

Analytics





Enterprises and government organizations today are faced with an exponentially growing onslaught of sophisticated cybersecurity attacks, targeting unexploited attack surfaces that leave SoCs unable to detect and respond with existing legacy solutions.

Since these solutions all have their separate data silos with no sharing between applications, there is no single solution that has access to all data relevant to the attack, so the ability to “zoom out” to see the bigger picture is lost.

Additionally, many current security solutions lack a high-performance backend capable of ingesting large volumes of data from multiple security sources, and also lack unifying this data into a single data model in a cloud-scale data lake.

To deal with this, Elysium Analytics has implemented file shippers, connectors, and parsers that support all cloud and on-premises sources, and scale out to any data volume. Our behavior analytics integrate with Snowflake in near real-time and inline as data is ingested and analyzed.

We created an advanced “layered” schema architecture that provides several different “views” into the same data with different schema layouts. Elysium is committed to providing an open security framework with add-ons that enable instant scoring of anomalous behaviors based on MITRE ATT&CK vectors. Our behavioral analytics are built on contextualization of data, and support machine learning and modeling, as well as support applications like threat hunting for rapid visualization of complex data which enables informed decision-making.



With Elysium Analytics, SOC analysts can now investigate possible threats from a single pane of glass powered by true cloud-scale compute; no more waiting in queue or switching between security consoles!

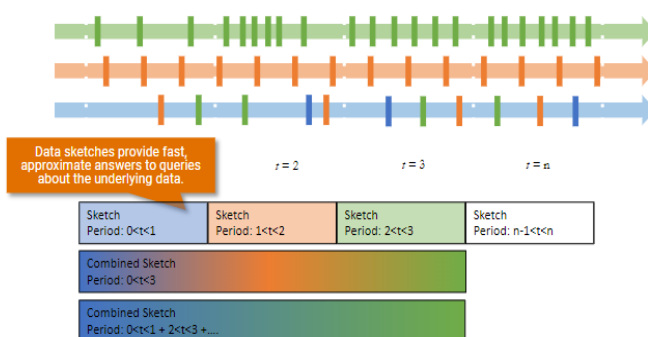
Elysium Analytics provides a single pane of glass that allows for aggregated views of all users' and entities' activities across an enterprise.

By using risk-based profilers — which perform data sketches across time intervals on security metrics baselining the behaviors of all users and entities — we gain full visibility into any anomalous and suspicious behavior through risk-based scoring of the security data.

We target specific threat behaviors that are established by the MITRE ATT&CK vectors, leveraging the benefits of an open community of knowledge sharing.

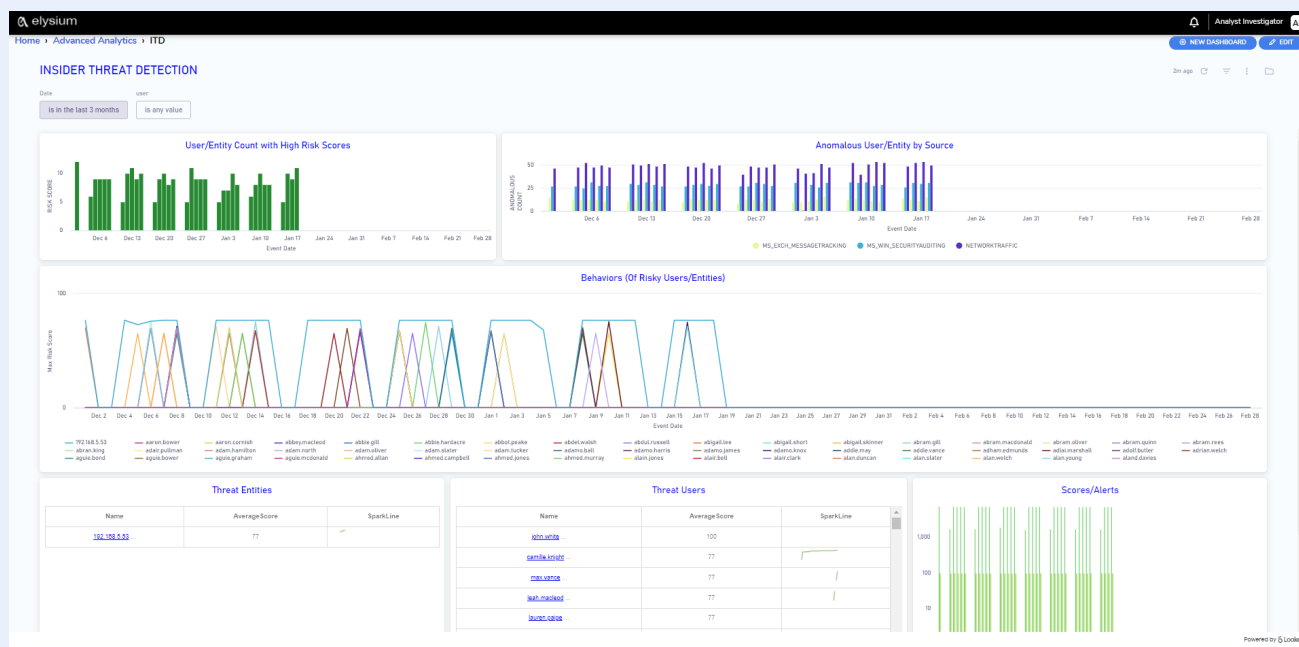
To unify the underlying data schema, Elysium Analytics has created an advanced “layered” schema architecture that provides several different “views” into the same data with different schema layouts.

Elysium Analytics is committed to providing an open security framework solution that, in addition to being the foundation for our ready-to-run behavioral models, serves as a platform for in-house development and 3rd party models. This allows customers to see all behaviors across any number of sources. Our dashboard can be customized and allows SOC analysts to identify and alert on behaviors of users who are exhibiting abnormal and suspicious activities.



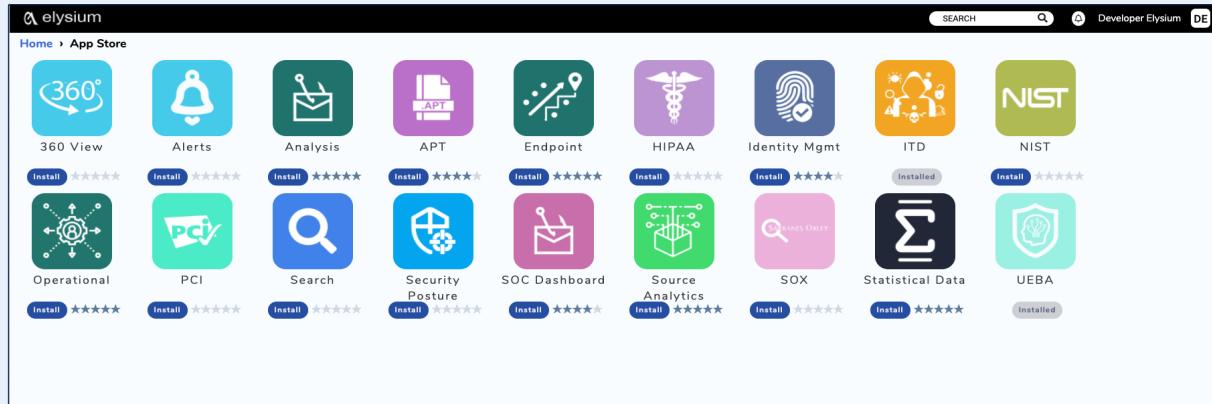
Elysium Risk-Based Scoring

To help an analyst understand the behaviors of a threat, Elysium unpacks the scores into specific behaviors that are contributing to the rise in a score. The Elysium Analytics models then score each of the contributing events and profiler statistics, which are the basis for individual user and entity scores. Additionally, we expose the underlying contributing events that led to the high score for the user or entity. To minimize the noise from irrelevant events, we filter out any events not relevant to the user's or entity's anomalous behaviors.



Elysium App Store

All applications are available on our App Store. Since we do not license applications separately like most vendors, you can install the full library and only be charged for actual usage by the minute. We have a broad library of apps and if there is a need to develop your own ML models or dashboards, you can leverage the existing ML data pipelines for quick development. Adjust the Elysium Analytics models for your specific environment or build your own proprietary models.



Results From Day One With Room to Grow

Elysium Analytics provides a unique AI-driven security analytics platform that comes with a wide array of ML-based security outcomes and behavioral models, all to help organizations detect and respond to advanced cyber attacks. In addition, you can also build your own ML models using the Databricks managed Spark platform with easy access to all your data on the Elysium Analytics platform.



Custom ML Models

Although Elysium Analytics offers numerous models out-of-the-box, we also provide the ability for a user to build custom models for specific use cases. Leveraging Databricks, you can create models using a Jupyter notebook where you can specify features and weights for domain-specific use cases. In addition to Databricks, we support several other cloud data science platforms.



Custom Dashboards

Leveraging Looker, you can build your own dashboards that supplement the dashboards Elysium Analytics provides out-of-the-box. A dashboard is essentially a collection of visualizations of queries, displayed all on one page. You can add filters to make the dashboard interactive and rearrange its tiles. After you've configured a dashboard to your liking, you can share it with your team. You can create as many dashboards as you like and tailor each dashboard to the specific needs of the users.

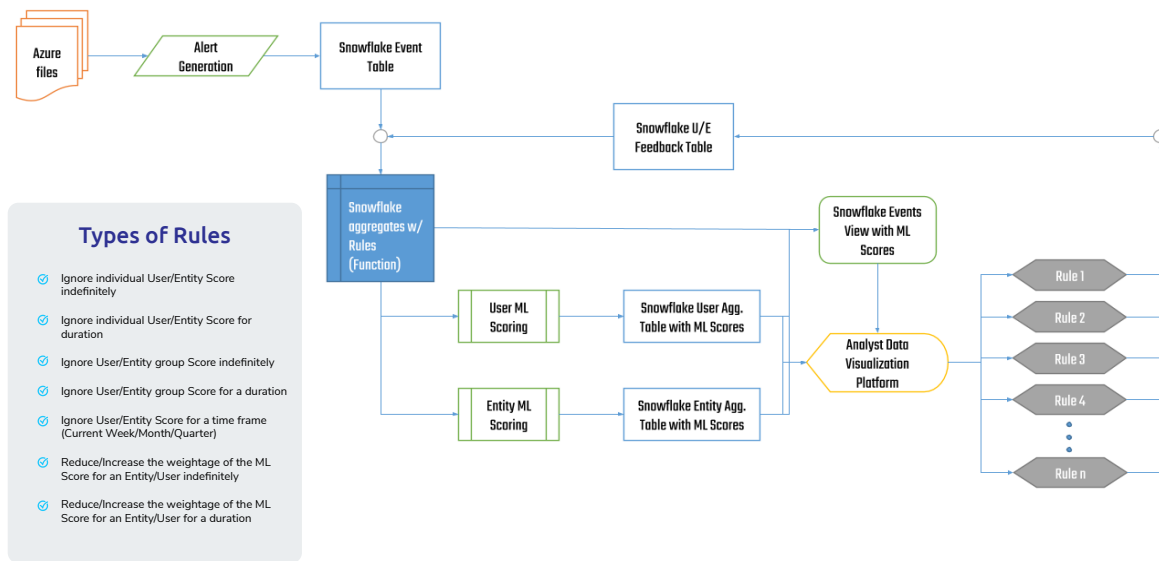


Feedback

Even Data Scientists don't always get everything right. This is why Elysium Analytics developed a feedback system that will provide immediate relief by giving you the ability to silence alarms for acceptable behaviors that were flagged as anomalous. Additionally, this feedback is applied towards training other models, leading to improved performance and accuracy.

ML Scoring with Feedback Loop

Event & Batch Scoring



Detected Behaviors

Elysium has built the following behavioral profilers for the support data sources. New profilers are released each month.


INITIAL ACCESS	EXECUTION	PERSISTENCE	PRIVILEGE ESCALATION	DEFENSE EVASION	CREDENTIAL ACCESS	DISCOVERY	LATERAL MOVEMENT	COLLECTION	COMMAND & CONTROL	EXFILTRATION	IMPACT
Abnormal user Agent String	Powershell	File Downloads	Windows AD	Clearing Audit Files	Shared Account	Port Usage	Windows RDP	File Activity	Reasoning Endpoints	Upload Bytes	File Activity
Unusual Domains	Command Line	Process Creation			Overall Activity	Network Scans	Device Association			Download Bytes	
Email Size, Encrypted, etc	Endpoint Protection Products	New Entities			New Accounts		SSH				
DNS Requests	High Velocity	New Scheduled tasks									
Websites											
Event IDs											
External Storage											
Geo-location											




About Elysium Analytics


Elysium Analytics is a machine learning based log analysis solution for security-minded, mid-sized to large enterprises who are challenged by the volume of security log data today, both from an infrastructure as well as an analytics and detection perspective. We have simplified onboarding of data, provided a scalable data lake analytics platform, and search on a pay-as-you-go basis. Since we are built on top of Snowflake, our SaaS solution is truly a cloud scale security analytics platform that removes the barriers from ingesting, contextualizing, searching, analyzing, and storing log data with a cost-effective and low-risk service. Unlike other log analysis vendors in the market, our SaaS offering is licensed on a usage basis, lowering cost and removing financial risk. You pay a low price for storage, and compute is billed by the minute of usage. Additionally, we have an open platform with no vendor lock-in, customizable analytics models, as well as APIs for end user development of analytics models.



 Elysium Analytics, Inc. 2550 Great America Way, Santa Clara, CA 95054

 elysiumanalytics.ai

 Phone: +1 (669) 209-0801

 info@elysiumanalytics.ai