KOGNOS + INTEL 471
Solution Brief

KOGNOS OPERATIONALIZES INTEL 471 THREAT INTEL WITH FULLY AUTONOMOUS HUNTS

The Challenge

Attackers are in your network. The key is to find them as fast as possible and shut them down to minimize, or ideally prevent, any impact. In order to do so, you need to quickly identify any anomalous behavior, figure out which is and isn't a threat, and trace those threats to understand exactly how long they've been there, everything they've touched and everything they did. If you miss anything (e.g., a machine or connection), it may enable an attacker to persist.

Unfortunately, uncovering attack behavior that attackers are trying to hide and pinpointing the events/alerts that are meaningful is difficult, even with tools to help you identify where to focus. The reality is, the onus remains squarely on the shoulders of analysts, who are often under-resourced and overwhelmed, to make the connections and fill in gaps of an attack's story, from beginning to end.

The Solution

Operationalize Intel 471 threat intelligence to proactively look for adversary stories in an environment.

Integrating Intel 471's intelligence into Kognos XDR Hunter helps to strengthen security teams' ability to quickly gather and hunt so they can proactively thwart malicious actors, threats, and imminent attacks from successfully infiltrating an organization, its products, and assets.

- Weaponize Intel 471 cyber underground intelligence to optimize hunts for the presence of cybercriminals using Intel 471 flagged IP, domains, URLs, process hashes in the environment, and investigate. autonomously to generate attack storylines.
- Provide security teams with the full context of cybercrime, including adversaries, attack types, attribution, etc. using Intel 471 threat intelligence as part of their storyline reviews.
- Remediating threats within minutes of an attacker entering the environment.

Highlights and Benefits

The Kognos platform streams Intel 471 threat intelligence feeds to the customer environment.

- Kognos hunts for presence of Intel 471 flagged IP, domains, urls, and process hashes in the environment and investigates autonomously to generate attack storylines.
- Security teams can view complete context of adversaries, attack types, attribution, etc. from Intel471 as part of storyline review.
- Security teams can now remediate threats within minutes of an attacker entering the environment.

Kognos at a glance

Kognos provides the first network effect to cyber threat hunting. The solution enables autonomous threat hunting that allows customers to share their hunt recipes and have strength in numbers. Founded on the principle that attacker behavior is indicative of attack methodology, attribution, and data for exfiltration, Kognos leverages the power of relationships using security aware AI to fundamentally reduce dwell time by tracing the attacker's path in real-time, independent of any XDR.

Technology Integrations:

- Endpoint data from Carbon Black, CrowdStrike, Microsoft Sysmon, Linux AuditD, MacOS OpenBSM
- SIEMs including Splunk, Elastic
- NDR platforms including RSA NetWitness and Zeek

Intel 471 at a glance

Intel 471 empowers enterprises, government agencies, and other organizations to win the cybersecurity war using near-real-time insights into the latest malicious actors, relationships, threat patterns, and imminent attacks relevant to their businesses.

Intel 471's TITAN platform collects, interprets, structures, and validates human-led, automation-enhanced results. Clients across the globe leverage this threat intelligence with our proprietary framework to map the criminal underground, zero in on key activity, and align their resources and reporting to business requirements. Intel 471 serves as a trusted advisor to security teams, offering ongoing trend analysis and supporting your use of the platform.