Cognyte

CASE STUDY

Accelerating Government SOC Operations with Luminar

ADVANCED SOC CHALLENGES

- Ensuring IT, OT and physical security systems are secure
- Facing advanced adversaries with different motives
- Lack of visibility into external and targeted threats

SOLUTION HIGHLIGHTS

- Analytics-driven, targeted cyber threat intelligence
- Extensive data coverage
  - Clear, Deep & Dark web monitoring
  - Domain name intelligence
  - Vulnerabilities and exploits
  - Technical intelligence
- Targeted monitoring plan
- Access to finished and historical intelligence

BENEFITS TO THE ORGANIZATION

- CTI insights about adversaries' capabilities, intentions, motives etc.
- Industry and region focused threat intelligence and reports
- Fine-tune threat hunting activities to identify unknown threats
- Timely detection of insider threats

A government authority responsible for the operation and management of airports, land terminals and country border controls, is also in charge of the cybersecurity resilience of its systems, which are spread across multiple locations and over a wide array of networks.

This government sector is considered a high-end target for threat actors, and different attack groups are using the Dark Web to buy access to compromised IT infrastructure of government and other high-profile targets.

OPERATING AN ADVANCED SOC

Servicing a number of airports throughout the country, as well as land terminals and border controls, this government authority is responsible for the safety and security of millions of people daily. The authority operates a Security Operations Center (SOC) that monitors its systems to detect threats in a timely manner. With a constant shortage of resources and staff, the SOC analysts are struggling to be more proactive and efficient, and to be able to prioritize their efforts, according to actual potential threats.

In addition, the SOC is responsible for protecting advanced systems of IT networks, OT infrastructure and physical security, and is required to attend to more types of threats and more advanced adversaries.

The authority was looking for a cyber threat intelligence (CTI) solution that will provide visibility and insights, and that will enable them to identify targeted threats to the organization's assets and infrastructure, such as stolen records, system vulnerabilities, cyber threats against executives and suppliers, etc. In other words, a solution that will monitor Deep and Dark Web platforms to identify relevant data leaks shared or traded by cybercriminals, exploits against products and systems, indications for potential future threats, and more.

VISIBILITY BEYOND THE ORGANIZATION

The authority chose to implement Cognyte's CTI solution, Luminar, because of its data coverage and Dark Web monitoring capabilities, threat intelligence research capabilities and proven methodologies for providing targeted threat intelligence. In addition, Cognyte brings over 25 years of operations in the cybersecurity and intelligence domains, and proven expertise in providing solutions to government entities.

Luminar is an analytics-driven cyber threat intelligence platform. As such, it helps extend visibility beyond the organization's infrastructure and provides targeted cyber threat intelligence. With Luminar, SOC teams and intelligence analysts get targeted threat data and access to premium intelligence outputs, built-in CTI methodologies, and proprietary repositories.

Luminar was deployed in the organization, and based on a "live" monitoring plan the system began to automatically gather and ingest relevant data from threat intelligence sources, according to the organization's critical assets, industry and predefined threat hunting requirements.

By monitoring and analyzing Clear, Deep & Dark Web sites, as well as closed hacking forums, social networks, instant messaging platforms and technical intelligence sources, Luminar uncovers malicious activities at their earliest stages, providing insights and leads for further investigation.

END-TO-END CYBER THREAT INTELLIGENCE

The authority's SOC is now continuously receiving **strategic threat intelligence** about adversaries' capabilities and intentions of attack groups that are relevant to their industry and region, including nation-state actors, criminals, terrorists and hacktivists.

In addition, **operational threat intelligence** brings great value with insights that enable to fine-tune threat hunting activities to identify unknown threats, better prioritize vulnerability management, and provide context enrichment and technical data to accelerate incident response.

Lastly, ongoing **tactical intelligence** with unique IOC data based on Deep and Dark Web data analysis, enables the SOC team to input that data into relevant cybersecurity systems and improve resilience and timely detection of threats.

> *"As a government authority, we face advanced adversaries and targeted attacks that are challenging to reveal at early stages.*
>
> *Luminar uncovers threats that target our industry and region, from outside of the organization, enabling us to optimize our threat hunting resources and improve our overall cyber resilience"*
>
> **Government authority CIO**

TARGETED INSIGHTS FOR ENHANCED RESILIENCE

Luminar helped the organization detect exposed records shared on the Dark Web, which indicated that employee used organizational email addresses on external third-party services. These findings led the organization to launch password-replacement procedures to mitigate potential spear-phishing attempts, and employees' cyber awareness initiatives.

In addition, as part of its ongoing activities, Luminar monitors black marketplaces, also known as bot markets, dedicated to selling digital assets, that contain information about the compromised system, including logins, passwords and cookies collected from websites visited by the victim. While using Luminar, several sales offers that include the organization's domains were discovered, which led the SOC team to carry out an investigation regarding a potential breach within the organization's internal network.

Building a high-end SOC with advanced solutions and targeted threat intelligence, this government authority is now positioned as an industry leader, with a SOC that maintains the cyber resilience of their entire operations, covering cybersecurity needs of their IT, OT and physical security systems.

Cognyte

About Cognyte Software Ltd.

Cognyte is the global leader in investigative analytics software that empowers governments and enterprises with Actionable Intelligence for a Safer World™.