Threat Hunting as a Service

Hypothesis-driven hunts run on a regular cycle against your own telemetry, surfacing the activity conventional controls miss and turning each finding into lasting detection.

The question it answers

Detection tools report what they were built to recognize. The threats that matter most are the ones designed not to look like anything a rule was written for. Hunting is the deliberate search for what the controls were never going to raise.

Built on the telemetry you already pay for

The service connects to the EDR, SIEM and network detection systems already in place and aggregates their telemetry and logs. No agents are introduced and no new licences are required.

Data is processed on a dedicated server, where analysis and pattern recognition can be applied at a depth a console query cannot reach. What the hunts learn is converted into detection content your team keeps.

How the hunts work

Threat intelligence-led hunts

Hunts driven by current indicators of compromise from active attack campaigns, analyzing known malicious patterns and adversary techniques to find similar activity in your environment.

Anomaly and pattern recognition hunts

Telemetry and logs examined for anomalies and advanced attack patterns, aimed at the unusual activity and sophisticated threats that evade traditional detection.

Real-time use-case development

Findings from both hunt types are turned into new real-time detection use-cases, so each cycle permanently improves your monitoring rather than only reporting on a moment.

Continuous adaptation

Hunting strategies are adjusted each cycle to track the evolving threat landscape and changes in your environment, so the hunts stay relevant instead of repeating.

AT A GLANCE

CYCLE
Monthly hunts, run systematically

MINIMUM TERM
One year

DATA SOURCES
Your existing EDR, SIEM and network detection

PROCESSING
Dedicated server, outside your production estate

AGENTS REQUIRED
None. No new licences

WHO THIS IS FOR

- SOCs that see alerts but have no structured way to look for what never alerted.
- Organizations that have invested in EDR and SIEM and want more out of the telemetry than the console returns.
- Teams under pressure to show a proactive posture to stakeholders and regulators.
- Security functions that need senior capacity without adding headcount.

How an engagement runs

01 Integration

Connections are established with your existing EDR, SIEM and network detection systems to aggregate the telemetry and logs the hunts need.

02 Aggregation and processing

Collected data is processed on a dedicated server, where the analysis techniques the hunts depend on can be applied at full depth.

03 Hunt cycle

Hunting runs on a monthly cycle, combining intelligence-led and anomaly-based techniques so the environment is examined regularly and systematically.

04 Use-case development

Each cycle produces new real-time detection use-cases from what the hunts found, handed to your team to run continuously.

05 Feedback and adaptation

Regular feedback and adjustment of hunting strategy against the current threat landscape and your specific environment.

WHY ALEXSTA

- Senior hands only. The operator whose experience you are buying does the work, rather than reviewing it.
- Every cycle leaves detection capability behind, so the value compounds instead of resetting each month.
- Conclusions carry their evidence and a stated confidence level, including what the evidence does not settle.

WHAT WE NEED TO SCOPE IT

- Size of the environment: number of endpoints and users.
- Count of applications exposed to the internet.
- The security technologies already in place and available for integration.
- Desired duration of the service, with a one-year minimum.

What you receive

Threat hunting report

A detailed account of each cycle: the hunts performed, what was found, and the potential threats identified, with the evidence behind each conclusion.

Real-time detection use-cases

New detection content derived from the hunts, written to run in your own tooling and owned by your team after handover.

Continuous improvement plan

Recommendations for strengthening monitoring and detection, informed by what each cycle reveals about coverage.

Environment-specific insight

Findings framed against your estate and threat profile, so security strategy is shaped by observation rather than by generic guidance.

Request an engagement

Hunting only pays back when it runs on a cycle. Tell us what telemetry you hold and we will tell you what a first year would realistically surface.

contact@alexsta-cybersecurity.com
+41 76 76 44884
alexsta-cybersecurity.com