Enterprise Strategy Group by TechTarget

TECHNICAL FIRST LOOK

NOVEMBER 2024

Proactive Cybersecurity With Lumen Advanced Managed Detection and Response Services

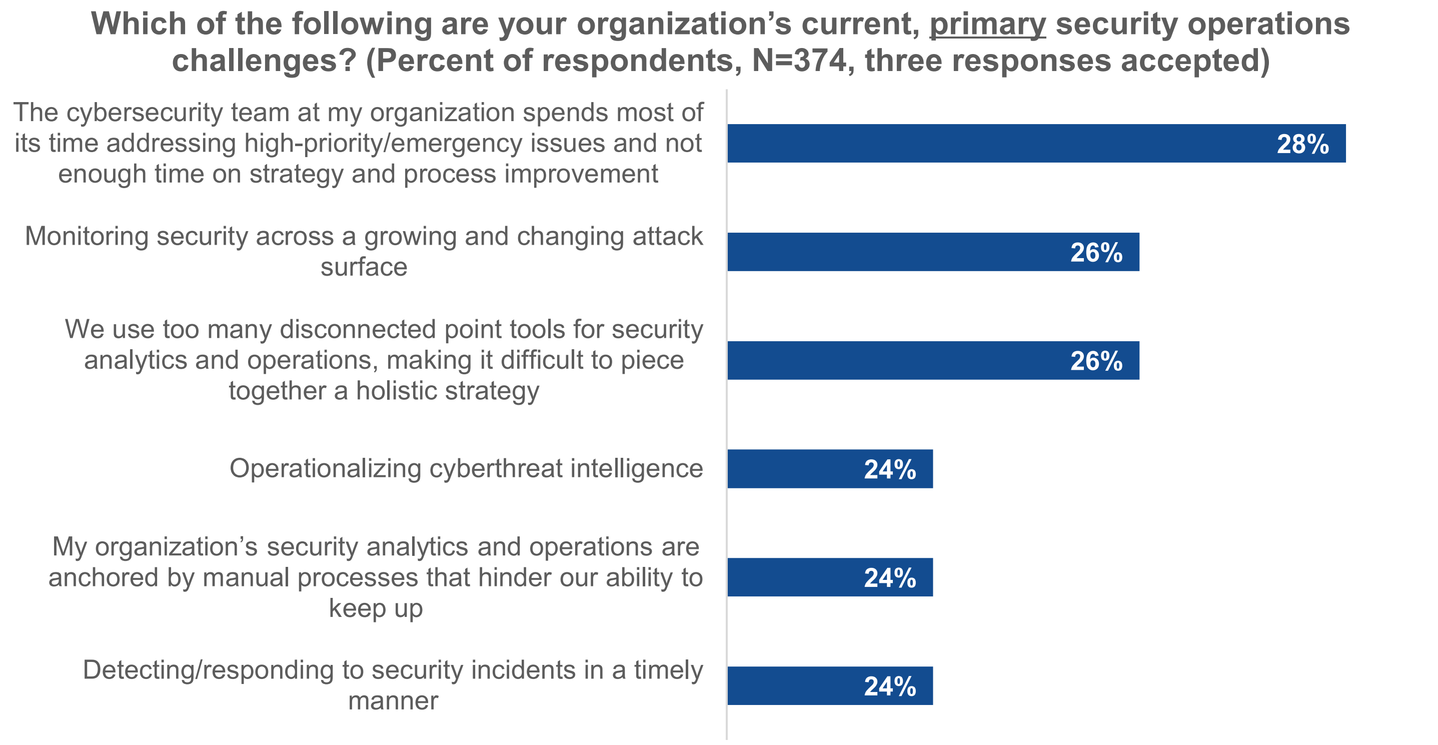
Alex Arcilla, Principal Analyst – Validation Services

Cybersecurity Challenges

Organizations, regardless of size, continually face cybersecurity challenges. Adversaries are constantly producing more sophisticated attacks, leveraging techniques such as phishing and credential theft and taking advantage of vulnerable assets. With an ever-growing attack surface that exposes new security gaps, along with a persistent threat landscape and the volume and complexity of security alerts, it is no wonder that managing security operations has become difficult and complex.[1]

Furthermore, the top primary security operations-related challenges that organizations reported facing vary and include high priority or emergency issues, dealing with too many disconnected tools, and detecting and responding to security incidents in a timely manner (see Figure 1).

Figure 1. Primary Security Operations Challenges



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

[1] Enterprise Strategy Group Research Report, *The Triad of Security Operations Infrastructure: XDR, SIEM, and MDR*, June 2024. All Enterprise Strategy Group research references and charts in this Technical First Look are from this report.

Staying ahead of threats and attacks is a never-ending task. The sophistication of today's threats and attacks has shown that organizations can no longer rely on any single approach or solution to protect against adversaries, such as traditional endpoint detection and response (EDR) and network detection and response (NDR) solutions. Organizations have realized that having the proper tools in place for detection and response, as well as defensive strategies supported by asset detection, vulnerability management, and identity protection, can collectively help in reducing entry points for adversaries. More importantly, these tools and methodologies would ideally be integrated in order to address any security gaps that would be overlooked by any individual tool.

However, integrating multiple and disparate tools and technologies into a comprehensive security operations function is too complex and expensive to build from scratch. Continually acquiring the skills and experience required for establishing a secure perimeter, obtaining and configuring the tools, integrating these tools with effective workflows, establishing the needed comprehensive visibility, and acquiring and operationalizing threat intelligence is too time-consuming. Detection and response times become longer, increasing an organization's cybersecurity risk. Moreover, the focus of establishing security operations is to mitigate the risk of events that have been *known to occur*, with little focus on what *could potentially occur*.

While organizations have turned to managed detection and response (MDR) providers to relieve the burden of bolstering their cybersecurity posture, these providers can also present challenges. Other offerings may not triage alerts, burdening the organization with responses that may not bolster its security posture sufficiently. While other offerings may use threat intelligence, any insights might not be tailored to the customer's IT environment. MDR providers might not also offer support for the current cybersecurity tools already implemented in the organization, making other offerings difficult to integrate.

Lumen Advanced Managed Detection and Response

Lumen Advanced Managed Detection and Response (A-MDR) is a service offering that provides comprehensive security operations capabilities 24/7 to minimize the entire attack surface of an organization's IT environment. The service is offered in modules depending on customers' immediate and long-term cybersecurity needs.

The service not only helps in strengthening the security of enterprise endpoints and network infrastructure but also other areas vulnerable to threats and attacks, including cloud applications, internet of things (IoT) infrastructure, and operational technology (OT). A-MDR also incorporates user entity and behavior analytics (UEBA) to detect and respond to vulnerabilities due to end-user behavior within an organization. Lumen A-MDR also offers comprehensive visibility into an organization's entire IT asset inventory to identify where threats may enter—whether located on premises, in the public cloud, in third-party environments (e.g., business partners), or in subsidiaries (as selected by the customer).

The service is backed by a 24/7 security operations center (SOC) for continuous monitoring, incident detection, triage, and analysis. Responses to threat attacks can also be automated with Lumen A-MDR, enabling faster response times.

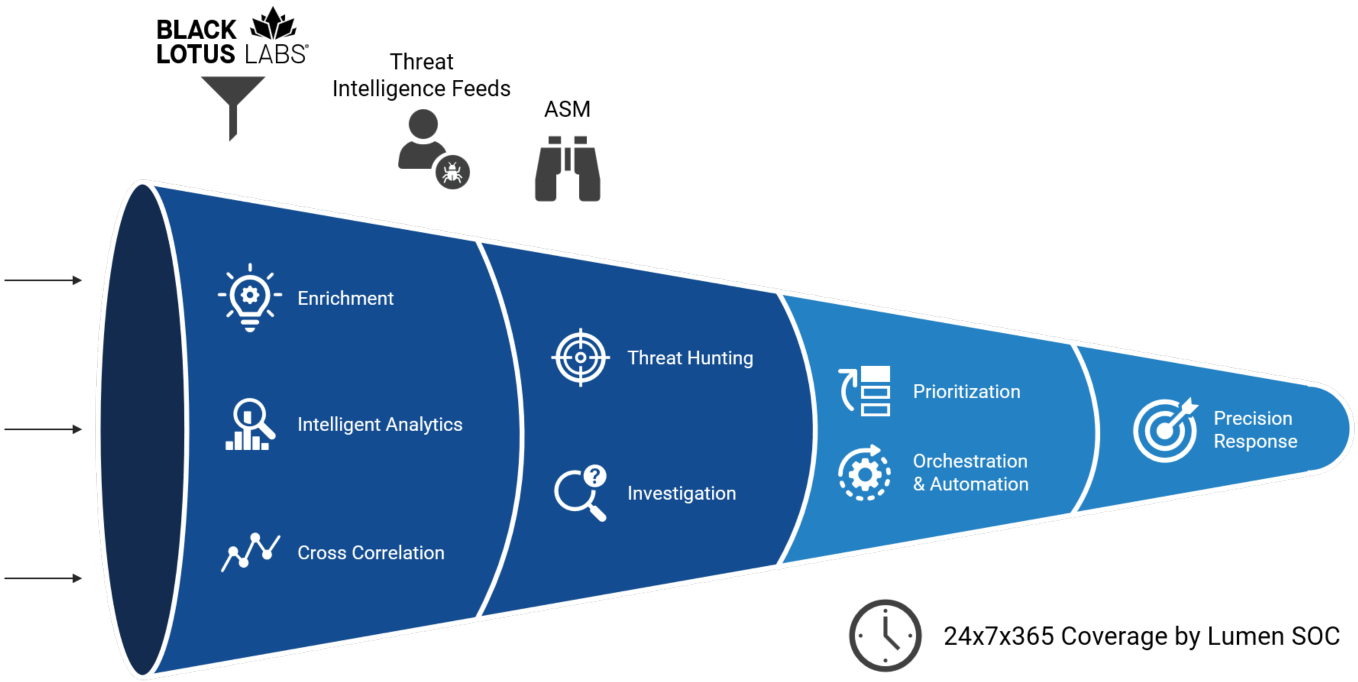
With Lumen A-MDR, organizations can scale easily to accommodate business or IT infrastructure growth as exposure to threats and attacks expands. The service's scalability can minimize the need for organizations to invest additional time, resources, or money in extending their security perimeter.

First Look

TechTarget's Enterprise Strategy Group reviewed Lumen A-MDR to highlight how it can help organizations proactively improve their security posture, without investing the time, expertise, and experience typically required when deploying an in-house SOC. Figure 2 shows how Lumen personalizes security coverage for each customer. Our analysis uncovered the following:

- Lumen A-MDR actively collects and analyzes data from multiple sources within and outside an organization to identify known and potential threats that can cause the most damage. By applying this approach, Lumen A-MDR can bolster an organization's security posture without needing to address all potential vulnerabilities (as per the 80/20 rule). At the same time, the organization does not need to spend the time and resources to prioritize those threats and vulnerabilities to address.

Figure 2. How Lumen Tailors Lumen A-MDR to Individual Customers



Source: Lumen and Enterprise Strategy Group, a division of TechTarget, Inc.

- As part of its threat intelligence, Lumen offers its own threat intelligence via Black Lotus Labs, Lumen's threat and research arm, to supply anonymized customer data obtained from the Lumen network backbone to uncover potential threats. Combining this data with data from other third-party threat intelligence feeds supports Lumen A-MDR in better uncovering the more dangerous threats and vulnerabilities to an organization. Again, such information is tailored and made actionable for individual customers.
- Lumen A-MDR also incorporates detection engineering, an internal group dedicated to mapping out scenarios and use cases that expose vulnerabilities. These use cases are then operationalized by Lumen's service to detect additional threats or attacks that can take advantage of those vulnerabilities. With detection engineering, a customer can be assured that Lumen A-MDR is working to proactively bolster its security posture based on its current IT environment and end-user activity.
- To obtain the most use out of the managed service, organizations can enlist the services of Lumen's cybersecurity analysts, Black Lotus Labs, security advisory consultants, and an incident response team that includes digital forensic analysts and incident responders. Should customers choose any or all of these professional services, they collaborate with individual customers to map out those scenarios that the organizations will most likely experience, while operationalizing how to monitor, identify, and respond to both known and potential threats and attacks. Offering these services eliminates the need for organizations to close any cybersecurity skills gaps that may have existed.
- Lumen A-MDR can be integrated with existing tools within the organization, as Lumen partners with multiple vendors that are already in the security space. This helps to minimize business disruption and security risk.

- Lumen's threat hunting provides another layer of protection to their A-MDR service by proactively seeking out hidden threats that may have evaded automated security tools.

Conclusion

Strengthening cybersecurity needs to remain top of mind for organizations or else they risk the loss of business, brand, and reputation. But no single tool or technology can comprehensively secure an organization against both known and potential threats across on-premises and cloud environments supporting production, IoT, and OT networks. An integration of the most appropriate solutions is necessary to cover detection and response, asset visibility, vulnerability management, and identity protection. Yet, combining these tools to build out in-house security operations is too expensive and complicated to accomplish should an organization not possess the time, resources, or relevant skills. To respond to the lack of in-house skills and resources, Enterprise Strategy Group found that 82% of research respondents are already using managed services for some or a majority of security operations.

Enterprise Strategy Group's reviewed Lumen A-MDR and believes it can help organizations strengthen their cybersecurity posture without the need to acquire and update the skills necessary to protect against ever-evolving threats and attacks. Lumen A-MDR integrates the necessary tools to decrease time to detection and response, hunt for new and evolving vulnerabilities via threat intelligence and scenario planning tailored to each customer, prioritize alerts that need immediate attention, and provide the comprehensive visibility necessary for ongoing monitoring. Combined with in-house security expertise, Lumen A-MDR delivers the capabilities needed to secure endpoints, networks, cloud, and identity. Based on our initial evaluation, we believe that Lumen A-MDR can help in closing known and unknown security gaps, enabling the business to operate with minimized downtime and risk.

About Enterprise Strategy Group
TechTarget's Enterprise Strategy Group provides focused and actionable market intelligence, demand-side research, analyst advisory services, GTM strategy guidance, solution validations, and custom content supporting enterprise technology buying and selling.

✉ contact@esg-global.com
www.esg-global.com