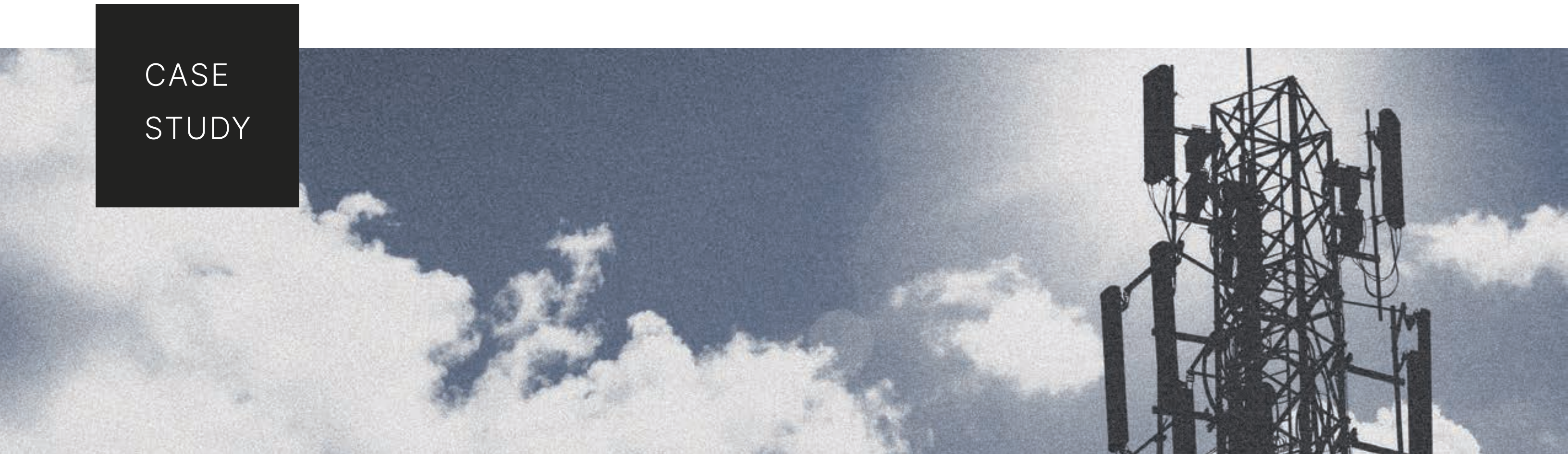
CASE STUDY



Recorded Future Intelligence Enables Nkom EkomCERT to Help Norwegian Telecoms Stay Ahead of Industry-Specific Threats

Government agency uses intelligence to prioritize vulnerabilities and track the evolving threat landscape for communications firms

USE CASES

- Enriching and prioritizing vulnerability data
- Providing situational awareness of impending attacks
- Mapping the threat landscape for long-term planning

CHALLENGE

A small security team needed access to a wide range of intelligence from the open and dark webs, filtered for a specific industry (telecom) and a specific region (Scandinavia).

SOLUTION

- Vulnerability Intelligence
- Splunk Enterprise Integration
- Threat Intelligence
- Brand Intelligence
- Research and Analyst on Demand services from the Recorded Future Insikt Group

OUTCOMES

- Vulnerabilities triaged and prioritized based on actual risk to Norwegian telecom companies
- Early warning of phishing, ransomware, DDoS, and other attacks
- Norwegian telecom companies and government agencies able to make better decisions about strengthening security programs over time

NKOM Nasjonal kommunikasjons- myndighet

Protecting Norway’s Telecom Industry

The Norwegian Communications Authority (Nasjonal kommunikasjonsmyndighet, or Nkom) is a government agency that supervises and supports organizations that provide electronic communications services in Norway, primarily telecommunications companies. One of its major responsibilities is ensuring the security and resilience of electronic communication networks.

Ole Kristoffer Apeland is Chief Security Engineer and Team Lead at Nkom EkomCERT. The team he leads works with Norwegian telecom and digital communication companies to help them prevent cyberattacks and to prepare for emerging threats.

Ole’s team was tasked with identifying malicious actors targeting telecom and ecommerce companies in Norway and determining the vulnerabilities they typically exploit to steal data, commit fraud, and disrupt networks. The team needed to go beyond general trends and generic vulnerability scores to pinpoint telecom industry-specific attacks active in Scandinavia or likely to be active there soon. Only with this information would Nkom EkomCERT’s telecom client firms be able to prioritize and mitigate the specific vulnerabilities representing real threats to their business.

The small group faced a similar challenge providing visibility into the evolving threat landscape for Norwegian telecom companies. They needed to monitor developments related to phishing, ransomware, distributed denial of service (DDoS) attacks, advanced persistent threats (APTs), consumer fraud, and other threats and provide insights to help Norwegian telecom and digital communication companies plan their investment in staff and security technologies.

Ole and his team realized they didn't have the resources to obtain the deep, real-time, sector-specific intelligence they needed to accomplish their mission. After evaluating intelligence offerings from several firms, they selected Recorded Future as the company that could provide the best intelligence and support.

> “Intelligence from Recorded Future enables us to separate vulnerabilities that pose immediate dangers to Norwegian telecom organizations from those that represent merely theoretical or long-term risks.”
>
> *Ole Kristoffer Apeland*
> *Chief Security Engineer and Team Lead, Nkom EkomCERT*

Enriching Vulnerability Data for Risk-Based Patching

Nkom EkomCERT receives a steady stream of newly discovered vulnerabilities from a variety of technology vendors and industry sources such as the CVE database. Before using Recorded Future's intelligence, the challenge was determining which vulnerabilities represented immediate threats to Norwegian telecom and digital communication companies, and the best approach to mitigating the attacks that exploit those vulnerabilities.

Ole's team uses Recorded Future Vulnerability Intelligence and Recorded Future's integration with Splunk Enterprise to enrich their vulnerability data in Splunk so they can get a clear picture of each vulnerability's risk to their organization, based on likelihood of exploitation. In a single pane of glass, the enrichment provided by the Recorded Future and Splunk Enterprise integration helps Nkom EkomCERT prioritize addressing the vulnerabilities that matter most.

“Recorded Future's Splunk Integration allows us to effectively prioritize and act with urgency on the right vulnerabilities. It helps us identify where our time is best spent, since there's often more work than there are people. The vulnerability enrichment that Recorded Future's Splunk Integration provides allows us to feel confident that we're spending our effort where it counts,” says Ole.

In the past, Ole's team leaned on other information sources for enrichment of their vulnerabilities, but did not find that the other vendors provided the level of enrichment they needed. Ole recounts, "We've used other vendors before to provide added vulnerability context, but their data and service did not meet our quality standards. We've been using Recorded Future Vulnerability Intelligence and the Splunk Integration for many years now, and it is quite central to our current operation."

In addition to relying on the enrichment that Recorded Future provides that can be accessed directly within their Splunk instance, they also depend on Vulnerability Intelligence within the Recorded Future Intelligence Platform to evaluate true risk. With intelligence, Ole and his team are able to see the context of each vulnerability with examples of the vulnerability previously being exploited, associations with attack types and threat actors, and a risk score. For Ole's team, a primary focus is identifying vulnerabilities for commonly used products within telecom companies and notifying their constituents. Once a potentially important vulnerability is identified, the team uses information from Recorded Future to assess it based on temporal metrics, especially its stage in the vulnerability lifecycle.

Using the Vulnerability Lifecycle

Vulnerabilities go through a lifecycle. They evolve over time from discovery and announcement (when exploits are theoretical), to the development of proof-of-concept code (which demonstrate that exploitation is possible but can't readily be used for attacks), to functional exploit code (which can be used by skilled attackers), to exploit kits being available on the dark web (which make exploitation easy for less skilled attackers), to active "in-the-wild" exploitation.

Vulnerabilities in the later stages of this timeline are ripe for exploitation and need to be remediated immediately. Those in the early stages represent future risks, but should only be addressed after high-priority vulnerabilities.

Intelligence from Recorded Future allows Nkom EkomCERT to assess vulnerabilities based on their stage of evolution. Nkom EkomCERT shares these assessments with Norwegian telecom companies and government agencies, so they can triage vulnerabilities and prioritize those that are most likely to be exploited in the near future.

Providing Situational Awareness of Impending Attacks

Telecom companies are exposed to a wide variety of cyberthreats: DDoS attacks on their networks, APTs, phishing, ransomware attacks on their business, and fraud campaigns against their customers. One of Nkom EkomCERT's responsibilities is providing Norwegian telecoms with early warnings about activities in these areas so they can prepare for the next wave of threats.

Ole's team relies on Recorded Future to uncover indicators of impending and ongoing attacks. To provide early warning, Recorded Future:

- Searches hundreds of dark web forums for "chatter" about threats to telecom organizations and to Scandinavian companies, including phishing campaigns and ransomware attacks
- Monitors dark web marketplaces for code and exploit kits that could be used in APTs targeting customer-facing applications and DDoS attacks on networks
- Scans code repositories and dark web marketplaces for stolen credentials associated with internet domains used by Norwegian telecom companies and their subsidiaries, to provide warning of account takeover and credential stuffing attacks

Because telecom firms now provide a wide variety of services, Recorded Future's data for Nkom EkomCERT covers a wide range of industry segments and technologies, including mobile phone and landline services, messaging and collaboration applications, internet services, and streaming media and entertainment.

Mapping the Threat Landscape for Long-Term Planning

Nkom EkomCERT plays a key role mapping the threat landscape for Norwegian telecom companies and other government agencies. To fill this role, Ole's team uses intelligence from Recorded Future to monitor the evolving activities of malicious actors and provide real-time visibility into trends related to phishing, ransomware, distributed denial of service (DDoS) attacks, APTs, consumer fraud, and other threats relevant to the telecom sector. The breadth and depth of Recorded Future's coverage of open and dark web sources, together with context and analysis of attacks, enables Nkom EkomCERT and Norwegian telecom and digital communication companies to anticipate and plan for the threats most likely to affect their operations.

Ole's team also makes extensive use of analysis and insights from the Recorded Future Insikt Group, a team of veteran threat researchers that provides Analyst on Demand services and targeted threat research to Recorded Future customers.

Nkom EkomCERT's cybersecurity expertise, bolstered by Recorded Future's information and insights, has helped Norwegian telecom companies and government agencies make intelligent decisions about allocating resources and strengthening their security programs over time.

How Recorded Future Supports Nkom EkomCERT's Success

Ole and his team feel that intelligence from Recorded Future has greatly strengthened their ability to provide guidance to Norway's telecom sector. They are especially pleased with Recorded Future's ability to:

- Enrich basic vulnerability data with context and temporal metrics
- Systematically monitor hundreds of open and dark web sites for indicators of impending attacks
- Produce information specific to telecom companies and specific to Scandinavia
- Continuously update intelligence to maintain situational awareness
- Provide data about critical cybersecurity trends and insight into how they apply to Nkom EkomCERT and its constituents.
- Provide prompt support and expert help

> “Recorded Future has been very helpful, and the support that we've gotten has helped us immensely. We're a small team. Insikt Group's analysis and the capabilities they bring have allowed us to offload analysis. We've been able to ask as many questions as we want. Insikt Group has greatly expanded the productivity and impact of our team.”
>
> *Ole Kristoffer Apeland*
> *Chief Security Engineer and Team Lead, Nkom EkomCERT*

ABOUT RECORDED FUTURE

Recorded Future is the world's largest intelligence company. The Recorded Future Intelligence Platform provides the most complete coverage across adversaries, infrastructure, and targets. By combining persistent and pervasive automated data collection and analytics with human analysis, Recorded Future provides real-time visibility into the vast digital landscape and empowers clients to take proactive action to disrupt adversaries and keep their people, systems, and infrastructure safe. Headquartered in Boston with offices and employees around the world, Recorded Future works with more than 1,300 businesses and government organizations across 60 countries. Learn more at recordedfuture.com.

www.recordedfuture.com @RecordedFuture