A CISO GUIDE TO MANAGED DETECTION RESPONSE/ MANAGED PREVENTION RESPONSE

Sponsored by Cyber Talk

In cyber security, you no longer choose your battles

New, sophisticated cyber attacks can dictate your cyber security strategies. As attacks become more advanced, the security practices that may have worked in the past can have diminishing returns. The security practices that may have worked in the past can have diminishing returns. As per Gil Shwed, the founder, and CEO of Check Point, "You don't pick your battles, they pick you," in speaking of the turnaround in the cyberthreat world. Attackers decide what you need to deal with.[1]

Against this landscape, your best cyber security is a solution that offers a comprehensive platform, protecting your organization against a wide spectrum of attacks. As a CISO, you no longer have the luxury of allocating security resources to target your biggest perceived threats. There are too many advanced attacks that can bring your operations to a halt for you to focus on isolated threat types.

Prevention and Detection Go Together

Acting on security alerts is a common practice and a necessity. However, the high volume of attacks can overwhelm your on-premise security team, threatening the ability to respond and remediate.

Third-party services play a valuable role to offload alert activities and provide other functions to your security operations centers (SOCs). These services use varying models to address alert overload, which can upgrade an organization's security posture.

> Healthcare organizations were a hard-hit cyberattack target in 2022.[2] "The average organization now uses 82 different tools, and even the most experienced staff can find it difficult to manage the steady stream of alerts they produce. **MDR can provide nonstop coverage to help teams optimize their solutions.**[3]

---

[1] "The Technology Letter: Check Point CEO Shwed: You Don't Pick Your Battles, They Pick You," by Tiernan Ray, The Technology Letter, January 3, 2023 https://blog.checkpoint.com/2023/01/04/the-technology-letter-check-point-ceo-shwed-you-dont-pick-your-battles-they-pick-you/

[2] "Global Cyberattacks Increased By 38% Last Year, Healthcare Hit Hard," by Jill McKeon, January 11, 2023 https://healthitsecurity.com/news/global-cyberattacks-increased-by-38-last-year-healthcare-hit-hard#:~:text=January%2011%2C%202023%20%2D%20Global%20cyberattacks,the%20government%20and%20education%20sectors

[3] "5 Takeaways about MDR for Healthcare Cybersecurity," by Tanya Candia, HealthTech, January 10, 2023 https://ramaonhealthcare.com/5-takeaways-about-mdr-for-healthcare-cybersecurity/

Too many alerts, not enough time

In a recent study, 79% of respondents reported having more than 500 cloud-security alerts open each day.[4] Since it can take up to 30 minutes to investigate each alert, the negative impact on security and staff is tangible.[2] Likewise, the 2022 Devo SOC Performance Report, cited information overload and growing workloads as a main factor in worker burnout.[5]

The need for outsourcing is a foregone conclusion.

Advantages and Disadvantages of Different Models for Incident Response

Third-party services offer different models for security-event detection and response. Security Information and Event Management (SIEM) is a legacy model that offers in-house staff tools to monitor security events. SIEM is detection without response. Next, adding outsourced staff gives you Managed Security Service Providers (MSSP), security monitoring and management from off-site operation centers.[6] MSSPs might support incident response, but they have concerns:

- Most organizations spend more time on security after hiring an MSSP
- MSSP's specializing in technology offer minimal incident response and forensics, plus they might not know how your internal systems work
- MSSP remote admin tools to access customer systems can be compromised[7]

For better alternatives, Managed Detection and Response (MDR), Managed Prevention and Response (MPR), Extended Detection and Response (XPR) and Extended Prevention and Response (XPR) have come into play.

---

[4] Security Staff, One-fifth of cybersecurity alerts are false positives, Security, March 15, 2022. https://www.securitymagazine.com/articles/97260-one-fifth-of-cybersecurity-alerts-are-false-positives

[5] Michael Hill, Information overload, burnout, talent retention impacting SOC performance, CSO, Oct 12, 2022. https://www.csoonline.com/article/3676135/information-overload-burnout-talent-retention-impacting-soc-performance.html?utm_source=Adestra&utm_medium=email&utm_content=Title%3A%20Information%20overload%2C%20burnout%2C%20talent%20retention%20impacting%20SOC%20performance&utm_campaign=Top%20Enterprise%20Stories&utm_term=Editorial%20-%20IDG%27s%20Top%20Enterprise%20Stories&utm_date=20221013165028&huid=8ca4b8cb-4faa-47a1-8c75-7476f1fb4901

[6] Anon. Managed Security Service Provider (MSSP), Gartner, as viewed on December 15, 2022. https://www.gartner.com/en/information-technology/glossary/mssp-managed-security-service-provider

[7] Jaikumar Vijayan, 6 risk factors to know when hiring an MSSP, CSO, August 2021. https://www.csoonline.com/article/3432156/6-risk-factors-to-know-when-hiring-an-mssp.html

> Gartner defines MDR as services that "provide customers with remotely delivered modern security operations center (MSOC) functions. These functions allow organizations to rapidly detect, analyze, investigate, and actively respond through threat mitigation and containment. MDR service providers offer a turnkey experience, using a predefined technology stack..."[8]

Outsourcing to MDR services is a growing trend.

- By 2025 half of organizations will be using MDR services.
- 94 percent of organizations are evaluating MDR services.
- 79 percent of organizations are considering adopting MDR soon.

Here is why.

Organizations investing in MDR services saw a 50 percent reduction in Mean time to Detect (MTTD) and Mean time to Respond (MTTR) as well as up to 50 percent lower costs for cyber security operations.[9]

Managed Detection Response and Managed Prevention Response

MDR's detection model is built on the fact that to support desired service levels, most security controls permit threats to enter an organization's environment while security teams analyze traffic for threats. When the detection system discovers a suspicious event, it issues a valid alert or a false positive. However, real attacks are already inside the environment. The MDR's staff must stop the attack, do forensic analysis to discover the extent of damage, then mitigate damage. In contrast, preventing threats from entering the IT environment is more efficient by minimizing alerts and preventing damage requiring forensic analysis and remediation. Managed Prevention Response (MPR) vendors lead with prevention for less costly labor.

---

[8] Anon, What are Managed Detection and Response (MDR) Services? Gartner, As viewed on December 5, 2022. https://www.gartner.com/reviews/market/managed-detection-and-response-services

[9] MDR statistics, PURPLESEC, as viewed on December 6, 2022. https://purplesec.us/resources/cyber-security-statistics/#MDR

Extended Detection and Response

Augmenting MDR/MPR, extended detection response/extended prevention response (XDR/XPR) identifies threats already inside an organization's environment. Whereas XDR emphasizes detection, XPR emphasizes preventing threats from spreading by continuously analyzing threat data from all security enforcement points. Like MPR, XPR minimizes forensics and remediation costs.

Five recommendations for choosing an MDR/MPR, XDR/XPR provider

1. Does the MDR/MPR provider lead with prevention or only detection?

Prevention means stopping attacks outside your IT environment. Utilizing AI, behavioral analysis and even chip-level threat analysis is necessary for your MDR/MPR's security stack to recognize new, unknown threats and minimize false positives. In addition, having a massive global threat intelligence network is vital for your MDR/MPR provider to prevent known threats from entering your environment.

2. How complete is security coverage?

In this new space, some vendors specialize in endpoint detection response (EDR) while other specialize in cloud detection response. Using a patchwork of specialty vendors will fragment security. Others claim to cover everything in the environment, while a few covers the entire environment: network, cloud, SaaS IoT, smartphones, endpoints, and the rest. For effectiveness, the best practice is to the find the MDR/MPR provider offering the most comprehensive security stack, consolidated into a single architecture.

3. What expertise does the SOC staff possess?

An MDR/MPR's staff should be intimately familiar with advanced cyber security and how it applies to your specific environment. The staff should also be knowledgeable in rapid response, forensics, and mitigation.

4. What is automation and AI's role?

Another way an MDR/MPR vendor can improve security while saving operating costs is to automate threat prevention and other operations. Be sure to inquire about the use of automation and AI in a vendor's stack.

5. For big threat data, size matters

Having big data on threats is critical to top-tier MDR/MPR vendors in 2 ways. First, big data on threats is critical for training AI engines to detect and block novel threats and unusual activity. Second, big data containing threat signatures is necessary for preventing known threats. It takes a large vendor to accumulate sufficient data to educate AI and block threats.

Conclusion:

Vendors who provide MDR/MPR and XDR/XPR services are improving the effectiveness of their customers' cyber security by helping them respond to high-volume alerts from cyber attacks.

Horizon, Check Point's prevention-first security operations and unified management suite, offers XDR, MDR and events management solutions for complete coverage of networks, endpoints, cloud, email, and IoT.

In regards to Horizon, CEO Shwed remarks, "The typical enterprise, a company anything from five hundred employees to even ten or twenty thousand employees, they simply cannot afford having what we call a security response team that will monitor the network twenty-four seven. It is expensive, but also, you cannot get the talent, there's not enough people like that."[10]

Conversely with Horizon, Check Point runs "one center that sees the data of hundreds of companies. By filtering the attacks from all those companies simultaneously, the Check Point sense of the threats gets sharper. It is a form of leverage that makes the task of defense more efficient. We learn from every customer."

To learn more about Horizon, please visit this webpage.

Horizon
MDR/MPR

[10] "The Technology Letter: Check Point SEO Shwed: You don't pick your battles, they pick you," Check Point blog, January 4, 2023 https://blog.checkpoint.com/2023/01/04/the-technology-letter-check-point-ceo-shwed-you-dont-pick-your-battles-they-pick-you/

Worldwide Headquarters
5 Shlomo Kaplan Street, Tel Aviv 6789159, Israel | Tel: +972-3-753-4599

U.S. Headquarters
959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 1-800-429-4391

www.checkpoint.com