ManageEngine
Log360

CASE STUDY

# Panther Systems leverages ManageEngine Log360's real-time correlation engine to thwart security attacks

The Advanced Threat Analytics add-on helps the company have the right mix of proactive and reactive security strategies

## About Panther Systems

Panther Systems, Inc. is a software provider for the world's pulp, paper, tissue, packaging, and nonwoven materials manufacturers. As manufacturers strive to improve quality, productivity, sustainability, and modernization to operate the factories of the future, Panther helps them stay ahead.

Panther supplies software that operates manufacturing environments, enforces business rules, and generates customer-facing communication. Panther develops interfaces to automate information and machines by installing, maintaining, and upgrading measurement and control devices. Panther also collects and reports manufacturing data intelligence, solving difficult problems daily.

## Challenges

Panther works with multiple manufacturers and producers. One of the major challenges that security professionals at Panther faced was monitoring which users accessed what resources and ascertaining if the access was legitimate or not.

As most cyberattacks target identities—user accounts—to compromise the network, monitoring user behavior to spot security threats was the primary challenge.

Furthermore, as third parties outside the organization accessed the resources within its network perimeter, correlating these security data points to detect a security threat in its initial stage was also crucial.

Panther had initially deployed a security solution that was not meeting its proactive threat hunting, network security auditing, and compliance management requirements. It started looking for an alternative that is easy to customize and use and has unified security and compliance capabilities.

## The solution: Log360

While choosing a SIEM solution for the organization, Panther shortlisted a few tools, but none of them matched the ease-of-use or affordable deployment and training of Log360. This made Curtis Allworth, systems administrator at Panther, choose Log360 over other products.

Using the following Log360 features, Panther was able to solve the challenges mentioned above:

- **Security analytics dashboard:** Log360's insightful security analytics dashboard provides Panther with a clear, comprehensive overview of its system's activities, allowing it to spot suspicious behavior with ease. By visualizing the log data in an intuitive manner, Panther is able to quickly identify potential security threats and take proactive measures to mitigate risks.

- **Event correlation engine:** Log360's event correlation engine helps Panther detect and neutralize critical security threats, identity-based attacks, and suspicious user behavior.

  **Advanced Threat Analytics add-on:** The solution's threat analytics module helps Panther quickly spot and neutralize malicious traffic interactions in the network. The prebuilt, dynamically updated threat feeds enhance Panther's threat detection capabilities by providing up-to-date information about known malicious IP addresses, domains, and URLs.

- **Log search:** The log search option in Log360 empowers Panther to efficiently locate specific logs or events within the log data. Whether it is a specific event, a particular user's activities, or a time range of interest, Log360's search option allows Panther to zero in on and extract the relevant logs. This saves the company valuable time and effort that would otherwise be spent manually sifting through mountains of log data.

## Impact

The implementation of Log360 has had a significant impact on Panther, revolutionizing its approach to security threat detection and response. As highlighted by Allworth, the ability to customize the correlation engine based on the organization's needs has empowered the company to fine-tune its threat detection capabilities.

Additionally, the timely, effective alerts provided by Log360 have become a valuable tool for detecting and responding to critical security events. Together, all these features have significantly strengthened Panther's security posture, ensuring the company can proactively defend against threats and maintain a secure environment for its operations.

## Other key features of Log360

- Identify insider threats through user and entity behavior analytics, which leverages machine learning for accurate threat detection.
- Prioritize threats that occur earlier in the attack chain by using the MITRE ATT&CK® framework in Log360.
- Safeguard cloud accounts from unauthorized access and ensure the protection of cloud-based data assets.
- Assess your AD environment regularly to spot security risks and get granular visibility into weak and risky configurations.

## 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.

$ Get Quote  Download