SCC Security Lifecycle

SCC's Security Lifecycle helps customers to align their security strategy with risk management and business requirements. The lifecycle is based on our continuous review and adaptation of technology and processes, using a four stage model: PREDICT, PREVENT, RESPOND, DETECT.

PREDICT

Our PREDICT stage is a consultative approach where we offer assessments to evaluate and understand your current security posture.

The ultimate goal of this stage is to assist our customers to discover the gaps or areas of improvement by looking at people, processes, technologies and regulation. We engage with organisations that:

- Require a 360 degrees review of their security infrastructure, policies and procedures.
- Need to know what security gaps exist in their systems and processes and how exposed they may be.
- Need to meet regulatory and compliance requirements.

PREVENT

We work closely with you to define, supply and implement the most appropriate solutions and services to ensure the consistency and effectiveness of your security strategy.

Organisations are adopting new business models that are increasing their attack surface and have a direct impact on their security strategy. At the PREVENT stage we provide security solutions that assure of customers' security across cloud environments and on-premise infrastructure.

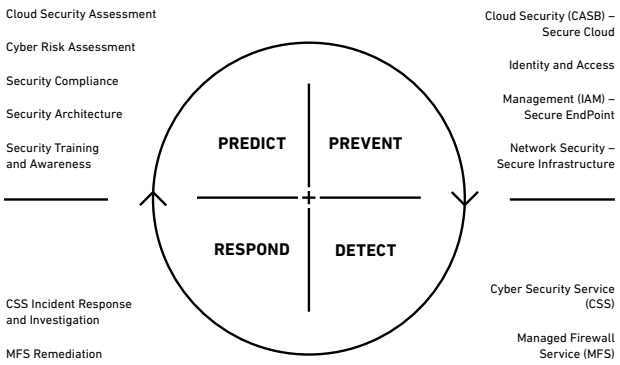
DETECT

The DETECT stage brings to customers the services that will address fundamental challenges around security operations and potential breaches.

SCC provide a Cyber Security Service (CSS) which delivers a full view of known and unknown security offences to your business by collecting data from multiple sources and proactively alerting when a threat is detected. Going further, CSS works in partnership with our clients and actively seeks to provide advice on the best course of action following detection of a threat. This service from SCC can help you meet your regulatory and security compliance requirements.

RESPOND

In the RESPOND stage, our services provide you a remediation plan for you to act upon with our support minimise the impact of a security breach that could be a cyber attack. We can deliver IBM IRIS incident response services and remediation tasks that will provide the next level of protection and risk management.



SCC Security Lifecycle

WHY SCC?

We provide the flexibility to align security services and solutions to the different levels of maturity that organisations have around their security strategy.

Our Security Lifecycle relies on a continuous improvement throughout these 4 stages, providing the flexibility for processes to react to new threats and also helping with an organisation's structural changes and overall business positioning.

This lifecycle approach is powered by our people who are specialists in each area, with knowledge that bridges the operational, commercial and technical processes.

WHY IBM QRADAR?

SCC's CSS service is powered by IBM QRadar which is an enterprise class toolset which is recognised as a leader by multiple independent analyst firms, including being the Gartner Magic Quadrant Leader in SIEM for the last 8 years. SCC complement our multi-tenanted deployment of QRadar with a team of highly experienced security professionals and proven operational processes to deliver the same CSS service we deliver to Government organisations to our commercial clients, adopting the IS027001 and NIST legislations as standard in every aspect of the service we provide. Built on years of experience SCC are able to significantly reduce both the time and cost of deployment by removing the need for complex professional services work to install and tune the tools, providing our clients quicker time to value.

For further information, contact us here:

+ 44 (0) 7972623387

kat.hill@scc.com

www.scc.com