Cognyte CASE STUDY

How a Large European Telecom Uses Luminar to Protect a Nation from Cyber-Attacks

CHALLENGES

- Ongoing targeted attacks
- Lack of visibility into Deep and Dark Web
- Risk of data leak

SOLUTION

- Continuous monitoring and analysis of Deep & Dark Web sites and forums
- Constant stream of intelligence about threat actors' capabilities and intents
- Access to unique historical intelligence
- Near real-time targeted intelligence about indications of leaked records and potential data breaches
- Strategic intelligence enrichment reports

OUTCOME

- Discovery of the telecom's leaked records and exposed servers
- Reveal of planned targeted attacks on the telecom
- Identification of attack groups directly targeting the telecom and the nation
- Strengthening the telecom's position as a national and commercial cybersecurity leader

A large European national telecom company, with over 21,000 employees and subsidiaries across the continent, is a prime target for cyber-attacks, as it serves national assets. The telecom maintains an advanced SOC, and as it considers cybersecurity strategic to its operations, aims to always improve its security resilience.

In January 2019 a cyber-attack targeting high-profile national organizations took place with the possibility of nation-state actors or their proxy groups, being behind the attacks. Although the attacks were not directed at the telecom, the government's security agencies, including ministerial involvement, reached out to the telecom's SOC, and used the SOC's advanced technologies and resources for defense operations.

INCREASE IN TARGETED CYBER-ATTACKS

Since 2019, the telecom has seen a rise in attacks on the country and on their organization specifically. The risk of being a target to nation-state attackers isn't new to any national telecom that is part of a country's critical infrastructure. They are used to being a prime target of various attack groups, including cybercriminals, nation state and hacktivists/terrorist groups.

While assessing their overall cyber defense capabilities, the telecom concluded that in order to improve their resilience they need to expand their monitoring capabilities to cover existing blind spots. For example, the telecom lacked the ability to monitor threat actors' activities outside the organization, including in the Deep and Dark Web.

The telecom began evaluating Luminar, Cognyte's Cyber Threat Intelligence (CTI) solution, at the end of 2019 and the solution was deployed at the beginning of 2020. What made the telecom choose Luminar was the combination of superior intelligence, both from a technological and human analyst perspective, built-in methodologies, ongoing support and high-end reports. In addition, Luminar can be leveraged by the telecom to be a new revenue stream, should they offer CTI services to their customers in a Managed Service Provider (MSP) model.

CONTINUOUS MONITORING OF CLEAR, DEEP & DARK WEB FOR AN INTELLIGENCE BOOST

Luminar was deployed within a few days, with no interference to operations. Following the telecom's team onboarding and training, the system became operational.

Luminar automatically gathers and ingests relevant data from threat intelligence sources, based on the telecom's critical assets, industry, region, 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 uncovered malicious activities at their earliest stages.

THE TELECOM USES LUMINAR TO SUPPORT VARIOUS USE-CASES INCLUDING:

THREAT ACTOR PROFILING

Access to threat intelligence insights about threat actors' nature and motives, in order to better understand and mitigate the threat

DEEP AND DARK WEB MONITORING

Providing near real-time targeted data about threat actors' activities and indications of leaked records and potential breaches

STRATEGIC INTELLIGENCE ENRICHMENT

Supporting specific investigations, such as analysis of state-sponsored threat actors, regional/industry specific risks and global ransomware activities

TIMELY DISCOVERY AND MITIGATION OF THREATS

Luminar became operational and proved valuable quite quickly. Following the deployment, the telecom's SOC analysts were able to uncover leaked records, discover exposed and vulnerable servers, and identify planned targeted attacks on both the telecom and the nation.

In addition, the telecom identified several attack groups that were directly targeting them and was able to reveal and mitigate attacks in a timely manner.

Cognyte

About Cognyte Software Ltd.

Cognyte is a global leader in investigative analytics software that empowers governments and enterprises with Actionable Intelligence for a Safer World™. Our open analytics software is designed to help governments and enterprises accelerate and improve the effectiveness of investigations by fusing, analyzing, and visualizing disparate data sets at scale to help organizations find the needles in the haystacks. Over 1,000 government and enterprise customers in more than 100 countries rely on Cognyte's solutions to accelerate and conduct investigations and derive insights, with which they identify, neutralize, and tackle threats to national security, personal safety, business continuity, and cyber security.