CWL
CyberWarFare Labs

Log Correlation and Attack Mapping

About CW Labs :

CW Labs is a renowned UK based Ed-tech company specializing in cybersecurity cyber range labs. They provide on-demand educational services and recognize the need for continuous adaptation to evolving threats and client requirements. The company has these primary divisions:

1. Cyber Range Labs
2. Up-Skilling Platform
3. Infinity Learning Platform

CWL provides customized on-site training for organizations and accepts bulk orders for corporate upskilling. For inquiries or more details, feel free to reach out at **support@cyberwarfare.live.**

About Speaker

Leo Saji

(Blue Team)

Security Analyst at Cyber Warfare Labs, primarily focused on the defensive side of cybersecurity. My work involves monitoring security events, analyzing potential threats, and investigating incidents using security solution tools.

Content

01: Introduction to Security Logs

In environments, every system and security device generates logs. These logs record activities such as user authentication, network connections, process execution, and system changes.

For SOC analysts, logs are the primary source of evidence when investigating security incidents.

example:

- A **Windows server** records user login attempts.
- A **firewall** logs incoming and outgoing network connections.
- An **endpoint security tool** records suspicious processes or malware activity.

02 : What is Log Correlation

Log correlation is the process of connecting related events from different log sources to identify suspicious activity or attack behavior.

Instead of analyzing logs individually, analysts correlate events based on:

- **Time**
- **User accounts**
- **IP addresses**
- **Host systems**

This allows analysts to reconstruct the entire attack sequence.

03 : Importance of Log Correlation in SOC

Detect Multi-Stage Attacks

Attackers rarely perform a single action.
Correlation helps identify attack chains across multiple systems.

Reduce False Positives

A single event may not indicate an attack.
Correlation allows analysts to focus on suspicious patterns rather than isolated alerts.

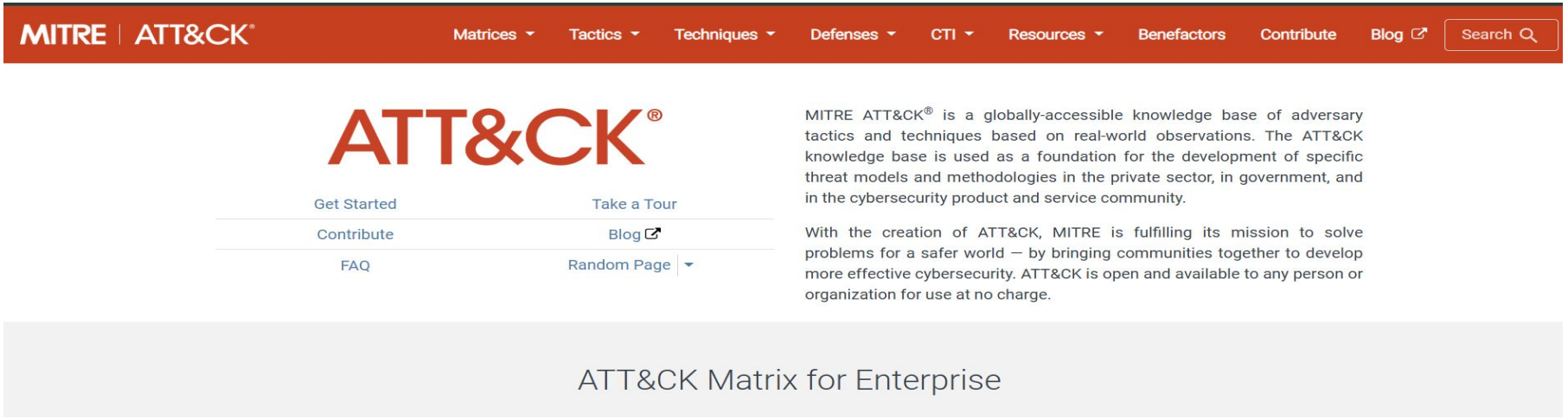
Improve Investigation Efficiency

Instead of searching multiple systems manually, correlated logs help analysts quickly reconstruct attacker activity.

04 : Mapping Attack to MITRE ATT&CK Techniques

What is MITRE ATT&CK?

MITRE ATT&CK is a globally used knowledge base of attacker behaviors and techniques based on real-world cyber attacks.



Tactics, Techniques, and Procedures (TTPs)

TTPs (Tactics, Techniques, and Procedures) describe the **behavior and methods used by attackers during cyber intrusions**.

1. Tactics – A tactic represents the attacker's objective or goal at a specific stage of the attack lifecycle.

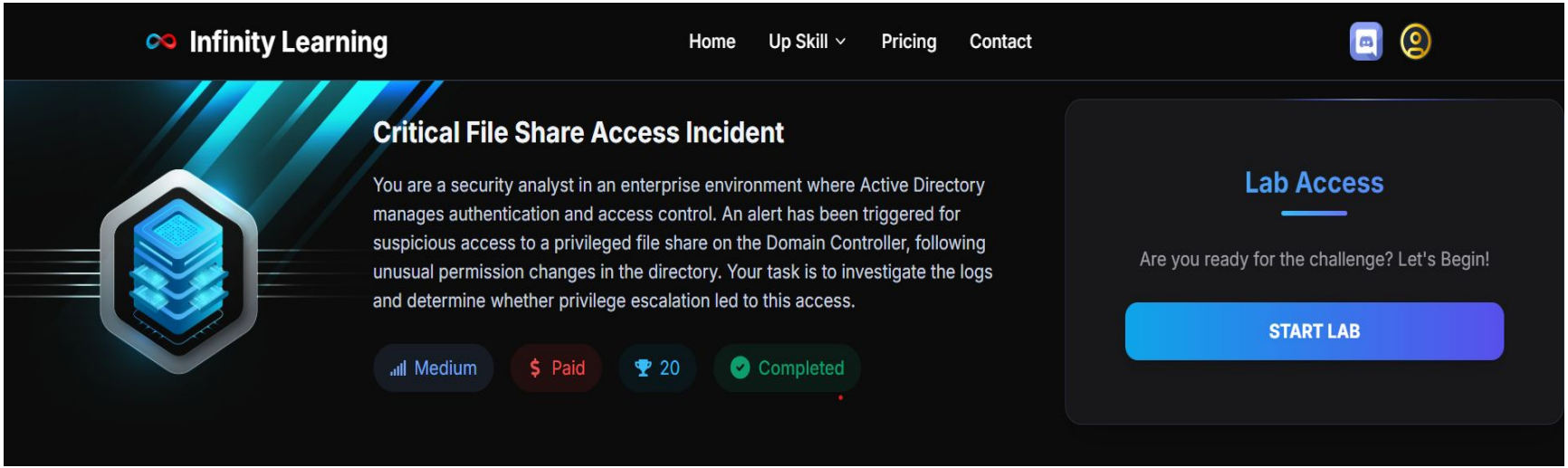
2. Techniques – A technique describes the method used by an attacker to achieve a specific tactic.

3. Procedures – A procedure refers to the specific implementation of a technique used by a threat actor.

MITRE ATT&CK®

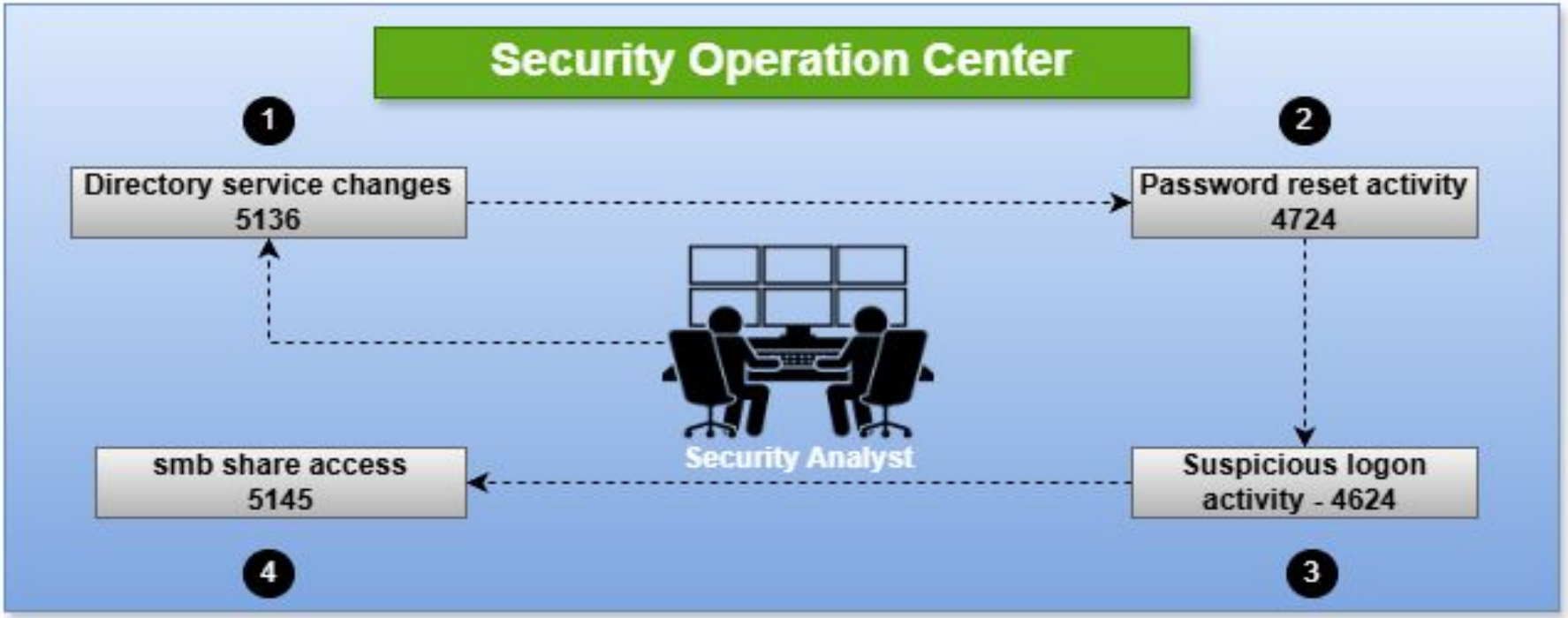
05 : Real Attack Scenario Example

Critical File Share Access Incident



Challenge Link:- [Critical File Share Access Incident]

Investigation Map



ATTACK MAPPING

#	ATTACK STEP	ACTIVITY DESCRIPTION	MITRE TECHNIQUE	SUB-TECHNIQUE	TACTIC(S)
1	Helpdesk Account Usage	Attacker authenticates using compromised helpdesk credentials to gain an initial foothold in the domain	T1078 Valid Accounts	T1078.002 Domain Accounts	Initial Access, Persistence
2	Abuse WriteOwner Permission	Attacker changes ownership of the svc_backup AD object by exploiting WriteOwner ACL rights	T1098 Account Manipulation	T1098.003 Additional Cloud / Domain Permissions (ACL Abuse)	Persistence, Priv. Escalation
3	Grant GenericAll Permission	Modify the ACL on the target account object to grant full control (GenericAll), enabling arbitrary changes	T1222 File & Directory Permissions Modification	T1222.001 Windows File and Directory Permissions Modification	Defense Evasion
4	Password Reset of svc_backup	Reset the service account password to take full control using the previously granted GenericAll permission	T1098 Account Manipulation	T1098.001 Additional Credentials	Persistence
5	Login as svc_backup	Authenticate to the domain using the newly controlled service account with elevated privileges	T1078 Valid Accounts	T1078.002 Domain Accounts	Priv. Escalation
6	Access SMB Share	Leverage the compromised service account to access internal network file shares and move laterally	T1021 Remote Services	T1021.002 SMB / Windows Admin Shares	Lateral Movement

06 : Conclusion

Modern cyber attacks rarely occur in a single step. Attackers typically perform multiple actions across different systems, making detection difficult when events are analyzed individually.

Log correlation enables security teams to connect events from different sources such as authentication logs, network logs, and endpoint activity to identify suspicious patterns and uncover the full attack sequence.

Once these events are correlated, mapping them to the MITRE ATT&CK framework provides additional context by linking observed activity to known attacker tactics and techniques. This helps analysts better understand the attacker’s behavior and the stage of the attack.

Thank You

For Professional Red Team / Blue Team / Purple Team / Cloud Cyber Range labs / Trainings

Please Contact :

support@cyberwarfare.live

To know more about our offerings, please visit: **cyberwarfare.live**