Wazuh Case Study

Antarex's MXOC+ Platform Powered by Wazuh

Executive Summary

Antarex focuses on providing engineering-driven Security Operations through its Managed Extended Operations Center+ (MXOC+). As customer environments became more complex and diverse, Antarex required a flexible and scalable foundation to build advanced detection, automation and compliance capabilities.

Tim Quek

Deputy CEO

"Traditional SIEM platforms limited our ability to scale and innovate. Wazuh removed these barriers with its open and scalable architecture"

Challenge

As Antarex expanded its Managed Security Services across diverse customer environments, maintaining efficiency, flexibility and detection accuracy became increasingly challenging:

- Limitations from proprietary SIEM platforms with high scaling costs
- Rigid integration models
- Difficulty onboarding heterogeneous and legacy environments
- Limited flexibility to continuously refine detection strategies
- Alert fatigue caused by high volumes of low-quality security events

They required a platform that enabled engineering flexibility while supporting scalable, outcome-driven security operations.

Solution

Antarex selected Wazuh for its open architecture, cost efficiency and detection extensibility aligned with its long-term MSSP strategy. Using Wazuh as the core engine of its MXOC+ platform, they deliver continuous monitoring, advanced detection engineering, threat intelligence correlation layers and automated response workflows across diverse environments.

Use Cases

- Managed Detection and Response (MDR) across multi-environment infrastructures.
- Threat detection aligned with MITRE ATT&CK
- Continuous Compliance monitoring and reporting
- Automated incident response and enrichment workflows

Wazuh Case Study

Antarex's MXOC+ Platform Powered by Wazuh

Results

In one customer case, Antarex reduced security-related tickets from over 100.000 to 20.000 within 12 months, achieving an 80% reduction in alert volume while improving detection accuracy. They also achieved:

- Enhanced visibility across endpoints, servers and infrastructure.
- Accelerated onboarding of new customer environments.
- Stronger alignment with compliance and regulatory requirements.
- Faster triage and incident response through structured workflows.
- Improved detection precision and operational efficiency.

Key Benefits

- Open and extensible security architecture.
- Advanced detection engineering capabilities.
- Real-time threat detection and response.
- Integrated compliance monitoring.
- Automated enrichment and response workflows.
- Scalable and cost-efficient SIEM/XDR foundation.

About Antarex

Industry

Cybersecurity Services.

Services

Managed Security Operations, Threat Intelligence, Detection and Response, AI-powered Cyber Defense.

Location

Singapore (HQ) with regional presence across Southeast Asia.

Company Summary

Antarex is a cybersecurity provider delivering fully managed, AI-powered security solutions designed for ISPs, enterprises and digital infrastructure environments, providing end-to-end protection across the entire attack surface: from network edge to core infrastructure.