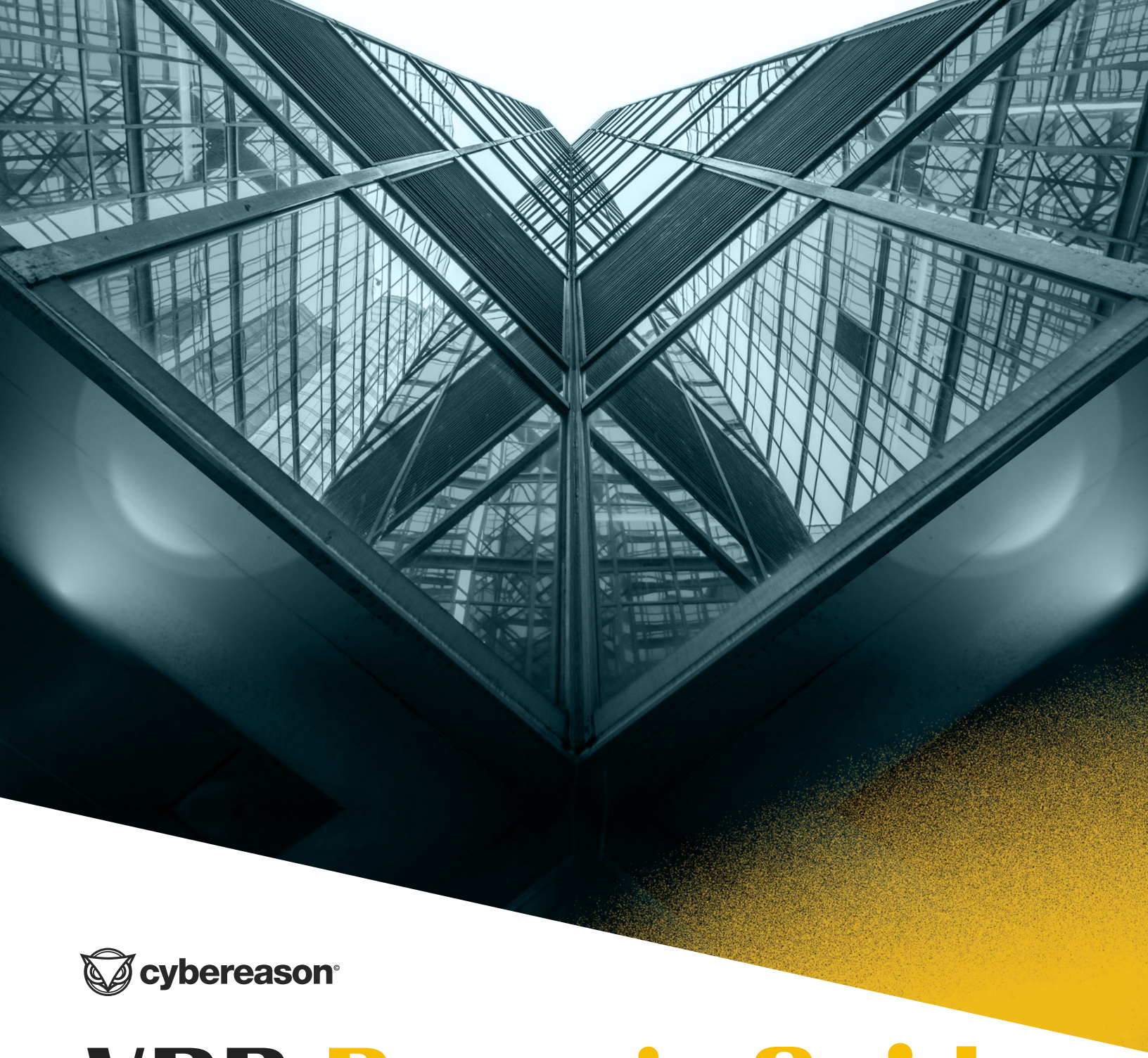

cybereason

XDR Buyer's Guide

THE ESSENTIAL GUIDE FOR EVALUATING EXTENDED DETECTION AND RESPONSE (XDR) FOR YOUR SECURITY PROGRAM

Table of Contents

1. What is XDR?

XDR, or Extended Detection and Response, is a modern cybersecurity approach combining multiple security technologies to provide comprehensive threat detection, response, and remediation capabilities. It aims to enhance the visibility and effectiveness of security operations by integrating and correlating data from various security tools and platforms. Often augmented with managed services, this SaaS offering provides holistic and unified cyber defense capabilities to simplify the management and operation of security products, processes, and data.

As enterprises increasingly encounter an evolving threat landscape and complex security challenges with workforces in multicloud, hybrid environments, XDR presents a more efficient, proactive solution. In contrast to solutions like endpoint detection and response (EDR), XDR broadens the scope of security across an organization's complete attack surface.

When attackers use creative, modern techniques, threats can hide and weave between security silos, spreading slowly over time to evade detection and gain stealthy persistence. This leads to security staff trying to triage and investigate the problem as it hits different parts of the business network. Traditional security tools, such as antivirus software or firewalls, typically operate in silos, making it difficult to detect and respond to coordinated cyber threats that cross critical thresholds.

XDR addresses this limitation by taking a broader approach to find these threats, looking at the bigger picture across multiple security layers - endpoint, server, email, identity, network, and cloud. By consolidating data and applying advanced analytics such as Artificial Intelligence and Machine Learning, XDR can provide a more holistic view of security incidents and enable faster and more accurate threat detection and response to end cyberattacks and minimize business disruptions.

2. What type of XDR solutions are available today?

In the market today, several vendors offer XDR solutions, each with its own set of definitions, features, and capabilities for effective and efficient response to advanced cyber attacks. While there are many XDR solutions available, not all are created equal or deliver the same type of value.

An effective XDR solution should ingest telemetry not only from endpoints, but also from the multiple security toolsets and platforms that the organization has deployed, which will ultimately maximize the value of existing solutions while also reducing the dependency of human resources along the journey. As the XDR landscape is continuously evolving, new innovations and offerings will emerge over time as organizations seek comprehensive and integrated security solutions.

XDR TYPES

NATIVE XDR

is built and provided by a single vendor as a cohesive and integrated offering. In a native XDR solution, all the components and functionalities required for Extended Detection and Response are developed, maintained, and delivered by the same vendor. The objective is to leverage existing tools within a single vendor to optimize the security outcome and investment.

OPEN XDR

In contrast, Open XDR vendors emphasize the interoperability with open platforms that aggregate telemetry and security data from diverse sources, and allow organizations to integrate multiple security products, regardless of the vendor, into a unified XDR system. This approach provides flexibility and scalability to organizations and allows them to build a comprehensive XDR framework tailored to their specific security needs and optimize investment of their existing infrastructure.

SIEM-BASED XDR

A SIEM-based XDR solution combines the traditional capabilities of a Security Information and Event Management (SIEM) system with the advanced threat detection and response functionalities of XDR. It integrates the log and event data collection, correlation, and analysis capabilities of a SIEM with additional features aimed at improving threat detection and response across multiple security domains.

3. What is the difference between XDR, SIEM, & SOAR?

XDR, SIEM and SOAR are all cybersecurity solutions that address different aspects of threat detection, response, and overall security operations.

- **Extended Detection and Response (XDR):** XDR is the latest concept that aims to provide comprehensive threat detection and response capabilities by integrating and correlating data from various security tools and platforms. It goes beyond traditional siloed approaches by collecting and analyzing data from endpoints, networks, servers, and cloud environments. XDR leverages advanced analytics and automation to detect and respond to advanced threats, offering a unified view of security incidents across an organization's broader attack surface.
- **Security Information and Event Management (SIEM):** SIEM is a technology that collects and analyzes log data and security events from various sources within an organization's IT infrastructure. SIEM solutions aggregate and correlate this data to identify patterns, anomalies, and potential security incidents. SIEM provides real-time monitoring, alerting, and reporting capabilities, helping security teams gain visibility into security events and enabling proactive threat detection. SIEM is typically focused on log and event data and often requires manual configuration, customization and tuning to meet specific security needs.
- **Security Orchestration, Automation, and Response (SOAR):** SOAR platforms automate and orchestrate security operations tasks and processes, including incident response, threat hunting, and remediation. SOAR solutions require manual integration with different security tools and systems to collect and analyze security alerts and events. They provide workflows, playbooks, and case management capabilities to streamline and automate incident response actions. SOAR platforms enable security teams to improve operational efficiency, reduce response times, and enforce consistent and repeatable processes.

In summary, the main differences between XDR, SIEM & SOAR are:

- **Scope:** XDR covers a broader range of security layers and collects data from multiple sources, including endpoints, workspaces, identity solutions, networks, and cloud environments. SIEM primarily focuses on log and event data, while SOAR integrates with various security tools and streamlines incident response processes.
- **Integration:** XDR integrates and correlates data from different security tools and platforms to provide a unified view of security incidents including full situation awareness and the malicious attack story into a visual attack tree. SIEM collects and analyzes log data from various sources and relies on SOAR to integrate with different security tools and orchestrate their actions.
- **Analytics:** XDR leverages advanced analytics, such as artificial intelligence, machine learning and behavioral analysis, to detect sophisticated threats. SIEM utilizes customized correlation rules and predefined algorithms to identify sets of patterns and anomalies. SOAR platforms focus on automating and orchestrating incident response tasks and processes.
- **Timeframe:** XDR provides real-time threat detection and response capabilities in a single platform. SIEM offers real-time monitoring and alerting. SOAR facilitates rapid and automated incident response actions from SIEM alerts.

Both XDR and SIEM & SOAR solutions have their own advantages and considerations.

XDR:

Pros

COMPREHENSIVE THREAT DETECTION:
XDR collects and analyzes data from multiple security layers, providing a holistic view of the organization's security posture and enabling the detection of sophisticated and coordinated attacks that span across different systems.

ADVANCED ANALYTICS:
XDR leverages advanced analytics techniques, such as AI, machine learning and behavioral analysis, to detect and respond to emerging threats and anomalies, improving the accuracy of threat detection and reducing false positives.

INTEGRATED RESPONSE:
XDR offers automated response actions and workflows, allowing security teams to quickly respond to security incidents and automate remediation processes in one unified defense platform. It facilitates a coordinated and streamlined approach to incident response across multiple security tools and platforms.

IMPROVED EFFICIENCY:
By consolidating security data and providing a unified view of incidents, XDR reduces the time and effort required for manual correlation and investigation. It enhances the efficiency of security operations by providing contextualized insights and actionable intelligence.

Cons

DEPLOYMENT COMPLEXITY:
Implementing an XDR solution may require significant integration efforts, as it involves collecting and correlating data from various security tools and platforms. Organizations need to ensure compatibility and proper configuration to achieve optimal results.

VENDOR LOCK-IN:
Native XDR solutions often come bundled with specific vendor ecosystems, which may limit flexibility and interoperability with existing security investments. Organizations should carefully consider vendor lock-in and evaluate integration capabilities.

CUSTOMIZABILITY:
XDR solutions are less flexible for creating custom correlation rules, dashboards, and reports compared to SIEM. Its main focus is on stopping attacks from progressing further, and typically offer basic traditional compliance use-cases at this stage.

SIEM & SOAR:

Pros

LOG AND EVENT ANALYSIS:
SIEM solutions excel at collecting, aggregating, and analyzing log and event data from various sources, providing real-time monitoring, alerting, and reporting capabilities. They offer deep visibility into security events and can identify potential threats based on predefined correlation rules.

CUSTOMIZABILITY:
SIEM solutions can be tailored to an organization's specific needs by creating custom correlation rules, dashboards, and reports. They allow organizations to define specific security policies and fine-tune the system to align with their unique security requirements.

PROCESS AUTOMATION:
SOAR platforms automate and orchestrate security operations tasks, reducing manual effort and response times. They streamline incident response workflows, enforce consistent processes, and integrate with various security tools to automate response actions.

COMPLIANCE AND REPORTING:
SIEM solutions provide valuable audit and compliance capabilities, allowing organizations to meet regulatory requirements and demonstrate adherence to security policies. They offer reporting functionalities to generate compliance reports and track security incidents.

Cons

ALERT OVERLOAD:
SIEM solutions can generate a large number of alerts, leading to alert fatigue and potentially causing important alerts to be overlooked or ignored. Proper tuning and customization are required to manage and prioritize alerts effectively.

LIMITED SCOPE:
SIEM solutions primarily focus on log and event data, which may not provide a comprehensive view of security incidents. They may not capture threats that occur outside the logged events or have limited visibility into the behavior of endpoints or cloud environments.

RESPONSE ORCHESTRATION COMPLEXITY:
While SOAR platforms automate incident response actions, implementing and configuring response playbooks can be complex. Organizations need skilled personnel to design and maintain the automation workflows effectively.

INTEGRATION CHALLENGES:
Integrating SIEM and SOAR solutions with existing security tools and platforms can be a complex task, requiring compatibility and proper configuration. Integration efforts may vary based on the ecosystem and APIs provided by different vendors.

It's important to note that the pros and cons mentioned above are general considerations, and the actual benefits and challenges may vary based on specific vendor offerings, implementation strategies, and the organization's unique requirements. Organizations should thoroughly evaluate the features, capabilities, and integration possibilities of XDR, SIEM, and SOAR solutions for informed decision making.

It's worth noting that XDR, SIEM, and SOAR are not mutually exclusive. Organizations may choose to adopt one or a combination of these solutions to build a comprehensive and layered security architecture based on their specific needs and requirements (e.g., balancing the risk of legal and regulatory compliance vs. cyber defense capability to end malicious attacks).

4. What is Managed XDR and its benefits?

Managed XDR (M-XDR) service refers to the outsourcing of XDR capabilities to a third-party service provider. With M-XDR, organizations partner directly with an XDR vendor or a managed security service provider (MSSP) to oversee and manage their XDR solution and security operation on their behalf. Key components and features of a managed XDR service include:

- **Monitoring and Alerting:** The managed service provider continuously monitors the organization's security environment using the XDR solution. They analyze security events, alerts, and incidents generated by the XDR solution and provide real-time notifications to the organization's security team.
- **Threat Detection and Analysis:** The managed service provider utilizes advanced analytics and threat intelligence to detect and analyze security threats. They identify suspicious activities, signs of compromise, and indicators of advanced threats by correlating and analyzing security data from various sources.
- **Incident Response and Remediation:** The managed service provider offers incident response capabilities to help organizations swiftly respond to security incidents. They work closely with the organization's internal security team to investigate and contain incidents, develop response strategies, and facilitate remediation actions.
- **Proactive Threat Hunting:** M-XDR services often include proactive threat hunting. The managed service provider employs security analysts who proactively search for signs of compromise and potential threats within the organization's network and endpoints. They conduct in-depth investigations to uncover hidden or advanced threats that may evade automated detection.
- **Expert Security Analysis and Guidance:** The managed service provider's team of security experts provides analysis and insights into security incidents, trends, and emerging threats. They offer recommendations and guidance to the organization's security team on improving security controls, implementing best practices, and optimizing the XDR solution.
- **Continuous Improvement and Optimization:** The managed service provider continuously reviews and updates the XDR solution configuration, rules, and policies to ensure optimal performance and effectiveness. They stay up to date with the evolving threat landscape and implement necessary adjustments to enhance the organization's security posture.
- **Reporting and Compliance Support:** M-XDR services include reporting capabilities to provide organizations with visibility into their security posture. The managed service provider generates regular reports on security incidents, threat trends, and compliance-related metrics. These reports help organizations demonstrate compliance with industry regulations and internal security policies.
- **Scalability and Flexibility:** M-XDR services are scalable and flexible to accommodate the organization's changing needs. The managed service provider can adjust resources, monitoring levels, and response capabilities based on the organization's security requirements, ensuring that the service aligns with the organization's growth and evolving threat landscape.

When leveraging M-XDR services, organizations can benefit from expert security capabilities, proactive threat hunting, round-the-clock monitoring, and incident response support while reducing the burden of managing and maintaining an XDR solution internally. M-XDR services can be particularly valuable for organizations that lack the internal resources or expertise while still maintaining control and visibility over their security posture. This enables organizations to focus on their core business operations while ensuring robust security measures are in place. For example:

- **Access to Expertise:** M-XDR services provide access to a team of experienced security professionals who specialize in XDR technologies. These experts have the knowledge and skills to effectively monitor, detect, and respond to security threats using the XDR solution. By leveraging their expertise, organizations can enhance their security capabilities without the need to hire and train additional staff.
- **24/7 Monitoring and Response:** M-XDR services typically offer round-the-clock monitoring of security events and incidents. Security analysts continuously monitor the organization's environment, detect potential threats, and respond promptly to security incidents, ensuring a rapid and effective response regardless of the time of day to assure service continuity.
- **Cost Savings and Predictable Expenses:** M-XDR services offer cost savings compared to building and maintaining an in-house security operations center (SOC) and XDR infrastructure. Instead of investing in hardware, software licenses, talents, training, and ongoing maintenance, organizations can leverage the expertise and infrastructure of the managed service provider. Additionally, managed services often follow a subscription-based model, providing predictable expenses and avoiding large upfront investments.

5. How can XDR enhance cyber resilience?

XDR can be beneficial for existing Security Operations Centers (SOCs), or organizations that outsource their security operations to managed service providers, for responding to and remediating security issues faster and more efficiently with automated actions and proven playbooks embedded as part of managed XDR services.

For Existing SOCs:

- **Enhanced Detection and Response:** XDR solutions provide advanced threat detection capabilities, leveraging multiple security data sources and employing analytics and machine learning techniques. This enhances the SOC's ability to detect and respond to a wide range of threats, including sophisticated and evasive attacks.
- **Centralized Visibility and Control:** XDR solutions offer a unified view of security events and incidents across endpoints, networks, cloud environments, and other data sources. This centralization of security data enables SOC analysts to have comprehensive visibility into the organization's security posture and facilitates efficient monitoring, analysis, and response.
- **Improved Efficiency and Automation:** XDR solutions automate several security operations tasks, such as threat hunting, investigation, and response workflows. This automation helps SOC analysts streamline their workflows, reduce manual effort, and focus on critical tasks, thereby improving overall operational efficiency and effectiveness.
- **Threat Intelligence Integration:** XDR solutions often integrate with external threat intelligence feeds, enriching security data with up-to-date information about emerging threats and attack patterns. This integration enhances the SOC's ability to detect and respond to new and evolving threats effectively.
- **Collaboration and Incident Management:** XDR solutions often provide features for collaboration and case management, enabling SOC analysts to work together efficiently. They can share information, collaborate on investigations, and manage incidents within a centralized platform, improving communication and coordination among SOC team members.

For Organizations Outsourcing Security Operations:

- **Enhanced Threat Detection and Response:** XDR solutions deployed by managed service providers can deliver improved threat detection capabilities across the organization's infrastructure. This helps ensure comprehensive coverage and timely response to security incidents, leveraging the expertise and resources of the vendor.
- **Access to Advanced Technologies:** XDR solutions used by managed service providers typically incorporate advanced technologies, such as machine learning, behavioral analytics, and threat intelligence integration. These technologies can augment the managed service provider's capabilities, enabling them to offer more robust and effective security services.
- **24/7 Monitoring and Support:** XDR solutions enable continuous monitoring of the organization's environment, allowing the managed service provider to deliver round-the-clock security monitoring and support. This ensures prompt detection and response to security incidents, regardless of the time zone or operational hours.
- **Efficient Incident Management and Reporting:** XDR solutions help managed service providers streamline incident management processes, enabling efficient handling, investigation, and resolution of security incidents. The solutions provide reporting and analytics capabilities that allow MSSPs to deliver comprehensive reports and insights to their clients.
- **Scalability and Flexibility:** XDR solutions used by managed service providers are designed to scale and adapt to the evolving needs of their clients. They can handle large volumes of security data, support diverse IT environments, and accommodate the requirements of multiple clients simultaneously.

By leveraging XDR solutions, both existing SOCs and organizations outsourcing security operations to managed service providers **can benefit from improved threat detection, response capabilities, efficiency gains, enhanced collaboration, and access to advanced technologies.** XDR helps strengthen their security posture and enables more effective protection against evolving cyber threats.

6. What are key considerations when evaluating XDR solutions?

When evaluating XDR solutions, several key requirements should be considered to ensure that the chosen XDR solution meets the organization's specific security needs and aligns with their overall cybersecurity strategy. Some key requirements to evaluate when considering XDR solutions include:

- **Threat Detection Capabilities:** Assess the XDR solution's ability to detect a wide range of threats, including known and unknown malware, advanced persistent threats (APTs), insider threats, lateral movement, data exfiltration, and other sophisticated attack techniques. Evaluate the solution's detection techniques, such as behavioral analysis, machine learning, threat intelligence integration, and anomaly detection.
- **Integration and Interoperability:** Determine the solution's integration capabilities with existing security tools, platforms, and data sources. Evaluate the ease of integration, compatibility with different vendor ecosystems, and the ability to collect and correlate data from endpoints, networks, servers, cloud environments, and other relevant sources. Ensure that the XDR solution can provide a unified view of security incidents and enable effective collaboration with other security technologies.
- **Automation and Orchestration:** Assess the XDR solution's automation and orchestration capabilities. Look for features such as automated response actions, playbooks, workflows, and case management functionalities. Evaluate the flexibility and ease of customization to accommodate specific incident response processes and enable streamlined, consistent, and efficient security operations.
- **Analytics and Contextualization:** Evaluate the XDR solution's analytics capabilities. Consider the depth and accuracy of analysis, the use of advanced analytics techniques (e.g., machine learning, behavioral analytics), and the ability to provide actionable intelligence and contextualized insights to security teams. Look for features like threat hunting capabilities, visualizations, and reporting functionalities.
- **Scalability and Performance:** Assess the XDR solution's scalability and performance. Consider its ability to handle increasing data volumes, support a growing number of endpoints and security events, and maintain real-time or near-real-time threat detection and response capabilities. Evaluate the solution's resource utilization, latency, and impact on the overall network and system performance.
- **Security and Compliance:** Evaluate the XDR solution's security features and compliance capabilities. Look for robust access controls, encryption mechanisms, authentication protocols, and secure data handling practices. Assess the solution's ability to support regulatory compliance requirements, generate audit trails, provide logging capabilities, and facilitate compliance reporting.

- **Vendor Support and Reputation:** Consider the reputation and reliability of the XDR solution vendor. Evaluate their track record in the cybersecurity industry, customer support capabilities, response times for support requests, and ongoing product updates, including patches and vulnerability management.
- **Total Cost of Ownership (TCO):** Evaluate the total cost of ownership associated with the XDR solution, considering factors such as licensing fees, implementation costs, maintenance and support costs, and any additional costs related to infrastructure or staffing requirements. Assess the value proposition and ROI the solution offers in terms of improved security outcomes and operational efficiencies.
- **Future Roadmap and Innovation:** Consider the XDR solution vendor's future roadmap and commitment to innovation. Assess their ability to adapt to evolving threat landscapes and introduce new features and capabilities to address emerging security challenges. Evaluate their vision for XDR and their investment in research and development.

By evaluating these key requirements, **organizations can make an informed decision when selecting an XDR solution that best aligns with the organization's security strategy,** addresses their specific needs, and provides a strong foundation for effective threat detection and response.

7. How to evaluate XDR with MITRE ATT&CK integration

Evaluating XDR with MITRE ATT&CK integration is an effective approach to assess the solution's ability to align with and leverage the MITRE ATT&CK framework for threat detection, analysis, and response. MITRE ATT&CK provides a comprehensive knowledge base of adversary tactics, techniques, and procedures (TTPs) that organizations can use to enhance their cybersecurity defenses. Here's how you can evaluate XDR with MITRE ATT&CK integration:

- **Mapping to MITRE ATT&CK:** Assess how well the XDR solution maps its detection capabilities and alerts to the MITRE ATT&CK framework. Determine whether the solution provides visibility into specific adversary techniques and whether it can generate alerts or reports that reference relevant ATT&CK techniques.
- **Detection Coverage:** Evaluate the XDR solution's coverage of the MITRE ATT&CK framework. Determine the extent to which the solution can detect a wide range of techniques across various stages of the attack lifecycle, including initial access, persistence, privilege escalation, lateral movement, exfiltration, and more.
- **MITRE ATT&CK Analytics:** Check if the XDR solution incorporates MITRE ATT&CK analytics or rule sets to enhance threat detection. This can include leveraging behavioral analytics, machine learning, or specific algorithms that align with ATT&CK techniques to improve the accuracy and efficacy of detection.
- **Threat Hunting with MITRE ATT&CK:** Assess the XDR solution's capability to perform threat hunting activities based on the MITRE ATT&CK framework. Evaluate whether the solution enables security analysts to proactively search for specific TTPs, investigate suspicious activities, and identify potential indicators of compromise (IOCs) aligned with ATT&CK techniques.
- **Reporting and Visualization:** Determine whether the XDR solution provides reporting and visualization features that leverage the MITRE ATT&CK framework. Look for reports or dashboards that display ATT&CK mappings, show the prevalence of specific techniques, or provide insights into the organization's security posture against various ATT&CK groups.

- **Remediation and Response Guidance:** Evaluate if the XDR solution offers remediation and response guidance aligned with MITRE ATT&CK. Check whether it provides actionable recommendations, playbooks, or response workflows that guide security teams on mitigating or responding to specific ATT&CK techniques effectively.
- **Threat Intelligence Integration:** Assess whether the XDR solution integrates with external threat intelligence feeds that incorporate MITRE ATT&CK data. Evaluate if the solution can leverage ATT&CK-based threat intelligence to enhance detection, contextualize alerts, and prioritize response actions.
- **Continuous ATT&CK Updates:** Determine if the XDR solution stays up to date with the latest updates and additions to the MITRE ATT&CK framework. Assess whether the solution vendor actively incorporates new ATT&CK techniques, tactics, or groups into their detection capabilities and ensures ongoing alignment with the evolving threat landscape.

By evaluating XDR solutions with MITRE ATT&CK integration, **organizations can benefit from enhanced threat detection and response capabilities, better contextualization of alerts, improved threat hunting,** and the ability to align their security operations with a widely recognized and comprehensive framework like MITRE ATT&CK.

8. What are the effective metrics to measure XDR deployment?

When measuring the performance of an XDR solution, several Service Level Objective (SLO) metrics can be defined to assess its effectiveness and efficiency. These metrics help evaluate the solution's performance in detecting and responding to security threats. Here are some SLO metrics that can be considered when measuring XDR performance:

- **Event and Log Ingestion Rate:** This metric measures the XDR solution's ability to ingest, process, and analyze security events and logs from various sources. It assesses the solution's scalability and performance in handling high volumes of data.
- **Detection Accuracy:** This metric assesses the accuracy of the XDR solution's threat detection capabilities. It measures the percentage of true positives (actual threats detected correctly) and false positives (false alarms or misidentifications) generated by the solution.
- **Service Availability Up Time:** XDR should be highly reliable and available with built-in redundancy, failover mechanisms, and resilience to ensure continuous operation and minimize downtime.
- **False Negative Rate:** The false negative rate measures the percentage of security incidents or threats that were not detected by the XDR solution. It indicates the solution's ability to avoid missing potential threats or overlooked malicious activities.
- **False Positive Rate:** The false positive rate measures the percentage of alerts or notifications generated by the XDR solution that are determined to be false alarms or non-malicious events. It reflects the solution's ability to reduce unnecessary alerts and prevent alert fatigue for security analysts.
- **Mean Time to Detect (MTTD):** MTTD measures the average time it takes for the XDR solution to detect a security incident from the time it occurred. It reflects the solution's ability to identify threats promptly and initiate the investigation process.
- **Mean Time to Investigate (MTTI):** MTTI metric measures the average time it takes for security analysts to investigate a security incident or alert triggered by the XDR solution. It includes the time required to gather additional information, analyze data, and determine the severity and impact of the incident.
- **Mean Time to Respond/Remediate (MTTR):** MTTR measures the average time it takes for the XDR solution to respond or contain to a security incident once it has been detected. It includes the time required for investigation, containment, eradication, and recovery processes.

It is important to define these SLO metrics in collaboration with the XDR solution vendor and align them with the organization's specific security objectives and operational requirements. Regular monitoring and analysis of these metrics can help track the performance of the XDR solution, identify areas for improvement, and ensure it meets the desired performance targets.