KOGNOS
never hunt alone

Case Study: Carbon Black Deployment Financial Services Company

THE FIRST AND ONLY THREAT HUNTING PLATFORM TO TRACE THE ADVERSARY'S PATH IN REAL-TIME.

Industry

Financial Services Company

Location

United States

Challenge

- Small security team struggling to keep up investigating only 10% of the alerts generated by different systems.
- Wanted to start a proactive threat hunting practice, but not enough time and resources to dedicate to it.

Solution

Kognos Autonomous XDR Hunter was deployed on-premise to autonomously hunt for emerging threats as well as to investigate thousands of alerts per week.

Customer

Financial Services Company

Background

The attacks in 2020 triggered an internal review which concluded that the team needed to step up their coverage and switch to a more proactive approach to protecting their environment. The team realized that in order to do it, they needed to augment their existing tools and processes with automation - as the team was already overwhelmed with a plethora of alerts generated from various tools.

Challenge

The challenges the organization faced included a relatively small security team of 7 supporting an organization of over 3500 employees. The team wanted to add a proactive threat hunting practice but was unable to do it given their time and resource constraints. Furthermore, they had 3000+ alerts generated from Carbon Black and Splunk every week - out of which they were only able to investigate around 10%.

The team needed help with increasing the investigative coverage of generated alerts across different data sources. They liked the deep Carbon Black telemetry, but felt they were not able to mine through the data effectively to thwart some of the emerging and more sophisticated attacks.

KOGNOS
never hunt alone

Case Study: Carbon Black Deployment Financial Services Company

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

Results

- 50K+ hunts per month protecting the environment from emerging threats
- 15K+ alerts per month autonomously investigated
- 3 to 5 *fully pre-investigated* stories, per day, identified by Kognos, with complete context that can be remediated in minutes

" Kognos offloaded 80%+ of the cumbersome data mining activity - freeing up an enormous amount of time – and enabling our team to identify and remediate the highest severity threats in real-time. "

- SOC Director

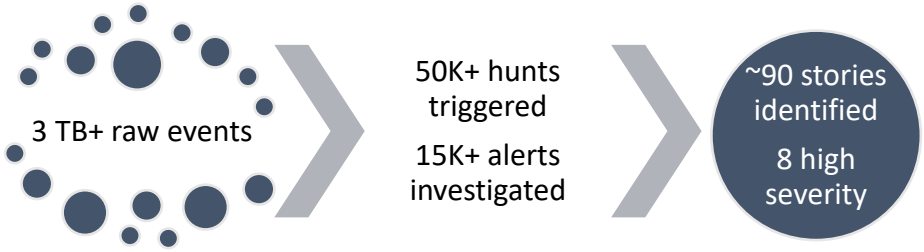
Solution

The Kognos autonomous XDR hunter was seamlessly deployed, connecting to the Carbon Black cloud via AWS S3 buckets, to stream raw events to Kognos and API-based access to Splunk for on-demand questioning of Splunk data. A total of 34 hourly and daily recurring hunts were setup for Lateral Movement tools, Living off the Land binaries, persistence mechanisms, rare processes, etc.

Both Carbon Black and Splunk alerts are now forwarded to Kognos for deeper investigation. As a result, 100% of the alerts are being investigated and 24/7/365 hunts are running to protect their environment. The team now periodically conducts review sessions of stories generated by Kognos to ensure there are no adversary activities within the environment - freeing up enormous amount of time that they would otherwise have to spend mining through Carbon Black and Splunk data.

Results

The Kognos attack-tracing, AI-powered threat hunting platform was able to provide visibility into all suspicious user sessions, with complete context explained as visual storylines. Given below are some of the statistics observed over a period of one month for 6000+ devices being continuously monitored:



Kognos automation helped the team reduce their workload by several man months for the same period, allowing the team to focus on other aspects of their security program. Furthermore, the team now feels confident that their new grid of autonomous hunts is effectively hunting down emerging attacks from multiple different perspectives.

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