elysium ANALYTICS

SOC Augmentation: Make your data do more

REIT CUSTOMER: IN-DEPTH SEARCH AND USER BEHAVIORAL ANALYSIS OF ESCALATED CASES IN THE SOC

Company Overview

Global Industrial REIT needed a solution with essential tools and capabilities required for in-depth analytics of escalated cases in the SOC. These capabilities provide in-depth analysis through baseline user and entity behaviors, eliminate noise in alerts, group alerts into actionable incidents, self-service dashboard, and full-text search across the historical data. Since Elysium is natively enabled on the Snowflake data lake and is ready for use from day one, this allowed the REIT customer to leverage Elysium solution with elastic compute and unlimited low-cost storage billed on a usage basis, providing better performance at any load at a far lower TCO than legacy solutions.

Problem

- Disconnected data silos requiring multiple queries on different solutions made post hoc investigations challenging
- Limited data retention compromised investigation effectiveness.
- SOC analysts challenged by proprietary query languages
- Legacy SIEM unable to scale to meet current and future telemetric volumes

Solution

- Elysium semantic security data lake with Full-text-search and out-of-the-box analytics

Benefits: Faster Threat detection

- Search across all IT data sources with master views
- Connected Data points across the logs
- Filter/Aggregation of alerts
- Optimized search indexes
- Elastic compute eliminates concurrency bottlenecks

Platform challenges

Considering two top requirements: being able to analyze data over several years in Snowflake and data ingestion is controlled by the global REIT, they realized that legacy platforms such as the Elastic Search would not meet their requirements without having the data directed to another platform, significant resource overprovisioning and the need to hire additional operational staff to manage and maintain the implementation.

Cost Challenges

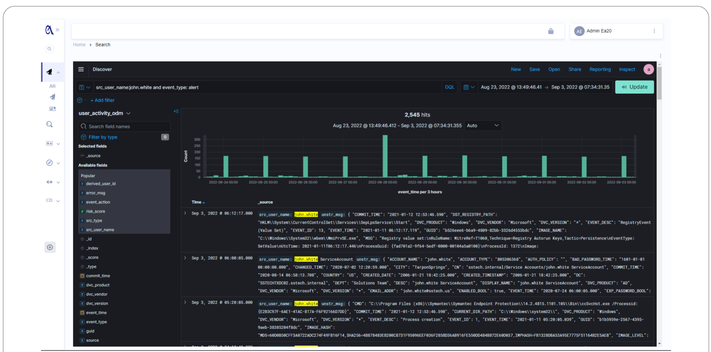
Considering the cost of running the solution on Elastic Search or a comparable platform ultimately would lead to missing capabilities to build new analytics and deliver data to internal stake holders without impacting the security team . This led the Global REIT to look for alternatives.

Enter Elysium Analytics and Snowflake

Since Elysium Analytics runs on Snowflake, the solution benefits greatly from a highly efficient cloud native platform where compute and storage are separated and the customer is billed on actual usage, eliminating the cost of infrastructure resources not being utilized as is the case in traditional on-premises or cloud deployments. Elysium deployed the Open Data Model to the customer's Snowflake so that Elysium Search and behavioral analytics will run seamlessly against their disparate sources. mapped the data in Snowflake to the Elysium.

Elysium Search

The customer appreciated the new search experience by combining the best aspect of OpenSearch, KQL, and the leading cloud scale data platform, Snowflake. You have fast access to all your data in one seamless data cloud where all your data is hot.



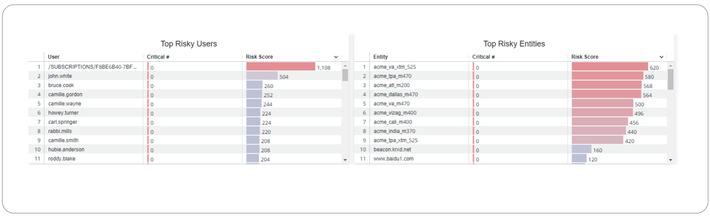
DATA SHARING OVER SNOWFLAKE DATA MARKETPLACE

Large global REIT had a requirement to enrich their data with Threat Intel and IP Location data to improve on their detection and remediation capabilities. Typically, in a legacy application such as Elasticsearch, Enrichment data is provided by 3rd party data vendor who provides regular updates to their data set which, then in turn, the customer can ingest through an ETL service, creating a replica of the data in their own data store used for analytics. For the REIT, having chosen Elysium Analytics, running on Snowflake, the process is significantly simpler and far more cost effective. Accessing enrichment data from two Snowflake Data marketplace vendors, ' have real time access to the 3rd party data with no ETL requirements, no duplication of data, and no maintenance overhead. This not only dramatically lowers the ingestion cost but also relieves Global REIT of all operational overhead associated with accessing this data.

With the data collection configured and the parsing and data mapping verified, data was immediately loading to Snowflake giving Global REIT full visibility to activity on the endpoints and network on our included out-of-the-box dashboards. This gave them immediate visibility to possible vulnerabilities and threats on their network as well as the ability to do full text search on any data.

The dashboard of immediate interest was:

Security Posture: Enterprise situational awareness dashboard to view key security indicators that are critical user and entity behaviors to be investigated. It also shows outlier events/total volume trend and shows top events and top notable event sources.



Self-Service Dashboards

Elysium Analytics bundles both Kibana and Looker, giving the global REIT not only access to out-of-the-box dashboards and analytics that are included in the solution but also provides the ability to customize or build their own dashboards at no additional charge. Typically, a BI application license would run well in excess of $100,000 per year and require significant set up efforts before you can run analytics on your data warehouse. With Looker already implemented as a part of the Elysium Analytics solution and with parsing and data mapping in place, Global REIT were able to quickly develop custom dashboards specific to their environment and use cases on Looker with minimal effort, no contract negotiations or up-front license expense, billed at the standard usage-based rate.

Machine Learning

Elysium Analytics has several machine learning models implemented providing additional critically important data points for detecting anomalous behavior on end users and entities. This is providing important visibility into user and entity behaviors.