ManageEngine
Log360

How to implement the MITRE ATT&CK framework using Log360

How to implement the MITRE ATT&CK framework using Log360 - Blueprint

The MITRE ATT&CK framework helps IT security teams boost the efficacy of security mechanisms to match recent sophisticated security threats. The adoption of this framework in IT security teams' cybersecurity plans is the result of organizations widening their security capabilities to not only accommodate preventive technologies but also early detection and effective incident response. The analytics-driven security approach is what helps organizations understand the specific tactics and techniques used by threat actors while carrying out cyberattacks.

What is MITRE ATT&CK?

MITRE ATT&CK (adversarial tactics, techniques, and common knowledge) is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations of cybersecurity threats.

Oddly resembling the periodic table, the ATT&CK Enterprise Matrix is arranged according to attack stages and focuses on adversarial behavior in Windows, Mac, Linux, and cloud environments. From the point of reconnaissance and initial system access to data theft or machine control, each stage includes several tactics and techniques that are commonly used by threat actors.

Tactics

As opposed to looking at indicators of compromise after an attack, security analysts can look in to the tactics that indicate an attack is in progress. These are the basic, short-term, tactical goals of a threat actor during an attack. Tactics denote the why of an attack technique.

Techniques

Similarly, techniques denote how the threat actor achieves a particular tactical goal by performing an action.

Common knowledge

Common knowledge is the documentation of various procedures used by threat actors in their tactics and techniques. Since, this is based on real-life examples, the framework serves as a go-to threat discovery and mitigation database.

Automate threat detection using Log360

Log360 incorporates the MITRE ATT&CK framework with its attack detection capabilities and enables the security operations centers to spot security threats accurately and immediately. Here are some examples.

Spot privilege escalation attempts

Attackers use process injection techniques where they inject code into processes in order to evade process-based defenses and potentially elevate privileges. Malware used since 2010 called Taidoor can perform DLL loading. Log360 detects suspicious activities like the Taidoor RAT DLL load and alerts the IT admins quickly. Log360 also detects suspicious Svchost activity such as attackers injecting shellcode into svchost.exe.

Never miss a single step

Attackers try to hide their tracks while carrying out their attacks. With the indicator removal on host technique, they may delete or alter generated artifacts on a host system, including logs. Log360 detects suspicious activities like cleared event logs or configurations using Webtulil. This helps to bring activities of intrusion to light and also gives way for better forensic analysis and incident response.

Sniff out suspicious activity

Attackers sift through network traffic to capture critical information including authentication material passed over the network. Log360 spots suspicious activities such as harvesting of Wi-Fi credentials or capturing a network trace using netsh.exe. This can prevent attackers from using data like user credentials to further their lateral movement and defense evasion activities.

Inside the Enterprise Matrix

The framework categorizes each tactic under various security attributes such as security engineering, intrusion detection, threat hunting, threat intelligence, red teaming, and risk management.

Reconnaissance (TA0043)

In this attack stage, the threat actor tries to gather information they can use to plan future operations. Techniques like vulnerability scanning allow them to gain critical information about their victims such as the organization, infrastructure, or staff.

Resource development (TA0042)

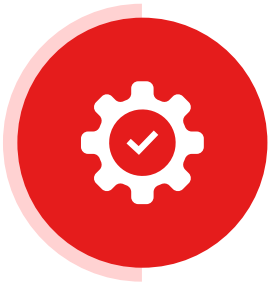
In this attack stage, the threat actor tries to establish resources they can use to support further operations. Techniques like compromising accounts and infrastructure lead them to create, purchase, or steal resources that can be used to support targeting.

Initial access (TA0001)

In this attack stage, the threat actor tries to gain their initial foothold within a network. Techniques like phishing enable attackers to gain access to the network and also allow continued access.

Execution (TA0002)

In this attack stage, the threat actor tries to run malicious code on network systems. Techniques like abusing PowerShell commands and scripts combined with techniques from other tactics allows attackers to explore a network and steal data.



Persistence (TA0003)

In this attack stage, the threat actor tries to maintain their foothold in the victim's network. Techniques like account manipulation enable the attackers to maintain access to victim systems.

Privilege escalation (TA0004)

In this attack stage, the threat actor tries to gain higher-level permissions by exploiting system weaknesses, misconfigurations, and vulnerabilities. Techniques like access token manipulation enable the attackers to gain permissions on a system or network.

Defense evasion (TA0005)

In this attack stage, the threat actor tries to avoid being detected in the network. Techniques like domain policy modification (modifying configuration settings of a domain to evade defenses) allow attackers to hide and avoid detection.

Credential access (TA0006)

In this attack stage, the threat actor tries to steal account names and passwords. Brute-force techniques like credential stuffing allows attackers to obtain legitimate credentials. Other techniques like stealing or forging Kerberos tickets and sub-techniques like golden ticket, silver ticket, and kerberoasting also allow them to steal credentials.

Discovery (TA0007)

In this attack stage, the threat actor tries to gain knowledge about their victim's environment. Techniques like file and directory discovery to obtain information in a certain file system allow attackers to gain knowledge about the system and internal network.

Lateral movement (TA0008)

In this attack stage, the threat actor tries to move through the network. Techniques like exploitation of remote services in which the attacker exploits remote services to gain unauthorized access to internal systems once inside the network allow the attacker to move laterally within an environment and bypass normal system access controls.

Collection (TA0009)

In this attack stage, the threat actor tries to gather data that could benefit their goal. Techniques like finding local system data and finding data from removable media like USB memory allows attackers to collect targeted data. Subsequently, the next goal is to exfiltrate the data.

Command and control (TA0011)

In this attack stage, the threat actor tries to communicate with compromised systems to control them. Using remote access software like Team Viewer and Go2Assist enable attackers to communicate with systems under their control within a victim network.

Exfiltration (TA0010)

In this attack stage, the threat actor tries to steal data. Techniques like automated exfiltration and data transfer size limits, where the attacker exfiltrates data in fixed size chunks instead of whole files to avoid detection while removing it, are used to extract data out of the target network.

Impact (TA0040)

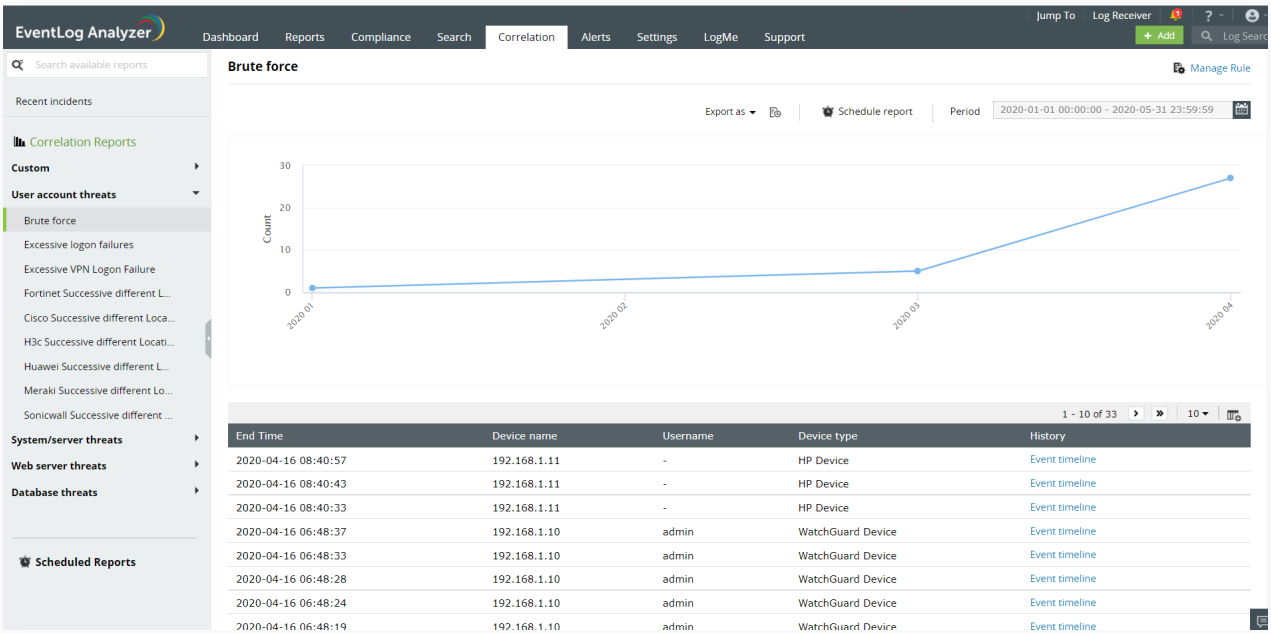
In this attack stage, the threat actor tries to move through the network. Techniques like exploitation of remote services in which the attacker exploits remote services to gain unauthorized access to internal systems once inside the network allow the attacker to move laterally within an environment and bypass normal system access controls.

Log360's ATT&CK module

By implementing MITRE ATT&CK with a security information and event management (SIEM) solution, organizations can not only improve their incident detection capabilities but also develop a more effective cybersecurity strategy.

- **Correlation for ATT&CK techniques:** Log360 provides out-of-the-box correlation rules for every technique. This not only helps detect security threats as soon as they occur but also provides a detailed event timeline with all the related security events. The timeline of the incident contains crucial information such as the source, time of the event, device type, severity and much more.

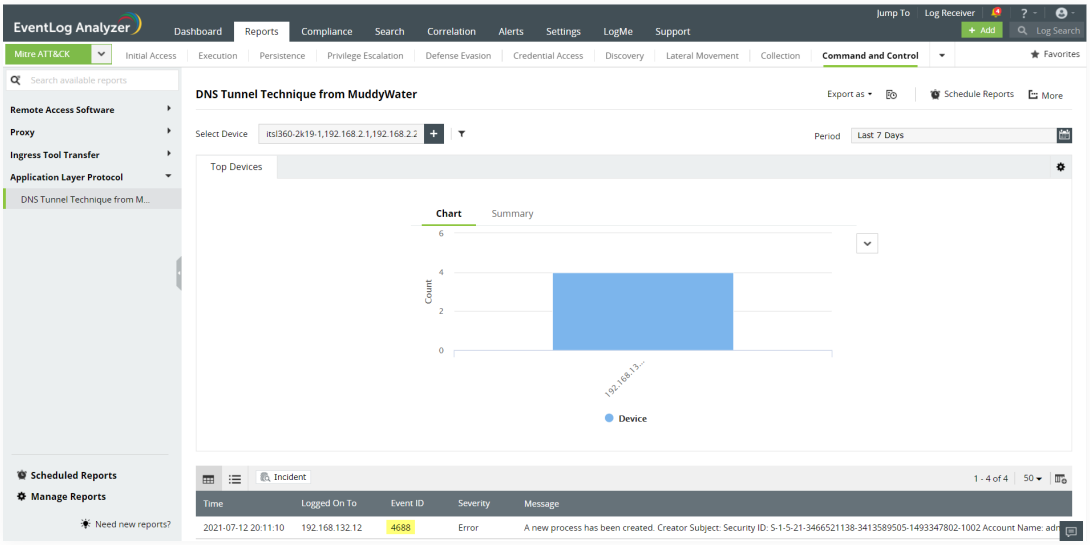
  For example, attackers may use brute-force techniques to gain access to accounts when passwords are unknown or when password hashes are obtained. Log360's correlation rule detects the brute-force security threat and provides a complete timeline of events.



IT security teams can also combine the different actions to form an attack pattern.

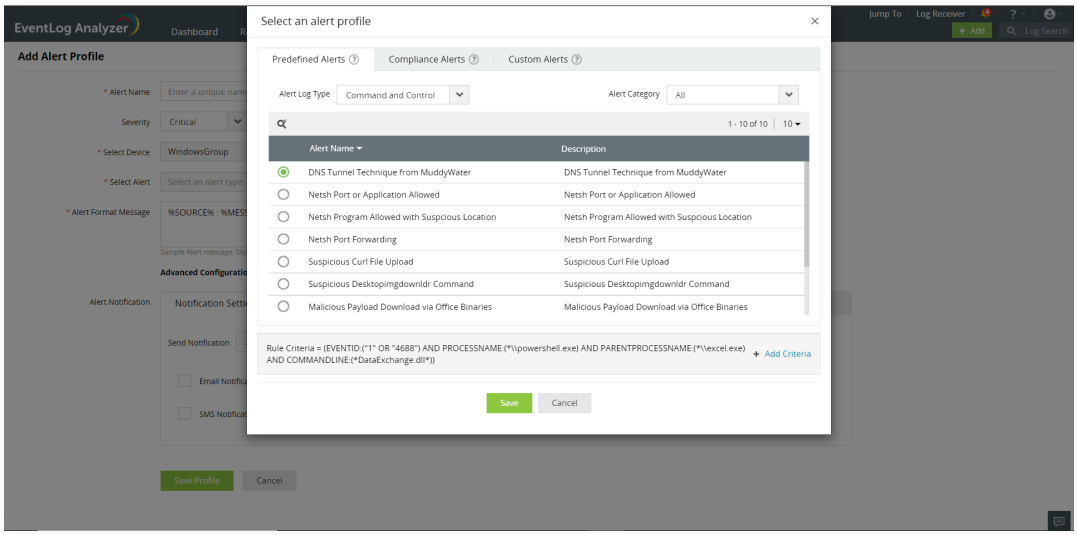
- **Security analytics dashboard:** Log360 provides holistic visibility into the 12 ATT&CK tactics and their corresponding techniques through the security analytics dashboard. Each of these techniques is complete with all the related security events and a corresponding, exhaustive list of crucial details like the time of the event, the source, the event ID, the severity, and much more.

For example, attackers may communicate using the Domain Name System (DNS) application layer protocol to avoid detection and network filtering by blending in with existing traffic, as seen in the command and control tactic. Log360 not only detects this security threat, but also provides a thorough view of exactly what happened during the event and how it happened. IT teams can then use this information to conduct an extensive incident investigation.



IT security teams can also add similar, suspicious events to an incident from here and speed up the incident resolution process.

- **Alert profiles:** To expedite incident resolution, Log360 allows security teams to create alert profiles for MITRE-ATT&CK-related security events. The solution then starts generating alerts as soon as it detects the particular security event. For example, every time Log360 detects a DNS tunnel technique attempt, it will immediately alert the security teams who can then further investigate the event.



The IT security teams can then quickly assign a technician to resolve the potential security threat.

How do organizations benefit from the ATT&CK framework implementation with Log360?

- The solution helps detect each technique accurately as it's mapped to the correlation module. Log360's correlation engine discovers sequences of events from across the network that indicate possible attacks, and quickly triggers alerts for the threat.

- Log360 helps expedite effective threat resolution, as the attack detection module is integrated with the incident management framework.

- Log360's incident workflows can be automated to mitigate security threats, thereby stopping attackers in their tracks and preventing a potential cyberattack.