Netox Oy

As a leading MDR provider combining cybersecurity and IT services, Netox Oy needed a way to instantly address emerging threats to minimize risk exposure, keep detection coverage relevant, and maintain uninterrupted protection. By using the SOC Prime Platform, Netox reduced detection engineering efforts by 70% while improving detection quality and achieving a 35% decrease in false positives. This efficiency freed up resources to focus on broader SOC priorities and scale security services to meet diverse customer needs.

Industry	Region	Company Size	SIEM & XDR in Use
MSSP/MDR	Northern Europe	200+ employees	Microsoft Sentinel, Microsoft Defender for Endpoint

SOC Tech Lead

“SOC Prime helps us to scale without making compromises on the quality of our detections. Custom feature requests are implemented quickly, with clear updates along the way. The development process is fast, transparent, and keeps us fully informed.”

Highlights

~360 Hours
Of Analyst Time Saved per Quarter on SOC Operations

70% Less
Time Spent on Content Development & Tuning

3X Faster
Deployment of New Detections for Emerging Threats

35% Reduction
In False Positives for Improved Alert Accuracy

- Rapid integration of new log sources for easier and more efficient monitoring across massive volumes of data
- Simplified multi-platform rule translation via Uncoder AI
- Efficient automation of content deployments to complex client environments
- Scaling a SOC service portfolio backed by AI and human expertise

Challenges

Continuously Growing Attack Surface
Netox provides follow-the-sun IT and security services, including Managed Detection and Response, SOC automation, and threat hunting. Creating high-quality detection content is time-consuming, and keeping it up to date requires careful prioritization to maintain security operations efficiency.

Detection Engineering Hurdles in Complex Environments
With clients’ infrastructure spanning multiple cloud platforms and hybrid networks, deploying and integrating detection content is a challenge. Manual deployments are time-consuming and prone to errors, limiting the team’s ability to expand monitoring and respond promptly to emerging threats.

Need for Multi-Platform Content Support & Consistency
Making detection rules effective across different SIEMs and EDRs while covering multiple log sources means constant updates and fine-tuning. Without automation and AI, this work becomes slow and resource-heavy, putting pressure on the SOC team and delaying threat response.

Alert Overload Reducing Operational Effectiveness
Operating around the clock, the in-house engineering team receives a large number of security alerts daily, making it hard to spot real threats. Accurate and timely detection content is essential to cut false positives and let analysts focus on the most critical incidents.

Solution

Netox Oy delivers a highly cyber-resilient, 24/7 managed business infrastructure to monitor, protect, and support its customers without interruption. Focused on scaling its SOC services portfolio and maintaining strong cyber defense, Netox partners with SOC Prime to ensure clients' operations run smoothly and securely. Netox leverages SOC Prime's Threat Detection Marketplace to access ready-to-use detection use cases and threat context for dozens of SIEM and EDR solutions while saving up to 360 hours per quarter on SOC operations. The AI-powered Active Threats feed enables Netox to proactively track and prioritize critical threats, while Uncoder AI helps to create, translate, and customize detection rules—reducing detection engineering efforts by 70%. With SOC Prime's automation and AI capabilities, Netox gets a 3X faster deployment of new detections for emerging threats, expands log source coverage, and eliminates alert fatigue, resulting in faster time-to-protection, broader visibility, and scalable, high-quality SOC services for its growing client base.

Achievements

70% Faster Detection Engineering

Using the continuously updated Threat Detection Marketplace library, Netox can quickly address emerging threats and keep strong 24/7 defenses for its clients. SOC Prime's AI-powered Active Threats feed helps the engineering team track the latest attacks, investigate proactively, and respond faster. This allows Netox to focus on the most critical risks for customers while dedicating more time to other high-value operations.

Delivering Scalable, High-Margin SOC Services In-House

With SOC Prime's product suite, Netox has scaled its security offerings and improved detection and response metrics while keeping content high-quality and up to date. Curated detection content relevant to the customers' threat profiles, combined with automation, AI, and human expertise, enables Netox to support a growing client base with the team it has on board.

Automated Detection Content Deployment

Netox offers a wide range of cybersecurity and IT services, with AI and automation embedded at the core. With deep expertise in Microsoft technologies and other platforms, Netox secures cloud, on-prem, and network environments while ensuring uninterrupted coverage and zero downtime. By partnering with SOC Prime, Netox seamlessly integrates with Azure DevOps and Microsoft Sentinel to automate error-free content deployment, speeding up both time-to-protection and time-to-value.

Scaling Threat Visibility While Reducing Noise

With SOC Prime, Netox integrates new log sources faster and with less effort, expanding monitoring scope and improving detection coverage across complex cloud, endpoint, and network environments. This leads to a 35% reduction in the false positive rate, improving alert accuracy and enabling the SOC team to focus on critical threats, driven by SOC Prime's high-quality detection content.

Automated Cross-Platform Rule Translation & Easier Fine-Tuning

Leveraging Uncoder AI, Netox applies SOC Prime's vast Sigma rule library across multiple SIEM and EDR platforms, ensuring consistent, verified, and accurate threat detection. The traditionally resource-intensive process, especially for complex detection algorithms, is streamlined through SOC Prime's AI capabilities, enabling the team to respond faster to customer requests, deliver clear updates, and customize rules more efficiently.

AI-Enhanced SOC Operations

Netox is investing heavily in AI to scale its human-driven SOC services backed by automation. By using SOC Prime's AI-powered technologies and expertise, Netox integrates advanced automation capabilities and intelligent detection into its workflows, improving efficiency and delivering more value to customers.

About Netox Oy

Netox Oy is a Finnish cybersecurity and IT services company operating as a 24/7 powerhouse—not just a SOC, but a fully integrated force that keeps businesses secure, productive, and resilient around the clock. Combining cutting-edge Microsoft technology with human expertise, Netox delivers comprehensive solutions across cybersecurity, modern work, and managed IT services. The company's "Always On, Always Secure" model unites detection, protection, and productivity into one seamless ecosystem. With certified excellence (ISO 27001 & ISO 20000) and a relentless focus on continuity and trust, Netox helps organizations operate securely, efficiently, and confidently in a digital world.