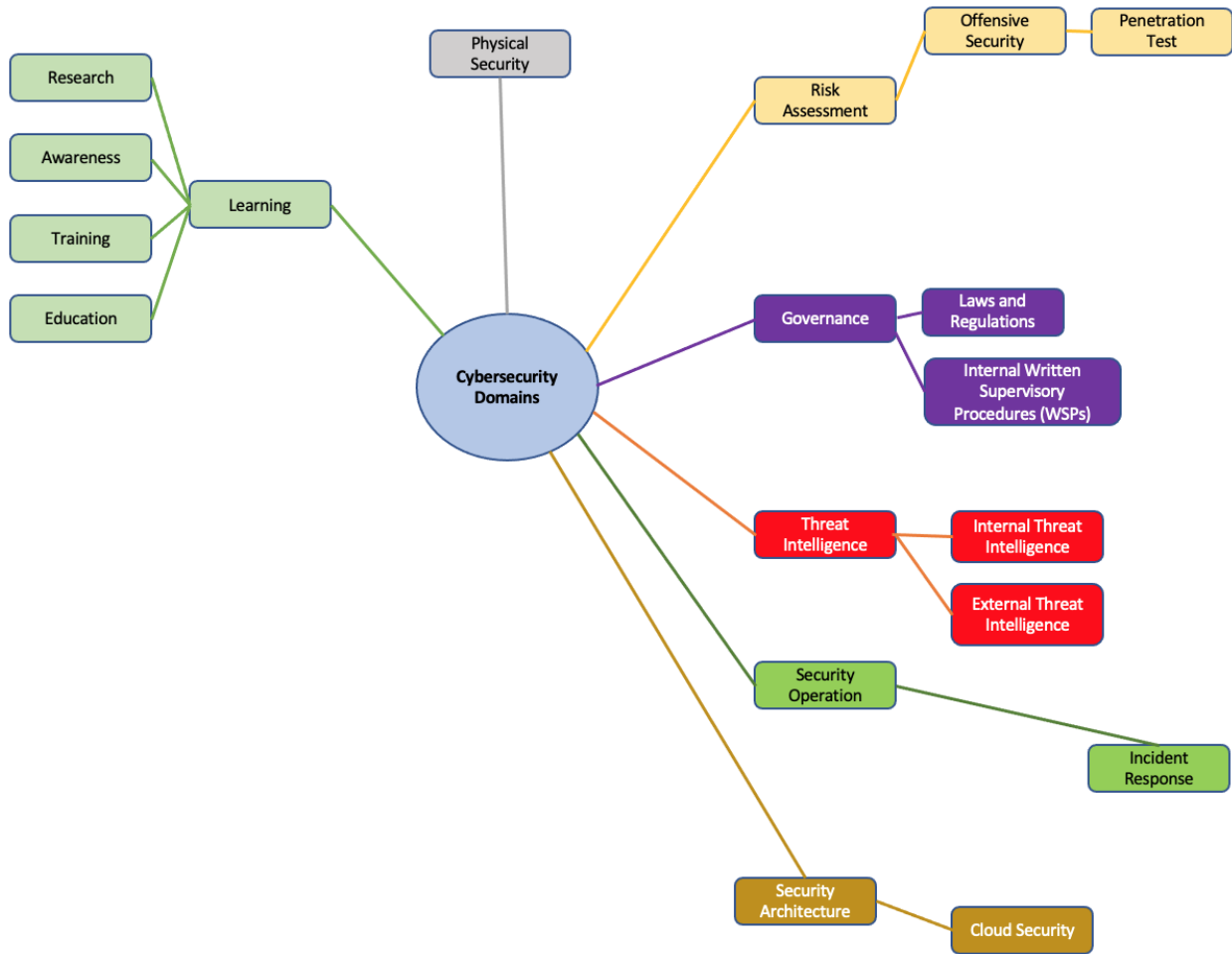
Chapter 1: New Career in Cyber... "Who Dis?"

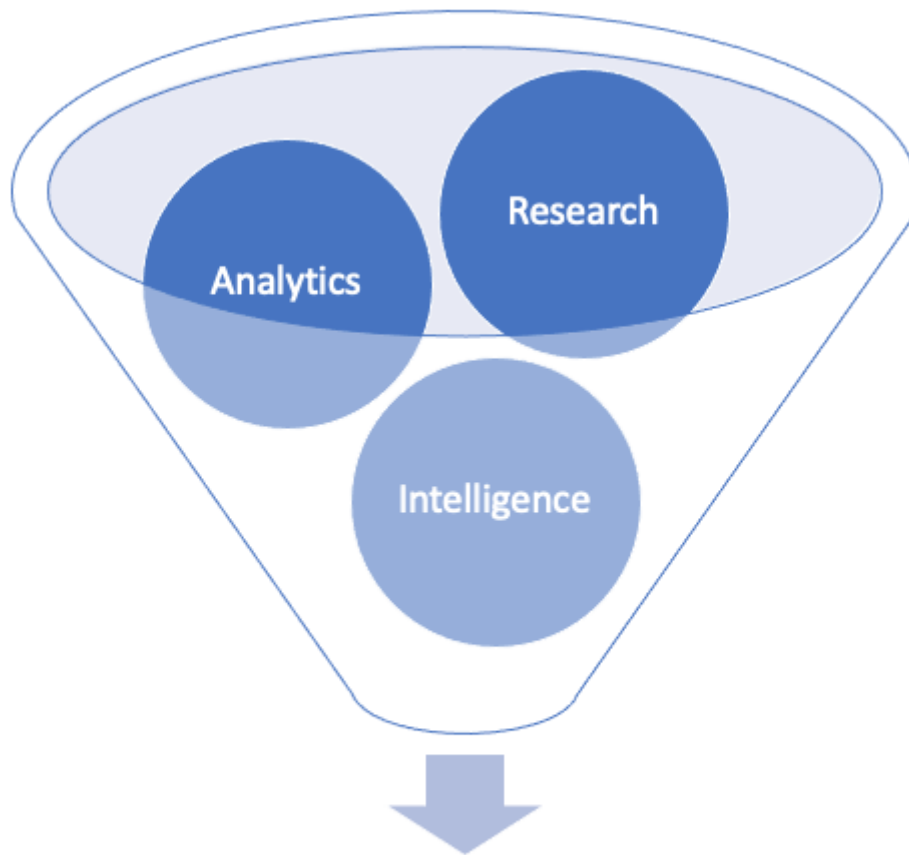




Chapter 2: Which Career Field Is Best for You?

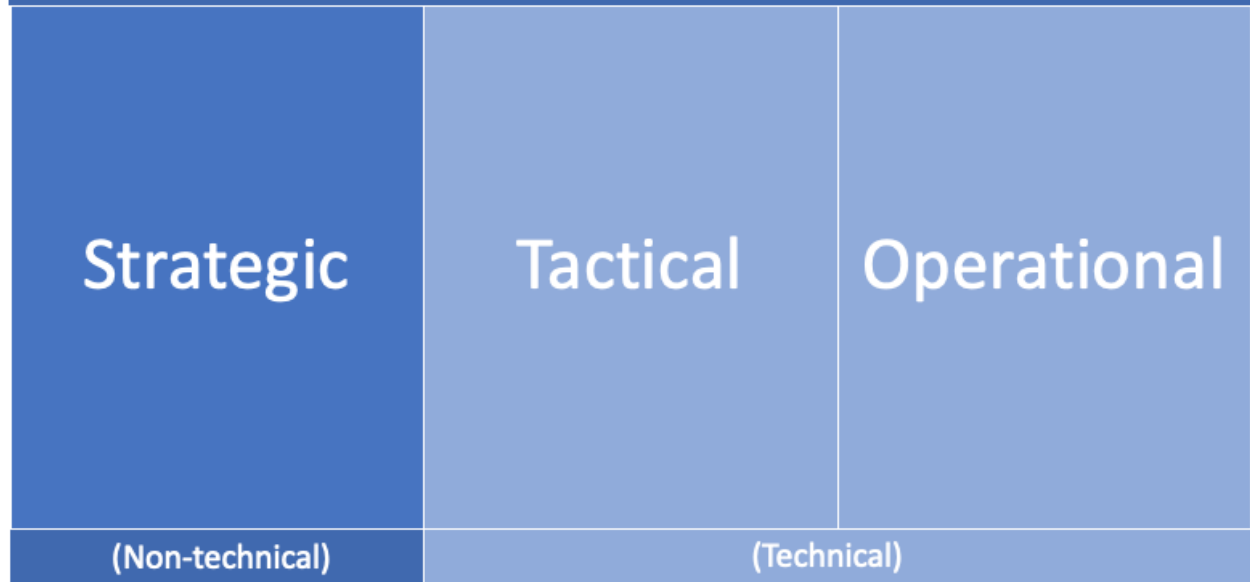


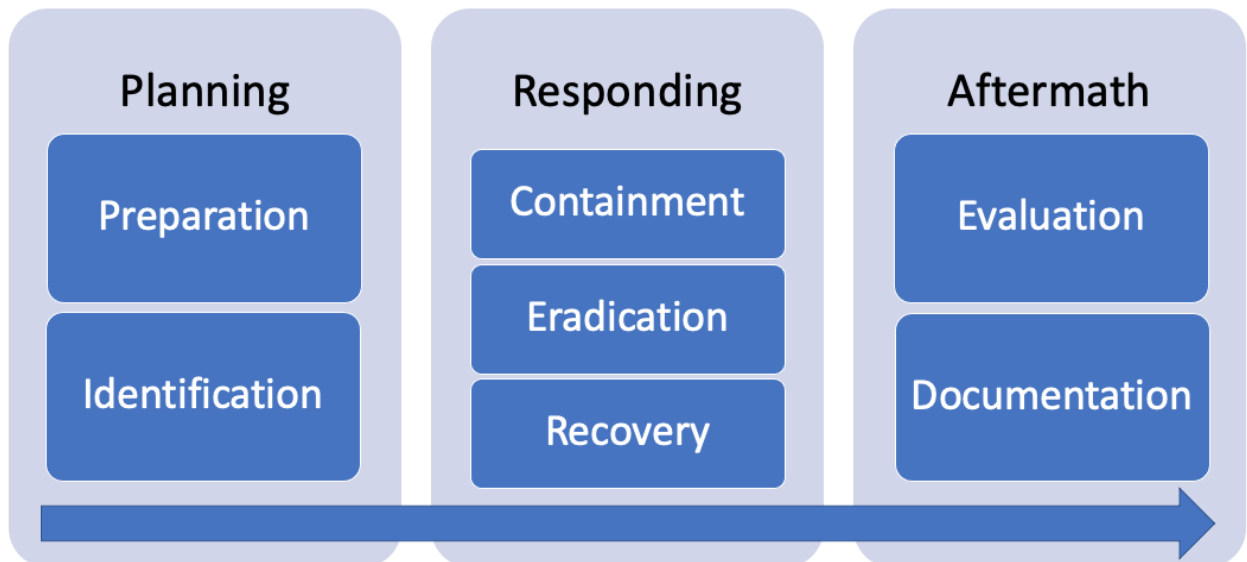
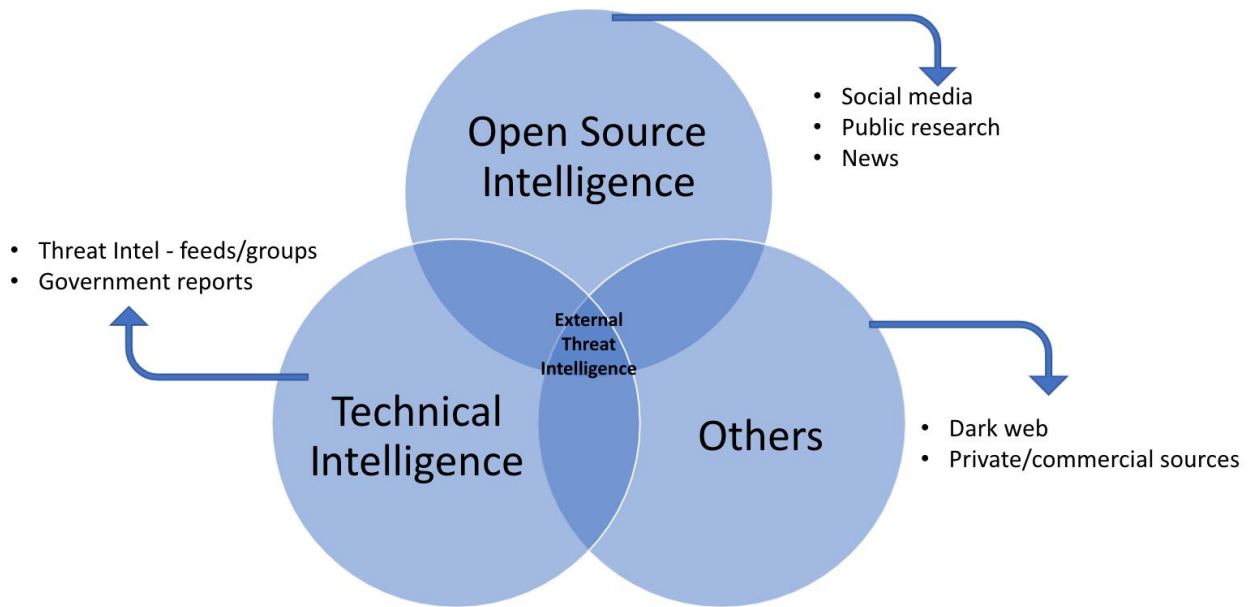


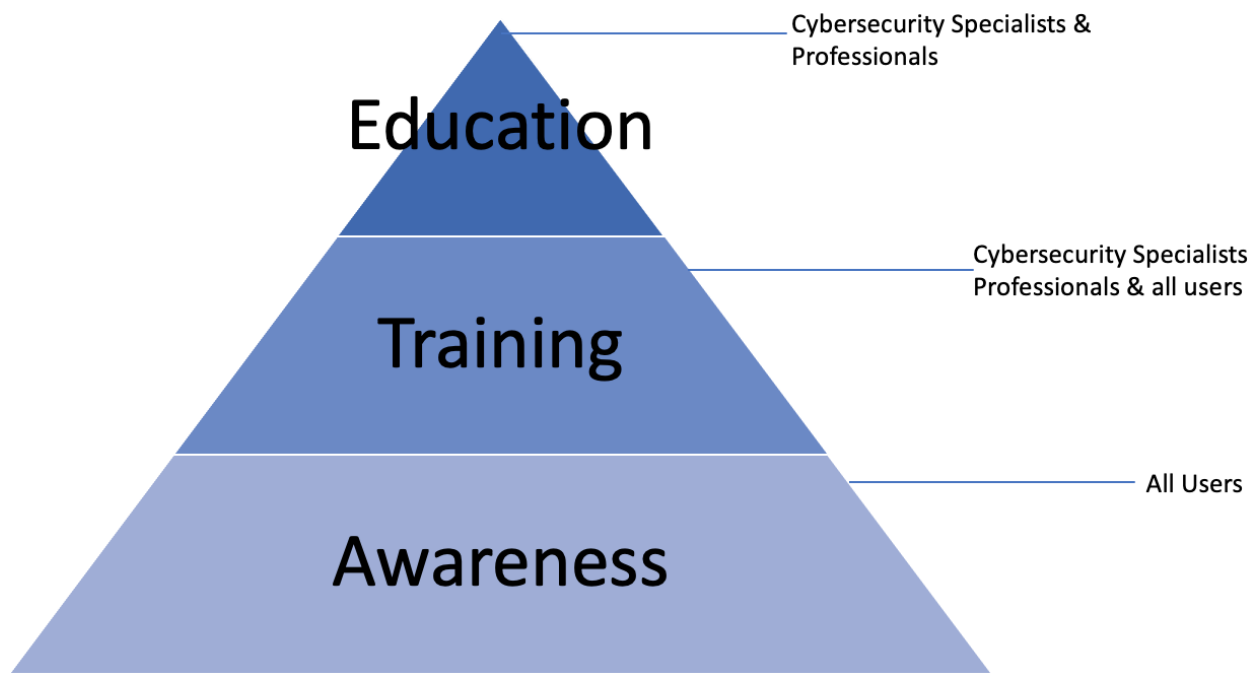
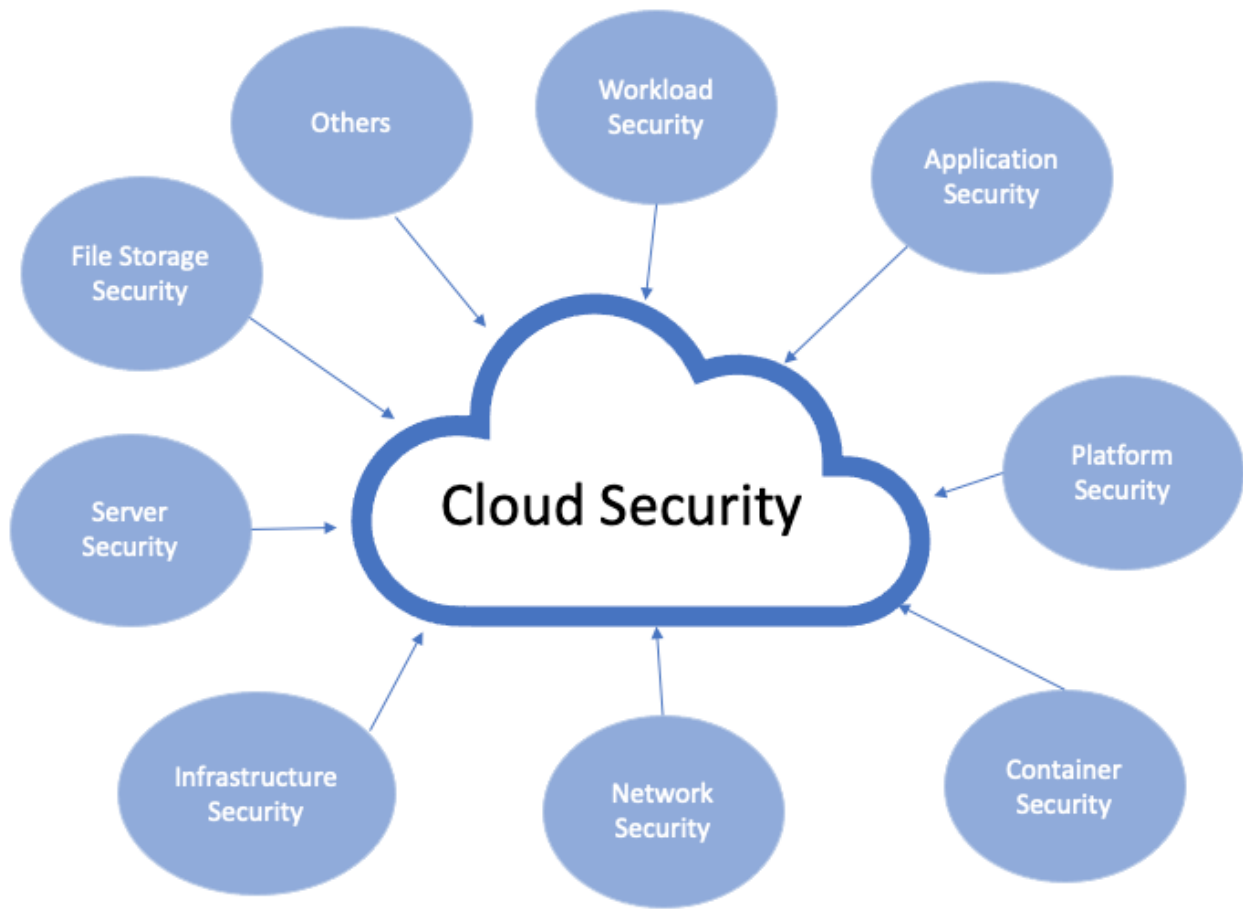


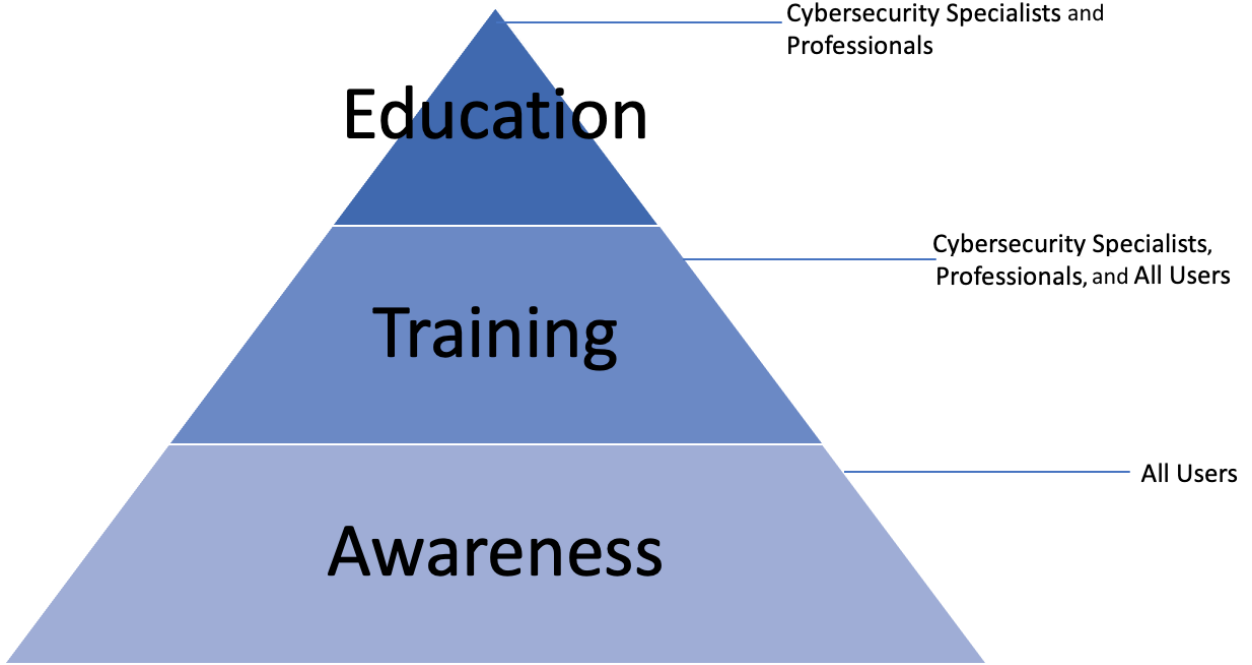
Cyber Threat Intelligence

Cyber Threat Intelligence Types



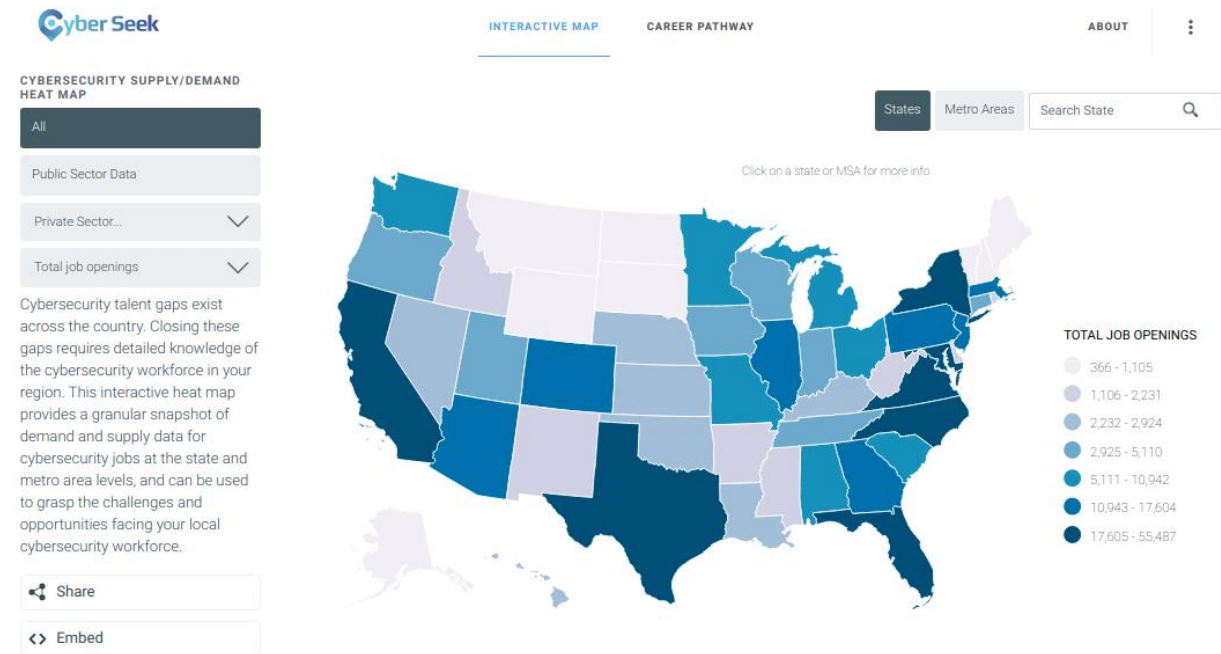




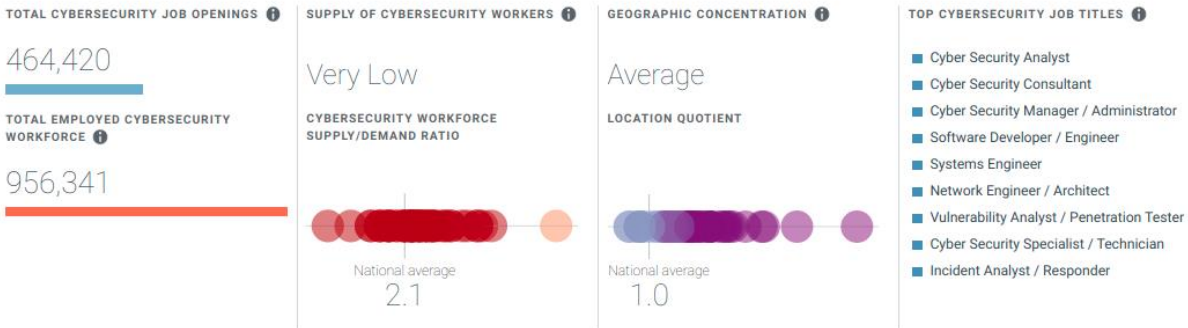




Chapter 3: Different Strokes for Different Folks



National level



**U.S. Department of Health and Human Services
Office for Civil Rights
Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information**

Under Investigation Archive Help for Consumers

Archive

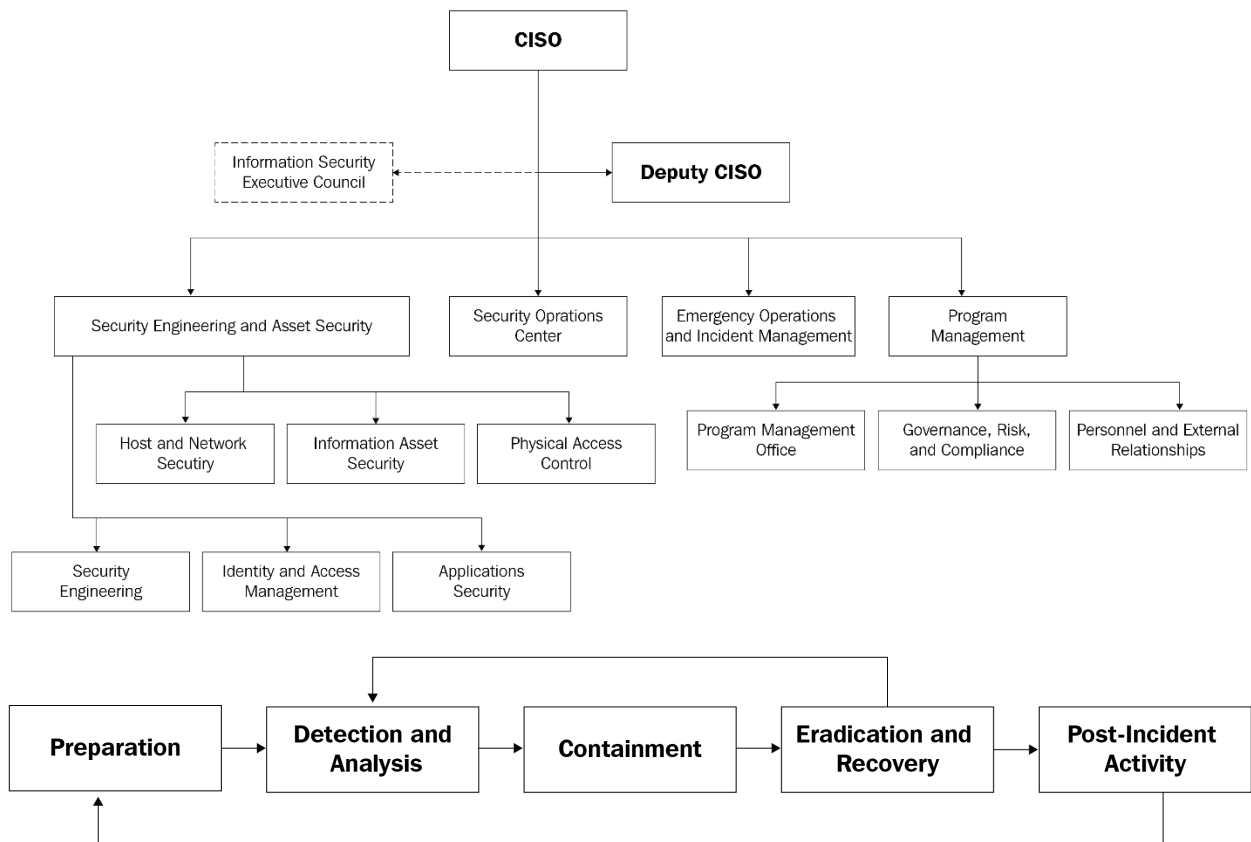
This page archives all resolved breach reports and/or reports older than 24 months.

Show Advanced Options Research Report

Breach Report Results							
Expand All	Name of Covered Entity	State	Covered Entity Type	Individuals Affected	Breach Submission Date	Type of Breach	Location of Breached Information
	Wellness Pharmacy	PA	Healthcare Provider	545	12/10/2020	Theft	Paper/Films
	26th & Lehigh Pharmacy	PA	Healthcare Provider	549	12/10/2020	Theft	Paper/Films
	Diamond Pharmacy	PA	Healthcare Provider	616	12/10/2020	Theft	Paper/Films
	RXN, Inc. d/b/a Lancaster Pharmacy	PA	Healthcare Provider	856	12/10/2020	Theft	Paper/Films
	Brigham and Women's Hospital	MA	Healthcare Provider	882	12/08/2020	Unauthorized Access/Disclosure	Email
	Hillcrest Nursing Center	IL	Healthcare	1030	11/24/2020	Unauthorized	Electronic Medical Record

On-site	IaaS	PaaS	SaaS
Applications	Applications	Applications	Applications
Data	Data	Data	Data
Runtime	Runtime	Runtime	Runtime
Middleware	Middleware	Middleware	Middleware
O/S	O/S	O/S	O/S
Virtualization	Virtualization	Virtualization	Virtualization
Servers	Servers	Servers	Servers
Storage	Storage	Storage	Storage
Networking	Networking	Networking	Networking

■ You Manage
■ Service provider manages



Chapter 4: Exploring Certifications and College

CompTIA Security +

- Cost
 - \$349 (Voucher)
 - \$100-\$200 (Materials, Videos, Test Book)
- 1-3 months of consistent study
- Exam
 - 90 minutes
 - 90 questions (Maximum)
 - 750 (on a scale of 100-900)
- Passing Without Industry Experience
 - Less challenging proper studying

Average Total Cost Per Month: \$160 / 3 Months

PACKAGES

PEN-200 course + 30 days lab access + OSCP exam certification fee	\$999
PEN-200 course + 60 days lab access + OSCP exam certification fee	\$1199
PEN-200 course + 90 days lab access + OSCP exam certification fee	\$1349
PEN-200 course + 365 days lab access + 2 OSCP exam attempts	\$2148

RETAKES

OSCP Certification Exam Retake Fee	\$150
------------------------------------	-------

LAB EXTENSIONS

PEN-200 lab access – extension of 30 days	\$359
PEN-200 lab access – extension of 60 days	\$599
PEN-200 lab access – extension of 90 days	\$799

Process of Auditing Information Services 21%

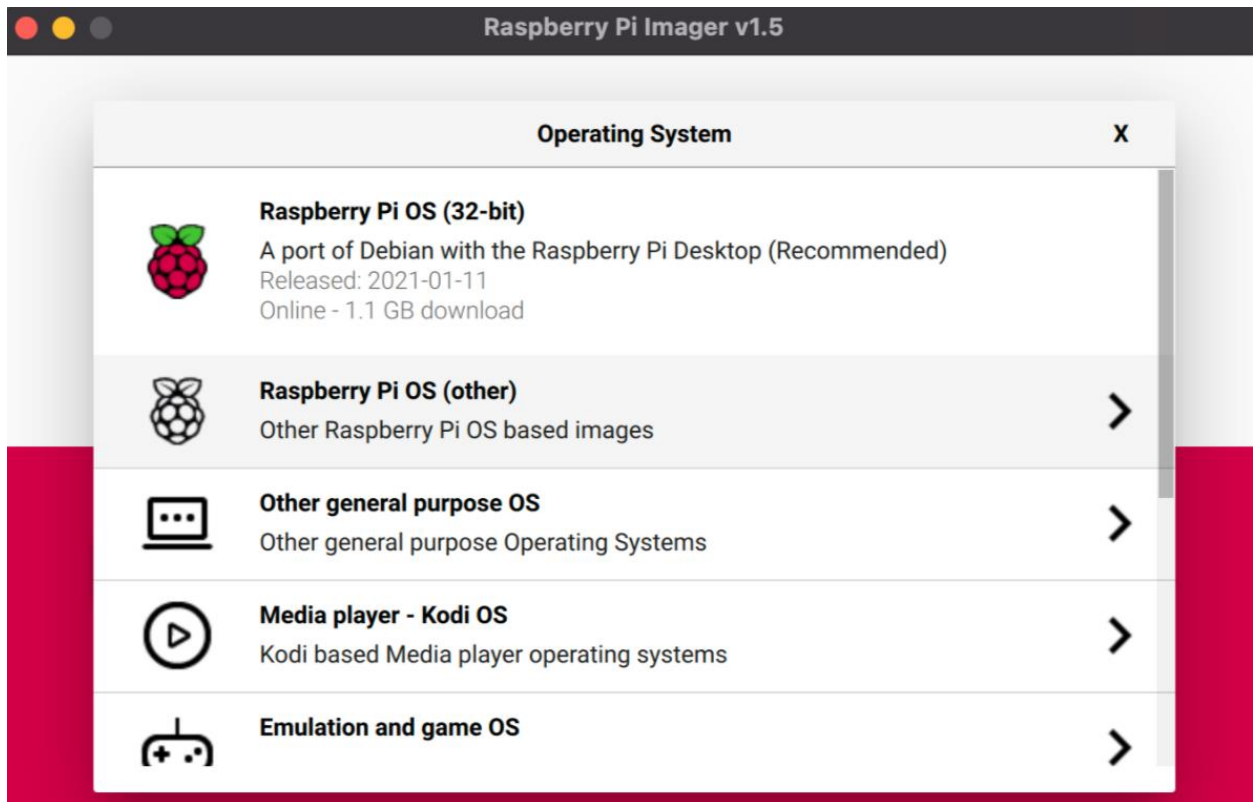
Governance and Management of Information Technology 16%

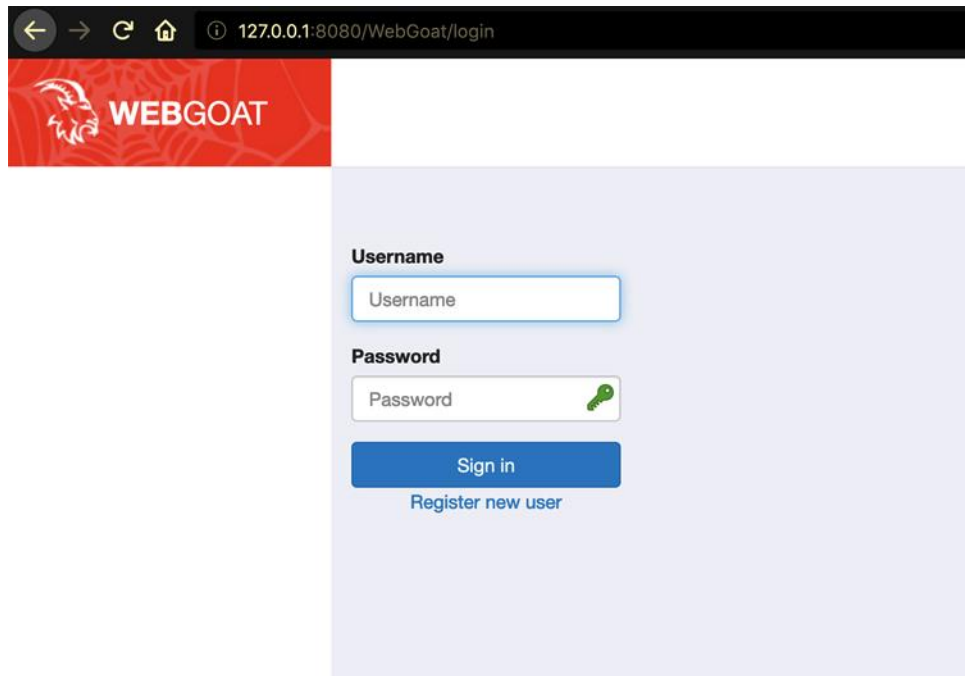
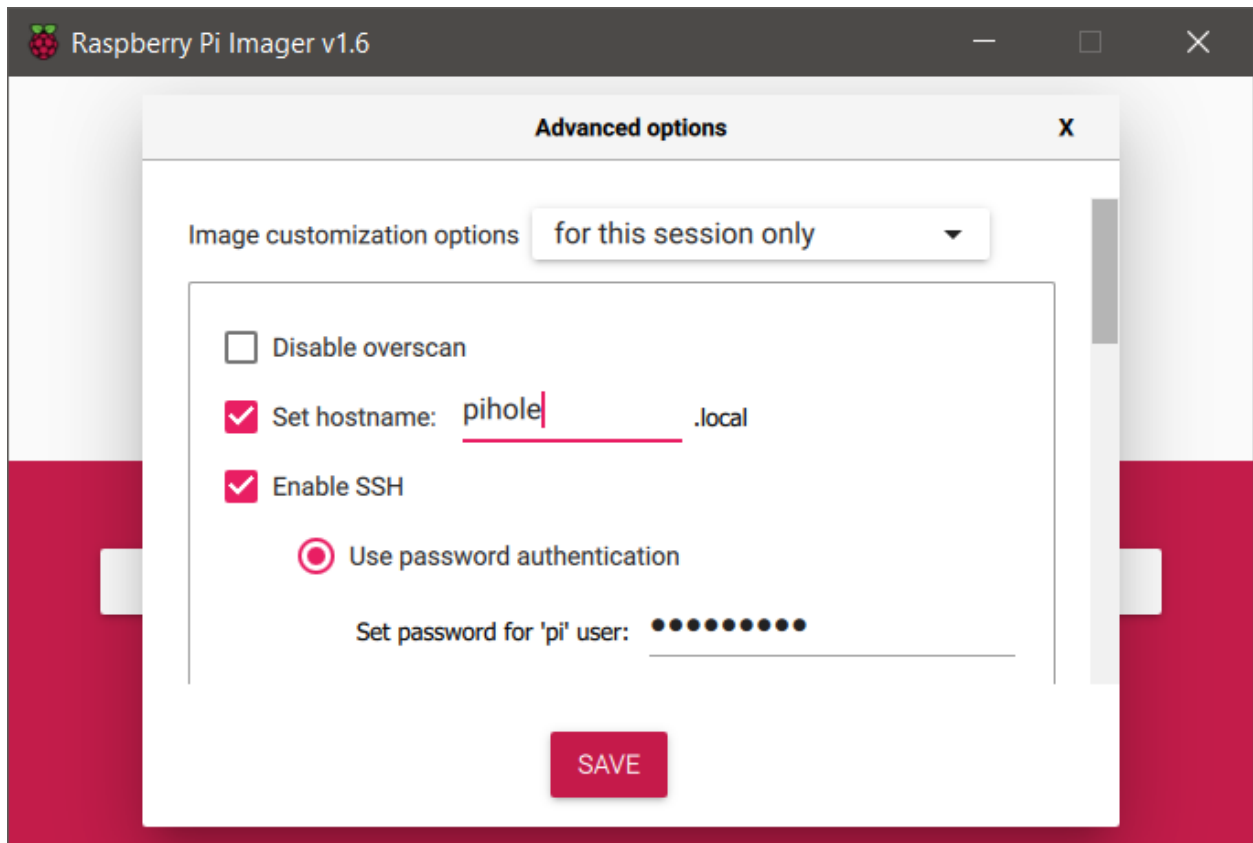
Information Systems Acquisition, Development and Implementation 18%

Information Systems Operations, Maintenance and Service Management 20%

Protection of Information Assets 25%

Chapter 5: Getting Hands-On Experience with No Experience







- Introduction >
- General >
- HTTP Basics
- HTTP Proxies
- Developer Tools
- CIA Triad
- Crypto Basics
- Writing new lesson
- (A1) Injection >
- (A2) Broken Authentication >
- (A3) Sensitive Data Exposure >
- (A4) XML External Entities (XXE) >
- (A5) Broken Access Control >
- (A7) Cross-Site Scripting (XSS) >
- (A8) Insecure Deserialization >
- (A9) Vulnerable Components >
- (A8:2013) Request Forgeries >
- Client side >
- Challenges >

HTTP Basics



Reset lesson



Concept

This lesson presents the basics for understanding the transfer of data between the browser and the web application and how to trap a request/response with a HTTP proxy.

Goals

The user should become familiar with the features of WebGoat by manipulating the above buttons to view hints, show the HTTP request parameters, the HTTP request cookies, and the Java source code. You may also try using [OWASP Zed Attack Proxy](#) for the first time.

How HTTP works:

All HTTP transactions follow the same general format. Each client request and server response has three parts: the request or response line, a header section and the entity body.

The client initiates a transaction as follows:

- The client contacts the server and sends a document request. A GET request can have url parameters and those parameters will be available in the web access logs.
 - GET /index.html?param=value HTTP/1.0
- Next, the client sends optional header information to inform the server of its configuration and the document formats it will accept.
 - User-Agent: Mozilla/4.06 Accept: image/gif,image/jpeg, /
- In a POST request, the user supplied data will follow the optional headers and is not part of the contained within the POST URL.



- Introduction >
- General >
- (A1) Injection >
- SQL Injection (intro)
- SQL Injection (advanced)
- SQL Injection (mitigation)
- Path traversal
- (A2) Broken Authentication >
- (A3) Sensitive Data Exposure >
- (A4) XML External Entities (XXE) >
- (A5) Broken Access Control >
- (A7) Cross-Site Scripting (XSS) >
- (A8) Insecure Deserialization >
- (A9) Vulnerable Components >
- (A8:2013) Request Forgeries >
- Client side >
- Challenges >

SQL Injection (intro)



Reset lesson



What is SQL injection?

SQL injections are the most common web hacking techniques. **A SQL injection attack consists of insertion or "injection" of malicious code via the SQL query input from the client to the application.** If not dealt with correctly, such an injection of code into the application can have an serious impact on e.g. data integrity and security.

SQL injections can occur, when unfiltered data from the client, e.g. the input of a search field, gets into the SQL interpreter of the application itself. If the input from the client does not get checked for containing SQL commands, hackers can easily manipulate the underlying SQL statement to their advantage.

Per example if the input is not filtered for SQL metacharacters like -- (comments out the rest of the line) or ; (ends a SQL query and that way can be used to chain them).

Example of SQL injection

Think of a web application, that allows to display user information, by typing a username into an input field.

The input will then be sent to the server and gets inserted into a SQL query which then is processed by an SQL interpreter.

The SQL query to retrieve the user information from the database looks like that:

```
"SELECT * FROM users WHERE name = '' + userName + ''";
```

The variable **userName** holds the input from the client and "injects" it into the query. If the input would be Smith the query then looks like that

```
"SELECT * FROM users WHERE name = 'Smith';
```

- Introduction >
- General >
- (A1) Injection >
- SQL Injection (intro)
- SQL Injection (advanced)
- SQL Injection (mitigation)
- Path traversal
- (A2) Broken Authentication >
- (A3) Sensitive Data Exposure >
- (A4) XML External Entities (XXE) >
- (A5) Broken Access Control >
- (A7) Cross-Site Scripting (XSS) >
- (A8) Insecure Deserialization >
- (A9) Vulnerable Components >
- (A8:2013) Request Forgeries >
- Client side >
- Challenges >

Show hints Reset lesson

1 2 3 4 5 6 7 8 9 10 11 12 13

Compromising Integrity with Query chaining

After compromising the confidentiality of data in the previous lesson, this time we are gonna compromise the **integrity** of data by using SQL **query chaining**.

The integrity of any data can be compromised, if an attacker per example changes information that he should not even be able to access.

What is SQL query chaining?

Query chaining is exactly what it sounds like. When query chaining, you try to append one or more queries to the end of the actual query. You can do this by using the ; metacharacter which marks the end of a query and that way allows to start another one right after it within the same line.

It is your turn!

You just found out that Tobi and Bob both seem to earn more money than you! Of course you cannot leave it at that.

Better go and *change your own salary so you are earning the most!*

Remember: Your name is John **Smith** and your current TAN is **3SL99A**.

Employee Name:

Authentication TAN:

MALWARE-TRAFFIC-ANALYSIS.NET

TRAFFIC ANALYSIS EXERCISES

- [2021-02-08](#) - Traffic analysis exercise - AscoLimited
- [2021-01-21](#) - Traffic analysis exercise - WokeMountain
- [2020-12-31](#) - Traffic analysis quiz - Pcaps for an ISC diary
- [2020-12-03](#) - Traffic analysis quiz - Pcap and alerts for an ISC diary
- [2020-11-13](#) - Traffic analysis exercise - QuietHub
- [2020-11-10](#) - Traffic analysis quiz - Pcap and alerts for an ISC diary
- [2020-10-22](#) - Traffic analysis exercise - Omegacast
- [2020-09-25](#) - Traffic analysis exercise - Trouble Alert
- [2020-09-14](#) - Traffic analysis quiz - Pcap and alerts for an ISC diary
- [2020-08-21](#) - Traffic analysis exercise - Pizza-Bender
- [2020-08-04](#) - Traffic analysis quiz - Pcap and alerts for an ISC diary
- [2020-07-31](#) - Traffic analysis exercise - TecSolutions
- [2020-06-12](#) - Traffic analysis exercise - Frank-n-Ted (What's going on?)
- [2020-05-28](#) - Traffic analysis exercise - Catbomber
- [2020-04-24](#) - Traffic analysis exercise - SteelCoffee
- [2020-03-14](#) - Traffic analysis exercise - Mondogreek
- [2020-02-21](#) - Traffic analysis exercise - All aboard the hot mess express!
- [2020-01-30](#) - Traffic analysis exercise - Sol-Lightnet
- [2019-12-25](#) - Traffic analysis exercise - It happened on Christmas day
- [2019-12-03](#) - Traffic analysis exercise - Icamaiden
- [2019-11-12](#) - Traffic analysis exercise - **Okay-boomer**
- [2019-10-05](#) - Traffic analysis exercise - Tinsolutions
- [2019-08-20](#) - Traffic analysis exercise - BadBundt
- [2019-07-19](#) - Traffic analysis exercise - So hot right now
- [2019-06-22](#) - Traffic analysis exercise - Phenomenoc
- [2019-05-02](#) - Traffic analysis exercise - BeguileSoft
- [2019-04-15](#) - Traffic analysis exercise - StingrayAhoy
- [2019-03-19](#) - Traffic analysis exercise - LittleTigers
- [2019-02-23](#) - Traffic analysis exercise - Stormtheory
- [2019-01-28](#) - Traffic analysis exercise - Timbershade
- [2018-12-26](#) - Two pcaps I provided for UA-CTF in November 2018
- [2018-12-18](#) - Traffic analysis exercise - Egnog soup
- [2018-11-13](#) - Traffic analysis exercise - Turkey and defence
- [2018-11-01](#) - Two pcaps I provided for UISGCON CTF in 2018
- [2018-10-31](#) - Traffic analysis exercise - Happy Halloween!
- [2018-09-27](#) - Traffic analysis exercise - Blank clipboard

2019-11-12-traffic-analysis-exercise.pcap

No.	Time	Source	Src Port	Destination	Dest Port	Protocol	CNameString	Info
156	19.327744	10.11.11.11		156 10.11.11.200		TCP		88 → 49161 [SYN, ACK]
157	19.327796	10.11.11.11		157 10.11.11.200		TCP		88 → 49160 [RST, ACK]
158	19.345827	10.11.11.200		158 10.11.11.11		TCP		49161 → 88 [ACK] Seq
159	19.346178	10.11.11.200		159 10.11.11.11		TCP		49161 → 88 [ACK] Seq
160	19.346243	10.11.11.200		160 10.11.11.11		KRB5		TGS-REQ
161	19.346271	10.11.11.11		161 10.11.11.200		TCP		88 → 49161 [ACK] Seq
162	19.347619	10.11.11.11		162 10.11.11.200		TCP		88 → 49161 [ACK] Seq
163	19.347621	10.11.11.11		163 10.11.11.200		KRB5	GILBERT-WIN7-	TGS-REP
164	19.350934	10.11.11.200		164 10.11.11.11		TCP		49161 → 88 [ACK] Seq
165	19.350935	10.11.11.200		165 10.11.11.11		TCP		49161 → 88 [FIN, ACK]
166	19.350997	10.11.11.11		166 10.11.11.200		TCP		88 → 49161 [ACK] Seq
167	19.351077	10.11.11.11		167 10.11.11.200		TCP		88 → 49161 [RST, ACK]
168	19.351263	10.11.11.200		168 10.11.11.11		TCP		49158 → 389 [ACK] Se
169	19.351351	10.11.11.200		169 10.11.11.11		LDAP		bindRequest(3) "<R00
170	19.351383	10.11.11.11		170 10.11.11.200		TCP		389 → 49158 [ACK] Se
171	19.352643	10.11.11.11		171 10.11.11.200		LDAP		bindResponse(3) succ
172	19.364131	10.11.11.200		172 10.11.11.11		LDAP		SASL GSS-API Integri

Frame 105: 68 bytes on wire (544 bits), 68 bytes captured (544 bits)

Ethernet II, Src: Dell_Ba:50:a9 (84:8f:69:8a:50:a9), Dst: Dell_80:a3:66 (00:14:22:80:a3:66)

Internet Protocol Version 4, Src: 10.11.11.200, Dst: 10.11.11.11

Transmission Control Protocol, Src Port: 49156, Dst Port: 135, Seq: 0, Len: 0

Source Port: 49156

Destination Port: 135

[Stream index: 0]

[TCP Segment Len: 0]

Sequence Number: 0 (relative sequence number)

Sequence Number (raw): 3081050339

[Next Sequence Number: 1 (relative sequence number)]

Acknowledgment Number: 0

Acknowledgment number (raw): 0

1000 ... = Header Length: 32 bytes (8)

Flags: 0x002 (SYN)

Window: 8192

[Calculated window size: 8192]

Checksum: 0x9313 [unverified]

0000 00 14 22 80 a3 66 84 8f 69 8a 50 a9 08 00 45 00 ... f . I . P . S . E .

0010 00 34 00 13 40 00 08 06 cf c8 0a 0b 0b c8 0a 0b ... 4 . @

0020 0b 0b c8 04 00 87 b7 a5 18 e3 00 00 00 88 02

0030 70 00 33 13 00 00 02 04 05 b4 01 03 03 08 01 01

0040 04 02 b5 2d

Destination Port (tcp.dstport), 2 bytes

Packets: 22828 - Displayed: 19615 (85.9%) Profile: Default

2019-11-12-traffic-analysis-exercise-answers.pdf

NOV 2019 TRAFFIC ANALYSIS EXERCISE ANSWERS

Link to exercise: <https://www.malware-traffic-analysis.net/2019/11/12/index.html>

Links to some tutorials I've written that should help with this exercise:

- Customizing Wireshark - Changing Your Column Display
- Using Wireshark: Identifying Hosts and Users
- Using Wireshark - Display Filter Expressions
- Using Wireshark: Exporting Objects from a Pcap

ENVIRONMENT FOR THE PCAP:

- LAN segment range: 10.11.11.0/24 (10.11.11.0 through 10.11.11.255)
- Domain: okay-boomer.info
- Domain controller: 10.11.11.11 - Okay-Boomer-DC
- LAN segment gateway: 10.11.1.1
- LAN segment broadcast address: 10.11.11.255

QUESTIONS:

- What operating system and type of device is on 10.11.11.94?
- What operating system and type of device is on 10.11.11.121?
- Based on the MAC address for 10.11.11.145, who is the manufacturer or vendor?
- What operating system and type of device is on 10.11.11.179?
- What version of Windows is being used on the host at 10.11.11.195?
- What is the user account name used to log into the Windows host at 10.11.11.200?
- What operating system and type of device is on 10.11.11.217?
- What IP is a Windows host that downloaded a Windows executable file over HTTP?
- What is the URL that returned the Windows executable file?
- What is the SHA256 file hash for that Windows executable file?
- What is the detection rate for that SHA256 hash on VirusTotal?
- What public IP addresses did that Windows host attempt to connect over TCP after the executable file was downloaded?
- What is the host name and Windows user account name used on that IP address?

Page 1 of 16

2019-11-12-traffic-analysis-exercise.pcap

ip.addr==10.11.11.94

No.	Time	Source	Src Port	Destination	Dest Port	Protocol	CNameString	Info
880	49.324095	10.11.11.94		880 10.11.11.11	880	DNS		Standard query 0x366
881	49.324241	10.11.11.94		881 10.11.11.11	881	DNS		Standard query 0x8ea
883	49.342415	10.11.11.94		883 10.11.11.11	883	DNS		Standard query 0xdcc
884	49.391855	10.11.11.11		884 10.11.11.94	884	DNS		Standard query respo
886	49.841700	10.11.11.94		886 10.11.11.11	886	DNS		Standard query 0x92a
887	49.841931	10.11.11.11		887 10.11.11.94	887	DNS		Standard query respo
888	49.851756	10.11.11.94		888 10.11.11.255	888	NBNS		Name query NBSTAT *<
893	50.345085	10.11.11.94		893 10.11.11.11	893	DNS		Standard query 0xdcc
894	50.345254	10.11.11.11		894 10.11.11.94	894	DNS		Standard query respo
896	50.824438	10.11.11.94		896 10.11.11.11	896	DNS		Standard query 0x8ea

Frame 880: 75 bytes on wire (600 bits), 75 bytes captured (600 bits)

Ethernet II, Src: HonHaiPr_d0:91:9d (38:b1:db:d0:91:9d), Dst: Dell_80:a3:66 (00:14:22:80:a3:66)

Internet Protocol Version 4, Src: 10.11.11.94, Dst: 10.11.11.11

User Datagram Protocol, Src Port: 56239, Dst Port: 53

Domain Name System (query)

```

0000  00 14 22 80 a3 66 38 b1 db d0 91 9d 00 00 45 00  ..".f8.....E.
0010  00 3d 75 af 40 00 40 11 9a 82 0a 0b 0b 5e 0a 0b  ..=u.@.....
0020  0b 0b db af 00 35 00 29 8c 65 36 60 01 00 00 01  .....5) ..e6'
0030  00 00 00 00 00 00 03 77 77 77 07 67 73 74 61 74  .....www.gstatic
0040  69 63 03 63 6f 6d 00 00 01 00 01                ..c.com.....

```

2019-11-12-traffic-analysis-exercise.pcap Packets: 22828 - Displayed: 758 (3.3%) Profile: Default

2019-11-12-traffic-analysis-exercise.pcap

ip.addr==10.11.11.94 && http

No.	Time	Source	Src Port	Destination	Dest Port	Protocol	Info
1192	63.989458	10.11.11.94		1192 216.58.194.35	1192	HTTP	GET /generate_204 HTTP/1.1
1194	64.008388	216.58.194.35		1194 10.11.11.94	1194	HTTP	HTTP/1.1 204 No Content
1203	64.383828	10.11.11.94		1203 216.58.194.35	1203	HTTP	GET /generate_204 HTTP/1.1
1205	64.406435	216.58.194.35		1205 10.11.11.94	1205	HTTP	HTTP/1.1 204 No Content
1253	66.465375	10.11.11.94		1253 216.58.194.35	1253	HTTP	GET /generate_204 HTTP/1.1
1258	66.489534	216.58.194.35		1258 10.11.11.94	1258	HTTP	HTTP/1.1 204 No Content
2362	91.205093	10.11.11.94		2362 64.98.145.30	2362	HTTP	GET / HTTP/1.1
2381	91.374999	64.98.145.30		2381 10.11.11.94	2381	HTTP	HTTP/1.1 303 See Other (text/html)
2385	91.703514	10.11.11.94		2385 216.58.194.35	2385	HTTP	GET /generate_204 HTTP/1.1
2389	91.734005	216.58.194.35		2389 10.11.11.94	2389	HTTP	HTTP/1.1 204 No Content
2602	94.765429	10.11.11.94		2602 52.218.228.130	2602	HTTP	GET /core/scripts/lrs/tin-can.min
3065	95.220143	52.218.228.130		3065 10.11.11.94	3065	HTTP	HTTP/1.1 200 OK (application/jav
3078	95.246355	10.11.11.94		3078 52.218.228.130	3078	HTTP	GET /templates/black-friday/black
3093	95.347073	52.218.228.130		3093 10.11.11.94	3093	HTTP	HTTP/1.1 200 OK (application/jav
3096	95.356485	10.11.11.94		3096 52.218.228.130	3096	HTTP	GET /templates/black-friday/snows
3114	95.478909	52.218.228.130		3114 10.11.11.94	3114	HTTP	HTTP/1.1 200 OK (application/jav
4734	120.743575	10.11.11.94		4734 216.58.194.35	4734	HTTP	GET /generate_204 HTTP/1.1
4735	120.774117	216.58.194.35		4735 10.11.11.94	4735	HTTP	HTTP/1.1 204 No Content
8469	148.714968	10.11.11.94		8469 216.58.194.35	8469	HTTP	GET /generate_204 HTTP/1.1
8471	148.733550	216.58.194.35		8471 10.11.11.94	8471	HTTP	HTTP/1.1 204 No Content
13313	193.044421	10.11.11.94		13313 216.58.194.35	13313	HTTP	GET /generate_204 HTTP/1.1

Frame 1203: 347 bytes on wire (2776 bits), 347 bytes captured (2776 bits)

Ethernet II, Src: HonHaiPr_d0:91:9d (38:b1:db:d0:91:9d), Dst: Cisco_97:4b:f0 (00:01:c9:97:4b:f0)

Internet Protocol Version 4, Src: 10.11.11.94, Dst: 216.58.194.35

Transmission Control Protocol, Src Port: 59848, Dst Port: 80, Seq: 1, Ack: 1, Len: 281

Hypertext Transfer Protocol

GET /generate_204 HTTP/1.1\r\n

Host: www.gstatic.com\r\n

Connection: keep-alive\r\n

Pragma: no-cache\r\n

Cache-Control: no-cache\r\n

User-Agent: Mozilla/5.0 (X11; CrOS x86_64 12239.92.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3809.136 Safari/537.36\r\n

Accept-Encoding: gzip, deflate\r\n

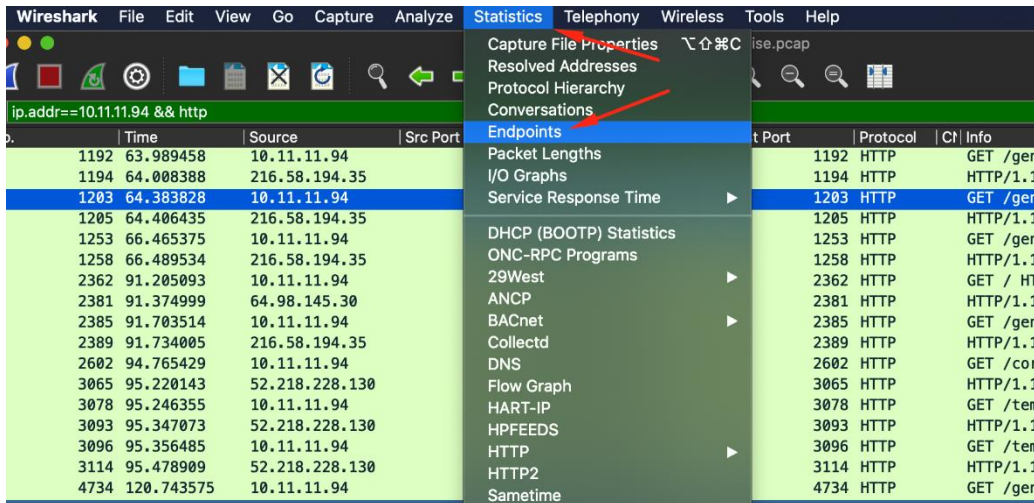
\r\n

[Full request URI: http://www.gstatic.com/generate_204]

[HTTP request 1/6]

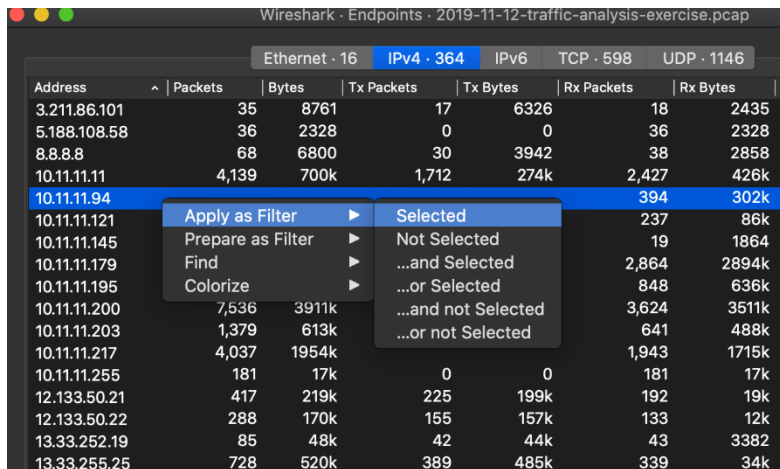
[Response in frame: 1205]

[Next request in frame: 1253]



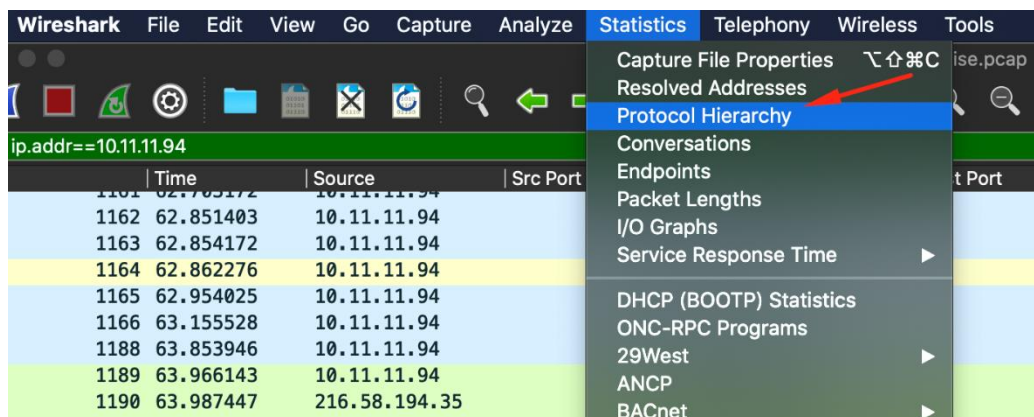
The screenshot shows the Wireshark Statistics menu with 'Endpoints' selected. The main window displays a packet list filtered by 'ip.addr==10.11.11.94 && http'. The packet list table is as follows:

No.	Time	Source	Src Port	Destination	Port	Protocol	Info
1192	63.989458	10.11.11.94				HTTP	GET /gen
1194	64.008388	216.58.194.35				HTTP	HTTP/1.1
1203	64.383828	10.11.11.94				HTTP	GET /gen
1205	64.406435	216.58.194.35				HTTP	HTTP/1.1
1253	66.465375	10.11.11.94				HTTP	GET /gen
1258	66.489534	216.58.194.35				HTTP	HTTP/1.1
2362	91.205093	10.11.11.94				HTTP	GET / HT
2381	91.374999	64.98.145.30				HTTP	HTTP/1.1
2385	91.703514	10.11.11.94				HTTP	GET /gen
2389	91.734005	216.58.194.35				HTTP	HTTP/1.1
2602	94.765429	10.11.11.94				HTTP	GET /cor
3065	95.220143	52.218.228.130				HTTP	HTTP/1.1
3078	95.246355	10.11.11.94				HTTP	GET /tem
3093	95.347073	52.218.228.130				HTTP	HTTP/1.1
3096	95.356485	10.11.11.94				HTTP	GET /tem
3114	95.478909	52.218.228.130				HTTP	HTTP/1.1
4734	120.743575	10.11.11.94				HTTP	GET /gen



The screenshot shows the 'Endpoints' statistics window in Wireshark. The 'IPv4' tab is selected, showing a table of IP addresses and their associated traffic statistics. A context menu is open over the IP address 10.11.11.94.

Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes
3.211.86.101	35	8761	17	6326	18	2435
5.188.108.58	36	2328	0	0	36	2328
8.8.8.8	68	6800	30	3942	38	2858
10.11.11.11	4,139	700k	1,712	274k	2,427	426k
10.11.11.94					394	302k
10.11.11.121					237	86k
10.11.11.145					19	1864
10.11.11.179					2,864	2894k
10.11.11.195					848	636k
10.11.11.200	7,536	391k			3,624	3511k
10.11.11.203	1,379	613k			641	488k
10.11.11.217	4,037	1954k			1,943	1715k
10.11.11.255	181	17k	0	0	181	17k
12.133.50.21	417	219k	225	199k	192	19k
12.133.50.22	288	170k	155	157k	133	12k
13.33.252.19	85	48k	42	44k	43	3382
13.33.255.25	728	520k	389	485k	339	34k



The screenshot shows the Wireshark Statistics menu with 'Protocol Hierarchy' selected. The main window displays a packet list filtered by 'ip.addr==10.11.11.94'. The packet list table is as follows:

No.	Time	Source	Src Port	Destination	Port	Protocol	Info
1161	62.795172	10.11.11.94					
1162	62.851403	10.11.11.94					
1163	62.854172	10.11.11.94					
1164	62.862276	10.11.11.94					
1165	62.954025	10.11.11.94					
1166	63.155528	10.11.11.94					
1188	63.853946	10.11.11.94					
1189	63.966143	10.11.11.94					
1190	63.987447	216.58.194.35					

Wireshark - Protocol Hierarchy Statistics - 2019-11-12-traffic-analysis-exerc

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	
▼ Frame	100.0	758	100.0	35050	
▼ Ethernet	100.0	758	3.0	10612	
▼ Internet Protocol Version 4	100.0	758	4.3	15168	
▼ User Datagram Protocol	25.9	196	0.4	1568	
Simple Service Discovery Protocol	1.1	8	0.4	1408	
NetBIOS Name Service	0.3	2	0.0	100	
Multicast Domain Name System	3.3	25	0.4	1419	
GQUIC (Google Quick UDP Internet Connections)	5.8	44	6.0	21137	
Domain Name System	15.4	117	2.1	7213	
▼ Transmission Control Protocol	73.9	560	83.2	29144	
Transport Layer Security	18.9	143	36.2	12694	
▼ Hypertext Transfer Protocol	22	22	46.5	16296	
Media Type	Apply as Filter ▶	Selected	3	44.8	15692
Line-based	Prepare as Filter ▶	Not Selected	1	0.0	97
Internet Group Management Protocol	Find	...and Selected	2	0.0	32
	Colorize	...or Selected			
	Copy as CSV	...and not Selected			
	Copy as YAML	...or not Selected			

2019-11-12-traffic-analysis-exercise.pcap

(ip.addr==10.11.11.94) && (http)

No.	Time	Source	Src Port	Destination	Dest Port	Protoc
1192	63.989458	10.11.11.94	1192	216.58.194.35	1192	HTTP
1194	64.008388	216.58.194.35	1194	10.11.11.94	1194	HTTP
1203	64.383828	10.11.11.94	1203	216.58.194.35	1203	HTTP
1205	64.406435	216.58.194.35	1205	10.11.11.94	1205	HTTP
1253	66.465375	10.11.11.94	1253	216.58.194.35	1253	HTTP
1258	66.489534	216.58.194.35	1258	10.11.11.94	1258	HTTP
2362	91.205093	10.11.11.94	2362	64.98.145.30	2362	HTTP
2381	91.374999	64.98.145.30	2381	10.11.11.94	2381	HTTP
2385	91.703514	10.11.11.94	2385	216.58.194.35	2385	HTTP
2389	91.734005	216.58.194.35	2389	10.11.11.94	2389	HTTP
2602	94.765429	10.11.11.94	2602	52.218.228.130	2602	HTTP
3065	95.220143	52.218.228.130	3065	10.11.11.94	3065	HTTP
3078	95.246355	10.11.11.94	3078	52.218.228.130	3078	HTTP
3093	95.347073	52.218.228.130	3093	10.11.11.94	3093	HTTP
3096	95.356485	10.11.11.94	3096	52.218.228.130	3096	HTTP
3114	95.478909	52.218.228.130	3114	10.11.11.94	3114	HTTP

```
Wireshark · Follow TCP Stream (tcp.stream eq 41) · 2019-11-12-traffic-analysis-exercise.pcap

GET /generate_204 HTTP/1.1
Host: www.gstatic.com
Connection: keep-alive
Pragma: no-cache
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (X11; CrOS x86_64 12239.92.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3809.136 Safari/537.36
Accept-Encoding: gzip, deflate

HTTP/1.1 204 No Content
Content-Length: 0
Date: Mon, 11 Nov 2019 22:21:08 GMT

GET /generate_204 HTTP/1.1
Host: www.gstatic.com
Connection: keep-alive
Pragma: no-cache
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (X11; CrOS x86_64 12239.92.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3809.136 Safari/537.36
Accept-Encoding: gzip, deflate

HTTP/1.1 204 No Content
Content-Length: 0
Date: Mon, 11 Nov 2019 22:21:10 GMT

GET /generate_204 HTTP/1.1
Host: www.gstatic.com
Connection: keep-alive
Pragma: no-cache
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (X11; CrOS x86_64 12239.92.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3809.136 Safari/537.36
Accept-Encoding: gzip, deflate

HTTP/1.1 204 No Content
Content-Length: 0
Date: Mon, 11 Nov 2019 22:21:35 GMT

GET /generate_204 HTTP/1.1
Host: www.gstatic.com
Connection: keep-alive
Pragma: no-cache
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (X11; CrOS x86_64 12239.92.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3809.136 Safari/537.36
Accept-Encoding: gzip, deflate
```

DEF CON

-welcome_to_the_defcon

DEF CON bot #3 04/12/2021

Hi @sluj12,

Welcome to the official DEF CON Discord Server.

By connecting you agree to the rules which can be found in [#{#-rules}](#).

You will receive a direct message from our bot (YAGPDB.xyz ID: 204255221017214977).

You have a limited amount of time to complete the reCAPTCHA.

Our Code of Conduct <https://defcon.org/html/links/dc-code-of-conduct.html> is our over-arching set of principles.

Welcome to the DEF CON server!

[DEF CON® Hacking Conference - Code of Conduct](#)

Code of Conduct for DEF CON Hacking Conference

Hi @dr.g,

Welcome to the official DEF CON Discord Server.

By connecting you agree to the rules which can be found in [#{#-rules}](#).

You will receive a direct message from our bot (YAGPDB.xyz ID: 204255221017214977).

You have a limited amount of time to complete the reCAPTCHA.

Our Code of Conduct <https://defcon.org/html/links/dc->

TALOS

Software Vulnerability Information Reputation Center Library Support Incident Response Careers

Talos Threat Source Newsletters

Talos Threat Source is a regular intelligence update from Cisco Talos, highlighting the biggest threats each week and other security news.

April 29, 2021

TALOS

THREAT SOURCE NEWSLETTER

All the security news you need to know

●● Medium


Where ideas take shape before they take off.

If you have a story to tell, knowledge to share, or a perspective to offer — welcome home. It's easy and free to post your thinking on any topic, whether it's a standalone piece, a blog, or a publication with other writers. And with tools that let you express yourself creatively and connect with a growing audience of 170 million readers, you'll have the chance to plant a seed, or even start a movement.

[Start writing](#) [Explore publishing tools](#)

<h3>Share your ideas.</h3> <p>Write about what matters to you, and give form to anything from a quick thought to a long story.</p>	<h3>Build an audience.</h3> <p>Find and engage with readers who care about what you have to say — and want to read more of it.</p>
--	--

Chapter 6: Time to Brand Yourself – Not the Burning Type

 **Jaclyn (Jax) Scott**
Founder ■ Managing Partner ■ Podcaster ■ Cyber Expert ■ Tech Blo...
1mo · 🌐


This is the second law enforcement intervention to remove malware from compromised machines without users notifications.

The first reporting happened around April 13th. I shared an article about the FBI having a court-approved order to remove web shells from compromised US-based Microsoft Exchange services without first notifying the servers' owners. Article: <https://lnkd.in/ehTyUaK>

Anyone else concerned about privacy? What cyber law covers this type of intervention?

[Josh Jackson](#) this is your lane. Can you shine some light on privacy versus security and the law which supports agencies intervening without organization's approval?

[#privacy](#) [#cybersecurity](#) [#technology](#)
<https://lnkd.in/ekDZHJq>



Emotet Malware Destroys Itself From All Infected Computers
thehackernews.com · 3 min read



← **DivaBytes777**
29 Tweets



DivaBytes777
@bytes777

Cyber Nerd, Tech Blogger, CTI Ninja (Self Proclaimed), Podcaster (Hackerz and Haecksen), Pizza lover. Find me on LinkedIn: [linkedin.com/in/iamjax/](https://www.linkedin.com/in/iamjax/).

📅 Joined July 2020

43 Following **48** Followers

Tweets Tweets & replies Media Likes

[Edit profile](#)





Instagram

Search



theycybersecurityhub

Follow



4,167 posts 314k followers 1 following

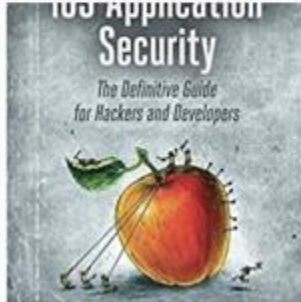
The Cyber Security Hub™
World's Premier Cyber Security Portal™

🔥 Face mask 📌

csh.creator-spring.com/listing/face-mask-binary

Followed by [julielikescoffee](#)

POSTS IGTV TAGGED





"Hi, Their Name

I love what you are doing at X Company. I am looking to connect with people like you to build a network of like-minded people supporting each other. It would be great to connect with you.

Enjoy your day,
Your Name"

PREMIUM



Sara Blakely 

Founder and CEO of SPANX

Followers 1,231,593

Unfollow

 **Sara Blakely**  · Following ⋮

Founder and CEO of SPANX
1mo · Edited · 

Remember the arrow must be pulled back in order to spring forward. Often when life is dragging us down with problems and dark times it's easy to feel defeated. But what if we flipped that thought on its head? When you're going t...see more






49,838 · 2,707 comments

SUBSCRIBE FOR WEEKLY VIDEOS



SIMPLY CYBER

MAKE AND TAKE YOUR CYBER CAREER FURTHER, FASTER








Gerald Auger - Simply Cyber
8.16K subscribers

SUBSCRIBE

HOME

VIDEOS

PLAYLISTS

COMMUNITY

CHANNELS

ABOUT



About Simply Cyber Channel (45 sec Trail... 



0:02 / 0:55

About Simply Cyber Channel (45 sec Trailer)

1,937 views · 1 year ago

Simply Cyber is an information security YouTube channel designed to help individuals go further, faster in the information security field.

I'm Gerald Auger, a full time cyber security professional with a passion for the field. The field is collaborative in nature, and I would like to help others successfully drive their career.

READ MORE



Gerald Auger - Simply Cyber

8.16K subscribers

SUBSCRIBE

HOME

VIDEOS

PLAYLISTS

COMMUNITY

CHANNELS

ABOUT



Description

✦ About Simply Cyber ✦

New Episodes every Monday at 12:00 EST

Simply Cyber brings Information security related content to help IT or Information Security professionals take their career further, faster. Current cyber security industry topics and techniques are explored to promote a career in the field. Topics cover offense, defense, governance, risk, compliance, privacy, education, certification, conferences; all with the intent of professional development.

♥ LET'S CONNECT ♥

Twitter: @Gerald_Auger https://twitter.com/Gerald_Auger

LinkedIn: www.linkedin.com/in/geraldauger

Twitch: https://www.twitch.tv/gerald_auger_simplycyber/about

Discord: <https://discord.gg/C8mtwCPuXq>

👕 Loving SimplyCyber?

➡ Check out SimplyCyber Branded Gear at TeeSpring: <https://teespring.com/stores/simplycyber>

🔥 SUBSCRIBE TO SIMPLY CYBER ON YOUTUBE

Subscribe <https://www.youtube.com/c/geraldauger>

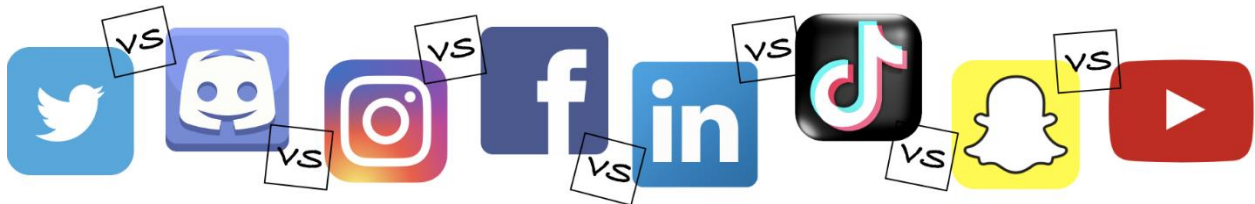
Stats

Joined Oct 2, 2011

154,380 views



Clubhouse
Drop-in Audio





Get unlimited access to everything on Medium

Plans starting at less than \$1/week. Cancel anytime.

- ✓ No ads
- ✓ Support quality writing
- ✓ Access on any device

Monthly
\$5/month

Annual
\$50/year (save \$10)

Chapter 7: How to Land a Jay-Oh-Bee!



CYBERSECURITY SUPPLY/DEMAND HEAT MAP

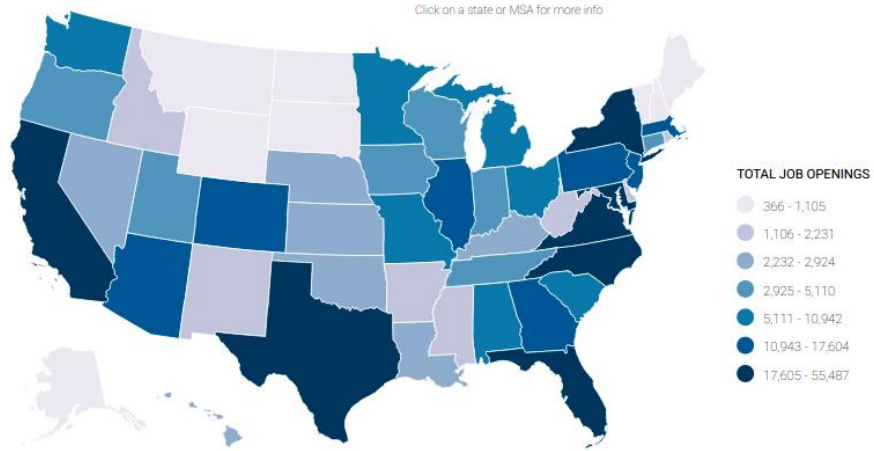
- All
- Public Sector Data
- Private Sector...
- Total job openings

States Metro Areas Search State 🔍

Cybersecurity talent gaps exist across the country. Closing these gaps requires detailed knowledge of the cybersecurity workforce in your region. This interactive heat map provides a granular snapshot of demand and supply data for cybersecurity jobs at the state and metro area levels, and can be used to grasp the challenges and opportunities facing your local cybersecurity workforce.

Share

Embed



National level

TOTAL CYBERSECURITY JOB OPENINGS ⓘ

464,420

TOTAL EMPLOYED CYBERSECURITY WORKFORCE ⓘ

956,341

SUPPLY OF CYBERSECURITY WORKERS ⓘ

Very Low

CYBERSECURITY WORKFORCE SUPPLY/DEMAND RATIO



GEOGRAPHIC CONCENTRATION ⓘ

Average

LOCATION QUOTIENT



TOP CYBERSECURITY JOB TITLES ⓘ

- Cyber Security Analyst
- Cyber Security Consultant
- Cyber Security Manager / Administrator
- Software Developer / Engineer
- Systems Engineer
- Network Engineer / Architect
- Vulnerability Analyst / Penetration Tester
- Cyber Security Specialist / Technician
- Incident Analyst / Responder

Most relevant

Any Time

25 mi (40 km)

Company

Salary

Location

Job Type

Experience Level

Turn on job alerts

off

720 Network Security Engineer Jobs in Seattle, Washington, United States (22 new)



Application Security Engineer

Protego Trust

Greater Seattle Area

Be an early applicant

4 weeks ago · [Apply Now](#)



Security Engineer

Highspot

Seattle, WA

Actively Hiring

4 days ago



Systems Engineer with Security Clearance

ClearanceJobs

Seattle, WA

Be an early applicant

1 month ago



Senior Forensic Structural Engineer, SE

Client Growth Resources

Seattle, WA

Be an early applicant

2 days ago



Staff Product Security Engineer

Flexport

Bellevue, WA

Be an early applicant

4 days ago



Senior Field Solution Architect - Network Security

CDW

Seattle, WA

Be an early applicant

5 days ago



Systems Engineer II

Verisk Financial

Bellevue, WA

Be an early applicant

3 weeks ago · [Apply Now](#)



Security Operations Engineer

Amazon

Seattle, WA

Be an early applicant

7 days ago



Security Engineer, Cloud Enterprise Infrastructure Protection Security

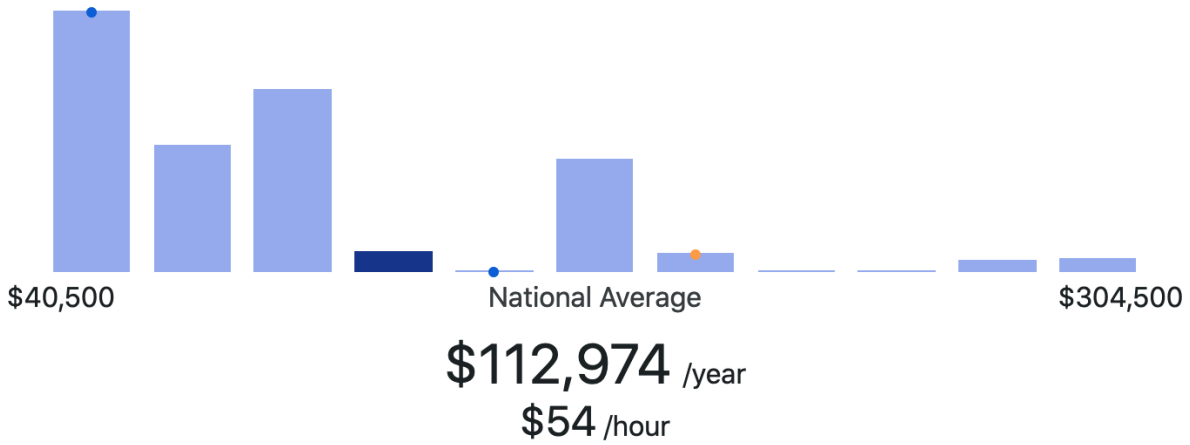
Google

Kirkland, WA

Be an early applicant

6 days ago

Yearly Monthly Weekly Hourly Table View



Cyber Security Salary Comparison by Location

Nationwide United States	\$112,974
Seattle, WA Washington	\$122,646

☰ > **Cyber Security Salaries** Austin, TX ▾

Overview Salaries Interviews Career Path

How much does a Cyber Security make in Austin, TX?

Industry Computer Software & Hardware ▾	Employer Size 51 to 200 Employees ▾	Experience 1-3 Years ▾
--	--	---------------------------

🟢 Very High Confidence

\$102,346 /yr

Average Base Pay

45 salaries

Not enough reports to show salary distribution






\$74K
Low

\$142K
High

No additional cash compensation has been reported for this role

The average salary for a Cyber Security is \$102,346 in Austin, TX. Salaries estimates are based on 45 salaries submitted anonymously to Glassdoor by Cyber Security employees in Austin, TX.

- Austin, TX Area or Sort: **Most Reports** ^

Company	Average Base Salary in (USD)
 IBM Cyber Security Engineer - Hourly Intern 3.9 ★ 2 salaries See 10 salaries from all locations	About \$21 - \$33 hourly
 General Motors (GM) Cyber Security Engineer 4 ★ 2 salaries See 5 salaries from all locations	About \$78K - \$95K \$78K \$95K
 Hewlett Packard Enterprise HPE Cyber Security Engineer 4 ★ 2 salaries See 3 salaries from all locations	About \$80K - \$130K \$80K \$130K
 Praetorian Cyber Security Engineer 4.5 ★ 2 salaries See 2 salaries from all locations	About \$100K - \$109K \$100K \$109K
 Texas Department of Public Safety Cyber Security Analyst 3.7 ★ 2 salaries See 2 salaries from all locations	About \$73K - \$92K \$73K \$92K

Sort: **Most Reports** ^

- Popular
- Most Reports**
- Salary: high ...
- Salary: low t...

Impact of organization's industry on the salary.

Banking and Finance



38%	● Under \$50K	4%	● \$111K-\$130K
22%	● \$51K-\$70K	2%	● \$131K-\$150K
24%	● \$71K-\$90K	2%	● \$271K-\$290K
8%	● \$91K-\$110K		

Healthcare



33%	● Under \$50K	17%	● \$91K-\$110K
17%	● \$51K-\$70K	17%	● \$111K-\$130K
17%	● \$71K-\$90K		

Industrial



56%	● Under \$50K	19%	● \$91K-\$110K
13%	● \$51K-\$70K	6%	● \$111K-\$130K
6%	● \$71K-\$90K		

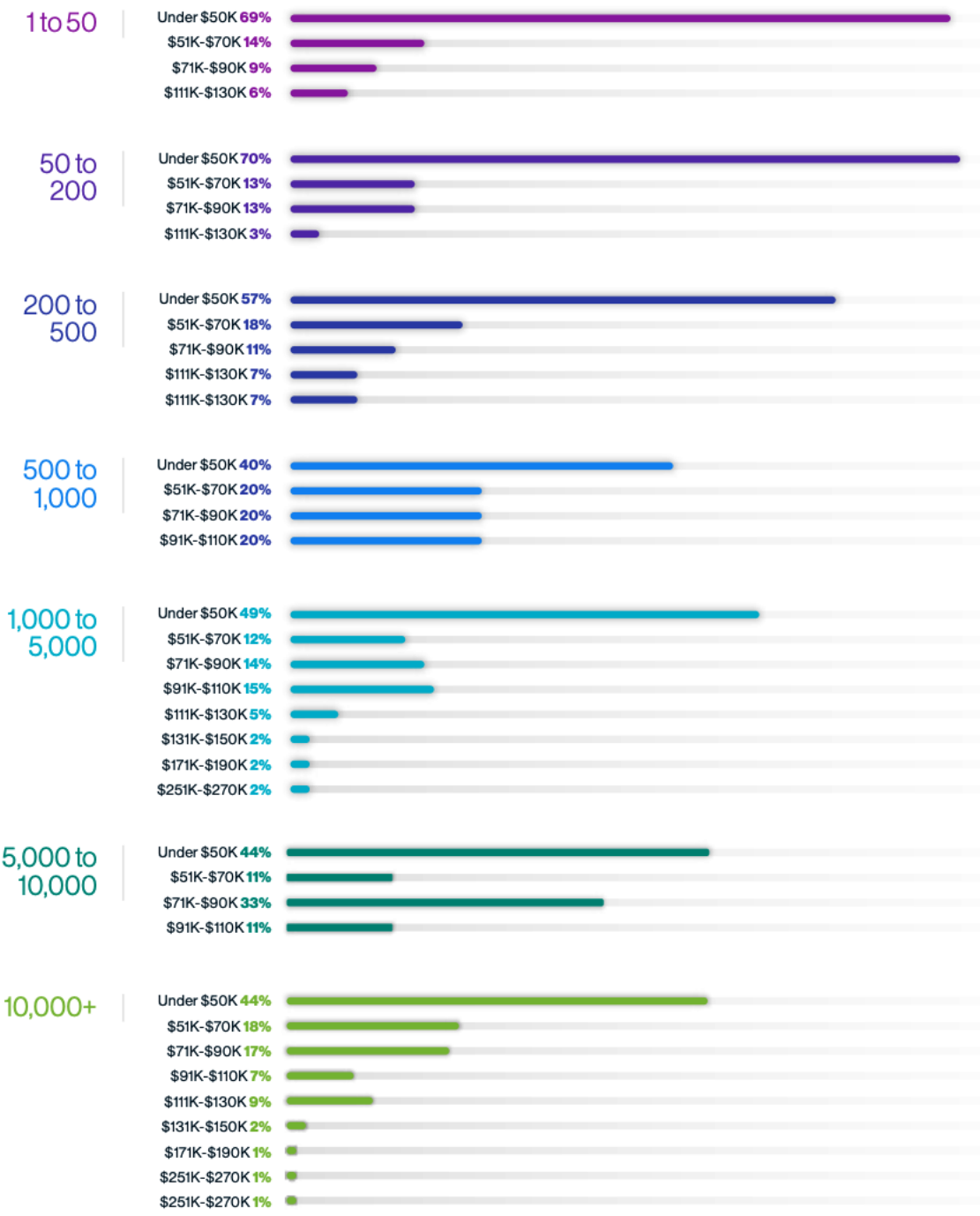
Retail



42%	● Under \$50K	17%	● \$71K-\$90K
33%	● \$51K-\$70K	8%	● \$91K-\$110K



Impact of organization's size on the salary.



SALARY FACTORS / INDIVIDUAL

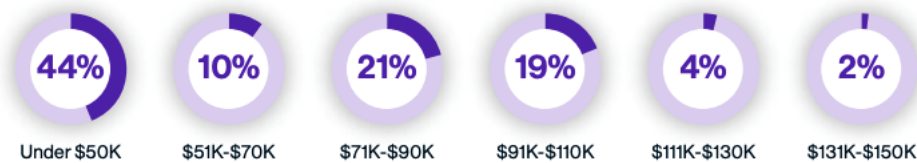
Experience

Impact of number of years in security position on the salary.

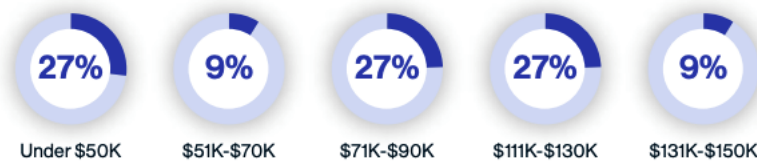
1-3 years



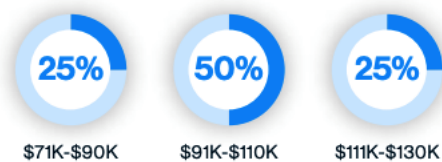
4-8 years



9-15 years



16 or more years

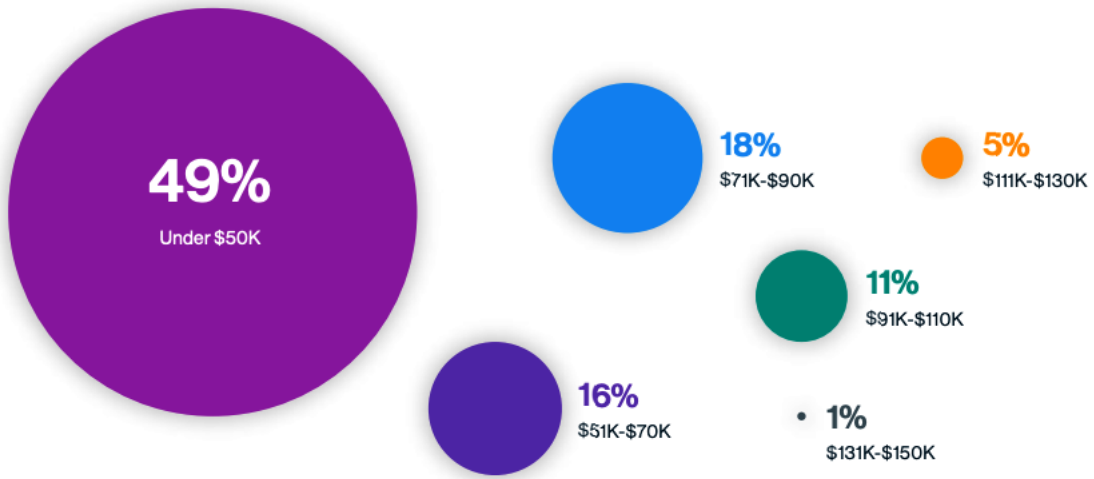


Certification

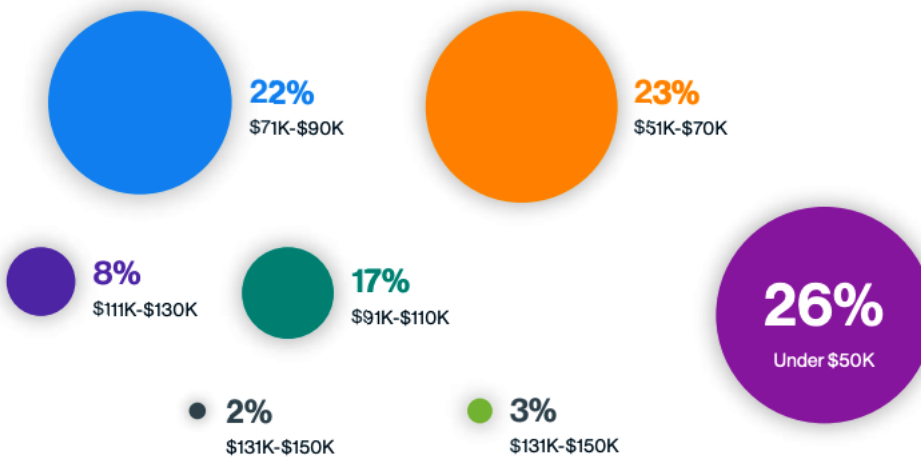
Security Analyst/
Threat Intelligence Expert 

Impact of academic degree in CS/engineering on the salary.

Academic Degree



No Academic Degree





best companies to work for



[All](#) [News](#) [Books](#) [Videos](#) [Shopping](#) [More](#) [Settings](#) [Tools](#)

About 25,270,000,000 results (0.71 seconds)

<https://fortune.com> › best-companies

100 Best Companies to Work For | Fortune

Top 10. 1Cisco. 2Salesforce. 3Hilton. 4Wegmans Food Markets. 5Rocket Companies. 6UKG. 7Texas Health Resources. 8Camden Property Trust. [Best Big Companies · 2017 · 2020 · 2016](#)

<https://www.glassdoor.com> › Award › Best-Places-to-W...

Best Places to Work | Glassdoor

Employees have spoken! Here are the Best Places to Work in 2021, according to employees. Did your company make it?

People also ask

What are the most fun companies to work for?



What are the best companies to work for in the Philippines?



What companies give the best benefits?



[Feedback](#)

<https://www.greatplacetowork.com> › Recent Lists

Fortune 100 Best Companies to Work For® 2021 | Great Place ...

Top 10

1 Cisco

2 Salesforce

3 Hilton

4 Wegmans Food Markets

5 Rocket Companies

6 UKG

7 Texas Health Resources

8 Camden Property Trust

9 Capital One Financial

10 American Express

A list

Security Engineer

Cloud Engineer

B list

Security Architect

Cybersecurity Analyst

Penetration Tester

C list

Network Engineer

Cybersecurity Consultant

Software Engineer

IT Support

Requirements:

- At least 4 years experience in an IT or security function, with at least 2 years of hands-on experience in a penetration testing role
- Experience with Python, PowerShell, or similar scripting language
- Experience using industry standard offensive security tools
- You have proven experience pen testing in web applications, network, wifi and cloud computing solution (AWS, GCP, Kubernetes)
- You have a proficiency with enterprise operating systems, including Linux and Windows
- You have practical experience with assessing encryption, IAM systems, VPN and authentication technologies
- You have extensive knowledge of TCP/IP networking and packet analysis
- You pride yourself on your proven attention to detail
- Excellent, efficient problem-solving skills
- Strong familiarity with at least one of the following: OWASP Top 10, PTES, or NSA Vulnerability and Penetration Testing Standards
- Experience facilitating penetration testing efforts in one or more of the following: Compliance frameworks (FedRAMP, PCI, SOCII, HIPAA)

Nice-to-haves:

- You have professional-level certifications (OSCP, GPEN, GWAPT, GXPN)
- Experience with higher-level programming languages (C, C++, etc.)
- Experience with API penetration testing
- Experience with containerization offensive techniques
- Exploit development, vulnerability research, bug bounty submissions

Education

- Bachelor's degree in a related field is desired, not required.
- DCSP, CEH, Security+ or other security related certifications is desired, not required. Experience:
- 8+ years of experience in information technology, preference to those with development, network, or systems administration experience.
- 6+ years of Penetration Testing

Experience

- 2+ years coding experience.
- Experience with at least three automation and scripting languages (e.g. PowerShell, BASH, Python).
- Experience and understanding of HIPAA, HITECH, and PCI preferred.
- Capture the Flag experience a plus.
- Bug bounty experience a plus.

Knowledge And Skills

- Basic knowledge and understanding of at least six computer programming language (e.g. JavaScript, .NET, AngularJS, Java, HTML, Assembly).
- Effective verbal and written communication skills. Should be able to adapt communication style to suit different audiences.
- Proficient with testing tools such as Burp, ZAP, OpenVAS, Impactor, CME, Wireshark, HackRF, or Metasploit.
- Ability to setup a virtual environment using VMware, Virtual Box, or similar technology.
- Understanding of password cracking and encryption technology.
- Familiarity with exploit development and tool development.

Bachelor's degree in computer science, information assurance, or related technical field or equivalent. At least 7 years' experience in information security administration, offensive tactics, monitoring and IR. At least 3 years' dedicated experience conducting penetration testing/red team engagements as a consultant or previous role in a professional organization. Proficient in scripting languages such as Python, PowerShell, Bash and Ruby. Competent with testing frameworks and tools such as Burp Suite, Metasploit, Cobalt Strike, Kali Linux, Nessus, PowerShell Empire and AutoSploit. Strong operating system knowledge across *nix, and Windows; proficient with networking protocols. Ability to obtain and maintain persistence within corporate systems, while avoiding detection. Familiarity with defensive and monitoring technologies such as intrusion prevention/detection systems (IPS/IDS), security information and event management systems (SIEMs), firewalls, endpoint protection (EPP) and endpoint detection/response (EDR) tools, as well as user and entity behavior analytics (UEBA). Understanding of OWASP, the MITRE ATT&CK framework and the software development life cycle (SDLC).

Preferred Skills

Current certifications such as OSCP, OSCE, CEH, GPEN, GWAPT, CREST, CISSP or other relevant certification. Self-starter requiring minimal supervision. Highly organized and efficient. Excellence in communicating business risk and remediation requirements from assessments. Analytical and problem-solving mindset. Demonstrates strategic and tactical thinking, along with decision-making skills and business acumen.

- Experience performing internal and external assessments
- Experience in leading a team during penetration tests
- Knowledge of server (Linux, Windows) and client (Windows, OS X, Linux) operating systems
- Knowledge and understanding of attack surfaces for enterprise systems and services
- Experience in at least one of PHP/Hack, Python, C/C++, Go or Java
- Experience working in cross-functional programs
- Experience translating technical concepts into language that is understood to audiences including software engineers, business and technical leaders
- 5+ years of experience practicing application security assessments and penetration tests
- Experience performing and leading whitebox and blackbox style assessments
- Experience with complex, multi-stage, multi-person pentests for new internal customers or external vendors
- Networking knowledge, including network virtualization technologies and ideally IPv6

Search and apply for jobs

Resume scanned

- By machine
- By human

Phone interview

In-person interviews

- Technical interview
- Behavioral interview

Getting hired/rejected

← → ↻ usajobs.gov 🔍 ☆

Explore Hiring Paths

The Federal Government offers unique hiring paths to help hire individuals that represent our diverse society. Learn more about each hiring path and your eligibility.

 Open to the Public U.S. citizens, nationals or those who owe allegiance to the U.S.	 Federal Employees Current or former, includes the competitive and excepted services
 Veterans	 Military Spouses
 National Guard & Reserves Current or prospective members	 Students & recent graduates
 Senior Executives	 Individuals with a disability
 Family of overseas employees	 Native Americans American Indian or Alaskan Native
 Peace Corps & AmeriCorps VISTA	 Special authorities

← → C linkedin.com/salary/

SALARY

security+engineer Seattle, Washington, United States Search

Security Engineer salaries
Greater Seattle Area

Base salary
\$120,000/yr
Range: \$90,400 - \$140,000

Median: \$120,000

See more insights

5,554 company results for "security+engineer"

	Expedia Group Security Engineer salaries Greater Seattle Area	\$116,000/yr Range: \$96,500 - \$140,000
	Tata Consultancy Services Security Engineer salaries Greater Seattle Area	\$97,100/yr Range: \$64,600 - \$146,000
	Amazon Security Engineer salaries Greater Seattle Area	\$114,000/yr Range: \$79,400 - \$164,000

payscale.com/research/US/Job=Cyber_Security_Analyst/Salary

Average Cyber Security Analyst Salary

How should I pay? What am I worth?

Price a Job Find market worth

Pay Skills Job Listings Employers

\$76,575 / year ▼
Avg. Base Salary (USD)

10% \$53k MEDIAN \$77k 90% \$117k

The average salary for a Cyber Security Analyst is \$76,575

Based on 2,985 salary profiles (last updated Jun 02 2021)

Base Salary	\$53k - \$117k	<input type="range"/>
Bonus	\$1k - \$12k	<input type="range"/>
Profit Sharing	\$508 - \$12k	<input type="range"/>
Commission	\$0 - \$15k	<input type="range"/>
Total Pay	\$50k - \$119k	<input type="range"/>

Is Average Cyber Security Analyst Salary your job title? Find out what you should be paid
Use our tool to get a personalized report on your market worth. [What's this?](#)

Location:
Seattle, Washington
United States (change)

Years in Field/Career:

Find your market worth »





How it works:

- 1 Enter city & years of experience
- 2 Add pay factors like skills & education
- 3 Find your market worth with a report tailored to you

Chapter 8: Giving Back to Others and Yourself



Chapter 9: Trusting the Process

S	Specific	Make your goals specific and narrow for more effective planning.	
M	Measureable	Define what evidence will prove you're making progress and reevaluate when necessary.	
A	Attainable	Make sure you can reasonably accomplish your goal within a certain timeframe.	
R	Relevant	Your goals should align with your values and long-term objectives.	
T	Time-based	Set a realistic, ambitious end-date for task prioritization and motivation.	