ManageEngine
Log360

USE CASE

Identifying a patient-zero machine using Log360

Identifying a patient-zero machine using Log360

In medical terms, patient zero refers to the first person to be infected with a new virus or bacteria. This term has made its way to the IT security world, where it's associated with the first machine to be infected with a new strain of malware or the first account to undergo a phishing scam.

In medical terms, patient zero will infect others who come in to contact with them. If uncontained, the illness will spread quickly and widely until medical experts discover a cure to eliminate the disease or effective medication to combat it. The same truth holds for IT security. It may take days, weeks, or even months after the initial patient-zero machine is infected and effectively mitigated. It's during this period when other devices on the network can fall victim to the attack. This is why detecting the patient-zero machine is of paramount importance.

With today's state-of-the-art IT management solutions, organizations can effortlessly identify such patient-zero machines and effectively mitigate the threat. Log360 is a comprehensive log management solution that provides various capabilities to identify patient-zero machines and successfully eliminate the threat they pose. Let's see how.

Machine-learning-based behavioral analytics to identify patient-zero machines: Log360 UEBA add-on

Traditional rule-based detection methods help in identifying patient-zero machines, however it's not always accurate. Using machine-learning-based behavioral analytics helps you accurately narrow down the patient-zero machine by detecting anomalous behaviors that are otherwise difficult to spot.

The Log360 UEBA add-on comes with prebuilt anomaly detection rules that help accurately spot patient-zero machines. You can identify several indicators of compromise (IoCs) and indicators of attack (IoAs) before they manifest into a cyberattack. Log360 helps you achieves this by monitoring the following indicators of insider threats:

- Unusual login times
- Logins from new or unusual systems
- Excessive authentication failures
- Unusual file accesses and modifications
- Privilege escalation and permission changes
- Unusual data transfers

Combining the capabilities of a threat intelligence platform and real-time correlation engine to spot patient-zero machines

One of the main indicators to identify a patient-zero machine is its communication with malicious sources. Log360 helps spot this indicator by combining its threat intelligence and correlation capabilities.

The threat intelligence platform of Log360 comes with built-in threat feed information that holds over 600 million malicious IP addresses and domains. You can gain even deeper insights into these malicious entities with the advanced threat analytics add-on. Log360's real-time correlation engine can check the network traffic logs for any of these malicious sources, and if there's a communication attempt from any blacklisted entities, the solution alerts you in real time. You can also configure your workflow profile to block this malicious traffic automatically.

The incident timeline report provides you with detailed information on which system in your network tried to contact a malicious source, when, and what it tried to communicate. This helps you effectively spot patient-zero machines in real time.

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/logmanagement/ and follow the LinkedIn page for regular updates.