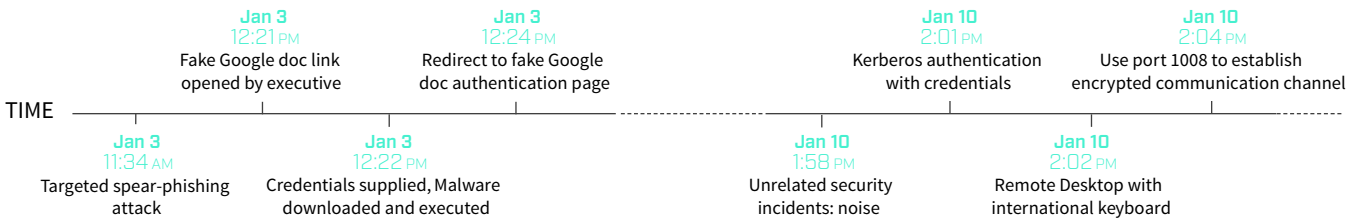
JASK

SECURITY OPERATIONS ACCELERATED

The SOC Model Is Broken. We Know How To Fix It. JASK believes the traditional, analyst-led security operations center (SOC) model is fundamentally broken. Teams spend more time on routine threats and keeping their SIEM up and running than on protecting their organizations from the most dangerous targeted attacks. Without a new approach and an innovative platform, SOCs can't scale to meet the volume and sophistication of modern attacks.

Example of Attack Scenario Seen Daily by Organizations Worldwide



TYPICAL SOC RESPONSE	Overworked analysts miss connections among parts of the attack over time	The content team is required to set up 100s of correlation rules in the SIEM.	Analysts can't identify the real attack in the "noise" of 100s of alerts
WHY DOES THE SOC DEFENSE POSTURE FAIL?	*Heavy reliance on legacy tech.* This old and costly technology leaves blind spots and doesn't provide required context.	*Manual and rule-based operations.* Alert-fatigued analysts can't distinguish real attacks from noise.	*Human limitations.* Security investigations involve billions of events and hundreds of alerts.

JASK Starts With A Clean Slate. JASK was founded with a simple mission: to deliver an artificial intelligence (AI)-based security analyst that automates 80 percent of threat detection in a SOC, allowing human security analysts to focus on mitigating real attacks.

JASK is designed for scale. Spark and Hadoop along with an elastic SaaS-driven infrastructure allows SOC teams to focus on real threats instead of infrastructure. JASK is built with a modern Lambda architecture to support organizations through the next decade of security challenges. It is focused on delivering three key outcomes:

1 DETECTING MODERN ATTACKS

Modern attacks are multipart and multi-stage, and can last for days or weeks. Adversaries' patterns—permutation and combination of attack vectors—are large, but modern compute clusters can detect them. JASK fingerprints these patterns with "Hacker Behavior Analytics."

2 USING AI TO AUTOMATE SECURITY ANALYSIS

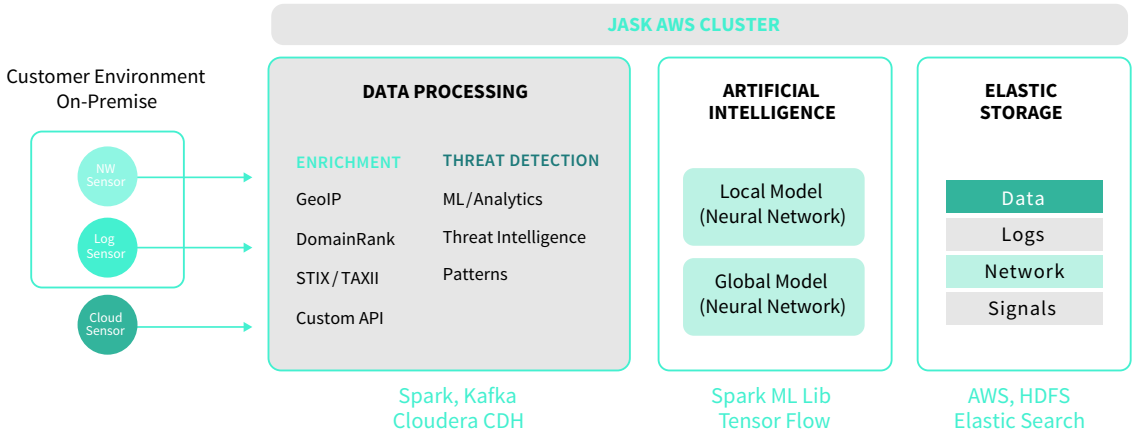
JASK automates the task of determining which alerts ("Signals") represent real hacker activity. Using deep learning/neural network-based learning, the system learns and adapts so it can identify the signals of a multipart and multistage attack. This insight from JASK enables security analysts to focus on true attacks, not noise.

3 EVOLVING THE "PREDICTIVE SOC"

Imagine a global SOC that can learn from attacks across each organization and deploy AI models to detect the latest threat. Hackers often use the same techniques and tools across attack campaigns. JASK uses shared analytics and AI models to predict the next attack.

JASK: SECURITY OPERATIONS ACCELERATED

JASK Technology: Big Data + Cloud In The DNA



LOG, NETWORK AND CLOUD SENSORS
Virtualized sensor collects network data using deep packet inspection (DPI). Log data in CEF and syslog from any device.

CONTEXT AND ENRICHMENT
Uniquely identify entities from network, endpoint, and log data. Enrichment includes GeoIP, IOCs, and internal custom data.

MULTIPLE THREAT DETECTION ENGINES
Anomaly Detection, Threat Intelligence, and Patterns/Analytics engines produce Signals.

ARTIFICIAL INTELLIGENCE (AI)
Machine-learning and deep-learning technologies connect the dots on Signals to identify real threats and create Smart Alerts.

INVESTIGATION
All raw logs and network events are stored for investigative analysis. Security analysts can use modern tools such as D3-based visualizations for ad-hoc queries and reports.

"TRAINING A MACHINE TO THINK LIKE A SECURITY PRO." **JASK AI 101**

CHARACTERISTICS OF THE JASK-POWERED SOC:

- Hundreds of thousands of data points from network and log data ingested per second.
- Machine-learning engines produce Signals that identify threatening events.
- AI engine automatically connects Signals to detect real attacks.
- Security Analysts can focus on a handful of Smart Alerts.