
MXOC+
Purpose-Built Platform.
Precision Engineering.
Always-On Experts.
Antarex

# Product Features

## Unified Platform

**Detection. Correlation. Response. All in One.**
MXOC+ unifies SIEM, XDR, threat intelligence, vulnerability, and active response into a single managed platform.

## Engineering Excellence

**Built-In Detection, Tailored for You**
Delivered with curated use cases, parsers, and playbooks ready to run from day one. Our engineers refine and tune them to match your unique environment and risk profile.

## 24/7 Expert SOC

**Human-Led, AI-Enhanced Response Around the Clock**
Round-the-clock threat hunting, triage, investigation, and response — led by seasoned analysts and accelerated by AI. Every alert is validated. Every incident is contained. All without draining your internal resources.

# Outcome

## Faster Threat Resolution

Automated playbooks and analyst-led response contain threats in minutes, not hours. Reducing dwell time and business risk.

## Less Noise, More Signal

Context-aware detection reduces alert fatigue and false positives, so your team only sees what matters.

## You Get Outcomes, Not Overhead

Delivered as a fully managed detection and response service, MXOC+ combines our unified platform, engineering expertise, and 24/7 SOC operations.

## Full Visibility Across All Assets

Consolidated detection and response across endpoint, network, cloud, Apps, and SaaS, nothing is missed.

## Audit-Ready Confidence

Aligned to NIST, PCI-DSS, ISO 27001, and more. With retained logs and reporting built in.

# How It Works

**Ingests Logs and Telemetry from Anywhere**
Supports all common formats and protocols — including API, syslog, agent, cloud connector, and more.

**Correlates and Enriches in Real Time**
Fuses raw telemetry with threat intelligence, vulnerability context, and behavioural signals to surface high-confidence threats.

**Prioritises with Context**
Threats are evaluated by severity, exploitability, and business relevance, not just rules.

**Responds with Automation or Analyst Review**
Playbooks act instantly, or escalate to SOC analysts for validation and containment.

**Continuously Updated by Antarex**
Detection logic, response playbooks, and intel sources are updated continuously — no maintenance required from your team.



antarexcyber.io hello@antarexcyber.io