happiest minds
The Mindful IT Company
Born Digital . Born Agile

Crafting powerful SIEM Use Cases using the MITRE ATT&CK Framework

The underlying principle of Security Information and Event Management (SIEM) is implementing an effective security strategy. This can be achieved by collecting relevant data from multiple sources, detecting discrepancies in the pattern, and taking prompt action.

It is typically seen in organizations that go for SIEM tools expecting reliable security threats and preventing breaches, which is an entirely different scene.

Often SIEM (Security Information and Event Management) administrators and content developers are challenged with use case of effective building when a new client is onboarded into their system.

There are various approaches like identifying data sources, categorizing them as percriticality, capturing the correct set of logs from the assets, etc. These logs from the assets need to be correlated in the SIEM correlation engine based on the developed use cases.

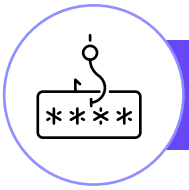
The challenge is to build an effective use case that must match the developed ones, capturing the incident and alerting on time.

Generally, from the gathered logs, important incidents like compromised user credentials, unauthorized system changes, privilege escalations, phishing, suspicious logins & data transfer, compliance violations, etc., can easily be built. The available SIEM technologies in the market, are enriched with a handful of default use cases that cover the above areas and helps to overcome the individual asset monitoring challenges.

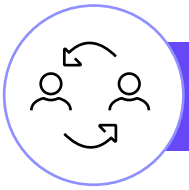
This whitepaper provides a detailed view of how to build effective SIEM use case with the MITRE ATT&CK® framework. Below are the examples of a few effective use cases covering the MITRE ATT&CK® framework to deliver contextual threat intelligence duly explained in the later part of the analysis.

Compromised Credentials

Brute Force Attacks - Password Guessing, Cracking, Spraying and Stuffing.

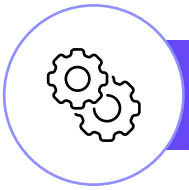


Steal or Forge Kerberos Tickets - Golden Ticket, Silver Ticket, Kerberoasting, ASREP Roasting



Alternate Authentication - Pass the Hash, Pass the Ticket

Credentials from Password Stores – keychain, security memory, a credential from web browsers, password manager



OS credential dumping – LSASS memory, security account manager, NTDS, LSA secret, cached domain credentials

It is also recommended to capture logon type 9, associated with new credentials – like Run As or mapping a network drive with alternate credentials. This logon type does not seem to show up in any events. It can clone its current token and specify new credentials for outbound connections.. The new session has the local identity but utilizes different credentials for other network connections.

Unauthorized System Changes

Appropriate rules are required to capture critical events like unauthorized changes to configurations or removal of audit trails. These changes should be alerted and escalated immediately to stop further damage and reduce risks.

Clearing up event and audit logs in Windows along with system logs in Linux and Mac, configuration change in network devices, etc. . are a few of the events for alerting unauthorized system changes.

Privilege Escalations

To build effective use cases for capturing privilege escalations, we need to have coverage in the system and root-level account monitoring. We also require local administrator accounts, user accounts with admin privileges, and specific system resources access for certain functions to perform. We can build a few separate lists based on the roles of the user's account and execute rules to alert for any alteration is done from those unauthorized privileged accounts.

Phishing

Phishing and spear phishing is an attempt to acquire confidential information from users for impersonating and committing fraud. . This encompasses attempts to acquire Personal Identifiable Information (PII) such as social security numbers, driving license details, passport details, bank account numbers and login credentials, credit card numbers, email, etc. It is critical that these data are protected across the organization. Phishing, particularly spear phishing, is often used to gain initial access within an organization when receiving a phishing email.

Use cases required to be built on the data points like who is the recipient, who clicked on the links, if any, or replied to the mail, the reputation of the sender address, validity of the link, if there is any attached file, how many received that mail, etc.

Suspicious Volume of Data Transfer

Sending or receiving suspicious amounts of data from a single user within a certain period often triggers indicators as it conflicts with the general pattern. Suppose User A has been uploading and downloading an average of 256MB of data per hour for the last three months. Suddenly, the same user increases his/her data utilization to 5MB per hour, which goes beyond the regular cycle. This should be alerted or escalated immediately to prevent the risk of data exfiltration or malware downloads.

Compliance Violations

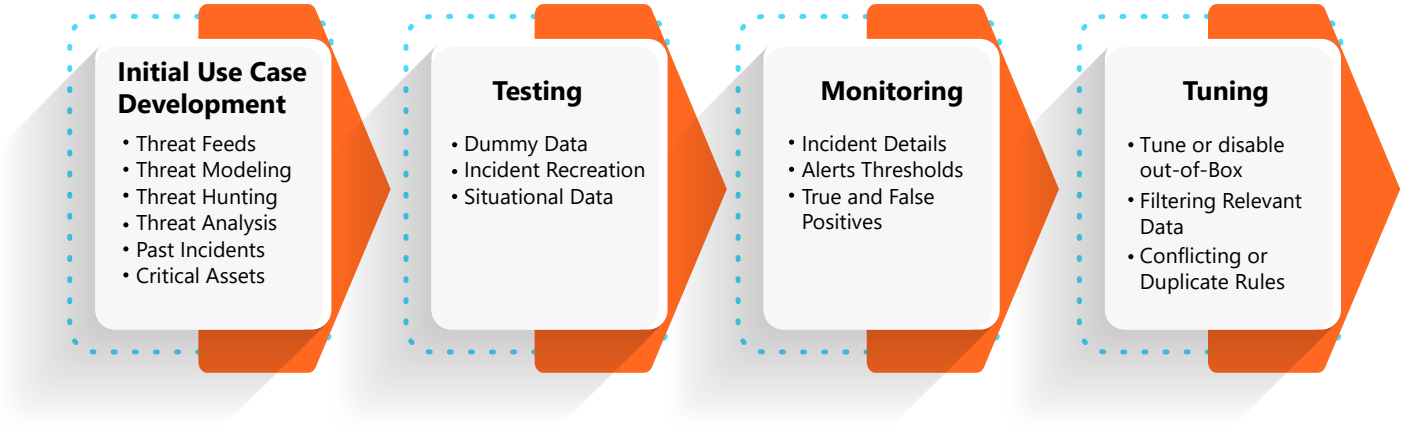
GDPR compliance is required for organizations that handle the data of the European Union (EU). Failing to comply can lead to massive fines and loss of reputation. For GDPR controls, it is critical to identify, monitor, respond to, and report. SIEM use cases facilitate organizations to meet GDPR requirements through threat detection, analysis, and compliance reporting.

A few other compliances include Health Insurance Portability and Accountability Act (HIPAA), The Payment Card Industry Data Security Standard (PCI DSS), The Federal Information Security Management Act (FISMA), Sarbanes-Oxley Act (SOX), California Consumer Privacy Act (CCPA), etc. Most SIEM technologies display default compliance rules in their products so that organizations can deploy use cases based on their requirements.

Approach

Basically, the wider log coverage we have in SIEM, the better the capturing of events, which eventually leads to better incidents, alerts, and reporting. We can follow the below steps as a starting point:

Use Case Building – Testing – Monitoring – Tuning



The initial use cases were built from the out-of-box rule sets or based on the framework or best practices. The past incidents are rolled out to the testing phase with a limited number of recipients in the content development or engineering team. Data feeds from the onboarded devices are contextualized by feeding intelligence from threat feeds, threat hunting, analysis, etc. A quick approach can be feeding dummy data for the deployed use case as an incident recreation or as situational data replication., The rule can be rolled out to production for further monitoring and alerting if the desired results are achieved.

The monitoring team then checks the context of the triggered rules and suggests further tuning if necessary. The content developer or engineering team then evaluates the triggered rules' efficiency, like how many are true & false positives, partially matched events, duplicate events, etc., and tunes the use case accordingly. The same will again go through the same process of monitoring and tuning as and when required.

Use Case Design Framework

Cyber kill chain and MITRE ATT&CK® framework are both suitable for effective design and deployment of use cases.

Mainly there are two phases in every cyber-attack. The Preliminary stage ,which is before the actual attack when the threat actor gathers intelligence and research on their targets and the Post attack phase is where the actual compromise and data breach may happen.

Phase – I Reconnaissance and **Weaponization** as in Cyber Kill Chain Framework

OR

Reconnaissance and **Resource Development** as in MITRE ATT&CK® Framework

Reconnaissance Techniques

- Active Scanning
- Gather Victim Host Information
- Gather Victim Identity Information
- Gather Victim Network Information
- Gather Victim Org Information
- Phishing for Information
- Search Closed Sources
- Search Open Technical Databases
- Search Open Websites/Domains
- Search Victim-Owned Websites

Resource Development

- Acquire Infrastructure
- Compromise Accounts
- Compromise Infrastructure
- Develop Capabilities
- Establish Accounts
- Obtain Capabilities
- Stage Capabilities

Phase – II Delivery, Exploitation, Installation, Command & Control, Action on objectives as in Cyber Kill Chain Framework

OR

Initial access, Execution, Persistence, Privilege escalation, Defense evasion, Credential access, Discovery, Lateral movement, Collection, Command & Control, Exfiltration, Impact as in MITRE ATT&CK® Framework

Please refer to **https://attack.mitre.org/matrices/enterprise/** for more details.

How to proceed with the MITRE ATT&CK® Framework

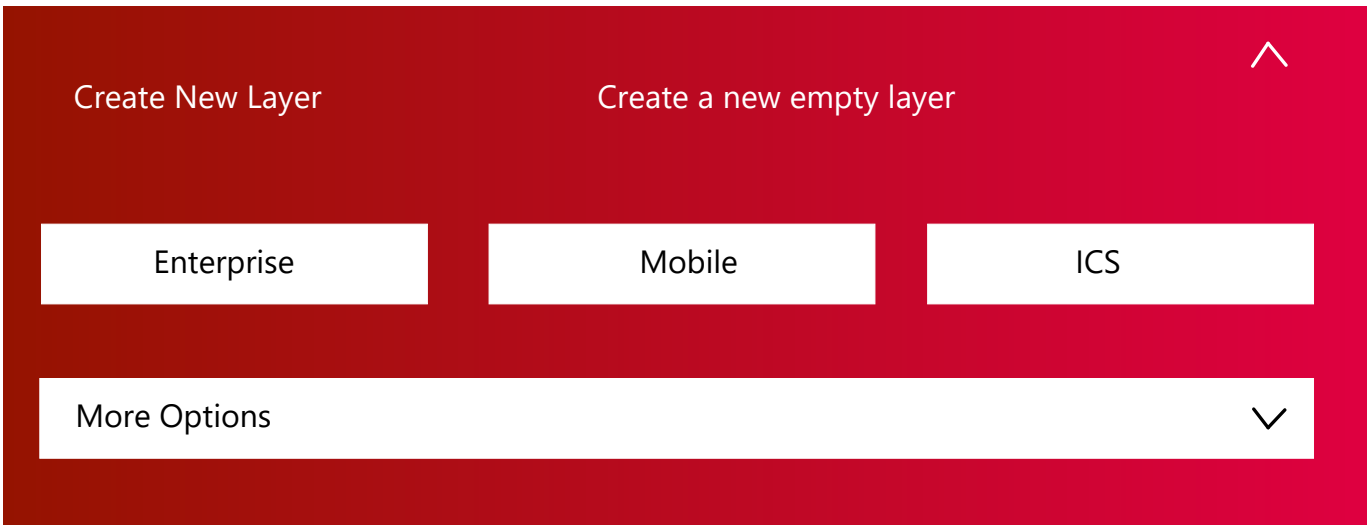
The primary focus of every security operations center (SOC) is to prepare use cases/rule sets as accurately as possible.

To achieve that, we can start with the rule list and validate the logic with already triggered incidents and the MITRE framework.

Go to https://mitre-attack.github.io/attack-navigator/ and select Create a new layer, then Enterprise.

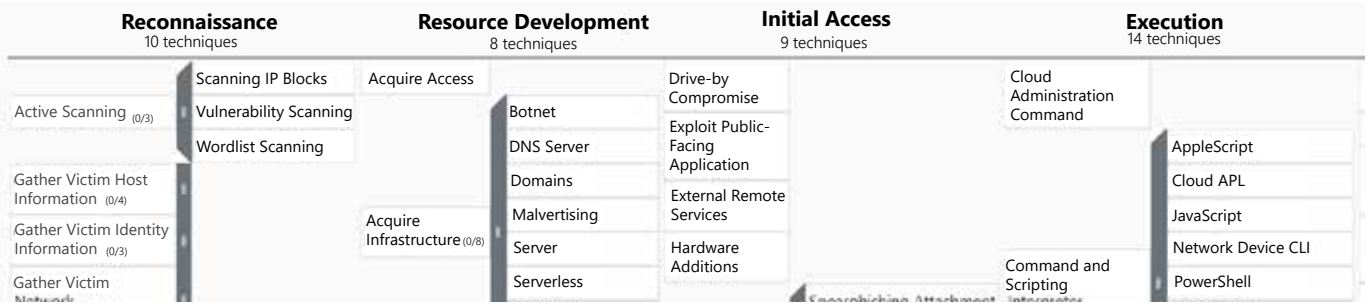
MITRE ATT&CK®Navigator

The ATT&CK Navigator is a web-based tool for annotating and exploring ATT&CK matrices. It can be used to visualize defensive coverage, red/blue team planning, the frequency of Defected techniques, and more.



It will give you a navigator panel like the one below.

Click on the vertical bars to expand each technique, giving you the details below.



You need to download it into Excel to work on that from this icon.

Let us take an example from the tactics – Defense Evasion and technique - System Binary Proxy Execution.

We will see the sub-technique Regsvr32, and the rule we will develop is Regsvr32 making outbound connections.

Hackers may manipulate Regsvr32.exe for proxy execution of malicious code. Regsvr32.exe is used to register and unregister object linking and embedding controls and DLLs on Windows systems.

Command opinions used before and after the regsvr32.exe call may also be useful in determining the origin and purpose of the script or DLL being loaded, like %regsvr32% in the command line.

Another example is the process creation like processes = filter processes where ((event_id == "1" OR event_id == "4688") AND parent_image_path == "regsvr32.exe" and exe != "regsvr32.exe*")

Another detection is like processes = filter process where ((event_id == "1" OR event_id == "4688") AND (process_path == "regsvr32.exe" and command_line == "scrobj.dll"))

So, to develop the rule, you need to find the string *regsvr32.exe* in the parent or target path or *scrobj.dll* in the command line, which can execute the COM scriptlet.

The next process is to verify whether the rule is triggering properly by running a script from the test machine and capturing the log.

Example like C:\Windows\System32>regsvr32 DLL name to be executed for generating the log and testing the rule.

Warning: Do not use these in production systems. Always use a test environment.

After, successful testing, you can mark the sub-technique as green. Likewise, you need to start making other rules and verify the existing rules' logic explained in the framework.

Conclusion

Organizations can use advanced threat intelligence solutions that support mapping to MITRE ATT&CK® to increase and streamline cyber threat intelligence data and more accurate incident detection. In this context, a complete profiling of the threat actors, malware, tactics, techniques, and sub-techniques should be made and reviewed with multiple test data. Also, technologies that automate this process should be incorporated after the evaluation process.

Author Bio

Samit Chowdhury
Senior Project Manager, Cyber Security

Samit Chowdhury has over 15 years of experience in cybersecurity. Currently, he is engaged in handling multiple SOC projects in Happiest Minds including Cyber Risk Protection Platform – a new and enhanced SOC platform to help clients fight against bad actors. He works in various security chapters and has made significant contributions to designing security solutions and mentoring blue teams.

About Happiest Minds

Happiest Minds Technologies Limited (NSE: HAPPSTMNDS), a Mindful IT Company, enables digital transformation for enterprises and technology providers by delivering seamless customer experiences, business efficiency and actionable insights. We do this by leveraging a spectrum of disruptive technologies such as: artificial intelligence, blockchain, cloud, digital process automation, internet of things, robotics/drones, security, virtual/ augmented reality,etc. Positioned as 'Born Digital . Born Agile', our capabilities span Product & Digital Engineering Services (PDES), Generative AI Business Services (GBS) and Infrastructure Management & Security Services (IMSS). We deliver these services across industry sectors such as automotive, BFSI, consumer packaged goods, e-commerce, EdTech, engineering R&D, healthcare, hi-tech, manufacturing, retail, and travel/transportation/hospitality. The company has been recognized for its excellence in Corporate Governance practices by Golden Peacock and ICSI. A Great Place to Work Certified™ company, Happiest Minds is headquartered in Bangalore, India with operations in the U.S., UK, Canada, Australia, and Middle East.

www.happiestminds.com

Write to us at

business@happiestminds.com