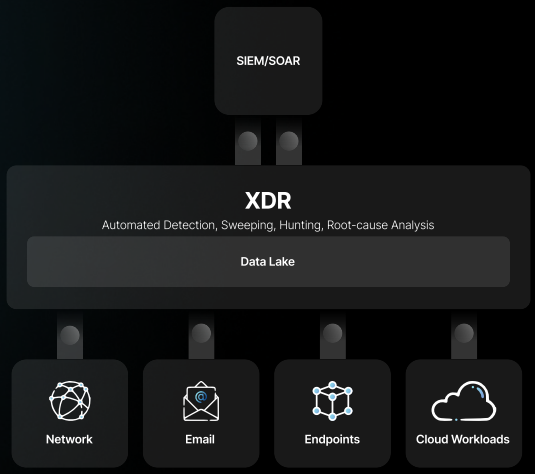
metron security

NEXT LEVEL SECURITY WITH XDR INTEGRATION

A STUDY IN UTILITY



Discover the transformative impact of Extended Detection and Response (XDR) on achieving leading-edge security. XDR enables holistic threat detection and response, centralizing data collection and analysis for a unified view of threats across the IT environment, resulting in a more efficient and effective security posture.

Common problems you might encounter when integrating in-house:

- Verifying the accuracy and effectiveness of the integration: In-house security teams must develop test scenarios and monitor the XDR platform for false positives or missed detections, which can be time-consuming.
- Ensuring both the XDR platform and yours are updated: Maintaining compatibility often requires ongoing adjustments to the integration code, and critical updates might be overlooked.
- In-house development introduces potential security vulnerabilities: Improper data handling and coding errors have the possibility of creating gaps in your overall security.
- Planning for the future can be difficult: If the integration is customized for a specific XDR platform without additional considerations, it could make switching to a different platform, in the future, difficult.
- Integration and maintenance require an ongoing effort from your security team: Putting resources into this process can create an ongoing strain on your resources and take your team's attention away from other important tasks

Leverage the Benefits of an XDR Platform

- Unified Visibility: XDR gathers data from various security tools across the organization's IT infrastructure, providing a holistic view of potential threats. This eliminates blind spots and helps identify sophisticated attacks that might otherwise go unnoticed by siloed security solutions.
- Reduced Alert Fatigue: XDR correlates data from multiple sources, filtering out false positives generated by individual security tools. This frees up security personnel to focus on genuine threats, improving overall efficiency.
- Faster Threat Hunting: XDR allows for faster investigation and mitigation of threats by providing a central platform to analyze all relevant data. Security teams can trace the entire attack timeline across various systems, leading to quicker containment.
- Advanced Threat Protection: XDR integrates threat intelligence feeds, enabling your solution to identify and block known attack methods. Additionally, this approach leverages machine learning to detect zero-day threats and anomalies that might indicate malicious activity.
- Reduced operational complexity and costs: XDR replaces multiple point solutions with a single platform, simplifying security management. By automating tasks and improving efficiency, XDR can also lead to significant cost savings.
- Enhanced incident prioritization: XDR uses advanced analytics to assess the risk of each incident, helping security teams focus on the most critical threats. This prioritization ensures that resources are allocated effectively and incidents are addressed in a timely manner.

Metron Advantage

Expertise: Well-built and continually-supported security integrations for any-sized organization.

Fully-Managed: Complete oversight on the end-to-end process of development, customization, app certification, and continued on-demand support.

Streamlined: Metron Security maintains coding standards, merges PR, and coordinates with the AWS team for all updates.

Speed: Get started within 24 hours with up to 2x-3x cost savings compared to in-house.

Zero Risk: Fixed cost and no upfront payment. Invoiced only after delivery.

About Metron

Metron empowers security teams by streamlining security operations. We integrate and automate solutions for over 200 security tools, including Splunk and QRadar. Our expertise spans standard integrations, custom SOAR playbooks, and Security Data Lakes, ensuring an efficient security posture for your organization.

Case Studies

01 | XDR + BAS for Enhanced Control and Insights

Integrating Extended Detection and Response (XDR) tools with a Breach and Attack Simulation (BAS) platform offers a powerful solution for organizations seeking to defend their networks.

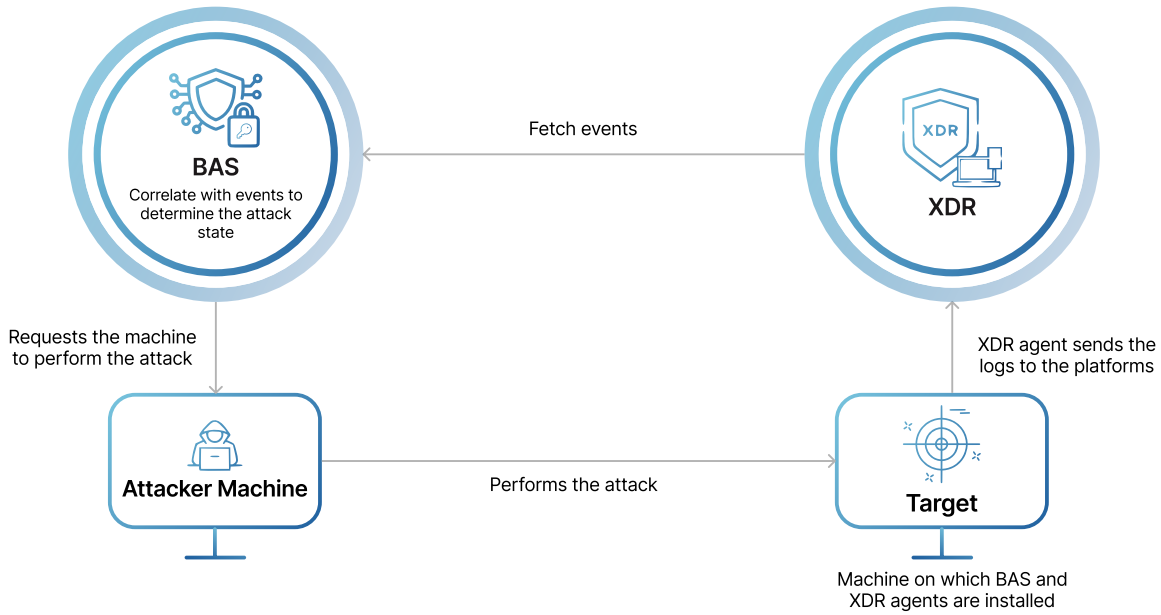
When XDR and BAS work together, they create a powerful security ecosystem:

- **BAS validates security controls:** By simulating attacks, BAS highlights weaknesses in your defenses. This allows for prioritization and rectification of vulnerabilities before a real attack occurs.
- **XDR leverages BAS insights:** Insights from BAS simulations can be used by the XDR platform to refine its detection rules. This improves the accuracy of threat identification by focusing on activities that mimic real attack patterns.

The XDR platform reacts to attacks that are simulated by the BAS platform as follows:

If the XDR platform is able to block the attack, security events are generated notifying the security teams. However, if the attack bypasses defenses, events are still generated, but alerts may not be triggered. This helps identify areas where security controls need improvement.

The integration of XDR and BAS creates a continuous security improvement cycle. BAS proactively identifies weaknesses, while XDR provides a comprehensive view of threat detection and response.



02 | XDR + XSOAR + IoT for Streamlined Intelligence

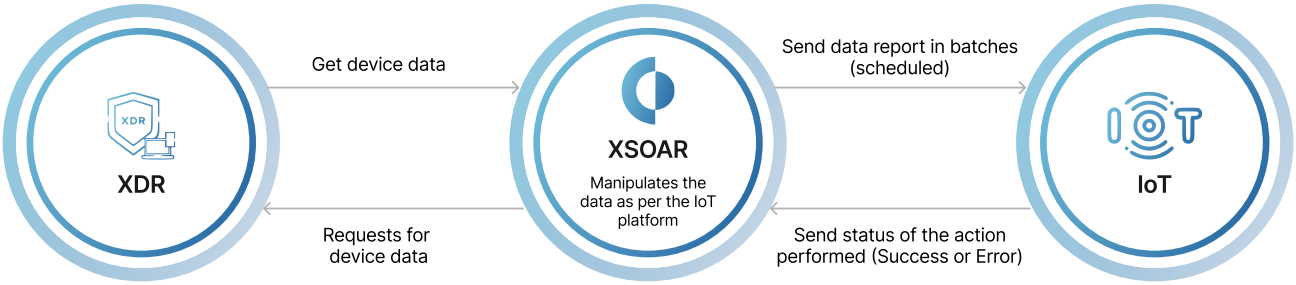
This integration streamlines how you manage your Internet of Things (IoT) security by leveraging the power of Extended Detection and Response (XDR) with XSOAR.

Data Flow:

- Security data is fetched from the XDR platform.
- XSOAR acts as a bridge, mapping the fetched data to the specific requirements of the IoT platform.

Benefits of this integration:

- **Enhanced Device Attributes:** XSOAR fills in missing or inaccurate details about devices within the IoT platform. This includes information like operating system version, MAC address, IP address, and hostname, resulting in more complete device profiles.
- **Improved Risk Identification:** XDR leverages risk information from XSOAR's endpoint protection. This comprehensive data allows XSOAR to perform a more thorough risk assessment for IoT devices, enabling better prioritization of security threats.



03 | XDR + IAM for Cohesive Insights and Alerts

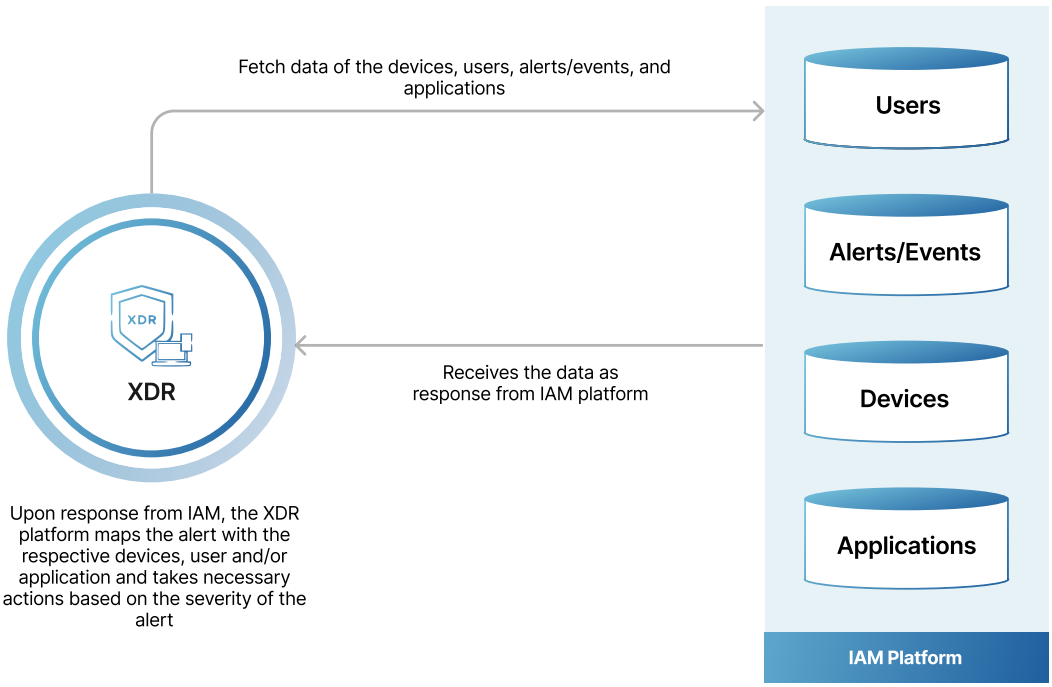
This integration between an XDR platform and an IAM aims to enrich the XDR with valuable data such as user information, device details, application activity, security alerts, and system telemetry.

In this integration:

- **XDR Platform:** Utilizes AI and behavioral analytics to proactively identify and respond to security threats. It provides a unified view across various security domains, offering comprehensive visibility.
- **IAM Solution:** Centralizes user access management for various personnel groups. It simplifies secure access to applications through single sign-on (SSO), multi-factor authentication (MFA), and user lifecycle management.

This approach empowers security teams to:

- **Identify risky user behavior:** Correlate user activity with network and endpoint events to detect potential threats before a breach occurs.
- **Gain context for security alerts:** Enrich security alerts with user and device context for faster and more informed decisions when responding.
- **Improve investigation efficiency:** Simplify threat investigations by providing an aggregated view of user, device, and application data.



About Metron

Metron Security provides on-demand and effective approaches to managing third-party integrations for security ecosystems. Since 2014, Metron has delivered automation solutions for 200+ security applications along with several hundred custom automation solutions.

Metron is trusted by many of the world's fastest-growing security companies and managed security service providers (MSSPs) owing to their transparent development processes, their expertise in understanding security products, and their fixed-cost model. Clients have experienced shorter development times and 2x-3x cost savings compared to deploying internal engineering teams for the same tasks.

Contact Us

prashant@metronlabs.com
www.metronlabs.com
+1 888 840 3282 (DATA)

AICPA SOC 2 Formerly SAS 70 Reports

SafeBreach ZEROFOX cybereason
paloalto NETWORKS DEVO digital shadows a ReliaQuest company