



## CASE STUDY

# Redefining Security with an Automated Threat Intelligence Analyst for MSSPs

## About **scunna**

Scunna is a Managed Security Service Provider (MSSP) specialized in providing services and automating the processes of detecting and responding to cyber incidents.

### Life Before Polaris

Before implementing Axur's Polaris, Scunna faced challenges in monitoring external context threats for their clients. Despite having vulnerability management tools, they lacked a solution that combined threat identification with action planning, which had to be performed by an analyst.

### Introducing Polaris for MSSPs

The introduction of Polaris revolutionized Scunna's vulnerability management approach.



*"What sets Polaris apart is how it provides thoroughly processed external context threat information, ready with the potential issue and its possible solutions."*

Paulo Reus, Operations Manager at Scunna's Cyber Defense Center.

Moreover, the Operations Manager emphasized its advantage over other solutions:



*"A traditional tool in our daily routine only points out the problem, not the solution. Polaris does both: it scans the environment, the infrastructure, and says: this threat exists, it's relevant to your setting, and here's what you can do about it."*

### Life After Polaris

One of the most impactful changes was the significant reduction in workforce needed to monitor and respond to threats.

### Significant Reduction in Workforce

Scunna estimates a workforce reduction of around 50% or more, highlighting the optimization of the security team to focus on more critical tasks.



*"Polaris automates an analyst's job. You no longer need to consult hundreds of information sources. Of course, you'll still need someone to validate the AI's information, but this reduces the number of people needed for this task and the effort they would have to put in."*

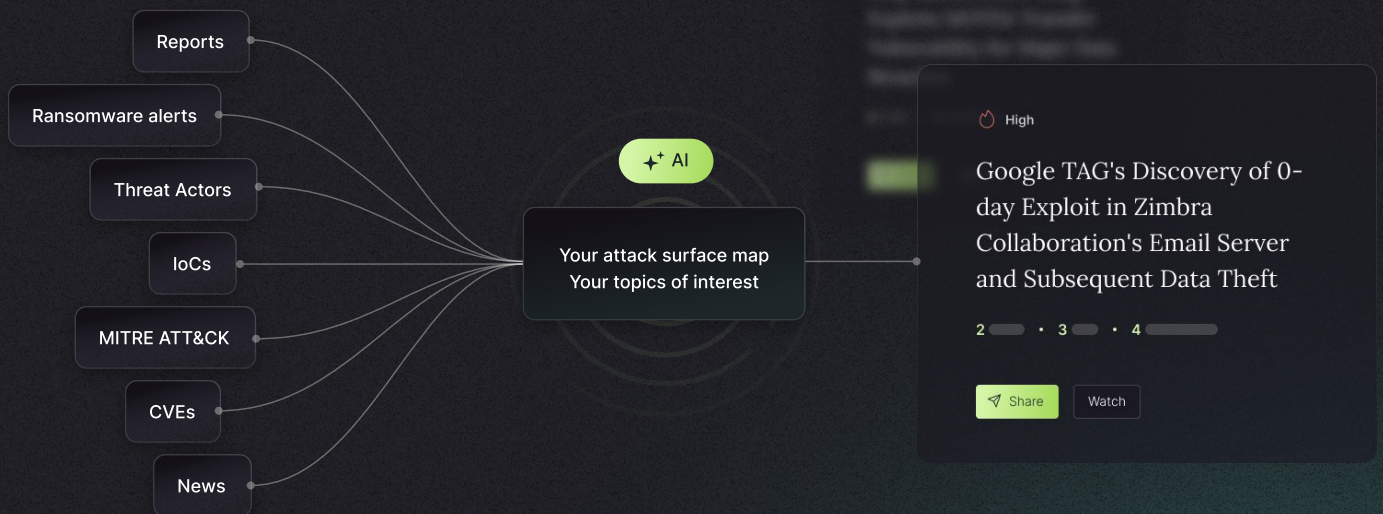
With Polaris, Scunna reinforces its position as a leading MSSP, proactively tracking and managing threats with automation, ensuring continuous defense against threats.

## About Polaris

Polaris is an AI-powered threat intelligence advisor that provides AI-curated, actionable insights tailored to attack surface maps.

## How Polaris works

- Everyday, Polaris scans thousands of sources looking for information about common vulnerabilities, ransomware alerts, Zero-Day exploits, IOCs, frameworks (MITRE ATT&CK), and exposures (CVEs).
- Its highly specialized LLM model sums up every relevant attack, threat, or vulnerability and cross-reference with your Attack Surface Map;
- So it sends curated, actionable alerts with only what you really need to know, nothing else.



## The Benefits of Polaris for MSSPs

The benefits of Polaris for threat management extend beyond risk identification.

- Time Saving: Polaris increases the screening of cyber threats by up to 180x, making analysts' day-to-day 33% more productive;
- Cost Reduction: complete more projects in less time and focus your key analysts only on what's most important;
- Optimized Decision Making: alerts with context and direction, facilitating incident response;
- Revenue Growth: sell more projects to your existing clients with the right analysis and action plans to address the risks.

Start now with a free trial to experience the power of an AI-Powered tool to accelerate your business growth.

Start your free trial

///AXUR

Polaris is powered by **Axur**, a leader in External Threat Intelligence, identifying and mitigating emergent threats for global organizations. With scalable intelligence and automations, Axur's solutions empower businesses and make the internet a safer place. Contact us at [contact@axur.com](mailto:contact@axur.com) or learn more about Polaris at [axur.com/polaris](https://axur.com/polaris)