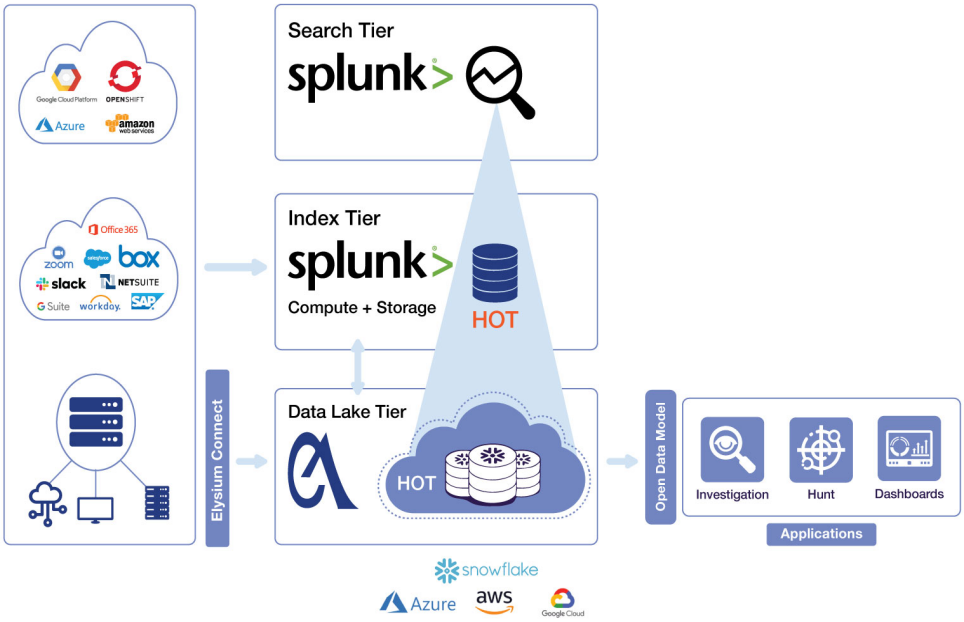
Run Queries from Splunk on a Snowflake Security Data Lake

with Elysium Analytics Splunk Add-On

Organizations going through digital transformation are seeing exponential growth in machine data, holding valuable information about transactions, employee and systems behaviors that supplies a foundation for effective analytics. However, as these datasets keep growing, it is challenging for organizations to cost-effectively manage them.

Splunk has been designed to help security teams quickly gain insights from these massive datasets. Yet, the explosive data growth has created significant operational overhead and cost pressure. Even cloud-based cached object storage, such as Splunk SmartStore, lacks the flexibility and cost-efficiency to meet new storage demands and keep pace with growing demands for storing data.

A more efficient solution to address these storage and analytics challenges is needed.



Benefits of Elysium Analytics' Splunk Add-on

- Run queries on a Snowflake security data lake from within the query bar through the Splunk application for ad-hoc queries on petabytes of your hot data, with no interruption to workflow.
- Load data from Splunk and add data directly from your sources. Bring security telemetry together into a unified taxonomy for a single source of truth with our open data model.
- Achieve consistent performance regardless of level of concurrency or complexity of the query, with Snowflake elastic compute using automatic scale up and scale out.
- Ingest, transform and deliver your data easily with our zero-operations, turnkey solution for faster, deeper insights, with little to no time managing infrastructure.

Connect a Cloud-Scale Security Data Lake to Your Splunk Implementation

Elysium Analytics has developed a Splunk Add-on that allows for users to run queries on a Snowflake security data lake from within the Splunk search bar. This allows ad-hoc queries on petabytes of hot data, with no interruption to workflow. You now have instant access to all data that otherwise may be rehydrated from archival storage at an excessive cost, considerable time penalty and operational overhead.

Expand your security use cases

With your data in a security data lake, you can further expand your use cases with our open platform and applications. We provide security analytics applications out-of-the-box which allow security teams to interact directly with their data using OpenSearch Dashboards, Looker, GraphML, and SQL. Security teams can also enable turnkey ML-based anomaly detection and alerting or build their own ML models with Jupyter Notebook. We provide unique flexibility visualizing data with integrated Looker, OpenSearch Dashboards, or the ability to easily implementing third-party BI tools with no data engineering.

Data integrity and compliance

With security baked into Snowflake from the beginning, security features are core to Snowflake, allowing you to focus on analyzing your data, not protecting it. Snowflake's data lake includes a multitude of features, such as dynamic data masking and end-to-end encryption for data in transit and at rest. In addition, support for ITAR compliance, SOC 2 Type 2 and PCI DSS compliance and HITRUST compliance all confirm the level of Snowflake security required by industries and state and federal governments. Snowflake uses the most sophisticated cloud security technologies available. The result is a secure and resilient service, giving you confidence to enable your most demanding data workloads through Snowflake.

Unlimited hot storage at low cost

Elysium Analytics' security data lake runs natively on Snowflake's optimized object storage with 7x compression, reducing storage cost equivalent to that of archival storage. With Elysium Analytics' Splunk Add-on, all log data on Snowflake is at once available for hot data queries through the Splunk interface, with no cache churn or rehydration slowing down response time. As Splunk ingests more data, Elysium Analytics' data lake storage will seamlessly scale, simplifying Splunk management and reducing operational costs.

Zero data engineering and operational overhead

Easily ingest, transform and deliver your data for faster, deeper insights. With Snowflake, data engineers can spend little to no time managing infrastructure, avoiding such tasks as capacity planning and concurrency handling. Now, you can focus on value-add activities to deliver your data.

Load data from Splunk and directly from log sources

Load data from Splunk with Heavy Forwarder or Data Stream Processor to Elysium Analytics for long-term retention of hot data in Snowflake. Then add data sources you are not ingesting to Splunk for a single-source-of-truth, security data lake searchable from Splunk.

Open data model

With our open data model, you can bring security telemetry together into a unified taxonomy for a single source of truth to detect and understand threats, with a shorter dwell time, more effectively. We will manage the data mapping for you. Create analytics models with rich context of user and entity behaviors. Democratize your data and enable downstream analytics for sharing and reuse of threat detection models, algorithms and analytics. With our high-level abstraction, no specialized data science is needed to productively access your data.

Unlimited query compute with usage-based billing

Query from Splunk on data in Snowflake with elastic compute for consistent performance regardless of concurrency or query level, which automatically and consistently scales up and scales out, as needed.

VISIT US ON SPLUNKBASE FOR ADDITIONAL DETAILS OR CONTACT US TO LEARN MORE.

elysium ANALYTICS

2550 Great America Way, Suite #101
Santa Clara, CA 95054

elysiumanalytics.ai