The Xari Xecure® Suite

XARI SIEM SOC+

Cybersecurity monitoring for businesses, combining automation and 24/7 expert human overview.

Why do organisations need cybersecurity monitoring?

Businesses today are constantly under threat of cyberattacks. You may think that your business is too small to be a target. Unfortunately, this isn't the case. Companies of all sizes are at risk. You must be on guard and protect your personal identifiable information, proprietary information, and other confidential data from being compromised or stolen. This is why you must use cutting-edge security strategies like a security information and event management system (SIEM) and Security Operations Centre (SOC).

What are SIEM and SOC?

SIEM (Security Incident and Event Management) is a tool that collects and normalises logs which are tested against a set of correlation rules that when triggered creates events for human analysts to analyse. It identifies, monitors, records, and analyses security events within a real-time IT environment. It provides a centralised and comprehensive view of the security of your IT infrastructure. A SIEM searches and filters data and can tell who did what, when, and from where. It uses predefined correlation rules from previously detected attack vectors. Then it provides audit-quality reports that can be used for compliance purposes.

SOC (Security Operations Centre) is a centralised unit of security analysts (and related job roles) that deal with security issues, using a variety of tools. A SOC uses SIEM software as a foundational component in gathering information from a high volume of diverse log data collected by computers and servers, as well as security devices like firewalls, intrusion detection/prevention services, databases, applications, switches, and routers.

When a cyber incident strikes, your organisation needs to respond in the fastest and most appropriate way. How confident are you that you have the best event monitoring and incident response plan? How sure are you that your IT team or service provider are rapidly and proactively monitoring and managing your cybersecurity position?

xarigroup

Xari Group Pty Ltd is a security-first MSP (Managed Services provider) based in Brisbane, with over 10 years of experience and expertise in IT and now cyber security, working with SMBs of varied size from diverse industries.

The Xari Xecure® Suite

XARI SIEM SOC+

Unfortunately, a SIEM is not a holistic cybersecurity solution. Organisations need more than a SIEM. You can invest vast amounts of time and money into a SIEM, but with the sophisticated and evolving attacks of today's threat landscape, you need more; you need a SOC with 24×7 network security monitoring. But building a SOC is also complicated, costly, and time-consuming. **In addition to buying and setting up your own SIEM, you'll need to train a team of security experts to implement it. For most organisations especially SMBs, budgets won't allow this.**

The Xari SIEM SOC+

Xari SIEM SOC+ provides the end-to-end security that companies need. It is essentially outsourcing a security service focused on threat detection and incident response. Xari SIEM SOC+ is cost-efficient because it doesn't require investment in additional hardware, software, or staff. It's quick and easy to deploy and manage, and you'll have the security experts, process and technology you need to run a SOC.

Xari SIEM SOC+ Features	Inclusions
Fully hosted, redundant, and managed SIEM platform	✓
In-depth Behavioural and Anomalous Activity Monitoring	✓
Proprietary, Pre-Tuned Rules Matrix and Customised Rules	✓
Ongoing Rule Tuning and False Positive Reduction	✓
Enriched Notifications Including Remediation Guidance	✓
Integrated Global Threat Database from Multiple Thread Feeds	✓
Over 2,200 Pre-built Compliance and standards-Based Reports	✓
Automated Notifications, 24/7x365	✓
Daily SOC Review for Human Oversight	✓
Forensic Investigation and Compliance Assistance	✓
Tier 3 Incident Response Escalation Support	✓
Event Log Consolidation and Management	✓
Network, Virtualisation, and Application Intelligence	✓
Configuration Change Management	✓
Custom Report Creation and Scheduling	✓
Comprehensive Device Support	✓
Weekly Device Discovery Validation	✓
Audit/Exam Support	✓

Xari SIEM SOC+ protects your IT infrastructure and resources wherever they reside, including on-premises, cloud infrastructure, and SaaS applications. Key unique benefits include:

- ✓ Completely customised monitoring and compliance
- ✓ Scalable & cost-effective coverage of some or all of the IT environment
- ✓ Turnkey solution, requiring no resource investment
- ✓ Custom support and remediation from a trusted MSP
- ✓ Exclusive – not available from legacy MSPs or MSSPs or from any standalone software or hardware product