HOOP cyber

HOOP Lake

Introducing HOOP Lake - a Data Centric Approach to Cyber Security Operations - Powered by AWS

At HOOP Cyber we believe that Cyber Security is fundamentally a Data Problem. The HOOP Lake approach Is set to change the way Security teams identify and combat emerging threats, enabling the broader retention of data for longer - optimised for search and addresses the challenge of how to detect threats across all your data in whatever format of wherever it may be stored.

HOOP Lake is a modern SOC/SIEM approach that empowers Security teams to accelerate adoption of Amazon Security Lake - there are 5 key building blocks that form the approach:

HOOP Orchestrate

Orchestrate your data flows - our orchestrator allows you to order and manipulate your ingest data sources based on your unique data set requirements. For example, your search actions may require additional fields to be captured, and our orchestrator will automatically add this to the streaming function, or you may want data enriched to a new regulatory standard, so we simply add additional components to the stream. Alternatively, you may want to enrich data prior to normalisation, or normalise before archiving. The HOOP Orchestrator uses modular blocks which allows streams to be manipulated without the need to re-write your streaming code.

HOOP Stream

Simply bring your own data - our data processor logic automatically receives log information from your data sources, and transforms this data into your target format, optimised and enriched for store, search and compliance. We focus on the OCSF and OSSEM standards, but also support others such as CIM. The purpose of our streamer is that it provides extremely high throughput and manipulation of data, based on how that log source needs to be treated. For example, we can enrich the stream with regulatory or threat intelligence data, we can truncate keywords and we can consolidate duplicate records with unique timestamps.

Contact us today

Email : hello@hoopcyber.com
Phone : +447899 062352
Web : www.hoopcyber.com

Official AWS Security Lake Services Partner

HOOP Lake

HOOP Store

Efficient store for your data - your normalised and enriched data is stored in a compressed and optimised format, allowing for common access and efficient search and the information is stored in a high performance DB with automatic compress/uncompress. We leverage Parquet tables to provide a high level of compression and high performance indexing, whilst our stream pre-event has already normalised the data for it to be stored in the most efficient manner.

HOOP Search

Natural language search for your data - our federated search capability allows you to optimally search centrally stored or distributed data, using natural language. Our search capability automatically builds this requirement into a native and optimised query language. Whether you want to search your data in DQL, KQL or other formats, our query capability allows natural language search to be automatically converted into a highly optimised search string, which ensures that the search is as advantageous as possible, making it more likely that you will remain in your free search tier.

HOOP Comply

Compliance metrics at your fingertips - your data is automatically enriched at point of ingestion, making on the fly dashboard reporting and visualisation simple. Whether you want to report in NIST or MITRE frameworks, our streaming process automatically categorises data based on your needs, making observability built in as standard. As we have a highly scalable stream and store process, our compliance dashboards are created in real time, using live data which provides the most accurate view of your estate.

Contact us today

Email : hello@hoopcyber.com
Phone : +447899 062352
Web : www.hoopcyber.com

Official AWS Security Lake Services Partner