elysium
ANALYTICS

Operational monitoring

IONIS PHARMACEUTICALS: MONITORING DISTURBANCES WITH BOOMI AND AZURE SQL LOGS

Ionis Pharmaceuticals (IONS), founded in 1989. is a biotechnology company based in Carlsbad, California that specializes in discovering and developing RNA-targeted therapeutics. The company has close to 5,000 employees and has a collaboration agreement with AstraZeneca; Biogen Inc.; and Roche. Ionis Pharmaceuticals, Inc

Full Visibility

By ingesting all log data from Boomi and Azure SQL over global locations, Ionis Pharmaceuticals gained full visibility of their business processes. Additionally, log data from their Azure SQL for additional observability of database activity allowing them to predict and isolate disturbances.

Operational Posture

Having gained full observability of all employees and servers across all global locations, Ionis Pharmaceuticals has full real-time visibility of their operational posture with out-of-the-box analytics apps for Boomi and Azure SQL.

Faster Disturbances detection

Machine learning-based analytics and alerting reduced meantime to detection by 90%. Full text search across all data and granular contextual 360 views into every user and entity lead to significantly faster detection and remediation. With no practical limit to data retention, all historical data is immediately available making remediation across the network significantly faster.

Observability of operational Disturbances

Being a pharmaceutical, they are required to retain all log data for several years in hot storage not only to be able to respond quickly should there be a need to access historical data but also to be able to run deep machine learning-based analysis on all historical data on a regular basis, surfacing any potential disturbances, with the latest algorithms and visualization platform.

Platform challenges

Considering two top requirements; being able to store data hot over several years as well as having access to significantly more compute for deep analytics on a regular, but infrequent, basis, Ionis Pharmaceuticals realized that legacy platforms such as the ELK Stack would not meet their requirements without significant overprovisioning leading to a high cost and the need to hire additional operational staff to manage and maintain the implementation. The cost of hot data retention became a concern as well as there was no practical way to scale up storage to hundreds of terabytes without going to a tiered hot-warm-cold architecture which would still be costly but, more importantly, not make most of the data available for days when it would have to be re-hydrated from cold storage.

Cost Challenges

Considering Elasticsearch, Ionis Pharmaceuticals realized that although they were only planning to ingest up to 50GBs per day initially, this would still mean that they would have to deploy several. Near term, they wanted to be able to add several additional data sources across their infrastructure which would increase their data ingestion to a significantly higher level. This configuration would add significant cost just in compute and storage cost, not taking onto consideration any licensing, support, or operational overhead cost. This led Ionis Pharmaceuticals to look for alternatives.

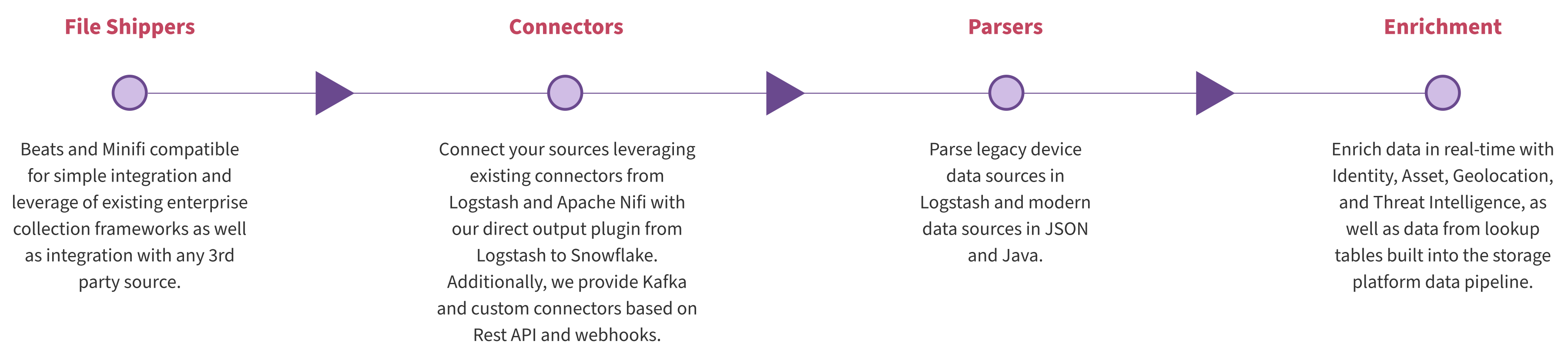
ENTER ELYSIUM ANALYTICS AND SNOWFLAKE

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 paying for resources not being utilized as is the case in traditional on-premises or cloud deployments.

Onboarding to the Elysium Analytics solution, a cloud native and cloud scale solution, proved to be simple. First Ionis Pharmaceuticals, as the leader in RNA-targeted therapeutics, must protect their business workflows. To do this they required Elysium to collect operational logs from the Boomi application. This provided a rich set of telemetry on the execution jobs of business processes, requiring ML baselining to detect disturbances in the job executions from errors or failed execution jobs. In addition to the Boomi logs, monitoring of their backend AZURE SQL jobs is necessary to detect disturbances in the running of business processes. Furthermore, Elysium Search provided a quick way to investigate anomalies once an alert is fired on an aberrant execution job or unusual CPU activity.

DATA COLLECTION FLOW

Data Collection: Near real-time data collection and shipping is facilitated by connecting to the Elysium Analytics collector service,



File Shippers

Beats and Minifi compatible for simple integration and leverage of existing enterprise collection frameworks as well as integration with any 3rd party source.

Connectors

Connect your sources leveraging existing connectors from Logstash and Apache Nifi with our direct output plugin from Logstash to Snowflake. Additionally, we provide Kafka and custom connectors based on Rest API and webhooks.

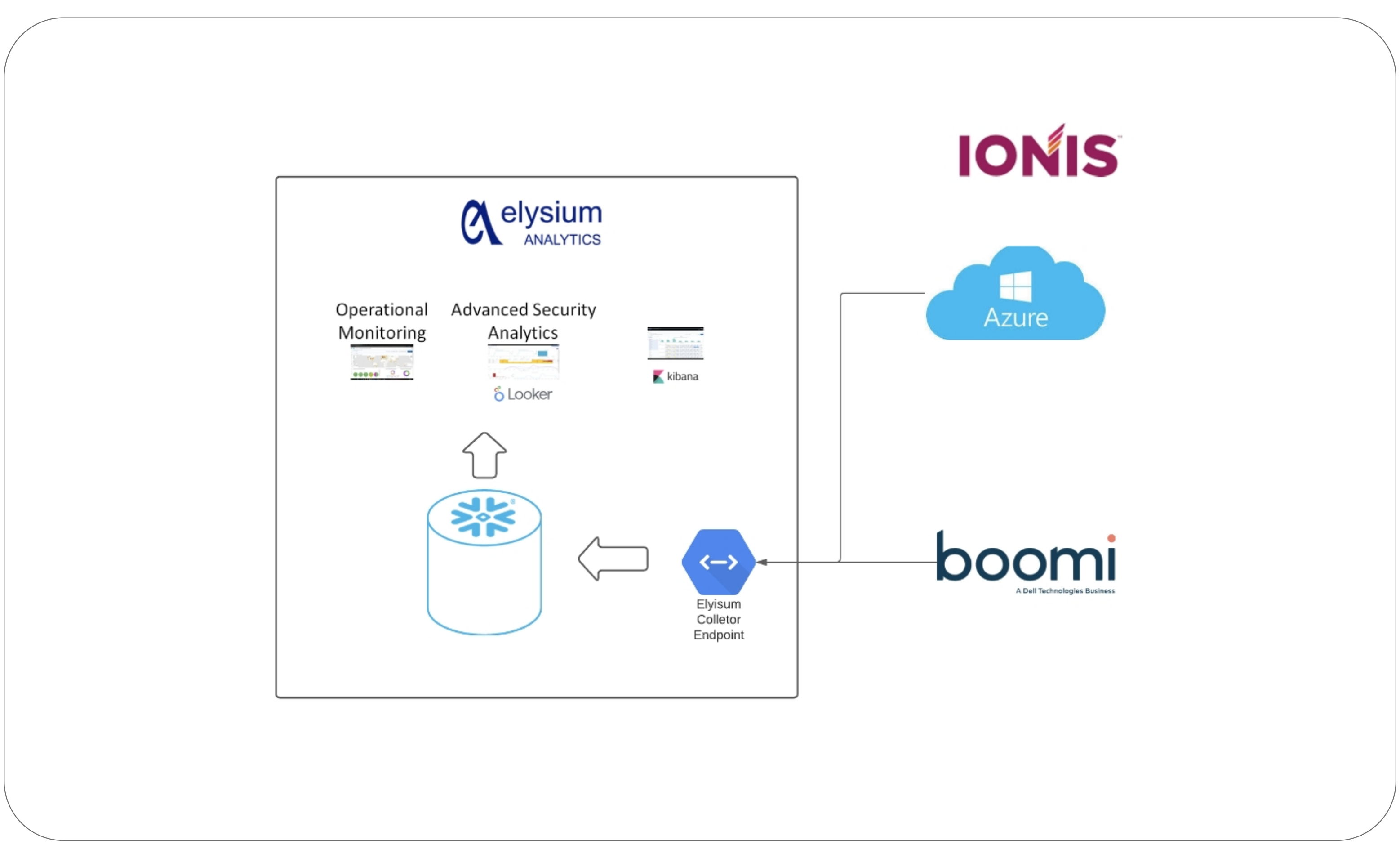
Parsers

Parse legacy device data sources in Logstash and modern data sources in JSON and Java.

Enrichment

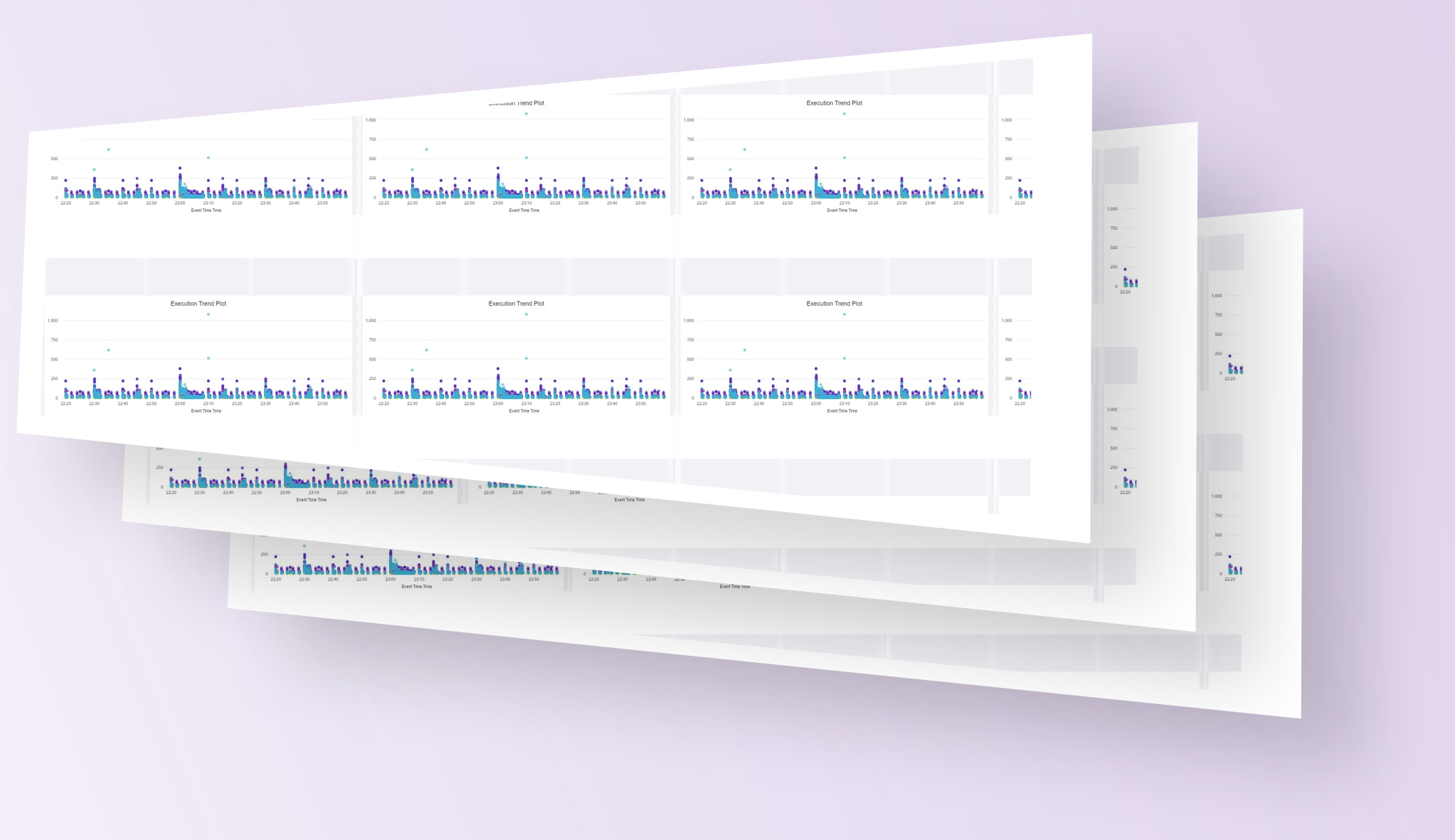
Enrich data in real-time with Identity, Asset, Geolocation, and Threat Intelligence, as well as data from lookup tables built into the storage platform data pipeline.

With the data collection configured and the parsing and data mapping verified, data was immediately loading to Snowflake giving Ionis Pharmaceuticals 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 Disturbances on their network as well as the ability to do full text search on any data.


elysium
ANALYTICS
Operational Monitoring
Advanced Security Analytics
Looker
kibana
Elyisum Colletor Endpoint
IONIS
Azure
boomi
A Dell Technologies Business

THE DASHBOARDS OF IMMEDIATE INTEREST WERE

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



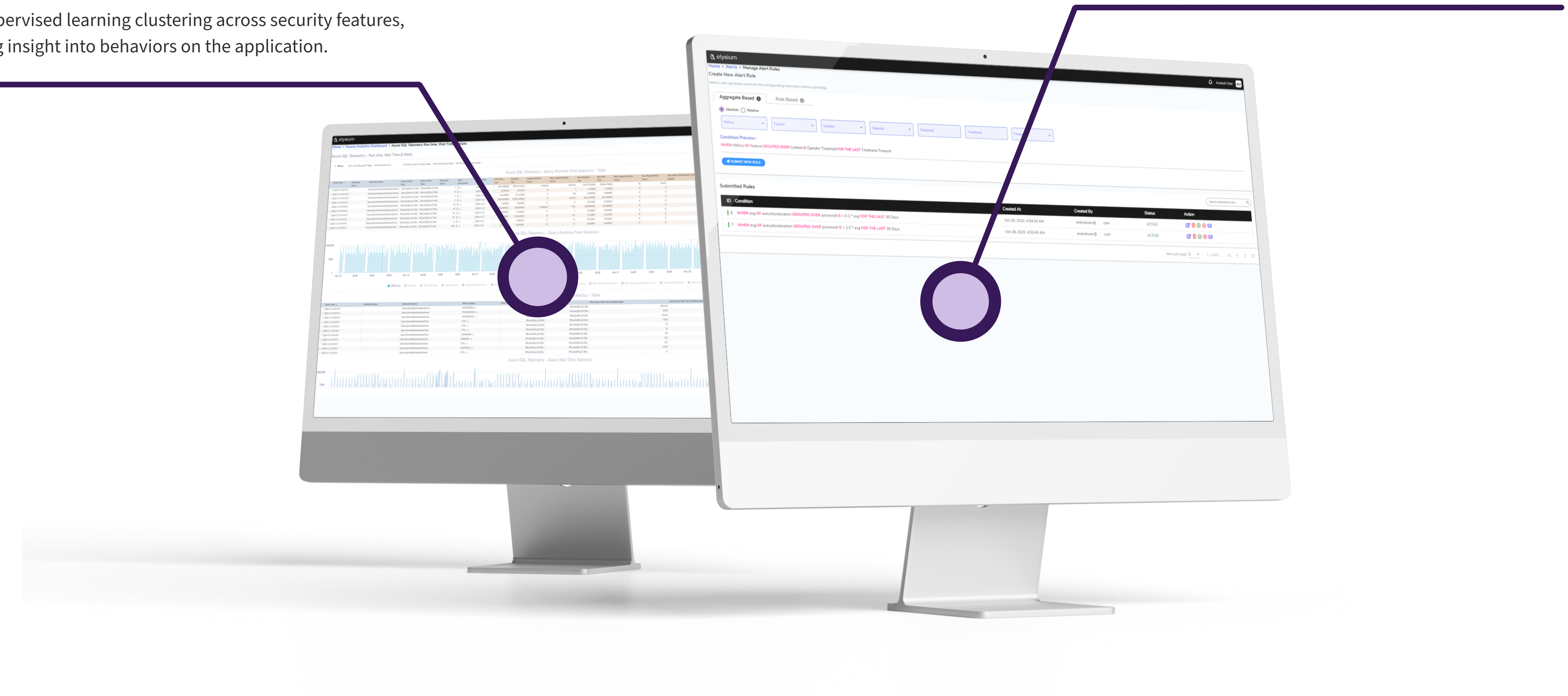
OPERATIONAL DISTURBANCE DETECTION

Alerting

Detect new application behaviors with customer alerting rules. New alerts can easily be set up with the alert configurator with full flexibility for anyone to configure alerts based on rules or aggregate values.

Operational Disturbance Detection

Shows operational assets that have crossed a threshold due to statistical anomalies and outliers from unsupervised learning clustering across security features, giving insight into behaviors on the application.



CUSTOM DASHBOARDS

Elysium Analytics bundles both Kibana and Looker, giving Ionis Pharmaceuticals 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, Ionis Pharmaceuticals 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 behavior