The Security Data Platform

With the continuing rise of breaches more companies are taking the initiative and adding a better means to discovering unknown threats by adding a platform for advanced security analytics.

Today's Cybersecurity Challenges

As attackers have become more sophisticated, attack surfaces have expanded, and the number of attacks increased, organizations find themselves exposed to an onslaught of novel and previously unseen attacks. Combined with the threat of inside rogue users, its clear organizations face an enormous challenge.

- Can't Access the Data
- Limited Advanced Analytics
- Long Time to Mitigation
- Lack of Tools Intended for Security AnalystsCan't Access the Data

Features and Benefits

To address these needs and challenges Elysium has assembled a solution accelerator combining a cohesive set of available open source products in a pre-integrated, pre-engineered package. As a services company there are no license fees for this solution. Our customers benefit from our services upon initial deployment by leveraging the work we've already invested in operationalizing this set of products.

The Four Key Foundation Capabilities:

Scalability	**Extensibility**
Deploy-ability	**Future Readiness**

Scalability

Modern Cybersecurity Architecture - When SOCs implement an Analytics Platform for Cybersecurity, they gain a single, comprehensive repository of security data that allows them to keep information online indefinitely.

Security Data Lake - Elysium has selected a best-of-breed storage stack based on Hadoop technology and ensures the implementation is easily and readily deployable through its extensive internal engineering testing and field deployments.

High Speed Ingestion - Security telemetry is constantly generated, and needs to be immediately collected, normalized and stored at extremely high speeds to make it easily accessible for advanced computation and analytics.

Efficient - Cost effective data storage is necessary so that logs and telemetry can be efficiently mined and analyzed with long term visibility and full packets can be extracted and reconstructed to help trace who the true attacker was, what data was leaked, and where that data was sent.

Accelerate Threat Mitigation - The Platform greatly speeds investigation and shortens the time for breach mitigation. This allows responders to immediately access historic and real-time data in order to quickly make it through their flagged events.

Extensibility

Application Framework - The solution is an application framework that enables a single view of diverse, streaming and batch processing security data at scale to aid security operations centers in rapidly detecting and responding to threats.

Pluggable Framework - An open pluggable framework enables easy creation of new parsers to integrate into batch and streaming feeds, enrichment processes, and the extensible analytics schema.

Standard BI Interface - All queries and reports are available in Zeppelin and Tableau, or use your own Enterprise standard!

Deploy-ability

Operationalization - Adding Kylo to the solution eases the management and configuration of your live data feeds.

continued...

Tested Parsers - Included are loading routines and parsers for the most common data sources such as MS Windows, Cisco ASA, Bluecoat, etc.

Compliance Reporting - Included are a complete set of compliance reports ready to fit into any organization's larger compliance initiative for regulations such as PCI, HIPAA, FISMA, NIST, etc.

Threat Intelligence - Adding OpenTAXI Server to the solution means all data sources can easily be enriched with the latest threat intelligence information for known bad IP addresses, domain names, and URLs.

Insider Threat Detection - Elysium included a comprehensive implementation of user behavior analysis including advanced statistical and machine-learning techniques with a human-assisted feedback loop.

Incident Response and Forensics Investigation - An augmentation to SIEM capabilities inclusive of packet replay utilities, evidence store and hunting services commonly used by SOC analysts.

Future Readiness

Real-time and Batch - All data loading parsing routines accommodate both batch and real-time processing.

Structured and Unstructured - To accommodate all scenarios Elysium deploys the solution with all data needs and enrichment processes going to both batch and real-time subsystems.

Spot and Metron - Elysium is committed to deploying solutions that will support analytics intended for either product, all in one environment.

Benefits to Security Personnel

CIO/CISO - Single view of risk, improved risk mitigation and proactive risk strategies.

Security Engineering - Security Processes and tools with a maintainable lifecycle.

Security Architecture - Ensure architecture enables security by preventing threats.

SOC Analyst - Increase proficiency and efficacy.

SOC Investigator - Removes many steps a traditional SOC environment requires to investigate more complicated attacks like APTs.

SOC Manager - Easier to assign Metron Cases to Analysts, verifies "completed" Metron cases.

Forensic Investigator - Reduces time lag associated with current big data ingest solutions to transform detection and response to cyber-attack from 8 months to days, or even minutes.

Security Platform Engineer - Streamlined operations and efficient maintenance of cyber security tool(s).

Security Data Scientist - Easier way to search, hunt and perform data science lifecycle activities.