JASK INSIGHT

Going from Records to Signals to Insights

Records processing in JASK differs from the methods SIEM solutions take to process events into alerts. JASK's multi-step analysis results in Insights - a collection of related threat signals that provide context and timeline for an analyst to review. This brief provides an overview of JASK's records analysis methodology.

Records Processing

JASK collects, parses, and normalizes enterprise security telemetry into a single, consistent data store. The data streams consist of all security-relevant data. This includes traditional security and alert sources (e.g., firewall, IDS/IPS, SIEM, etc.) but also sources that contain security-related data not typically captured (e.g., network traffic, user entities). As appropriate, the telemetry referencing external assets (e.g., domain names, file hashes, etc.) are enriched with external context.

Because JASK does not charge for data ingestion rates or volume, customers do not need to compromise on visibility in selecting data sources. For clarity, due to flexibility in records ingestion, JASK can be added to, or sit in place of, the SIEM.

Signal Generation

From records, JASK generates Signals. Existing alerts within your environment are converted into Signals, however, Signals encompass a much broader scope to include "records of interest". As an example, HTTPS connections to servers with self-signed SSL Certificates or unusually high data transfer rates for a server could never be promoted to an alert that requires an analyst's attention. However, they are interesting, especially if they are linked to other related Signals.

Signals are generated using a variety of methods:

- Existing alerts are converted into Signals
- Threat Intel match: file hash, connection to a known bad IP address
- Pattern match: rules and conditions such as a SYN flood or suspicious logon attempts
- A data stream anomaly: deviation from an established baseline

As expected, more signals may be generated than traditional alerts, particularly as additional data streams are consumed by JASK.

Insight Creation

An Insight is the set of related Signals, presented to an analyst with the context required for a decision. This can be a procedural shift in the SOC: the analysts no longer look at individual alerts to triage; the analysts now look at Insights. In the previous section, it was noted that more signals are generated than alerts. Following that assertion, there are far fewer Insights than traditional alerts.

Insights leverage machine learning algorithms trained on security analyst procedures to collect related alerts and add contextual data (e.g., 3rd party threat intelligence), automating the alert triage process. The creation of an Insight occurs when the collection of signals exceeds a predetermined threshold, surfacing the case for a human analyst to review.

No single signal is deemed sufficient to demand an analyst's attention. This is a critical concept: while an existing alert would be converted into a JASK Signal. But that single signal would not be brought to the attention of an analyst.