splunk> turn data into doing™

CASE STUDY

Denmark's Largest Utility and Telecommunications Company Accelerates Incident Response to Save 35 Hours Every Week

Key Challenges

After building their own log analytics and incident response capabilities, the Norlys team faced a range of challenges, from repetitive tasks and too many tools to slow webUIs and cumbersome processes.

Key Results

With the Splunk platform, Norlys has integrated threat intelligence, automated repetitive tasks and centralized investigations for faster response times and more productive employees.

NORLYS

Industry: Utility and Telecommunications

Solutions: Security

Delivering critical services means security must be a priority.

As Denmark's largest power, utility and telecommunications company servicing 1.5 million customers, Norlys understands the need for fast response to security alerts. Since they didn't have incident response or security capabilities when the security department was formed, the Norlys team built their own log analytics and incident response capabilities from the ground up.

This homegrown approach presented challenges, from manual workflows, repetitive tasks and too many tools to a lack of context, slow webUIs and difficult-to-maintain processes. To solve these problems, Norlys turned to Splunk, choosing Splunk® Enterprise Security (ES) as its SIEM tool and Splunk® SOAR as its security orchestration, automation and response (SOAR) platform.

Finding the Bad Guys

Norlys now combats threats with actionable intelligence, using Splunk ES for everything from threat hunting and feed ingestion to investigation dashboards and correlation searches. "If we have suspicious activity on an endpoint, we go to that specific dashboard in ES and can see all of the movements," says Tibor Földesi, security automation analyst at Norlys. "I just enter the hostname for a single machine, and I can see all of the endpoint response logs. ES lets you see everything going on in your environment to find the bad guys."

Data Driven Outcomes

35 hrs
of work saved per week

30 sec
to complete processes that once took 30 minutes

98%
less time to open tickets

To maximize its investment, Norlys receives support from Splunk Professional Services. "If we are unable to do something the best way we think possible, we reach out to the Splunk Professional Services team. Professional Services are really key to success," says Földesi. "With Professional Services, we learned that we could get immediate value out of ES and Splunk SOAR by automating opening tickets between systems. I don't want to open tickets every day, and now I don't have to."

Saving 35 Hours Every Week

Thanks to the automation and orchestration of Splunk SOAR, Norlys now solves security problems faster.

With Splunk SOAR, Földesi first created a specific playbook for responding to an antivirus alert. Upon receipt of the alert, the Splunk SOAR playbook automatically triggers an endpoint detection and response (EDR) tool to analyze the endpoint for suspicious activity, retrieve the quarantined file, submit it to a malware sandbox for detonation and analysis, and then generate a report for the security analyst. Before this playbook was created, Norlys encountered these alerts many times a day, each of which demanded the team's time and attention.

> Automation is changing how teams traditionally use a SIEM. We heavily rely on Splunk SOAR and Enterprise Security. They complement each other in a very good way and allow us to improve security capabilities for the entire company."
>
> **Tibor Földesi,** Security Automation Analyst, Norlys

> Tickets that used to take 10 minutes to create manually are now created in an instant. And some tickets are automatically initiating enrichment actions that take only 30 seconds versus 30 minutes if done manually."
>
> **Tibor Földesi,** Security Automation Analyst, Norlys

"This is a very advanced playbook," says Földesi. "A hundred percent of the investigation is automatic, and no human interaction is needed. I used to do this part manually before, but with Splunk SOAR, I only have to step in at the end of the analysis and make an educated decision about what actions to take."

The Norlys security team operates on a specific promise: if something is annoying, automate it. As a result, the team uses 20 different playbooks every day to save time and money. "Splunk SOAR saves us 35 hours per week — about five hours per day. We can now finally focus on the important tasks." says Földesi.

Quality Workflows, Quality Security

With Splunk implemented in day-to-day workflows, Norlys security analysts have been able to better protect their organization. "Automation is changing how teams traditionally use a SIEM," says Földesi. "We heavily rely on Splunk SOAR and Enterprise Security. They complement each other in a very good way and allow us to improve security capabilities for the entire company."

21-15232-Splunk-Norlys-CS-103