Plan Your Amazon Security Lake Journey

Questions to ask on the road to democratizing your security data with AWS and Industry Leaders

1. Data ingestion

What logs are you currently collecting and why?
Identify the logs you need to keep to enhance the protection of your data and workloads.

2. Data collection

Is there a use case for collecting these logs or a compliance mandate?
With Amazon Security Lake, you centralize data from AWS environments, SaaS providers, on premises, and cloud sources into a purpose-built data lake stored in your account.

3. Data processing

How does Security Lake process and analyze data?
With support for OCSF (Open Cybersecurity Schema Framework), Amazon Security Lake centralizes, transforms, and makes your security data available to your preferred analytics tools, removing inconsistencies.

4. Data analytics

How is data analytics used to extract valuable insights from Security Lake?
Apply analytical tools and services from AWS and AWS Partners to extract meaningful patterns and identify trends and anomalies in the processed data.

5. Detection and response

How can Security Lake be used for security log analytics, investigations, threat hunting, and other applicable use cases?
Detect potential security threats and unusual activities from your data across your entire organization using your analytics tool of your choice in a common open source format while retaining complete control and ownership over that data.

6. Data Reporting and Visualization

How can you effectively utilize data reporting and visualization techniques to derive insights?
Translate valuable insights into visual reports and intuitive dashboards to facilitate informed decision-making and enhance communication.

7. Data Retention

What key considerations should be discussed when planning for data storage and retention of logs?
You can securely store pertinent data in Amazon Simple Storage Service with customizable retention settings for compliance, historical analysis, and future references. Utilize Amazon S3 tiering to effectively manage storage costs by implementing data retention policies.

8. Continuous Improvement

How do you plan to continuously enhance the security of your workloads, applications, and data?
You must regularly assess and refine strategies to effectively address evolving security challenges.

9. Conclusion

Do you have a data lake to help you improve your security posture and compliance mandates?
Do you have a data lake to help you improve the protection of your data and workloads? Start building your Security Lake now with a 15-day trial.