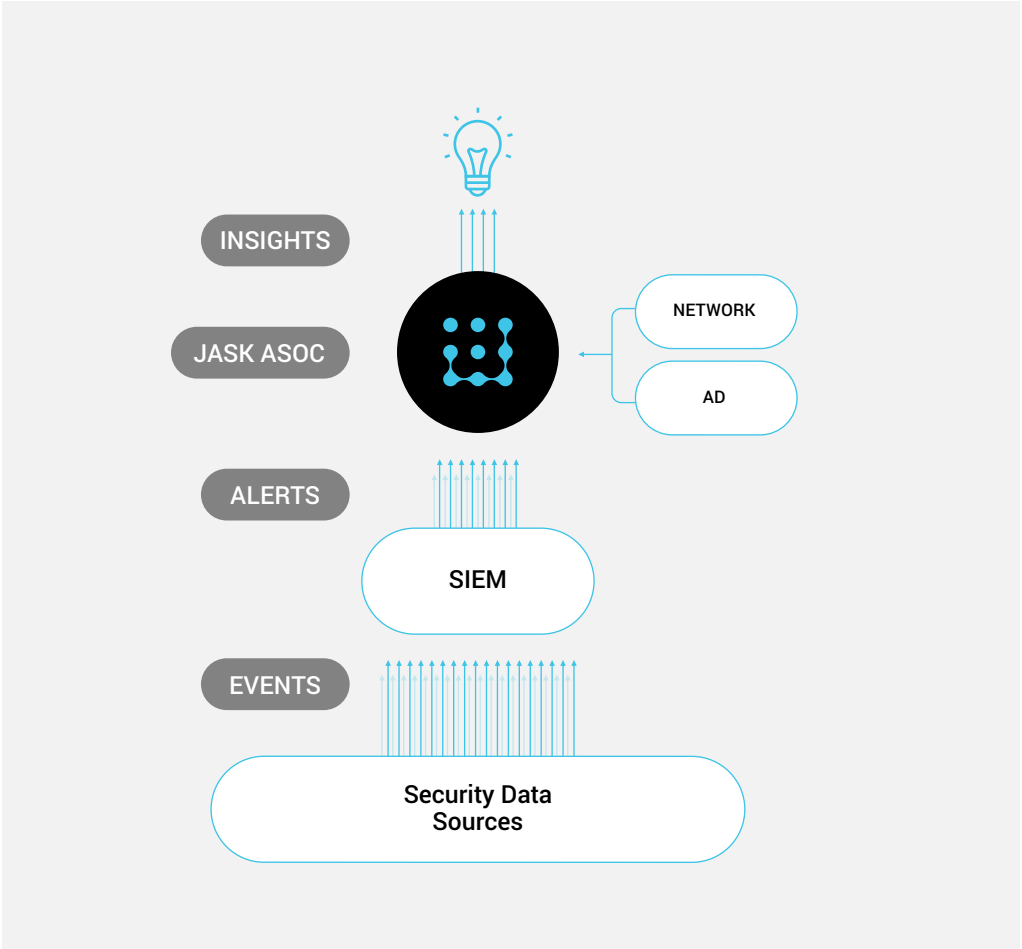
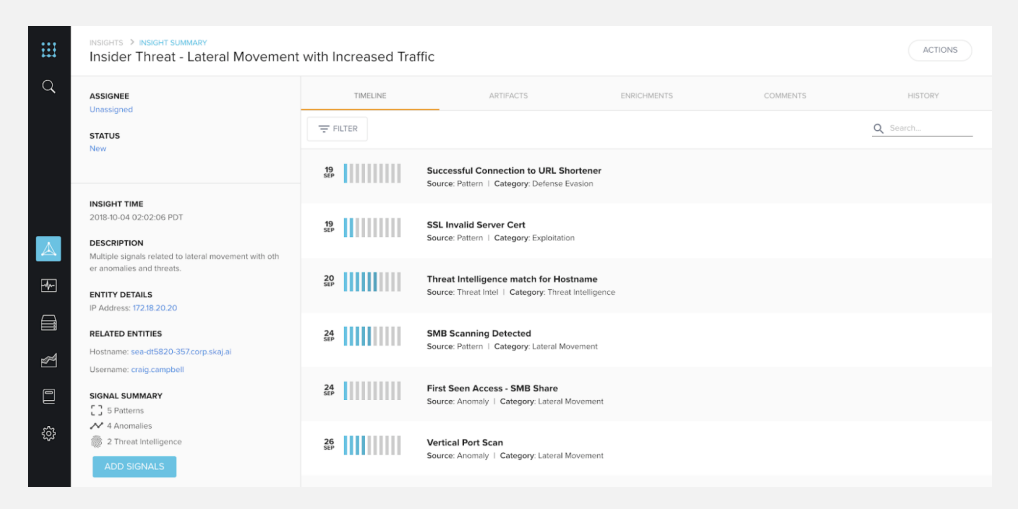
// AUGMENTING SIEM

The easiest way to start using JASK today

SOC analysts are fighting a losing battle because SIEMs commonly fail to provide critical context and visibility for each alert. Constraints on data ingestion force organizations to limit their data sources. Without the supporting events, such a network traffic or user behavior, analysts are forced to make sense of alerts while missing critical pieces of information. This is compounded by the alert fatigue faced by many SOCs, where analysts routinely face more than 1,000 alerts on a daily basis. As the threat landscape continues to become more dynamic, more security tools are implemented, creating an exponential increase in the alert volume. Under these extraordinary conditions, analysts are under immense pressure to triage and respond to more alerts than ever.

JASK solves this issue for the SOC by leveraging the power of Artificial Intelligence to enable the analysts to become more effective. JASK takes the collective experience of seasoned security analysts to automate the triage of SIEM alerts. Using JASK to augment your SIEM allows analysts to work with a handful of JASK Insights rather than validating each and every low-fidelity SIEM alert, dramatically improving the efficiency of your analysts and enabling them to better manage and reduce the risks to your organization.





Insights, Not Alerts

Analysts spend the bulk of their time investigating SIEM alerts to determine the valid alerts from the noise. Unfortunately, while this is necessary, the effort is largely manual, extraordinarily time consuming, and worse of all, isn't effectively reducing the risk to the organization.

Leveraging Artificial Intelligence, JASK automates the triage process. The intelligent collection of signals into a JASK Insight completes the "storyline" of a potential incident, where the grouping of signals now provides critical context. JASK also understands and learns the common sources of threat intelligence enrichment that analysts frequently leverage and automatically adds this to the Insight. Freed from the manual effort of triaging each and every alert for validity, the analyst is enabled to dig into the Insight and immediately begin the higher value functions of investigations, threat hunting, and response.

High Fidelity Visibility

Most SOCs have limited visibility into their enterprise. Cost constraints imposed by SIEM licensing models force many organizations to limit the amount of data they ingest. This compromise generally results in only core security sources to be considered: Firewalls, IDS/IPS, endpoint AV, and secure web/email gateways.

JASK completely reframes this issue. By focusing on grouping related signals into an Insight, what may have been a low-fidelity event, is now a critical component of an Insight, providing greater depth and detail that a SIEM fails to deliver.

Furthermore, JASK doesn't penalize customers for including more data for analysis. Because enterprise visibility requires the full breadth of security and security-related sources.

Cloud-based Architecture

The modern SOC needs a modern technology architecture. JASK's cloud-native architecture enables capabilities that legacy on-premises solutions cannot overcome.

The cloud provides scale. The JASK platform provides automatic scaling as event and data sources increase or spike to ensure processing occurs when you most critically require it. And unlike on-premises solutions that can only analyze a fraction of the ingested data, JASK isn't constrained by hardware processing power. Our machine learning models analyze the full breadth of data – all of the standard security sources, plus the addition of network, user, etc.

Furthermore, as a SaaS solution, JASK excels at speed of innovation. New capabilities and updated learning from our machine learning algorithms are available quickly - not limited to your ability to schedule and implement an upgrade to your systems.