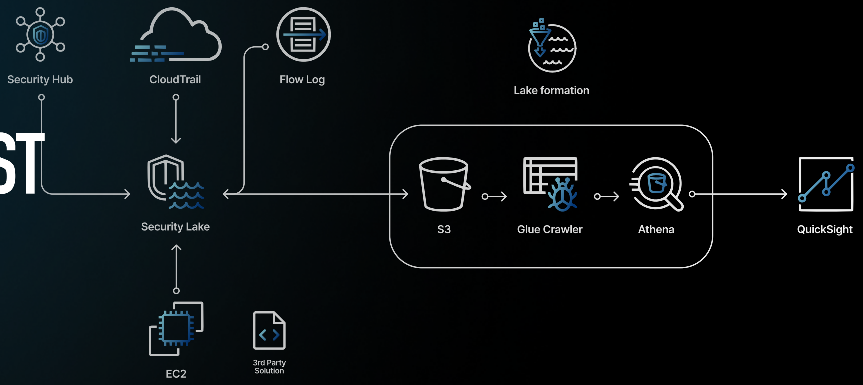
metron security

LEVERAGE THE CLOUD-FIRST POWER OF AMAZON'S SECURITY PORTFOLIO



Effortlessly Connect with the AWS Security Ecosystem

Avoid these common problems of going solo or integrating in-house:

- Your engineers would have to spend time researching and setting up Amazon Security tools.
- If there is a new API or version change, you will have to pull valuable engineering resources to quickly fix the underlying problem.
- It can be difficult and complex to coordinate IAM roles, data access policies, and security configurations across various AWS services like S3, Lambda, and EC2.
- In-house development efforts may not address all technical issues like missing commands, API availability loss, event transmission/capture failure, etc.
- Having expertise in managing granular permission in order to avoid over-privilege and potential access leaks is a must.
- Managing the integration requires ongoing effort to build and maintain the integration code, monitor its performance, and troubleshoot. This can strain internal resources.
- Keeping third party libraries updated to fix vulnerabilities can be time consuming when done in-house.
- It is crucial to have dedicated resources to keep up with regular security updates for various AWS services and application dependencies.
- Your team must ensure there is sufficient collaboration between development, security, and operations teams which can otherwise lead to security gaps and vulnerabilities.

Empower Your App with OCSF and AWS Security

Metron Security simplifies your security integration with AWS using the Open Cybersecurity Schema Framework (OCSF) and AWS Security Lake. This powerful combination enables:

- **Unified Data Ingestion:** Seamlessly ingest security data from AWS and leading security providers like Cisco and Palo Alto Networks for comprehensive analysis.
- **Simplified Management:** Leverage OCSF's standardized format for easier data interpretation and reduced complexity.
- **Enhanced Threat Detection:** Gain a consolidated view of your security posture across different platforms, facilitating swift threat identification and response.

Our expertise further enhances your experience by:

- **Configuring AWS Services:** We will ensure your security solution is seamlessly integrated within the AWS ecosystem.
- **Building Custom Playbooks:** Our team will develop specific responses for various security scenarios within leading SOAR platforms.

Amazon Security Lake Capabilities

Deep Expertise with AWS Security: Benefit from our experience in developing end-to-end solutions using AWS security features.

Open Cybersecurity Schema Framework (OCSF) Integration: Leverage the power of OCSF to ingest data from leading security providers like Amazon, Cisco, CrowdStrike, SentinelOne, Palo Alto Networks, and several others.

Configuration and Integration Guidance: Our team can assist you in configuring AWS services and implementing your integration solution, ensuring smooth functionality and compatibility.

AWS Marketplace Support: If you plan to publish your app on the AWS Marketplace, we provide guidance in building and certifying your app to meet the platform's requirements.

Top Use Cases: Amazon Security Lake + XDR

01 | Ingest from Multiple Platforms

Use Amazon Security Lake as the source of security events. Ingest logs from multiple security vendors with a single integration. This ensures that your customers have centralized access to critical security data across multiple vendors.

02 | Enhanced Log Visualization

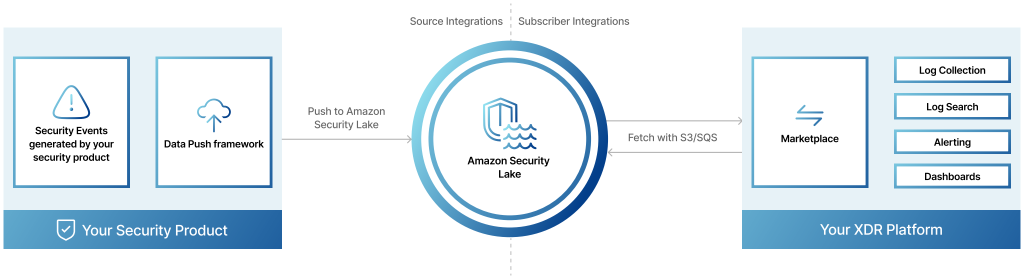
With the integration in place, you can visualize security logs in a more meaningful manner within the XDR Platform. This allows you to gain valuable insights into security events and quickly identify patterns or anomalies, empowering you to make informed decisions sooner.

03 | Effortless Data Search

A standard, normalized schema means you can correlate events across multiple security vendors. You can utilize various options and categories to search for specific information, allowing you to rapidly locate the data you need for effective threat detection and response.

04 | Highlighted Important Fields

The XDR platform highlights important fields such as source IP, destination IP, and details or error messages within the logs. This helps you prioritize and focus on critical security information, ensuring that you don't miss any key insights during your investigations.



Example of an Amazon Security Lake Data Ingested App

05 | OCSF Schema Compatibility

The integration utilizes the Open Cybersecurity Schema Framework (OCSF), enabling you to search across vendors and analyze security data using a standardized schema. This simplifies the process of extracting insights and intelligence from the collected data, promoting interoperability and collaboration.

06 | Dashboards and Visualization

XDR platforms provide powerful dashboards and visualization capabilities that allow you to effectively analyze and interpret security data from Amazon Security Lake and XDR. You can create customized dashboards tailored to your specific needs, enabling you to monitor and track security events in real-time.

07 | Cross-Account Access

The integration uses a SQS queue and S3 bucket (standard features of Amazon Security Lake) for secure and efficient data transmission. Cross-account access is utilized to ensure seamless communication between the customers AWS Security Lake and your XDR platform, while removing the need for handling access and secret keys.

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.

Contact Us

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