DYOPATH
Driving Your Organization's PATH to IT Success

Guide Sheet: Threat Detection & Response

According to the Ponemon Institute, 70% of IT professionals say their organization is unfit to respond to a cyber attack due to the lack of a cybersecurity response plan. With restricted budgets, limited personnel, and no time to parse through the thousands of logs generated daily, businesses have sought out solutions to automate threat detection and response. From Security Incident and Event Management (SIEM) technology to advanced Managed Detection and Response (MDR) solutions, enterprises are quickly modernizing their security solution to adapt to the needs of the evolving threat landscape.

Did you know?

30 billion
devices will be connected to the Internet by 2023 - 45% of those will be mobile

76%
of cybersecurity professionals claim that threat detection & response is more difficult today than it was to years ago

280 days
is the average length it takes to respond to a cybersecurity incident

Threat Detection & Response Solutions

Security Incident & Event Management

Gartner explains that Security information and event management (SIEM) solutions "support threat detection and security incident response through the real-time collection and historical analysis of events from a wide variety of event and contextual data sources. It also delivers compliance reporting and incident investigation through analysis of historical data from these sources." SIEM were first used as log management systems typically for compliance purposes, but over the years, they have grown to be more complex.

Because of their increased capabilities like threat detection and user and entity behavioral analysis, many SOC teams rely on these solutions to help streamline their risk management processes. However, because SIEM solutions can only look for specific attacks using rules programmed by the system, SIEM tools typically aren't ideal for detecting advanced threats and can leave businesses with gaps in their visibility.

solutions@dyopath.com
1.866.609.PATH

Endpoint Threat Detection and Response

Gartner defines Endpoint Detection and Response (EDR) solutions as "solutions that record and store endpoint-system-level behaviors, use various data analytics techniques to detect suspicious system behavior, provide contextual information, block malicious activity, and provide remediation suggestions to restore affected systems." They go on to explain that the primary capabilities of EDR solutions include detecting security incidents, containing the incident at the endpoint, investigating security incidents, and providing remediation guidance.

EDR solutions are great for businesses who are looking to gain more visibility into their attack surface to uncover incidents that would otherwise remain invisible. With an EDR solution, enterprises can detect, investigate, and remediate modern, complex threats that are advanced and persistent enough to evade your traditional perimeter defenses.

Managed Detection and Response (MDR)

Managed Detection and Response (MDR) solutions, according to Gartner, "offer turnkey threat detection and response via modern, remotely delivered, 24/7 security operations center capabilities and technology." Gartner expands on this, adding that MDR service providers "offer a turnkey experience, with many using a predefined technology stack covering endpoints, networks, cloud services, operational technology (OT)/Internet of Things (IoT) and other sources, to collect relevant logs, data and other telemetry (e.g., forensic data, contextual information). This telemetry is analyzed via the provider's platform using a range of analytics, threat intelligence (TI) and manual analysis from experts skilled in incident detection and response. Human-performed, threat-hunting services complement realtime monitoring and detection capabilities to find novel and sophisticated threats."

Extended Detection and Response (XDR)

Gartner explains the latest emerging threat detection and response solution, Extended Detection and Response (XDR), as "a unified security incident detection and response platform that automatically collects and correlates data from multiple proprietary security components." Primarily, XDR solutions offer "centralization of normalized data; correlation of security data and alerts into incidents; and a centralized incident response capability that can change the state of individual security products as part of incident response or security policy setting."

Because multiple standalone security tools can complicate the threat detection and prevention process, XDR solutions enable businesses to move away from this traditional siloed approach of detection and response solutions. Instead, with XDR, enterprise can improve their security operation center's productivity by giving analyst a holistic view of the threat landscape, automating incident response workflows, and limiting the impact of an incident.

Conclusion

In order to minimize the risks your business faces on a daily basis, you need a robust cybersecurity management program in place, but with limited resources, IT professionals know this is never as easy as most think it seems. While utilizing multiple security tools does enable security teams to better managed various attack vectors, the truth is: a siloed approach to threat detection and response will no longer cut it. In fact, ESG Research found that 66% of organizations feel that their threat detection and response effectiveness is limited because it is based on multiple independent point tools. Instead, businesses need a seamless solution that can detect and respond to all advanced, unknown threats faster and with unprecedented accuracy in one single location. As enterprises look toward the future, especially in our new remote workforce-era, monitoring endpoints is going to be more important than ever. Makes sure your organization is protected against advanced endpoint threats by learning more about DYOPATH, a solution designed specifically to simplify your cybersecurity management.

1.866.609.PATH

Texas Office:
13430 Northwest Fwy,
Suite 1000
Houston, TX, 77040

Illinois Office:
425 N. Martingale Rd.
Suite 1900
Schaumburg, IL 60193

solutions@dyopath.com