ManageEngine
Log360

USE CASE

Detecting anomalous user behavior using risk assessment

Detecting anomalous user behavior using risk assessment

A user's activities don't seem quite right. You then find out that the user has more privileges than they require. Was it an oversight? An escalation of privilege? Or was it a case of account compromise? Is it possible to quantify the security risk your organization is exposed to? Seemingly minor anomalies could indicate an advanced persistent threat (APT). Once attackers infiltrate your network, they can slowly weaken your defenses from the inside and cause serious damage. Incorporating risk assessment with attack detection can help you uncover APTs.

Consider this scenario. Jane from Marketing logs on at a very odd hour and installs multiple applications in one go. She then views sensitive customer data and copies several files that she has never accessed before. Finally, she initiates a connection with a suspicious domain and begins transferring files rapidly. This is how an advanced attack involving an insider might play out.

On the other hand, an external attacker could compromise the network by using phishing links or social engineering tactics and stay in the network for an extended period. Once installed, malware is difficult to spot, as it is optimized to avoid detection. One way of discovering an APT is to detect anomalies in behavior and continually assess the risk posed by each anomalous action.

How Log360 can help

Detecting APTs with machine learning and threat intelligence

Log360's User and Entity Behavior Analytics module uses machine learning to detect anomalies in user behavior. If an action or a series of unusual actions are detected, a risk score will be added in each case. The moment multiple applications are installed on Jane's computer, a count anomaly will be triggered and a risk score will be added. Further, the logon at an unusual time will be logged as a time anomaly. Besides spotting anomalies in behavioral patterns, the threat intelligence module will raise an alert the moment Jane's computer connects to a suspicious domain. Log360 integrates with globally reputed threat feeds and alerts you when a suspicious domain or IP intrudes into your network. With these built-in tools, Log360 can help detect an advanced attack at multiple stages even if it initially evades detection.

Preempting attack scenarios

Besides spotting anomalies in user behavior, Log360 also offers risk scores to point you towards specific attack scenarios such as insider attacks, data exfiltration, or account compromise. For instance, a user who has copied an unusually high volume of files will be classified as “high risk for data exfiltration” and “not so high risk for account compromise.” Since the user is already present in the network and no other behavioral anomaly has been detected, you may have an insider threat on your hands. You can then proceed to place the user under a watch list to alert you of any further suspicious activities they might perform so you can investigate right away.

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, 2020.

Get the report

About Log360

Log360 is a unified SIEM solution with integrated DLP and CASB capabilities that detects, prioritizes, investigates and responds to security threats. Vigil IQ, the solution's TDIR module, combines threat intelligence, ML-based anomaly detection and rule-based attack detection techniques to detect sophisticated attacks, and it offers an incident management console for effectively remediating detected threats. Log360 provides holistic security visibility across on-premises, cloud and hybrid networks with its intuitive and advanced security analytics and monitoring capabilities.

For more information about Log360, visit manageengine.com/log-management/ and follow the LinkedIn page for regular updates.

ManageEngine Log360

$ Get Quote

Download