MIDWEST
RELIABILITY
ORGANIZATION

Welcome to the 2023 Hybrid Security Training

Cris Zimmerman Manager, Outreach & Stakeholder Engagement

Steen Fjalstad, Director of Security MRO

MRO Logistics, Safety & E-Plan

- Safety – First Aid, CPR and AED
- Food and beverages
- Restrooms
- Emergency plan – severe weather/evacuation
- Monitoring the Chat for questions
- Wi-Fi – Connect to: Sheraton-MeetingRoom

2023 Security Conference Survey

https://www.surveymonkey.com/r/GTGH759

Disclaimer for organizational group hosted events or materials:

Midwest Reliability Organization (MRO) is committed to providing outreach, training, and non-binding guidance to industry stakeholders on important industry topics. Subject Matter Experts (SMEs) from MRO’s organizational groups and the industry may develop materials, including presentations, provided as a part of the event. The views expressed in the materials are those of the SMEs and do not necessarily express the opinions and views of MRO. Vendors presenting at, or attending, MRO events are not affiliated, associated, endorsed by MRO.

CISA / INL Training Overview

Kelly Johnson

Why?

- CISA & INL are in the training business?!
- **Mission:** Lead the national effort to understand and manage cyber and physical risk to our critical infrastructure.
- **Vision:** Secure and resilient critical infrastructure for the American people.
- CISA Services Catalog
  - Training Available Through CISA

Web-based Trainings

15 web-based courses accessed through the CISA Virtual Learning Portal

- OPSEC
- ICS architecture
- ICS cybersecurity
- IT cybersecurity
- Cybersecurity Risk
- Attack Methodologies in IT & ICS
- Incident Response
- Defense-In-Depth for ICS Networks
- Cybersecurity for Managers
- 301v (pre-req to 301L) (Labs)
- 401v (Labs)

https://ics-training.inl.gov/

401L Instructor-led Training

401L - ICS Evaluation

- Held at INL facilities in Idaho
- 3 days of hands-on instruction

- Topics include:
  - Cybersecurity Evaluation Tool (CSET)
  - Network segmentation
  - Network monitoring
  - Identifying ICS vulnerabilities
  - Assessing risk
  - ICS dependencies
  - Supply chain risk
  - Creating a findings report
  - Presenting to management

301L Instructor-led Training

301L - ICS Cybersecurity

- Held at INL facilities in Idaho
- At least once a month
- 4 days of hands-on instruction
- Small group break-out sessions with instructors

- Topics include:
  - ICS architecture
  - Strategies for IT & OT
  - Wireless
  - Network discovery
  - Defense-in-depth
  - Offensive attacker perspective

301L Red vs. Blue

- 7-hour exercise w/ 1.5 hour debrief
- Acme Chemical Co. scenario
- Student-led Blue & Red teams
- Instructors aid teams in exercise
- Real IT & OT systems – CI focused
- Balance cybersecurity and operations

- Real-time Incident Response
- Test your skills attacking or defending control systems!

301L Escape Rooms

- Escape room challenges based on learning objectives in the class
- Designed for people of all skill-levels
- Traditional escape room brain teasers
- Cyber challenges
- ICS systems
- 8 scenarios
- Fun and engaging
- **Free to attend!**
- See us for more info

Solar, Wind, and Fire

- Acme energy is under cyber attack affecting critical infrastructure systems
- Help restore power and ONG operations
- Cyber challenges
- ICS systems
- Network discovery
- Wireless
- Lock picking
- Augmented Reality

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

CISA

Network Discovery & Wireless

Chris Johnson

Network Discovery

Passive Discovery	Active Discovery
Similar to your senses	Similar to active SONAR
Observations are evaluated for mapping the surroundings	Pulses are sent out, and the returns are evaluated for mapping

Passive Discovery

What is passive network discovery?

- Using information stored locally on a compromised host to identify new host and network targets
- Attempt to identify new targets without sending any network packets

Why perform passive network discovery?

- More difficult to detect than active discovery
- May provide valuable information that active discovery cannot
- When active discovery is not possible (i.e., ICS)

Passive Discovery (Continued)

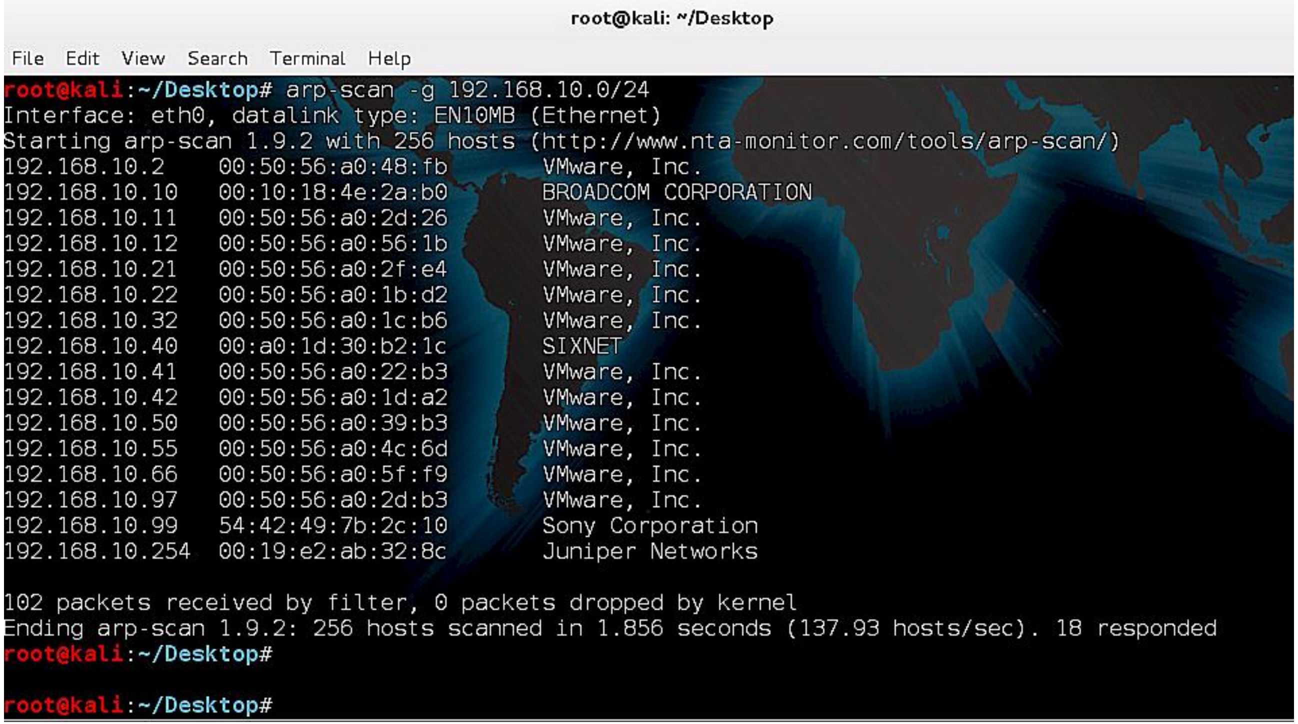
Tools
Tcpdump, Wireshark
Ipconfig (windows)
Ifconfig (linux)
Netstat
Arp
Net
Route
Iptables
EtherApe (GUI)

History Files
.bash_history
RDP
Log Files

Caches
Arp
Nbtstat
DNS
Browser

Configuration Files
Custom Scripts (cron, startup)
Apache (mysql, etc.)
Resolv.conf, hosts

Example – Arp-Scan



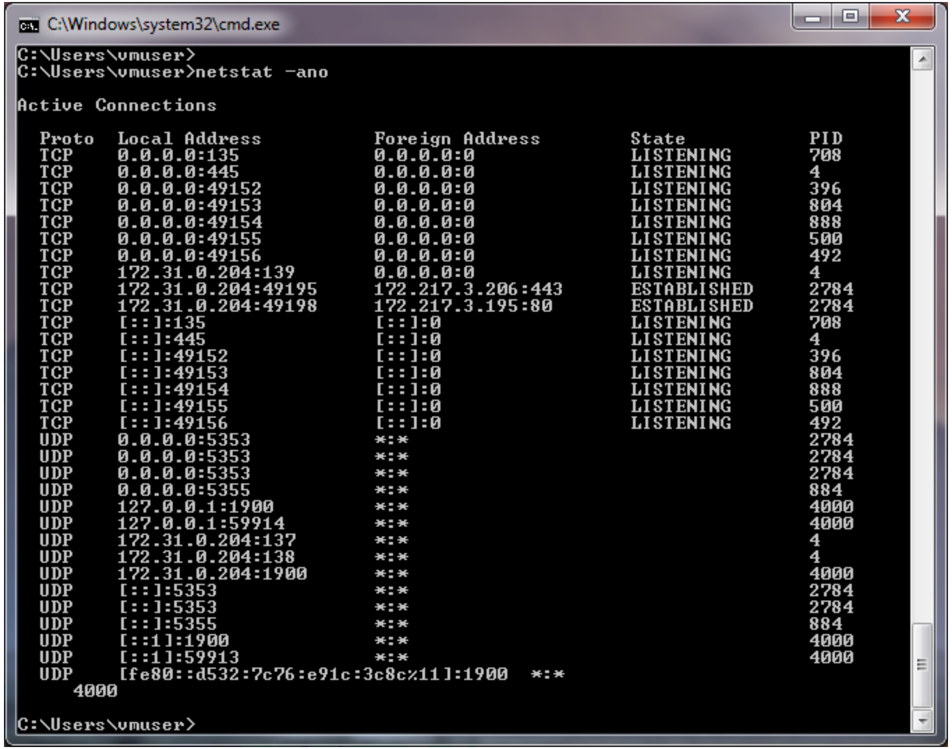
```
root@kali:~/Desktop# arp-scan -g 192.168.10.0/24
Interface: eth0, datalink type: EN10MB (Ethernet)
Starting arp-scan 1.9.2 with 256 hosts (http://www.nta-monitor.com/tools/arp-scan/)
192.168.10.2    00:50:56:a0:48:fb       VMware, Inc.
192.168.10.10   00:10:18:4e:2a:b0       BROADCOM CORPORATION
192.168.10.11   00:50:56:a0:2d:26       VMware, Inc.
192.168.10.12   00:50:56:a0:56:1b       VMware, Inc.
192.168.10.21   00:50:56:a0:2f:e4       VMware, Inc.
192.168.10.22   00:50:56:a0:1b:d2       VMware, Inc.
192.168.10.32   00:50:56:a0:1c:b6       VMware, Inc.
192.168.10.40   00:a0:1d:30:b2:1c       SIXNET
192.168.10.41   00:50:56:a0:22:b3       VMware, Inc.
192.168.10.42   00:50:56:a0:1d:a2       VMware, Inc.
192.168.10.50   00:50:56:a0:39:b3       VMware, Inc.
192.168.10.55   00:50:56:a0:4c:6d       VMware, Inc.
192.168.10.66   00:50:56:a0:5f:f9       VMware, Inc.
192.168.10.97   00:50:56:a0:2d:b3       VMware, Inc.
192.168.10.99   54:42:49:7b:2c:10       Sony Corporation
192.168.10.254  00:19:e2:ab:32:8c       Juniper Networks

102 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.9.2: 256 hosts scanned in 1.856 seconds (137.93 hosts/sec). 18 responded
root@kali:~/Desktop#

root@kali:~/Desktop#
```

Example – Netstat

Tools

- Tcpdump, Wireshark
- Ipconfig (windows)
- Ifconfig (Linux)
- Netstat
- Arp
- Net
- Route
- Iptables
- EtherApe (GUI)

Windows Command: `netstat -nob`



```
C:\Users\vmuser>
C:\Users\vmuser>netstat -ano

Active Connections

  Proto  Local Address          Foreign Address        State           PID
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       708
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:49152          0.0.0.0:0              LISTENING       396
  TCP    0.0.0.0:49153          0.0.0.0:0              LISTENING       804
  TCP    0.0.0.0:49154          0.0.0.0:0              LISTENING       888
  TCP    0.0.0.0:49155          0.0.0.0:0              LISTENING       500
  TCP    0.0.0.0:49156          0.0.0.0:0              LISTENING       492
  TCP    172.31.0.204:139       0.0.0.0:0              LISTENING       4
  TCP    172.31.0.204:49195     172.217.3.206:443      ESTABLISHED     2784
  TCP    172.31.0.204:49198     172.217.3.195:80       ESTABLISHED     2784
  TCP    [::]:135               [::]:0                 LISTENING       708
  TCP    [::]:445               [::]:0                 LISTENING       4
  TCP    [::]:49152             [::]:0                 LISTENING       396
  TCP    [::]:49153             [::]:0                 LISTENING       804
  TCP    [::]:49154             [::]:0                 LISTENING       888
  TCP    [::]:49155             [::]:0                 LISTENING       500
  TCP    [::]:49156             [::]:0                 LISTENING       492
  UDP    0.0.0.0:5353           *:*                                    2784
  UDP    0.0.0.0:5353           *:*                                    2784
  UDP    0.0.0.0:5353           *:*                                    2784
  UDP    0.0.0.0:5355           *:*                                    884
  UDP    127.0.0.1:1900         *:*                                    4000
  UDP    127.0.0.1:59914        *:*                                    4000
  UDP    172.31.0.204:137       *:*                                    4
  UDP    172.31.0.204:138       *:*                                    4
  UDP    172.31.0.204:1900      *:*                                    4000
  UDP    [::]:5353              *:*                                    2784
  UDP    [::]:5353              *:*                                    2784
  UDP    [::]:5355              *:*                                    884
  UDP    [::1]:1900             *:*                                    4000
  UDP    [::1]:59913            *:*                                    4000
  UDP    [fe80::d532:7c76:e91c:3c8c%11]:1900  *:*
    4000

C:\Users\vmuser>
```

Active Discovery

What is active network discovery?

- Send network packets and wait for a response to identify host and network targets
- Extremely noisy and easily detectable

Why use active network discovery methods?

- Identify targets that cannot be otherwise identified using passive discovery techniques
- Provides specific service, port, and version information for a given target
- Identify vulnerabilities of accessible services

Nmap

- Designed to allow system administrators and curious individuals to scan large networks to determine which hosts are up and what services they are offering
- Can be **DANGEROUS** to IT, SCADA, and PCS systems

A fast and informative network scanner that
can be safely used on isolated nonproduction SCADA/Control System Networks

Nmap (Continued)

What is Nmap?

- Open-source tool for network mapping and security auditing

Why use Nmap?

- Much faster than manual discovery
- Can scan an entire network quickly and offers several options to customize a scan and its results

How does Nmap work?

- Uses raw packets to determine
  - Hosts on the network
  - Services (ports)
  - Operating systems
  - etc.
- Two-stage process
  - Host discovery
  - Port scanning

Host Discovery

What is Host Discovery (HD)?

- Process of identifying active and interesting hosts on a network

Why does Nmap do HD?

- To significantly reduce the amount of time to complete network scans
- Narrows a set of IP ranges into a list of active or interesting hosts to be port scanned

How does HD work?

- Uses combination of ARP, ICMP, TCP SYN, and TCP ACK packets to identify active hosts

Nmap Common HD Options

Option	User Level	Speed	Packet Type	Notes
-sn	User	Fast	ICMP echo	Ping only, no port scan
-PA	Root	Fast	TCP Ack	WAN default, Port 80, stateless
-PS	User	Fast	TCP Syn	WAN default, Port 80, stateful
-PE	Root	Fast	ICMP echo	
-PR	User	Fastest	ARP	LAN default
-PU	Root	Slowest	UDP	Slow, unreliable, firewall
-PN	User	-	-	No ping, no HD

Port Scanning

What is port scanning (PS)?

- Process of identifying the status of interesting ports on hosts that are discovered on a network

Why does Nmap do PS?

- To identify ports open on a host

How does PS work?

- Attempts to communicate with each port within a specified set of ports
- Port scans are performed on hosts identified as active or interesting during HD

Nmap Port States

Open	Closed	Filtered	Unfiltered	Open | Filtered	Closed | Filtered
Application on target machine is listening for connections or packets on that port.	No application listening at the moment.	Firewall, filter, or other network obstacle is blocking the port so that Nmap cannot tell if the port is open or closed. Nmap received no response.	Port is accessible, but Nmap not able to determine if the port is open or closed.	Unable to determine if the port is open or filtered.	Unable to determine if the port is closed or filtered.

Nmap Common Port Scanning Options

Option	User Level	Packet Type	Notes
-sS	Root	TCP Syn	Privileged default
-sT	User	TCP connect	Uses connect system call
-sA	Root	TCP Ack	Firewall rule sets, stateful?
-sF	Root	TCP Fin	Filter evasion
-sX	Root	TCP FIN, PSH, URG	Filter evasion
-sN	Root	TCP NULL	Filter evasion
-sU	Root	UDP	Find UDP services
-p	-	-	Specify ports to scan

Timing and Performance Options

What are timing and performance options?

- Settings used to control scanning delays, timeouts,
- retries, and parallelism

Why use timing and performance options?

- Help speed up scanning process
- Slow down scan to avoid IDS detection

Timing and performance options:

- Manual options are available, but templates are usually sufficient
- Template timing options offer throttling abilities not available using manual options

Nmap Timing and Performance Templates

Option	Nickname	Speed	Notes
-T0	Paranoid	Slowest	IDS avoidance, 5-min packet delay
-T1	Sneaky	Slower	IDS avoidance, 5-sec packet delay
-T2	Polite	Slow	Conserve bandwidth target resources
-T3	Normal	Moderate	Default timing options used by Nmap
-T4	Aggressive	Fast	Maximum dynamic scan delay 10 ms
-T5	Insane	Fastest	Maximum dynamic scan delay 5 ms

ICS Challenges

- Scans can cause computer systems to restart
- Scans can cause embedded devices to freeze or lose configuration, and in some severe cases, requires vendor involvement
- Nmap considerations:
  - Use connect scan (-sT) to prevent dangling connections
  - Don’t use OS (-O) and Version Detection (-sV)
  - Slow the scan down by reducing the rate at which packets are being generated and sent by Nmap
  - Consider using exclusion lists (--exclude or --excludefile)

Wi-Fi Assessment

Concepts, Tools, Analysis:

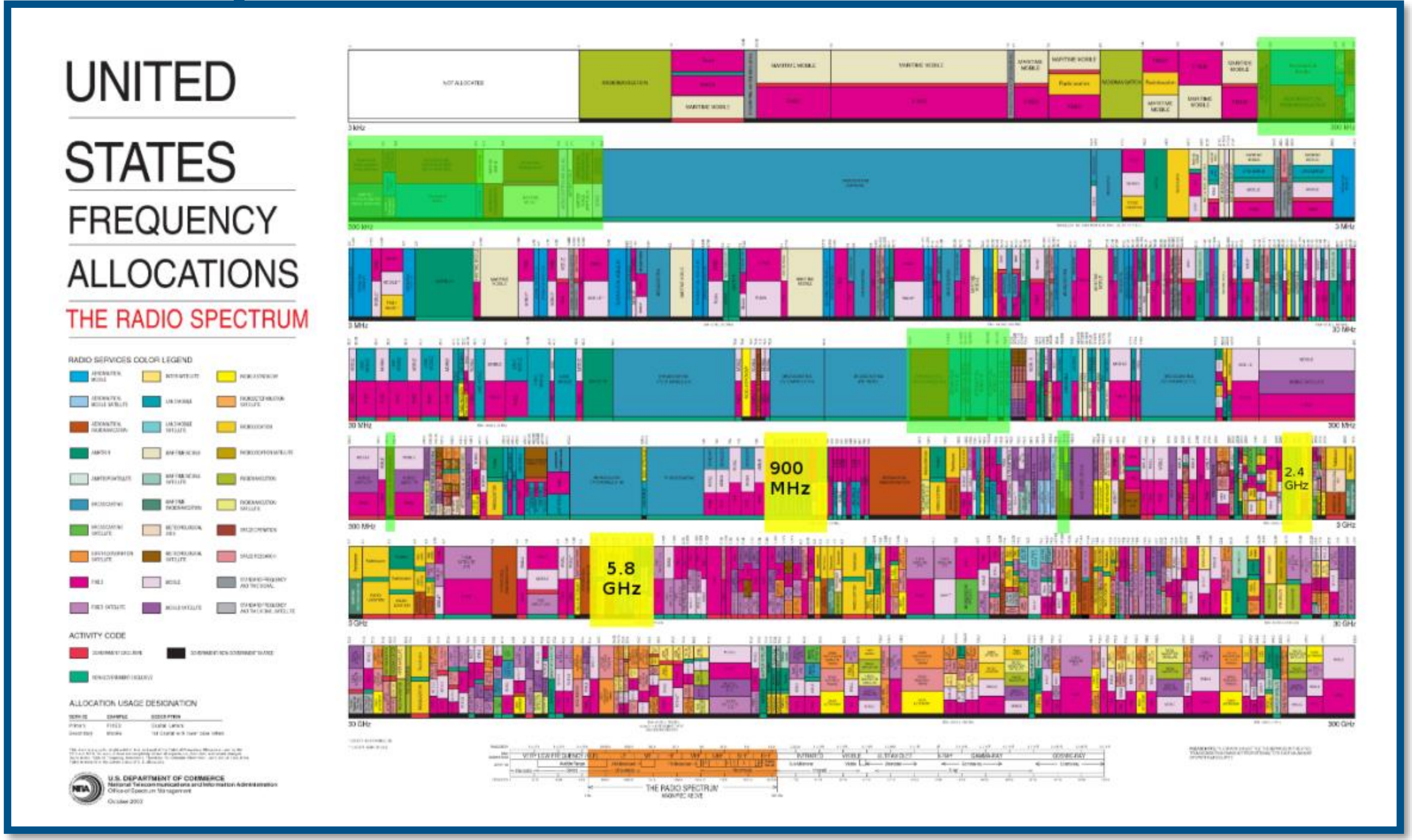
High-level Wireless Communications Discussion

IEEE 802.11 Protocols, a.k.a. Wi-Fi, and Threats

Packet Capture Tools

Aircrack-ng and other tools

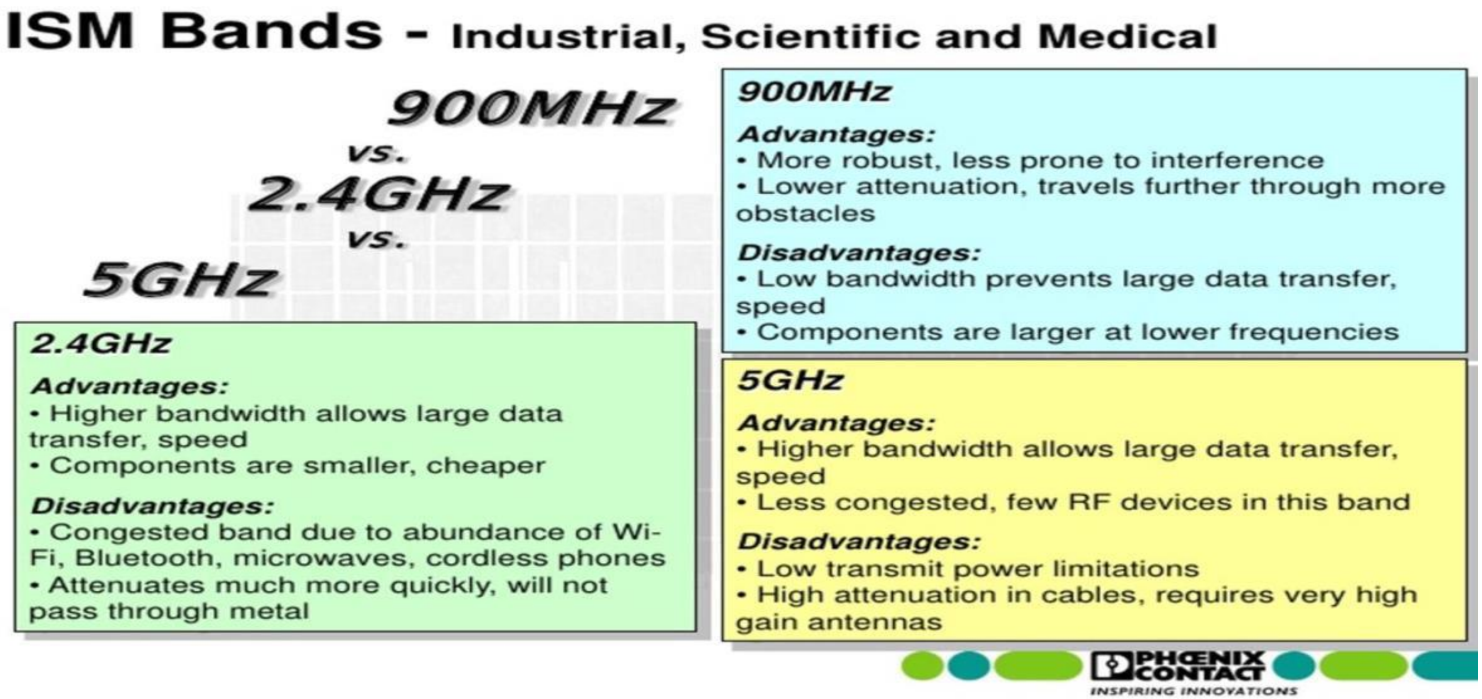
Radio Spectrum



Wireless Devices by Spectrum

Frequency	Devices
108 to 330 MHz	Aviation frequencies, Instrument Landing System (ILS), Very High Frequency Omni-Directional Range (VOR), glideslope, Air Training Command (ATC)
900 MHz	Cordless phones, wireless industrial control systems (ICS) valves, switches, controllers, HVAC controls, etc.
2.4 GHz	Wi-Fi routers, Bluetooth, Bluetooth Low Energy (BLE), ZigBee, printers, microwave ovens, remote controlled (RC) toys, baby monitors, cordless landline phones, key fobs, cell phones, WirelessHART, MiWi, Internet of Things (IoT), ICS, etc.
5.8 GHz	Wi-Fi routers, printers, RC devices, cell phones, cordless phones

Industrial, Scientific, Medical (ISM) Bands



ISM Bands - Industrial, Scientific and Medical

900MHz vs. 2.4GHz vs. 5GHz

900MHz

Advantages:

- More robust, less prone to interference
- Lower attenuation, travels further through more obstacles

Disadvantages:

- Low bandwidth prevents large data transfer, speed
- Components are larger at lower frequencies

2.4GHz

Advantages:

- Higher bandwidth allows large data transfer, speed
- Components are smaller, cheaper

Disadvantages:

- Congested band due to abundance of Wi-Fi, Bluetooth, microwaves, cordless phones
- Attenuates much more quickly, will not pass through metal

5GHz

Advantages:

- Higher bandwidth allows large data transfer, speed
- Less congested, few RF devices in this band

Disadvantages:

- Low transmit power limitations
- High attenuation in cables, requires very high gain antennas

PHOENIX CONTACT

INSPIRING INNOVATIONS

Source: Phoenix Contact, image: https://image.slidesharecdn.com/industrialwirelesscommunication-100616093544-phpapp01/95/industrial-wireless-communication-17-728.jpg?cb=1276697969

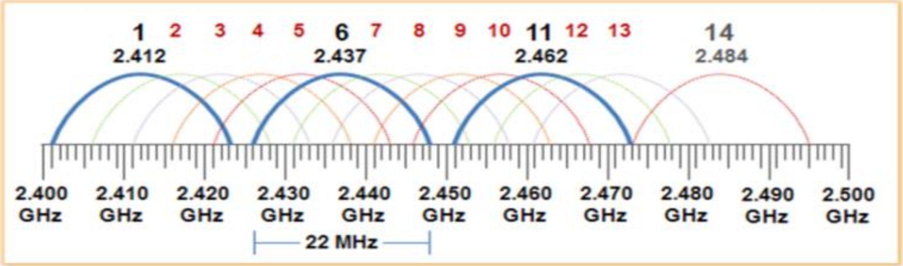
Wi-Fi Spectrum

2.4
GH
z

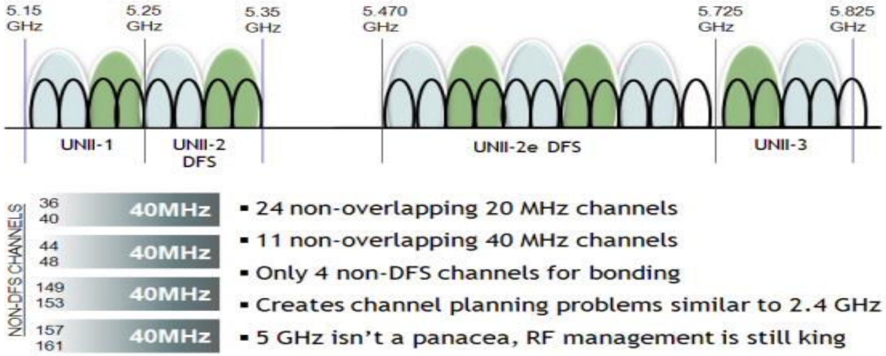
- 11 Channels
- 20 to 40 MHz width
- IEEE 802.11b,g,n
- 54 to 300 Mbps

5.8
GH
z

- 4 to 24 Channels
- 20 to 160 MHz width
- IEEE 802.11a,n,ac, etc.
- 54 Mbps to 1Gbps



Source: https://i.stack.imgur.com/ymo5p.png

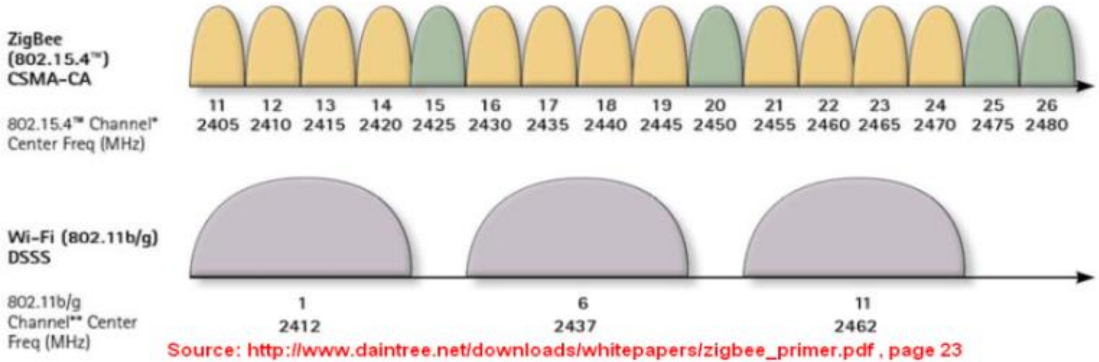


- 24 non-overlapping 20 MHz channels
- 11 non-overlapping 40 MHz channels
- Only 4 non-DFS channels for bonding
- Creates channel planning problems similar to 2.4 GHz
- 5 GHz isn't a panacea, RF management is still king

Source: Network World http://images.techhive.com/images/idge/imported/article/nww/2010/08/080210-infog-1-100272864-orig.jpg

IEEE 802.15.4 Spectrum

- Common Uses
  - Building Automation/Security
  - Residential Control
  - Industrial
  - Tracking
  - Sensors
  - Metering
  - Light Bulbs

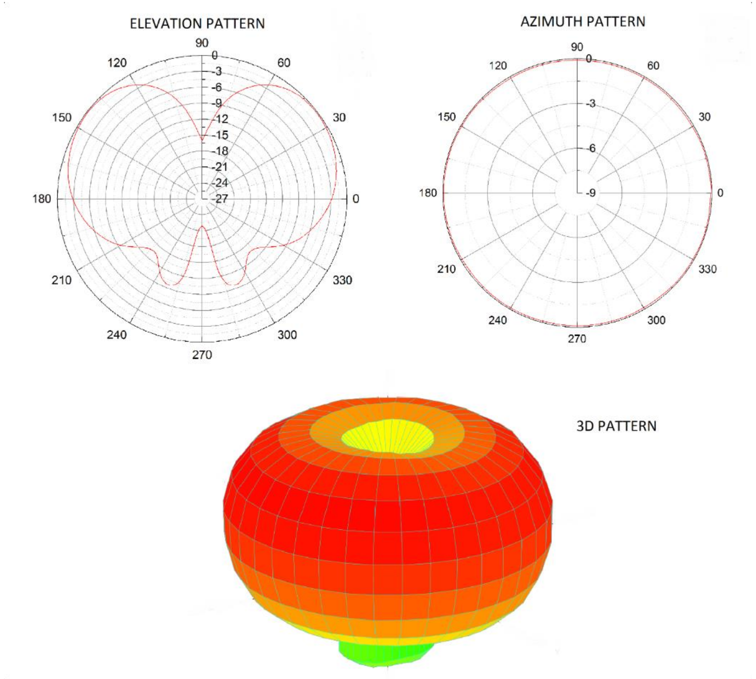


Source: http://www.daintree.net/downloads/whitepapers/zigbee_primer.pdf , page 23

Technology

- Runs at 2.400 to 2.4835 GHz or 2.4 GHz ISM band
- Frequency hopping spread spectrum
- 79 different channels at 1 MHz width, each with guard bands on each end
- Bluetooth low energy (BLE) channels are 2 MHz each
- 1 to 3 Mbps data streaming speed
- Personal area networks with a 10 meter range
- Most personal devices use Bluetooth. Roughly 4 billion devices were shipped in 2018. ~10 billion devices in the world
- Bluetooth 5 increases range and uses less energy
- Many devices are in ‘discoverable’ mode by default

Omni-Directional Antennas



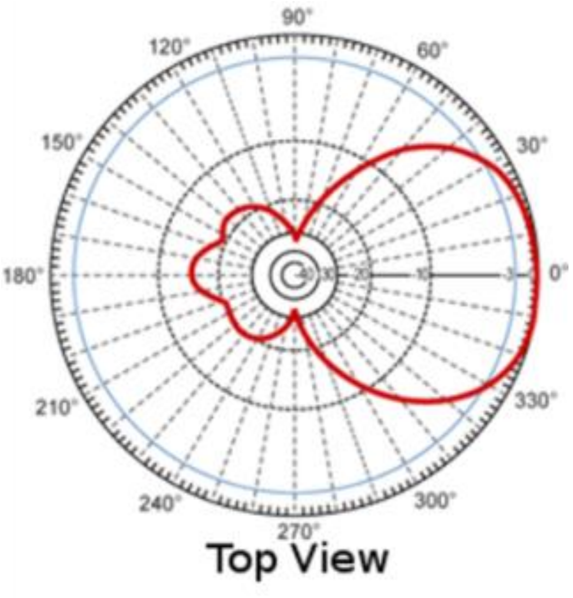
- Transmit and receive signals from any direction
- Most devices use some form of Omni directional antenna
- Difficult to identify location of signals

Source: Christmaslightsetc.com

Source: Amazon.com

Source: http://www.mpantenna.com/omnidirectional-antenna-radiation-patterns/

Directional Antenna



- Directional signal transmission and reception
- Reduces propagation pattern significantly
- Aids in signal hunting
- Increases reception gain when pointed at a source

Source: Amazon.com

Source: superbrightleds.com

Source: L-com http://www.l-com.com/multimedia/diagrams/d_HG2412P_1.gif

Wi-Fi Access Point (AP)

Wi-Fi Routers

Printers

Home made

MiFi Devices

IOT

Smart Phones

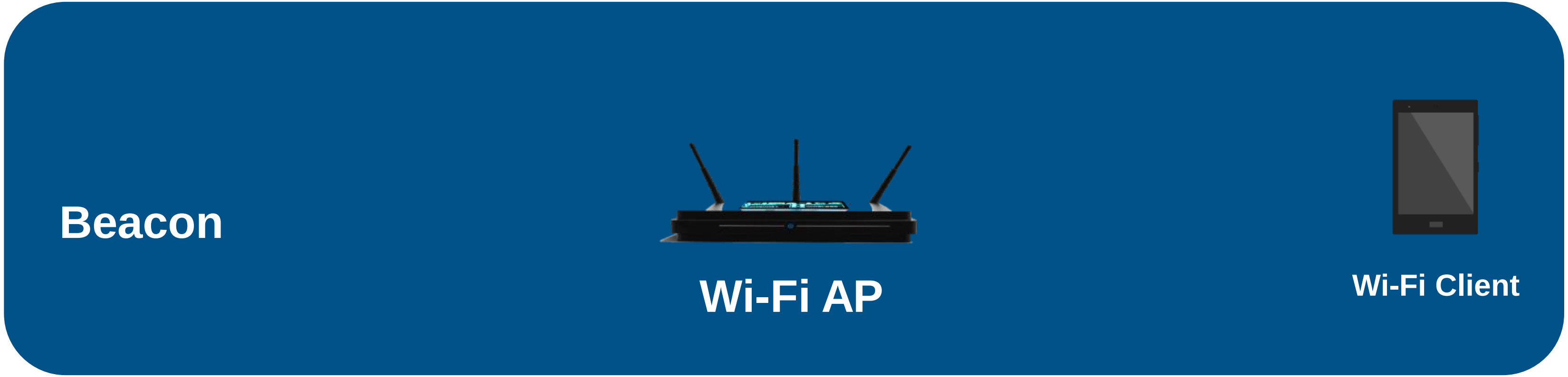
Cars

Appliances

Wi-Fi Encryption Types

Open	No Encryption
WEP	Wired Equivalent Privacy 1997 (obsolete)
WPA	Wi-Fi Protected Access 2003
WPA2	Wi-Fi Protected Access Version 2 2004
WPS	Wi-Fi Protected Setup 2006
WPA3	Wi-Fi Protected Access Version 3 2018
Certified Enhanced Open	Wi-Fi CERTIFIED Enhanced Open 2018

Wi-Fi AP Packet Data – Beacon



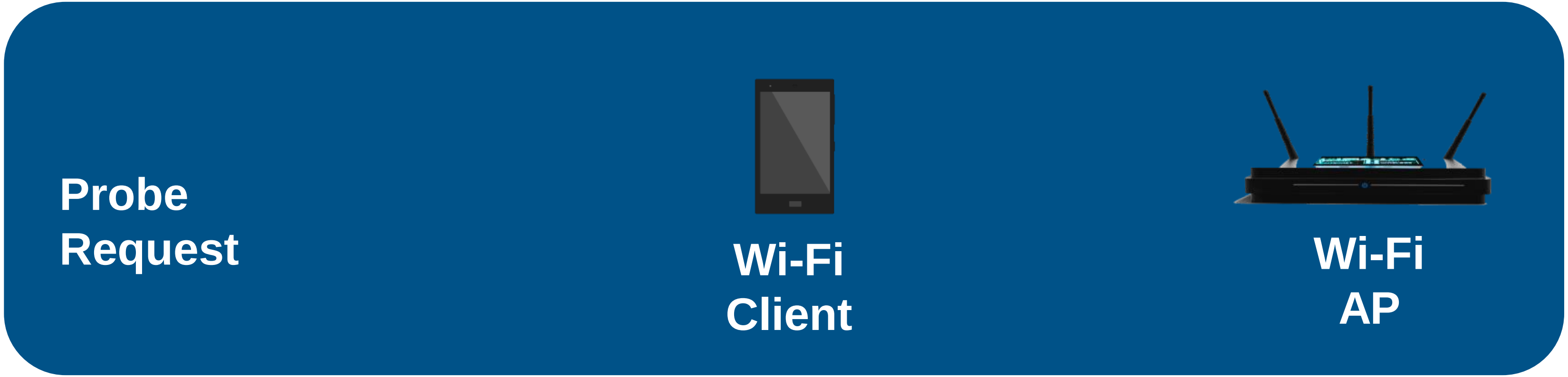
Beacon

Wi-Fi AP

Wi-Fi Client

- AP Wi-Fi beacon typically transmitted every 50 to 100ms, depending on configuration
- Usually contains source MAC BSSID, destination MAC, power, channel, encryption type, cipher type, auth type, name ESSID
- Wi-Fi clients do not transmit a beacon, only a probe request

Wi-Fi Client Packet Data – Probe Request



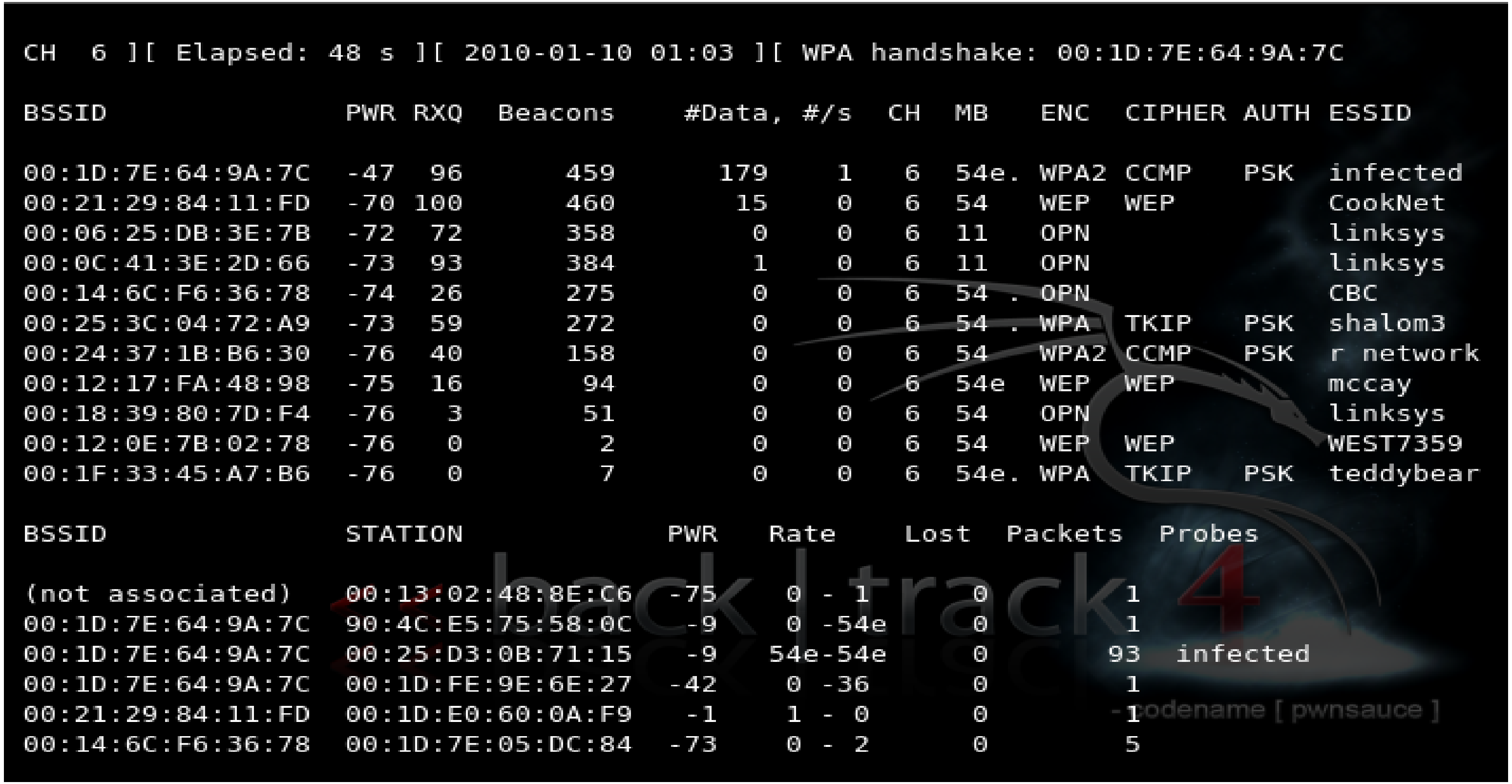
Probe Request

Wi-Fi Client

Wi-Fi AP

- Probe Request contains a request for capabilities by SSID from the client or a broadcast to all APs
- Occurs when Wi-Fi Client is not connected to an AP
- Saved SSIDs are used in Probe Requests
- AP broadcasts a Probe Response – similar to a beacon
- Prior AP SSIDs can be unintentionally revealed
- Good for reconnaissance by attackers and eavesdroppers
- Can be an aid to AP spoofing or Evil Twin attack

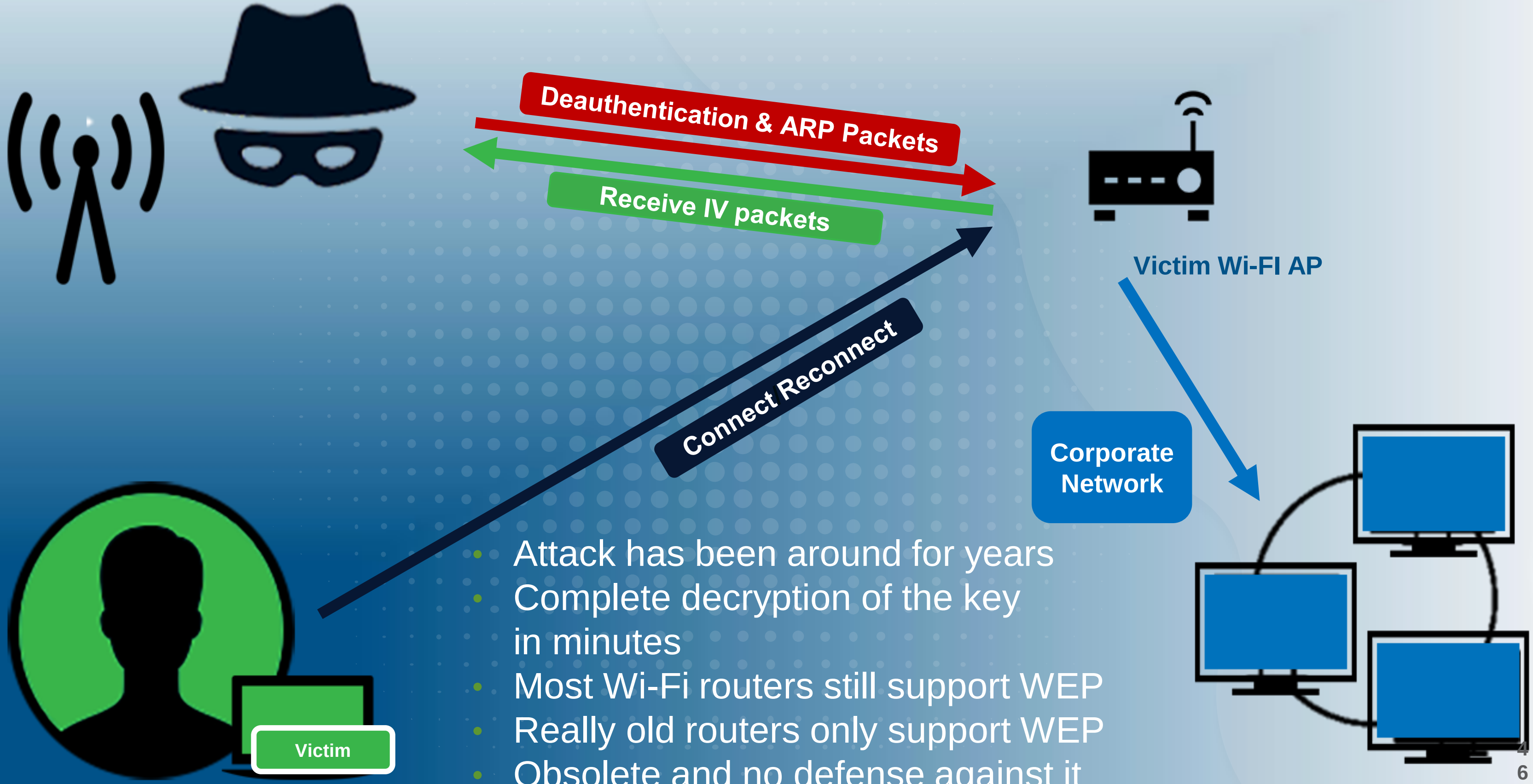
airodump-ng capture



```
CH  6 ][ Elapsed: 48 s ][ 2010-01-10 01:03 ][ WPA handshake: 00:1D:7E:64:9A:7C

BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

00:1D:7E:64:9A:7C  -47  96      459      179    1   6  54e. WPA2 CCMP   PSK  infected
00:21:29:84:11:FD  -70 100      460       15    0   6  54   WEP  WEP         CookNet
00:06:25:DB:3E:7B  -72  72      358        0    0   6  11   OPN              linksys
00:0C:41:3E:2D:66  -73  93      384        1    0   6  11   OPN              linksys
00:14:6C:F6:36:78  -74  26      275        0    0   6  54 . OPN              CBC
00:25:3C:04:72:A9  -73  59      272        0    0   6  54 . WPA  TKIP   PSK  shalom3
00:24:37:1B:B6:30  -76  40      158        0    0   6  54   WPA2 CCMP   PSK  r network
00:12:17:FA:48:98  -75  16       94        0    0   6  54e  WEP  WEP         mccay
00:18:39:80:7D:F4  -76   3       51        0    0   6  54   OPN              linksys
00:12:0E:7B:02:78  -76   0        2        0    0   6  54   WEP  WEP         WEST7359
00:1F:33:45:A7:B6  -76   0        7        0    0   6  54e. WPA  TKIP   PSK  teddybear

BSSID              STATION            PWR   Rate    Lost  Packets  Probes

(not associated)   00:13:02:48:8E:C6  -75    0 - 1      0        1
00:1D:7E:64:9A:7C  90:4C:E5:75:58:0C   -9    0 -54e     0        1
00:1D:7E:64:9A:7C  00:25:D3:0B:71:15   -9   54e-54e     0       93  infected
00:1D:7E:64:9A:7C  00:1D:FE:9E:6E:27  -42    0 -36      0        1
00:21:29:84:11:FD  00:1D:E0:60:0A:F9   -1    1 - 0      0        1
00:14:6C:F6:36:78  00:1D:7E:05:DC:84  -73    0 - 2      0        5
```

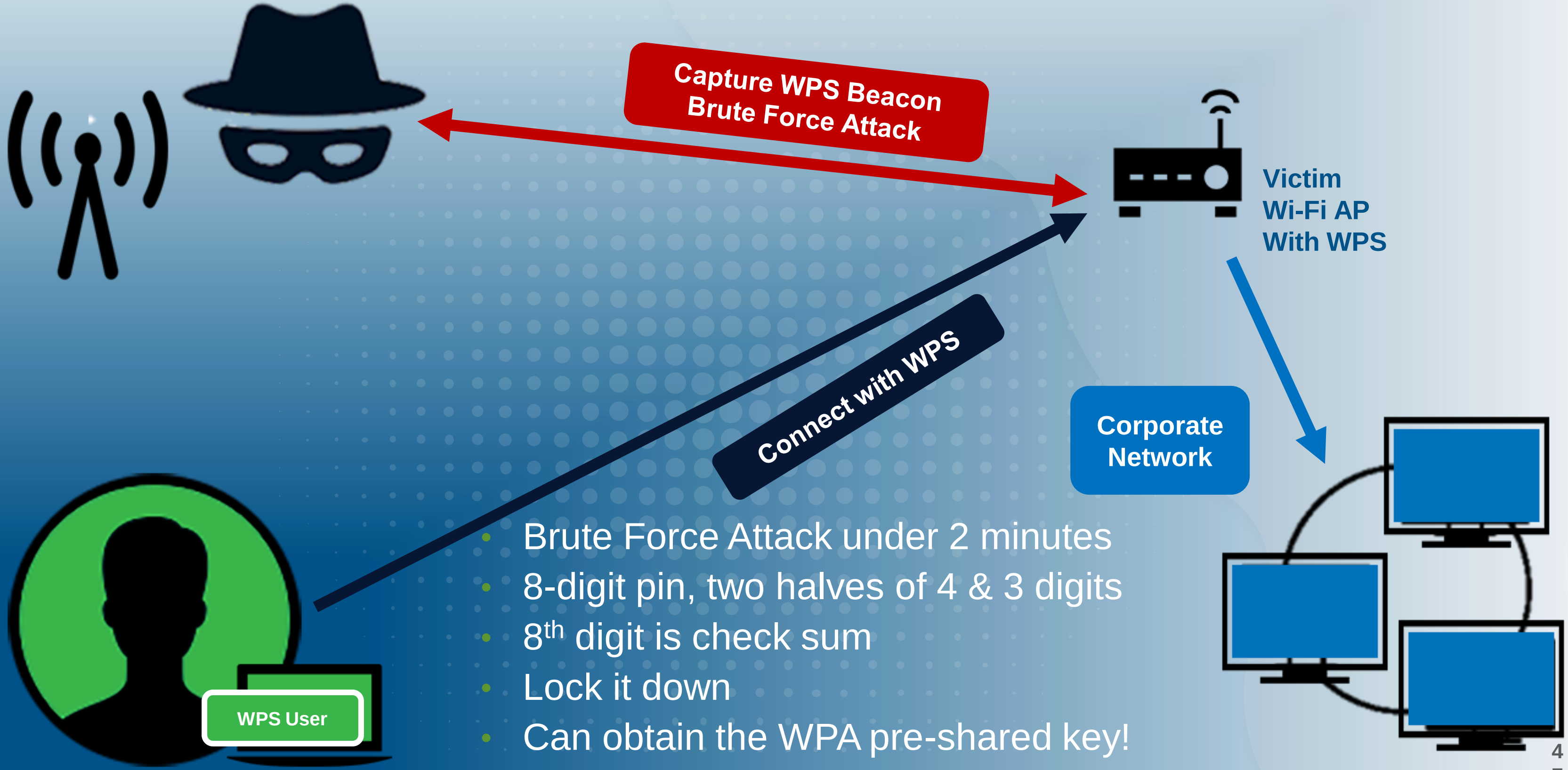
Source: question-defense.com

WEP Attack



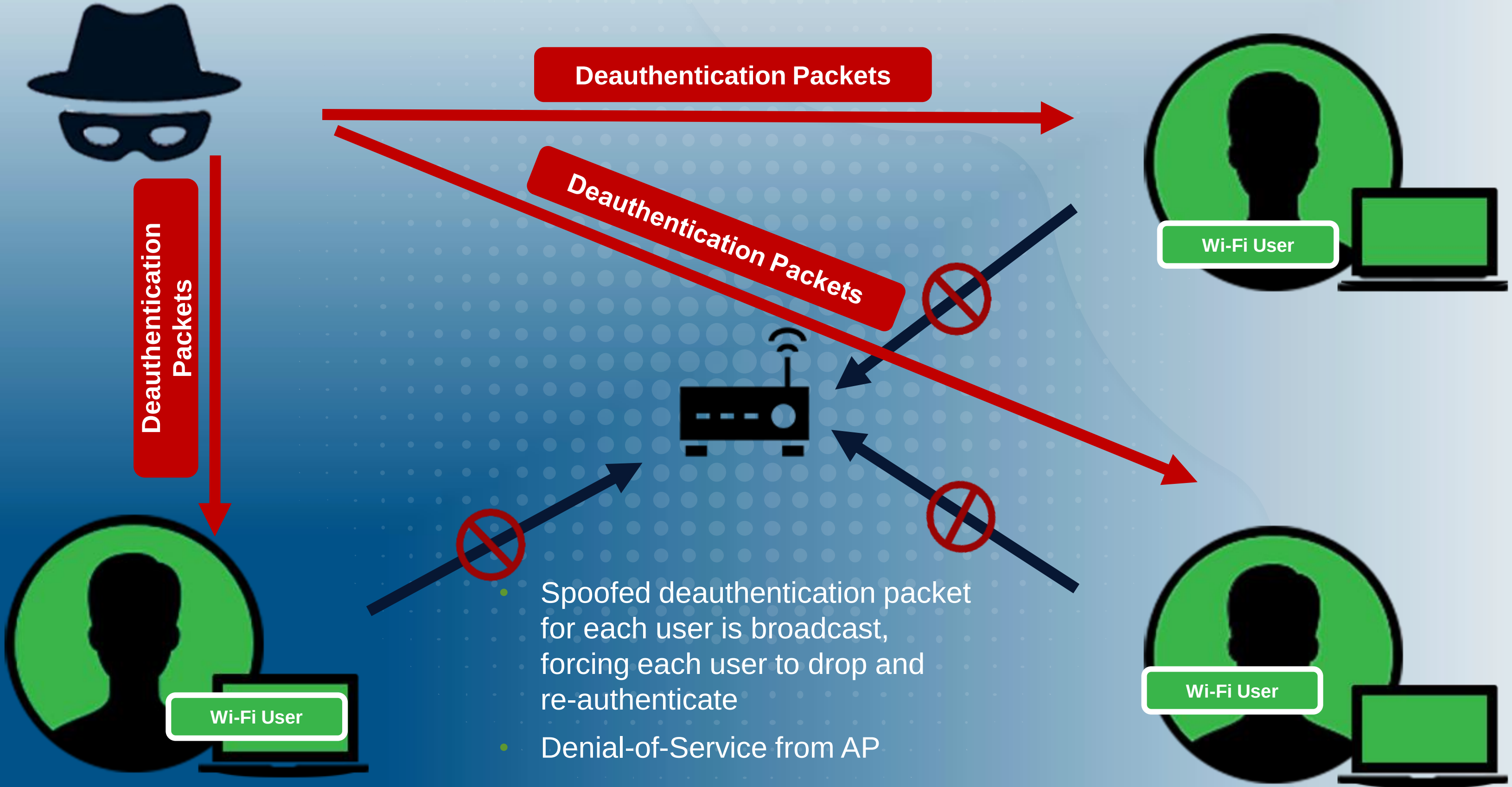
- Attack has been around for years
- Complete decryption of the key in minutes
- Most Wi-Fi routers still support WEP
- Really old routers only support WEP
- Obsolete and no defense against it

WPS Attack



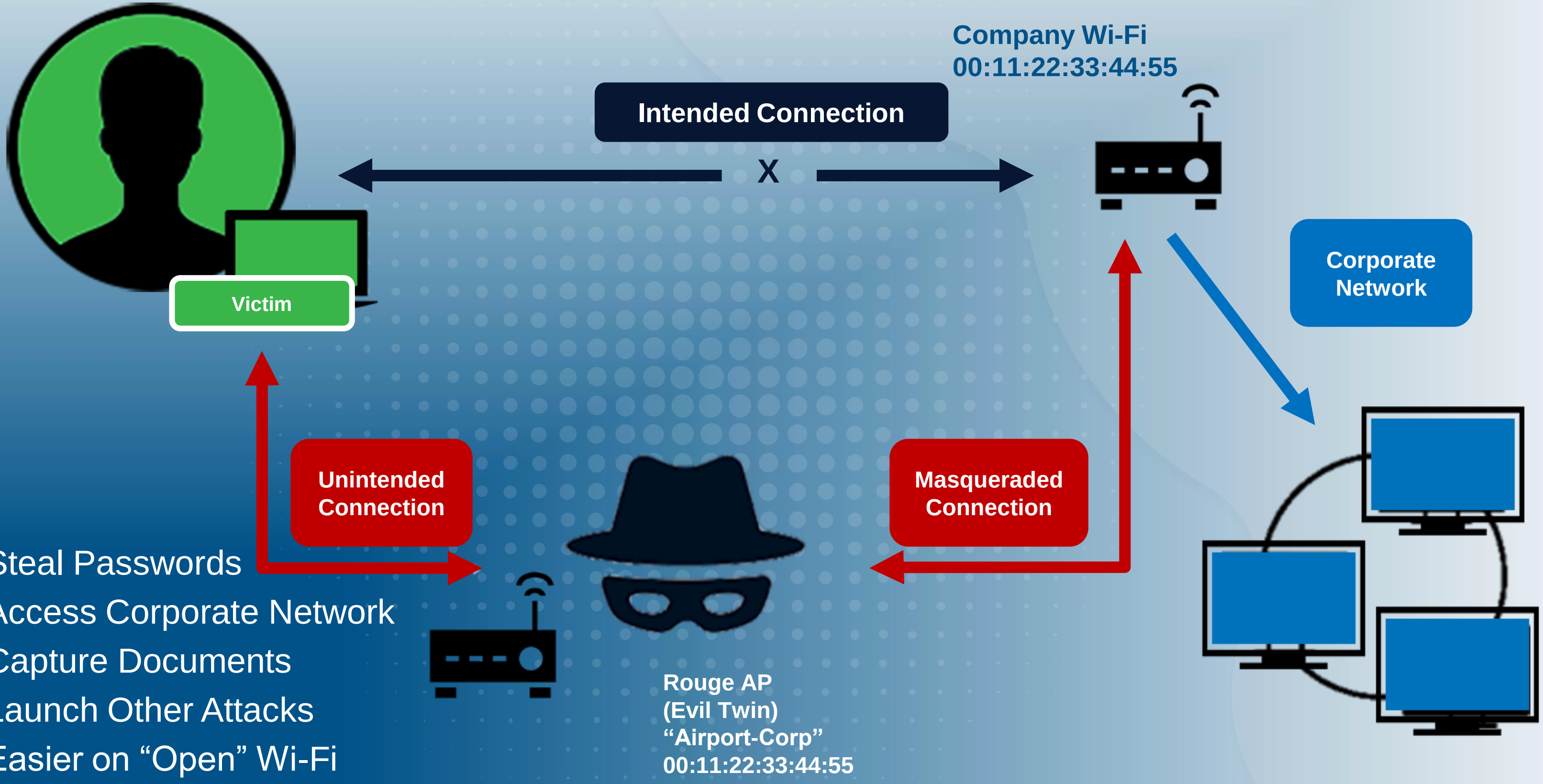
- Brute Force Attack under 2 minutes
- 8-digit pin, two halves of 4 & 3 digits
- 8th digit is check sum
- Lock it down
- Can obtain the WPA pre-shared key!
- Rare

Wi-Fi De-authentication DOS Attack



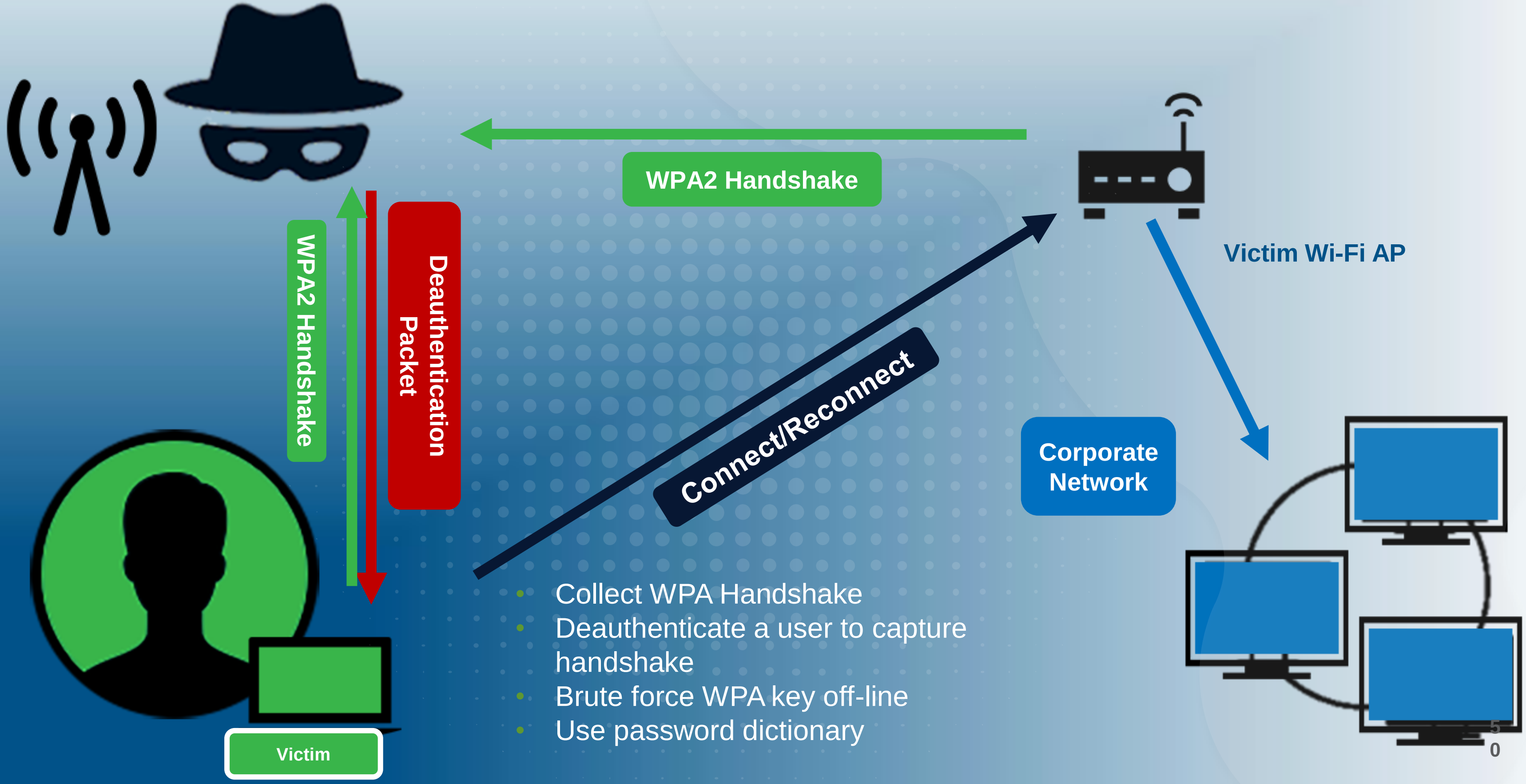
- Spoofed deauthentication packet for each user is broadcast, forcing each user to drop and re-authenticate
- Denial-of-Service from AP

Evil Twin (Machine-in-the-Middle) Attack



- Steal Passwords
- Access Corporate Network
- Capture Documents
- Launch Other Attacks
- Easier on “Open” Wi-Fi

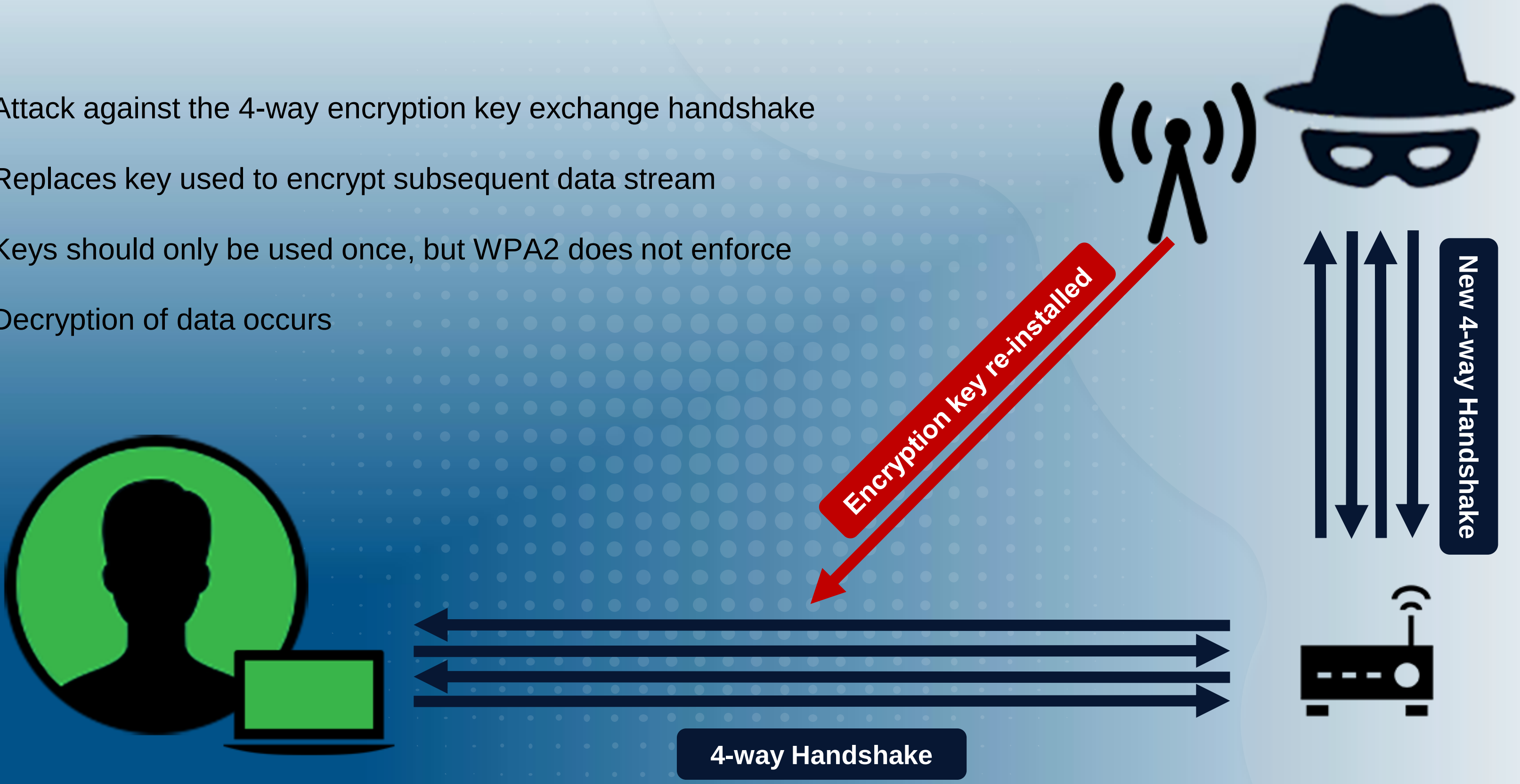
WPA/WPA2 Handshake Attack



- Collect WPA Handshake
- Deauthenticate a user to capture handshake
- Brute force WPA key off-line
- Use password dictionary

WPA2 Key Reinstallation AttaCK (KRACK)

- Attack against the 4-way encryption key exchange handshake
- Replaces key used to encrypt subsequent data stream
- Keys should only be used once, but WPA2 does not enforce
- Decryption of data occurs



RF Capture Tools

Wi-Fi Monitoring Hardware

- A few chipsets that are compatible:
  - Atheros
  - Ralink
  - Realtek
- Some example Wi-Fi hardware:
  - TP-Link WN722N V1 only
  - Alfa AWUS036NH
  - Panda Wireless PAU09

Source: https://www.wirelesshack.org/best-kali-linux-compatible-usb-adapter-dongles-2016.html

Aircrack-ng Suite of Tools

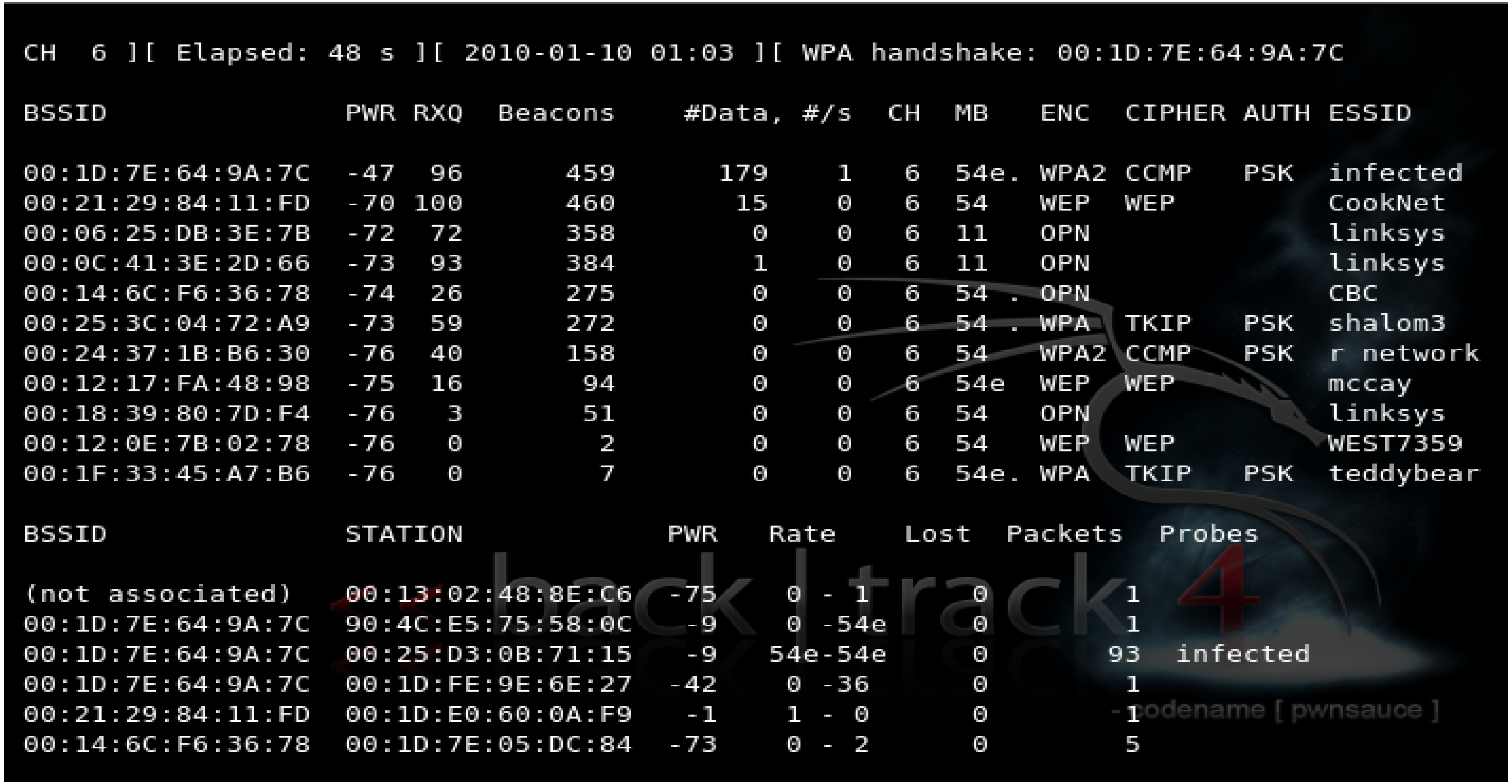
- airbase-ng
- aircrack-ng
- airdecap-ng
- airdecloak-ng
- airdriver-ng - REMOVED in 1.2 rc 1
- airdrop-ng
- aireplay-ng
- airgraph-ng
- **airmon-ng**
- **airodump-ng**
- airolib-ng
- airserv-ng
- airtun-ng
- besside-ng
- dcrack
- easside-ng
- packetforge-ng
- tkiptun-ng
- wesside-ng

Monitor Mode

- Sets the mode of the Wi-Fi interface into monitor mode, where every packet can be seen by the interface on every network - but not connected. ‘Promiscuous mode’ allows capturing packets after a connection is made to a network.
- Aircrack-ng, Kismet, and Wireshark can use the mode to perform their actions.
- Monitor mode allows not only monitoring but packet injection.
- Monitor mode must be stopped in order to return the Wi-Fi hardware to ‘normal’ use.

Source: https://www.wirelesshack.org/best-kali-linux-compatible-usb-adapter-dongles-2016.html

airodump-ng capture



```
CH  6 ][ Elapsed: 48 s ][ 2010-01-10 01:03 ][ WPA handshake: 00:1D:7E:64:9A:7C

BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

00:1D:7E:64:9A:7C  -47  96      459      179    1   6  54e. WPA2 CCMP   PSK  infected
00:21:29:84:11:FD  -70 100      460       15    0   6  54   WEP  WEP         CookNet
00:06:25:DB:3E:7B  -72  72      358        0    0   6  11   OPN              linksys
00:0C:41:3E:2D:66  -73  93      384        1    0   6  11   OPN              linksys
00:14:6C:F6:36:78  -74  26      275        0    0   6  54 . OPN              CBC
00:25:3C:04:72:A9  -73  59      272        0    0   6  54 . WPA  TKIP   PSK  shalom3
00:24:37:1B:B6:30  -76  40      158        0    0   6  54   WPA2 CCMP   PSK  r network
00:12:17:FA:48:98  -75  16       94        0    0   6  54e  WEP  WEP         mccay
00:18:39:80:7D:F4  -76   3       51        0    0   6  54   OPN              linksys
00:12:0E:7B:02:78  -76   0        2        0    0   6  54   WEP  WEP         WEST7359
00:1F:33:45:A7:B6  -76   0        7        0    0   6  54e. WPA  TKIP   PSK  teddybear

BSSID              STATION            PWR   Rate    Lost  Packets  Probes

(not associated)   00:13:02:48:8E:C6  -75    0 - 1     0        1
00:1D:7E:64:9A:7C  90:4C:E5:75:58:0C   -9    0 -54e    0        1
00:1D:7E:64:9A:7C  00:25:D3:0B:71:15   -9   54e-54e    0       93  infected
00:1D:7E:64:9A:7C  00:1D:FE:9E:6E:27  -42    0 -36     0        1
00:21:29:84:11:FD  00:1D:E0:60:0A:F9   -1    1 - 0     0        1
00:14:6C:F6:36:78  00:1D:7E:05:DC:84  -73    0 - 2     0        5
```

Source: question-defense.com

Airodump-ng syntax

- -R uses Regular Expressions to filter on ESSID (name)
- -w write output to a file
- -c capture on specific channels

  By default , airodump-ng hops on 2.4GHz channels 1-14.

  To capture on both 2.4GHz and 5GHz channels use: -c 1-165

- Usage: airodump-ng <options> <interface>
- Examples:

```
airodump-ng -R acme wlan0mon
```

-filters on ESSID names with acme and hops 2.4GHz channels 1-14

```
airodump-ng -R acme -c 1-165 wlan0mon
```

-hops through 2.4GHz and 5GHz channels

```
airodump-ng -R acme -w mycapture wlan0mon
```

-writes output to a file named mycapture

Wireless AP Hunting

- RSSI **Received Signal Strength Indicator**
  - Filter in on the exact ESSID name using -R <name>
  - Filter in on the exact channel using -c <channel number>
  - Directional antennas work the best
  - Remember the power levels are measured in negative dB
  - For reference -30 is a strong signal, -90 is weak
  - Take it slow

Questions

What questions do you have?

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

CISA

Network Intrusion Detection

What We've Learned

Scot Donecker

Enterprise Architect

Generation Systems

Sunflower Electric Power Corporation

September 26, 2023

Who am I?

Scot Donecker

Enterprise Architect

Generation Systems

Sunflower Electric Power Corporation

Where are you currently?

Security Information and Event Management (SIEM):

- Do you have a SIEM or similar centralized log management system? (e.g. Splunk, Arctic Wolf, LogRhythm, NitroSecurity, etc.)

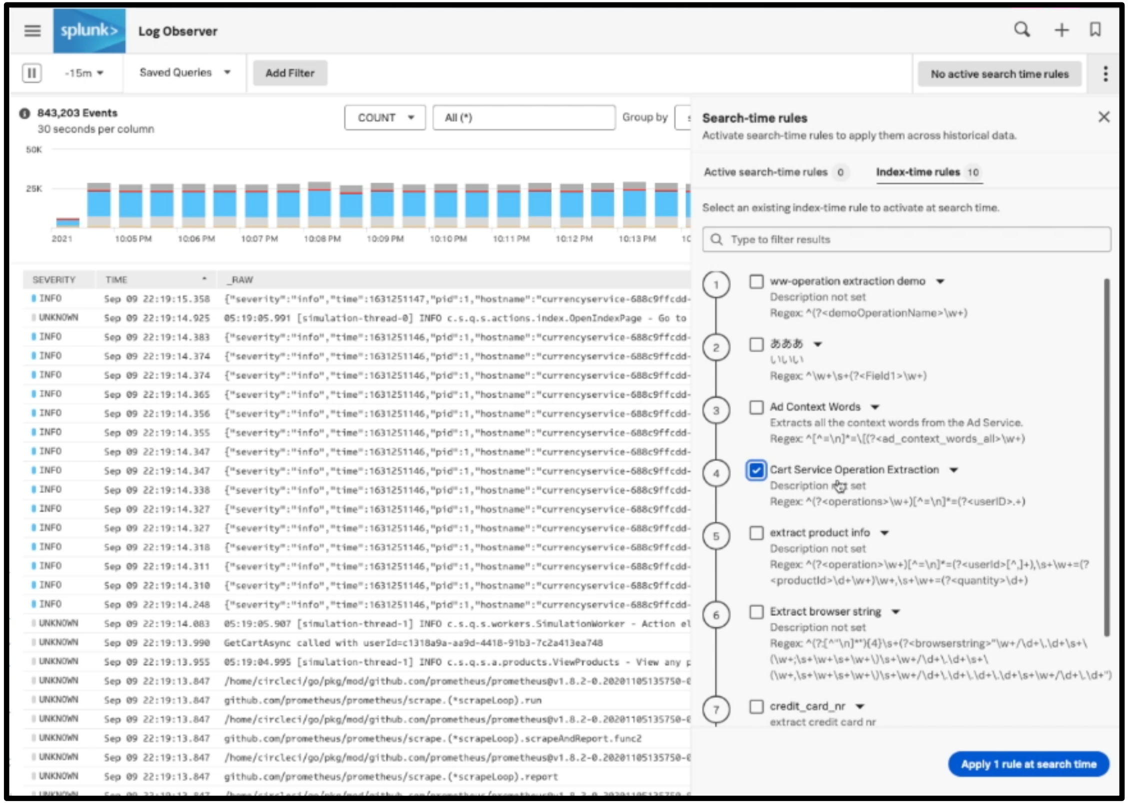
Network Intrusion Detection (NID) or Network Monitoring Solution (NMS):

- Do you have a NID or NMS in place?

Security Operation Center (SOC):

- Do you have a dedicated cyber security analyst or SOC?

Our Journey



```
SEVERITY  TIME                  _RAW
INFO      Sep 09 22:19:15.358   {"severity":"info","time":1631251147,"pid":1,"hostname":"currencyservice-688c9ffcdd-
UNKNOWN   Sep 09 22:19:14.925   05:19:05.991 [simulation-thread-0] INFO c.s.q.s.actions.index.OpenIndexPage - Go to
INFO      Sep 09 22:19:14.383   {"severity":"info","time":1631251146,"pid":1,"hostname":"currencyservice-688c9ffcdd-
INFO      Sep 09 22:19:14.374   {"severity":"info","time":1631251146,"pid":1,"hostname":"currencyservice-688c9ffcdd-
INFO      Sep 09 22:19:14.374   {"severity":"info","time":1631251146,"pid":1,"hostname":"currencyservice-688c9ffcdd-
INFO      Sep 09 22:19:14.365   {"severity":"info","time":1631251146,"pid":1,"hostname":"currencyservice-688c9ffcdd-
INFO      Sep 09 22:19:14.356   {"severity":"info","time":1631251146,"pid":1,"hostname":"currencyservice-688c9ffcdd-
INFO      Sep 09 22:19:14.355   {"severity":"info","time":1631251146,"pid":1,"hostname":"currencyservice-688c9ffcdd-
INFO      Sep 09 22:19:14.347   {"severity":"info","time":1631251146,"pid":1,"hostname":"currencyservice-688c9ffcdd-
INFO      Sep 09 22:19:14.347   {"severity":"info","time":1631251146,"pid":1,"hostname":"currencyservice-688c9ffcdd-
INFO      Sep 09 22:19:14.338   {"severity":"info","time":1631251146,"pid":1,"hostname":"currencyservice-688c9ffcdd-
INFO      Sep 09 22:19:14.327   {"severity":"info","time":1631251146,"pid":1,"hostname":"currencyservice-688c9ffcdd-
INFO      Sep 09 22:19:14.327   {"severity":"info","time":1631251146,"pid":1,"hostname":"currencyservice-688c9ffcdd-
INFO      Sep 09 22:19:14.318   {"severity":"info","time":1631251146,"pid":1,"hostname":"currencyservice-688c9ffcdd-
INFO      Sep 09 22:19:14.311   {"severity":"info","time":1631251146,"pid":1,"hostname":"currencyservice-688c9ffcdd-
INFO      Sep 09 22:19:14.310   {"severity":"info","time":1631251146,"pid":1,"hostname":"currencyservice-688c9ffcdd-
INFO      Sep 09 22:19:14.248   {"severity":"info","time":1631251146,"pid":1,"hostname":"currencyservice-688c9ffcdd-
UNKNOWN   Sep 09 22:19:14.083   05:19:05.907 [simulation-thread-1] INFO c.s.q.s.workers.SimulationWorker - Action el
UNKNOWN   Sep 09 22:19:13.990   GetCartAsync called with userId=c1318a9a-aa9d-4418-91b3-7c2a413ea748
UNKNOWN   Sep 09 22:19:13.955   05:19:04.995 [simulation-thread-1] INFO c.s.q.s.a.products.ViewProducts - View any p
UNKNOWN   Sep 09 22:19:13.847   /home/circleci/go/pkg/mod/github.com/prometheus/prometheus@v1.8.2-0.20201105135750-0
UNKNOWN   Sep 09 22:19:13.847   github.com/prometheus/prometheus/scrape.(*scrapeLoop).run
UNKNOWN   Sep 09 22:19:13.847   /home/circleci/go/pkg/mod/github.com/prometheus/prometheus@v1.8.2-0.20201105135750-0
UNKNOWN   Sep 09 22:19:13.847   github.com/prometheus/prometheus/scrape.(*scrapeLoop).scrapeAndReport.func2
UNKNOWN   Sep 09 22:19:13.847   /home/circleci/go/pkg/mod/github.com/prometheus/prometheus@v1.8.2-0.20201105135750-0
UNKNOWN   Sep 09 22:19:13.847   github.com/prometheus/prometheus/scrape.(*scrapeLoop).report
```

Search-time rules

Activate search-time rules to apply them across historical data.

Active search-time rules 0 | Index-time rules 10

Select an existing index-time rule to activate at search time.

Type to filter results

1 ☐ ww-operation extraction demo
Description not set
Regex: `^(?<demoOperationName>\w+)`

2 ☐ あああ
いいい
Regex: `^\w+\s+(?<Field1>\w+)`

3 ☐ Ad Context Words
Extracts all the context words from the Ad Service.
Regex: `^[^=\n]*=\[(?<ad_context_words_all>\w+)`

4 ☑ Cart Service Operation Extraction
Description not set
Regex: `^(?<operations>\w+)[^=\n]*=(?<userID>.+)`

5 ☐ extract product info
Description not set
Regex: `^(?<operation>\w+)[^=\n]*=(?<userId>[^,]+),\s+\w+=(?<productId>\d+\w+)\w+,\s+\w+=(?<quantity>\d+)`

6 ☐ Extract browser string
Description not set
Regex: `^(?:[^"\n]*"){4}\s+(?<browserstring>"\w+/\d+\.\d+\s+\(\w+;\s+\w+\s+\w+\)\s+\w+/\d+\.\d+\s+\(\w+,\s+\w+\s+\w+\)\s+\w+/\d+\.\d+\.\d+\.\d+\s+\w+/\d+\.\d+")`

7 ☐ credit_card_nr
extract credit card nr

Apply 1 rule at search time

Security Information and Event Management:

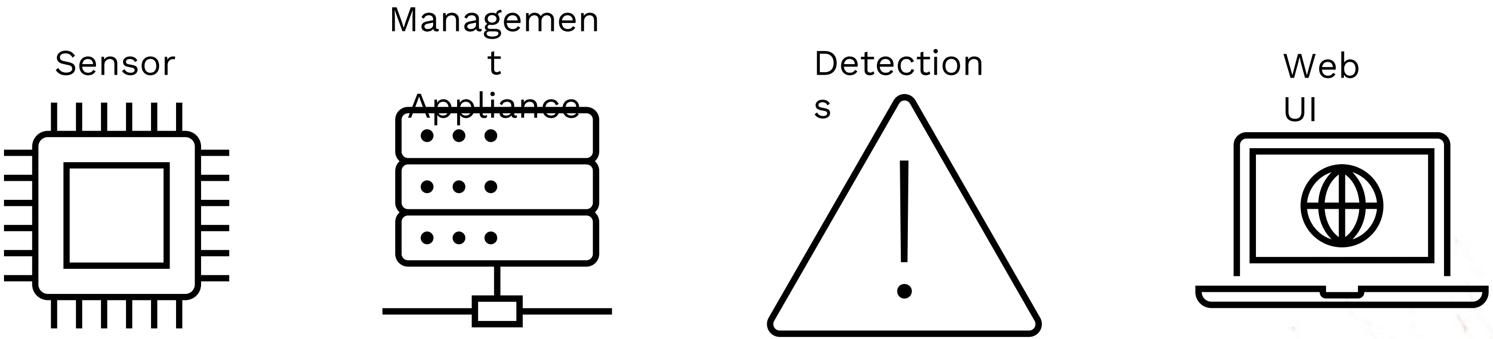
Pros:

- Irrefutable source of information
- Ability to correlate events from a diverse set of log sources
- Incredibly useful for investigations occurring post-mortem

Cons:

- Need to know exactly what you're looking for
- Not great at instantaneous alerting, due to the large number of resources required

Basic Architecture



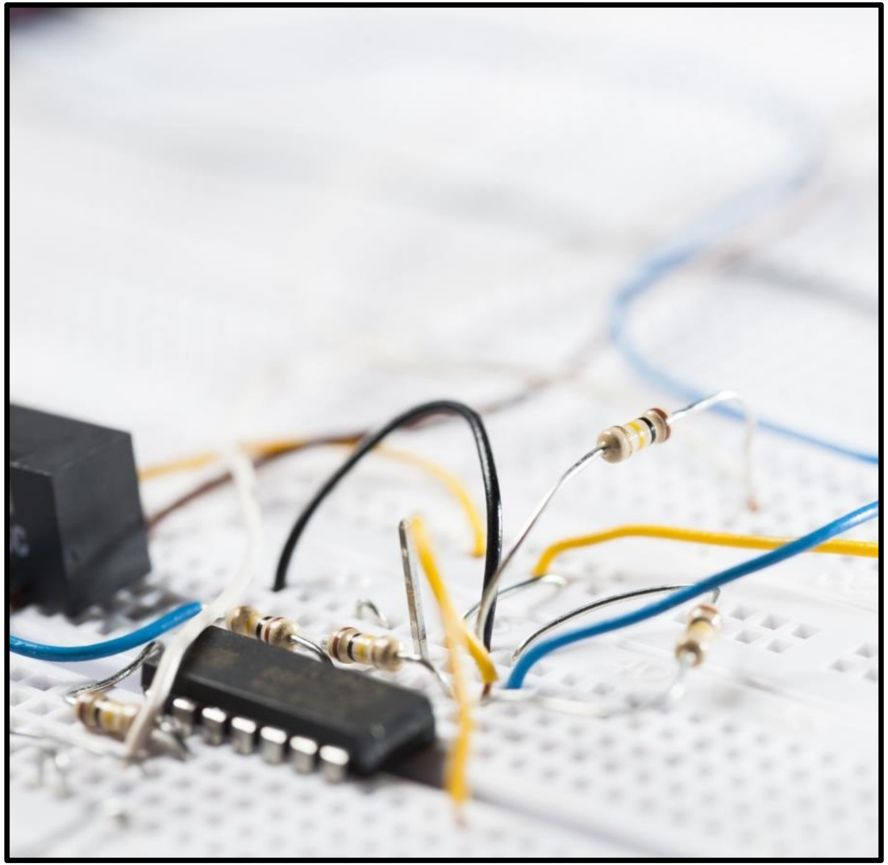
Sensor

Management Appliance

Detections

Web UI

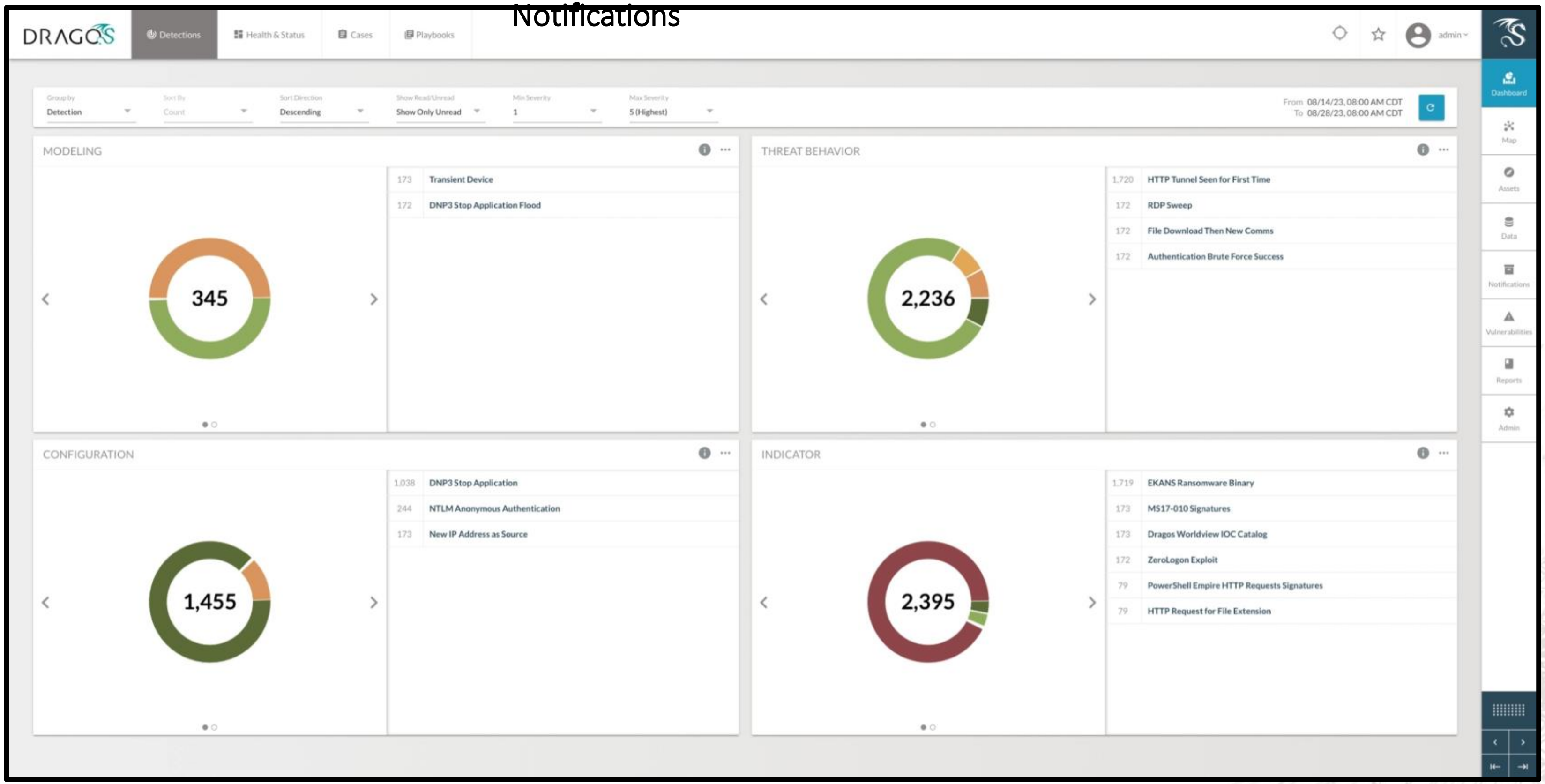
Our Experience



1. Automated detections and notifications.
2. Custom detection capabilities.
3. Asset identification.
4. Network flow mapping.
5. Third-party threat intelligence.
6. Setup and implementation.
7. Cloud hosting options.
8. SIEM integration.
9. Vulnerability Assessment.

Dragos

Automated Detections and Notifications



Group by: Detection
Sort By: Count
Sort Direction: Descending
Show Read/Unread: Show Only Unread
Min Severity: 1
Max Severity: 5 (Highest)

From 08/14/23, 08:00 AM CDT
To 08/28/23, 08:00 AM CDT

MODELING

173	Transient Device
172	DNP3 Stop Application Flood

THREAT BEHAVIOR

1,720	HTTP Tunnel Seen for First Time
172	RDP Sweep
172	File Download Then New Comms
172	Authentication Brute Force Success

CONFIGURATION

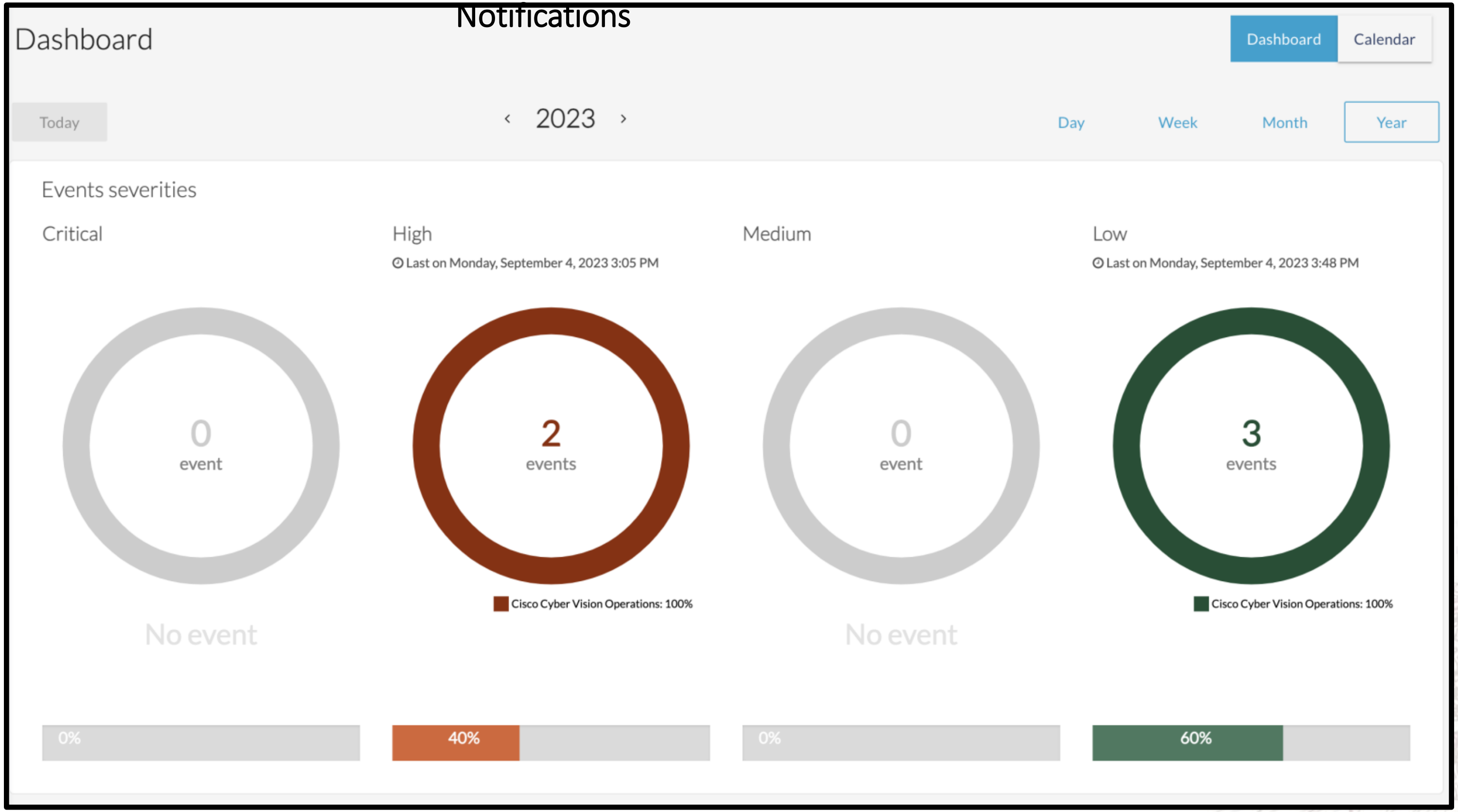
1,038	DNP3 Stop Application
244	NTLM Anonymous Authentication
173	New IP Address as Source

INDICATOR

1,719	EKANS Ransomware Binary
173	MS17-010 Signatures
173	Dragos Worldview IOC Catalog
172	ZeroLogon Exploit
79	PowerShell Empire HTTP Requests Signatures
79	HTTP Request for File Extension

Cisco Cyber Vision

Automated Detections and Notifications



Dashboard

Dashboard | Calendar

Today

‹ 2023 ›

Day | Week | Month | Year

Events severities

Critical

0 event

No event

0%

High

Last on Monday, September 4, 2023 3:05 PM

2 events

🟥 Cisco Cyber Vision Operations: 100%

40%

Medium

0 event

No event

0%

Low

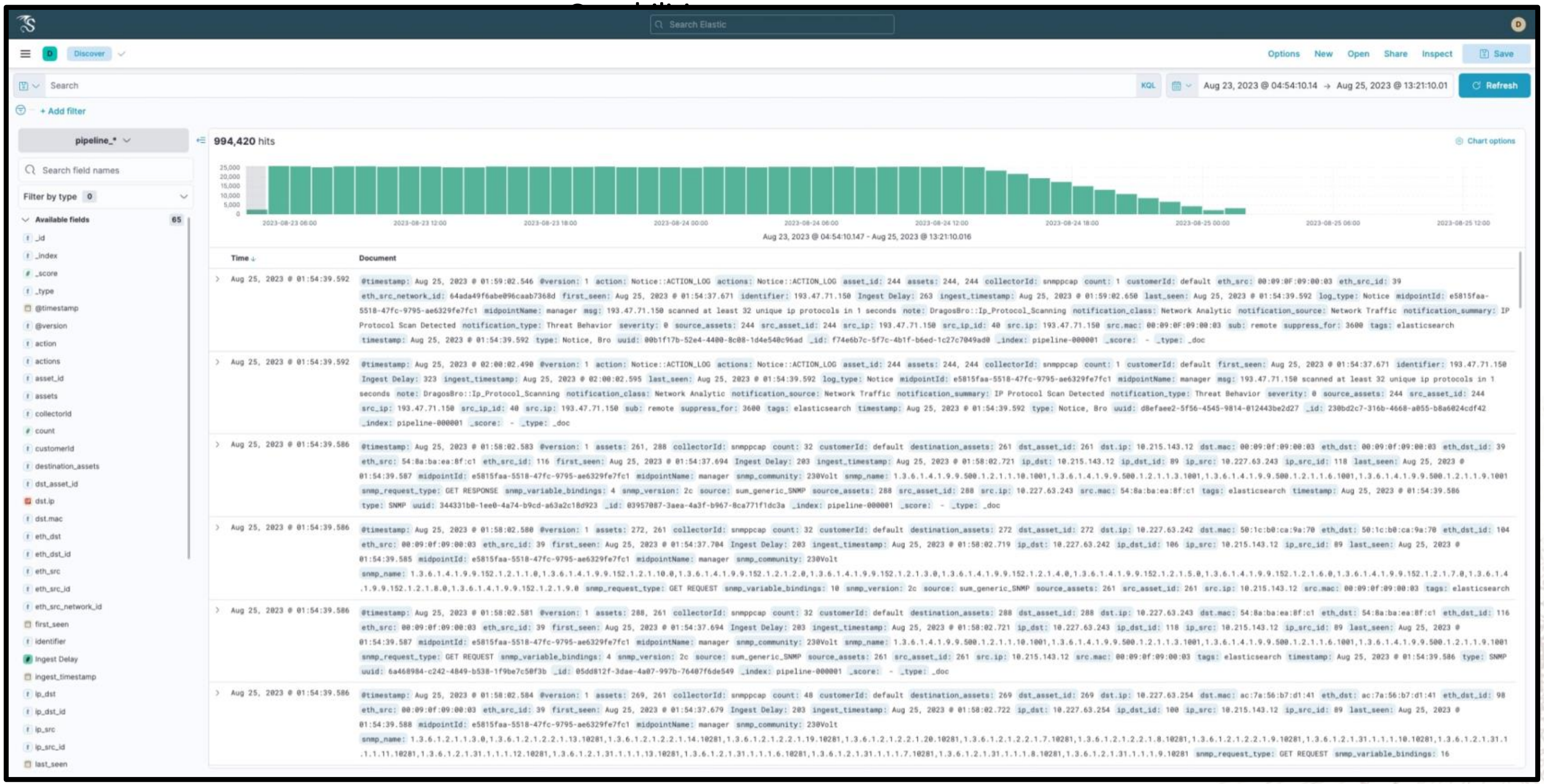
Last on Monday, September 4, 2023 3:48 PM

3 events

🟩 Cisco Cyber Vision Operations: 100%

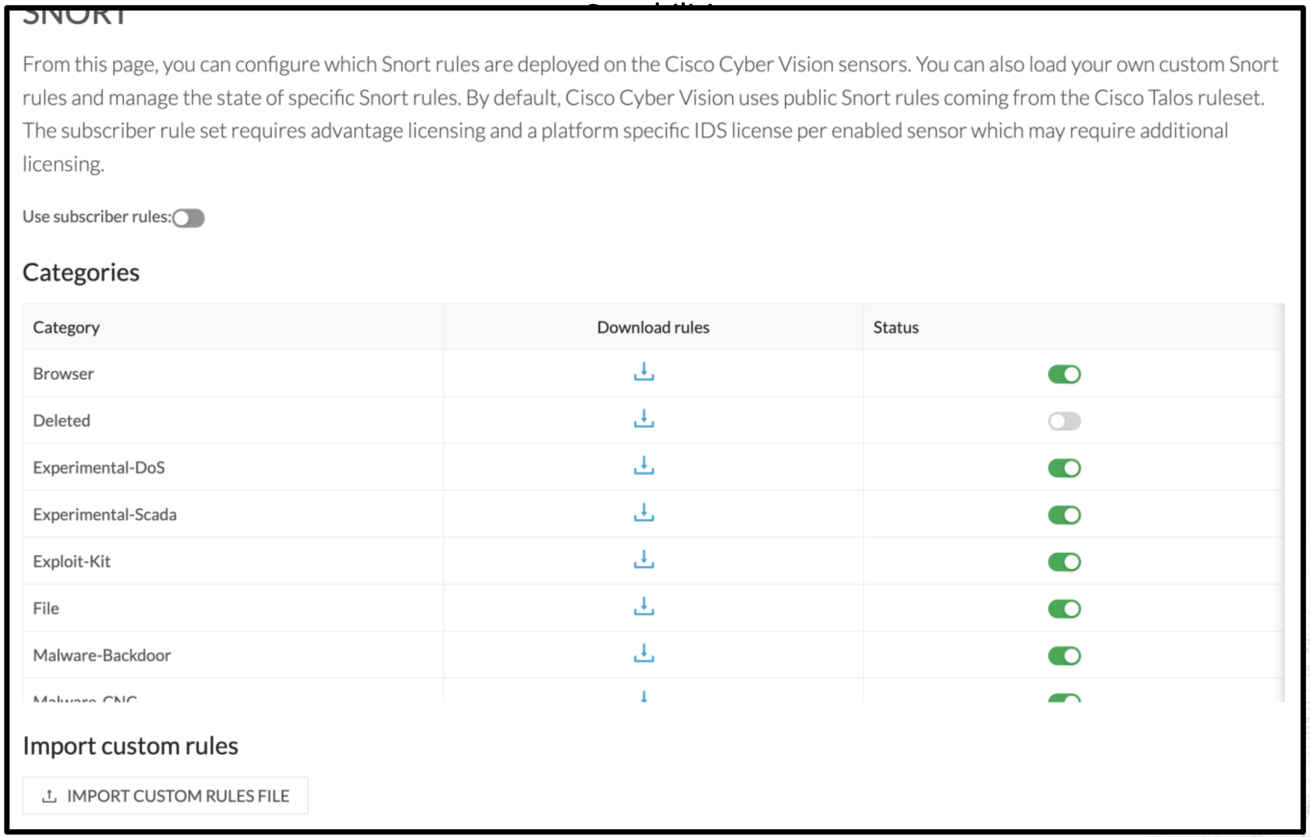
60%

Custom Detection



```
Time ↓                        Document

> Aug 25, 2023 @ 01:54:39.592  @timestamp: Aug 25, 2023 @ 01:59:02.546 @version: 1 action: Notice::ACTION_LOG actions: Notice::ACTION_LOG asset_id: 244 assets: 244, 244 collectorId: snmppcap count: 1 customerId: default eth_src: 00:09:0F:09:00:03 eth_src_id: 39
                               eth_src_network_id: 64ada49f6abe096caab7368d first_seen: Aug 25, 2023 @ 01:54:37.671 identifier: 193.47.71.150 Ingest Delay: 263 ingest_timestamp: Aug 25, 2023 @ 01:59:02.650 last_seen: Aug 25, 2023 @ 01:54:39.592 log_type: Notice midpointId: e5815faa-
                               5518-47fc-9795-ae6329fe7fc1 midpointName: manager msg: 193.47.71.150 scanned at least 32 unique ip protocols in 1 seconds note: DragosBro::Ip_Protocol_Scanning notification_class: Network Analytic notification_source: Network Traffic notification_summary: IP
                               Protocol Scan Detected notification_type: Threat Behavior severity: 0 source_assets: 244 src_asset_id: 244 src_ip: 193.47.71.150 src_ip_id: 40 src.ip: 193.47.71.150 src.mac: 00:09:0F:09:00:03 sub: remote suppress_for: 3600 tags: elasticsearch
                               timestamp: Aug 25, 2023 @ 01:54:39.592 type: Notice, Bro uuid: 00b1f17b-52e4-4400-8c08-1d4e540c96ad _id: f74e6b7c-5f7c-4b1f-b6ed-1c27c7049ad0 _index: pipeline-000001 _score: - _type: _doc

> Aug 25, 2023 @ 01:54:39.592  @timestamp: Aug 25, 2023 @ 02:00:02.490 @version: 1 action: Notice::ACTION_LOG actions: Notice::ACTION_LOG asset_id: 244 assets: 244, 244 collectorId: snmppcap count: 1 customerId: default first_seen: Aug 25, 2023 @ 01:54:37.671 identifier: 193.47.71.150
                               Ingest Delay: 323 ingest_timestamp: Aug 25, 2023 @ 02:00:02.595 last_seen: Aug 25, 2023 @ 01:54:39.592 log_type: Notice midpointId: e5815faa-5518-47fc-9795-ae6329fe7fc1 midpointName: manager msg: 193.47.71.150 scanned at least 32 unique ip protocols in 1
                               seconds note: DragosBro::Ip_Protocol_Scanning notification_class: Network Analytic notification_source: Network Traffic notification_summary: IP Protocol Scan Detected notification_type: Threat Behavior severity: 0 source_assets: 244 src_asset_id: 244
                               src_ip: 193.47.71.150 src_ip_id: 40 src.ip: 193.47.71.150 sub: remote suppress_for: 3600 tags: elasticsearch timestamp: Aug 25, 2023 @ 01:54:39.592 type: Notice, Bro uuid: d8efaee2-5f56-4545-9814-012443be2d27 _id: 230bd2c7-316b-4668-a055-b8a6024cdf42
                               _index: pipeline-000001 _score: - _type: _doc

> Aug 25, 2023 @ 01:54:39.586  @timestamp: Aug 25, 2023 @ 01:58:02.583 @version: 1 assets: 261, 288 collectorId: snmppcap count: 32 customerId: default destination_assets: 261 dst_asset_id: 261 dst.ip: 10.215.143.12 dst.mac: 00:09:0f:09:00:03 eth_dst: 00:09:0f:09:00:03 eth_dst_id: 39
                               eth_src: 54:8a:ba:ea:8f:c1 eth_src_id: 116 first_seen: Aug 25, 2023 @ 01:54:37.694 Ingest Delay: 203 ingest_timestamp: Aug 25, 2023 @ 01:58:02.721 ip_dst: 10.215.143.12 ip_dst_id: 89 ip_src: 10.227.63.243 ip_src_id: 118 last_seen: Aug 25, 2023 @
                               01:54:39.587 midpointId: e5815faa-5518-47fc-9795-ae6329fe7fc1 midpointName: manager snmp_community: 230Volt snmp_name: 1.3.6.1.4.1.9.9.500.1.2.1.1.10.1001,1.3.6.1.4.1.9.9.500.1.2.1.1.3.1001,1.3.6.1.4.1.9.9.500.1.2.1.1.6.1001,1.3.6.1.4.1.9.9.500.1.2.1.1.9.1001
                               snmp_request_type: GET RESPONSE snmp_variable_bindings: 4 snmp_version: 2c source: sum_generic_SNMP source_assets: 288 src_asset_id: 288 src.ip: 10.227.63.243 src.mac: 54:8a:ba:ea:8f:c1 tags: elasticsearch timestamp: Aug 25, 2023 @ 01:54:39.586
                               type: SNMP uuid: 344331b0-1ee0-4a74-b9cd-a63a2c18d923 _id: 03957087-3aea-4a3f-b967-8ca771f1dc3a _index: pipeline-000001 _score: - _type: _doc

> Aug 25, 2023 @ 01:54:39.586  @timestamp: Aug 25, 2023 @ 01:58:02.580 @version: 1 assets: 272, 261 collectorId: snmppcap count: 32 customerId: default destination_assets: 272 dst_asset_id: 272 dst.ip: 10.227.63.242 dst.mac: 50:1c:b0:ca:9a:70 eth_dst: 50:1c:b0:ca:9a:70 eth_dst_id: 104
                               eth_src: 00:09:0f:09:00:03 eth_src_id: 39 first_seen: Aug 25, 2023 @ 01:54:37.704 Ingest Delay: 203 ingest_timestamp: Aug 25, 2023 @ 01:58:02.719 ip_dst: 10.227.63.242 ip_dst_id: 106 ip_src: 10.215.143.12 ip_src_id: 89 last_seen: Aug 25, 2023 @
                               01:54:39.585 midpointId: e5815faa-5518-47fc-9795-ae6329fe7fc1 midpointName: manager snmp_community: 230Volt
                               snmp_name: 1.3.6.1.4.1.9.9.152.1.2.1.1.0,1.3.6.1.4.1.9.9.152.1.2.1.10.0,1.3.6.1.4.1.9.9.152.1.2.1.2.0,1.3.6.1.4.1.9.9.152.1.2.1.3.0,1.3.6.1.4.1.9.9.152.1.2.1.4.0,1.3.6.1.4.1.9.9.152.1.2.1.5.0,1.3.6.1.4.1.9.9.152.1.2.1.6.0,1.3.6.1.4.1.9.9.152.1.2.1.7.0,1.3.6.1.4
                               .1.9.9.152.1.2.1.8.0,1.3.6.1.4.1.9.9.152.1.2.1.9.0 snmp_request_type: GET REQUEST snmp_variable_bindings: 10 snmp_version: 2c source: sum_generic_SNMP source_assets: 261 src_asset_id: 261 src.ip: 10.215.143.12 src.mac: 00:09:0f:09:00:03 tags: elasticsearch

> Aug 25, 2023 @ 01:54:39.586  @timestamp: Aug 25, 2023 @ 01:58:02.581 @version: 1 assets: 288, 261 collectorId: snmppcap count: 32 customerId: default destination_assets: 288 dst_asset_id: 288 dst.ip: 10.227.63.243 dst.mac: 54:8a:ba:ea:8f:c1 eth_dst: 54:8a:ba:ea:8f:c1 eth_dst_id: 116
                               eth_src: 00:09:0f:09:00:03 eth_src_id: 39 first_seen: Aug 25, 2023 @ 01:54:37.694 Ingest Delay: 203 ingest_timestamp: Aug 25, 2023 @ 01:58:02.721 ip_dst: 10.227.63.243 ip_dst_id: 118 ip_src: 10.215.143.12 ip_src_id: 89 last_seen: Aug 25, 2023 @
                               01:54:39.587 midpointId: e5815faa-5518-47fc-9795-ae6329fe7fc1 midpointName: manager snmp_community: 230Volt snmp_name: 1.3.6.1.4.1.9.9.500.1.2.1.1.10.1001,1.3.6.1.4.1.9.9.500.1.2.1.1.3.1001,1.3.6.1.4.1.9.9.500.1.2.1.1.6.1001,1.3.6.1.4.1.9.9.500.1.2.1.1.9.1001
                               snmp_request_type: GET REQUEST snmp_variable_bindings: 4 snmp_version: 2c source: sum_generic_SNMP source_assets: 261 src_asset_id: 261 src.ip: 10.215.143.12 src.mac: 00:09:0f:09:00:03 tags: elasticsearch timestamp: Aug 25, 2023 @ 01:54:39.586 type: SNMP
                               uuid: 6a468984-c242-4849-b538-1f9be7c50f3b _id: 05dd812f-3dae-4a07-997b-76407f6de549 _index: pipeline-000001 _score: - _type: _doc

> Aug 25, 2023 @ 01:54:39.586  @timestamp: Aug 25, 2023 @ 01:58:02.584 @version: 1 assets: 269, 261 collectorId: snmppcap count: 48 customerId: default destination_assets: 269 dst_asset_id: 269 dst.ip: 10.227.63.254 dst.mac: ac:7a:56:b7:d1:41 eth_dst: ac:7a:56:b7:d1:41 eth_dst_id: 98
                               eth_src: 00:09:0f:09:00:03 eth_src_id: 39 first_seen: Aug 25, 2023 @ 01:54:37.679 Ingest Delay: 203 ingest_timestamp: Aug 25, 2023 @ 01:58:02.722 ip_dst: 10.227.63.254 ip_dst_id: 100 ip_src: 10.215.143.12 ip_src_id: 89 last_seen: Aug 25, 2023 @
                               01:54:39.588 midpointId: e5815faa-5518-47fc-9795-ae6329fe7fc1 midpointName: manager snmp_community: 230Volt
                               snmp_name: 1.3.6.1.2.1.1.3.0,1.3.6.1.2.1.2.2.1.13.10281,1.3.6.1.2.1.2.2.1.14.10281,1.3.6.1.2.1.2.2.1.19.10281,1.3.6.1.2.1.2.2.1.20.10281,1.3.6.1.2.1.2.2.1.7.10281,1.3.6.1.2.1.2.2.1.8.10281,1.3.6.1.2.1.2.2.1.9.10281,1.3.6.1.2.1.31.1.1.1.10.10281,1.3.6.1.2.1.31.1
                               .1.1.11.10281,1.3.6.1.2.1.31.1.1.1.12.10281,1.3.6.1.2.1.31.1.1.1.13.10281,1.3.6.1.2.1.31.1.1.1.6.10281,1.3.6.1.2.1.31.1.1.1.7.10281,1.3.6.1.2.1.31.1.1.1.8.10281,1.3.6.1.2.1.31.1.1.1.9.10281 snmp_request_type: GET REQUEST snmp_variable_bindings: 16
```

Custom Detection



SNORT

From this page, you can configure which Snort rules are deployed on the Cisco Cyber Vision sensors. You can also load your own custom Snort rules and manage the state of specific Snort rules. By default, Cisco Cyber Vision uses public Snort rules coming from the Cisco Talos ruleset. The subscriber rule set requires advantage licensing and a platform specific IDS license per enabled sensor which may require additional licensing.

Use subscriber rules: ○

Categories

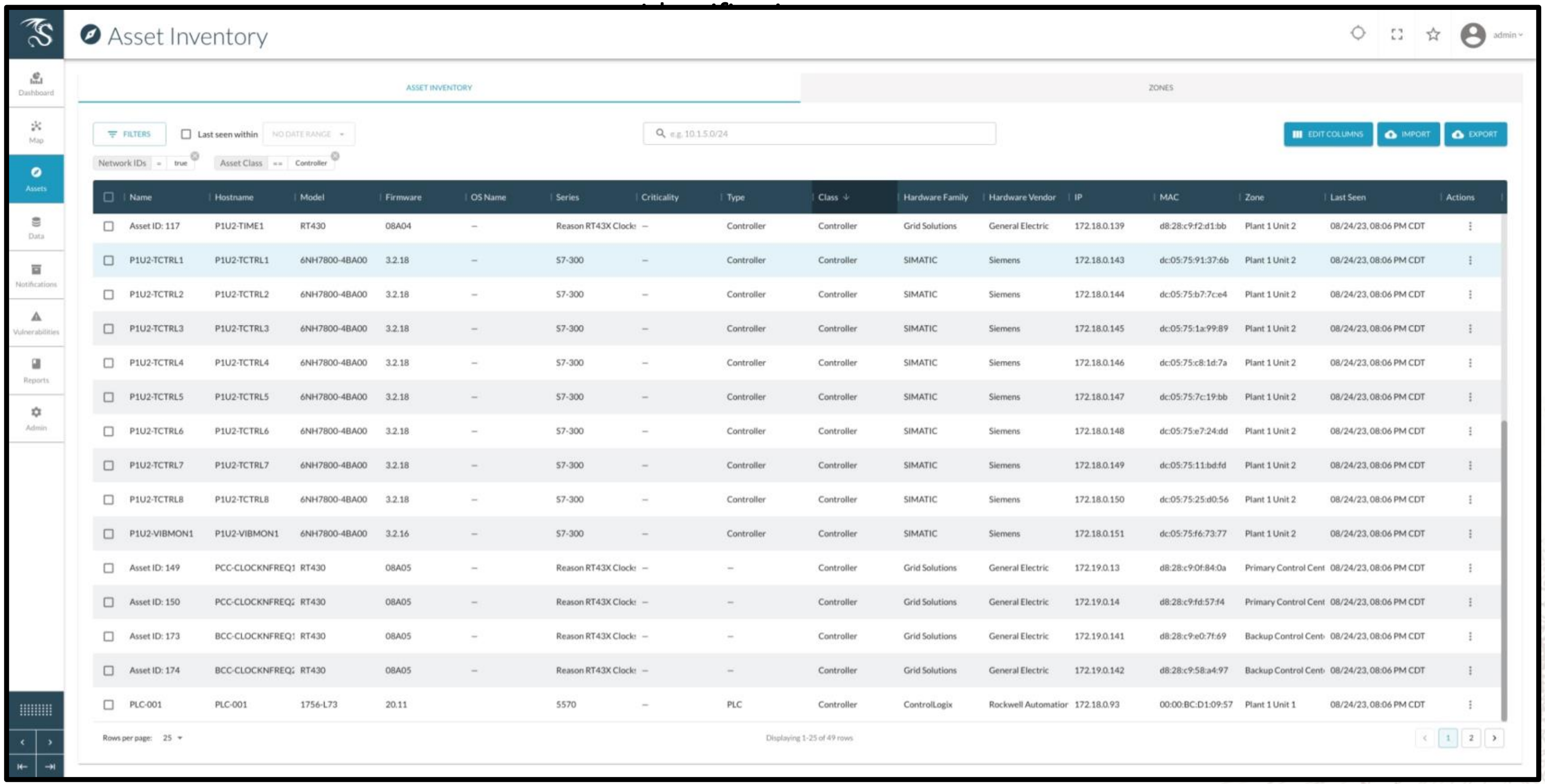
Category	Download rules	Status
Browser	↓	●
Deleted	↓	○
Experimental-DoS	↓	●
Experimental-Scada	↓	●
Exploit-Kit	↓	●
File	↓	●
Malware-Backdoor	↓	●
Malware-CNC	↓	●

Import custom rules

IMPORT CUSTOM RULES FILE

Dragos

Asset



□	Name	Hostname	Model	Firmware	OS Name	Series	Criticality	Type	Class ↓	Hardware Family	Hardware Vendor	IP	MAC	Zone	Last Seen	Actions
□	Asset ID: 117	P1U2-TIME1	RT430	08A04	–	Reason RT43X Clock:	–	Controller	Controller	Grid Solutions	General Electric	172.18.0.139	d8:28:c9:f2:d1:bb	Plant 1 Unit 2	08/24/23, 08:06 PM CDT	⋮
□	P1U2-TCTRL1	P1U2-TCTRL1	6NH7800-4BA00	3.2.18	–	S7-300	–	Controller	Controller	SIMATIC	Siemens	172.18.0.143	dc:05:75:91:37:6b	Plant 1 Unit 2	08/24/23, 08:06 PM CDT	⋮
□	P1U2-TCTRL2	P1U2-TCTRL2	6NH7800-4BA00	3.2.18	–	S7-300	–	Controller	Controller	SIMATIC	Siemens	172.18.0.144	dc:05:75:b7:7c:e4	Plant 1 Unit 2	08/24/23, 08:06 PM CDT	⋮
□	P1U2-TCTRL3	P1U2-TCTRL3	6NH7800-4BA00	3.2.18	–	S7-300	–	Controller	Controller	SIMATIC	Siemens	172.18.0.145	dc:05:75:1a:99:89	Plant 1 Unit 2	08/24/23, 08:06 PM CDT	⋮
□	P1U2-TCTRL4	P1U2-TCTRL4	6NH7800-4BA00	3.2.18	–	S7-300	–	Controller	Controller	SIMATIC	Siemens	172.18.0.146	dc:05:75:c8:1d:7a	Plant 1 Unit 2	08/24/23, 08:06 PM CDT	⋮
□	P1U2-TCTRL5	P1U2-TCTRL5	6NH7800-4BA00	3.2.18	–	S7-300	–	Controller	Controller	SIMATIC	Siemens	172.18.0.147	dc:05:75:7c:19:bb	Plant 1 Unit 2	08/24/23, 08:06 PM CDT	⋮
□	P1U2-TCTRL6	P1U2-TCTRL6	6NH7800-4BA00	3.2.18	–	S7-300	–	Controller	Controller	SIMATIC	Siemens	172.18.0.148	dc:05:75:e7:24:dd	Plant 1 Unit 2	08/24/23, 08:06 PM CDT	⋮
□	P1U2-TCTRL7	P1U2-TCTRL7	6NH7800-4BA00	3.2.18	–	S7-300	–	Controller	Controller	SIMATIC	Siemens	172.18.0.149	dc:05:75:11:bd:fd	Plant 1 Unit 2	08/24/23, 08:06 PM CDT	⋮
□	P1U2-TCTRL8	P1U2-TCTRL8	6NH7800-4BA00	3.2.18	–	S7-300	–	Controller	Controller	SIMATIC	Siemens	172.18.0.150	dc:05:75:25:d0:56	Plant 1 Unit 2	08/24/23, 08:06 PM CDT	⋮
□	P1U2-VIBMON1	P1U2-VIBMON1	6NH7800-4BA00	3.2.16	–	S7-300	–	Controller	Controller	SIMATIC	Siemens	172.18.0.151	dc:05:75:f6:73:77	Plant 1 Unit 2	08/24/23, 08:06 PM CDT	⋮
□	Asset ID: 149	PCC-CLOCKNFREQ1	RT430	08A05	–	Reason RT43X Clock:	–	–	Controller	Grid Solutions	General Electric	172.19.0.13	d8:28:c9:0f:84:0a	Primary Control Cent	08/24/23, 08:06 PM CDT	⋮
□	Asset ID: 150	PCC-CLOCKNFREQ:	RT430	08A05	–	Reason RT43X Clock:	–	–	Controller	Grid Solutions	General Electric	172.19.0.14	d8:28:c9:fd:57:f4	Primary Control Cent	08/24/23, 08:06 PM CDT	⋮
□	Asset ID: 173	BCC-CLOCKNFREQ:	RT430	08A05	–	Reason RT43X Clock:	–	–	Controller	Grid Solutions	General Electric	172.19.0.141	d8:28:c9:e0:7f:69	Backup Control Cent	08/24/23, 08:06 PM CDT	⋮
□	Asset ID: 174	BCC-CLOCKNFREQ:	RT430	08A05	–	Reason RT43X Clock:	–	–	Controller	Grid Solutions	General Electric	172.19.0.142	d8:28:c9:58:a4:97	Backup Control Cent	08/24/23, 08:06 PM CDT	⋮
□	PLC-001	PLC-001	1756-L73	20.11		5570	–	PLC	Controller	ControlLogix	Rockwell Automatior	172.18.0.93	00:00:BC:D1:09:57	Plant 1 Unit 1	08/24/23, 08:06 PM CDT	⋮

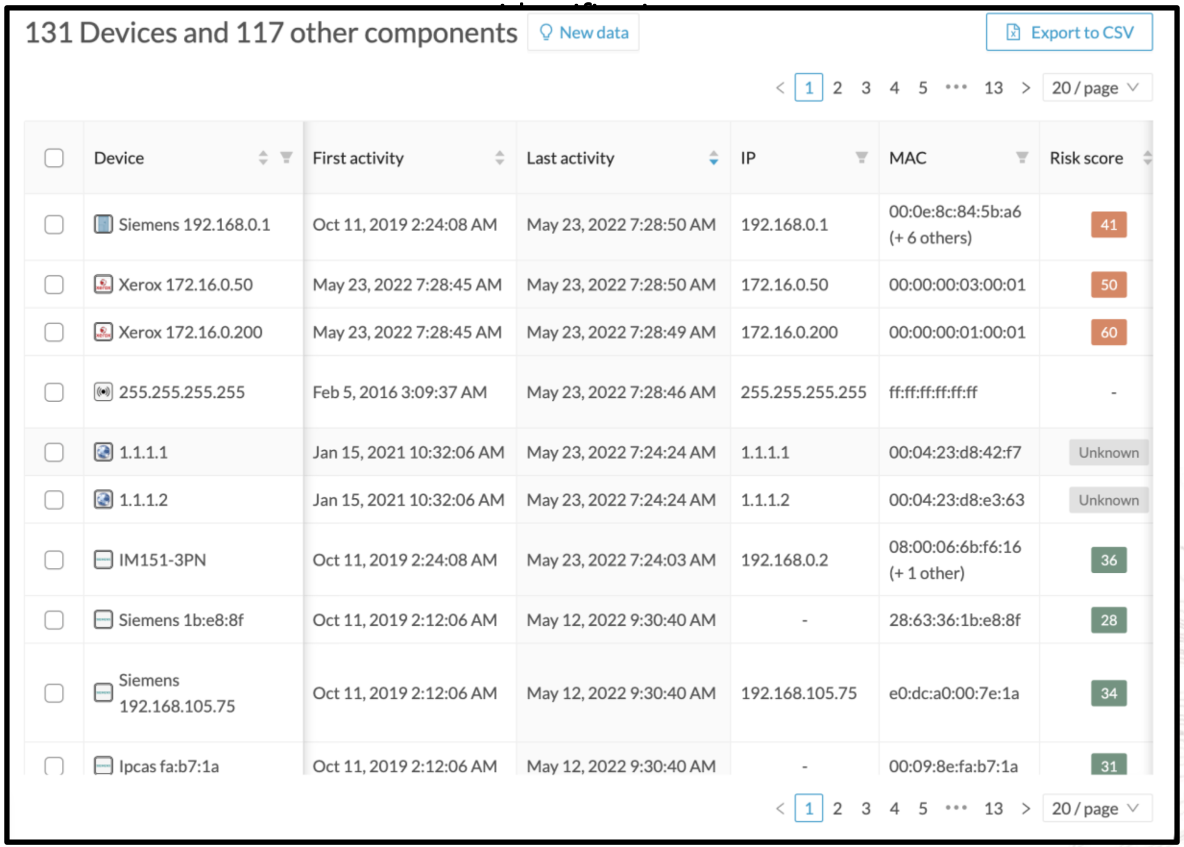
Rows per page: 25

Displaying 1-25 of 49 rows

‹ 1 2 ›

Cisco Cyber Vision

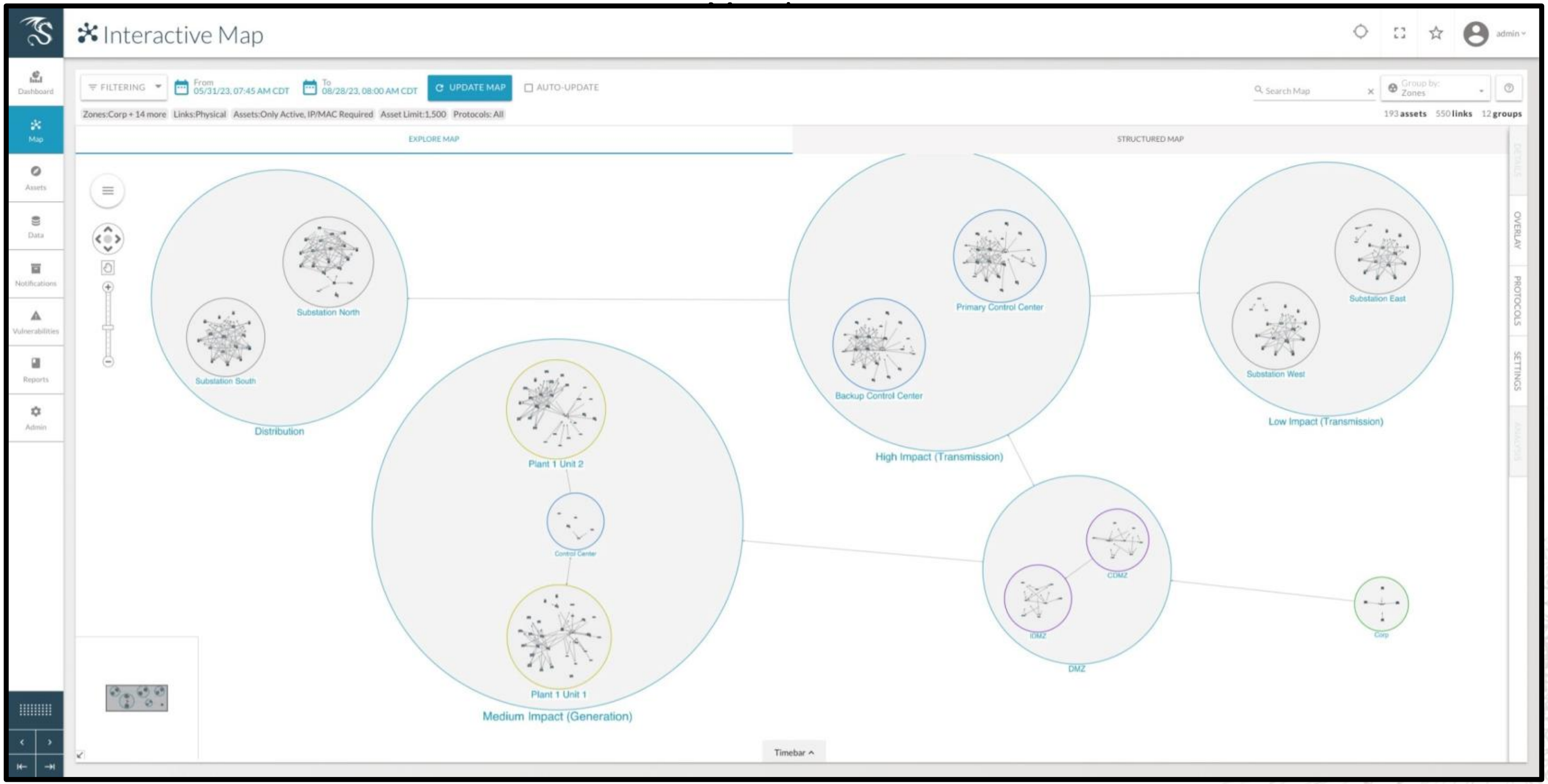
Asset



131 Devices and 117 other components

□	Device	First activity	Last activity	IP	MAC	Risk score
□	Siemens 192.168.0.1	Oct 11, 2019 2:24:08 AM	May 23, 2022 7:28:50 AM	192.168.0.1	00:0e:8c:84:5b:a6 (+ 6 others)	41
□	Xerox 172.16.0.50	May 23, 2022 7:28:45 AM	May 23, 2022 7:28:50 AM	172.16.0.50	00:00:00:03:00:01	50
□	Xerox 172.16.0.200	May 23, 2022 7:28:45 AM	May 23, 2022 7:28:49 AM	172.16.0.200	00:00:00:01:00:01	60
□	255.255.255.255	Feb 5, 2016 3:09:37 AM	May 23, 2022 7:28:46 AM	255.255.255.255	ff:ff:ff:ff:ff:ff	-
□	1.1.1.1	Jan 15, 2021 10:32:06 AM	May 23, 2022 7:24:24 AM	1.1.1.1	00:04:23:d8:42:f7	Unknown
□	1.1.1.2	Jan 15, 2021 10:32:06 AM	May 23, 2022 7:24:24 AM	1.1.1.2	00:04:23:d8:e3:63	Unknown
□	IM151-3PN	Oct 11, 2019 2:24:08 AM	May 23, 2022 7:24:03 AM	192.168.0.2	08:00:06:6b:f6:16 (+ 1 other)	36
□	Siemens 1b:e8:8f	Oct 11, 2019 2:12:06 AM	May 12, 2022 9:30:40 AM	-	28:63:36:1b:e8:8f	28
□	Siemens 192.168.105.75	Oct 11, 2019 2:12:06 AM	May 12, 2022 9:30:40 AM	192.168.105.75	e0:dc:a0:00:7e:1a	34
□	Ipcas fa:b7:1a	Oct 11, 2019 2:12:06 AM	May 12, 2022 9:30:40 AM	-	00:09:8e:fa:b7:1a	31

Network Flow



Interactive Map

FILTERING

From 05/31/23, 07:45 AM CDT

To 08/28/23, 08:00 AM CDT

UPDATE MAP

□ AUTO-UPDATE

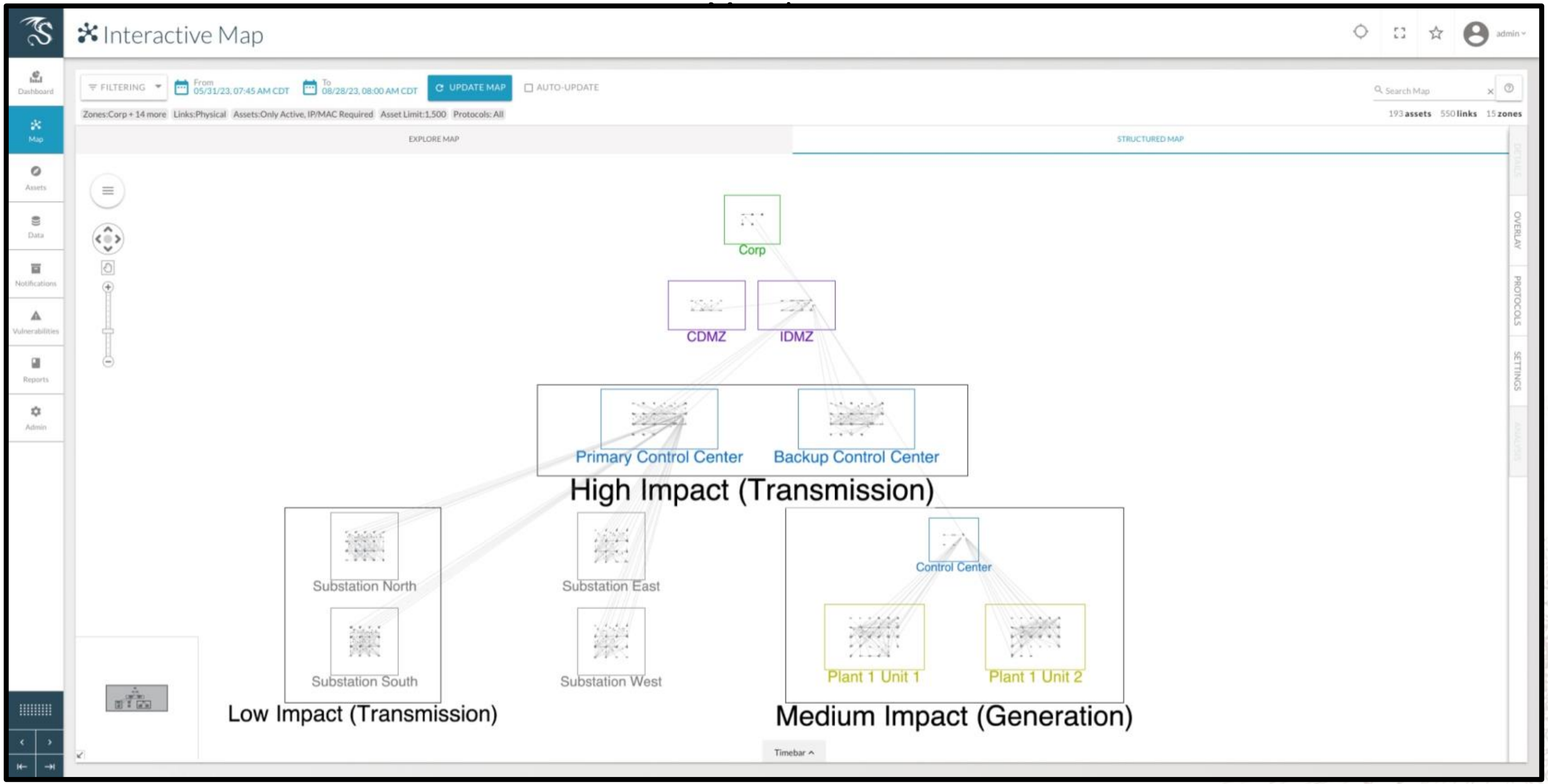
Zones:Corp + 14 more · Links:Physical · Assets:Only Active, IP/MAC Required · Asset Limit:1,500 · Protocols: All

Group by: Zones

193 assets 550 links 12 groups

Dragos

Network Flow



Interactive Map

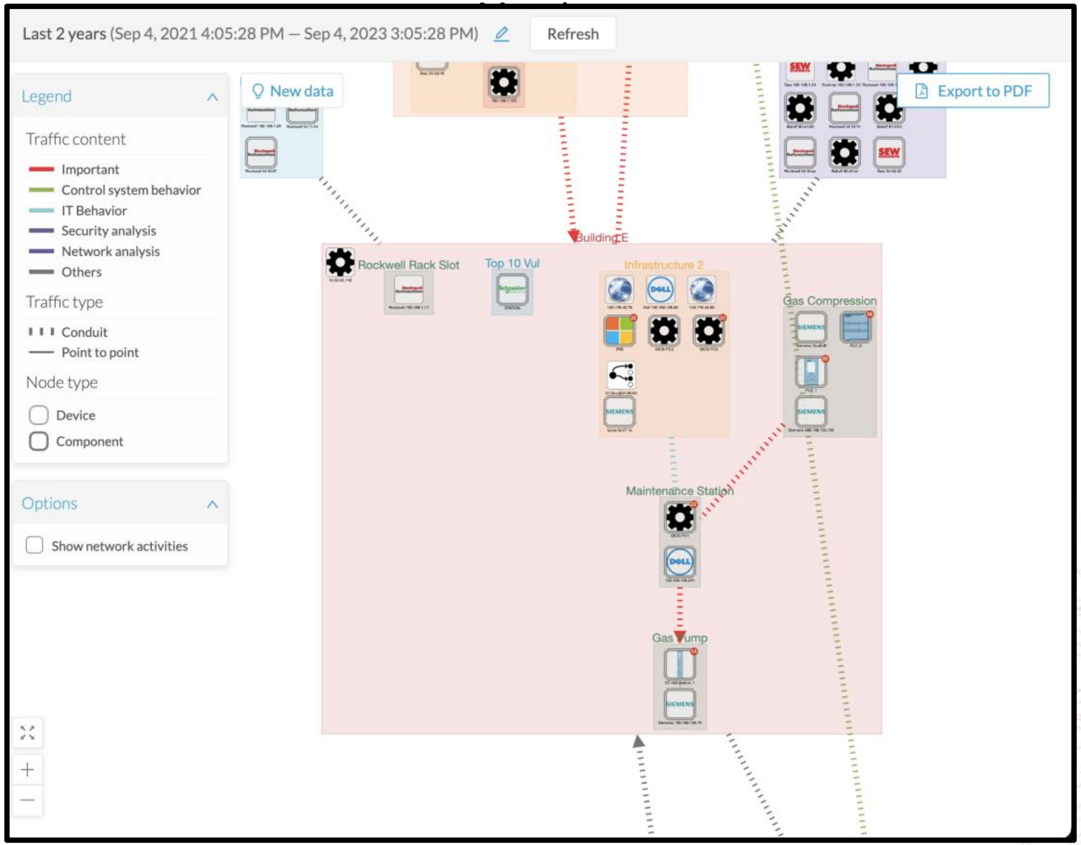
FILTERING | From 05/31/23, 07:45 AM CDT | To 08/28/23, 08:00 AM CDT | UPDATE MAP | □ AUTO-UPDATE

Zones:Corp + 14 more | Links:Physical | Assets:Only Active, IP/MAC Required | Asset Limit:1,500 | Protocols: All

193 **assets** 550 **links** 15 **zones**

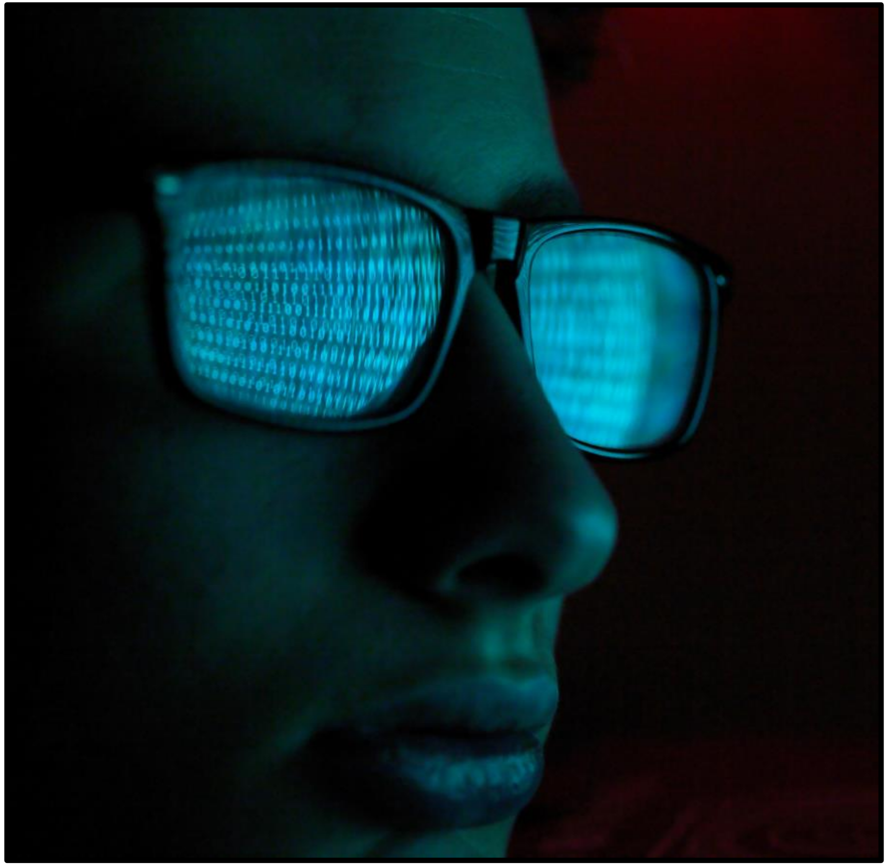
Cisco Cyber Vision

Network Flow



Last 2 years (Sep 4, 2021 4:05:28 PM — Sep 4, 2023 3:05:28 PM)

Third-party Threat Intelligence



Dragos

- WorldView

Cisco Cyber Vision

- Talos Intelligence Group

Setup and Implementation

Dragos:

- Rackmount the sensor appliance(s) and run associated cabling.
- Configure some basic addressing information.
- SPAN traffic from an Ethernet switch to start monitoring.

Cisco Cyber Vision:

- Set up the Cyber Vision Center virtual appliance or rackmount the physical appliance and run associated cabling. This only needs to happen once though.
- Configure a compatible Ethernet switch with IOX; may also need to upgrade firmware.
- Load the IOX Cyber Vision virtual application onto the Ethernet switch.
- Configure the VLAN, virtual application interface, ERSPAN, etc.
- Enable any necessary routing between the Ethernet switch and the Cyber Vision Center appliance.

Cloud Hosting Options

Dragos:

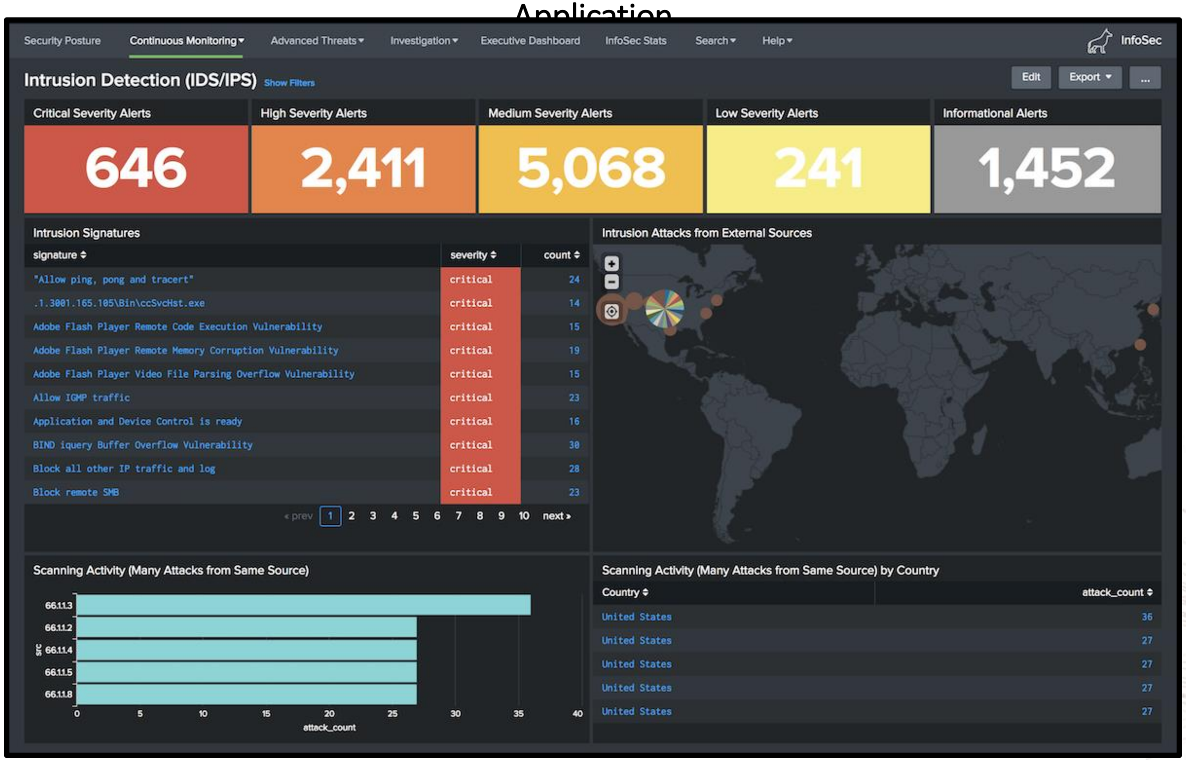
- Fully hosted solution utilizing Amazon Web Service (AWS).
- Includes licenses, automatic updates, and assistance with third-party integrations.

Cisco Cyber Vision:

- Can work with AWS, but you are responsible for management, licensing, etc.

SIEM Integration

Splunk InfoSec Application



Intrusion Detection (IDS/IPS)

Critical Severity Alerts	High Severity Alerts	Medium Severity Alerts	Low Severity Alerts	Informational Alerts
646	2,411	5,068	241	1,452

Intrusion Signatures

signature ⇕	severity ⇕	count ⇕
"Allow ping, pong and tracert"	critical	24
.1.3001.165.105\Bin\ccSvcHst.exe	critical	14
Adobe Flash Player Remote Code Execution Vulnerability	critical	15
Adobe Flash Player Remote Memory Corruption Vulnerability	critical	19
Adobe Flash Player Video File Parsing Overflow Vulnerability	critical	15
Allow IGMP traffic	critical	23
Application and Device Control is ready	critical	16
BIND iquery Buffer Overflow Vulnerability	critical	30
Block all other IP traffic and log	critical	28
Block remote SMB	critical	23

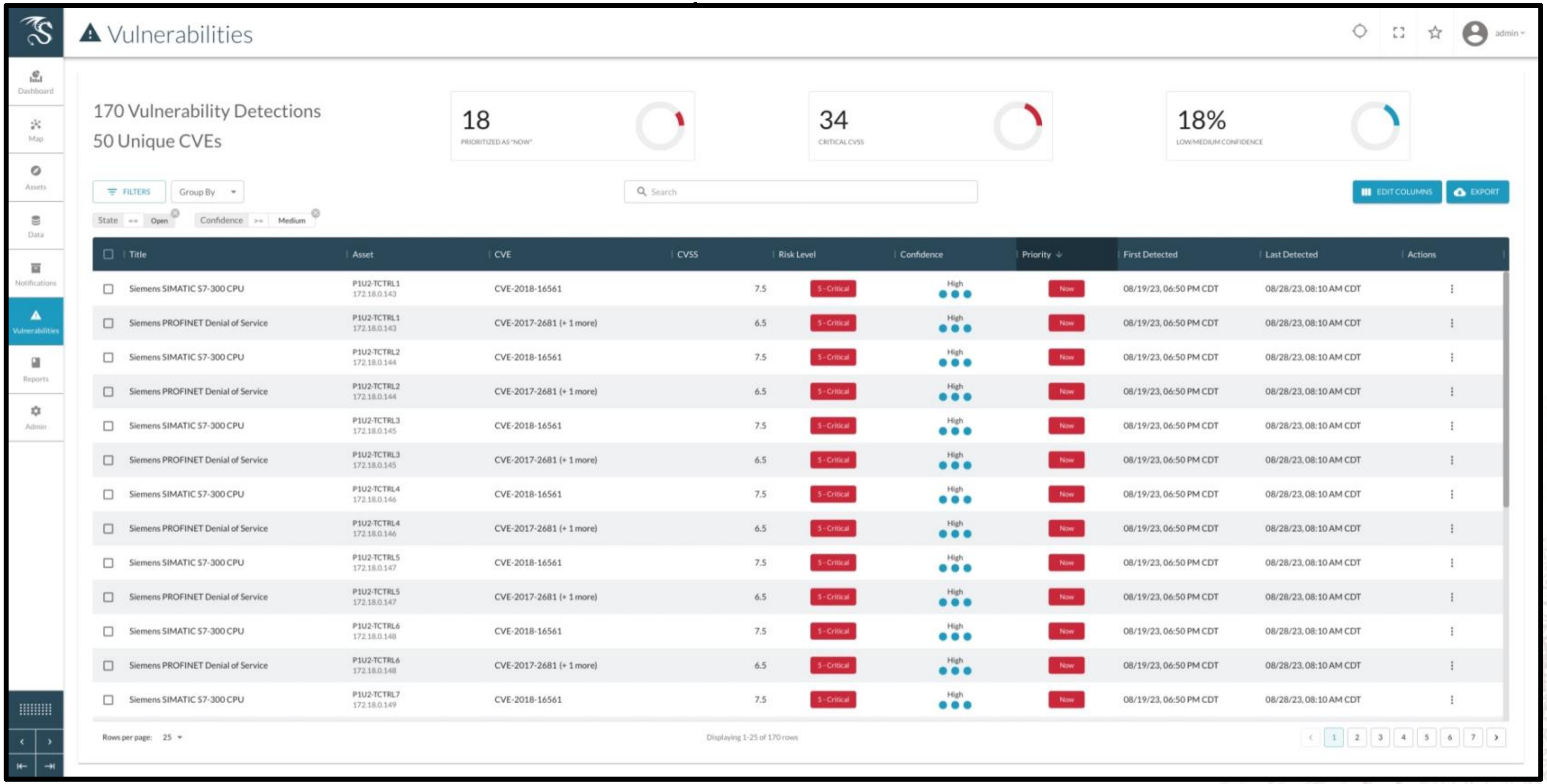
Intrusion Attacks from External Sources

Scanning Activity (Many Attacks from Same Source)

Scanning Activity (Many Attacks from Same Source) by Country

Country ⇕	attack_count ⇕
United States	36
United States	27
United States	27
United States	27
United States	27

Vulnerability



Vulnerabilities

170 Vulnerability Detections
50 Unique CVEs

18
PRIORITIZED AS "NOW"

34
CRITICAL CVSS

18%
LOW/MEDIUM CONFIDENCE

State == Open
Confidence >= Medium

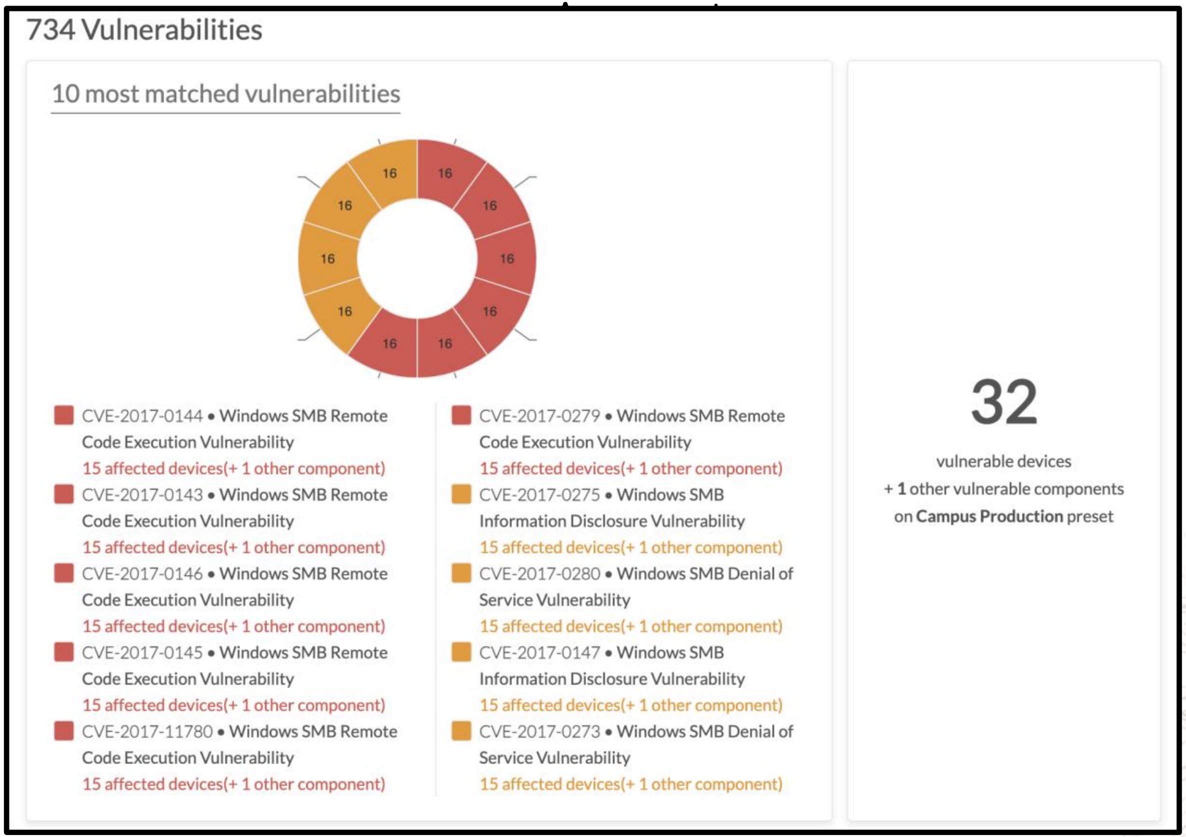
□	Title	Asset	CVE	CVSS	Risk Level	Confidence	Priority ↓	First Detected	Last Detected	Actions
□	Siemens SIMATIC S7-300 CPU	P1U2-TCTRL1 172.18.0.143	CVE-2018-16561	7.5	5 - Critical	High ●●●	Now	08/19/23, 06:50 PM CDT	08/28/23, 08:10 AM CDT	⋮
□	Siemens PROFINET Denial of Service	P1U2-TCTRL1 172.18.0.143	CVE-2017-2681 (+ 1 more)	6.5	5 - Critical	High ●●●	Now	08/19/23, 06:50 PM CDT	08/28/23, 08:10 AM CDT	⋮
□	Siemens SIMATIC S7-300 CPU	P1U2-TCTRL2 172.18.0.144	CVE-2018-16561	7.5	5 - Critical	High ●●●	Now	08/19/23, 06:50 PM CDT	08/28/23, 08:10 AM CDT	⋮
□	Siemens PROFINET Denial of Service	P1U2-TCTRL2 172.18.0.144	CVE-2017-2681 (+ 1 more)	6.5	5 - Critical	High ●●●	Now	08/19/23, 06:50 PM CDT	08/28/23, 08:10 AM CDT	⋮
□	Siemens SIMATIC S7-300 CPU	P1U2-TCTRL3 172.18.0.145	CVE-2018-16561	7.5	5 - Critical	High ●●●	Now	08/19/23, 06:50 PM CDT	08/28/23, 08:10 AM CDT	⋮
□	Siemens PROFINET Denial of Service	P1U2-TCTRL3 172.18.0.145	CVE-2017-2681 (+ 1 more)	6.5	5 - Critical	High ●●●	Now	08/19/23, 06:50 PM CDT	08/28/23, 08:10 AM CDT	⋮
□	Siemens SIMATIC S7-300 CPU	P1U2-TCTRL4 172.18.0.146	CVE-2018-16561	7.5	5 - Critical	High ●●●	Now	08/19/23, 06:50 PM CDT	08/28/23, 08:10 AM CDT	⋮
□	Siemens PROFINET Denial of Service	P1U2-TCTRL4 172.18.0.146	CVE-2017-2681 (+ 1 more)	6.5	5 - Critical	High ●●●	Now	08/19/23, 06:50 PM CDT	08/28/23, 08:10 AM CDT	⋮
□	Siemens SIMATIC S7-300 CPU	P1U2-TCTRL5 172.18.0.147	CVE-2018-16561	7.5	5 - Critical	High ●●●	Now	08/19/23, 06:50 PM CDT	08/28/23, 08:10 AM CDT	⋮
□	Siemens PROFINET Denial of Service	P1U2-TCTRL5 172.18.0.147	CVE-2017-2681 (+ 1 more)	6.5	5 - Critical	High ●●●	Now	08/19/23, 06:50 PM CDT	08/28/23, 08:10 AM CDT	⋮
□	Siemens SIMATIC S7-300 CPU	P1U2-TCTRL6 172.18.0.148	CVE-2018-16561	7.5	5 - Critical	High ●●●	Now	08/19/23, 06:50 PM CDT	08/28/23, 08:10 AM CDT	⋮
□	Siemens PROFINET Denial of Service	P1U2-TCTRL6 172.18.0.148	CVE-2017-2681 (+ 1 more)	6.5	5 - Critical	High ●●●	Now	08/19/23, 06:50 PM CDT	08/28/23, 08:10 AM CDT	⋮
□	Siemens SIMATIC S7-300 CPU	P1U2-TCTRL7 172.18.0.149	CVE-2018-16561	7.5	5 - Critical	High ●●●	Now	08/19/23, 06:50 PM CDT	08/28/23, 08:10 AM CDT	⋮

Rows per page: 25

Displaying 1-25 of 170 rows

‹ 1 2 3 4 5 6 7 ›

Vulnerability



734 Vulnerabilities

10 most matched vulnerabilities

🟥 CVE-2017-0144 • Windows SMB Remote Code Execution Vulnerability
15 affected devices(+ 1 other component)

🟥 CVE-2017-0143 • Windows SMB Remote Code Execution Vulnerability
15 affected devices(+ 1 other component)

🟥 CVE-2017-0146 • Windows SMB Remote Code Execution Vulnerability
15 affected devices(+ 1 other component)

🟥 CVE-2017-0145 • Windows SMB Remote Code Execution Vulnerability
15 affected devices(+ 1 other component)

🟥 CVE-2017-11780 • Windows SMB Remote Code Execution Vulnerability
15 affected devices(+ 1 other component)

🟥 CVE-2017-0279 • Windows SMB Remote Code Execution Vulnerability
15 affected devices(+ 1 other component)

🟧 CVE-2017-0275 • Windows SMB Information Disclosure Vulnerability
15 affected devices(+ 1 other component)

🟧 CVE-2017-0280 • Windows SMB Denial of Service Vulnerability
15 affected devices(+ 1 other component)

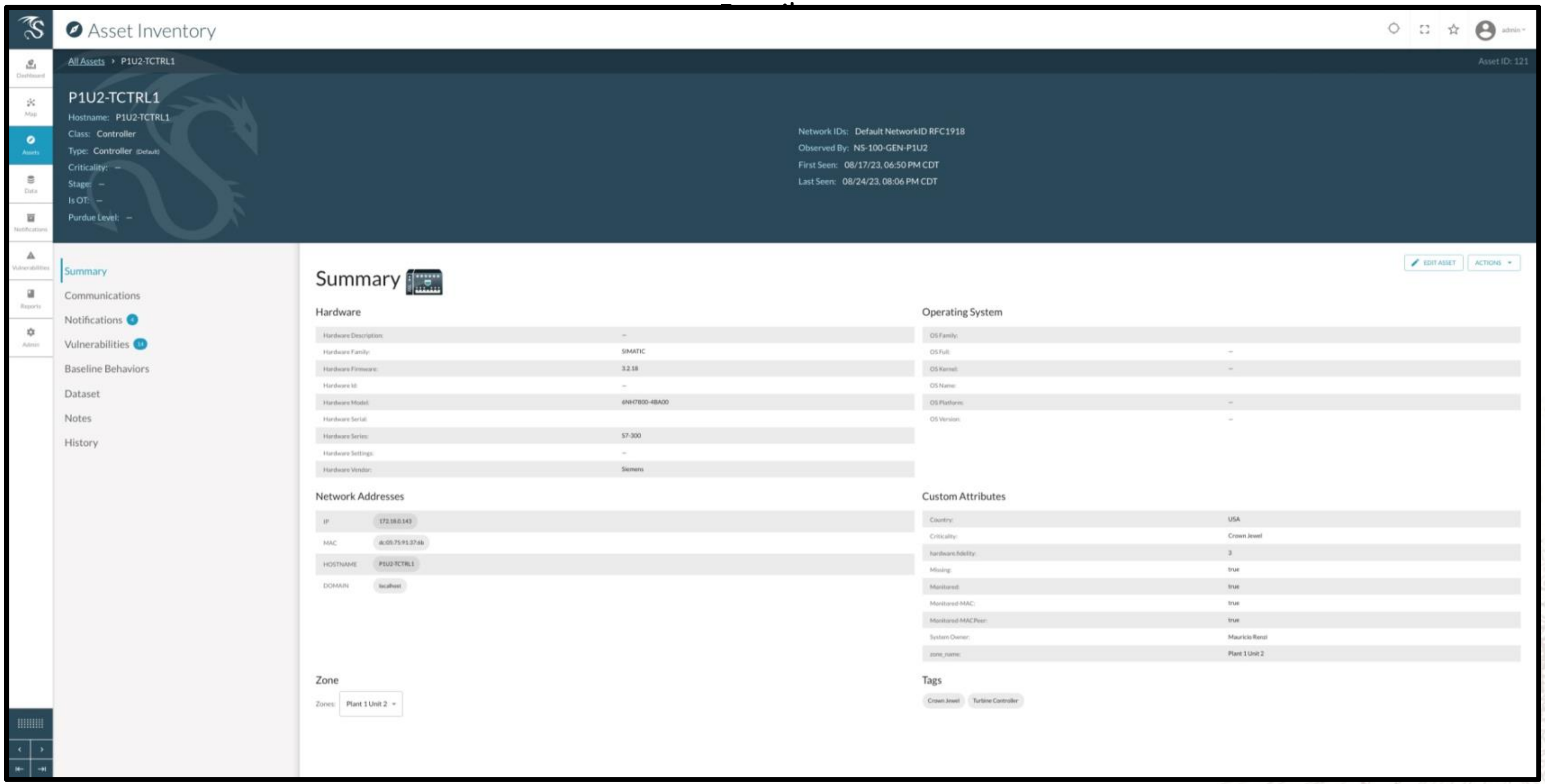
🟧 CVE-2017-0147 • Windows SMB Information Disclosure Vulnerability
15 affected devices(+ 1 other component)

🟧 CVE-2017-0273 • Windows SMB Denial of Service Vulnerability
15 affected devices(+ 1 other component)

32

vulnerable devices
+ **1** other vulnerable components
on **Campus Production** preset

Asset



All Assets › P1U2-TCTRL1

Asset ID: 121

P1U2-TCTRL1

Hostname: P1U2-TCTRL1
Class: Controller
Type: Controller (Default)
Criticality: –
Stage: –
Is OT: –
Purdue Level: –

Network IDs: Default NetworkID RFC1918
Observed By: NS-100-GEN-P1U2
First Seen: 08/17/23, 06:50 PM CDT
Last Seen: 08/24/23, 08:06 PM CDT

- Summary
- Communications
- Notifications 4
- Vulnerabilities 14
- Baseline Behaviors
- Dataset
- Notes
- History

Summary

Hardware

Hardware Description:	–
Hardware Family:	SIMATIC
Hardware Firmware:	3.2.18
Hardware Id:	–
Hardware Model:	6NH7800-4BA00
Hardware Serial:	
Hardware Series:	S7-300
Hardware Settings:	–
Hardware Vendor:	Siemens

Operating System

OS Family:	
OS Full:	–
OS Kernel:	–
OS Name:	
OS Platform:	–
OS Version:	–

Network Addresses

IP	172.18.0.143
MAC	dc:05:75:91:37:6b
HOSTNAME	P1U2-TCTRL1
DOMAIN	localhost

Custom Attributes

Country:	USA
Criticality:	Crown Jewel
hardware.fidelity:	3
Missing:	true
Monitored:	true
Monitored-MAC:	true
Monitored-MACPeer:	true
System Owner:	Mauricio Renzi
zone_name:	Plant 1 Unit 2

Zone

Zones: Plant 1 Unit 2

Tags

Crown Jewel
Turbine Controller

Tips for getting the most out of a potential solution

Network segmentation and zoning:

- This will help organize the network flow map and allow you to more quickly ascertain what's taking place in your network.

Implement a centralized firewall:

- This will help save on the number of sensors needing to be deployed in your environment.

Standardize addressing schemes:

- This will help you identify your assets, since the asset identification capabilities of these systems are currently limited in terms of scope.

Questions?

Scot Donecker

Enterprise Architect

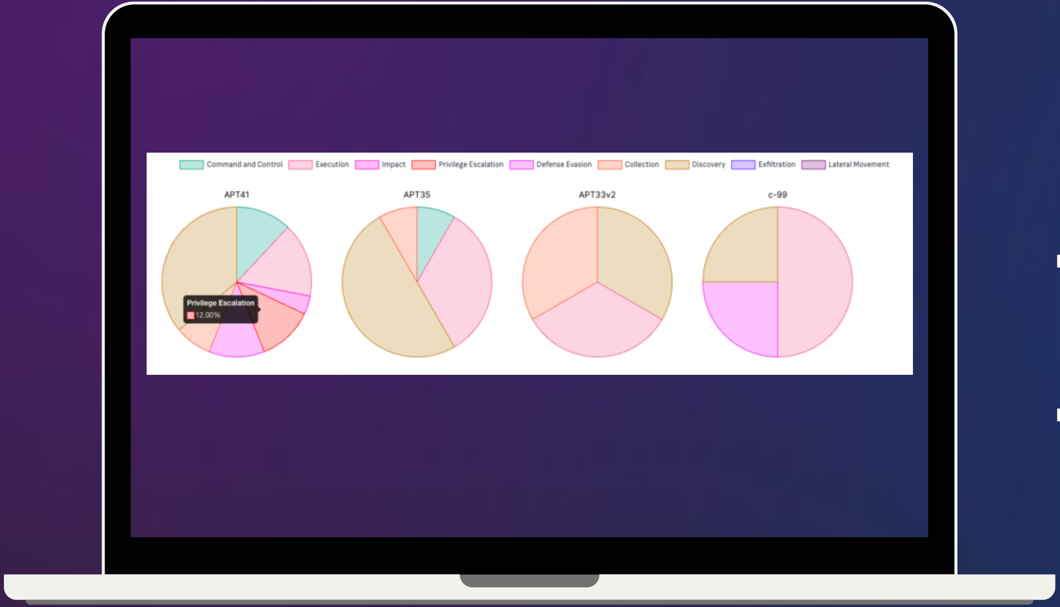
scot.donecker@sunflower.net

620-277-4779

RESPOND

DETECT

ATTACK



Introduction To Purple Teaming 101

@scythe_io

Intro

I’m Bryson

SCYTHE

GRIMM

ICS

Follow me **@brysonbort** for cooking, unicorns and infosec

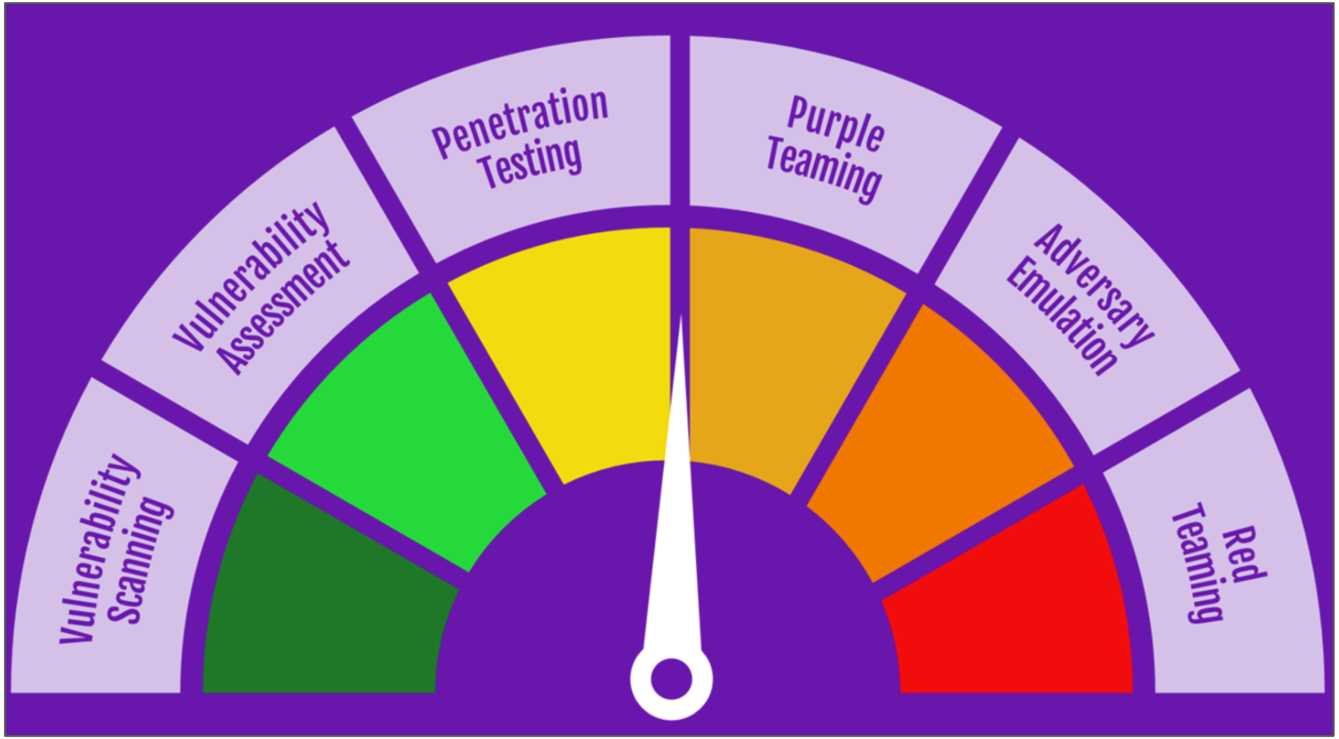
The Fish Tank

That thing you didn’t think about

What Is Purple Teaming?

Collaborative + Milestone-Driven Exercise

Testing Maturity



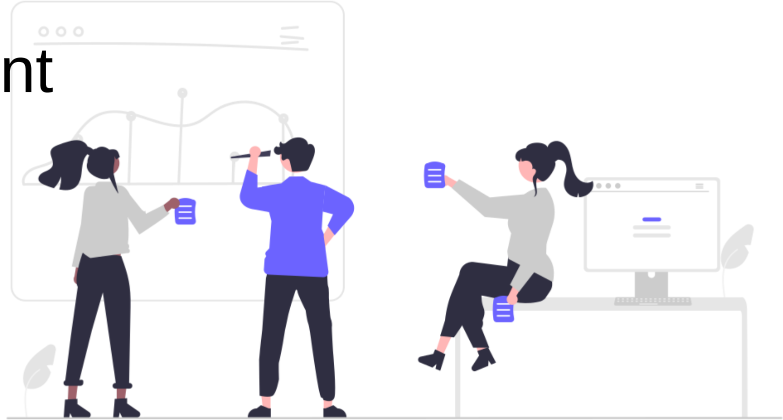
https://scythe.io/library/building-an-internal-red-team-go-purple-first

Poll:
Who’s done a Purple Team?

Purple Team

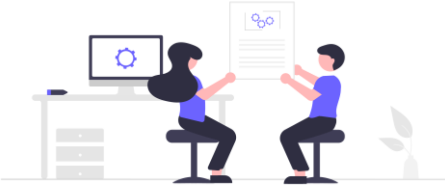
It starts with Leadership

- Organizational Change
- Cross-Functional Engagement



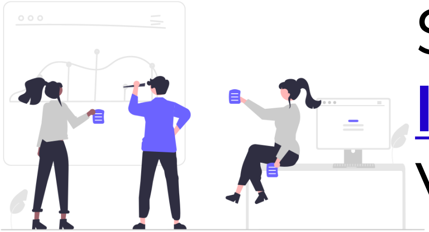
Why Purple Team?

Train Defenders



Improve Process Between Teams

Security is Defined by the Threat



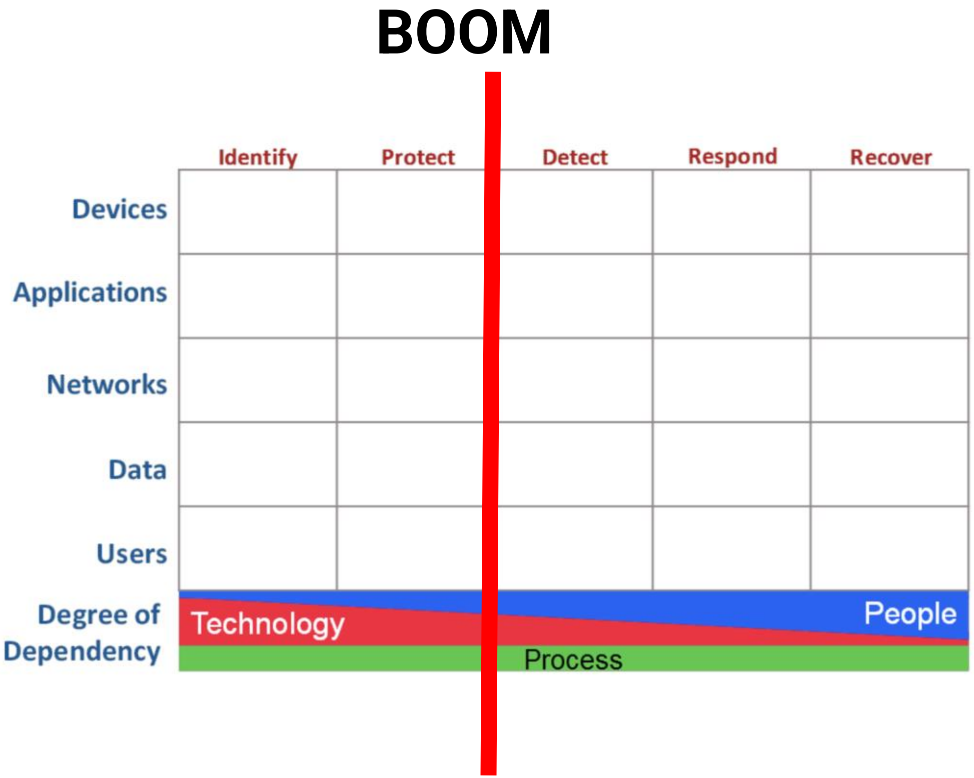
Show **Immediate** Value

Foster a collaborative culture and mentality

Where Do We Go: Cyber Defense Matrix

Structural
Awareness

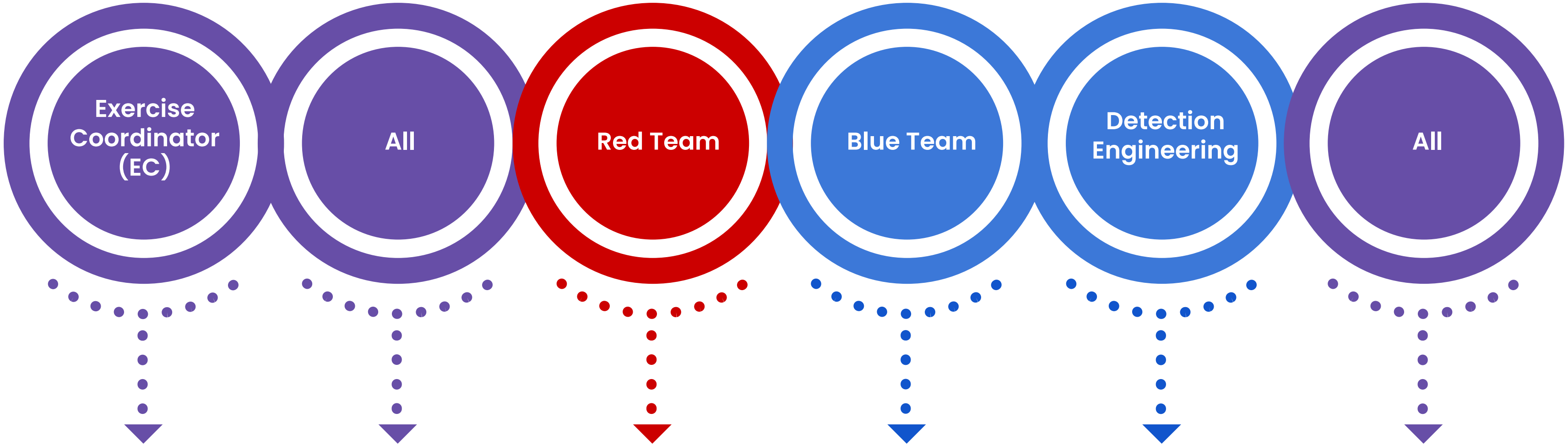
Operational
Awareness



	Identify	Protect	Detect	Respond	Recover
Devices					
Applications					
Networks					
Data					
Users					

https://cyberdefensematrix.com/ - *Sounil Yu*

Purple Team Exercise Flow



Exercise Coordinator (EC)

Present adversary, TTPs, and technical details

All

Table-top discussion of security controls and expectations for TTP execution

Red Team

Emulate the TTP while sharing the screen so everyone sees and learns what an attack looks like

Blue Team

Follow process to detect and respond to TTPs, share screen to confirm identification of artifacts

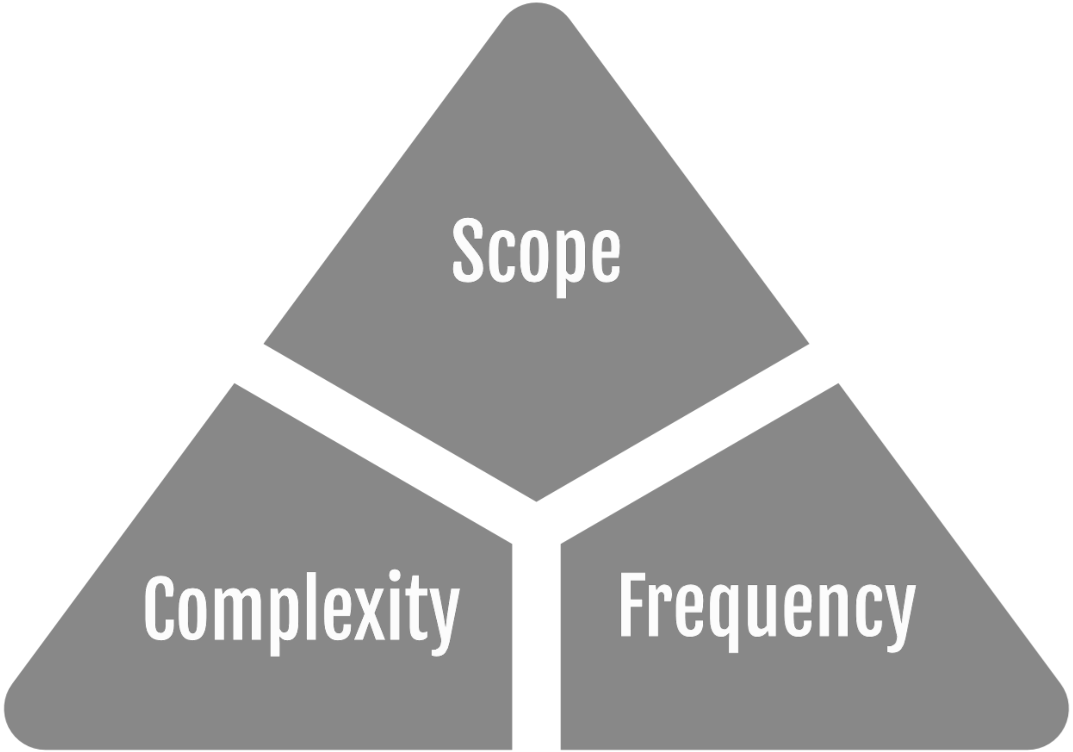
Detection Engineering

Can any adjustments or tuning to security controls and/or logging be made to increase visibility

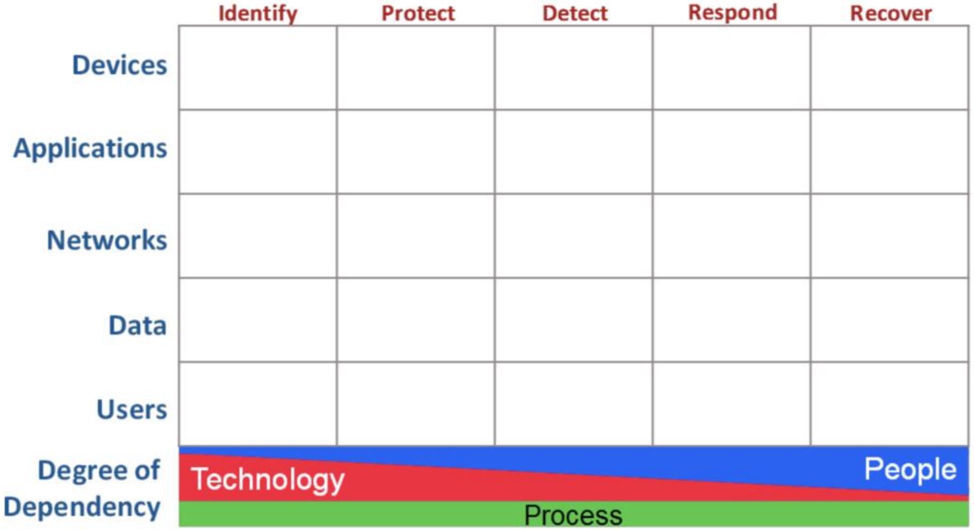
All

Repeat procedure and record new results, move to next TTP

Testing



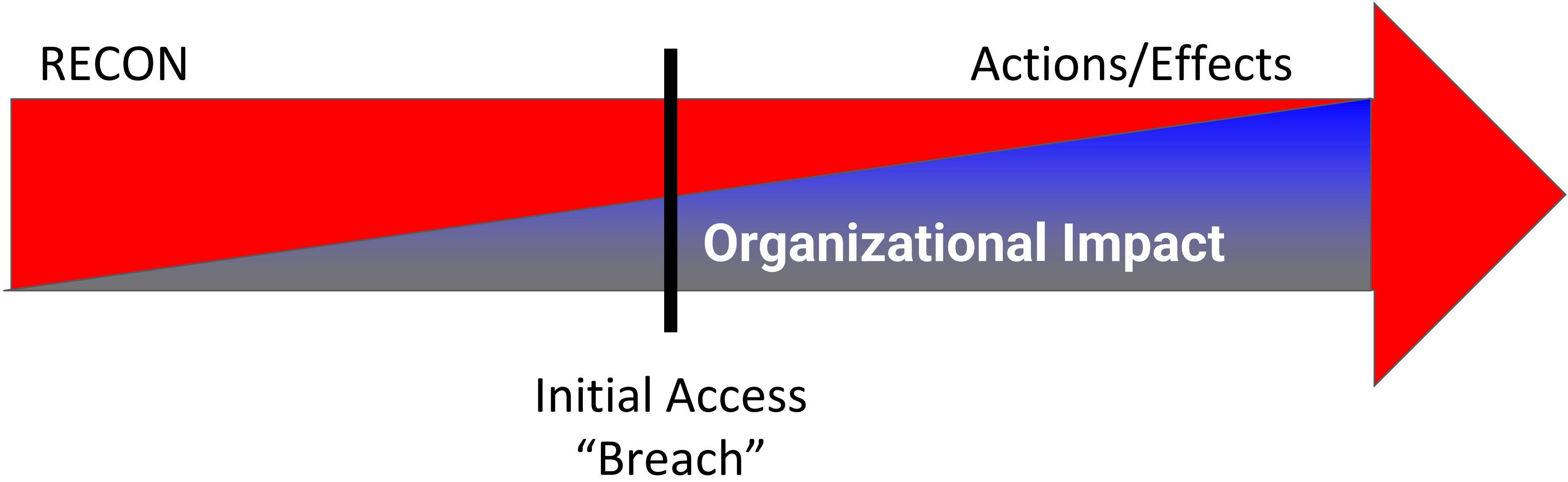
What’s in Scope?



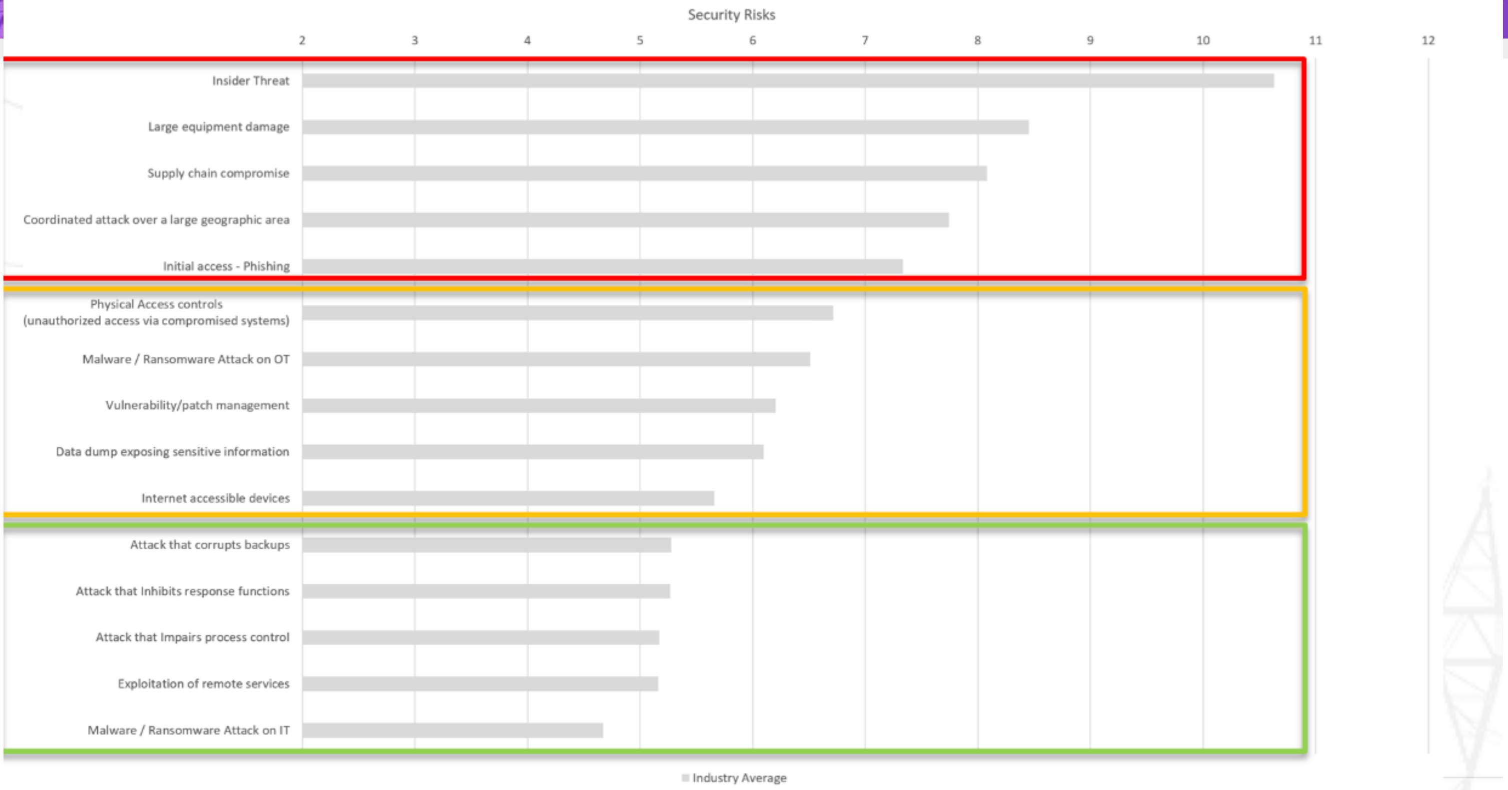
	Identify	Protect	Detect	Respond	Recover
Devices					
Applications					
Networks					
Data					
Users					

https://cyberdefensematrix.com/ - *Sounil Yu*

Scope: Bryson's Attack Model (BAM)



Security Risk Ranking



Scope: Efficiency in Testing

Why Assume Breach?

- Cost = Be the APT (on the cheap)
- Insider Threat
- Zero Day
- Phishing emails land
- Already breached

Additional Resources

- https://www.scythe.io/library/why-assume-breach
- https://posts.specterops.io/revisiting-phishing-simulations-94d9cd460934

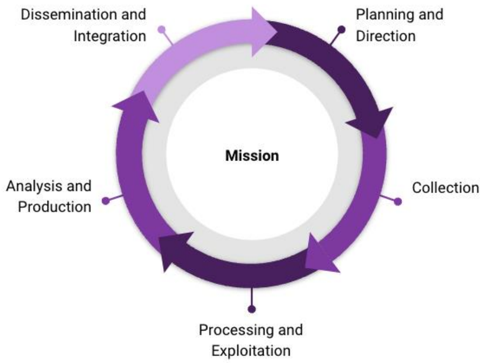
Types of Cyber Threat Intelligence

Our Focus

David Bianco: http://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html

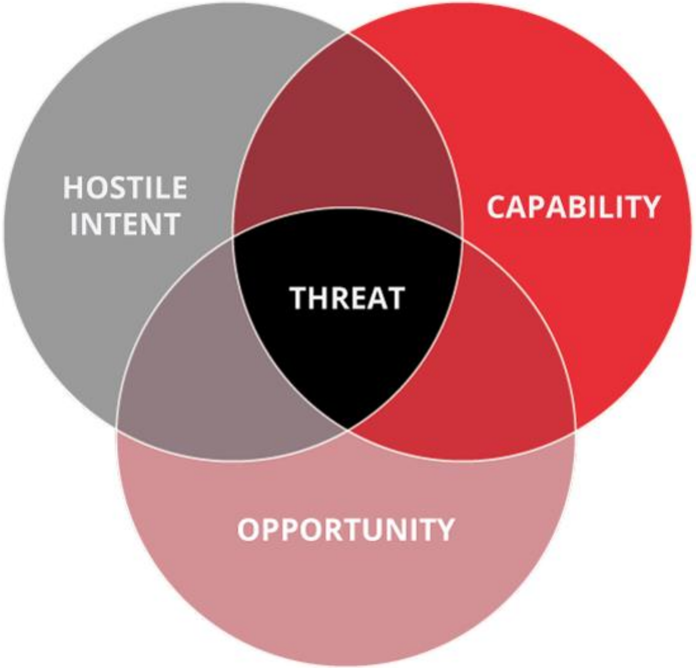
Intelligence Requirements

- Objectives the CTI Team should seek to fulfill.
- Examples:
  - Who is potentially targeting us?
  - Who should we prioritize to defend against?
  - What would it look like if they got in?
  - Would we detect them?



What is a Threat?

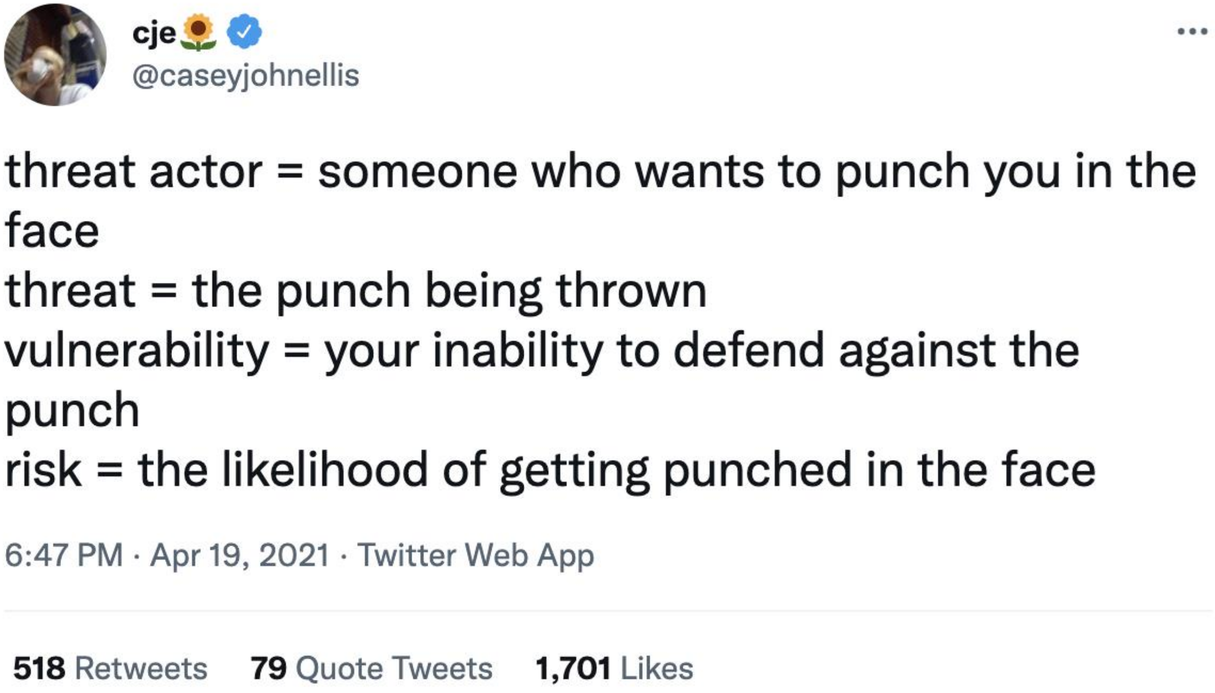
Who or What they are targeting.



The tools, exploits, training, and tradecraft the actor has access to.

The one area the organization has influence over: Limit opportunity through surface reduction, detection, and response.

Definitions



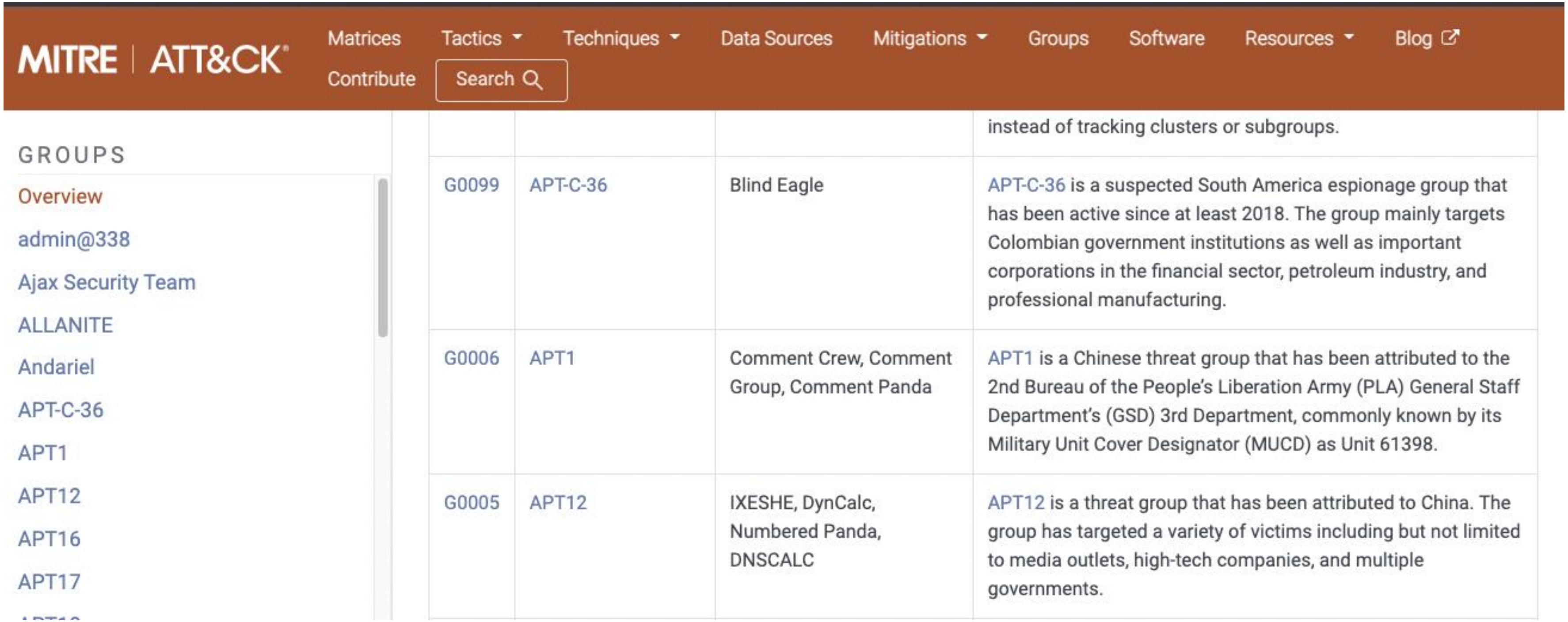
cje🌻 ✓
@caseyjohnellis

threat actor = someone who wants to punch you in the face
threat = the punch being thrown
vulnerability = your inability to defend against the punch
risk = the likelihood of getting punched in the face

6:47 PM · Apr 19, 2021 · Twitter Web App

518 Retweets 79 Quote Tweets 1,701 Likes

ATT&CK Groups



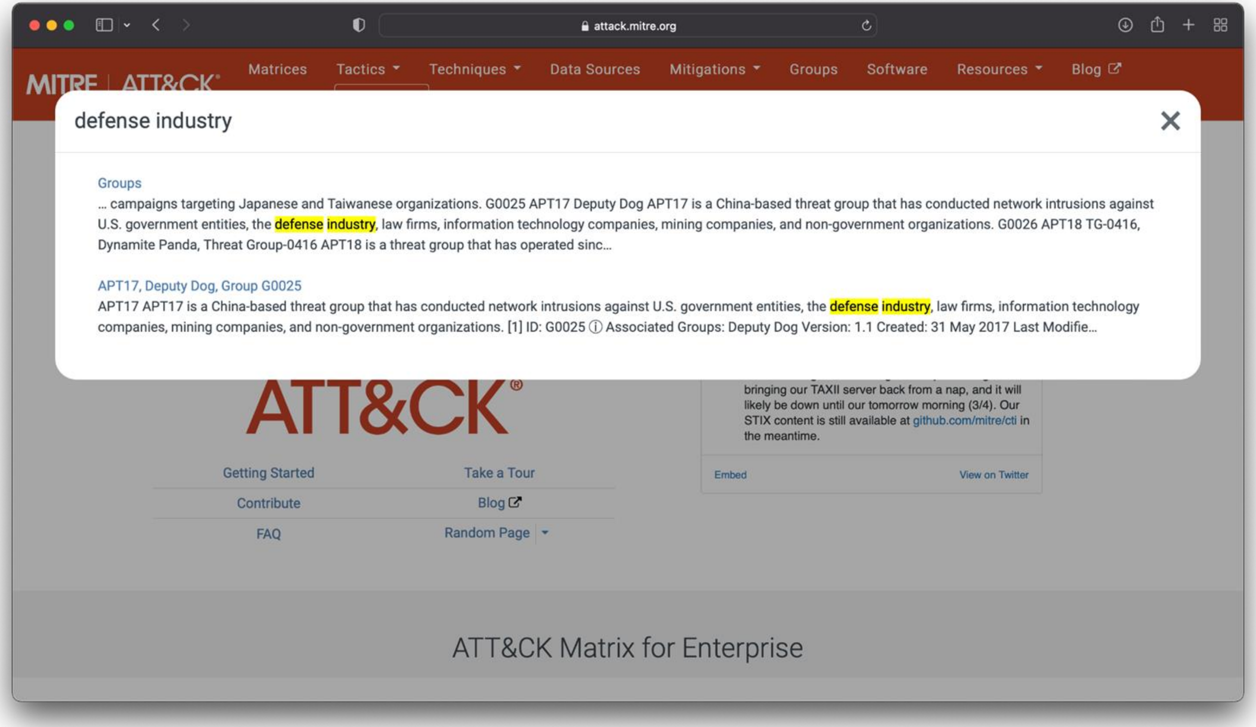
GROUPS

- Overview
- admin@338
- Ajax Security Team
- ALLANITE
- Andariel
- APT-C-36
- APT1
- APT12
- APT16
- APT17

			instead of tracking clusters or subgroups.
G0099	APT-C-36	Blind Eagle	APT-C-36 is a suspected South America espionage group that has been active since at least 2018. The group mainly targets Colombian government institutions as well as important corporations in the financial sector, petroleum industry, and professional manufacturing.
G0006	APT1	Comment Crew, Comment Group, Comment Panda	APT1 is a Chinese threat group that has been attributed to the 2nd Bureau of the People's Liberation Army (PLA) General Staff Department's (GSD) 3rd Department, commonly known by its Military Unit Cover Designator (MUCD) as Unit 61398.
G0005	APT12	IXESHE, DynCalc, Numbered Panda, DNSCALC	APT12 is a threat group that has been attributed to China. The group has targeted a variety of victims including but not limited to media outlets, high-tech companies, and multiple governments.

https://attack.mitre.org/groups/

Threat Modeling 101



defense industry

Groups

… campaigns targeting Japanese and Taiwanese organizations. G0025 APT17 Deputy Dog APT17 is a China-based threat group that has conducted network intrusions against U.S. government entities, the defense industry, law firms, information technology companies, mining companies, and non-government organizations. G0026 APT18 TG-0416, Dynamite Panda, Threat Group-0416 APT18 is a threat group that has operated sinc…

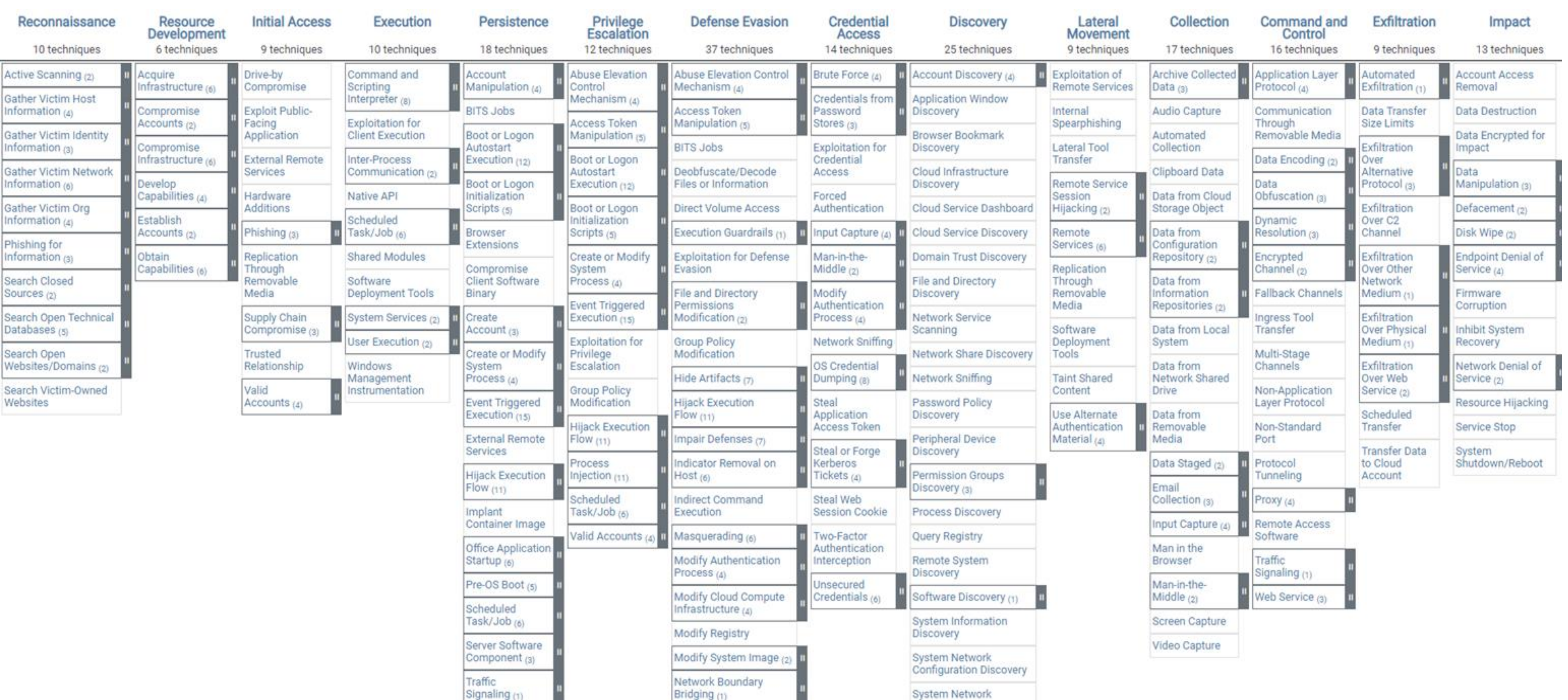
APT17, Deputy Dog, Group G0025

APT17 APT17 is a China-based threat group that has conducted network intrusions against U.S. government entities, the defense industry, law firms, information technology companies, mining companies, and non-government organizations. [1] ID: G0025 ⓘ Associated Groups: Deputy Dog Version: 1.1 Created: 31 May 2017 Last Modifie…

bringing our TAXII server back from a nap, and it will likely be down until our tomorrow morning (3/4). Our STIX content is still available at github.com/mitre/cti in the meantime.

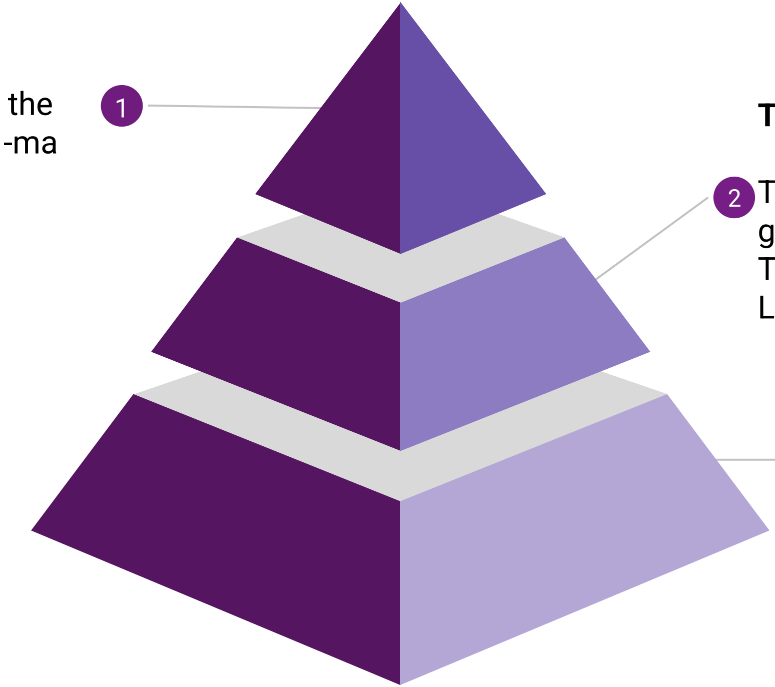
ATT&CK Matrix for Enterprise

MITRE ATT&CK®



Reconnaissance 10 techniques	Resource Development 6 techniques	Initial Access 9 techniques	Execution 10 techniques	Persistence 18 techniques	Privilege Escalation 12 techniques	Defense Evasion 37 techniques	Credential Access 14 techniques	Discovery 25 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 16 techniques	Exfiltration 9 techniques	Impact 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			
						Modify Registry		Software Discovery (1)					
						Modify System Image (2)		System Information Discovery					
						Network Boundary Bridging (1)		System Network Configuration Discovery					
								System Network					

Tactics, Techniques, and Procedures (TTPs)



1

Procedures

How the technique was carried out. For example, the attacker used procdump -ma lsass.exe lsass_dump

2

Techniques

Techniques represent the tactical goal of the procedure. For example, T1003.001 - OS Credential Dumping: LSASS Memory.

3

Tactics

Tactics represent the strategic goal of the adversary. For example, TA006 - Credential Access

https://www.scythe.io/library/summiting-the-pyramid-of-pain-the-ttp-pyramid

Simulation

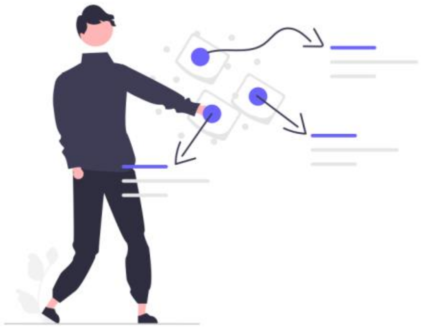
```
cmd /c SCHTASKS /CREATE /SC DAILY /TN \"MyTasks\\Task1\" /TR \"C:\\different.exe\" /ST 11:00 /F
```

Simulation:

- Exact commands
- Good for controls validation

Challenges:

- Signature based security testing



Emulation

```
cmd /c SCHTASKS /CREATE /SC DAILY /TN \"MyTasks\\Task1\" /TR \"C:\\update.exe\" /ST 11:00 /F
```

Scheduled Task T1053.005

Emulation:

- Look at behaviors (ATT&CK)
- Better for emulating adaptive behavior and adversaries
- Good for controls validation

Challenges:

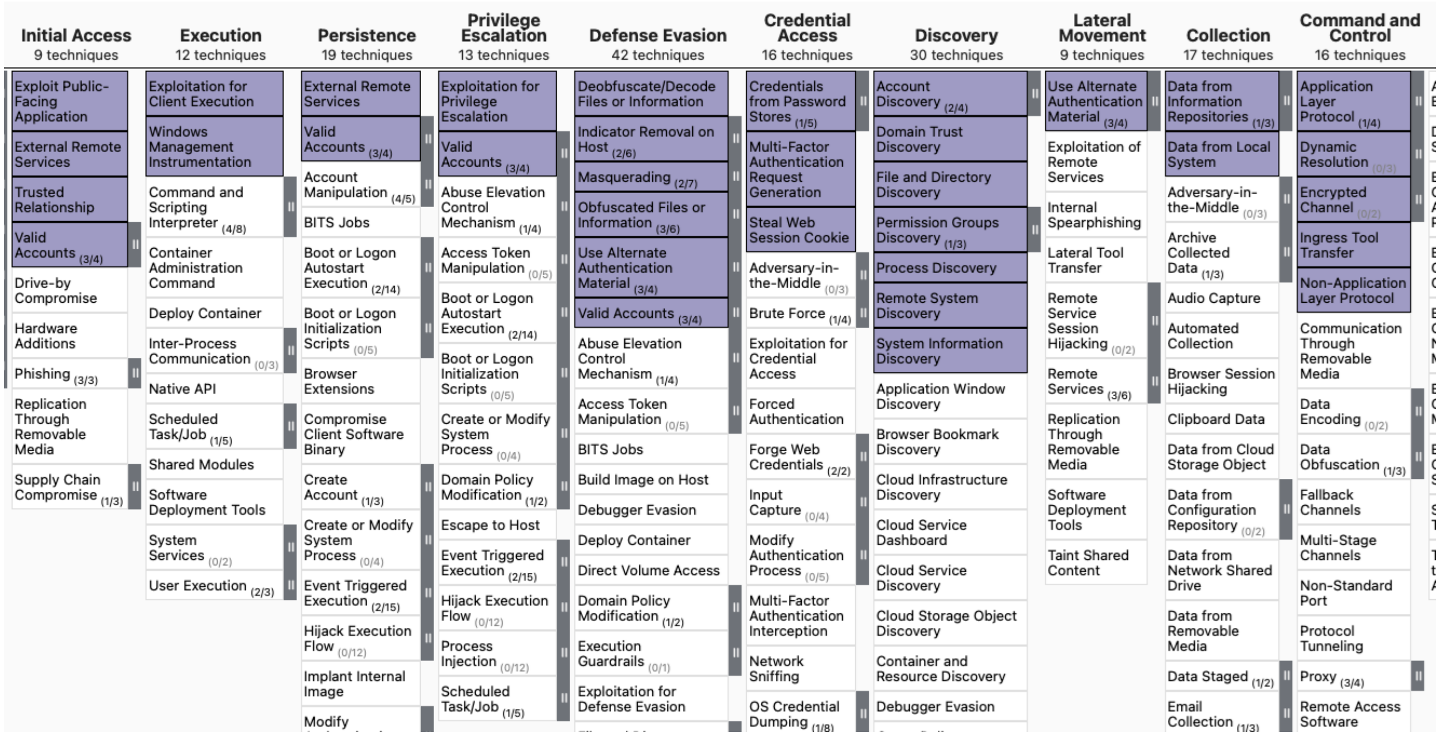
- More time and effort

Plan: Tactics & Techniques

Tactic	Description
Description	Orangeworm is a group that has targeted organizations in the healthcare sector in the United States, Europe, and Asia since at least 2015 for corporate espionage.
C2	T1071 - Application Layer Protocol; T1071.001 - Web Protocols; T1008 - Fallback Channel
Execution	T1218 - Signed Binary Proxy Execution; T1218.011 - Rundll32; T1059 - Command and Scripting Interpreter; T1059.003 - Windows Command Shell; T1569 - System Services; T1569.002 - Service Execution
Defense Evasion	T1036 - Masquerading; T1036.004 - Masquerade Task or Service; T1027 - Obfuscated Files or Information; T1027.001 - Binary Padding; T1070 - Indicator Removal on Host; T1070.004 - File Deletion; T1070.005 - Network Share Connection Removal; T1140 - Deobfuscate/Decode Files or Information
Discovery	T1087 - Account Discovery; T1087.001 - Local Account; T1087.002 - Domain Account; T1201 - Password Policy Discovery; T1069 - Permission Groups Discovery; T1069.002 - Domain Groups; T1069.001 - Local Groups; T1057 - Process Discovery; T1018 - Remote System Discovery; T1082 - System Information Discovery; T1016 - System Network Configuration Discovery T1049 - System Network Connections Discovery; T1033 - System Owner/User Discovery; T1007 - System Service Discovery T1083 - File and Directory Discovery;T1124 - System Time Discovery; T1135 - Network Share Discovery
Persistence	T1136.001 - Local Account; T1136.002 - Domain Account; T1543.003 - Windows Service
Lateral Movement	T1021 - Remote Services; T1021.002 - SMB/Windows Admin Shares; T1105 - Ingress Tool Transfer; T1570 - Lateral Tool Transfer

https://www.scythe.io/library/threatthursday-orangeworm

Present Tactics & Techniques – ATT&CK Navigator



Initial Access
9 techniques

- Exploit Public-Facing Application
- External Remote Services
- Trusted Relationship
- Valid Accounts (3/4)
- Drive-by Compromise
- Hardware Additions
- Phishing (3/3)
- Replication Through Removable Media
- Supply Chain Compromise (1/3)

Execution
12 techniques

- Exploitation for Client Execution
- Windows Management Instrumentation
- Command and Scripting Interpreter (4/8)
- Container Administration Command
- Deploy Container
- Inter-Process Communication (0/3)
- Native API
- Scheduled Task/Job (1/5)
- Shared Modules
- Software Deployment Tools
- System Services (0/2)
- User Execution (2/3)

Persistence
19 techniques

- External Remote Services
- Valid Accounts (3/4)
- Account Manipulation (4/5)
- BITS Jobs
- Boot or Logon Autostart Execution (2/14)
- Boot or Logon Initialization Scripts (0/5)
- Browser Extensions
- Compromise Client Software Binary
- Create Account (1/3)
- Create or Modify System Process (0/4)
- Event Triggered Execution (2/15)
- Hijack Execution Flow (0/12)
- Implant Internal Image
- Modify

Privilege Escalation
13 techniques

- Exploitation for Privilege Escalation
- Valid Accounts (3/4)
- Abuse Elevation Control Mechanism (1/4)
- Access Token Manipulation (0/5)
- Boot or Logon Autostart Execution (2/14)
- Boot or Logon Initialization Scripts (0/5)
- Create or Modify System Process (0/4)
- Domain Policy Modification (1/2)
- Escape to Host
- Event Triggered Execution (2/15)
- Hijack Execution Flow (0/12)
- Process Injection (0/12)
- Scheduled Task/Job (1/5)

Defense Evasion
42 techniques

- Deobfuscate/Decode Files or Information
- Indicator Removal on Host (2/6)
- Masquerading (2/7)
- Obfuscated Files or Information (3/6)
- Use Alternate Authentication Material (3/4)
- Valid Accounts (3/4)
- Abuse Elevation Control Mechanism (1/4)
- Access Token Manipulation (0/5)
- BITS Jobs
- Build Image on Host
- Debugger Evasion
- Deploy Container
- Direct Volume Access
- Domain Policy Modification (1/2)
- Execution Guardrails (0/1)
- Exploitation for Defense Evasion

Credential Access
16 techniques

- Credentials from Password Stores (1/5)
- Multi-Factor Authentication Request Generation
- Steal Web Session Cookie
- Adversary-in-the-Middle (0/3)
- Brute Force (1/4)
- Exploitation for Credential Access
- Forced Authentication
- Forge Web Credentials (2/2)
- Input Capture (0/4)
- Modify Authentication Process (0/5)
- Multi-Factor Authentication Interception
- Network Sniffing
- OS Credential Dumping (1/8)

Discovery
30 techniques

- Account Discovery (2/4)
- Domain Trust Discovery
- File and Directory Discovery
- Permission Groups Discovery (1/3)
- Process Discovery
- Remote System Discovery
- System Information Discovery
- Application Window Discovery
- Browser Bookmark Discovery
- Cloud Infrastructure Discovery
- Cloud Service Dashboard
- Cloud Service Discovery
- Cloud Storage Object Discovery
- Container and Resource Discovery
- Debugger Evasion

Lateral Movement
9 techniques

- Use Alternate Authentication Material (3/4)
- Exploitation of Remote Services
- Internal Spearphishing
- Lateral Tool Transfer
- Remote Service Session Hijacking (0/2)
- Remote Services (3/6)
- Replication Through Removable Media
- Software Deployment Tools
- Taint Shared Content

Collection
17 techniques

- Data from Information Repositories (1/3)
- Data from Local System
- Adversary-in-the-Middle (0/3)
- Archive Collected Data (1/3)
- Audio Capture
- Automated Collection
- Browser Session Hijacking
- Clipboard Data
- Data from Cloud Storage Object
- Data from Configuration Repository (0/2)
- Data from Network Shared Drive
- Data from Removable Media
- Data Staged (1/2)
- Email Collection (1/3)

Command and Control
16 techniques

- Application Layer Protocol (1/4)
- Dynamic Resolution (0/3)
- Encrypted Channel (0/2)
- Ingress Tool Transfer
- Non-Application Layer Protocol
- Communication Through Removable Media
- Data Encoding (0/2)
- Data Obfuscation (1/3)
- Fallback Channels
- Multi-Stage Channels
- Non-Standard Port
- Protocol Tunneling
- Proxy (3/4)
- Remote Access Software

https://mitre-attack.github.io/attack-navigator/

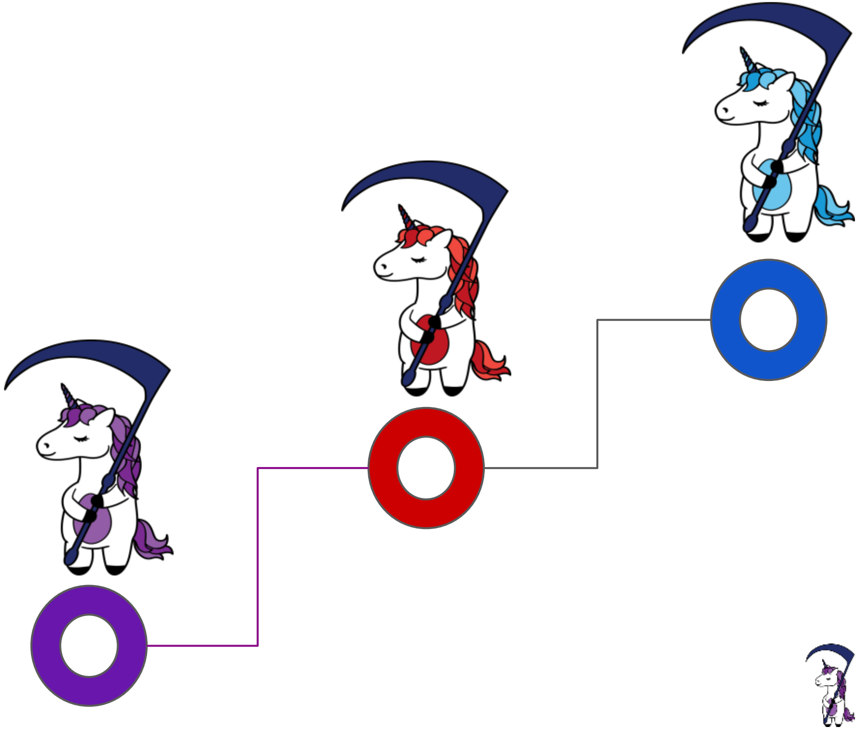
Challenges in Building Emulation Plans

- Beware of unsafe or potentially attack surface introducing tests (web shells)
- There may not be CTI for all parts of the emulation plan
  - This is where you may have to get creative!
- CTI data is historic
  - It may not represent current threat actor capabilities!
- Old TTPs may not work in a modern environment
- CTI reports are still mostly ingested manually

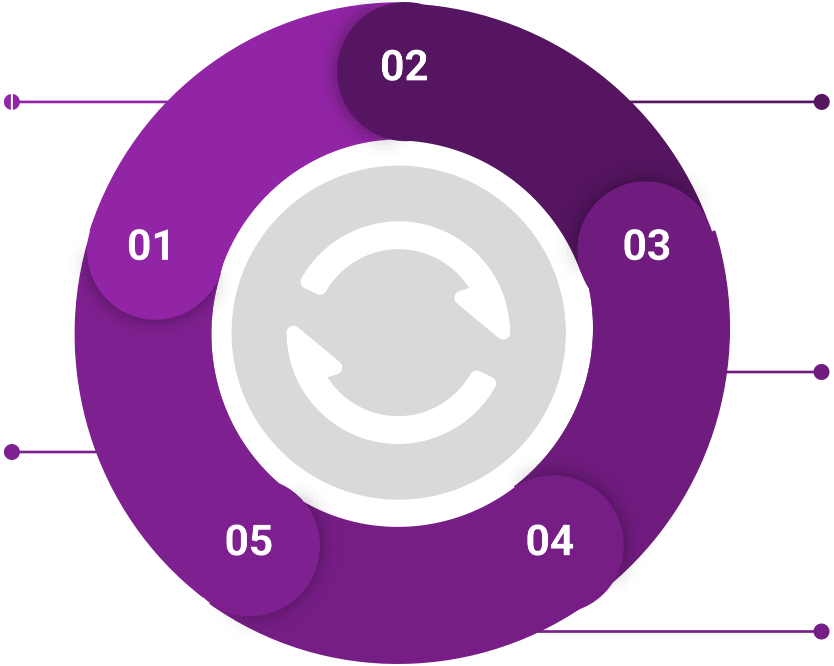
Testing

Your choice of testing tools matters:

- Realism
- Flexibility
- Replayability
- Collaboration/Communication
- Reliability
- Trustworthiness
- Library



Operationalized Purple Team



New CTI or TTPs

- CTI, Red, or Blue discover/share/notify
- Assign CTI, Red, and Blue Team member

Analyze & Organize TTPs

- Map to MITRE ATT&CK
- Correlate with previous tests

Tabletop Discussion

- Expected Detection and Response

Emulate Attack

- Threat Understanding
- Deployment, Integration, Creation

Detection Engineering

- Detection Understanding
- Deployment, Integration, Creation
- Repeat attack for training and validation

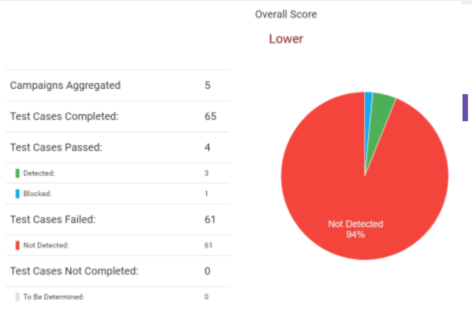
Measuring Outcomes: Metrics

Visibility - What Can I See?

- Host
- Network
- Central Logging (SIEM)

Time - How Long Until I See It?

- Time to log
- Time to detect
- Time to alert

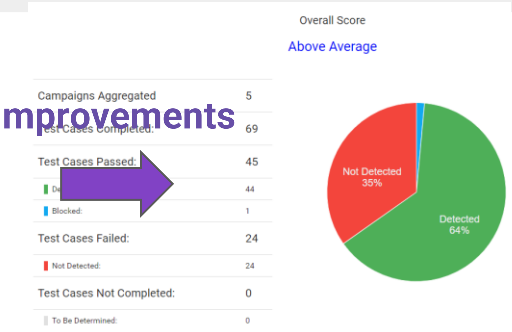


Overall Score

Lower

Campaigns Aggregated	5
Test Cases Completed:	65
Test Cases Passed:	4
🟩 Detected:	3
🟦 Blocked:	1
Test Cases Failed:	61
🟥 Not Detected:	61
Test Cases Not Completed:	0
▯ To Be Determined:	0

Improvements

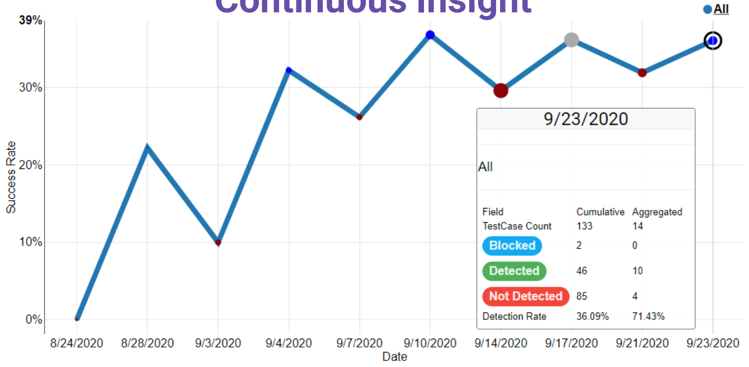


Overall Score

Above Average

Campaigns Aggregated	5
est Cases Completed:	69
Test Cases Passed:	45
🟩 De	44
🟦 Blocked:	1
Test Cases Failed:	24
🟥 Not Detected:	24
Test Cases Not Completed:	0
▯ To Be Determined:	0

Continuous Insight



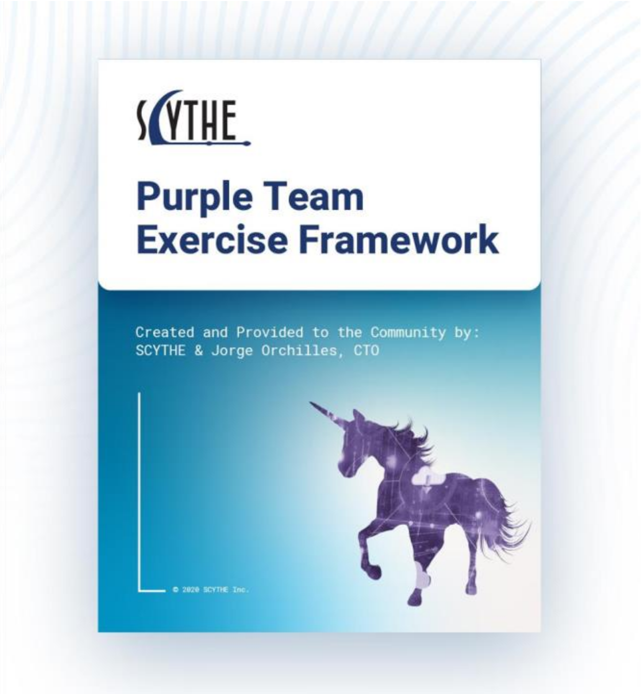
9/23/2020

All

Field	Cumulative	Aggregated
TestCase Count	133	14
Blocked	2	0
Detected	46	10
Not Detected	85	4
Detection Rate	36.09%	71.43%

Leadership teams like metrics

THE DEFINITIVE GUIDE TO PURPLE TEAMING (maintained)

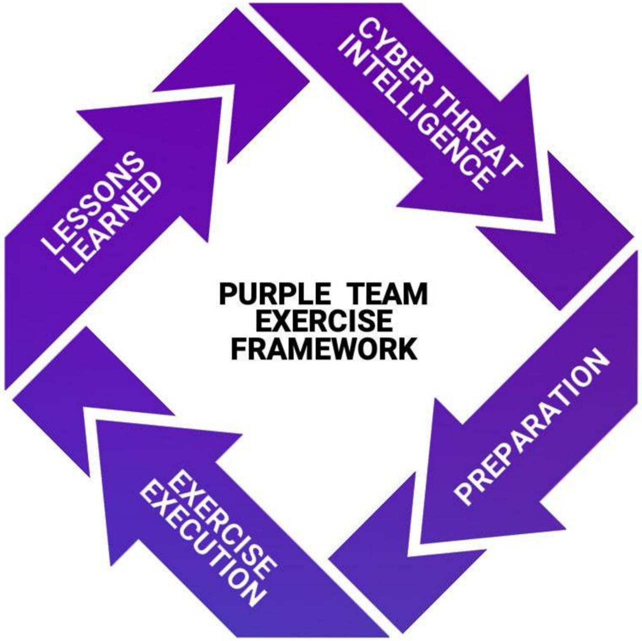


SCYTHE

Purple Team Exercise Framework

Created and Provided to the Community by:
SCYTHE & Jorge Orchilles, CTO

© 2020 SCYTHE Inc.



PURPLE TEAM EXERCISE FRAMEWORK

CYBER THREAT INTELLIGENCE

PREPARATION

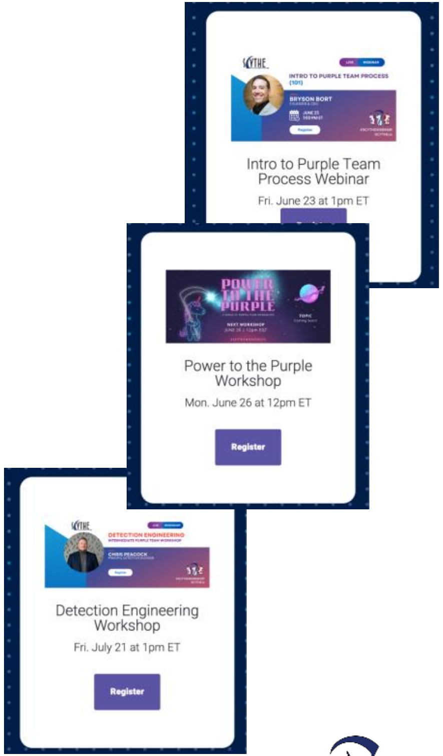
EXERCISE EXECUTION

LESSONS LEARNED

https://github.com/scythe-io/purple-team-exercise-framework

Tips

- Start simple: Purple Teaming is its own process maturity
- It's OK to deviate from plan to accomplish objective
- MITRE ATT&CK is NOT a Bingo Card
  - It takes time to go from Wild to Matrix
- Security tools/processes make some TTPs difficult
- Document the good and the bad
  - Highlight wins: Red AND Blue



Intro to Purple Team Process Webinar

Fri. June 23 at 1pm ET

Power to the Purple Workshop

Mon. June 26 at 12pm ET

Register

Detection Engineering Workshop

Fri. July 21 at 1pm ET

Register

- SCYTHE offers free training and workshops every month!

https://scythe.io/workshops

Resources

Purple Team Exercise Cheat Sheet

Key Questions	Best Case	Minimum	Notes
Who's involved?	Red Team, Blue Team, CTI Team, Leadership Team	Someone that can execute a test and document a result	Get buy-in or sign off from the highest level possible
What systems are tested?	Production Systems, multiple systems to validate results (servers & endpoints)	Test System	Data generation, data collection, and environment for testing
Logistics?	Remote: Screen share In Person: Shared space	Note keeping tool to record actions	Document/record as much as possible
Security tools?	Everything in SOC & DFIR, tuned for production	A tool that's results can be applied to production	If a tool/control blocks progress, document and shift to audit mode to move through depth

Resource: Simplified Process

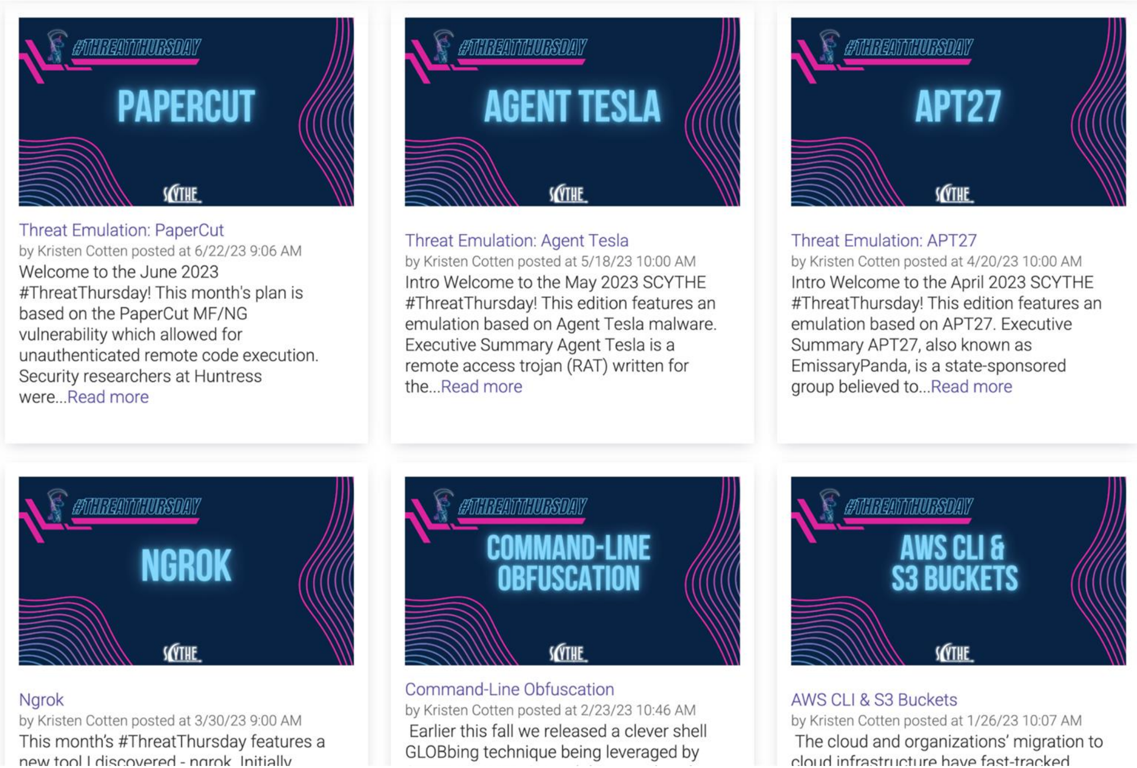
Katie Nickels Shmoocon 2020 A Simple Process to Start

1. Know your organization
2. Know your threats
3. Prioritize and match them up
4. Make it actionable

Resources

- MITRE ATT&CK Training by Katie Nickels and Adam Pennington
  - https://attack.mitre.org/resources/training/cti/
- MITRE ATT&CK Defender Series by MITRE hosted on Cybrary
  - https://www.cybrary.it/course/mitre-attack-defender-mad-attack-fundamentals/
- SCYTHE Blog on Simplifying ATT&CK
  - https://www.scythe.io/library/simplifying-the-mitre-att-ck-framework
- SCYTHE blog on ATT&CK Navigator
  - https://www.scythe.io/library/scythe-att-ck-navigator
- TRAM
  - https://github.com/center-for-threat-informed-defense/tram
- Chrome Extension
  - https://chrome.google.com/webstore/detail/attck-powered-suit

Resources: Adversary Emulation Plans



Threat Emulation: PaperCut

by Kristen Cotten posted at 6/22/23 9:06 AM

Welcome to the June 2023 #ThreatThursday! This month's plan is based on the PaperCut MF/NG vulnerability which allowed for unauthenticated remote code execution. Security researchers at Huntress were...Read more

Threat Emulation: Agent Tesla

by Kristen Cotten posted at 5/18/23 10:00 AM

Intro Welcome to the May 2023 SCYTHE #ThreatThursday! This edition features an emulation based on Agent Tesla malware. Executive Summary Agent Tesla is a remote access trojan (RAT) written for the...Read more

Threat Emulation: APT27

by Kristen Cotten posted at 4/20/23 10:00 AM

Intro Welcome to the April 2023 SCYTHE #ThreatThursday! This edition features an emulation based on APT27. Executive Summary APT27, also known as EmissaryPanda, is a state-sponsored group believed to...Read more

Ngrok

by Kristen Cotten posted at 3/30/23 9:00 AM

This month's #ThreatThursday features a new tool I discovered - ngrok. Initially

Command-Line Obfuscation

by Kristen Cotten posted at 2/23/23 10:46 AM

Earlier this fall we released a clever shell GLOBbing technique being leveraged by

AWS CLI & S3 Buckets

by Kristen Cotten posted at 1/26/23 10:07 AM

The cloud and organizations' migration to cloud infrastructure have fast-tracked

Monthly Emulation Plan Release

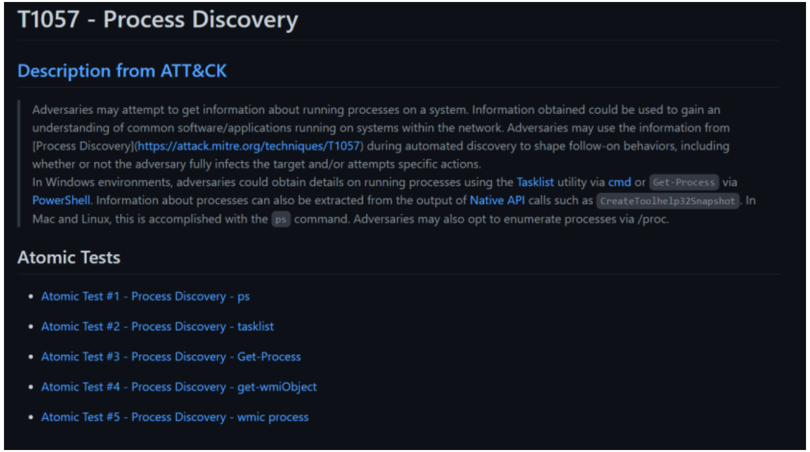
- ○ Procedure Level
- ○ CTI Source Cited
- ○ Detections Included

https://www.scythe.io/threatthursday

Atomic Red Team: Walkthrough

Visit the GitHub: https://github.com/redcanaryco/atomic-red-team

Getting Started Guide: https://github.com/redcanaryco/atomic-red-team/wiki/Getting-started



T1057 - Process Discovery

Description from ATT&CK

> Adversaries may attempt to get information about running processes on a system. Information obtained could be used to gain an understanding of common software/applications running on systems within the network. Adversaries may use the information from [Process Discovery](https://attack.mitre.org/techniques/T1057) during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions.
> In Windows environments, adversaries could obtain details on running processes using the Tasklist utility via cmd or `Get-Process` via PowerShell. Information about processes can also be extracted from the output of Native API calls such as `CreateToolhelp32Snapshot`. In Mac and Linux, this is accomplished with the `ps` command. Adversaries may also opt to enumerate processes via /proc.

Atomic Tests

- Atomic Test #1 - Process Discovery - ps
- Atomic Test #2 - Process Discovery - tasklist
- Atomic Test #3 - Process Discovery - Get-Process
- Atomic Test #4 - Process Discovery - get-wmiObject
- Atomic Test #5 - Process Discovery - wmic process

Atomic Red Team

Bringing atomic testing to the security space!

- https://atomicredteam.io/atomicredteam
- https://github.com/redcanaryco/atomic-red-team
- https://github.com/redcanaryco/AtomicTestHarnesses

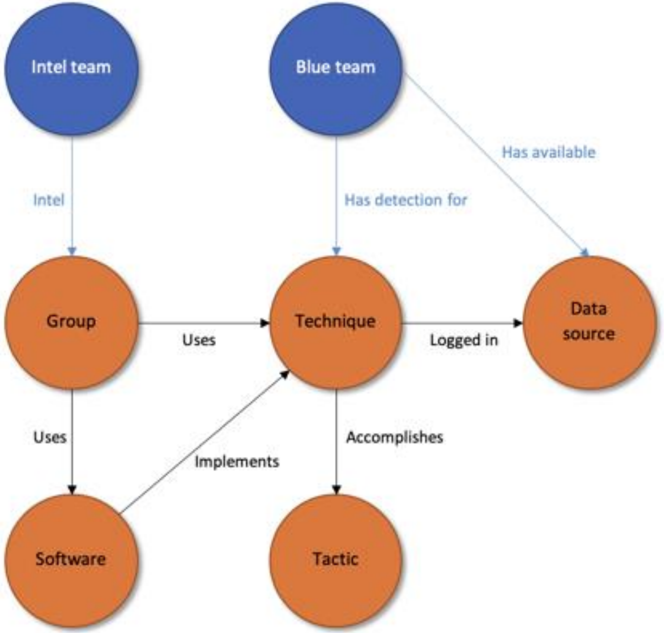
Inspired Additional tooling and tests!

- https://github.com/swimlane/atomic-operator
- https://github.com/DataDog/stratus-red-team

DETT&CT

Blue Team

- Data Sources
- Visibility
- Detection

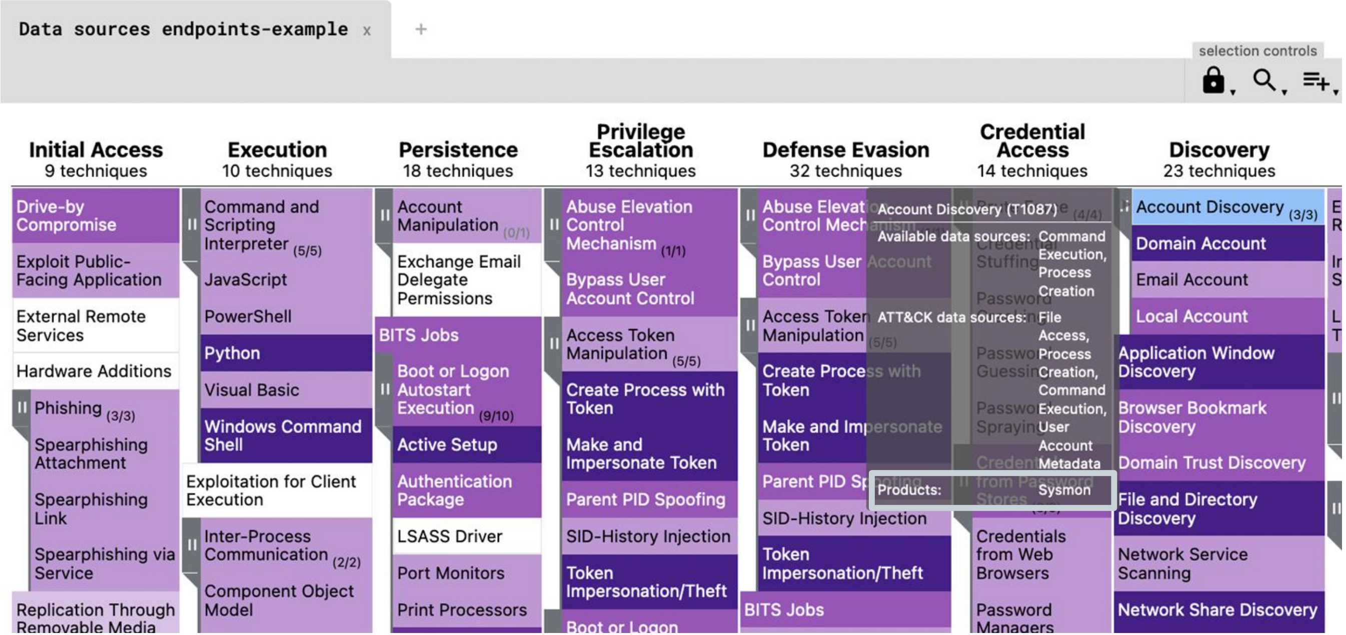


https://www.mbsecure.nl/blog/2019/5/dettact-mapping-your-blue-team-to-mitre-attack

https://github.com/rabobank-cdc/DeTTECT

Collection: DeTT&CT

Leverage DeTT&CT to visualize coverage and map your log sources



Data sources endpoints-example x +

selection controls

Initial Access 9 techniques
- Drive-by Compromise
- Exploit Public-Facing Application
- External Remote Services
- Hardware Additions
- Phishing (3/3)
- Spearphishing Attachment
- Spearphishing Link
- Spearphishing via Service
- Replication Through Removable Media

Execution 10 techniques
- Command and Scripting Interpreter (5/5)
- JavaScript
- PowerShell
- Python
- Visual Basic
- Windows Command Shell
- Exploitation for Client Execution
- Inter-Process Communication (2/2)
- Component Object Model

Persistence 18 techniques
- Account Manipulation (0/1)
- Exchange Email Delegate Permissions
- BITS Jobs
- Boot or Logon Autostart Execution (9/10)
- Active Setup
- Authentication Package
- LSASS Driver
- Port Monitors
- Print Processors

Privilege Escalation 13 techniques
- Abuse Elevation Control Mechanism (1/1)
- Bypass User Account Control
- Access Token Manipulation (5/5)
- Create Process with Token
- Make and Impersonate Token
- Parent PID Spoofing
- SID-History Injection
- Token Impersonation/Theft
- Boot or Logon

Defense Evasion 32 techniques
- Abuse Elevation Control Mechanism
- Bypass User Account Control
- Access Token Manipulation (5/5)
- Create Process with Token
- Make and Impersonate Token
- Parent PID Spoofing
- SID-History Injection
- Token Impersonation/Theft
- BITS Jobs

Credential Access 14 techniques
- Brute Force (4/4)
- Credential Stuffing
- Password
- Password Guessing
- Password Spraying
- Credentials from Password Stores
- Credentials from Web Browsers
- Password Managers

Discovery 23 techniques
- Account Discovery (3/3)
- Domain Account
- Email Account
- Local Account
- Application Window Discovery
- Browser Bookmark Discovery
- Domain Trust Discovery
- File and Directory Discovery
- Network Service Scanning
- Network Share Discovery

Account Discovery (T1087)
Available data sources: Command Execution, Process Creation
ATT&CK data sources: File Access, Process Creation, Command Execution, User Account Metadata
Products: Sysmon

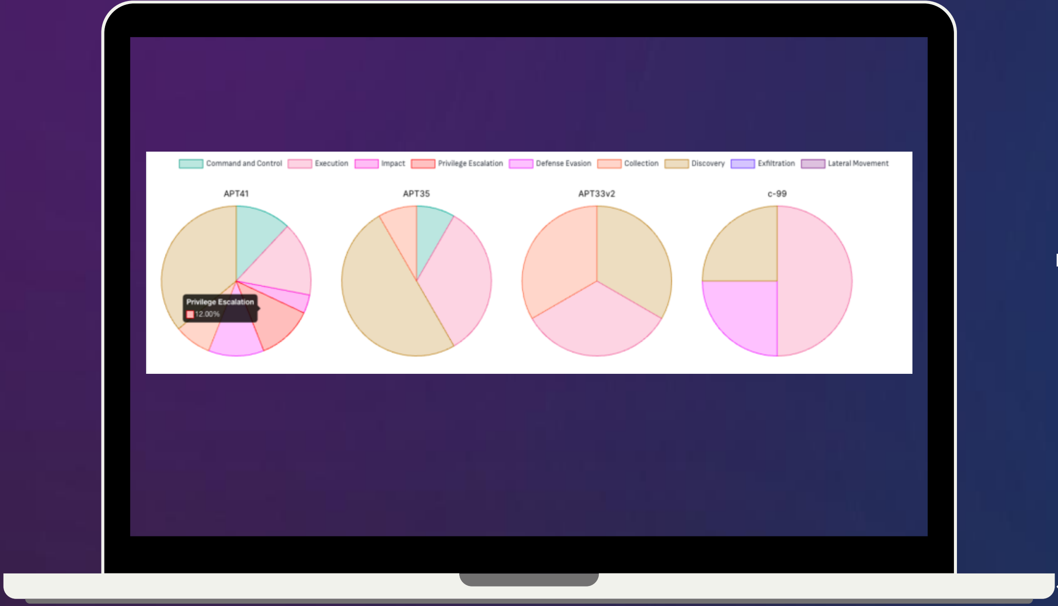
https://rabobank-cdc.github.io/dettect-editor/

SCYTHE

RESPOND

DETECT

ATTACK



Purple Teaming in OT 101

@scythe_io

A Play in 3 Acts

Act 1

We had several attacks over the preceding year:

- Physical breach of the electric fence
- Nigerian actors successfully tricked a major customer into a BEC
- Network penetration to print server*

*https://www.rsaconference.com/Library/presentation/USA/2018/no-ious-with-iot-2

Act 2

Conducts rigorous endeavor to physically and logically separate IT and OT networks across 11 major sites across North America. Each site averaged in excess of $100M of equipment that could easily result in loss of life.

Design, deploy and validate!

Act 3

Vendor drives on site and deep underground.

Act 3

Physically isolated OT network:

- Holds up miles of earth to prevent collapse
- Air quality

Act 3

Vendor plugs in his laptop without

- Security/control of the laptop,
- Software update or
- Other to-be-deployed configuration changes.

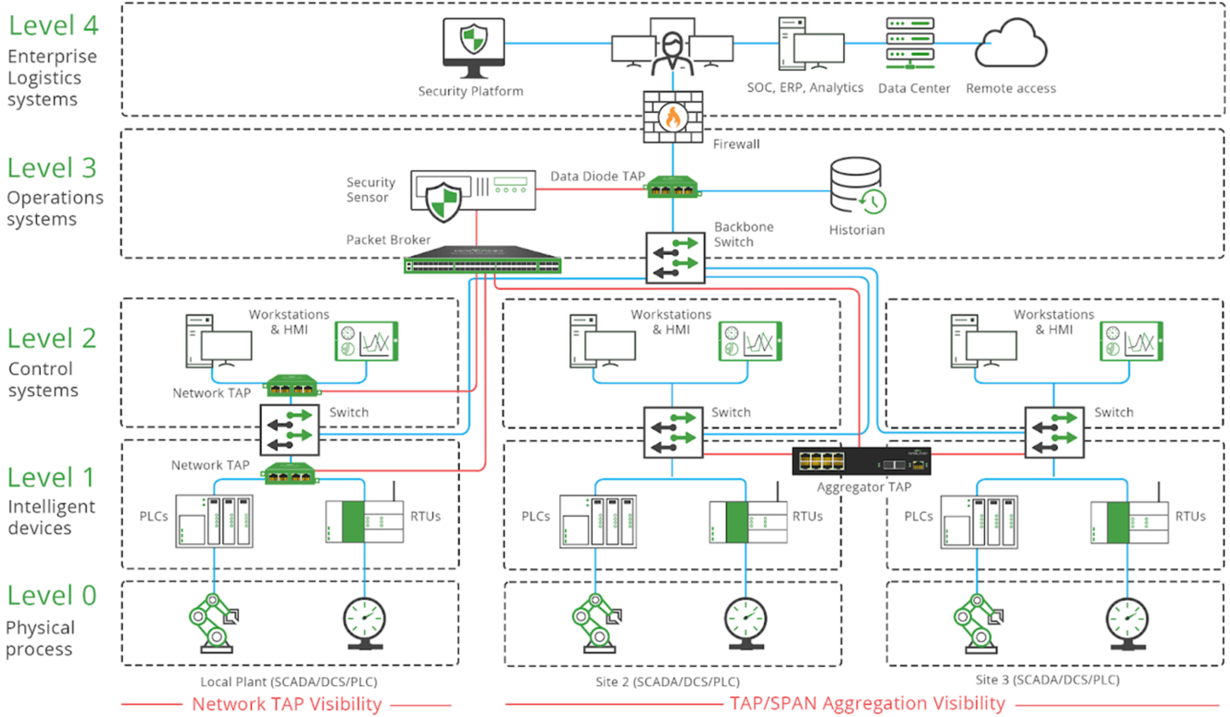
Fin

What is ICS?

Any computer that is at least 20 years old

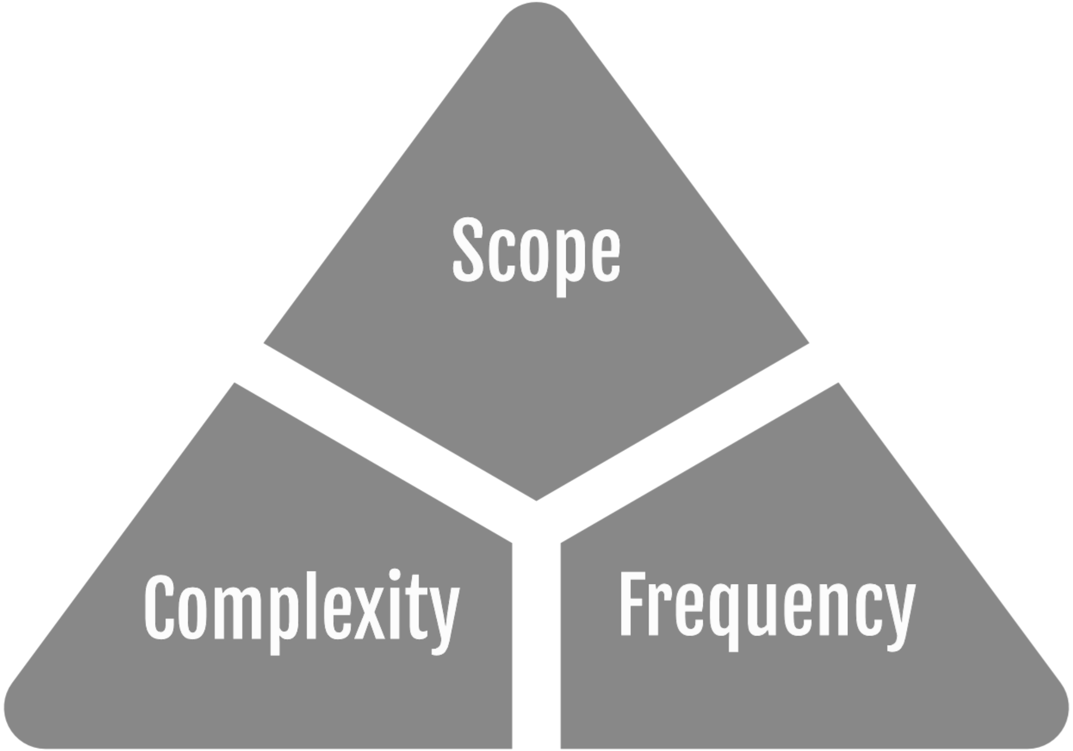
What is OT: Purdue Model

Enterprise IT systems and networks (Layer

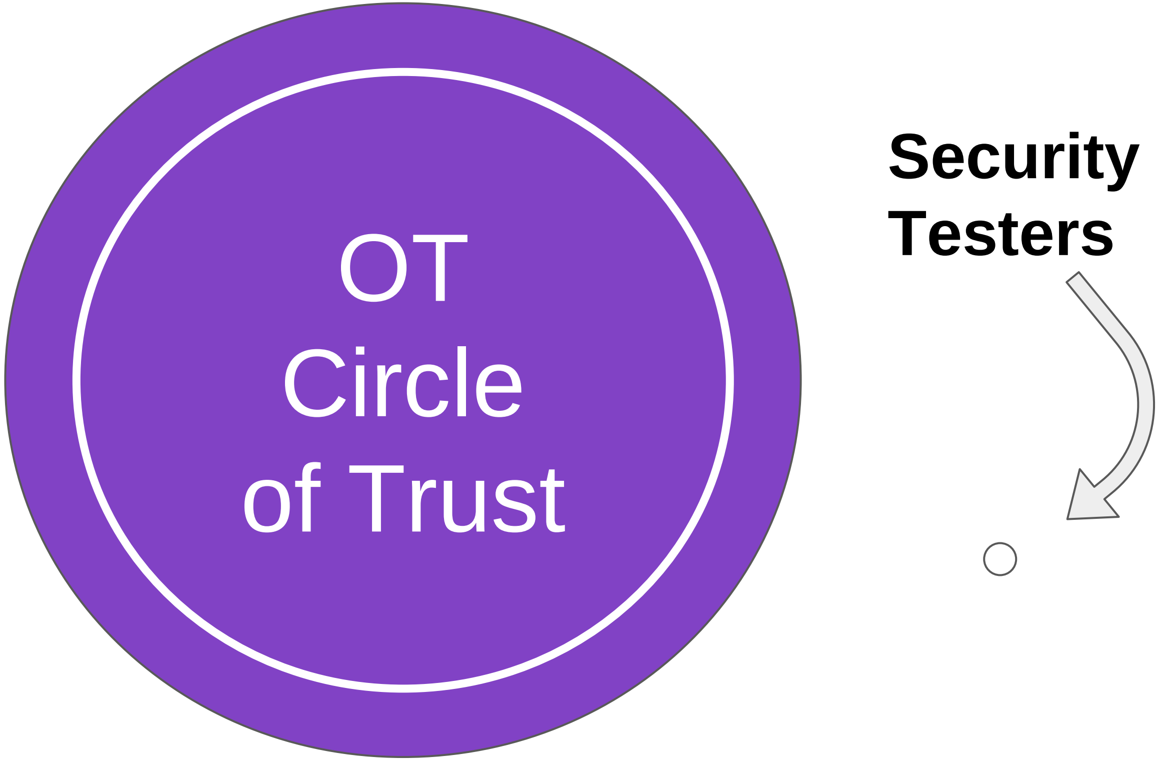


https://www.garlandtechnology.com/blog/ot-segmentation-best-practices-for-a-more-secure-industrial-network

Testing



Building Trust

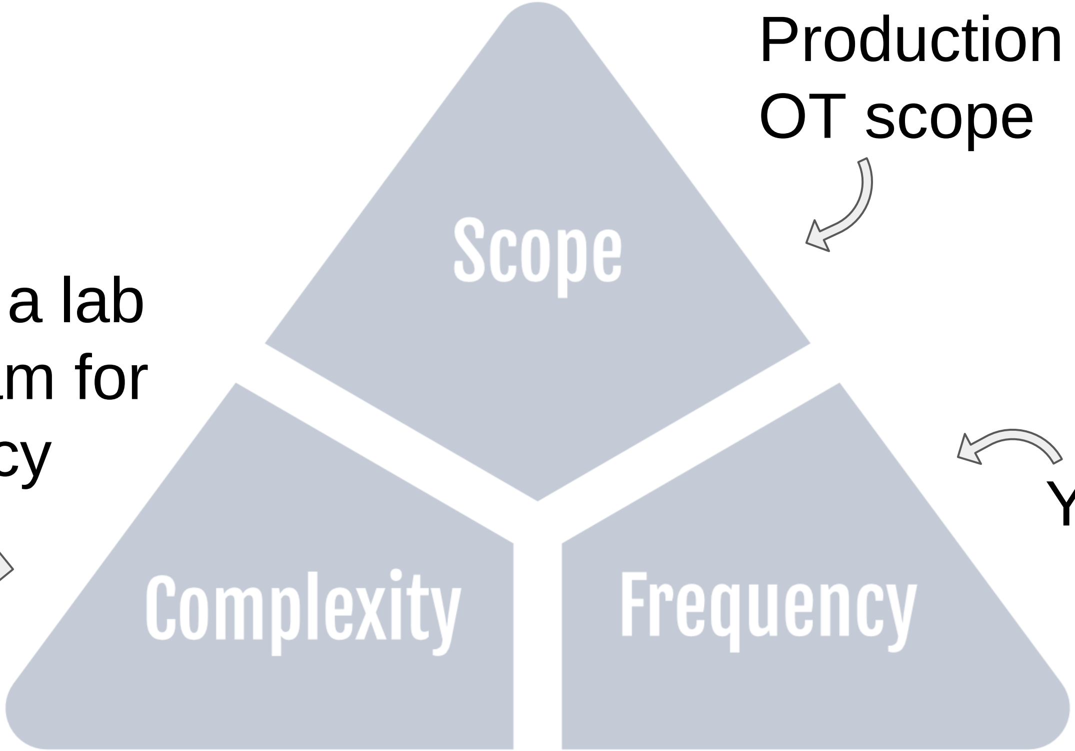


OT
Circle
of Trust

Security
Testers

Trust Through Testing

- Validate in a lab
- Purple Team for transparency



Production decides OT scope

You decide!*

Trust Through Testing

Complexity

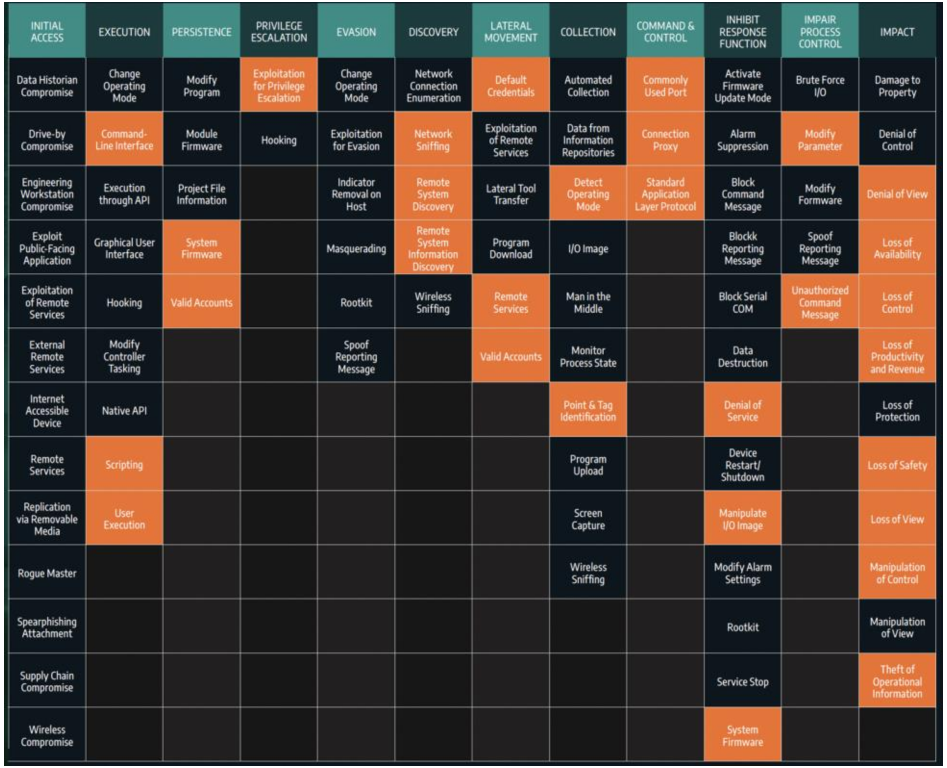
Frequency

Adversary Emulation in OT

- **Planning**
  - Access vs Impact
- **Execution**
  - Emulate emerging threat
- **Measure** protection, detection, and response between beachhead* and OT (access operations)

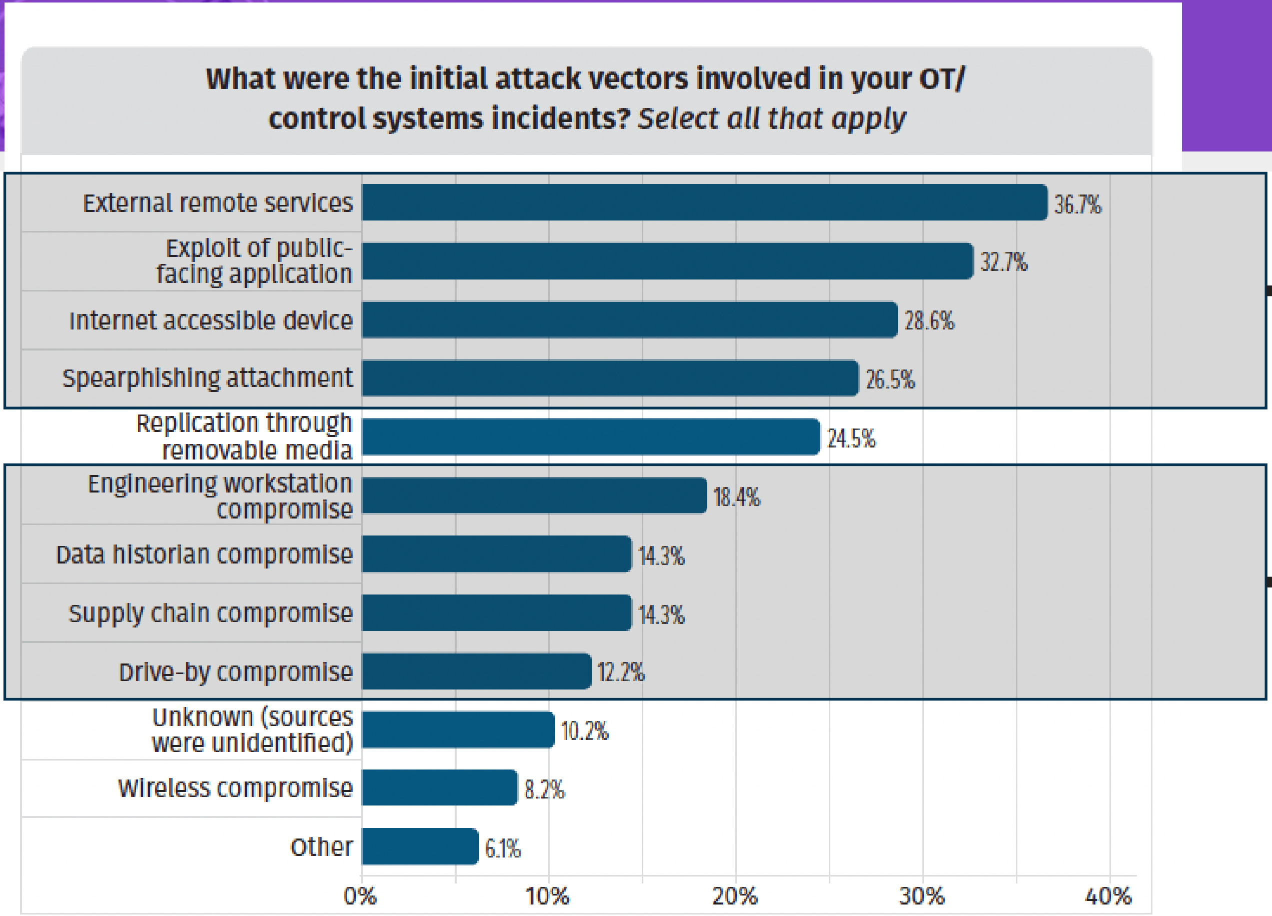
- **Opportunities**
  - Discovery
  - Lateral Movement

** - we'll get to this shortly!*



INITIAL ACCESS	EXECUTION	PERSISTENCE	PRIVILEGE ESCALATION	EVASION	DISCOVERY	LATERAL MOVEMENT	COLLECTION	COMMAND & CONTROL	INHIBIT RESPONSE FUNCTION	IMPAIR PROCESS CONTROL	IMPACT
Data Historian Compromise	Change Operating Mode	Modify Program	Exploitation for Privilege Escalation	Change Operating Mode	Network Connection Enumeration	Default Credentials	Automated Collection	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/O	Damage to Property
Drive-by Compromise	Command-Line Interface	Module Firmware	Hooking	Exploitation for Evasion	Network Sniffing	Exploitation of Remote Services	Data from Information Repositories	Connection Proxy	Alarm Suppression	Modify Parameter	Denial of Control
Engineering Workstation Compromise	Execution through API	Project File Information		Indicator Removal on Host	Remote System Discovery	Lateral Tool Transfer	Detect Operating Mode	Standard Application Layer Protocol	Block Command Message	Modify Formware	Denial of View
Exploit Public-Facing Application	Graphical User Interface	System Firmware		Masquerading	Remote System Information Discovery	Program Download	I/O Image		Blockk Reporting Message	Spoof Reporting Message	Loss of Availability
Exploitation of Remote Services	Hooking	Valid Accounts		Rootkit	Wireless Sniffing	Remote Services	Man in the Middle		Block Serial COM	Unauthorized Command Message	Loss of Control
External Remote Services	Modify Controller Tasking			Spoof Reporting Message		Valid Accounts	Monitor Process State		Data Destruction		Loss of Productivity and Revenue
Internet Accessible Device	Native API						Point & Tag Identification		Denial of Service		Loss of Protection
Remote Services	Scripting						Program Upload		Device Restart/ Shutdown		Loss of Safety
Replication via Removable Media	User Execution						Screen Capture		Manipulate I/O Image		Loss of View
Rogue Master							Wireless Sniffing		Modify Alarm Settings		Manipulation of Control
Spearphishing Attachment									Rootkit		Manipulation of View
Supply Chain Compromise									Service Stop		Theft of Operational Information
Wireless Compromise									System Firmware		

https://www.dragos.com/blog/industry-news/chernovite-pipedream-malware-targeting-industrial-control-systems/



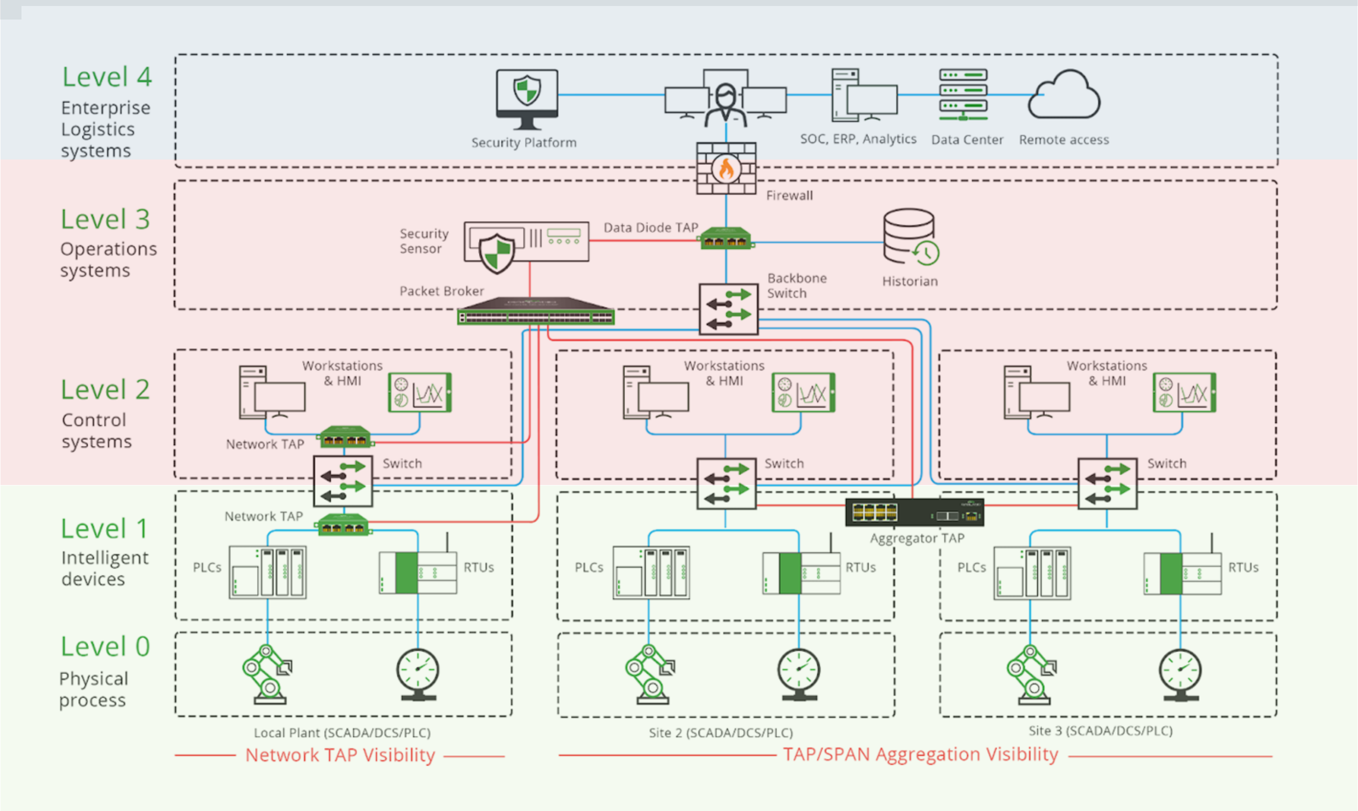
What were the initial attack vectors involved in your OT/ control systems incidents? *Select all that apply*

SANS Institute

Internet Accessible

Threat Modeling

Enterprise IT systems and networks (Level 4)



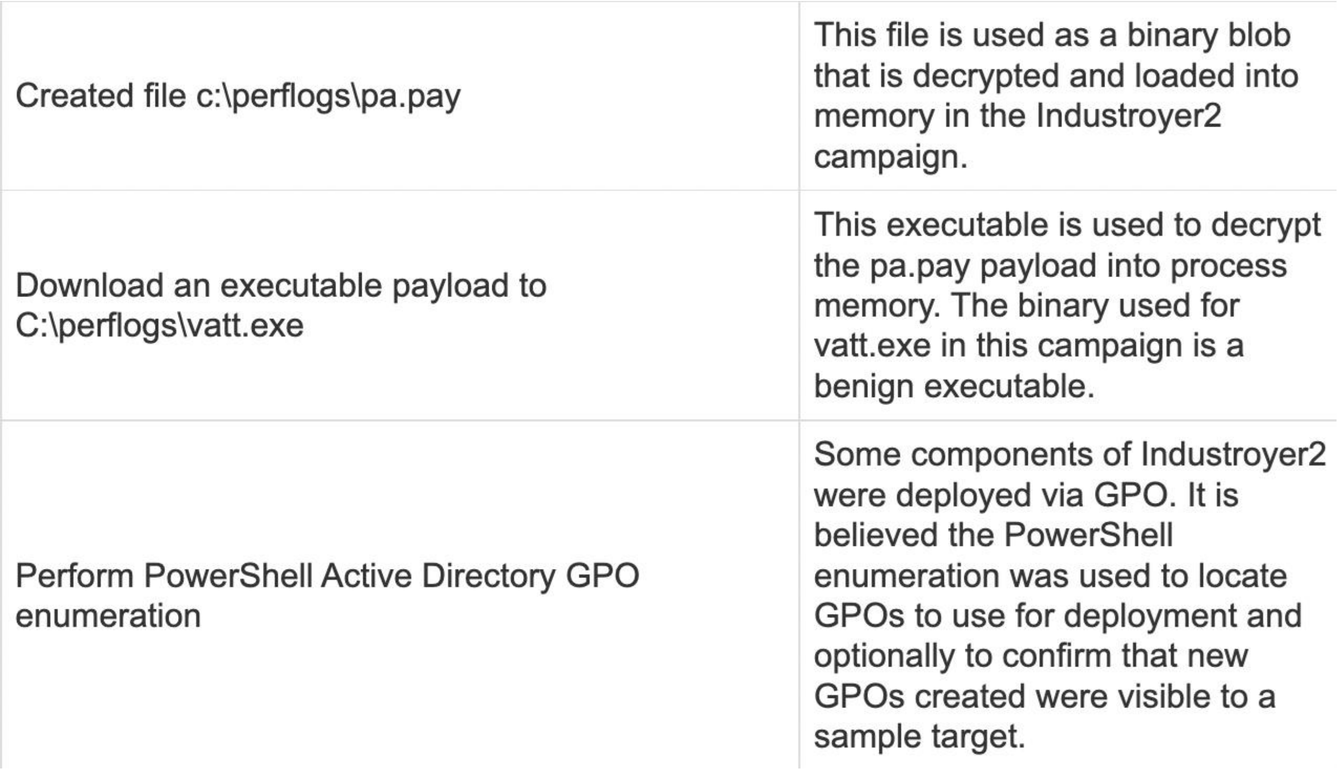
SCOPE: Testing

Stages of Testing		Lab	Production
1	Passive	✓	✓
2	Active	✓	✗

SCOPE: Testing

Stages of Testing		Lab	Production
1	Passive	✓	✓
2	**OT Vendor Tools with Industrial Protocols**	✓	✓
3	Active	✓	✗

Actions on Objective



Created file c:\perflogs\pa.pay	This file is used as a binary blob that is decrypted and loaded into memory in the Industroyer2 campaign.
Download an executable payload to C:\perflogs\vatt.exe	This executable is used to decrypt the pa.pay payload into process memory. The binary used for vatt.exe in this campaign is a benign executable.
Perform PowerShell Active Directory GPO enumeration	Some components of Industroyer2 were deployed via GPO. It is believed the PowerShell enumeration was used to locate GPOs to use for deployment and optionally to confirm that new GPOs created were visible to a sample target.

Testing Capability

Signaturable

Emulation

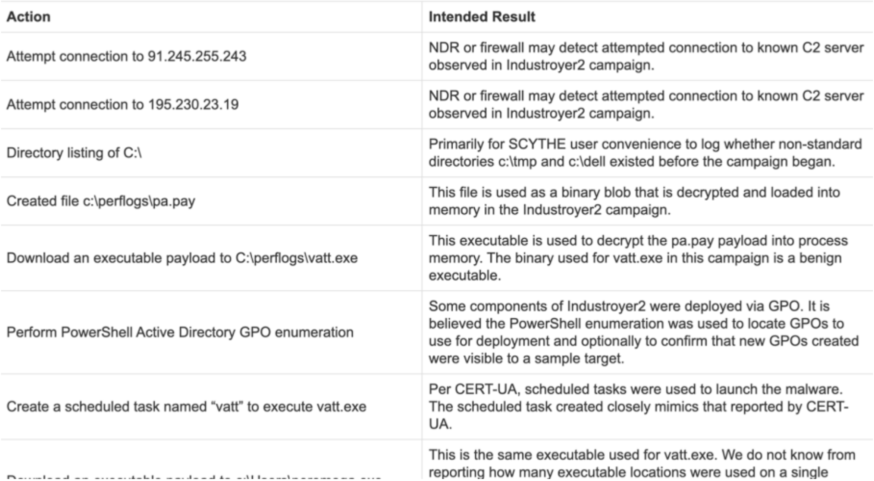
https://www.scythe.io/library/threat-emulation-industroyer2-operation

ICS Threats Library

Industroyer: 4 distinct modules targeting specific ICS communication protocols (IEC 60870-5-101, IEC 60870-5-104, IEC 61850, and OLE for Process Control Data Access (OPC DA))

Industroyer2: standalone executable targeting IEC-104 controllers.

IEC-104 is used for power system monitoring and control over TCP and is mainly implemented in Europe and the Middle East.



Action	Intended Result
Attempt connection to 91.245.255.243	NDR or firewall may detect attempted connection to known C2 server observed in Industroyer2 campaign.
Attempt connection to 195.230.23.19	NDR or firewall may detect attempted connection to known C2 server observed in Industroyer2 campaign.
Directory listing of C:\	Primarily for SCYTHE user convenience to log whether non-standard directories c:\tmp and c:\dell existed before the campaign began.
Created file c:\perflogs\pa.pay	This file is used as a binary blob that is decrypted and loaded into memory in the Industroyer2 campaign.
Download an executable payload to C:\perflogs\vatt.exe	This executable is used to decrypt the pa.pay payload into process memory. The binary used for vatt.exe in this campaign is a benign executable.
Perform PowerShell Active Directory GPO enumeration	Some components of Industroyer2 were deployed via GPO. It is believed the PowerShell enumeration was used to locate GPOs to use for deployment and optionally to confirm that new GPOs created were visible to a sample target.
Create a scheduled task named “vatt” to execute vatt.exe	Per CERT-UA, scheduled tasks were used to launch the malware. The scheduled task created closely mimics that reported by CERT-UA.
Download an executable payload to c:\Users\peramoga.exe	This is the same executable used for vatt.exe. We do not know from reporting how many executable locations were used on a single

https://www.scythe.io/library/threat-emulation-industroyer2-operation

Living off the Land (LOLBAS)

A LOLBin/Lib/Script must:

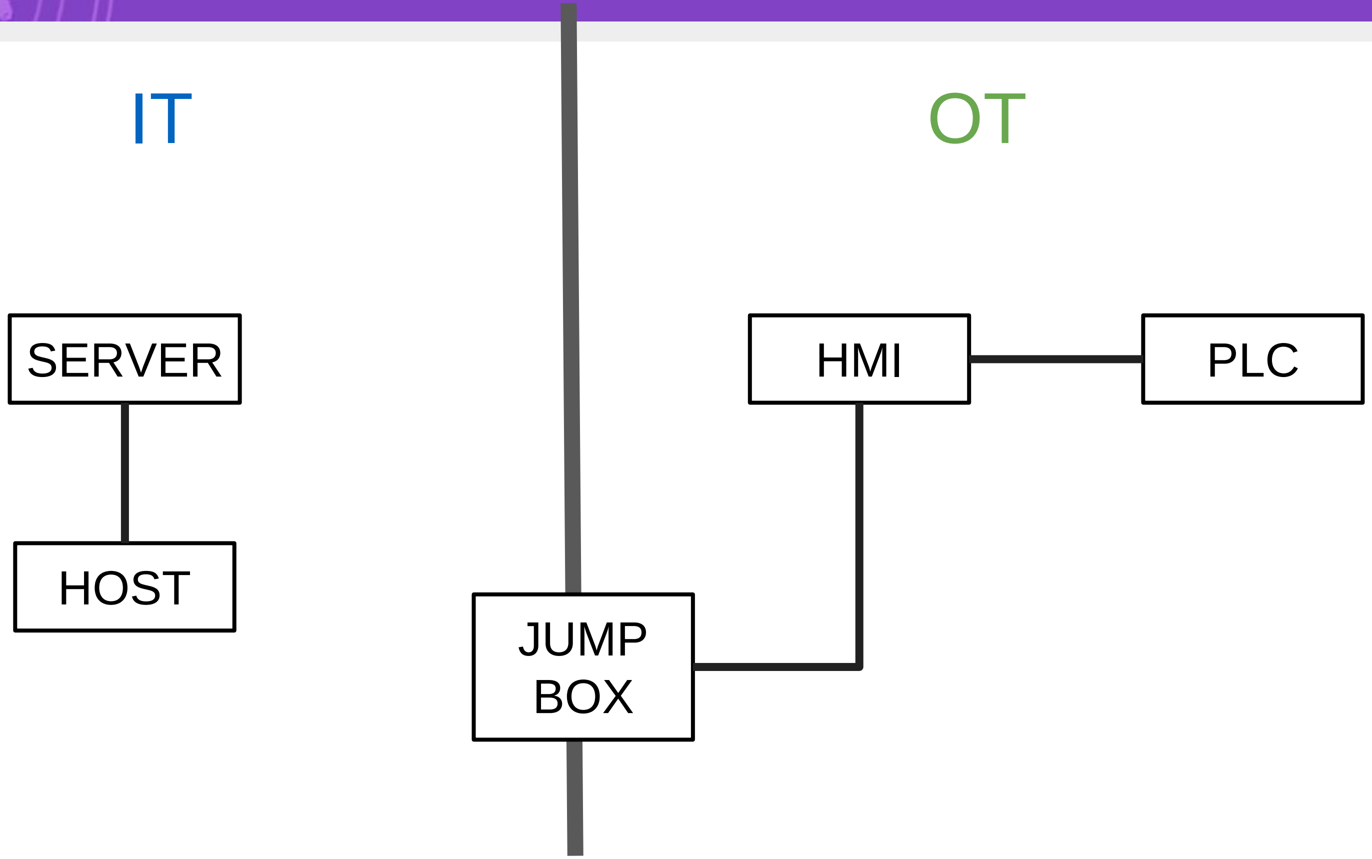
- Be a Microsoft-signed file, either native to the OS or downloaded from Microsoft.
- Have extra "unexpected" functionality. It is not interesting to document intended use cases.
- Exceptions are application allow-listing bypasses
- Have functionality that would be useful to a threat or red team

Living off the Land: ICS Edition!

A LOLBin/Lib/Script must:

- Be an OT Vendor application, either native to the device ecosystem and/or downloaded from the vendor.
- Have device-specific functionality. ~~It is not interesting to document intended use cases.~~
- ~~Exceptions are application allow-listing bypasses~~
- Have functionality that would be useful to a threat or red team

SCOPE: Exercise

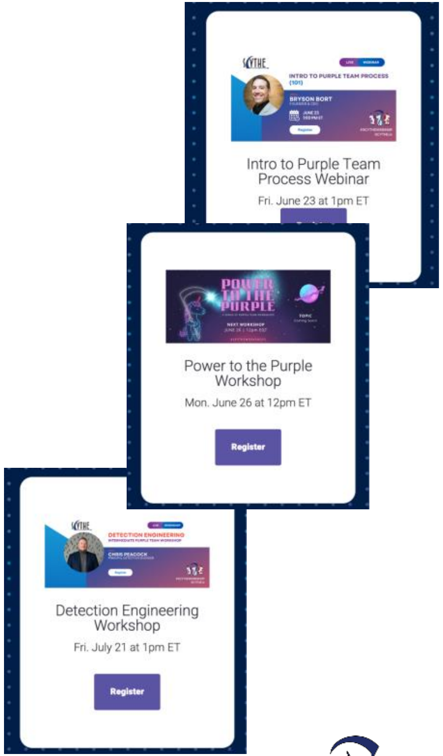


Tips

- OT starts with TRUST
- Safety, Availability, and Revenue
- IT **protects** OT
  - Great place to start!
  - Iterate toward OT
- Access vs Impact

SCYTHE offers free training and workshops every month!

https://scythe.io/workshops



Intro to Purple Team Process Webinar

Fri. June 23 at 1pm ET

Power to the Purple Workshop

Mon. June 26 at 12pm ET

Register

Detection Engineering Workshop

Fri. July 21 at 1pm ET

Register

Resources

Resources

Multiverse of Convergence with Bryson Bort and Tim Schulz, SANS ICS Summit
https://www.youtube.com/watch?v=kTTRFicw20o

A Collection of Resources for Getting Started in ICS/SCADA Cybersecurity by Rob Lee, Dragos
https://www.robertmlee.org/tag/resource-list/

ICS Village
https://www.icsvillage.com
https://hack-the-plant.simplecast.com/

Thank You!

2023 Security Training Survey:

https://www.surveymonkey.com/r/GTGH759