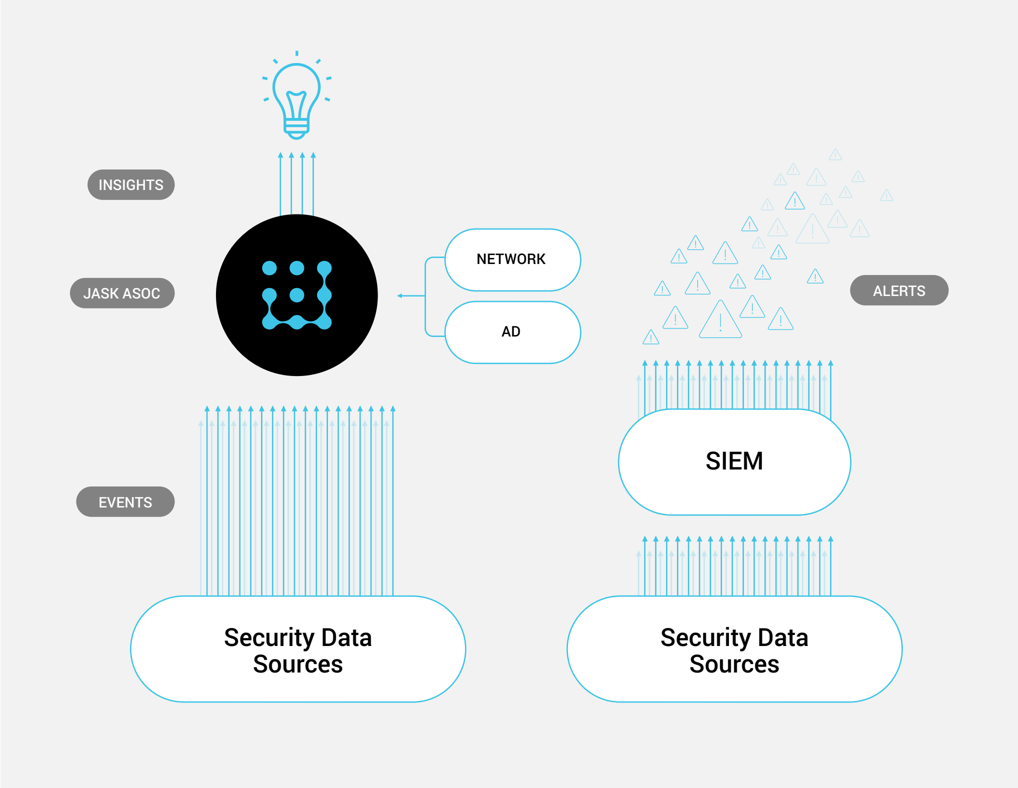
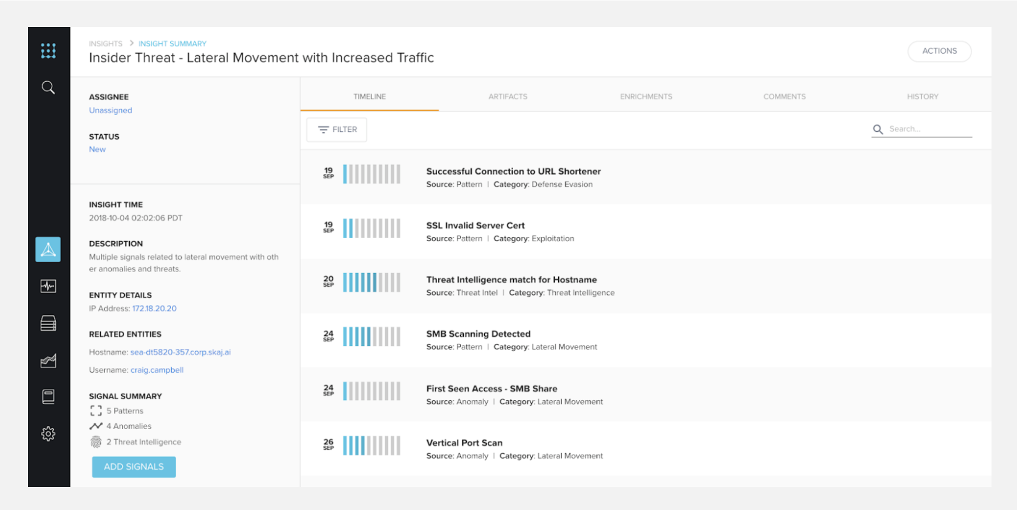
// REPLACING SIEM

Modernize your SOC with the JASK Autonomous SOC Platform

As alerts skyrocket due to the dynamic nature of today's threat landscape and are generated by new point solutions, the SOC needs to evolve to keep pace. The legacy SIEM architecture no longer meets the needs of the modern SOC. Analysts today spend too much time triaging each alert, due to lack of context and visibility, leaving little time available to perform more valuable risk-mitigating functions such as threat hunting. Worse yet, due to the tremendous alert volume, many organizations don't even manage to review all the alerts, leaving potential critical issues lingering.

JASK tips the balance in favor of the modern SOC by leveraging Artificial Intelligence to automate the alert triage process. By freeing the analysts of this low-level task, they are enabled to perform higher impact activities to reduce cyber risk, such as threat hunting and response planning. JASK provides the platform to leverage machine learning, which learns from the actions of experienced security analysts, to automate the grouping of related threat signals into JASK Insights. By surfacing JASK Insights, rather than triggering alerts for individual suspicious events, the analyst no longer needs to address each low-fidelity alert. Instead, the analysts are immediately launched into the investigation and threat hunting phase - truly reducing the overall risk to the organization.





Insider Threat - Lateral Movement with Increased Traffic

ASSIGNEE
Unassigned

STATUS
New

INSIGHT TIME
2018-10-04 02:02:06 PDT

DESCRIPTION
Multiple signals related to lateral movement with other anomalies and threats.

ENTITY DETAILS
IP Address: 172.18.20.20

RELATED ENTITIES
Hostname: sea-dt5820-357.corp.skaj.ai
Username: craig.campbell

SIGNAL SUMMARY
5 Patterns
4 Anomalies
2 Threat Intelligence

19 SEP — **Successful Connection to URL Shortener**
Source: Pattern | Category: Defense Evasion

19 SEP — **SSL Invalid Server Cert**
Source: Pattern | Category: Exploitation

20 SEP — **Threat Intelligence match for Hostname**
Source: Threat Intel | Category: Threat Intelligence

24 SEP — **SMB Scanning Detected**
Source: Pattern | Category: Lateral Movement

24 SEP — **First Seen Access - SMB Share**
Source: Anomaly | Category: Lateral Movement

26 SEP — **Vertical Port Scan**
Source: Anomaly | Category: Lateral Movement

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.