What Does it take to become the next blue team expert ? (Defense)

Ts.Syahmi bin suleiman

Lead, Threat intelligence & threat hunting
(Bluesify Intelligence)

Bluesify solutions sdn. Bhd.

 # dig syahmi.suleiman ANY

Current :

- Bluesify Solutions Sdn Bhd (2018 – Present)
- Lead Threat Intelligence, Threat Hunting & Incident Response
- OWASP Member (syahmi.suleiman@owasp.org)
- hxxps://www[.]linkedin[.]com/in/syahmi-suleiman/

History :

- Cyber Threat Analyst (Security Operation Center, SOC) – T1, T2
- Senior Response Engineer (ADE; Architecture, Development, Engineering)
- Deployment & Configuration in Splunk Enterprise
- Threat Intelligence, Threat Hunting, Incident Response
- Investigation using Splunk & EDR
- Server Hardening (CIS Benchmark)

Education :

- KPTM KL (Computer Science)
- APU/APIIT (IT, Information System Security)

CIAS-ISAO COMMUNITY CYBERSECURITY PROGRAMS

MBOT LEMBAGA TEKNOLOGIS MALAYSIA MALAYSIA BOARD OF TECHNOLOGY

MITRE ATT&CK Defender ATT&CK® SECURITY OPERATIONS CENTER ASSESSMENT CERTIFICATION

MITRE ATT&CK Defender ATT&CK® CYBER THREAT INTELLIGENCE CERTIFICATION

CompTIA CySA+

Agenda

1 - People, Process & Technology :

- Blue Team (SOC) / Cyber Defense Center
- Process, MITRE ATT&CK, Cyber Kill Chain
- Threat Intelligence
- SIEM
- Splunk (SIEM) & Install Splunk

2 - Blue Team Expertise :

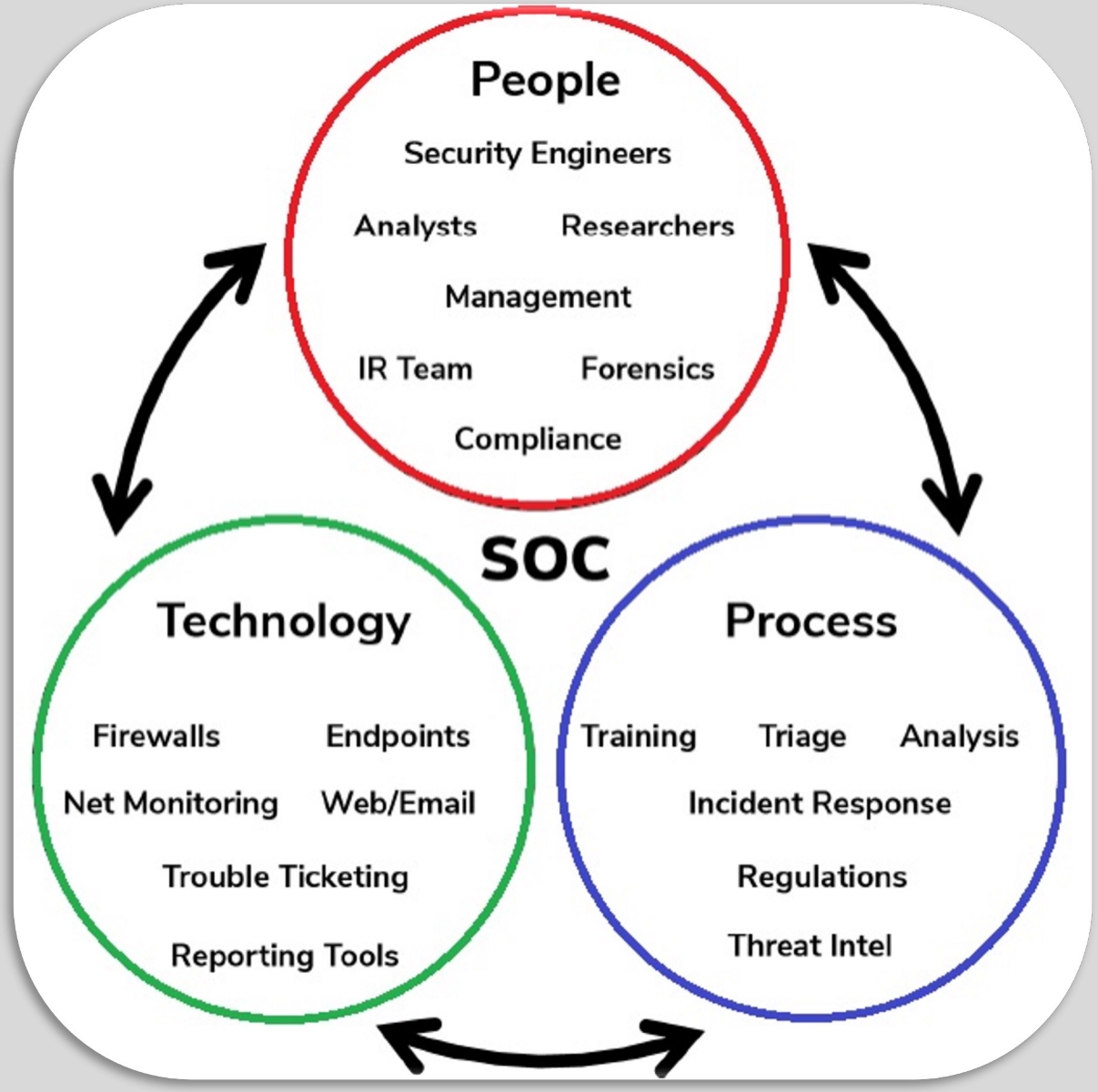
- Understanding The Technology
- Cyber Threat Use Cases + Understanding in Offensive
- Threat Intelligence
- IoC vs IoA

3 – Use Cases :

- Find Suspicious or Malicious Activity About.....
- Web Log - Detection Log4j or Log4Shell
- Regular Expression (Regex) for Detection
- Idea To Detect The CrackMapExec Behavior
- Tips for Phishing Email Investigation
- Cyber Threat Intelligence (CTI) Perspective

People, process & technology

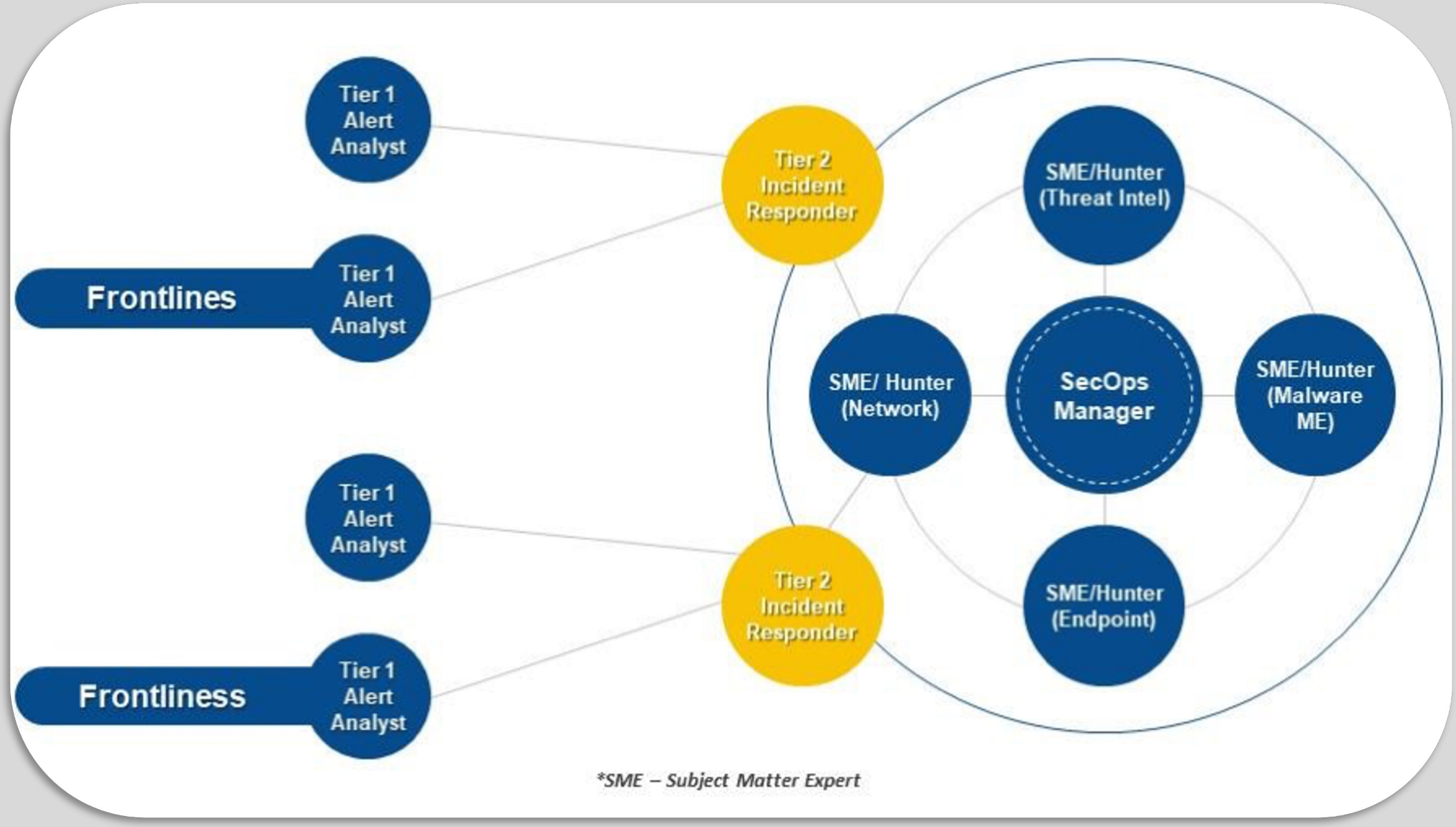
People, Process & Technology



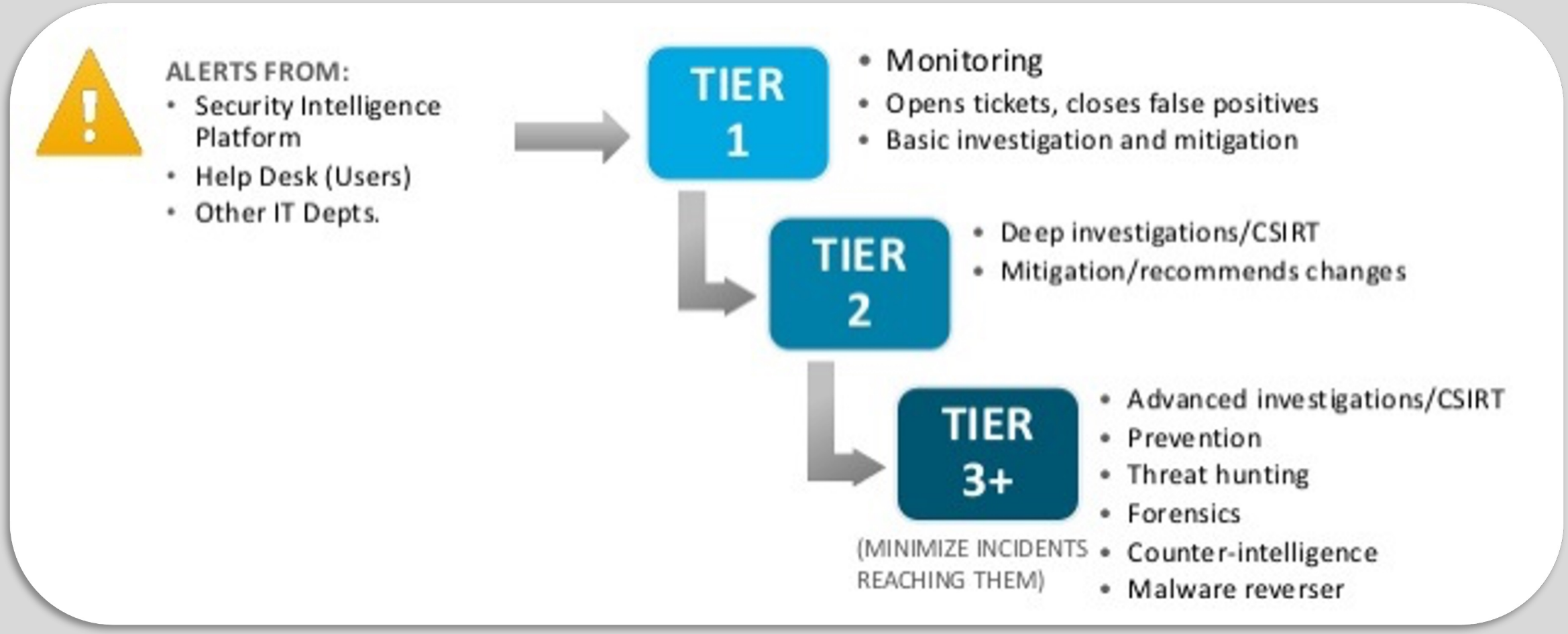
Blue Team (SOC) / Cyber Defense Center

What Do You Imagine ?

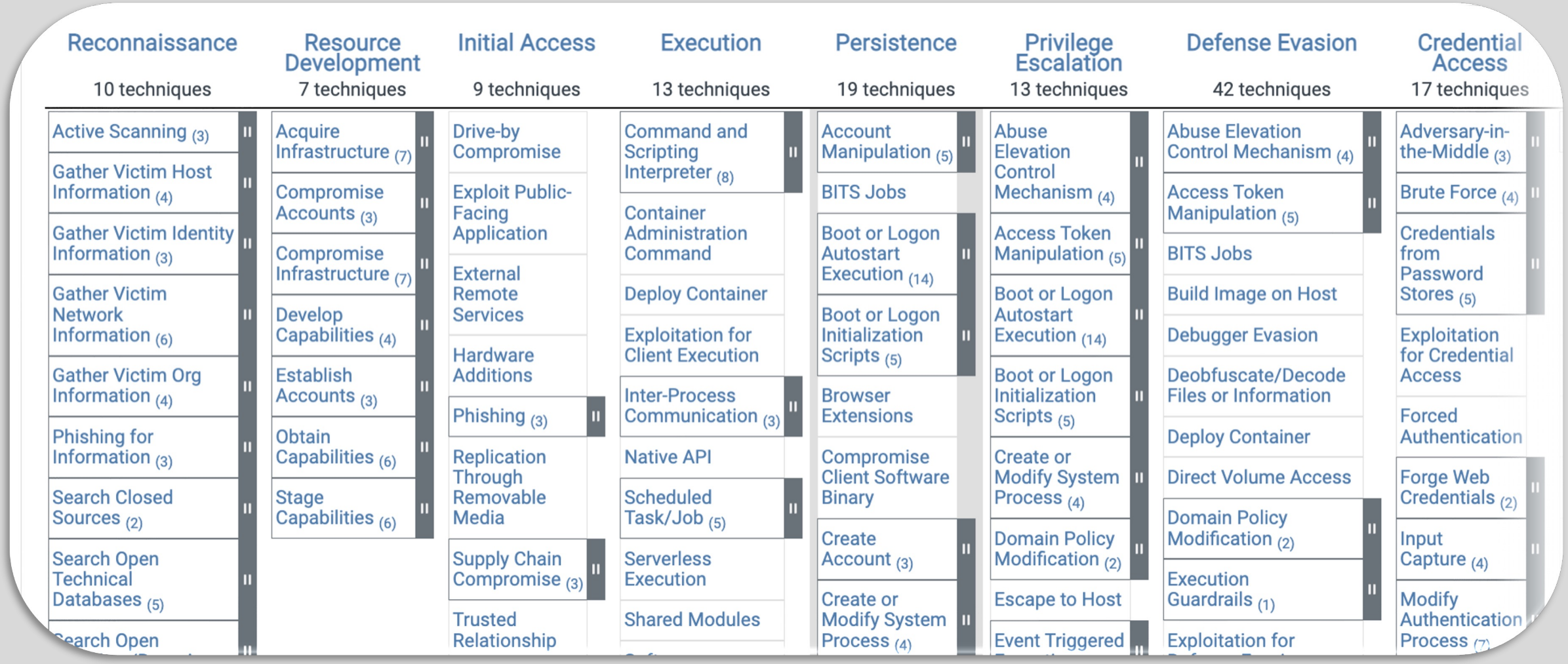
Blue Team (SOC) / Cyber Defense Center – cont.



Process, MITRE ATT&CK, Cyber Kill Chain

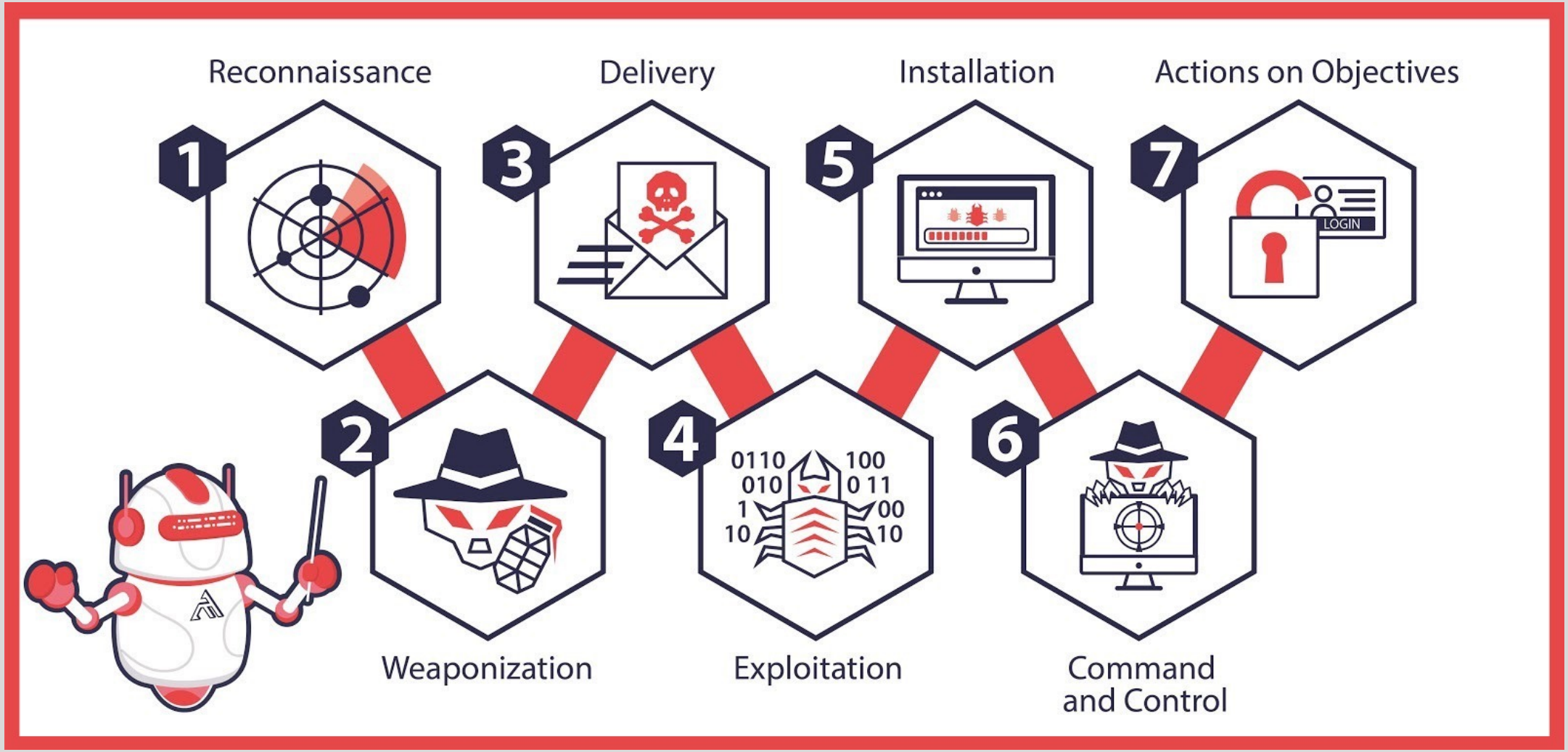


Process, MITRE ATT&CK, Cyber Kill Chain – cont.



https://attack.mitre.org/matrices/enterprise/

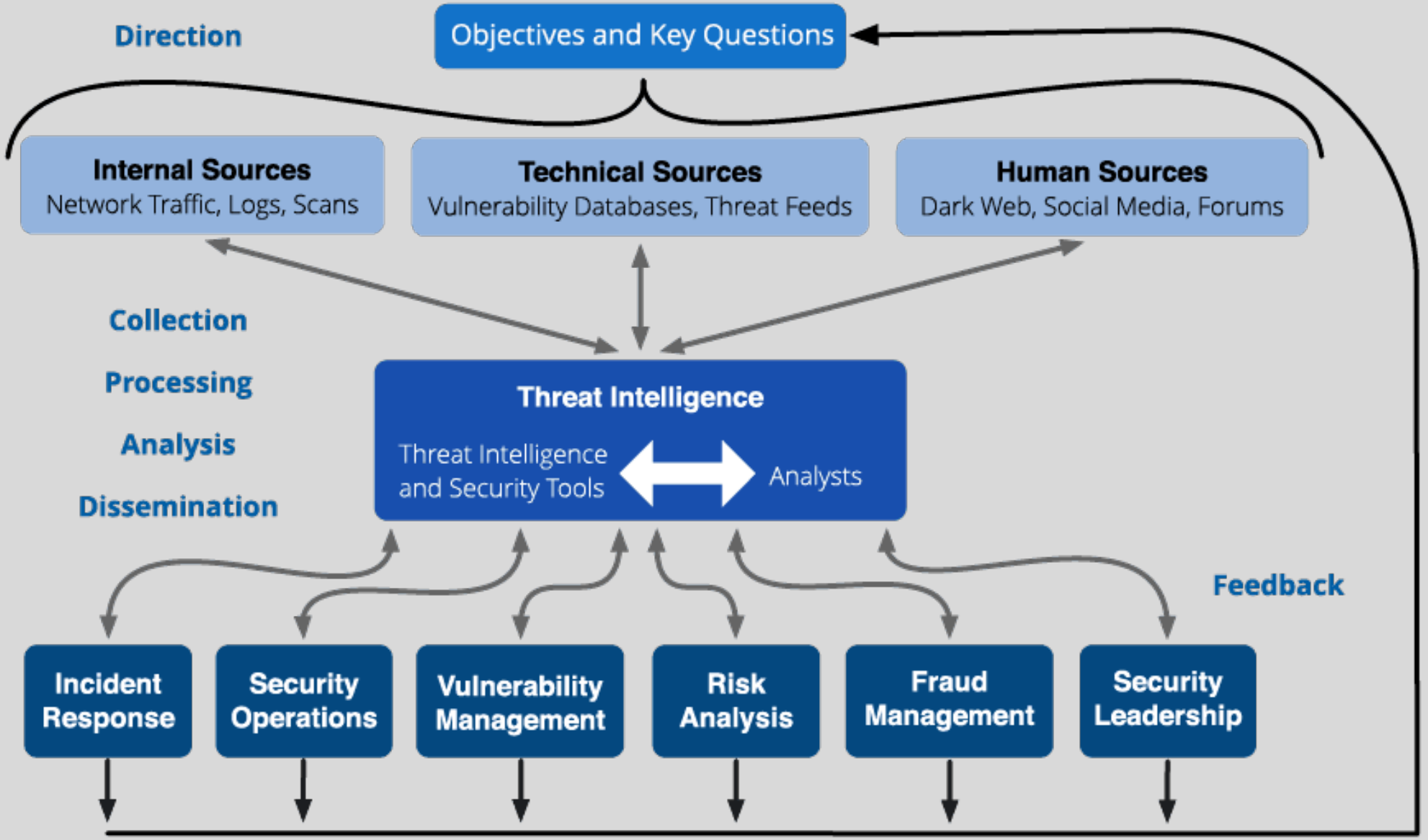
Process, MITRE ATT&CK, Cyber Kill Chain – cont.



https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

Threat Intelligence - Basic Lifecyle

Threat Intelligence – Process in CTI



Threat Intelligence – Simplified Category of CTI

TACTICAL

Focused on performing malware analysis & enrichment, as well as ingesting atomic, static, and behavioral threat indicators into defensive cybersecurity systems.

STAKEHOLDERS:
- SOC Analyst
- SIEM
- Firewall
- Endpoints
- IDS/IPS

"Mechanic"

OPERATIONAL

Focused on understanding adversarial capabilities, infrastructure, & TTPs, and then leveraging that understanding to conduct more targeted and prioritized cybersecurity operations.

STAKEHOLDERS:
- Threat Hunter
- SOC Analyst
- Vulnerability Mgmt.
- Incident Response
- Insider Threat

"Race Car Driver"

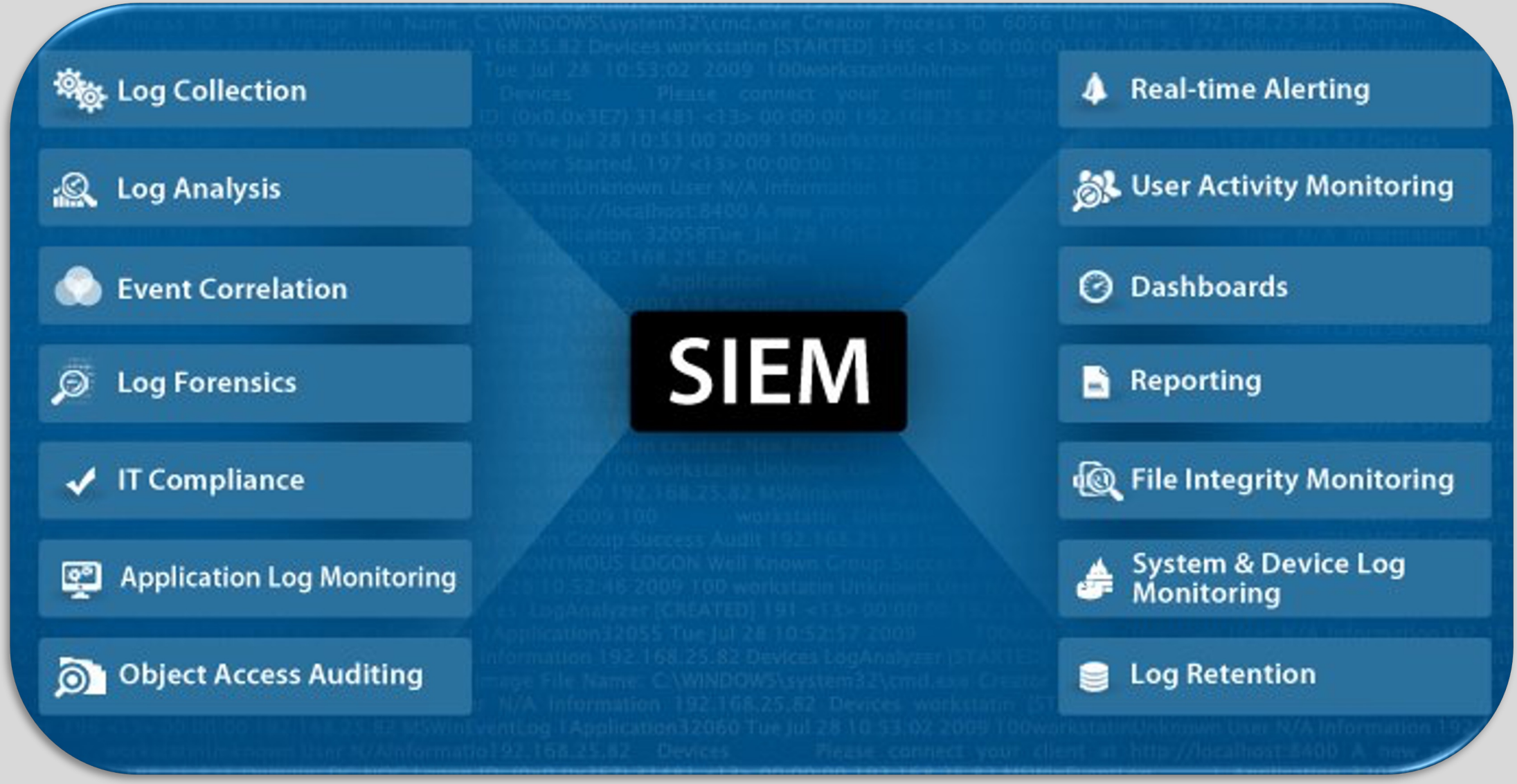
STRATEGIC

Focused on understanding high level trends and adversarial motives, and then leveraging that understanding to engage in strategic security and business decision-making.

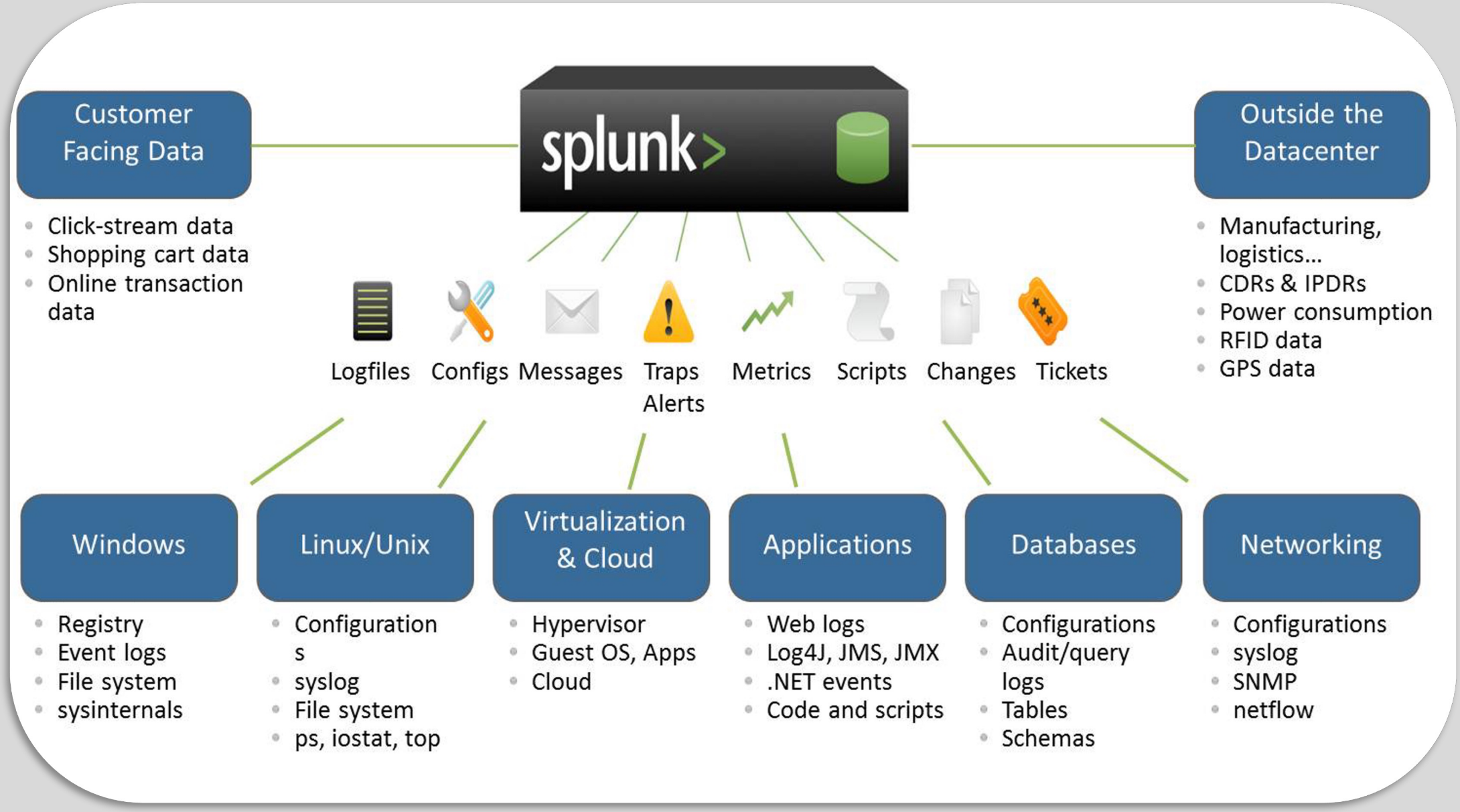
STAKEHOLDERS:
- CISO
- CIO
- CTO
- Executive Board
- Strategic Intel

"The Owner"

Security Information and Event Management (SIEM)



Splunk (SIEM)


Customer Facing Data
Click-stream data
Shopping cart data
Online transaction data
splunk>
Outside the Datacenter
Manufacturing, logistics…
CDRs & IPDRs
Power consumption
RFID data
GPS data
Logfiles
Configs
Messages
Traps
Alerts
Metrics
Scripts
Changes
Tickets
Windows
Registry
Event logs
File system
sysinternals
Linux/Unix
Configuration s
syslog
File system
ps, iostat, top
Virtualization & Cloud
Hypervisor
Guest OS, Apps
Cloud
Applications
Web logs
Log4J, JMS, JMX
.NET events
Code and scripts
Databases
Configurations
Audit/query logs
Tables
Schemas
Networking
Configurations
syslog
SNMP
netflow

Install Splunk (SIEM)

- wget -O splunk-9.0.2-17e00c557dc1-Linux-x86_64.tgz "https://download.splunk.com/products/splunk/releases/9.0.2/linux/splunk-9.0.2-17e00c557dc1-Linux-x86_64.tgz"

- mv splunk... /opt
- cd /opt
- tar xvzf splunk....

- cd splunk/bin
- splunk/bin/splunk (OR ./splunk) start --accept-license
- splunk/bin/splunk (OR ./splunk) enable boot-start

maybe can consider to disable firewalld

Ingest Data Sources in Splunk

- Click on “Splunk Enterprise” logo, and choose “Add Data”
- Choose “Upload”, and the drag the file... After Done, click Next

- **For web-access-log.log;** Select Sourcetype Web>”Access Combined”

Then, click Next and choose index as “main”. Review and Submit.

| index=main sourcetype=access_combined

- **For test-1.log;** Select “Save As”, create new sourcetype named “fgt-test-1”

Then, click Next and choose index as “main”. Review and Submit.

| index=main sourcetype=fgt-test-1

- **For firewall-log.csv;** Select “Save As”, create new sourcetype named “fgt-app-server”

Then, click Next and choose index as “main”. Review and Submit.

| index=main sourcetype=fgt-app-server

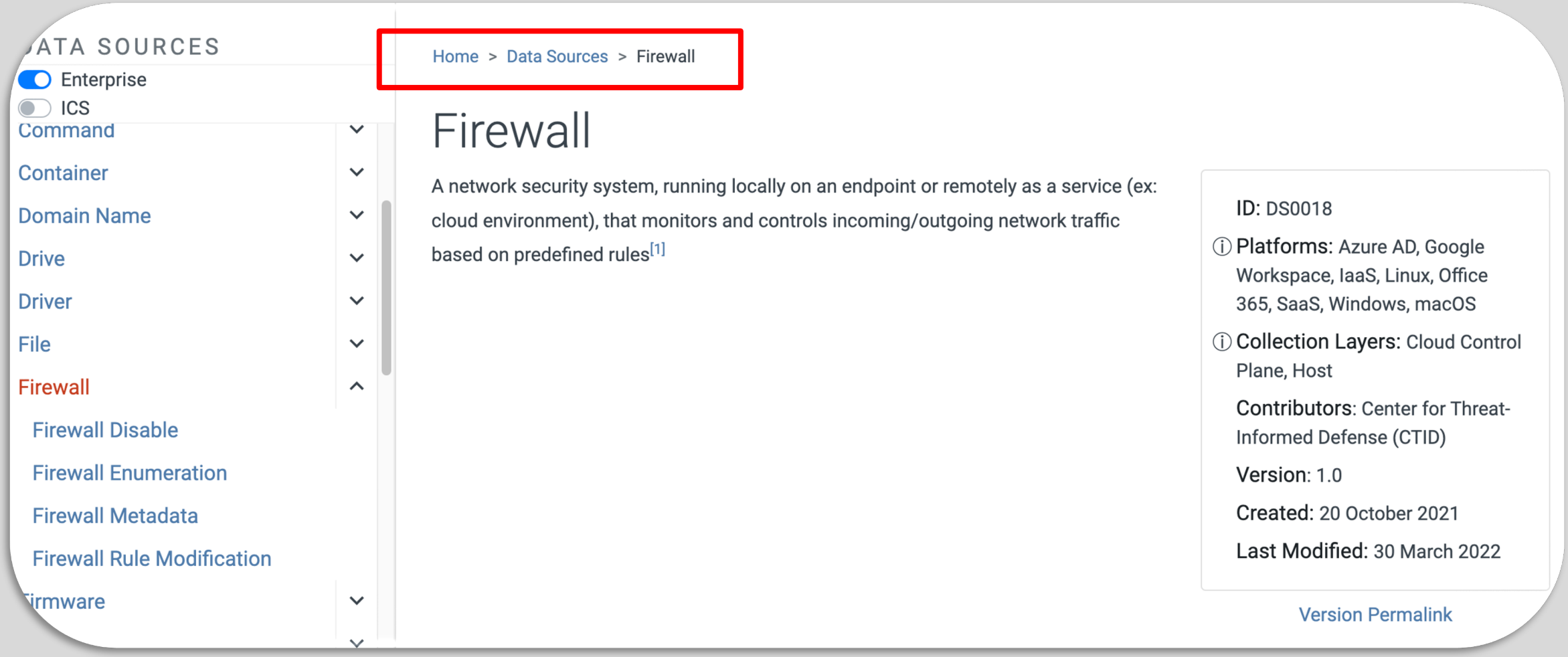
What do you need as Blue team warrior

Understanding On The Technology

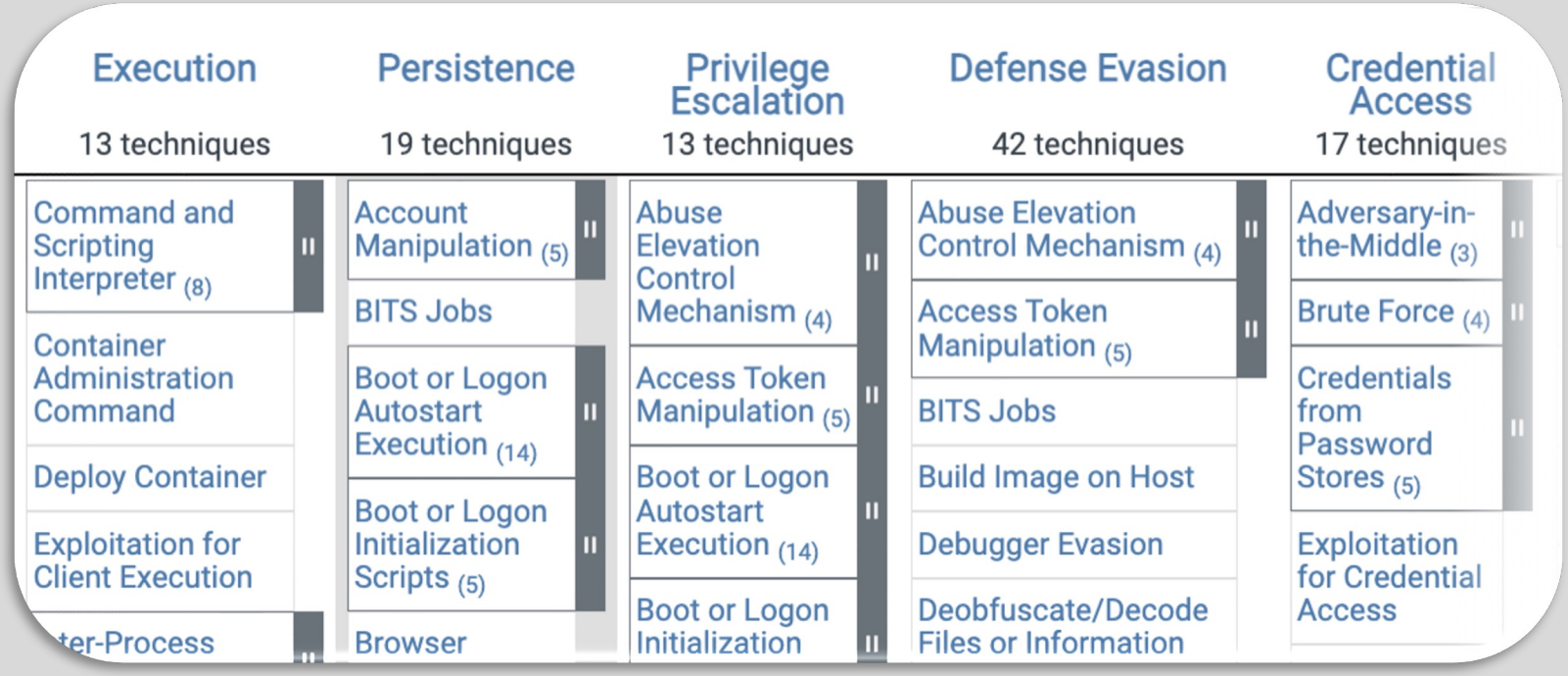
```
| tstats count where (index=fw_* OR index=dns* OR index=crowdstrike) by index, sourcetype
```

...dex	sourcetype
crowdstrike	CrowdStrike:Event:Streams:JSON
dns_windows	stream:dns
fw_fortigate	fortigate_event
fw_fortigate	fortigate_traffic
fw_fortigate	fortigate_utm
fw_pfsense	pfsense
fw_pfsense	pfsense:cron
fw_pfsense	pfsense:dhcpd
fw_pfsense	pfsense:filterlog
fw_pfsense	pfsense:nginx
fw_pfsense	pfsense:ntpd
fw_pfsense	pfsense:syslogd

Understanding On The Technology – cont.



Cyber Threat Use Cases + Understanding in Offensive



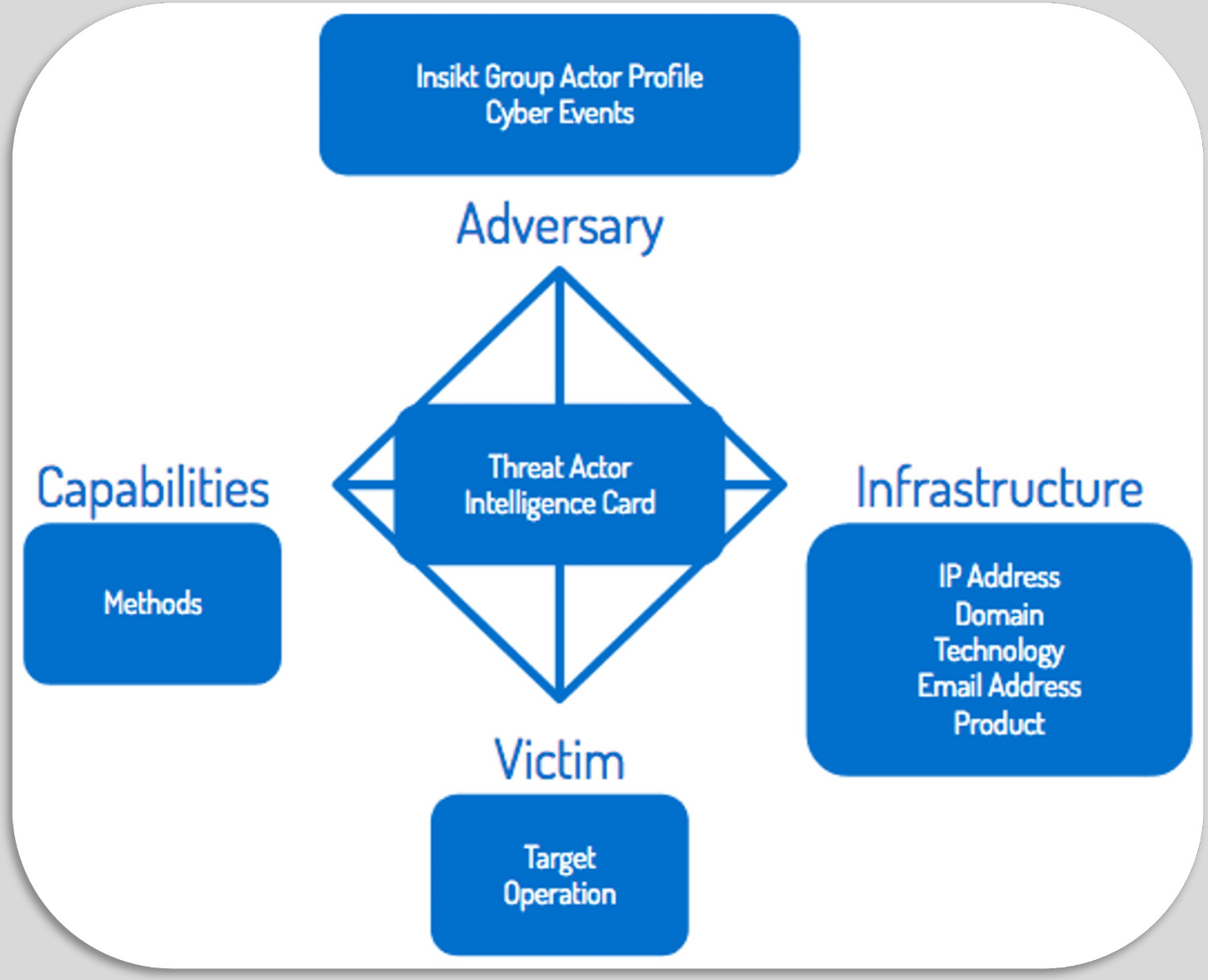
https://www.socinvestigation.com/uefi-persistence-via-wpbbin-detection-response/

Detection for UEFI Persistence via WPBBIN

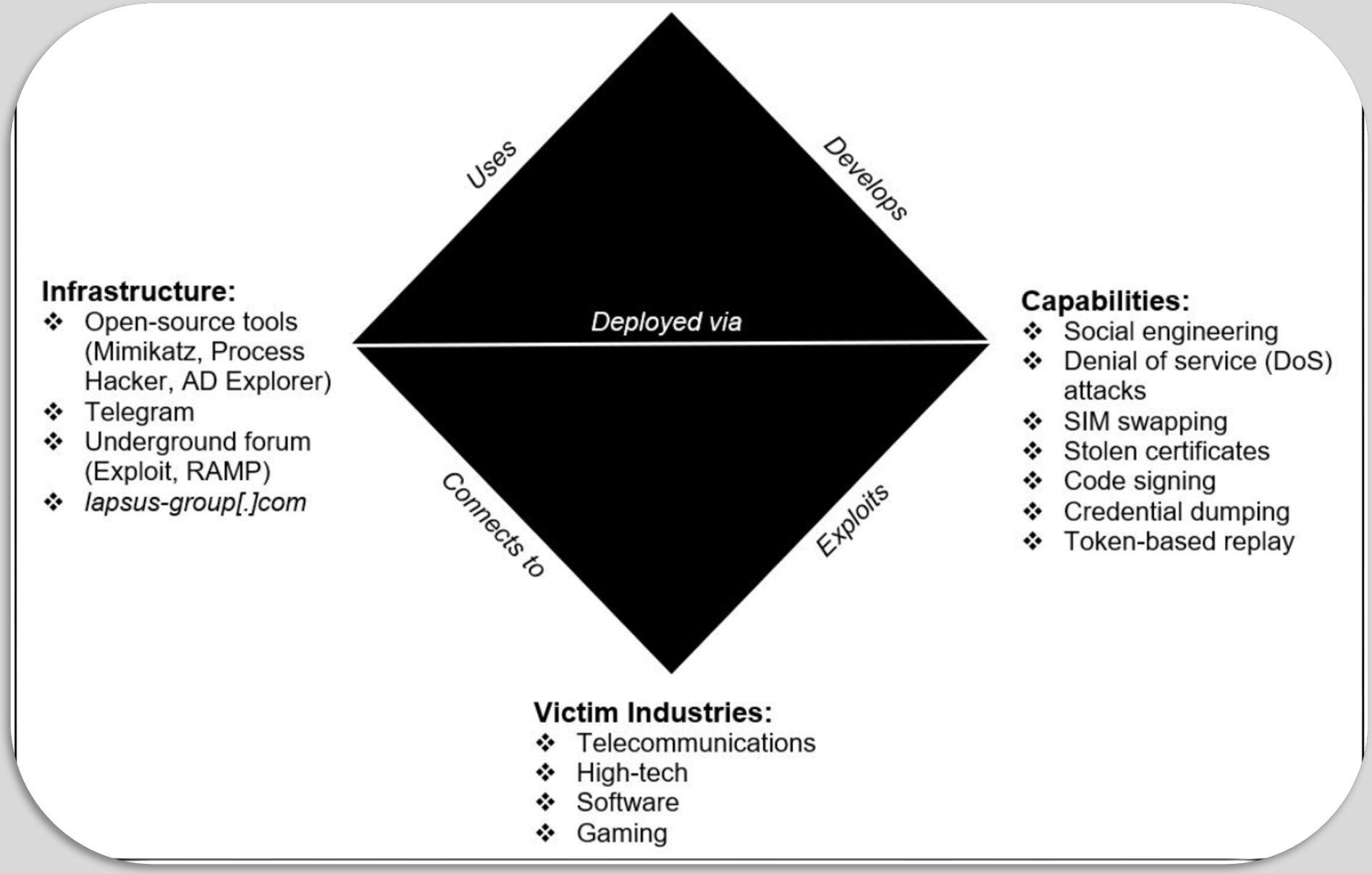
Splunk:

```
source="WinEventLog:*" AND ((TargetFilename="*wpbbin.exe") OR Image="*\\wpbbin.exe")
```

Threat Intelligence



Threat Intelligence – LAPSUS$ As A Sample



Indicator of Compromise vs Indicator of Attack

Use cases

Remember !

Different environment, might have different log pattern

Different technology, might have different log pattern

Find Suspicious or Malicious Activity About.....

 # to search for what are the indexes and sourcetypes available

| tstats count where index= by index, sourcetype*

 # to search for specific log type by using index and sourcetype

index=main sourcetype=fgt-app-server

 # to display the result and values by using table function

| table _time, ...

 # to display statistical results and values using stats functions

| stats count by values(field_name) AS “renaming”, count by <fieldname>

Find Suspicious or Malicious Activity About..... – cont.

index=main sourcetype="fgt_test-1"

Use your understanding about cyber security to pin pinpoint which one is suspicious or malicious

Do You Want Clue ?? You Sure ??

Web Log - Detection Log4j or Log4Shell

 # to search for specific log type by using index and sourcetype

index=main sourcetype=access_combined

 # to display the result and values by using table function

| table _time, ...

 # to display statistical results and values using stats functions

| stats count by values(field_name) AS “renaming”, count by <fieldname>

Regular Expression (Regex) for Detection

 # Open up the file sample given in GDrive, “sample-regex-for-log4j.txt”

 # CNP in Regex101 site, we do the Regex to detect the Log4Shell attack

(?<log4j>\$?\{?\${(jndi|env|:|lower|upper):(\w+|\W+)(\w+|\W+)(\w+|\W)(\S+}./.\w+[^\/]+\S+).+})

 # Use Splunk to detect Log4Shell

Idea To Detect The CrackMapExec Behavior

 # Check with MITRE ATT&CK > Software > CrackMapExec

 # Search for it’s behavior, research on what it is

Googling it ! Makes the Internet useful for you.....

 # Basically; research, understand, implement

 # Leveraging the CTI to detect or hunting the behavior

Tips For Phishing Email Investigation

FROM & TO

Your Experience in Investigation

- Before, During & After
- Anomaly / Suspicious

Cyber Threat Intelligence (CTI) Perspective

une 14, 2021

Behind the scenes of business email compromise: Using cross-domain threat data to disrupt a large BEC campaign

Microsoft 365 Defender Research Team
Microsoft Threat Intelligence Center (MSTIC)

HREAT INTELLIGENCE BRIEF

Anatomy of a Compromised Account

How BEC Actors Use Credential Phishing and Exploit Compromised Accou

AGARI by HelpSystems

What Methods are Used to Access Compromised Accounts?

In nearly all accounts that were auto-validated by a phishing site, we observed a consistent pattern in which the user agent string linked to the activity was *BAV2ROPC*. Based on our research, *BAV2ROPC* is a user agent string linked to the use of an OAuth 2.0 token. OAuth tokens are commonly used to access applications without requiring a user to share their password directly with a third-party and are frequently leveraged in APIs. More than 90% of the times we saw this *BAV2ROPC* user agent string, it was associated with an automated credential validation event.

When accounts were accessed manually, 15% of attackers used an email client, such as Microsoft Outlook or Apple Mail, while a vast majority of actors simply logged directly into an account using a browser. The most common browser used to access our compromised accounts was Chrome, followed by Firefox, Edge, Opera, and Safari. Nearly two-thirds of actors accessing compromised accounts were using a Windows operating system, compared to 35% that were using Mac OS X. Interestingly, a small percentage of actors used a mobile device to ccess our accounts and only one used a Linux operating system.

- Credentials checks with user agent "BAV2ROPC", which is likely a code base using legacy protocols like IMAP/POP3, against Exchange Online. This results in an ROPC OAuth flow, which returns an "invalid_grant" in case MFA is enabled, so no MFA notification is sent.
- Forwarding rule creations with Chrome 79.
- Email exfiltration with an POP3/IMAP client for selected targets.

Cyber Threat Intelligence (CTI) Perspective – cont.

Basic Authentication and Exchange Online – February 2021 Update

By The_Exchange_Team

Published 02-04-2021 09:00 AM 91.5K Views

We previously announced we would begin to disable Basic Auth for five Exchange Online protocols in the second half of 2021. Due to the pandemic and the effect it has on priorities and work patterns, we are announcing some important changes to our plan to disable Basic Auth in Exchange Online. Please read this post carefully, as there's a lot of detail.

The first change is that until further notice, we will **not** be disabling Basic Auth for any protocols that your tenant is ***using***. When we resume this program, we will provide a minimum of twelve months notice before we block the use of Basic Auth on any protocol being used in your tenant.

Latest New FQDN

Date&Time	FQDN	Domain Name
22:09:03 04/06/2021	feedback-smtp.eu-west-1.amazonses.com	amazonses.com
09:30:18 19/05/2021	a87-226.smtp-out.us-west-2.amazonses.com	amazonses.com

Region Name	Feedback Endpoints for Custom MAIL FROM Sending Configurations
Asia Pacific (Sydney)	feedback-smtp.ap-southeast-2.amazonses.com
Asia Pacific (Tokyo)	feedback-smtp.ap-northeast-1.amazonses.com
Canada (Central)	feedback-smtp.ca-central-1.amazonses.com
Europe (Frankfurt)	feedback-smtp.eu-central-1.amazonses.com
Europe (Ireland)	feedback-smtp.eu-west-1.amazonses.com

Cyber Threat Intelligence (CTI) Perspective – cont.

Total Unique IP	Country	Result Status	Logon Error	Value Name	Value/Agent	Sparkline	First Attempt	Latest Attempt	Total Failed
788	71	Failed	IdsLocked	RequestType	1		22/04/2021	23/04/2021	3625
			InvalidUserNameOrPassword	ResultStatusDetail	BAV2ROPC		01:49:27	17:19:23	
				UserAgent	OAuth2:Token				
				UserAuthenticationMethod	UserError				


End... See you around...