Data Collection

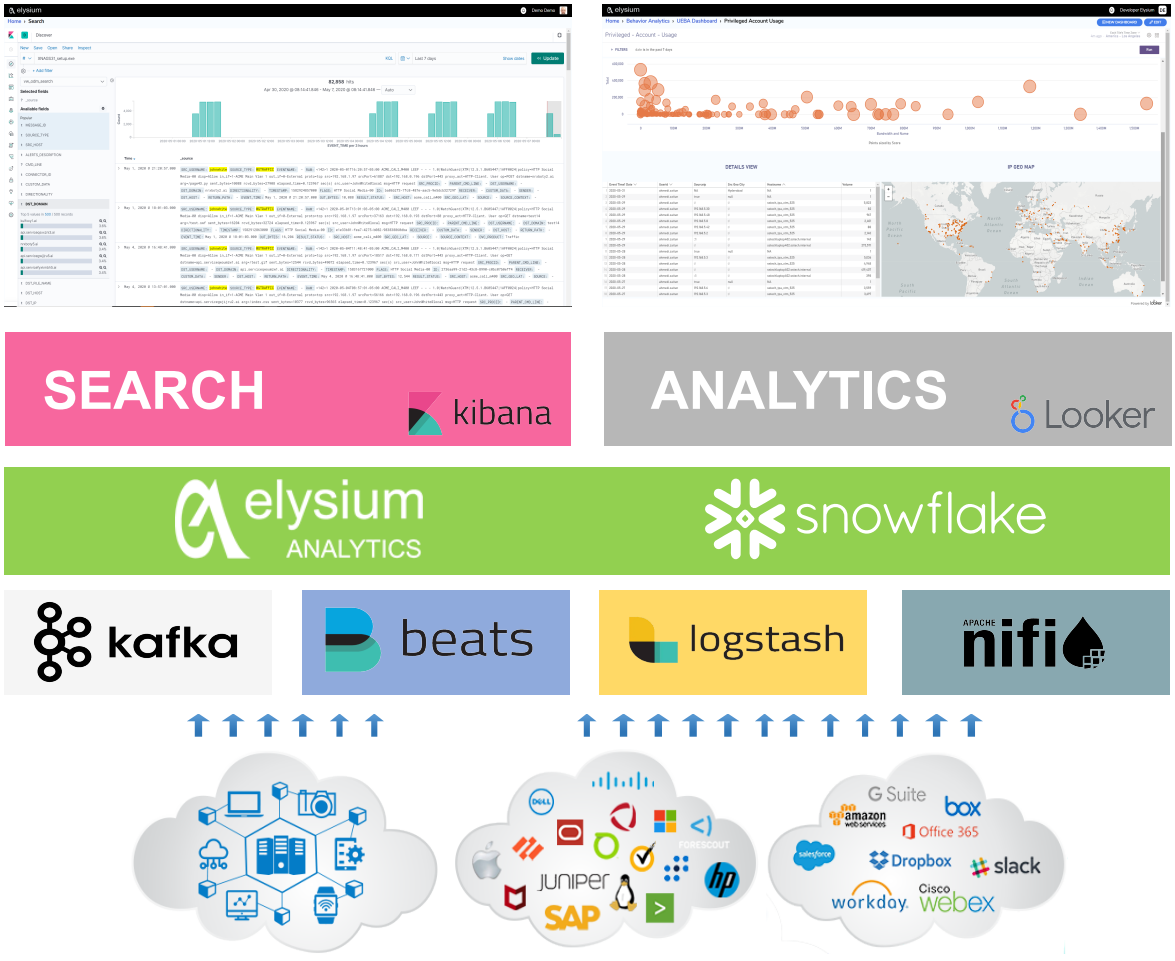
elysium
ANALYTICS

The big data **Challenge**

Any number of advanced algorithms or visualization tools and dashboards will do little in the effort of detecting cyber threats without the right data.

Log files have to be collected, parsed, enriched, and loaded into a scalable data lake where it can be accessed, processed, and stored for real-time and future analysis. Security challenges today are a “big data” challenge. A true cloud-scale security solution has to be capable of collecting all the data in an enterprise to enable data-driven analytics.

Log aggregation, the process of collecting logs from multiple computing systems, parsing them and applying the data to a data model that makes it easily searchable and explorable, can be challenging with an exponential increase in number of sources and data volume. The fact that the log sources are often distributed on-premise, in the cloud or across different clouds makes collection of data even more complex and costly.



Elysium Analytics provides a scalable, robust and flexible architecture, delivered as a service, that assures secure and reliable collection, parsing and loading of any type of log data as well as network traffic data into a cloud scale data lake built on top of Snowflake’s data warehouse.

Simple and flexible

Set up and flow your security data to Snowflake and customize, enrich, and parse the data on the stream before it even hits the data warehouse.

Secure & reliable

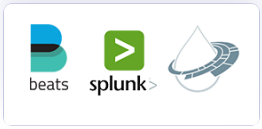
Never lose an event. Our checks and balances ensures error handling without slowing down your pipeline

Scalable

We scale to any number of data sources at high or low volume

Data Collection Flow

File Shippers



Beats, Minifi, Splunk Forwarder compatible for simple integration and leverage of existing enterprise collection frameworks

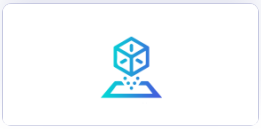
Connectors

Connect your sources leveraging existing connectors from Logstash and Apache Nifi with our direct output plugin from Logstash to Snowflake

Parsers

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

Enrichment



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

Collect, Parse, Enrich, Load

With integration of all your security and log sources, Elysium Analytics automatically collects all the data you need from any source. Easily parse, map, and group your data in Elysium Analytics Open Data Model for full context and fast analytics. Context and Threat Intel enrichment add event and non-event contextual information to security event data in order to transform raw data into meaningful insights.

Collect your data

With integration to all your security and log sources, Elysium Analytics automatically collects all the data you need from any source; cloud, on-prem, or SIEM solution. Leveraging Kafka, Logstash, Beats, and Nifi

Parse your data

Parse, map, and group your data in Elysium Analytics Open Data Model for full context and fast analytics.

Enrich your data

Context enrichment adds event and non-event contextual information to security event data in order to transform raw data into meaningful insights. User typically enrich with geo data, asset lookup data, and more.

Add Threat Intel to your data

Enrich your data with Threat Intel and get a broad view of the threat landscape external to your organization allowing your security team to more effectively detect threats, measure overall relevant risk exposure, and become more effective at mitigation. We have implemented a RESTful API as well as STIX & TAXII support for simple ingestion into our data lake

Load your data

Loading your data into the data lake is billed by the second and can be configured to continuous loading or batch loading. Since you are billed by the compute resources you consume, you can configure frequency and capacity based on what your needs are.

Connect to your data

Combine all your on-prem IT logs, enterprise network logs, cloud logs and network traffic data into one scalable data lake and combine your in-cloud and on-prem data silos into one scalable Snowflake data lake

Anomaly detection relies on excellent algorithms but perhaps even more importantly having the right data to process. We have developed a broad library of Collectors, Parsers and Plug-ins that allows you to collect and load all security related data as well as data for context and enrichment into our data lake. Our data collection is delivered as a cloud service; all you need to do is to point your data sources to our infrastructure and we will take of it from there.

Cloud Apps

Collect, aggregate and analyze logs from any cloud application source. Simple setup. Get the whole picture from all your cloud applications, infrastructure, and devices.

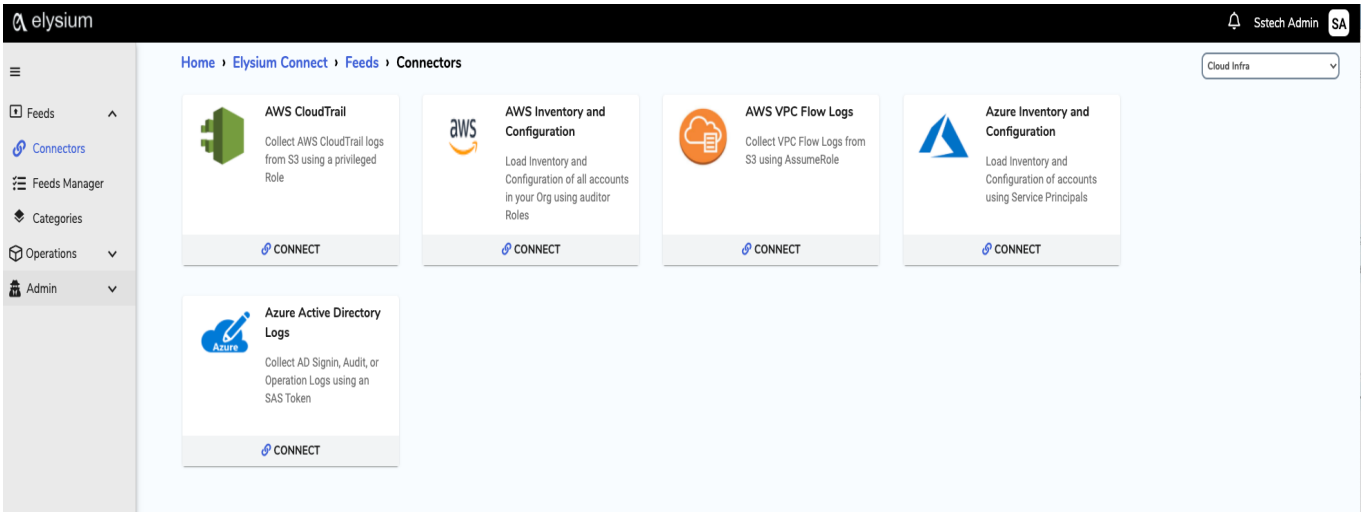
Security Devices

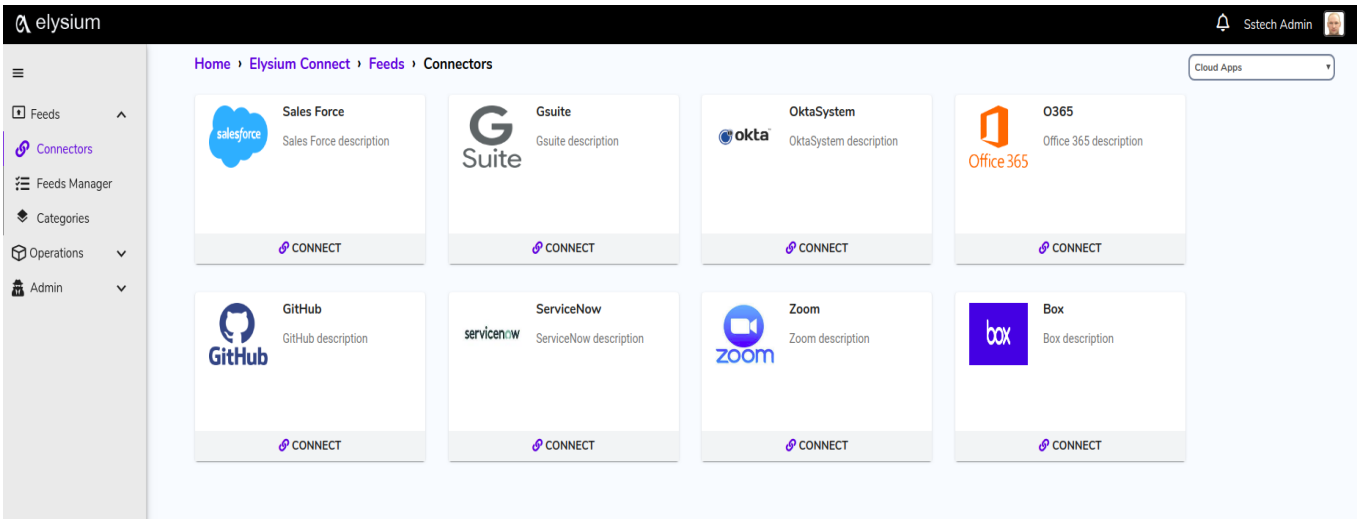
Collect all log data from your all your security devices, on-premises and cloud implementations for a consolidated view of all activity across all your security solutions and retain the data for as long as you need to.

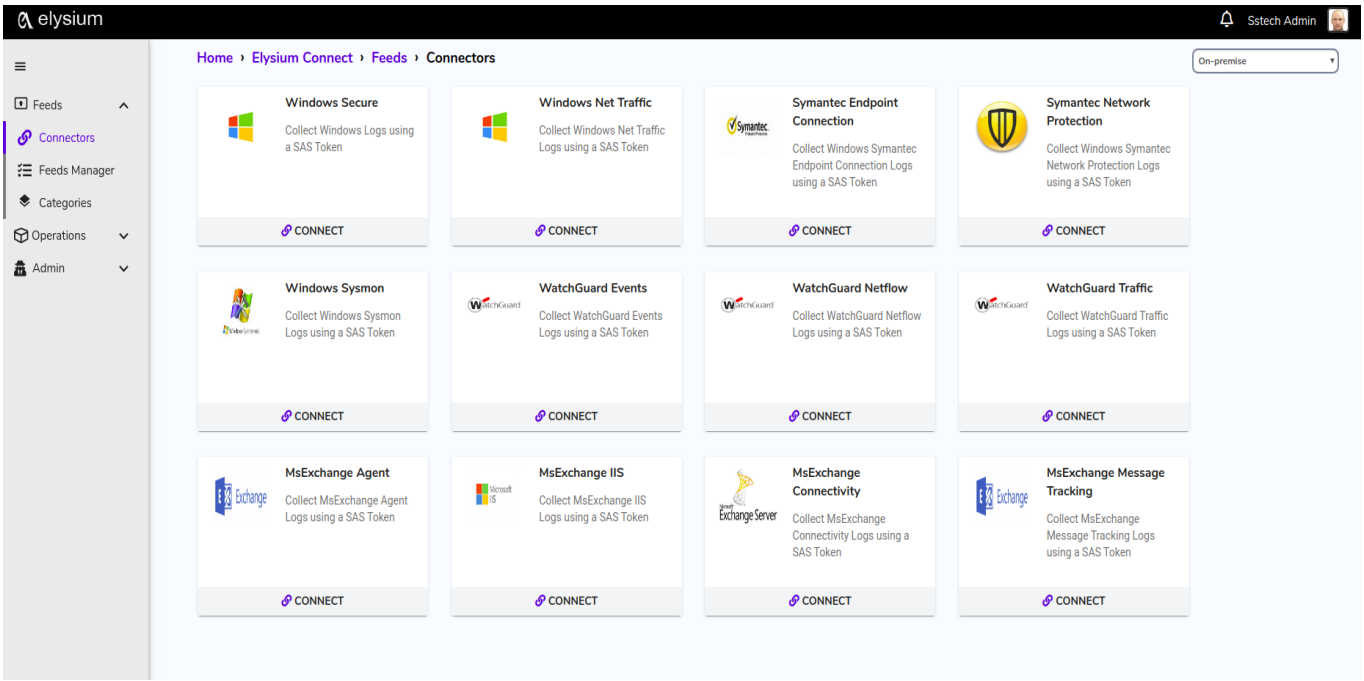
Enterprise Network

Collect all your enterprise network and endpoint device logs for full visibility to all activity across all layers of your network.

Collector	Description
Auditbeat	Collects your Linux audit framework data and monitor the integrity of your files
Filebeat	Tails and ships log files
Functionbeat	Reads and ships events from serverless infrastructure.
Heartbeat	Pings remote services for availability
Journalbeat	Reads and ships event from Journald
Metricbeat	Fetches sets of metrics from the operating system and services
Packetbeat	Monitors the network and applications by sniffing packets
Winlogbeat	Fetches and ships Windows Event logs
NXLog	Fetches and ships Windows Event logs
Minifi	Can transmit the data from any IOT device


elysium
Sstech Admin
SA
Home › Elysium Connect › Feeds › Connectors
Cloud Infra
Feeds
Connectors
Feeds Manager
Categories
Operations
Admin
AWS CloudTrail
Collect AWS CloudTrail logs from S3 using a privileged Role
CONNECT
AWS Inventory and Configuration
Load Inventory and Configuration of all accounts in your Org using auditor Roles
CONNECT
AWS VPC Flow Logs
Collect VPC Flow Logs from S3 using AssumeRole
CONNECT
Azure Inventory and Configuration
Load Inventory and Configuration of accounts using Service Principals
CONNECT
Azure Active Directory Logs
Collect AD Signin, Audit, or Operation Logs using an SAS Token
CONNECT


elysium
Sstech Admin
Home › Elysium Connect › Feeds › Connectors
Cloud Apps
Feeds
Connectors
Feeds Manager
Categories
Operations
Admin
Sales Force
Sales Force description
CONNECT
Gsuite
Gsuite description
CONNECT
OktaSystem
OktaSystem description
CONNECT
O365
Office 365 description
CONNECT
GitHub
GitHub description
CONNECT
ServiceNow
ServiceNow description
CONNECT
Zoom
Zoom description
CONNECT
Box
Box description
CONNECT


elysium
Sstech Admin
Home › Elysium Connect › Feeds › Connectors
On-premise
Feeds
Connectors
Feeds Manager
Categories
Operations
Admin
Windows Secure
Collect Windows Logs using a SAS Token
CONNECT
Windows Net Traffic
Collect Windows Net Traffic Logs using a SAS Token
CONNECT
Symantec Endpoint Connection
Collect Windows Symantec Endpoint Connection Logs using a SAS Token
CONNECT
Symantec Network Protection
Collect Windows Symantec Network Protection Logs using a SAS Token
CONNECT
Windows Sysmon
Collect Windows Sysmon Logs using a SAS Token
CONNECT
WatchGuard Events
Collect WatchGuard Events Logs using a SAS Token
CONNECT
WatchGuard Netflow
Collect WatchGuard Netflow Logs using a SAS Token
CONNECT
WatchGuard Traffic
Collect WatchGuard Traffic Logs using a SAS Token
CONNECT
MsExchange Agent
Collect MsExchange Agent Logs using a SAS Token
CONNECT
MsExchange IIS
Collect MsExchange IIS Logs using a SAS Token
CONNECT
MsExchange Connectivity
Collect MsExchange Connectivity Logs using a SAS Token
CONNECT
MsExchange Message Tracking
Collect MsExchange Message Tracking Logs using a SAS Token
CONNECT

Parser Name	Description
MSFT Exchange	Microsoft email events
Windows Audit	Windows audit and sysmon events
Bluecoat	Web proxy events
WatchGuard - DNS	Web proxy DNS events
WatchGuard - VPN	Web proxy VPN events
Cisco ASA	Firewall and VPN events
Windows Sysmon	Windows system monitoring events
Symantec Endpoint Protection	Anti-virus events
Barracuda	Web email events
Palo Alto	Firewall, Proxy and VPN events
Web Sphere	Web traffic events
FireEye	Web download traffic inspection events
Source Fire	IDS events
Bro/Zeek	Flow data
Snort IDS	IDS events
Netflow, IPFIX	Flow data
AWS	Cloud security events
Azure	Cloud security events
AS/400 and iSeries	Mainframe
Box	Cloud services
Checkpoint OPSEC/LEA	Firewall and VPN events
Cisco SDEE	Content delivery events
Cloud/SaaS solutions	Cloud events
Cradlepoint	Network edge events
Flat files (single-line and multi-line, compressed or uncompressed)	Custom flat file events

Parser Name	Description
Flex Database Log Adapter for system and custom logs written to database tables (e.g., Oracle, SQL Server, MySQL) (ODBC & JDBC protocols)	Custom db events
Flow data (e.g., IPFIX, NetFlow, sFlow, J-Flow, SmartFlow)	Flow data
McAfee A/V	Anti-virus events
McAfee HIPS	Endpoint monitoring events
MSFT IIS	Web traffic events
Netflow, IPFIX	Flow data
Office 365	Microsoft Office 365 events
Qualys	Vulnerability events
Rapid7	Collectoin of web proxy events
Redhat Enterprise	OS events
Salesforce	CRM vents
SNMP	Traps event
Snort IDS	IDS events
Sourcefire eStreamer	IDS streaming events
Squid	Web proxy events
Symantec DLP	DLP events
Tenable Security Center	Security events
UDP/TCP and secure syslog	Custom network events
Vendor-specific APIs (example sources):	Collectoin of web proxy events
Vulnerability scanners (example sources):	Vulnerability events
Vendor-specific APIs (example sources):	Collectoin of web proxy events
Vulnerability scanners (example sources):	Vulnerability events

Plugin	Description
azure_event_hubs	Receives events from Azure Event Hubs
beats	Receives events from the Elastic Beats framework
cloudwatch	Pulls events from the Amazon Web Services CloudWatch API
couchdb_changes	Streams events from CouchDB's _changes URI
dead_letter_queue	read events from Logstash's dead letter queue
elasticsearch	Reads query results from an Elasticsearch cluster
exec	Captures the output of a shell command as an event
file	Streams events from files
ganglia	Reads Ganglia packets over UDP
gelf	Reads GELF-format messages from Graylog2 as events
generator	Generates random log events for test purposes
github	Reads events from a GitHub webhook
google_cloud_storage	Extract events from files in a Google Cloud Storage bucket
google_pubsub	Consume events from a Google Cloud PubSub service
graphite	Reads metrics from the graphite tool
heartbeat	Generates heartbeat events for testing
http	Receives events over HTTP or HTTPS
http_poller	Decodes the output of an HTTP API into events
imap	Reads mail from an IMAP server
irc	Reads events from an IRC server
java_generator	Generates synthetic log events
java_stdin	Reads events from standard input
jdbc	Creates events from JDBC data
jms	Reads events from a Jms Broker
jmx	Retrieves metrics from remote Java applications over JMX
kafka	Reads events from a Kafka topic
kinesis	Receives events through an AWS Kinesis stream

Plugin	Description
log4j	Reads events over a TCP socket from a Log4j SocketAppender object
lumberjack	Receives events using the Lumberjack protocl
meetup	Captures the output of command line tools as an event
pipe	Streams events from a long-running command pipe
puppet_facter	Receives facts from a Puppet server
rabbitmq	Pulls events from a RabbitMQ exchange
redis	Reads events from a Redis instance
relp	Receives RELP events over a TCP socket
rss	Captures the output of command line tools as an event
s3	Streams events from files in a S3 bucket
salesforce	Creates events based on a Salesforce SOQL query
snmp	Polls network devices using Simple Network Management Protocol (SNMP)
snmptrap	Creates events based on SNMP trap messages
sqlite	Creates events based on rows in an SQLite database
sqs	Pulls events from an Amazon Web Services Simple Queue Service queue
stdin	Reads events from standard input
stomp	Creates events received with the STOMP protocol
syslog	Reads syslog messages as events
tcp	Reads events from a TCP socket
twitter	Reads events from the Twitter Streaming API
udp	Reads events over UDP
unix	Reads events over a UNIX socket
varnishlog	Reads from the varnish cache shared memory log
websocket	Reads events from a websocket
wmi	Creates events based on the results of a WMI query
xmpp	Receives events over the XMPP/Jabber protocol

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

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

Phone: +1 (669) 209-0801

info@elysiumanalytics.ai