HUNTERS

HUNTERS SOC PLATFORM

The **AI-Driven**, Next-Gen SIEM for Small Teams

The stakes are high and threats evolve at machine speed. It shouldn't feel impossible to run a SOC, but most SIEMs can't keep up. They collapse under the complexity, leaving SOC teams scrambling.

You don't have time (or money) for this.
You need a solution that works the way you need it to — **Out of the Box.**

Big Impact Without Big Headcount

- Deploy in days, not months
- Fixed cost data ingestion
- Full context alerts
- Specific recommendations
- Automated triage
- Streamlined investigation

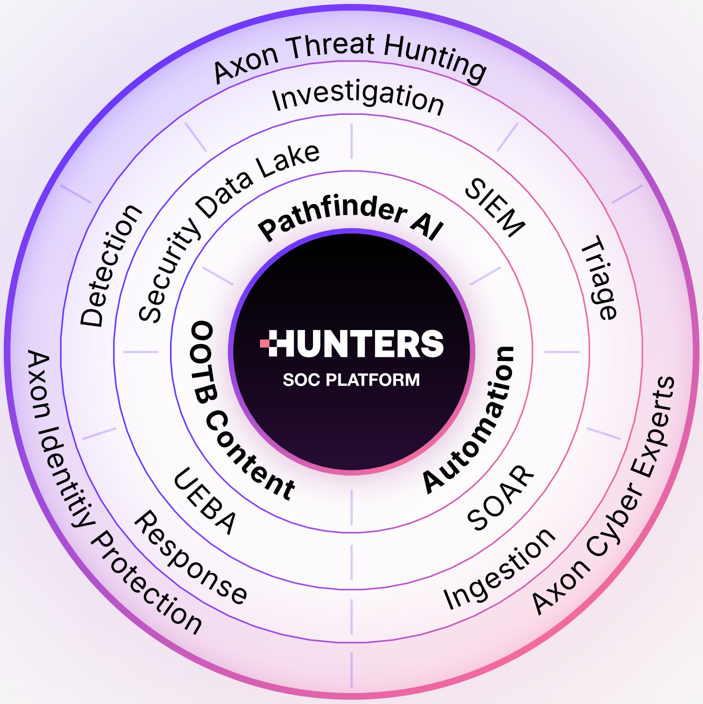
Without...

- Extensive user training
- Ongoing maintenance
- Detection Engineering
- Rule Updating

Hunters SOC Platform is a Next-Gen SIEM built to empower small security teams like yours.

With an **AI-driven platform**, Hunters automates ingestion, detection, triage, investigation, and response. All at machine speed. This reduces your alert triage time, ensuring your team focuses on critical threats with complete context and confidence.

A True All-in-One SOC Platform



Reduce blind spots

Automatically pulls security data from all sources into an open security data lake.

Have deeper visibility into threats

AI-powered analysis diminishes excessive alerts by enriching data and correlating related signals into Attack Stories, which are then followed by advanced threat detections

Take confident action

Every lead is enriched with key context and dynamically adjusted Risk Scoring. Pathfinder AI then summarizes findings, explains detection logic, and suggests next steps.

Streamline remediation efforts

Take direct action with out-of-the box remediation playbooks, AI-generated response plans, and connections to ticketing and other security tools.

Key Benefits

INGESTION
Full Security Visibility Without Complexity

- ✓ See the whole picture by ingesting, normalizing, and retaining all **your security data**–at a fixed cost.
- ✓ Eliminate costly data management by **bringing your own data lake** or let Hunters handle it for you.
- ✓ Break down silos with **interoperability across security tools**, ensuring control over your data—without vendor lock-in.

DETECTION
Stop Threats Before They Escalate

- ✓ Detect threats with **advanced detection and UEBA** before they become incidents.
- ✓ Prioritize and track real threats with **AI-powered correlation** and connect the timeline in **Attack Stories**.
- ✓ Free up analyst time with **pre-built, always-on, continuously tuned** detections mapped to MITRE ATT&CK.

TRIAGE & INVESTIGATION
AI That Thinks Like an Analyst

- ✓ Reduce alert fatigue and false positives with **automated alert triage**, prioritization, and contextual enrichment.
- ✓ **Pathfinder AI** provides findings, explanations & next steps—**all out of the box.**
- ✓ Investigate attacks utilizing **fast, simple, Search** over OCSF-mapped data.

RESPONSE
Act Faster, Contain Threats Sooner

- ✓ Contain threats immediately with Built-in **response automation.**
- ✓ Make remediation easy with pre-built response and **one-click integrations** with ticketing systems.
- ✓ WIth AI **prioritizing the most critical threats**, you focus on what truly matters.

AXON

Need extra help? Team Axon acts as an extension of your team, offering rapid response, threat hunting, and security insights to keep you ahead of cyber risks.

It’s time for something better. With Hunters SOC Platform, you eliminate the cost or complexity you have come to expect from previous SIEM technology. Make the switch to the Next-Gen SIEM for small teams, built for battle, not bureaucracy.

Trusted by Security Teams Like Yours

> “With Hunters, we reduced false positives by 80% and investigations that took hours now take minutes. It’s a game-changer for small security teams."
>
> **— Director of Cyber Defense,**
> **Leading Global Enterprise**

HUNTERS

See Hunters In Action →