Anvilogic: Modern Security Operations Platform for Snowflake

Unify detection across hybrid, multi-cloud logging repositories and security data lakes powered by Snowflake.
Seamlessly combine legacy and new cloud workloads.

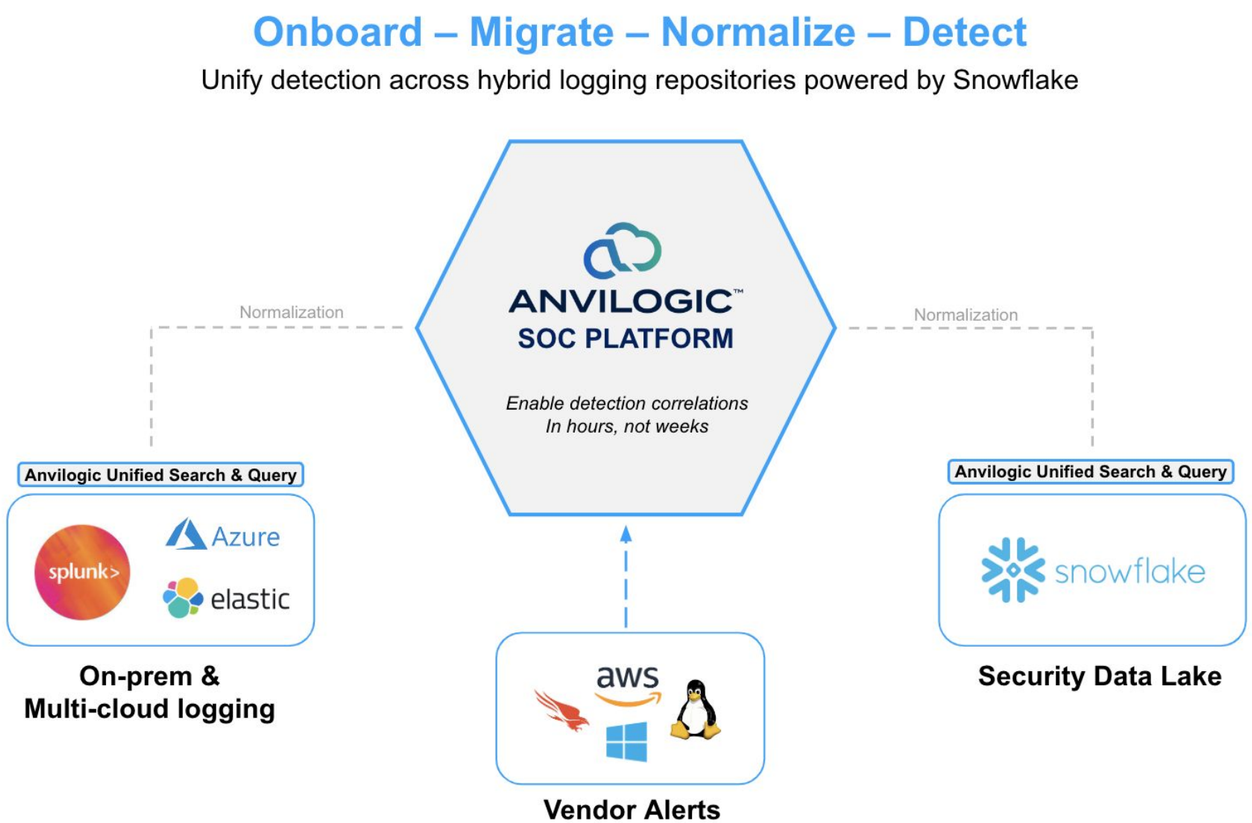
Modernize your security operations architecture.

Move away from data monoliths. Quickly build a security data lake on Snowflake.
Continuously prioritize alerts, detect, hunt and triage across all your platforms.

Easily Migrate Data & Gain Detection Efficacy: Prepare for new & future cloud workloads
Enable your security team to simplify tool complexity and easily detect, hunt, triage and respond across old and future workloads without needing to be cloud experts. Automatically onboard new cloud logs to Snowflake or migrate existing data sources from other hybrid and multi-cloud data repositories. This helps to augment existing people and process to keep up with the changing business needs.

Reduce Time to Detect & Respond: Automated Threat Detection (ATD) powered by Snowflake
Gain insights through centralized hunting and triage interface to help teams better correlate alerts, while also being able to deliver uniform detection and response across Snowflake and data monoliths, reducing impact on overall security operations and reducing mean-time-to-detect and respond to threats.

Reduce Cost & Scale Your Security for the Future
Anvilogic natively integrates with Snowflake, enabling security teams to seamlessly re-balance data from legacy, costly SIEMS and data monoliths while providing clear visibility and highly-accurate behavioral detections across all of your organizational hybrid-cloud and multi-cloud data platforms. Leverage machine learning and get recommendations that help to provide guidance on your critical data sources and steps to implement detections.



Security the way you need it. *Keep your data where you want it.* *Spend your time the way you want to.*

Anvilogic is a SaaS platform, Built to power modern security operations

Data Flow Deployment Architecture

Anvilogic powered by Snowflake

Data, Workloads, Alerts & Signal

- Easily and cost effectively detect across all logs, no matter where it's stored
- Gain access and highly-accurate behavioral-pattern detections to over 10x more data
- Anvilogic Unified Search queries your logs, normalizes, tags and enriches your alerts and signal to easily unify across data sources from hybrid, multi-cloud and security data lakes to correlate and deploy detections
- Easily move data from logging repositories seamlessly into Snowflake
- Reduce management costs by 50%

Detect, Hunt & Triage

- Effectively detect behavioral attack-patterns across singular incidents to identify and hunt for threats powered by Snowflake
- Anvilogic enables teams to continually assess, prioritize and detect across massive amounts of logging data that is cheaply stored in Snowflake
- Leverage Anvilogic to automatically ingest and prioritize security product alerts, like Crowdstrike, Proofpoint, Carbon Black, and more
- Anvilogic's Automated Threat Detection (ADT) powered by Snowflake helps teams continuously prioritize, maintain, tune and deliver unified detections across organizational workflows
- Anvilogic's Armory provides Snowflake Detection Content to quickly deploy detections for AWS Cloudtrail logs, VPC Flow logs and Crowdstrike FDR
- Centralized hunting and triage of alerts from across logging repositories and security data lakes
- Drive productivity of SOC teams - detection engineers, security analyst, threat investigators/hunters

Continuous Maturity Recommendations

- Anvilogic powered by Snowflake Security Data Lakes enables security teams to modernize and create a foundation for their security operations strategy
- ML-Driven recommendations for migrating data and detections to Snowflake for improved detection efficacy and optimizing cost
- ML-Driven Recommendations to help assess and prioritize detection state across

Recommended Detection Content

- Over 800 ready-to-deploy detections (more added daily)
- Daily detections updated based on trending threats
- Trending topics directly in the Anvilogic platform
- Purple Team threat research & intelligence
- Premium Threat Scenario Detection Packs
- Data Normalization & Parsing alerts

Anvilogic's Splunk & Snowflake Integration

Data Flow

- Data Normalization & Parsing alerts
- Data flows from Splunk to Snowflake
- Data schema normalizes, tags and enriches

Detect

- Machine Learning Models
- Anvilogic Automated Threat Detection (ATD) insights help to correlate alerts from Splunk and Snowflake
- ATD provides a summarized view of all alerts from various frameworks, like MITRE ATT&CK, Kill Chain and more

Hunt & Triage

- Anvilogic event summary dashboard centralizes hunting and triage interface and provides investigation-worthy spotlight events, which are delivered from Anvilogic's ATD and threat research team
- Machine Learning further enriches data to help find and remove false positives or unwanted alerts
- Anvilogic threat hunting team augments your existing threat hunting to determine and escalate suspicious activity
- Significant alerts are sent to triage dashboard for investigation

Continuous Maturity & ML-Recommendations

- ML-Driven recommendations for migrating data and detections to Snowflake for improved detection efficacy and optimizing cost
- ML-Driven recommendations to help assess and prioritize detection state across various security tools

Technical Requirements

Setting up Snowflake

- Your organization will need to be using or considering moving to Snowflake
- No Snowflake? Anvilogic makes it quick and easy to deploy Snowflake and can help offset the management of the security detections and schema updates
- One-time only, step-by-step copy-paste for set-up regardless of data sources
- You'll need the *accountadmin* role in Snowflake to configure the integration
- Run provided commands in documentation to create the database schemas, and warehouse
- Run provided commands in documentation to create roles with restricted access to Snowflake
- Create an S3 storage integration so Snowflake can store generated user identities and access management (IAM) entity following step-by-step copy-paste documentation
- Then it's time to get your data in…it's actually pretty simple

Easily troubleshoot & validate

- Easily verify Snowflake is being used by the Anvilogic Platform by checking the Maturity Score, Data Feeds, and Data Repository column
- Documentation for troubleshooting is provided

Getting data into Snowflake…it's pretty simple

The data will be in a format that can be recognized and used by the Anvilogic content framework to produce events of interest (EOIs) and generate detections across all logs leveraging the Anvilogic Platform.

Cloudtrail Logs

- Cloudtrail Documentation
  - One-time, step-by-step process of copy-pasting to create the following:
    - Staging table to prepare your data files for loading
    - Data source table with necessary table columns to define the schema of your Cloudtrail data
    - Staging to create an external staging table where your Cloudtrail data files are stored
    - Automated Snowpipe for integration with your AWS S3 bucket that allows data loads to trigger automatically
    - Create a stream to populate the data table
    - Create tasks to start the data flowing from Cloudtrail to Snowflake

VPC Flow Logs

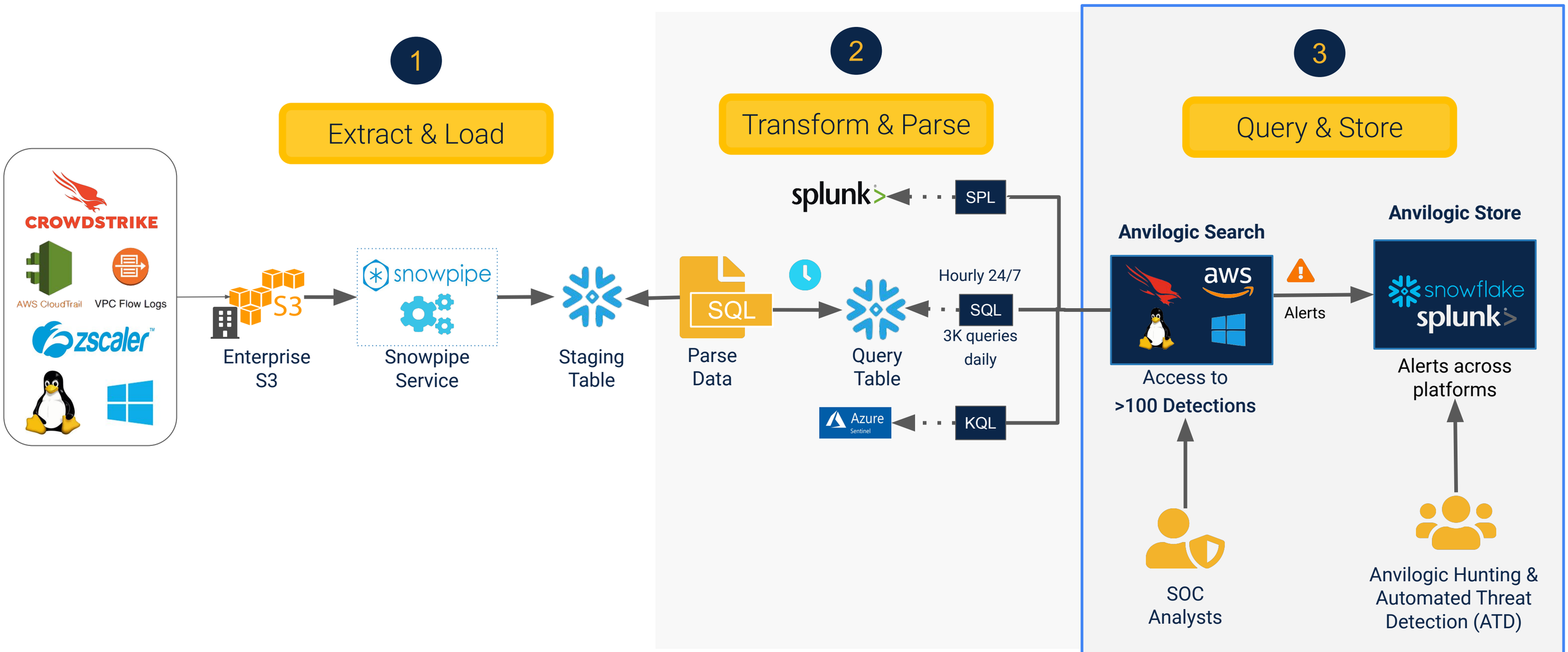
- VPC Flow Logs Documentation
  - One-time, step-by-step process of copy-pasting for the following process:
    - Data source table with the necessary table columns to define the schema of your VPC Flow data
    - Permissions to the Snowflake role
    - If you already have data sources integrated with Snowflake you only need to update the allowed storage locations
    - Create external staging table where your VPC Flow data files are stored
    - Create an automated Snowpipe for integration with your AWS S3 bucket allowing data loads to be triggered automatically

Crowdstrike FDR

- Documentation Coming soon
  - One-time, step-by-step process of copy-pasting for the following process:
    - Staging table to prepare data
    - S3 integration to insert S3 path for notification queue
    - Staging to create external staging table
    - Automated Snowpipe for integration with AWS S3 buckets
    - Staging to create external staging per data type to run tasks against stream
    - Create a stream to process rollup and populate the data table with enriched identity and host information

…Many more being frequently released

Anvilogic for Snowflake



ANVILOGIC