ManageEngine
Log360

DATASHEET

Incident management in Log360

A security incident is a single or series of unwanted or unexpected cyber security events that are likely to compromise an organization's cybersecurity and disrupt its regular operations. Cybersecurity incident management is a complete security process built for preparing, detecting, reporting, assessing, responding to, dealing with, and learning from cybersecurity incidents that occur in the organization's environment.

Log360, ManageEngine's SIEM solution, provides a reliable end-to-end incident management system that helps organizations manage security incidents in an efficient and time-saving manner. Using various techniques and mechanisms, Log360's incident management system reduces the mean time to detect (MTTD) and mean time to resolve (MTTR) an incident. To effectively do this, Log360 leverages actionable intelligence.

Incident detection

It's critical to detect a security incident as soon as it occurs, so you can mitigate the threat immediately, and contain or reduce the impact of a cyberattack. Log360 helps detect security incidents and data breaches that pose a challenge for your organization using a number of mechanisms.

• Real-time event correlation engine

Log360 analyzes your network logs to string clues together and identify indicators of an attack. Although an individual event may not indicate a security threat, correlating it with a sequence of related events could say otherwise. Log360 comes with over 30 prebuilt correlation rules to detect several common attacks. The following is an example of a correlation rule that highlights an attack pattern.

"A rule that detects multiple VPN logon failures followed by a successful VPN logon and an immediate remote login in a Windows device, after which suspicious software is installed."

When it comes to cybersecurity, there is no one-size-fits-all solution. This is why Log360 enables you to customize existing attack rules or build new ones from scratch with the flexible rule builder interface to suit your organization's needs. For more in-depth information on critical security incidents like compromised accounts, infected devices, and more, Log360 provides an attack timeline containing the time, source, and activity for each detected incident.

• User and entity behavior analytics (UEBA)

An organization's log data contains deep insights into user behavior. This includes a user's login and logout times, their user privileges, accessible data, and much more. Log360 leverages this information and builds a standard baseline of behavior for each user and entity in the network. When there is a deviation to this accepted behavior, the solution marks it as an anomalous activity. The solution then assigns risk scores to this activity based on its deviation from the standard baseline.

This helps security admins prioritize investigation and response of high-risk incidents. Log360 UEBA uses machine learning to detect behavior anomalies and strengthens your defenses against insider threats, account compromise, and data exfiltration.

• Threat intelligence

Threat intelligence employs threat feeds to identify incidents. Log360's threat intelligence module leverages threat data from various sources like STIX/TAXII-based threat feeds that provide the latest and most reliable threat information available to help mitigate cyberthreats. This information includes blacklisted IP addresses, URLs, and domains that are known to be malicious. With a regularly updated threat database, Log360 is able to detect evolved security incidents in your network instantly.

Incident response

To maintain your organization's cybersecurity posture, it's important to respond to security threats quickly and effectively. Log360 enables you to do this with an efficient incident response system in place.

Incident workflow

With Log360, you can utilize an automated response system that defines a set of actions when triggered by a particular incident. For example, you can block the USB port on a potentially compromised device and email the status to a security admin right away. Responding to this incident can mitigate data exfiltration attempts.

By configuring automated workflows, organizations can get a head start when it comes to incident resolution, saving time and effort. Apart from triggering actions, you can also raise a ticket for every incident detected in your Information Technology Infrastructure Library (ITIL) tool using workflow management. This not only helps in closely tracking the incident resolution process, but also ensures accountability when it comes to dealing with security incidents.

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