Deployed Security Operations Centre (DSOC)

Overview

DSOC provides a centralised command and control capability for the collection and correlation of Security events from varying classifications of data.

DSOC can be extended to take advantage of Symantec's EAL accredited solutions and integrate with most commercial off-the-shelf security technologies.

Symantec's CLAS Consultants can design, build and, integrate DSOC into an existing or new security architecture, allowing organisations to:

- Control and manage their entire infrastructure
- Maximise their investments in existing security products and gain an improved overall security posture.

DSOC sites within the customer environment

Integrated, proactive security system -

Combines central logging, alerting, and reporting functions with correlation, risk prioritisation, and management capabilities to build an integrated, proactive security system.

DSOC located within customer site and IT domain providing real time cyber oversight

Stage 1

Central integration and correlation architecture - Uses a set of scalable, extensible, and secure technologies to integrate and correlate existing security technologies, providing an interoperable and manageable secure command and control capability.

Internal monitoring centre - Provides a unified internal monitoring and analysis capability. Events generated by disparate security products will be collected, correlated and prioritised across geographies and network tiers, turning security data into prioritised, actionable information. This enables organisations to minimise the complexities associated with managing vast amounts of security event data while maximising control over the security infrastructure.

Stage 2

Once the core architecture is in place (1), external security data feeds and security intelligence can be added to provide vital trending and context to activity monitored internally.

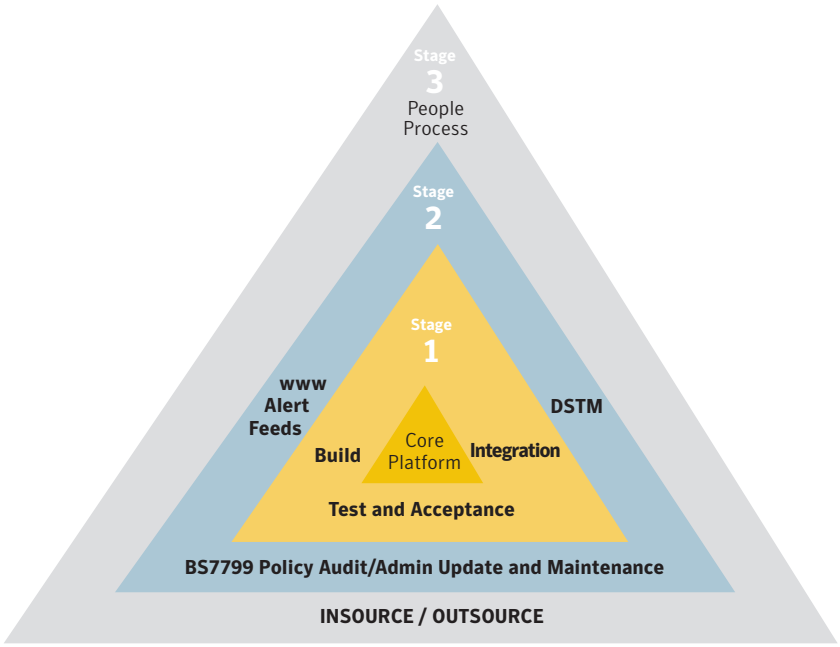
- **Total cyber oversight** - Leverages Symantec's' Global Intelligence Services to track security events on a global basis, providing proactive intelligence and early warning of active attacks.
- **Security policy and compliance management** - Enables organisations to understand their level of security by defining, measuring, and reporting on the compliance of information systems with pre-set corporate security policies, industry-standard security policies, or government regulations.
- **Intrusion detection and prevention** – Enabling organisations to monitor traffic, detect internal and external intrusion attempts, and respond to attacks in real time.
- **Global intelligence** - Leverages Symantec's Threat Management System to track security events on a global basis, providing proactive intelligence, correlating them with your various operating systems to provide early warning of threats allowing you to take action to protect yourself before the event.

Providing capabilities in line with GSEC **Memo 22** and **Memo 37**.

Stage 3

Insourcing/Outsourcing – Once the Core Architecture (1) is in place with the necessary security feeds streaming data and threat information (2) Symantec is able to offer a number of extended services utilising Symantec's expert analysts and support teams to support:

1 Client staff onsite part or full time
2 A complete managed service onsite, or
3 A tailored transition combining 1 and 2 above.



Information Integrity