

USE CASE

Using Log360 to spot privilege escalations

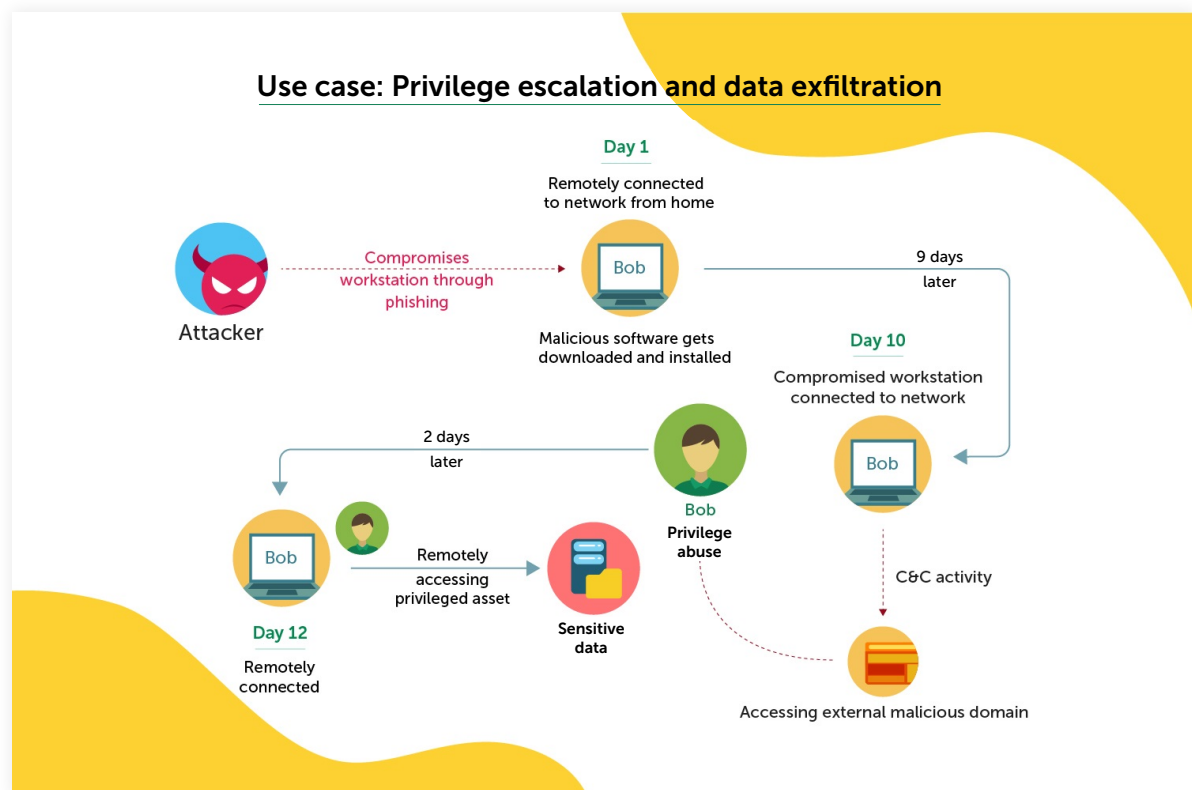


Using Log360 to spot privilege escalations

Privilege escalation attacks are aimed at gaining access to your network's most sensitive resources. Attackers exploit vulnerabilities such as bugs, application configuration errors, and unpatched operating systems to compromise a user account and elevate the user account's privileges. They may do this several times, until they have enough privileges to carry out an attack, steal confidential data, deploy malware, create back doors, or carry out whatever other objective they have.

Detecting an attempted or even a successful privilege escalation gives you a better chance at preventing intruders from gaining the power they need to carry out their main attack. So how do you ensure your organization can successfully spot privilege escalations?

How Log360 helps



ManageEngine Log360, a simple to use SIEM solution, has a multifaceted approach to spotting privilege escalations. With capabilities such as extensive auditing, reporting and alerting, threat intelligence, correlation and behavior analytics, here's how you can leverage Log360 to detect and prevent privilege escalations.

Monitor user account changes in real time:

To spot privilege escalations successfully, you need to ensure you have visibility on user actions in your network. Log360 provides multiple security dashboards to track user activity in real time. With complete user audit trails and an alerting console, you'll can be notified of anything from user logons and logoffs to user group and account changes.

Detect and remediate suspicious installations:

Log360 has a robust, rule-based correlation engine that can spot patterns in your incoming log data. With a slew of built-in rules and a custom rule builder, you can detect suspicious software installations, services, malware, and more in your workstation devices.

Spot malicious command and control (C&C) server activity in real time:

Log360's built-in, self-updating STIX/TAXII feeds processor ensures you have ample threat intelligence to detect intruders in your network. Log360 then correlates threat feeds with network log data and notifies you of access attempts from malicious domains, URLs, and IP addresses, which can occur during privilege escalation attacks.

Detect privilege escalation attacks with behavioral analytics:

Attackers ensure that they remain inconspicuous when carrying out privilege escalation attacks, making it difficult to detect them. Log360's User Entity Behavior Analytics (UEBA) add on identifies any actions unusual to a specific user, such as remote logons during odd hours and access to multiple sensitive files. Log360 then proceeds to increase the user's risk score and notifies the security admin in real time.

Automate workflows to reduce response time:

Log360's automated incident response system has workflows to perform specific actions such as killing a process, blocking a USB, and more as soon as correlation alerts are triggered. This is one of the quickest ways to stop malicious activities such as illicit software installations, as and when they happen in your network. You can carry out further investigation with detailed, out-of-the-box correlation reports.

Equip your organization with Log360 to spot and prevent privilege escalations.

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, a comprehensive SIEM solution, helps enterprises thwart attacks, monitor security events, and comply with regulatory mandates.

Log360 bundles a log management component for better visibility into network activity and an incident management module that helps quickly detect, analyze, prioritize, and resolve security incidents. Log360 also offers an innovative ML-driven user and entity behavior analytics add-on that baselines normal user behaviors and detects anomalous user activities, as well as a threat intelligence platform that brings in dynamic threat feeds for security monitoring. Log360 helps ensure organizations combat and proactively mitigate internal and external security attacks with effective log management and in-depth AD auditing.

For more information about Log360, visit our website.

ManageEngine
Log360[\\$ Get Quote](#)[↓ Download](#)