Building digital trust

Managed security solution protects Asia-based global firm

Challenges

- Wanted to focus on core business by outsourcing cybersecurity to industry experts
- Required consistent cybersecurity controls across the organization including insider threats and transactional fraud
- Needed 24/7 security monitoring and support

Solutions

- Security Log Monitoring
- Managed Security Behavioral Analytics
- Customized Security Advisory Consulting

Results

- Improved cyber defense with comprehensive security services
- Major security events stopped before causing harm
- More frequent assessment of threat detection rules and areas for improvement
- Company-wide cybersecurity

Challenge

Refocus business resources by outsourcing cybersecurity

The biggest challenges faced by this real estate firm were business and data security. They needed to refocus on their core business while ensuring compliance with data protection and privacy laws, as well as aligning business objectives with a proactive risk management strategy. The firm sought a trusted managed security services provider (MSSP) to overhaul its cybersecurity strategy, safeguard operations, mitigate risks and establish an environment of trust for its entire ecosystem.

The firm's existing cybersecurity defenses needed fortification to manage IT security round the clock. The firm also required early detection capabilities, to triage cyber threats and incidences before they occurred as well as comprehensive security processes to effectively manage and respond to threats.

LUMEN® TECHNOLOGIES

The ability to monitor users' activities and behavior against insider threats was also a high priority. They required log collection and correlation from their networks and servers across Asia Pacific, Europe, the United Kingdom and United States to help track incidents and prioritize events for analysis and immediate action.

Solution

Comprehensive managed security services and 24/7 threat monitoring

Three critical services to boost cybersecurity efforts across the organization were selected:

1. Lumen Security Advisory Consultants provided oversight and proactive daily management of risks, working closely with the firm's decision-makers to proactively identify and address security risks and ensure IT policies were best suited to their business.
2. Managed Security Behavioral Analytics (MSBA) complements Security Log Monitoring (SLM) in applying user & entity behavioral analytics monitoring. This provides advanced visibility of cyberthreats from within the organization—such as hijacked accounts, login anomalies, credential/identify theft, malicious user and network activities which may not be as effectively covered by SLM. The Lumen team customized the MSBA algorithm to detect signs of fraud and misuse on the firm's file servers, DNS servers and ERP applications and database systems.
3. Lumen provisioned SLM to collect, parse, correlate incidents in real time and apply analytics to detect security anomalies. This data was conveyed to Lumen's 24/7 SOC team for review and investigation, enabling quicker identification and mitigation of suspected security risks. Lumen actively monitored several hundred devices for the firm, including firewalls, servers and network infrastructure devices.

Results and future plans

Improved cyber defense with comprehensive security services

By outsourcing vital components of cybersecurity, the firm was able to manage their vast business and operations and keep it safe in the hands of experts.

Significant security events have been stopped in their tracks—including halting the spread of malware that had managed to evade the corporate antivirus software, suspicious activity detected from a privileged user account and occasional data exfiltration activities.

Since January 2019, the prevalence of risky incidents and the need for escalation to the firm has trended downwards. Lumen Security Advisory Consultant continues to work with the firm to calibrate their threat detection rules or use cases and recommend areas for improving their security posture. Close alignment between Lumen's SOC and the customer's corporate IT security has also ensured synergy.

The next phase has Lumen extending the current security services to include monitoring of cloud services and audit logs for the firm.

LUMEN® TECHNOLOGIES