ManageEngine
Log360

CASE STUDY

Unleash real-time security intelligence:

Discover how Log360's correlation engine empowered Paradyn's MSSP services

Company: Paradyn | Industry: IT services and IT consulting | Country: Ireland

About Paradyn

With the merger of Irish telecom, managed service, and network infrastructure companies, Paradyn stands out a premier managed security service provider (MSSP) and consulting service launched from a partnership between Irish Telecom, Netforce, and Exigent Networks.

Beyond desktop support, Paradyn provides its clients managed connectivity, which means it actively monitors, supports and maintains their entire infrastructure. Additionally, it creates, maintains, and supports local and wide area networks as well as clients' firewalls, network switches, servers, and workstations. Paradyn provides this through one managed service contract as the single supplier of these services.

> *I'm extremely happy with Log360 and the ManageEngine team's excellent customer support, and will definitely recommend others in my industry to give this SIEM solution a shot.*
>
> McGrainor remarked,
> Information security and technology officer.

Paradyn detected critical security threats with Log360

Utilizing ManageEngine Log360 in a client's environment, which is crucial for protecting sensitive data, enabling effective incidence response, and preventing further damage, Paradyn detected two security threats and resolved them.

Log360 delivers effective measures against worm-related threats

Detecting worm activities and other suspicious installations in their clients environment helps businesses defend the interests of their customers and maintain a robust security posture. Paradyn encountered a worm activity in their client's environment. Edward McGrainor, a SOC engineer at Paradyn, explained how both an internal and external security threat occurred, and how Log360 helped them to overcome these threats.

"Before deploying Log360, one of our clients had come across a 'worm' issue on their network. Though the client had initially purchased Log360 for compliance purposes, with help of a custom correlation report, we were able to identify and isolate the devices that were affected by the worm issue from the network," McGrainor said, adding, "Our customer would have taken 20 times longer to do this without the aid of Log360."

Leveraging Log360 for disgruntled employee risk mitigation

Another obstacle that Paradyn found was due to a disgruntled employee who was let go recently. As McGrainor explains, "The employee was trying to tamper with sensitive files before leaving. With the help of ManageEngine Log360, we were alerted about unauthorized access to sensitive data and authentication failures, and were able to avoid a data breach."

Challenges

As a managed security service provider, Paradyn has to ensure security around the clock for its clients. It needs to continuously monitor clients' networks to detect security threats, analyze their impact, and automatically neutralize them before they result in a full-blown attack. This requires a strong threat detecting spotting system that combines different detection mechanisms. These could include a rule-based correlation that connects the dots between disparate security data points, an machine learning-based anomaly detection model for detecting suspicious behaviors and changes in patterns, and signature-based mechanisms that spot known threats. Paradyn previously used another SIEM product, but it didn't have effective threat detection that met security needs. Paradyn required a tool that monitors real-time activity and protects its network infrastructure.

An MSSP's responsibility also includes implementing a proactive security strategy for its clients, wherein the cyber risks in the network are minimized by meeting compliance mandates. Paradyn found the solution it needed to provide holistic security across its network environment from a single console, balance its security strategies effectively, and ensure compliance with regulatory mandates such as the GDPR when it choose Log360.

The Solution

Deploying Log360 helps Paradyn detect and mitigate its clients' organizations in many ways:

- ### Security analytics:
  With Log360's intuitive security dashboard feature, Paradyn's IT admins can have a quick look at all the security events taking place in a network from a single console. It's comprised of numerous widgets which can be customized to their requirements like security events or recent alerts, so IT admins can detect suspicious threats in their network and resolve them efficiently.

- ### Correlation reports for security threats:
  Log360's event correlation helps Paradyn's security analysts comprehend the logs collected from heterogeneous sources and at different time periods, so they can analyze patterns and anomalies of each security events. This helps them hunt for threats proactively, as well as investigate and resolve the threats.

- ### Log search:
  Log360 has a powerful search engine, so threat hunters can backtrack to get information on particular logs or security events so they can extract any crucial data to file an incident report. Log360's advanced options save their search queries so they can generate informative security reports.

- ### Compliance reports:
  Log360's audit-ready compliance reports provide violation alerts that assist in the GDPR audit process.

- ### Log forensic analysis:
  It's not possible to detect threats all the time in an organization, as it's likely there will be volumes of log data that often require months for threat hunters to evaluate. By conducting a forensic analysis, threat hunters at Paradyn were able to mitigate existing threats, anticipate possible network security issues, and identify vulnerabilities in the network that can lead to a data breach. These techniques help Paradyn analyze reports proficiently as well as provide a more secure IT network environment.

- ### Advanced threat intelligence:
  Paradyn security analysts are able to protect their network environment by receiving alerts about blacklisted and malicious IP addresses, domains, and URLs utilizing Log360's threat intelligence module.

Impact

McGrainor is pleased Paradyn switched to Log360 for its SIEM solution. The organizations' IT admins found the product's dashboard features impressive as these helped them monitor threats with ease.

"I'm extremely happy with Log360 and the ManageEngine team's excellent customer support, and will definitely recommend others in my industry to give this SIEM solution a shot," McGrainor remarked.