SYGNIA

MARCH 2024

SYGNIA'S ANNUAL FIELD REPORT

THE DEFENDER'S PERSPECTIVE: DETECTION

To combat ever-evolving threats, security solutions must adapt and evolve. This is where Extended Detection and Response (XDR) emerges as a critical weapon in the fight against cybercrime.

Driven by the increasing complexity of cyber threats and the need for centralized and integrated security solutions, **the XDR market is experiencing explosive growth**. As technology trends continue to accelerate, we can expect to see a wave of exciting new features emerge within the XDR space. In this installment of **Sygnia's Annual Field Report: The Defender's Perspective - Detection** the Sygnia Managed XDR (MXDR) team delves into the burgeoning XDR market, exploring key trends that shaped the past year and predicting the next "killer features" that will change the XDR market and redefine cybersecurity paradigms.

In the following sections, we will explore: The field report is a compilation of findings derived from Sygnia's Incident Response, Adversarial Tactics, Enterprise Security, MXDR, Engagement Managers and Legal teams, each to be published individually in the coming weeks. Key findings include:

- **Trends from 2023**: Examining the major forces that shaped the XDR market in the past year, including technological advancements, market dynamics, and user adoption.
- **Unveiling 2024's Landscape**: Analyzing anticipated trends and emerging technologies that will further propel the XDR market forward in the coming year.

TRENDS FROM 2023

1. Commonality in Incident Types and Alerts

- The majority of incidents addressed by Sygnia's MXDR team last year pertained to privilege escalation and the detection of Ghost hosts. Additionally, Sygnia's MXDR team regularly identified initial instances of lateral movement within our clients' networks.
- The most frequent alerts observed were associated with the detection of IOCs, the execution of network scanning tools, and incidents involving multi-factor authentication (MFA).

2. Adding Third Party and Supply Chain Indicators to the Threat Landscape

- Third-party and supply chain risks increasingly threaten clients' environments. By systematically mapping these risks through technology or systems and integrating them into the monitoring framework, along with continuous updates of CVEs and IOCs by our CTI team, we enhance our clients' cybersecurity posture.

3. Time to Detect & Time to Respond:

> Continuous enhancement of both time to detect (TTD) and time to respond (TTR) is a critical client requirement. The capacity to promptly alert, investigate, and respond is vital from the client's perspective.

4. Closing the Loop and Adding Value to Detection Services

> Clients seek value from service providers beyond mere incident alerts. They expect mitigation measures and recommendations provided by analysts familiar with their business processes and security environment. This demonstrates clear and unmatched value to the client.

5. One Stop Shop for Cybersecurity Services

> Collaboration with red teams and posture services, constantly enhancing and challenging cybersecurity concepts, stands as a significant differentiator in providing services to clients.

In conclusion, the analysis of last year's trends underscores the importance of addressing common incident types, enhancing detection capabilities, mitigating third-party risks, and prioritizing swift response times.

UNVEILING 2024'S LANDSCAPE

1. Enhanced Automation and AI-Driven Threat Detection:

> Machine learning (ML) and artificial intelligence (AI) are poised to significantly automate security tasks like threat detection and response. This advancement will empower XDR solutions to become more proactive and efficient, thereby alleviating the workload on security analysts.

> AI-powered threat analysis will facilitate rapid identification and prioritization of critical threats by XDR solutions, enabling organizations to respond with greater efficacy.

> Through advanced analytics, organizations will gain deeper insights into security data, enabling them to recognize trends and patterns indicative of potential threats more effectively.

2. Integration with Security Operations Center (SOC) Tools:

- XDR solutions will soon begin to be integrated more seamlessly with other SOC tools, including Security Information and Event Management (SIEM) and Security Orchestration, Automation, and Response (SOAR) platforms. This integration will foster a unified security ecosystem, empowering organizations to manage their security posture with greater effectiveness.
- The popularity of open-source XDR solutions will rise, enabling organizations to tailor their security solutions to their unique requirements.
- Cloud-based XDR solutions will gain further momentum, providing organizations with a more scalable and cost-effective means of deploying XDR technology.

3. Enhanced Threat Hunting Capabilities:

- XDR solutions are poised to offer advanced threat hunting capabilities, empowering security analysts to proactively identify and investigate potential threats.
- XDR solutions will be able to leverage data from various sources, such as endpoints, networks, and the cloud, to provide a comprehensive view of the security landscape.
- Threat hunting will undergo further automation, with XDR solutions utilizing AI and ML to detect suspicious activity and notify security analysts more promptly.

4. Continuous Threat Intelligence and Threat Sharing:

- XDR solutions will seamlessly integrate with threat intelligence feeds, ensuring organizations have access to the most current information on emerging threats and vulnerabilities.
- Organizations will be able to share threat intelligence data with each other, helping to improve overall security posture.
- XDR platforms will utilize threat intelligence data to autonomously update security policies and detection mechanisms, enhancing overall security efficacy.

5. Increased Focus on User Behavior Analytics:

- XDR solutions will increasingly incorporate user behavior analytics (UBA) to detect anomalous user activity that may indicate a security compromise.
- UBA will be used to identify insider threats and other malicious actors.
- XDR platforms will be able to leverage UBA data to automatically block suspicious activity.

6. Enhanced Data Privacy and Security:

- XDR solutions will be designed with data privacy and security in mind.
- Organizations will be able to control who has access to their data and how it is used.
- XDR platforms will comply with relevant data privacy regulations, such as the General Data Protection Regulation (GDPR).

7. Enhanced Scalability and Performance:

- XDR solutions will be able to scale to meet the needs of large organizations.
- XDR platforms will be able to handle large volumes of data without compromising performance.
- Organizations will be able to deploy XDR solutions on-premises, in the cloud, or in a hybrid environment.

Additional Predictions:

- XDR solutions will become more user-friendly and intuitive.
- Expect XDR vendors to offer more flexible licensing options.
- The XDR market is likely to witness further consolidation, with larger vendor acquiring smaller competitors.
- Managed XDR services are expected to become increasingly attractive to medium-sized businesses given the escalating challenge of recruiting proficient cyber experts.

In conclusion, the next breakthrough feature in XDR solutions is poised to be a fusion of AI-driven threat detection, streamlined automation, seamless integration with diverse security tools, and advanced threat hunting capabilities. As technological advancements persist, we anticipate the emergence of increasingly innovative and robust XDR solutions in the future.

WANT TO KNOW MORE ABOUT ONE OF OUR SOLUTIONS?

As the trusted advisor and cybersecurity service provider of leading organizations worldwide, Sygnia protects the enterprise through a variety of solutions that are aligned with the current threat landscape. From OT and Cloud Security to Ransomware Readiness, our Enterprise Solutions are borne out of frontline experience and a deep understanding of the threat actor mindset.