KOGNOS
never hunt alone

TURBOCHARGE YOUR CARBON BLACK DEPLOYMENT
WITH KOGNOS AUTONOMOUS THREAT HUNTING

Introduction

While reflecting on the breaches of 2020, there is a trend that has become clear: intruders are becoming more brazen in their choice of tactics and targets. From supply chain subversion to ransoming critical utilities, no organization is being spared. The threat and risk landscapes are constantly changing, but this trend is adding a sense of urgency to adopting a more proactive approach to an organization's information security program.

The price-of-admission to a modern information security program is endpoint telemetry, along with the other sensors. From these disparate indicators, spread across several or more data sources - often representing terabytes or petabytes of data - an analyst can piece together an intrusion, given enough time and resources.

Endpoint telemetry from Carbon Black is a good source for threat hunting, but it's also voluminous and can easily overwhelm your analysts. Carbon Black has partnered with Kognos to enable fully autonomous threat hunting - on top of Carbon Black telemetry - to provide machine assistance to threat hunters who want to proactively hunt.

To identify sophisticated adversaries, security teams need to do proactive hunting based on multiple hypotheses - and perform deep investigations of the telemetry.

Carbon Black – High Fidelity Telemetry

Carbon Black collects and visualizes deep telemetry from endpoints, giving security teams unparalleled visibility. The high-fidelity telemetry contains process execution, library loads, registry access, and file activity - as well as network connections and DNS queries. Many organizations effectively use Carbon Black data for passive monitoring, manual investigations and responding to threats.

However, to identify sophisticated adversaries, security teams need to do *proactive hunting* based on multiple hypotheses - and perform deep investigations of the telemetry to filter the adversary activity from the raw telemetry. *Doing this is hard even for the most skilled threat hunters - but doing it continuously and consistently is humanly impossible.*

KOGNOS
never hunt alone

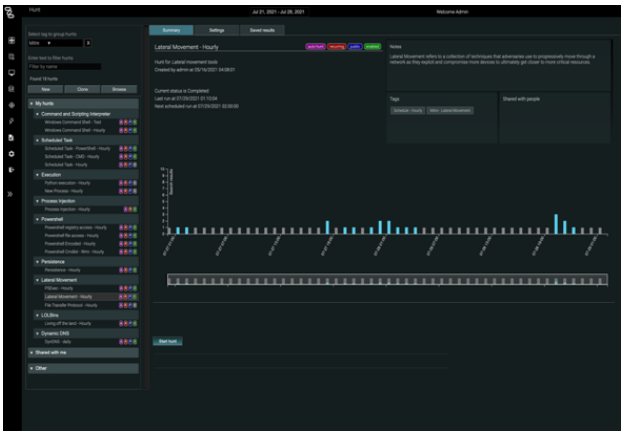
Kognos – Autonomous Threat Hunting

The Kognos hunting platform is built around its unique *Attack-Tracing AI,* imbibed with security domain knowledge to hunt down adversaries by

1) Constantly predicting next steps based on observed activity, and;
2) Asking additional exploratory questions to trace adversary's every step as they move around the environment

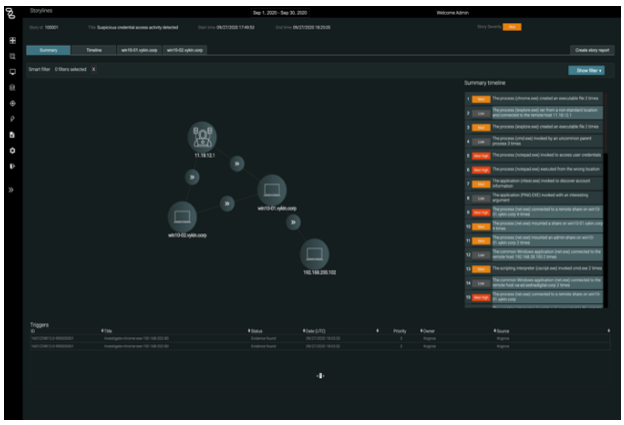
Point and Click Hunting

The Kognos platform allows threat hunters to do point and click hunting using Carbon Black data via hundreds of hunt hypotheses. The system will look for behaviors associated with these hypotheses and investigate autonomously using the *Attack-Tracing AI* powered inquiry engine to ask millions of forensic questions at machine speeds.



Kognos mines the Carbon Black data to autonomously investigate malicious users or external actors throughout the environment - and presents the findings as attack storylines, allowing the analyst to detect and stop emerging attacks. *This level of deep questioning of Carbon Black data will trace out even the subtlest of attackers as they intentionally try to hide in normal behavior to evade defense.*

Tracing Attackers In Real Time



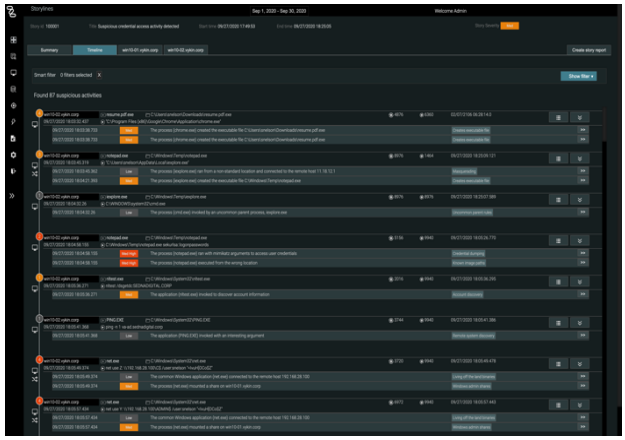
Once a hunt hypothesis is triggered, the Kognos Attack-Tracing AI engine will start the interrogation of Carbon Black data to trace attacker's every step and present them as visual storylines - with interactive summary views for your security team to review and understand the adversary activity in mere minutes.

Alerts generated by Carbon Black will also be picked up by Kognos and investigated autonomously to provide complete context as attack storylines.

Pre-investigated Attack Timelines

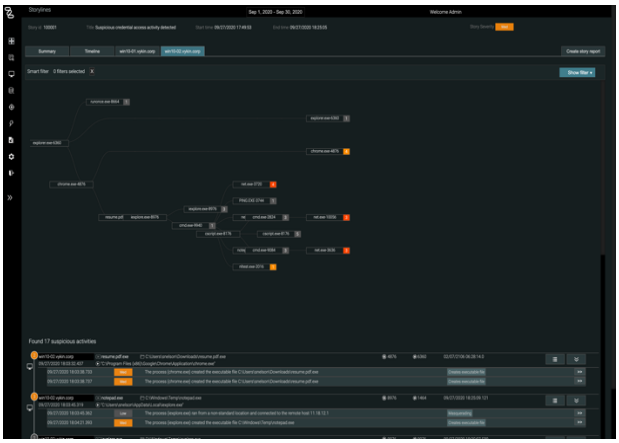
The detailed timeline of adversary's every activity is enumerated as evidence with additional context.

This view also provides options to take further actions including threat intel lookups, quarantining processes, isolating devices, setting firewall rules, DNS sinkholing, etc.



The evidence can also be traced back to the raw Carbon Black events for complete context.

Real-time Response



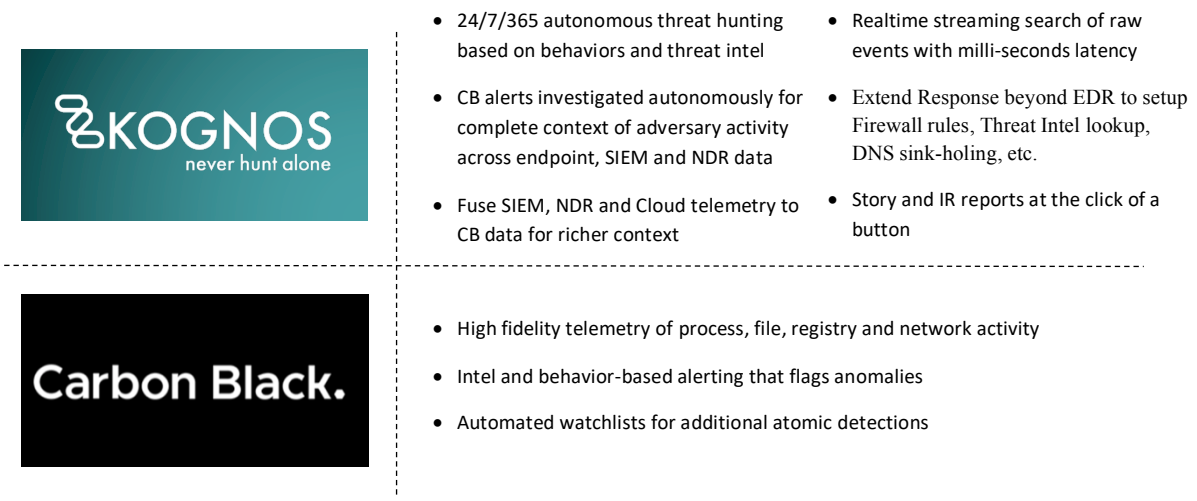
The command sequences that the attacker executed in each device is also traced and enumerated for complete context.

The multi-machine storyline, timeline and the command context provide multiple perspectives for the security team to understand the story in minutes and respond to it in real-time.

With the combination of comprehensive telemetry from Carbon Black and Kognos autonomous threat hunting, organizations can now proactively look for adversary behaviors - stopping attacks before they hit your critical assets.

Autonomously Trace Attackers' Steps From Carbon Black Data

The Kognos autonomous hunter connects directly with the Carbon Black cloud APIs to bring the power of Kognos automation to Carbon Black EDR. Once connected the data is continuously imported and transformed into machine understandable relationship graphs that can be interrogated by the attack tracing AI.



Let your team hunt across terabytes of telemetry, moving them up the value chain with fully automated hunts and investigations, and enabling them to collaborate with the team and community to find advanced threats.

The combination of Carbon Black and Kognos redefines your security posture with autonomous and proactive hunting and investigations - stopping all attacks before they can cause serious harm.

About Kognos

Launched in 2020, Kognos is the cybersecurity industry's first and only autonomous XDR investigator platform that detects, investigates, and responds to attack campaigns. 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.