Cognyte CASE STUDY

How a Critical National Infrastructure Uses Luminar to Proactively Reveal and Mitigate Threats in the Making

CHALLENGES

- Lack of visibility into industry related threats
- Protecting vulnerably high-risk personnel
- Complexity of monitoring different types of assets
- Ongoing phishing attempts against customers

SOLUTION

- Real-time monitoring of multiple sources
- Addressing all required use-cases in a single solution
- Threat actor profiling and industry intelligence
- Human analyst support

OUTCOME

- Discovery of suspicious domains and potential phishing attempts
- Identifying leaked records and fraudulent activities
- Exposure of third-party risks and insider threats

A National European Critical National Infrastructure (CNI) organization is responsible for the management, production and distribution of 95% of the country's energy, and employs 40,000 people in its 800 plants.

This CNI organization was looking to implement a Cyber Threat Intelligence (CTI) solution in order to expand its visibility into threats and become more proactive in its defense strategy. The organization issued a bid based on several cybersecurity issues they wanted to address.

Industry intelligence. Visibility into industry-related attacks and threat intelligence about attack groups and attack vectors that are used to target the specific industry, enables to learn and better understand how to remain secure and resilient. The organization did not have access to such information and requested a solution that can provide updates on attacks targeting similar entities.

Phishing. The organization had received complaints from customers about phishing attempts, impersonations, and fraud activities. This was not acceptable and management requested a solution that provides early warnings that will enable them to proactively address this and avoid such incidents either using take-down services or even warning customers in time, to be aware of such possible attempts.

Executive protection. High-risk and sensitive personnel are always a target in such organizations, as they can have access privileges or information that can facilitate attacks. The organization decided to continuously monitor high-risk senior management to check their exposure level and help reduce their personal attack surface.

Monitoring a variety of assets. The organization was looking for a wide solution that will provide threat intelligence for all their assets including IT and OT, as well as assets related to their subsidiaries, parent company and third-party suppliers. They were looking for the ability to monitor these assets over multiple sources, such as the Deep and Dark Web, social networks and technical forums, to identify risk to the brand, detect data leaks, and uncover exposed and vulnerable assets.

This CNI organization selected Cognyte's Luminar for its ability to monitor and collect data from a wide array of sources regarding different types of assets, to provide visibility into industry-related attacks and technical analysis of attacks on critical infrastructure organizations globally, and to automatically deliver digital footprint risk assessments. In addition, they found great value in having access to analysts that provide ongoing professional services and support in multiple languages.

CONTINUOUS COMPREHENSIVE MONITORING AT SCALE

Luminar was deployed within a few days, with no interference to operations. Following the CNI's team onboarding and training, the system became operational. Luminar has the capacity to continuously monitor the CNI's ~2,000 IT and OT assets and to scale with the company.

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.

Luminar began gathering and ingesting relevant data from threat intelligence sources, based on the CNI's critical assets, industry, region, and predefined threat hunting requirements. The automated monitoring enabled the identification of leaked records and mentions in the Deep and Dark Web in real-time. The monitoring plan is dynamic and the assets can be changed and updated in real-time and still ensure the monitoring is accurate. In addition, reconnaissance activities are performed to reveal exposures of the high-risk personnel and recommend how to minimize the personal attack surface.

Luminar is also used to monitor new domain registrations that impersonate the organization in order to provide early warnings and suggest take-down procedures, and to monitor social media networks to alert in real-time when customers mention such potentially fraud-related activity.

PROACTIVE DISCOVERY AND MITIGATION OF THREATS

Since its implementation, Luminar has delivered threat intelligence findings regarding all the issues that drove the organization to deploy a CTI solution to begin with, enabling the organization to proactively mitigate threats in the making. Among the threats identified by Luminar were:

- Suspicious domains and potential phishing attempts
- Ransomware attacks that have hit suppliers
- Leaked records
- Hacktivists attacks against the nation resulted in attacks against the CNI
- Fraud activities on energy consumption meters
- Customers defaming the company over social media
- Exposed and vulnerable servers
- Employees that suffered a bot attack and had their credentials traded on the Dark Web

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™.