Advanced Security Defence

With our 24/7 Security Operations Centre (SOC)

SOC-as-a-Service

Our SOC-as-a-Service provides continuous monitoring, proactive threat detection and expert incident response to help protect your organisation 24/7. By combining advanced technology with experienced security analysts, we help reduce cyber risk while easing the burden on internal IT teams..

Cyber threats are becoming more sophisticated, requiring more than traditional security controls. KickSecure's fully managed Security Operations Centre (SOC) combines advanced technology, AI-assisted analytics and expert security specialists to provide 24/7 threat detection, investigation and response, helping strengthen your security posture and improve cyber resilience.

Technology

Security Operations Data Sources

- Endpoints
- Network
- Cloud Resources
- Microsoft 365
- Microsoft Azure
- Identity & Access Management
- Log Events & Machine Data
- System & Application Data
- Threat Intelligence
- User Behaviour Analytics
- Web & Proxy
- Vulnerability Assessments

Data Collection & Analysis

- Data collection and normalisation
- Event correlation
- Log enrichment
- Behavioural analytics
- AI-assisted threat detection
- Risk identification and prioritisation
- Automated response workflows

People & Process

Security Operations

- Continuous monitoring
- Security optimisation
- Compliance reporting
- Business continuity
- Incident management
- Threat intelligence
- Security performance reporting

Threat Detection & Investigation

- Threat detection
- Incident investigation
- Proactive threat hunting
- Impact assessment
- Risk prioritisation
- Escalation management

Incident Response

- Threat containment
- Automated response
- Alert management
- Remediation activities
- Operational support

Kick