elysium ANALYTICS

THE ELYSIUM COGNITIVE SIEM

Product Brief

Enterprises today are faced with an onslaught of new, sophisticated cybersecurity breaches targeting expanded attack surfaces that leave security operation centers unable to respond. These new & innovative threats overwhelm legacy tools. Combined with the threat of inside rogue users, organizations face multiple challenges including:

- **Access vulnerabilities for massive volumes of data being generated**
- **Lack of advanced analytics to identify immediate & high-risk threats**
- **Increased time to resolution & mitigation due to lack of tools**

Leveraging the Big Data stack for data ingestion, processing and analysis, the Cognitive SIEM is built from the ground up on open source technologies to enable machine-learning algorithms.

- **It utilizes real-time events and threat processing of complex data to enable labeling for machine learning.**
- **Built to handle contextual search of structured and unstructured data, Elysium provides an agile, flexible platform scalable for your enterprise.**

The Elysium Cognitive SIEM™ comprises a high-performance security solution that leverages a dynamic cooperative system with network-wide visibility and control that adapts to changing risks. The result is significant improvement in security operations:

- **Reduce false positives by 70-80%**
- **Reduce MTTR by up to 75%**
- **Virtual SOC addresses most Tier 1 tasks through automation**
- **360 User/Entity views**
- **Dramatic improvements in agility by leveraging opensource stack and connectivity to all data sources**

KEY BENEFITS

- **Advanced open source solution for security analytics**
- **Intelligible machine learning with interpretable models providing full transparency for scoring mechanisms**
- **Baselining of users & entities**
- **A purpose-built open data model to simplify analytics**
- **Prioritization of threats with risk-based scoring for users and entities**

ELYSIUM DATA LAKE

Built on top of the proven, standardized Hadoop Stack, our Cognitive SIEM is available for on-prem, hybrid-cloud and cloud instances, all supplying unlimited scale and high availability. Implemented with our Open Data Model, the Cognitive SIEM makes it easy for upstream analytics and downstream source integrations with full extensibility to integrate with any SIEM, database, file source and API, for a powerful, agile enterprise architecture.

ELYSIUM CONNECTORS

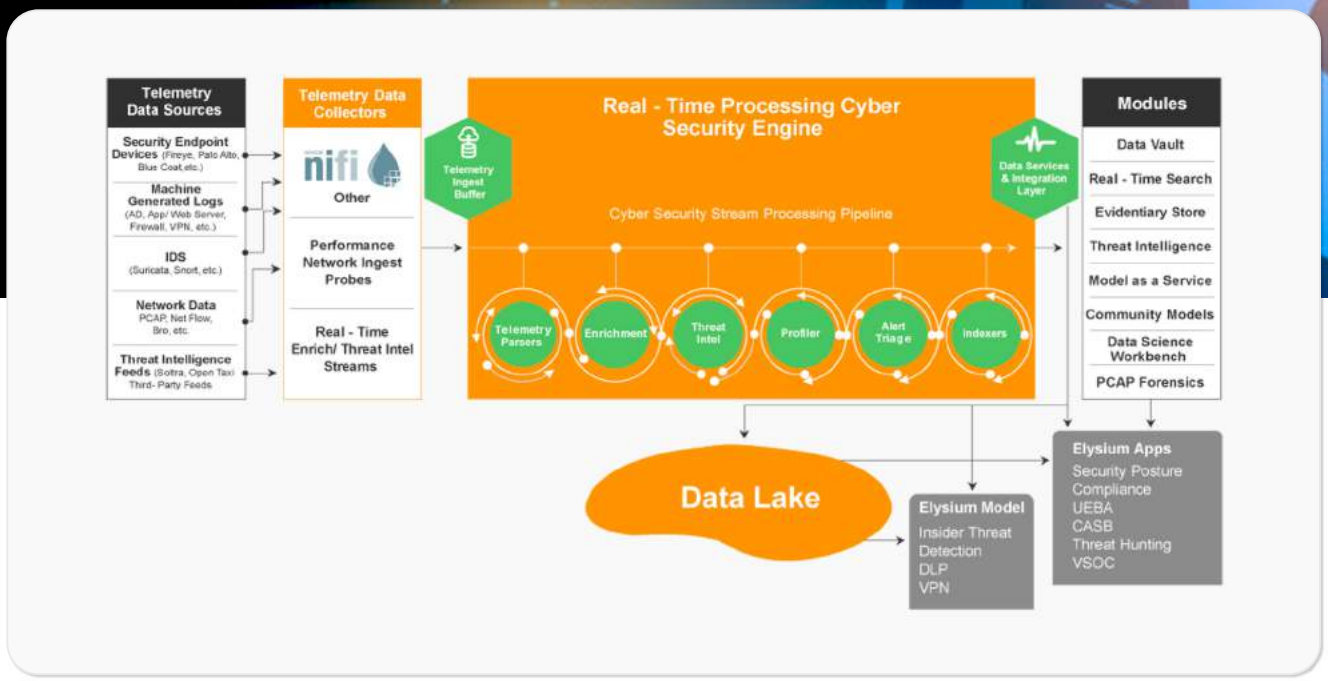
Includes a catalog of standard connectors as well as tools to fast track custom sources. Elysium supports a variety of data sources, including cloud and non-technical data sources (e.g. badge readers & social media) that are not usually supported by log management solutions.

ELYSIUM OPEN DATA MODEL

Elysium Analytics has created an advanced “layered” schema architecture that provides several different “views” into the same data with different schema layouts. Elysium is committed to providing open security framework deployments with add-ons that enable our customers to utilize analytics created for this open security framework.

ELYSIUM ANALYTICS

Our Cognitive SIEM offers intuitive analytics for cloud security, compliance reporting, endpoint protection, user and entity base lining to identify anomalous behavior, and vulnerability detection on enterprise assets.



ELYSIUM PLATFORM ARCHITECTURE

ELYSIUM MODELS

As attackers become more sophisticated and attack surfaces expand, the number of attacks has grown almost exponentially. Organizations find themselves exposed to an onslaught of novel and previously unseen attacks. With this torrent of threats, humans are not equipped to analyze patterns over billions of records or to manage the vast number of false positives. Elysium has designed intelligible machine learning so that SOC analytics can connect the dots when a model detects a new threat across numerous features.

ELYSIUM VIRTUAL SOC

Our virtual SOC enables security teams to have a force-multiplier effect for productivity by employing specific models for all users - i.e. each user will have an allocated model to track behavior and to report suspicious patterns to the user through our Chatbot conversation utility.

ELYSIUM ANALYTICS EXCHANGE

Elysium offers a Data Analytics Marketplace for advanced analytics notebooks to promote content from analytics professionals from around the world. Our marketplace also has a machine-learning accelerator to quickly explore and develop advanced analytics POCs and commercialize new analytics.

USE CASE MODULES

- UEBA
- CASB
- Threat Hunting
- Insider Threat Detection
- Data Loss Prevention
- Remote Access Monitoring
- Compliance Reporting

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

Phone: 669-209-0801

www.elysiumanalytics.us