Security Operations Centre (GTN-CERT)

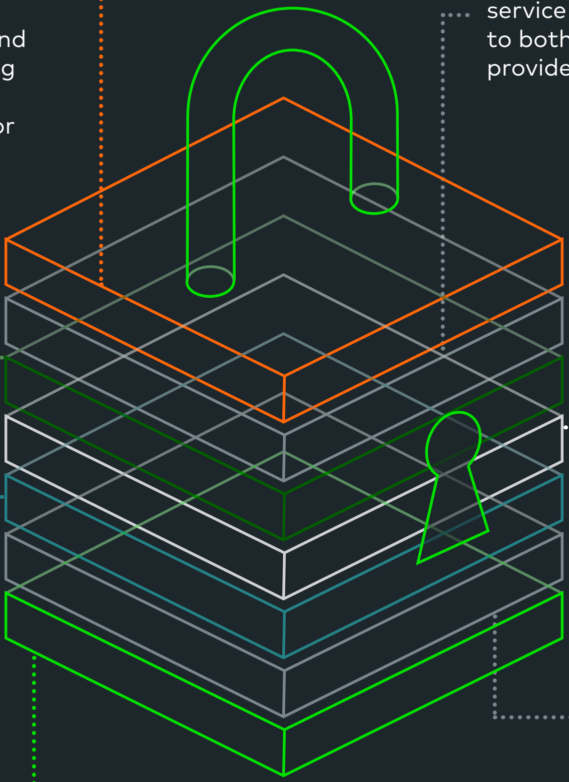
Getronics Security Operations Centre, a registered computer emergency response team (CERT), assists organisations in achieving their desired security posture and compliance objectives through a range of services, with a focus on Threat Lifecycle Management (TLM) and especially detection and response. All services are designed to be fully ITIL and NIST aligned.

Services available today are:

Enterprise Log Management for the automated collection, processing, parsing and storage of logs. Using a machine data fabric of over 600,000 rules to enable detection of security events, standardize input from different log sources and meet compliance controls including ISO27001:2013 and over 40 other frameworks for specific national or industry verticals.

Cybersecurity Incident Response Team to rapidly analyse, plan and manage the containment, mitigation and eradication of any security breach through pre-planned Courses of Action that can be adapted to the context of a wide range of over 30 distinct attack types such as ransomware.

Configuration Assurance providing analysis against configuration policies such as CIS framework and a range of other standards including USGCB and FDCC to enable device hardening through highly granular controls. Support for desktop and server operating systems as well as browsers, database and IIS, Apache and more.



Reconnaissance Assessment provides a point-in-time assessment of attack vectors through OSINT analysis. This can both inform efforts to minimize attack surfaces and focus detection on the path most likely to be chosen by an attacker. Findings are presented in accordance with NIST Security Controls.

Cybersecurity Analytics for continuous monitoring and alarm triage. Leveraging a modern MITRE ATT&CK based detection playbook for known attacker techniques, tactics and procedures. The service is built on a market leading SIEM to both maximize detection ability and provide compliance reporting.

Vulnerability Management for discovery and audit scanning to identify and track Common Vulnerabilities and Exposures (CVE) within the client estate. Provides risk-prioritized remediation reports to help focus efforts where the best return will be gained as well as trend and executive reports to management readers.

Firewall Assurance to efficiently import and analyse configuration, policy and access compliance. Ensures the organization is not exposed to risk through overly permissive rules, deviation from vendor best practise or violations of specific compliance frameworks.

Security Operations Centre (GTN-CERT)

Other service elements are available, fully integrated with the SIEM for seamless detection workflows, such as:

- **Network Traffic Analysis (NTA)** with full packet capture and layer 2-7 DPI/DPA
- **File and Registry Integrity Monitoring (FIM)** with real-time and interval options
- **User and Entity Behaviour Analytics (UEBA)** for anomaly detection and risk rating
- **Endpoint Management** - DLP, EDR, NDR, MFA etc.

Getronics' Cybersecurity Threat Intelligence is used to inform and guide many of the services and provide efficient cross-referencing of security events with known Indicators of Compromise (IOC) and attacker behaviour.

The service mix is tailored to meet client compliancy requirements and a structured approach is used to ensure cost efficiency through a Security Operations Maturity Model supported by a Configuration Management Framework .

Why Getronics?

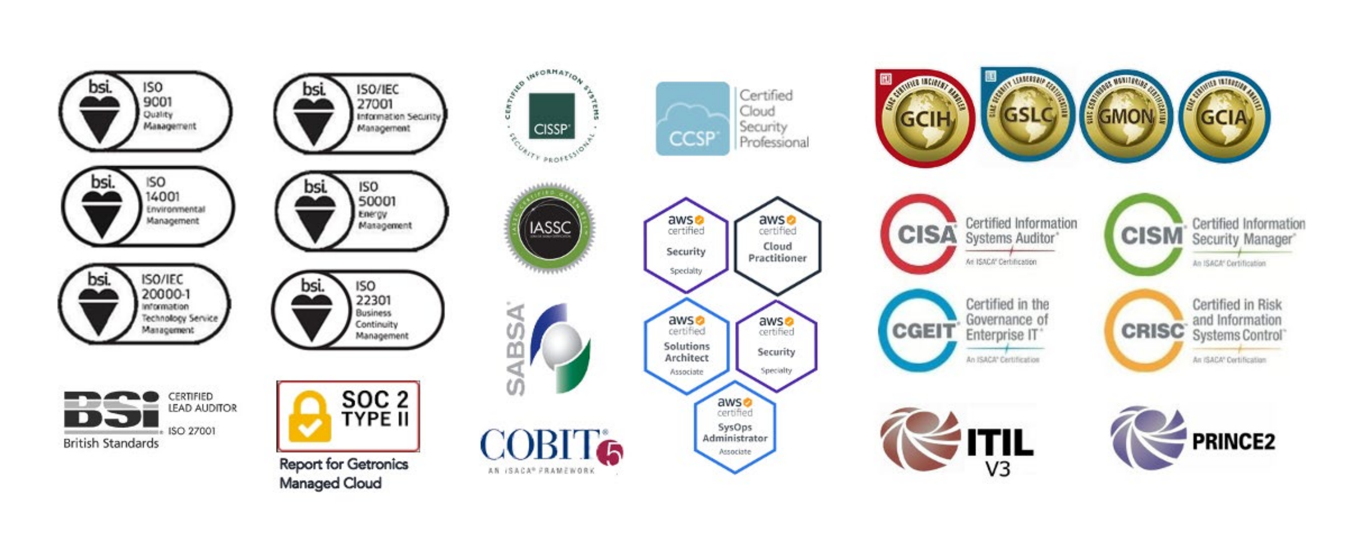
Our skilled staff and experience in security operations provides a cost efficient and dynamic security service that can be rapidly deployed. The Services are fully accredited to ISO27001:2013 and are subject to an internal and external audit and review programme to ensure it continues to meet and improve on the requirements mandated.

Outsourcing Protective Monitoring to Getronics removes the strain from your internal teams, with improved cost and service efficiencies when compared to dedicated solutions.

Getronics works with clients to become a trusted partner for security consulting, design, implementation, and support in matters relating to cyber security and compliance.

We have a flexible Consultative approach and a framework that is designed to capture business requirements and customer specific business needs with our services being hosted and delivered from within the EU.

Accreditations and reporting


bsi. ISO 9001 Quality Management
bsi. ISO/IEC 27001 Information Security Management
bsi. ISO 14001 Environmental Management
bsi. ISO 50001 Energy Management
bsi. ISO/IEC 20000-1 Information Technology Service Management
bsi. ISO 22301 Business Continuity Management
BSI British Standards CERTIFIED LEAD AUDITOR ISO 27001
SOC 2 TYPE II
Report for Getronics Managed Cloud
CISSP
IASSC
SABSA
COBIT 5 AN ISACA FRAMEWORK
CCSP Certified Cloud Security Professional
aws certified Security Specialty
aws certified Cloud Practitioner
aws certified Solutions Architect Associate
aws certified Security Specialty
aws certified SysOps Administrator Associate
GCIH
GSLC
GMON
GCIA
CISA Certified Information Systems Auditor An ISACA Certification
CISM Certified Information Security Manager An ISACA Certification
CGEIT Certified in the Governance of Enterprise IT An ISACA Certification
CRISC Certified in Risk and Information Systems Control An ISACA Certification
ITIL V3
PRINCE2