

Security Operations Management Service

Operational Excellence for Security Operations & Incident Response

At a Glance

- Implement security and service management processes and procedures for effective security operations and incident management
- Identify existing processes for automation
- Define and implement comprehensive operational procedures and run-book
- Identify key reports and dashboard views for automation
- Improving efficiency and automation of your security operations across the enterprise

With the increase in external and internal security threats, and a rising tide of security incidents, organizations are enhancing their security operations and incident response methods and procedures to apply intelligence to proactively divert security threats and increase responsiveness to security events, improve efficiency, and accelerate the automation of security operations. To realize the potential of these technologies, you need comprehensive procedures which span security operations and incident response that aligns with business goals, tailored to your particular risks, and customized to your industry and your overarching business and service management processes.

A good set of procedures and an effective operational run-book, uniting your security operations and incident response processes with your business and service management approach, can efficiently translate potential security events and insights into proactive measures to eliminate security threats or increase response to potential risks. Effective management processes will promote actionable incident handling, and increase the overall effectiveness of your security management.

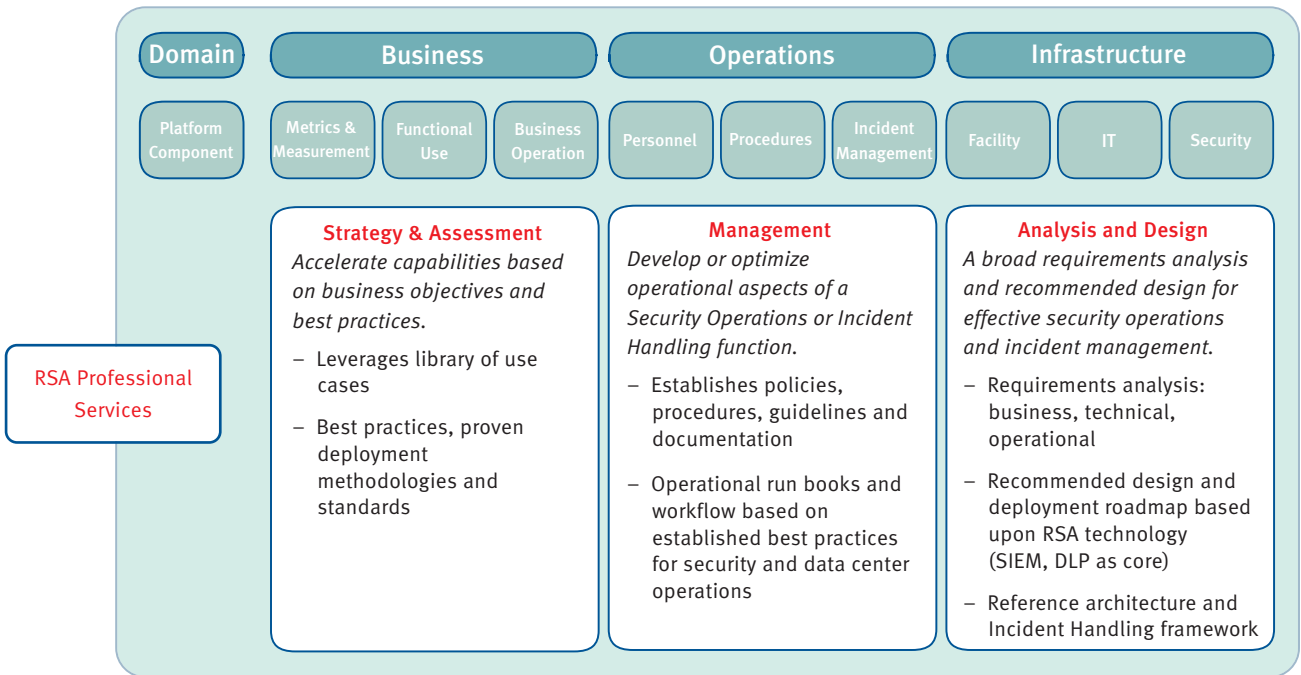
Security Operations Management Service

The Security Operations Management Service is designed to assist organizations with the strategic alignment and automation of security, operations, and compliance processes and reports and enable them to administer an incident handling program on a day-to-day basis. Through the development of processes and procedures, this service aligns operational strategies and methodologies with business requirements.

Currently, in many organizations, technology such as security incident and event management (SIEM) is deployed tactically to address a specific issue or for use simply as a log integrator. Such limited deployment that aggregates security logs, without supporting processes and procedures, fails to exploit the full potential of the SIEM platform to reduce risk and automate security operations. When SIEM is strategically deployed to meet critical business challenges, it is easier to manage security consistently across the enterprise and reduce costs associated with compliance and IT overhead. A comprehensive operational capability allows you to automate as many processes as possible to meet security and compliance goals, while keeping staffing at existing or reduced levels.

This service from RSA increases the return on your investment in security operations by defining effective processes and procedures, centralizing activities and identifying automation efficiencies which, collectively, ensure alignment with business drivers and your overall objectives. The service includes the development of processes and procedures for security management, incident response, compliance reporting and IT operations. For instance, a security review may result in the development of plans for automating aspects of the security operations center (SOC) such as corporate ticketing.





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 Security Operations Management Service encompasses strategies for security management, incident response, compliance reporting and IT operations:

- **Security Management** provides an assessment and roadmap to improve information security management and incident handling operations and procedures. The engagement determines the threats and priorities for incident handling at your organization. This allows for deployment of associated technology solutions such as SIEM to provide create a centralized view of information security and incident handling for improved operations and increased efficiency.
- **Personnel.** Identification and development of the staffing and resourcing model; staff selection and training requirements, roles & responsibilities
- **Incident Response.** Development of security operations management workflow and process for developing, escalating and remediating incidents and alerts
- **Compliance Reporting** considers business need, contractual, legislative and regulatory requirements. It shows you where to align regulatory compliance requirements with ISO 27002 controls. Recommendations include procedures to automate your compliance reporting requirements.

- **Procedures.** Development of the necessary policies, standards and guidelines for the staff along with comprehensive documentation and operational run-book for day-to-day administration
- **IT Operations** provides assessment of IT operations and automation recommendations for improved operations and increased efficiency. Examples include capacity planning, troubleshooting, fault/event detection, Service Desk and Incident Management, and performance. The engagement also helps you to determine the criticality of infrastructure components, and the access requirements to information assets.

Based on best practices, proven deployment methodologies and standards such as ISO, SANS, and the NIST standards for log management, event management and incident handling procedures. RSA security and IT consultants will discover current capabilities, record current status, and align these elements with your business goals and objectives. The final report documents areas to streamline and where to improve efficiency through automation of processes.