ManageEngine
Log360

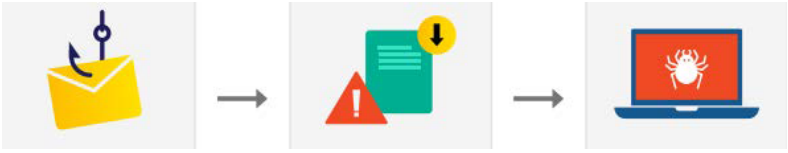
USE CASE

Using Log360 to detect intrusions

Using Log360 to detect intrusions

Can my network hold out against near constant infiltration attempts? This question is sure to be top of mind for every security administrator. In the present threat landscape, it is only a matter of time until a hacker makes an infiltration attempt. Malicious actors employ sophisticated social engineering and spear phishing techniques to trick users into taking their bait. Once compromised, these infected systems can be controlled by hackers through remote access. It is therefore essential to detect compromised systems within the organization besides external threats.

How Log360 can help

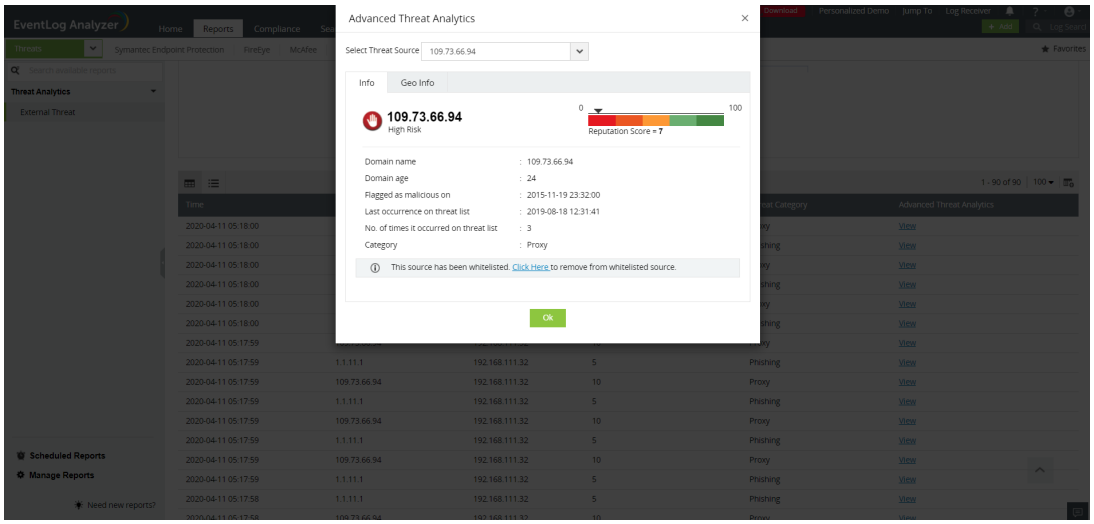


Phishing attack > Malicious file download > System compromise

Detecting and mitigating external intrusions

- Log360 aggregates data from IDS and IPS devices, firewalls, and Active Directory infrastructure, and alerts you of any possible intrusion attempt in real time.
- Once an intrusion is detected, you can investigate it further based on the source, destination, and severity.
- Besides detection and analysis, you can automate your response to these events with workflows that can minimize critical response time during an attack.

Log360's threat intelligence module



Using threat intelligence to detect compromised systems within the network

- When a system is compromised, it often comes under the control of an external command-and-control server. If a system compromise goes undetected at its onset, another opportunity to spot it is when the infected system attempts to communicate with the external server.
- By corroborating data from reputed threat feeds, Log360 alerts you when a system attempts to communicate with a malicious source.
- Once a malicious source is flagged, the system can give you details such as the reputation score, age, and geolocation of the domain to aid your analysis.

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.