Advanced Security Defence

WITH OUR 24/7 SECURITY OPERATIONS CENTRE (SOC)

Yesterday's security is no match for the evolving threats and attack methods used by today's cyber criminals. You need to build a comprehensive security defence using proactive strategies and advanced security controls to dramatically improve your security posture, enabling you to confidently protect your business-critical systems and data.

KickSecure SOC leverages the power of people, processes and technology. Our fully managed SOC-as-a-service solution leverages the power of people, processes and technology to quickly detect and remediate threats or breach events, thereby ensuring a more preventative approach to cybersecurity.

SOC-As-A-Service

Technology

Security Operations Data Sources

- Endpoints
- Network
- Cloud Resources
- Log Events & Machine Data
- Vulnerability Assessments
- Unstructured Data
- System & Application Data
- External Threat Intel
- User Behaviour Analytics
- Web & Proxy

Data Aggregation & Qualification

- Data Compression
- Combination Filtering
- Structure Formatting
- Interrelation Analysis
- Search and Machine Analytics
- Identify Risks & Qualify Threats
- Automated Response

People & Process

Security Intelligence & Operational Processes

- Maintenance
- Performance & Efficiency
- Recovery & Continuity
- Regulatory Compliance
- Incident & Crisis Handling
- Data Fusion and Visualisation
- Security Control Actions or Changes

Threat Investigation Triage

- Isolate & Assign Severity
- Incident Investigation
- Real-Time Threat Hunting
- Impact Analysis
- Triage or Escalate

Incident Response

- Containment
- Automated Response
- Notifications/Alerts
- Remediation Actions
- IT Operations Support

- 24/7 X 365 Monitoring and Response
- Event Tracking Records for Compliance
- Operational Performance Analytics
- Continuous Vulnerability Checks

www.kickict.co.uk/kicksecure