KOGNOS
autonomous XDR investigator

KOGNOS AUTONOMOUS EDR HUNTER

THE FIRST AND ONLY PLATFORM TO LEVERAGE THE POWER OF RELATIONSHIPS TO AUTONOMOUSLY HUNT FOR ATTACKS/CAMPAIGNS

TECHNOLOGY

THE POWER OF RELATIONSHIPS

- Revolutionary way of looking at security data
- Events give you alerts, relationships give you attack campaigns
- Trace the attacker's path in real-time as they move around in your environmeent

AI THAT UNDERSTANDS SECURITY

- Make machines understand security data & Investigate autonomously
- Data collection v/s data understanding
- No more open-ended analytics and no more false positives

DEEP ARSENAL OF SECURITY QUESTIONS

- Thousands of MITRE mapped dynamic questions
- No more writing complex rules or scripts
- No more cumbersome

Hunting for threats in EDR data

Most organizations are collecting 25 MB of telemetry each day per endpoint. For a ten thousand device environment, this translates to around 7.5TB of data each month. A threat can easily diffuse into this massive data volume making it humanely impossible for a hunter to trace the adversary's activities. Hunters need machines to assist in this endeavor to produce any meaningful results. Kognos EDR Hunter is an autonomous EDR threat hunting platform, allowing an organization's valuable endpoint telemetry to be put to proactive hunting as opposed to post breach forensic analysis.

How to solve it?

Kognos EDR Hunter is the first and only platform that allows threat hunters to do point and click hunting. The autonomous platform enables hunters to spend their time deciding what IOCs or behaviors to hunt for, but leave the data mining to machines to locate the suspect artifacts and investigate them to uncover every step the adversary took across the environment. The threat hunter as a result can now review machine-investigated storylines that are associated with the IOC or behavior of interest and remediate them holistically.

KOGNOS
autonomous XDR investigator

KOGNOS AUTONOMOUS EDR HUNTER

THE FIRST AND ONLY PLATFORM TO LEVERAGE THE POWER OF RELATIONSHIPS TO AUTONOMOUSLY HUNT FOR ATTACKS/CAMPAIGNS

Kognos seamlessly integrates endpoint data from Carbon Black, CrowdStrike, Microsoft Sysmon, Linux AuditD, MacOS OpenBSM. It only takes 15 minutes to set up and your threat hunters can start triggering autonomous hunts right away.

Machine-assisted threat hunting

- Ability to do ad-hoc searches for processes, behaviors, process actions, network, etc. as part of the hunt process and trigger full investigations.
- Ability to integrate threat intelligence to hunt for the presence of suspicious artifacts and trigger full investigations.
- Ability to look for suspect behaviors, including Lateral Movement, Persistence Mechanisms, Living off the land binaries, etc. artifacts and trigger full investigations.

Fully autonomous continuous threat hunting

- Ability to convert any ad-hoc searches to scheduled hunts to be run at hourly, daily, weekly boundaries and trigger full investigations. The identified stories are bubbled up based on the risk profile of the story.

Kognos continuously monitors billions of relationships to detect suspicious behavior. Once detected, Kognos uses an AI powered inquiry engine to ask thousands of forensic questions per second to fully contextualize the attack and present the findings as complete attack campaigns, allowing the analyst to respond in real-time

Trace the adversary's path in real-time as they move around in the environment

USE CASES

LATERAL MOVEMENT TOOL USAGE

Sophisticated attackers use various entry vectors to establish their initial foothold and then laterally move across the infrastructure looking for high profile targets. Trace the attacker's path as the attacker propagates within your infrastructure

LIVING-OFF-THE-LAND TOOL USAGE

Stealthy attackers often use malware-less attacks to evade detection and live off the land. Trace the attacker's LOTL activity by evaluating their cumulative behavior across their entire chain of activity

INSIDER THREATS

Insiders threats are the hardest to detect as their identity, access and majority of their behavior looks legitimate. Detect unusual user behavior as the system tracks through the user's entire chain of activity

KOGNOS
autonomous XDR investigator

KOGNOS AUTONOMOUS EDR HUNTER

THE FIRST AND ONLY PLATFORM TO LEVERAGE THE POWER OF RELATIONSHIPS TO AUTONOMOUSLY HUNT FOR ATTACKS/CAMPAIGNS

PRODUCTS

AUTONOMOUS EDR HUNTER

- Eliminate data fatigue
- Eliminate analysis bias
- Review EDR hunt results as attack storylines in real-time

AUTONOMOUS XDR HUNTER

- Eliminate tool fatigue
- Eliminate data fatigue
- Review unified storylines acros all your security products

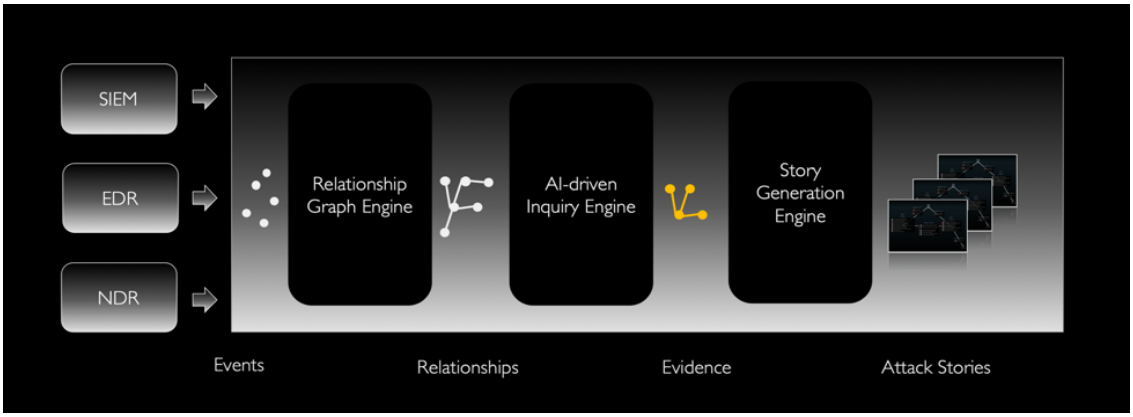
AUTONOMOUS ALERT INVESTIGATOR

- Elimiinate alert fatigue
- Eliminate false positives
- Review fully investigated attack storylines in real-time

ENABLE THE FULL KOGNOS AUTOMATION SUITE TO

- Detect attempted, failed and active campaigns.
- Lower your MTTD/MTTR to minutes

How it works?



RELATIONSHIP GRAPH ENGINE

The relationship graph engine interprets high fidelity EDR events and forms relationship graphs which are essential in understanding the full scope and impact of the attack as it allows the system to cumulatively look at risk across the entire adversarial activity

AI- DRIVEN INQUIRY ENGINE

The AI-driven inquiry engine will investigate hundreds of billions of relationships by asking thousands of forensic questions per second to identify relevant evidence highlighting the entire attacker's path in real-time

STORY GENERATION ENGINE

The story generation engine continuously fuses the evidence collected to form easily understandable attack stories and timelines of the complete attack allowing the analysts to respond in real-times

Kognos continuously monitors billions of relationships to detect suspicious behavior. Once detected, Kognos uses an AI powered inquiry engine to ask thousands of forensic questions per second to fully contextualize the attack and present the findings as complete attack campaigns, allowing the analyst to respond in real-time

Trace the adversary's path in real-time as they move around in the environment

See the products in action

Please request a demo via our website at https://www.kognos.io/book-a-demo/ or reach us at info@kognos.io.

2064 Walsh Ave, STE C1
Santa Clara,
CA - 95050