CASE STUDY

ELITE SECURITY INTELLIGENCE DRIVES STOCKHOLM PUBLIC TRANSPORTATION'S NEED FOR SPEED

OVERVIEW

Stockholm Public Transportation, or Storstockholms Lokaltrafik (in their local Swedish), is the organization responsible for running all land- and sea-based public transport systems in Stockholm — capital of Sweden, home to more than 2.4 million people, and the cultural, political, and economic center of Sweden.

Challenge

As transportation systems become increasingly connected and operators shift to digitalized operational technology (OT) to improve efficiencies, cyber threats are rising in parallel. While threat actors' motivations vary, experts agree that attacks on these critical infrastructure systems are particularly concerning because, in addition to data loss, breaches may result in large-scale disruption or even physical damage.

Serving more than 900,000 people each day, Stockholm Public Transportation works to ensure efficient travel across the densely populated county, while advancing public transportation safety. Citizens rely heavily on its interconnected transportation network of metros, buses, trains, local railways, and shuttle boats, and even minor disruptions can have major impacts on daily life.

The organization's IT security team has the massive responsibility of protecting the organization from evolving cyber threats. Yet, until recently, they lacked visibility into the specific vulnerabilities putting their business at greatest risk of attack.

"All of our IT infrastructure is outsourced, and we were experiencing a lag between the time vulnerabilities were discovered and when we got insights from the solution provider to help us address issues," recalls IT manager Niklas Perdhe. "We had a serious need for speed."

Solution

After learning about Recorded Future at an industry seminar, the team decided to put elite security intelligence to the test. Their primary goal was to continuously monitor the organization's tech stack for vulnerabilities to eliminate the dangerous detection gap and accelerate response times.

To power the world's most advanced commercial collection platform, Recorded Future combines a patented algorithm process with world-class human analysis — fusing an unrivaled range of open source, dark web, technical sources, and original research to deliver context around newly disclosed vulnerabilities in organizations' existing technologies.

Instead of waiting for new threats to be catalogued in the NIST National Vulnerability Database (NVD), Recorded Future's security intelligence platform automatically detects reporting of new observables — from vulnerabilities and exploits, to threat actors targeting the organization and the transportation industry at large. It immediately delivers alerts on new and relevant exploits in real time to Stockholm Public Transportation — approximately 11 days before they are published by the NVD.

> With Recorded Future's risk scores and simple severity level system, we easily understand what matters most, and where to focus our efforts."
>
> *-Håkan Ruthberg, IT security coordinator, Stockholm Public Transportation*

With access to real-time risk scores for any IP address, domain, hash, and CVE appearing on the internet, the team instantly understands which vulnerabilities need to be addressed, and which ones are less relevant.

"When it comes to patching, prioritization is the name of the game," says IT security coordinator, Håkan Ruthberg. "With Recorded Future's risk scores and simple severity level system, we easily understand what matters most, and where to focus our efforts."

Results

"The ability to actively monitor our environment and exposure, pinpoint vulnerabilities that present real risk, and make informed decisions quickly has been invaluable to our organization," says Niklas.

The IT security team isn't the only group that has benefited from this unprecedented intelligence. "By minimizing off-cycle patches, we've significantly lowered disruption to production," explains Håkan. "Additionally, we use insights and on-demand reports from Recorded Future to communicate cyber risk in a clear, effective way to our board."

Impressed by the success of their initial use case, the team plans to extend security intelligence to reduce risk in third-party risk workflows, as well.

"We work with a large and ever-expanding ecosystem of contractors," says Niklas. "By applying security intelligence to this area, we'll gain deeper insights into our partners' security postures to reduce overall risk, and also streamline due diligence work as we onboard new providers."