

Security Operations Analysis & Design Service

Advancing Your Security Operations Capability

At a Glance

- Establishes a plan for the implementation or enhancement of security operations capabilities and procedures, spanning business, technical and operational domains
- Provides an overall design, centered on SIEM and DLP, as well as an Incident Handling framework.
- Based on best practices and proven deployment methodologies and standards such as ISO, SANS and NIST.
- Leverages RSA's real world customer experience, as well as EMC's global Critical Incident Response Team

Companies today face opposing challenges as they secure their operations and information from risk. On one side, threats are increasing, as are the sophistication of attacks. On the other side are today's economic realities; budgets are shrinking, resources are constrained and the costs of managing a security incident larger than ever.

An advanced security operations function centers upon processes that, on a daily basis, enable an organization to more effectively protect critical resources and ensure compliance through incident detection, response and key remediation activities. Specifically:

- Thoughtful identification and development of a comprehensive security operations program
- Effective design of a security operations system that centers upon integrated use of SIEM, DLP & threat intelligence technologies and systems.
- Integration with service management and network operations technologies such as service desk, change and configuration management, and operational frameworks such as ITIL.

- Creation of a sustainable framework for long term security and information risk management

With an advanced security operations function established, organizations will have the processes and capabilities in place to effectively initiate a comprehensive information risk management program.

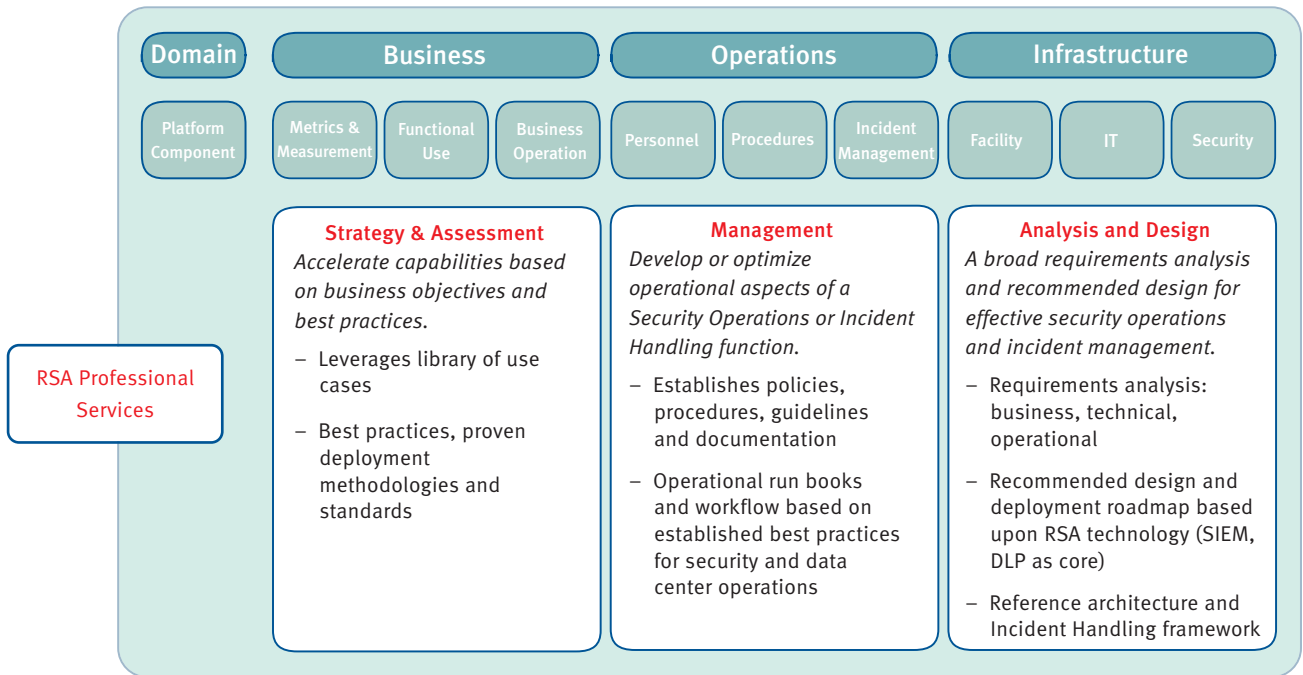
Security Operations Analysis and Design

This consultative and advisory service provides a broad-based analysis of security operations requirements and current state capabilities, and recommends a solution design to meet specific security operations and incident management objectives. It also includes an incident handling framework and next steps for the development of appropriate operational and management policies and procedures. The Security Operations Analysis and Design service can establish your baseline for advanced security operations and can also be the first step towards a more advanced security operations program, or security operations center (SOC) set of capabilities.

Based on an analysis of the business, and the operational and technical requirements for an overall incident handling and data loss prevention capability, this engagement includes four primary components:

- A high level review of the business requirements to support a security operations function
- A detailed review of the technical and operational requirements to support a security operations function, in particular the security information and event management (SIEM) and data loss prevention (DLP) requirements as the core security technologies within the SOC
- Reference architectures for the RSA enVision® platform and RSA® Data Loss Prevention solutions to meet prescribed requirements
- Incident handling framework and next steps for more comprehensive solution design and operations planning.





RSA Professional Services

Security Operations Framework RSA Professional Services offers a suite of consulting and advisory services which address the requirements of any company seeking to advance their Security Operations function.

Scope and Approach

The growth in sophistication of hacker attacks and insider risk is driving organizations to tackle information risk exposure more aggressively. This is testing the traditional view of security operations – limited primarily to security event collection and analysis – and broadening the scope of security operations. An advanced capability today needs to span the monitoring and protection of sensitive information, as well as the infrastructure it may reside on or may traverse across, and be capable of monitoring and reporting information security risks from various sources across the enterprise.

In response to this need, RSA Professional Services has developed the Security Operations Analysis and Design Service, which takes a broad view to span every aspect of advancing a customer’s security operations’ function – from requirements gathering and analysis through the design of an appropriate solution, roadmap and set of incident response framework.

The scope and approach to delivering this service involves the following four phases:

Phase 1: Solution Strategy

- Pre-site kick off outlining strategy, objectives and engagement planning
- On-site workshop based analysis of security operations requirements, as defined by Business, Operational and Technical needs
- Identification of event sources and data for monitoring
- Walk through of incident handling process

Phase 2: Solution Design

- Development of the technical solution design based on the requirements
- Identification of security event sources, data protection requirements, configuration, event volumes and performance, and storage requirements
- Development of appropriate SIEM and DLP solution configurations

Phase 3: Review of Preliminary Solution Analysis & Design Report

Phase 4: Final Report and Presentation