

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)



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 :

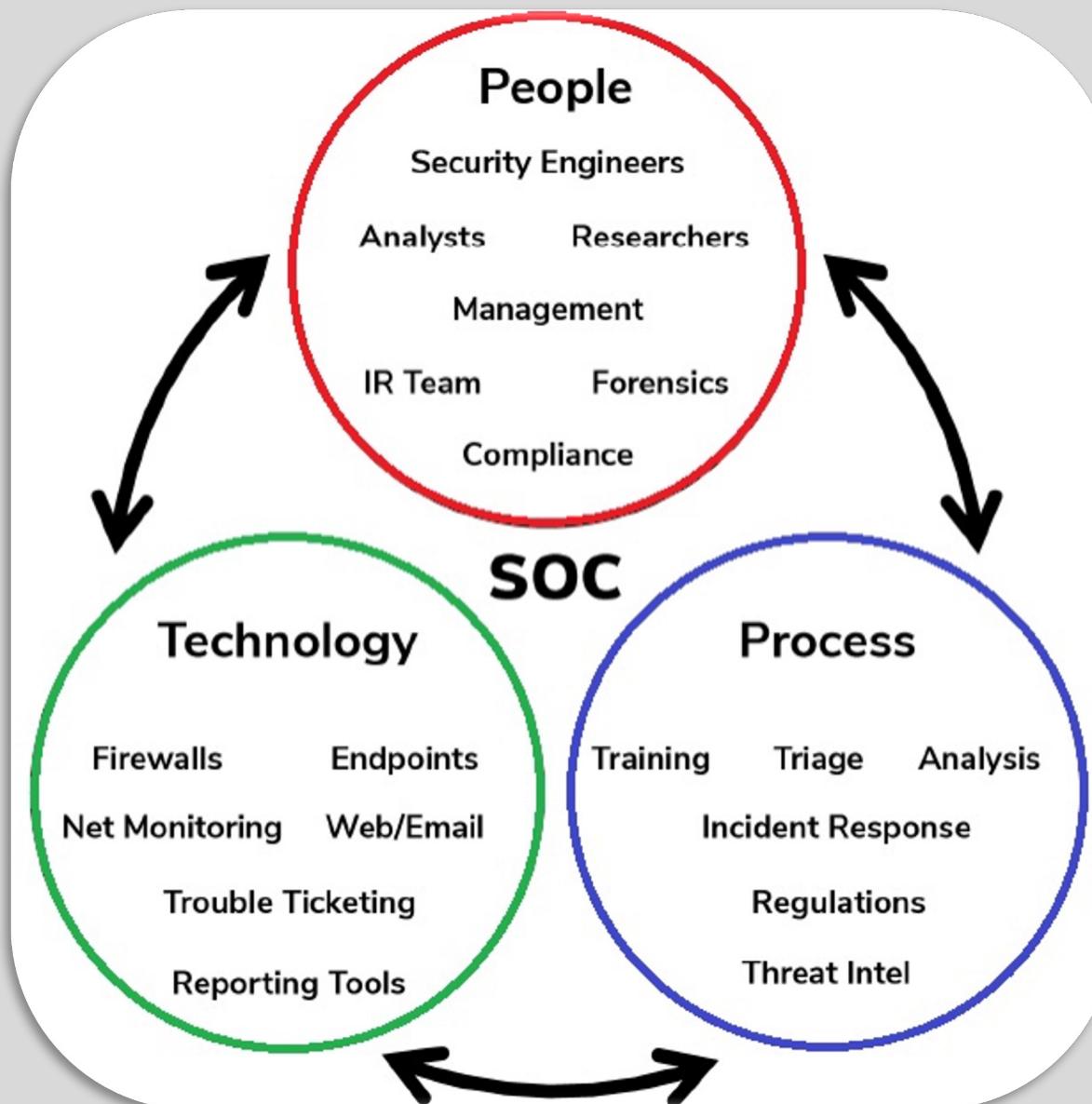
- Find Suspicious or Malicious Activity About.....
- Web Log - Detection Log4j or Log4Shell
- Regular Expression (Regex) for Detection
- Idea To Detect The CrackMapExec Behavior
- Tips for Phishing Email Investigation
- Cyber Threat Intelligence (CTI) Perspective



PEOPLE, PROCESS & TECHNOLOGY



People, Process & Technology

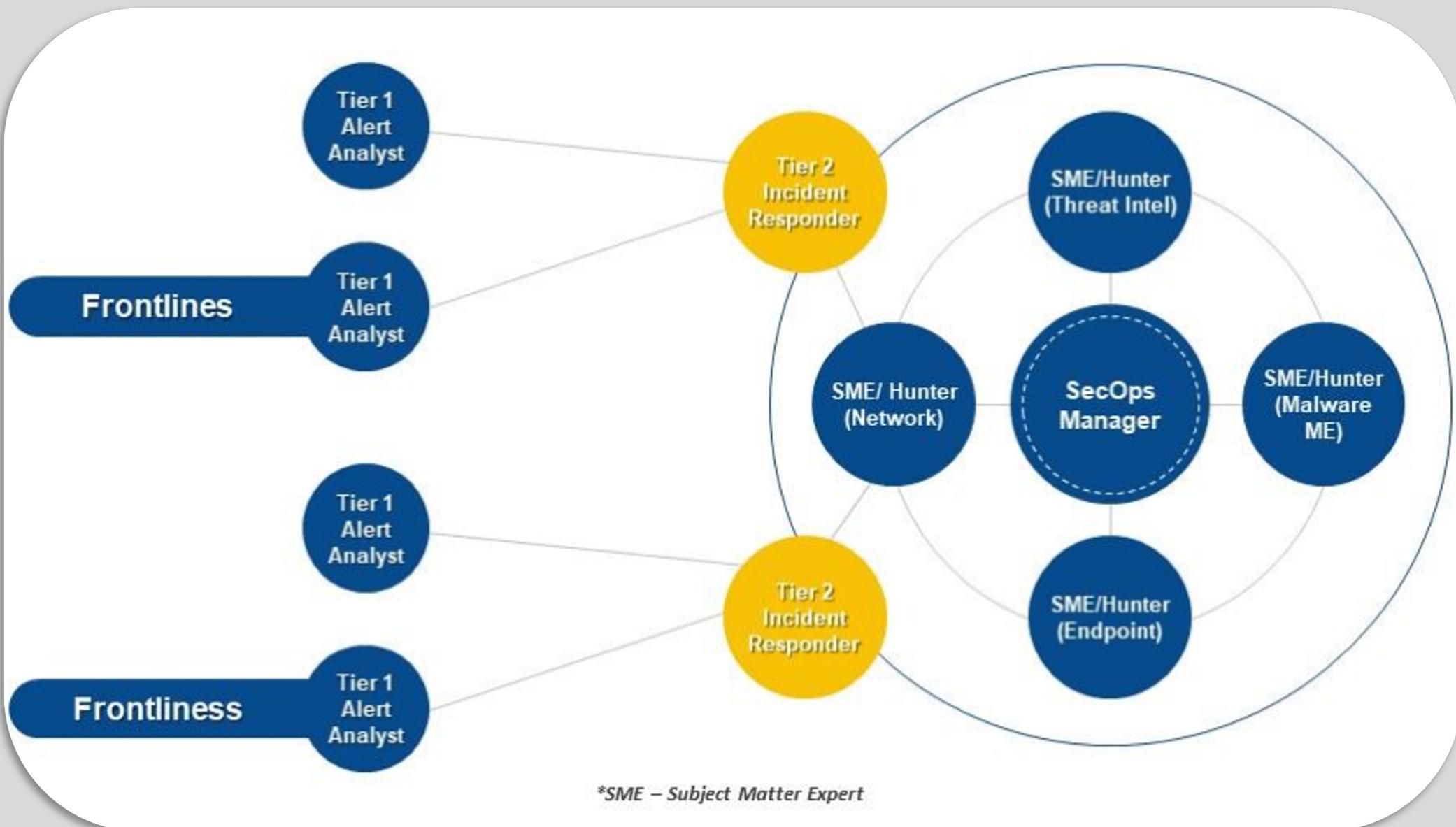


Blue Team (SOC) / Cyber Defense Center

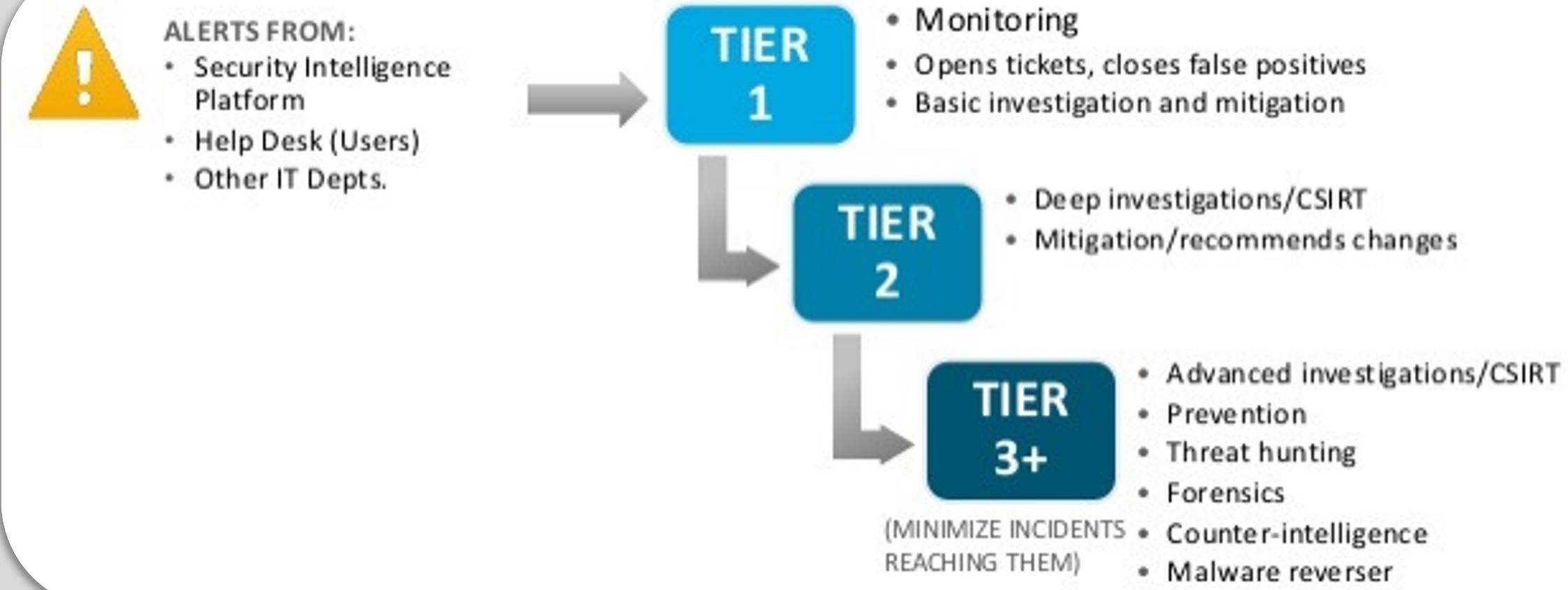


WHAT Do You IMAGINE ?

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



Process, MITRE ATT&CK, Cyber Kill Chain



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

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access
10 techniques	7 techniques	9 techniques	13 techniques	19 techniques	13 techniques	42 techniques	17 techniques
Active Scanning (3)	Acquire Infrastructure (7)	Drive-by Compromise	Command and Scripting Interpreter (8)	Account Manipulation (5)	Abuse Elevation Control Mechanism (4)	Abuse Elevation Control Mechanism (4)	Adversary-in-the-Middle (3)
Gather Victim Host Information (4)	Compromise Accounts (3)	Exploit Public-Facing Application	Container Administration Command	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Brute Force (4)
Gather Victim Identity Information (3)	Compromise Infrastructure (7)	External Remote Services	Deploy Container	Boot or Logon Autostart Execution (14)	BITS Jobs	Build Image on Host	Credentials from Password Stores (5)
Gather Victim Network Information (6)	Develop Capabilities (4)	Hardware Additions	Exploitation for Client Execution	Boot or Logon Initialization Scripts (5)	Boot or Logon Autostart Execution (14)	Debugger Evasion	Exploitation for Credential Access
Gather Victim Org Information (4)	Establish Accounts (3)	Phishing (3)	Inter-Process Communication (3)	Browser Extensions	Boot or Logon Initialization Scripts (5)	Deobfuscate/Decode Files or Information	Forced Authentication
Phishing for Information (3)	Obtain Capabilities (6)	Replication Through Removable Media	Native API	Compromise Client Software Binary	Create or Modify System Process (4)	Deploy Container	Forge Web Credentials (2)
Search Closed Sources (2)	Stage Capabilities (6)	Supply Chain Compromise (3)	Scheduled Task/Job (5)	Create Account (3)	Domain Policy Modification (2)	Direct Volume Access	Input Capture (4)
Search Open Technical Databases (5)	Trusted Relationship	Serverless Execution	Shared Modules	Create or Modify System Process (4)	Escape to Host	Domain Policy Modification (2)	Modify Authentication Process (7)
Search Open					Event Triggered	Execution Guardrails (1)	Exploitation for Credential Access

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

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

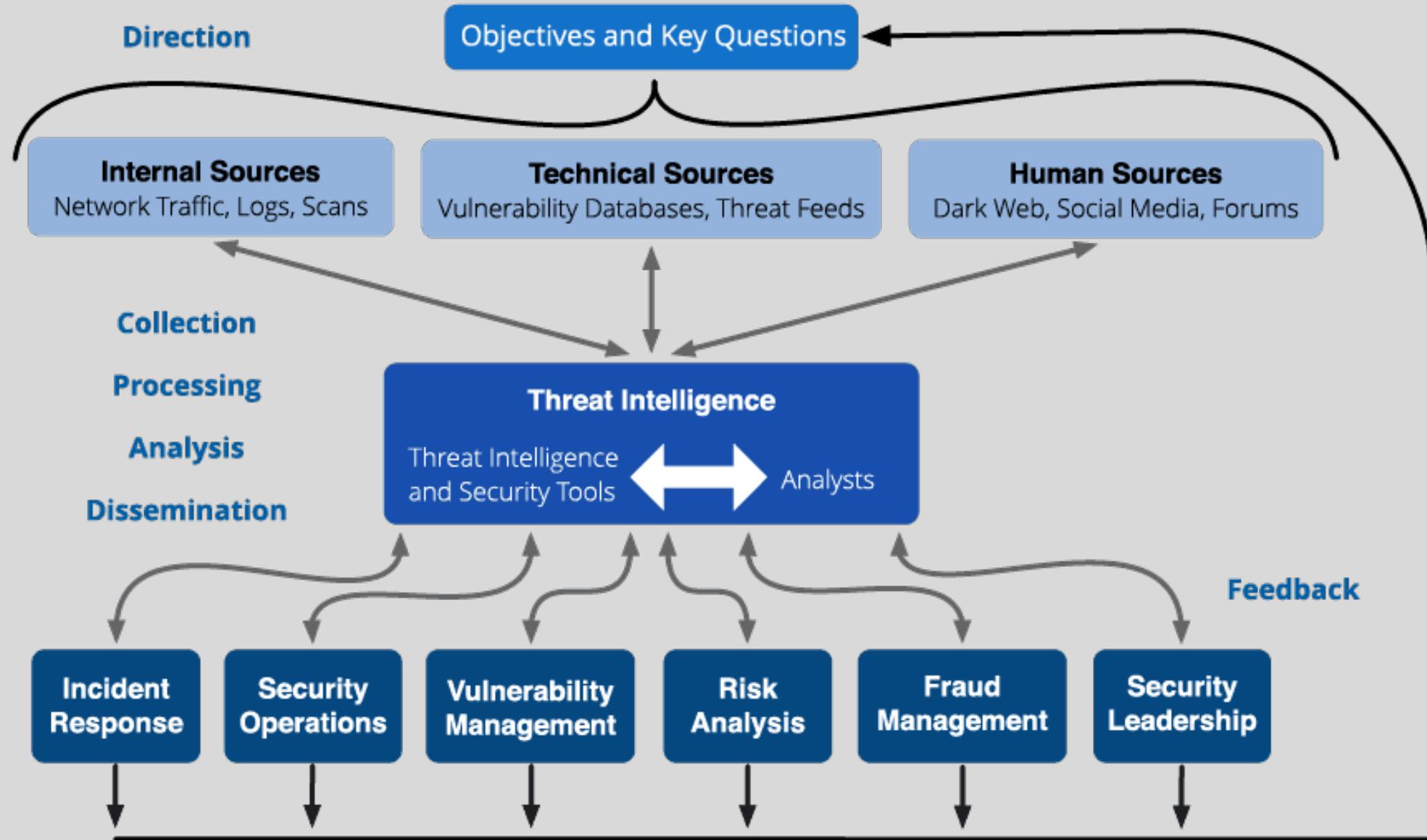


<https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html>

Threat Intelligence - Basic Lifecycle



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.

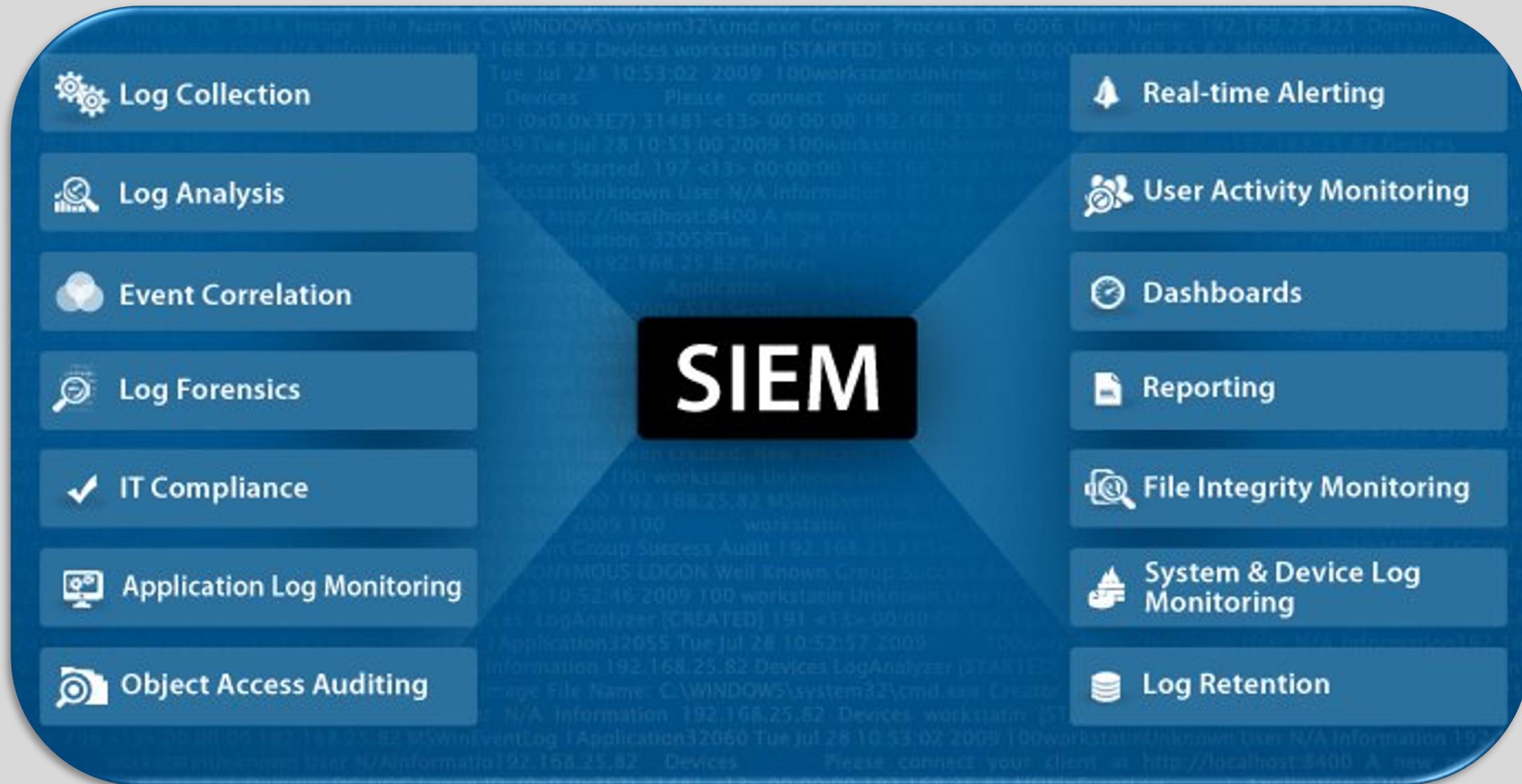
STAKEHOLDERS:

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

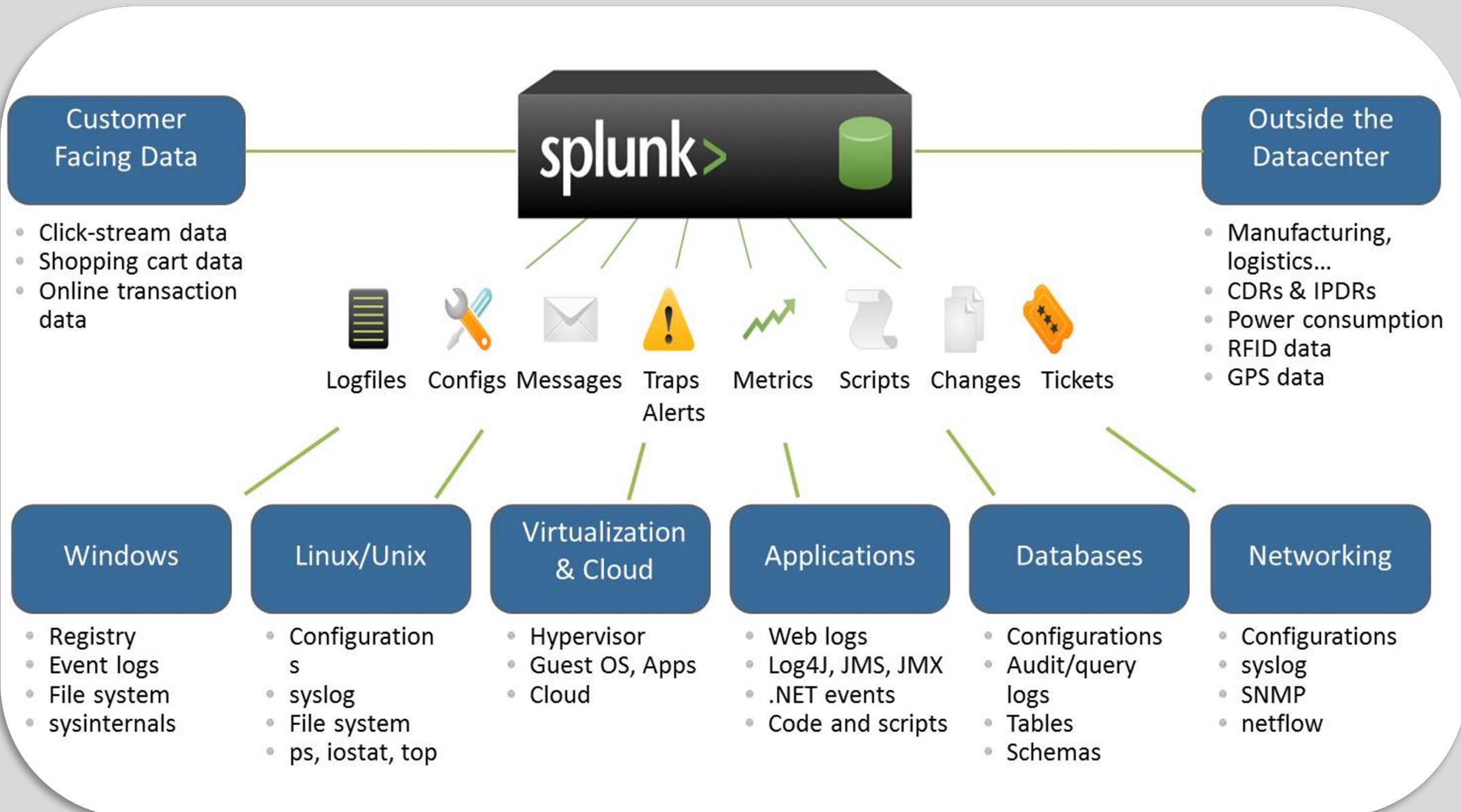


"The Owner"

Security Information and Event Management (SIEM)



Splunk (SIEM)



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
```

index	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.

The screenshot shows a web-based interface for managing data sources. On the left, there's a sidebar titled 'DATA SOURCES' with a tree view of categories: Enterprise (selected), ICS, Command, Container, Domain Name, Drive, Driver, File, Firewall (selected), Firewall Disable, Firewall Enumeration, Firewall Metadata, Firewall Rule Modification, and Firmware. The 'Firewall' node has a red box drawn around it. The main content area shows the breadcrumb navigation 'Home > Data Sources > Firewall'. The title 'Firewall' is displayed prominently. A detailed description follows: 'A network security system, running locally on an endpoint or remotely as a service (ex: cloud environment), that monitors and controls incoming/outgoing network traffic based on predefined rules' with a link '[1]'. To the right, there's a summary box containing metadata: ID: DS0018, Platforms: Azure AD, Google Workspace, IaaS, Linux, Office 365, SaaS, Windows, macOS, Collection Layers: Cloud Control Plane, Host, Contributors: Center for Threat-Informed Defense (CTID), Version: 1.0, Created: 20 October 2021, and Last Modified: 30 March 2022. At the bottom right of the summary box is a 'Version Permalink' link.

DATA SOURCES

- Enterprise
- ICS
- Command
- Container
- Domain Name
- Drive
- Driver
- File
- Firewall
- Firewall Disable
- Firewall Enumeration
- Firewall Metadata
- Firewall Rule Modification
- Firmware

Home > Data Sources > Firewall

Firewall

A network security system, running locally on an endpoint or remotely as a service (ex: cloud environment), that monitors and controls incoming/outgoing network traffic based on predefined rules^[1]

ID: DS0018

Platforms: Azure AD, Google Workspace, IaaS, Linux, Office 365, SaaS, Windows, macOS

Collection Layers: Cloud Control Plane, Host

Contributors: Center for Threat-Informed Defense (CTID)

Version: 1.0

Created: 20 October 2021

Last Modified: 30 March 2022

Version Permalink

Cyber Threat Use Cases + Understanding in Offensive

Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access
13 techniques	19 techniques	13 techniques	42 techniques	17 techniques
Command and Scripting Interpreter (8)	Account Manipulation (5)	Abuse Elevation Control Mechanism (4)	Abuse Elevation Control Mechanism (4)	Adversary-in-the-Middle (3)
Container Administration Command	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Brute Force (4)
Deploy Container	Boot or Logon Autostart Execution (14)	Boot or Logon Autostart Execution (14)	BITS Jobs	Credentials from Password Stores (5)
Exploitation for Client Execution	Boot or Logon Initialization Scripts (5)	Boot or Logon Initialization	Build Image on Host	Exploitation for Credential Access
User-Process	Browser		Debugger Evasion	
			Deobfuscate/Decode Files or Information	

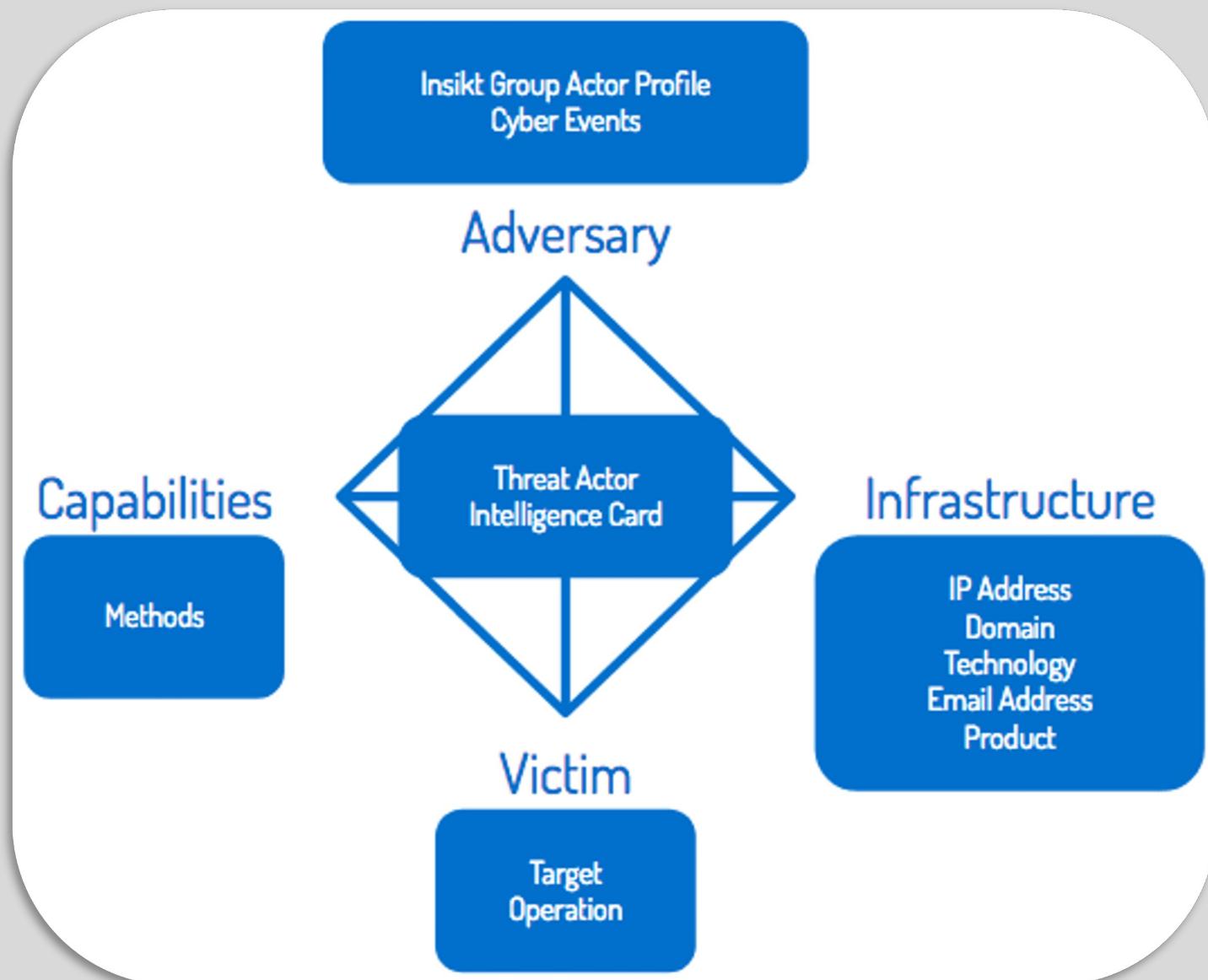
<https://www.socinvestigation.com/uefi-persistence-via-wpbbin-detection-response/>

Detection for UEFI Persistence
via WPBBIN

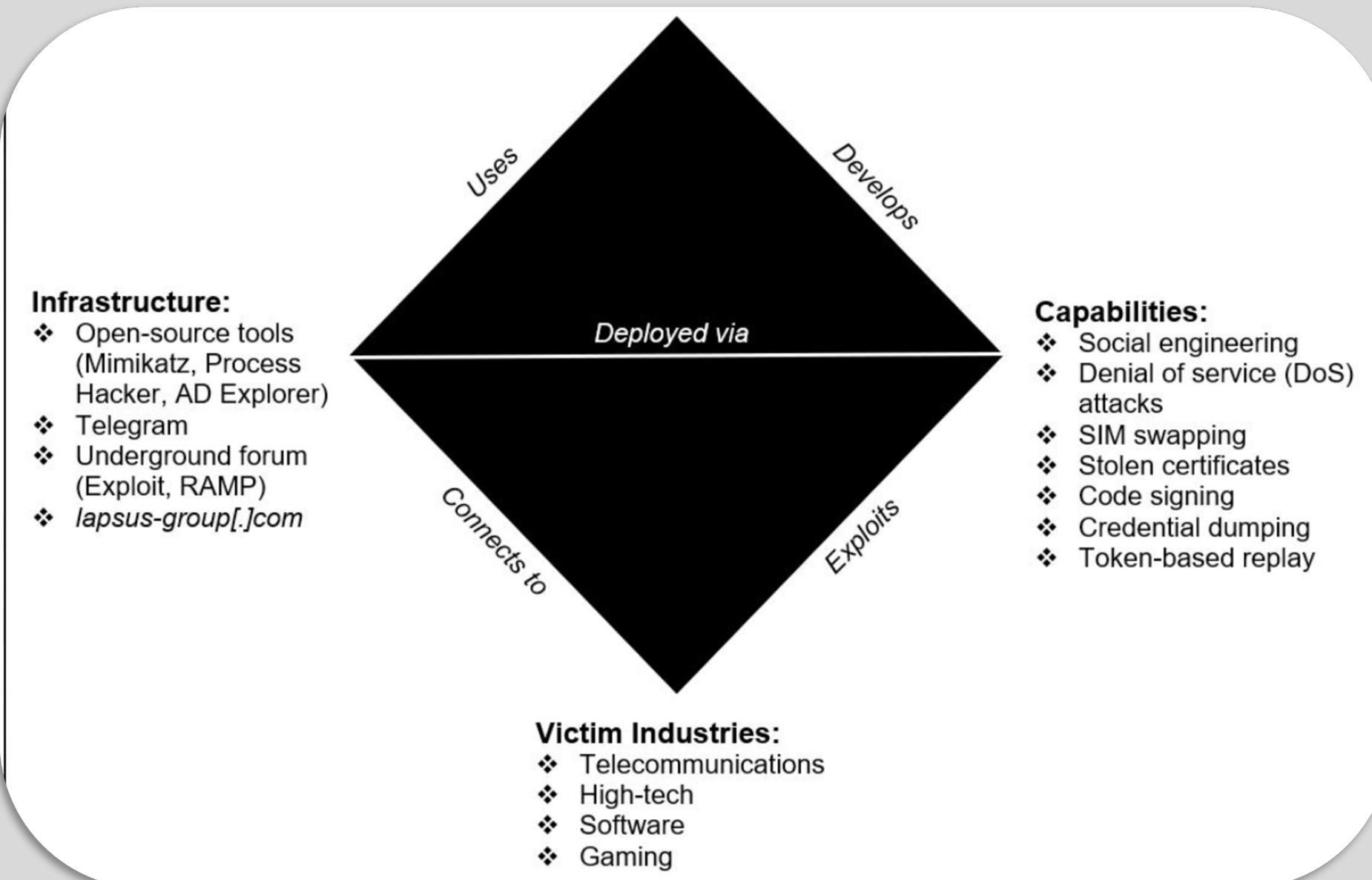
Splunk:

```
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+[^\r\n]+\\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

June 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)

THREAT INTELLIGENCE BRIEF

Anatomy of a Compromised Account

How BEC Actors Use Credential Phishing
and Exploit Compromised Accounts

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 access 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

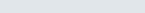
We previously [announced](#) we would begin to disable Basic Auth for five Exchange Online protocols in the second half of 2021. Due to the pandemic and the effect it has on priorities and work patterns, we are announcing some important changes to our plan to disable Basic Auth in Exchange Online. Please 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	Country	Result	Logon Error	Value Name	Value/Agent	Sparkline	First Attempt	Latest Attempt	Total Failed
IP		Status							
788	71	Failed	IdsLocked InvalidUserNameOrPassword	RequestType ResultStatusDetail UserAgent UserAuthenticationMethod	1 BAV2ROPC OAuth2:Token UserError		22/04/2021 01:49:27	23/04/2021 17:19:23	3625



END... SEE YOU AROUND...