ManageEngine
Log360

USE CASE

Detecting APTs using MITRE ATT&CK TTPs

As cyberattackers are constantly improving their sophisticated techniques, combating advanced persistent threats (APTs) requires the combined capabilities of a security solution and a frequently updated threat intelligence database. The cyber kill chain is built on the notion that cyberattackers carry out an attack in stages. The tactics and techniques used by attackers in these stages are curated in the form of a knowledge base called ATT&CK, short for adversarial tactics, techniques, and common knowledge.

This framework, which is based on real world examples, not only helps organizations detect security threats, but also ensures that they identify loopholes in their defenses and create a more resilient cybersecurity strategy. According to ATT&CK data, cyberattackers use tactics, techniques, and procedures (TTPs) to achieve their mission, with tactics being the highest level of attack behavior. Some of the tactics that are used to exploit an organization's network include initial access, execution, persistence, privilege escalation, credential access, collection, and exfiltration. Attackers utilize around 260 different techniques to carry out these tactics.

Let's see how Log360 incorporates MITRE ATT&CK tactics and techniques to detect APTs.

Mitigating pass-the-hash attacks using Log360

A pass-the-hash attack is a technique where the cyberattacker captures a password hash as opposed to the user's cleartext password. The attacker reuses the stolen hashed user credential to pass it through for NTLM authentication. The technique is mostly used to move laterally within a network to obtain sensitive data and other assets.

In this case, consider an attacker who compromises a low-level employee account. Once the attacker is successfully inside the network, they leverage other vulnerabilities to switch accounts, machines, and IP addresses. Once the attacker manages to secure administrative privileges, they are free to carry out their objective, like gaining access to the organization's sensitive resources.

How Log360 helps

Since lateral movement is achieved through multiple steps, the related events are scattered throughout the network, taking place in different machines, using different credentials, and with different IP addresses. At first glance, these events may seem unrelated and completely normal. However, the sequence of the occurrences indicates malicious intentions. Log360 is a security information and event management solution that analyzes log data in real time from multiple sources in an environment.

Log360 can detect pass-the-hash attacks by auditing all logons and credential use and inspecting them for any inconsistencies. Unusual remote logins correlating with writing and executing binaries are events that indicate suspicious activity. For example, a successful logon attempt would trigger an event ID 4624 (Logon Type 3, NTLM). This event followed by event ID 4768, which is generated when a Kerberos authentication ticket is requested, and event ID 4769, when a Kerberos service ticket is requested, indicates a potential pass-the-hash attempt.

Through Log360's real-time monitoring feature, IT admins can monitor these events to detect abnormal and potentially malicious activity and prevent privilege abuse. Once these events are correlated and signal suspicious activity, the solution detects a possible pass-the-hash attack attempt immediately and alerts the IT administrator to the detected threat via email or SMS. The administrator can then quickly investigate the threat.

Log360's correlation engine provides an attack timeline for each detected security incident that allows the administrator to investigate the event details thoroughly, including details like the changes that were made, who made them, when they were made, how often, and how they were made.

By discovering the event's origin and cause, IT admins can quickly respond to the incident. With the help of Log360's incident management system, the detected incident can be assigned a workflow where the compromised user account will be immediately disabled, minimizing the damage. The IT admin can also reset the password for the compromised user, which causes the stolen password hash to become invalid.

By leveraging MITRE ATT&CK tactics and techniques, Log360 enables IT teams to improve incident detection, investigation, and response to advanced persistent threats.

Gartner's Peer Insights Voice of the Customer 2023 is out!

ManageEngine named a Customers' Choice for SIEM

Check out why

Latest Gartner Magic Quadrant for SIEM is out!

ManageEngine recognized in Gartner's Magic Quadrant for Security Information and Event Management, 2024.

Get the report

ManageEngine Log360, an integrated solution that combines ADAudit Plus and EventLog Analyzer into a single console, is a one-stop solution for all log management and network security challenges. This solution offers real-time log collection, analysis, monitoring, correlation, and archiving capabilities that help protect confidential data, thwart internal security threats, and combat external attacks. Log360 comes with over 1,200 predefined reports and alert criteria to help enterprises meet their most pressing security, auditing, and compliance demands. For more information about Log360, visit manageengine.com/log-management.

ManageEngine Log360

$ Get Quote

Download