



Service Overview

# Infrastructure and Operations Security Consulting

## Ensure Security, Compliance and On-going Effectiveness

### Overview

Perhaps no area of information security has a greater impact on the business than infrastructure and operations security. IT infrastructure, where data is in use, in motion or at rest, is the target for those wishing to steal sensitive data or disrupt business operations. And, Security Operations is typically the front line, after all the controls are established and in place, where threats can be uncovered and risk avoided or, in the event of breach, incident response can mitigate damage.

Security best practices involve building security into the infrastructure – not merely establishing a perimeter defense around it. Advanced Security Operations' role is, therefore, to provide visibility, both within and on the perimeter, to monitor for threats and execute against policy violations.

Of course the best security, as we all know, is that which no one experiences – there's minimal, if any, impact on customers and employees, necessary information is perceived to be freely accessible and the otherwise complex nature of protecting a company from risk is transparent. Well developed infrastructure and operations security and practices can facilitate this.

### Accelerating Infrastructure and Operations Security

Organizations that leverage information for competitive advantage have common traits. They deliver strategic value by leveraging information to drive the business; they are highly efficient and they are operationally excellent.

The RSA Security Practice of EMC Consulting is the global leader in helping customers understand their infrastructure and operations security requirements, implement industry leading solutions and ensure continued and ongoing lifecycle operations excellence.

We focus on operational capabilities which are essential to monitoring critical security or compliance conditions. Our combined consulting, assessment and enablement services provide a current-state gap analysis and assessment of an organization's operational requirements. This includes a comprehensive view across security information event sources to define roadmaps, integration and operational plans to achieve world-class security operations and incident response capabilities. RSA capabilities include solution delivery, dashboard and report development, and ongoing management services.

Our infrastructure security capabilities leverage EMC's heritage as a leader in storage, IT infrastructure and virtualization by offering consultative services which address the major considerations for a secure infrastructure while helping to accelerate business innovation.

## Security Operations Services

### Strategy & Assessment

This is appropriate for customers with established security operations processes, those who are establishing new security operations processes or those seeking to advance their capabilities based on industry best practices and current state gap analysis. This service provides an actionable set of vendor and product-agnostic recommendations.

The Security Operations Strategy & Assessment service offering has four primary components:

- Definition of strategic objectives, stakeholders and target capabilities
- Review of existing capabilities
- Gap analysis between target and existing capabilities
- Prioritized recommendations and remediation

This service spans a company’s business, operational and technical requirements for security operations. It takes a consultative, product-agnostic approach to evaluate and optimize existing client investments in technology while providing a functional roadmap planning future investments.

### Analysis & Design

This service is for clients who want a broad evaluation of security operations requirements which recommend solutions designed to meet the customer’s objectives for security operations and incident management. It also includes an incident handling framework and next steps for the development of appropriate policies and procedures for security operations.

The Security Operations Analysis and Design service establishes the optimum design and recommendations based upon a four step process:

- Business requirements analysis and definition
- Technical, operational requirements for SIEM and data loss prevention
- Solution design
- Incident handling framework and next steps for security operations management

It addresses business, operational and technical infrastructure requirements via a workshop driven approach with technical emphasis.

## Building a Target Capabilities Model

- Provides a consistent, customer-specific framework for assessing the existing state against project objectives
- Incorporates the frameworks or standards in use by the customer (ITIL, COBIT, etc.)
- Maps required capabilities to the security policy, compliance objectives and other business requirements

Define Objectives and Requirements	Gather Information	Identify and Analyze Gaps	Recommendations
<ul style="list-style-type: none"> <li>– Interview stakeholders</li> <li>– Identify key objectives, constraints, criteria</li> <li>– Build a customized Target Capabilities Model</li> </ul>	<ul style="list-style-type: none"> <li>– Analyze relationships between security operations and other functions</li> <li>– Review runbook processes</li> <li>– Review existing reporting capabilities</li> <li>– Inventory tools and existing use cases</li> </ul>	<ul style="list-style-type: none"> <li>– Map current capabilities to the Target Capabilities Model</li> <li>– Itemize deficiencies</li> <li>– Assign risk levels and prioritization</li> <li>– Identify required actions and effort to remediate</li> </ul>	<ul style="list-style-type: none"> <li>– Propose phased approach to achieve key business objectives by remediation gaps between existing state and the Target Capabilities Model</li> </ul>

## Management

For clients seeking the development of more comprehensive policies, procedures, guidelines and documentation for an effective security operations function, including operational “runbooks” and workflow that support the ability to run a security operations center/function or incident handling program on a day to day basis

The Security Operations Management service takes a consultative approach and emphasizes day-to-day operational needs. The objective is the formation of operational policies and practices, and establishes consensus, rationale and strategy with input by all impacted constituents. This service offer provides the following:

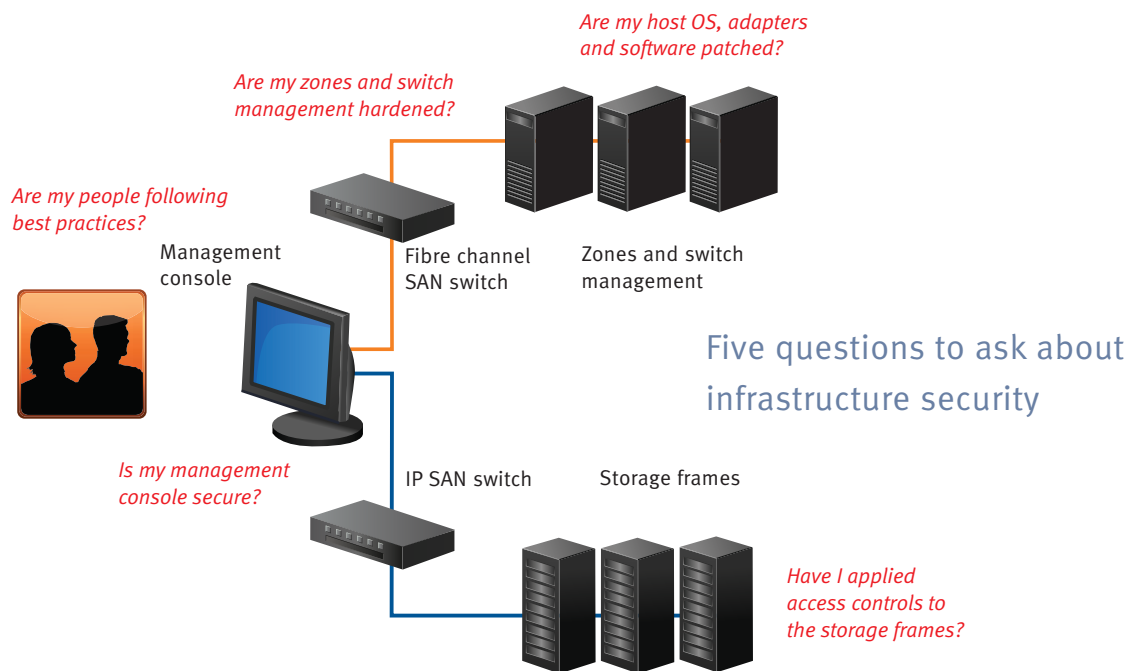
- Development of security policies, standards, and guidelines
- Development of staffing and resource model
- Workflow analysis/development
- Development and documentation of Incident Handling Process
- Operational “runbook” for day-to-day CIRT/SOC administration.

## Infrastructure Security Services

### Assessment for Storage Hardening

Helps improve protection of business-critical information by appraising the security of your SAN, NAS and CAS storage components and configuration. This service is designed to:

- Checks security of entire storage infrastructure: Storage-area network (SAN), network-attached storage (NAS) systems (others, too), SAN fabric switches, storage management interfaces
- Review storage security management, policies, roles and responsibilities, configuration and change management
- Assess storage security technology: architecture, access control, IP-based transport security
- Assess operational controls: administration, media controls, labeling, physical environment



---

## Summary

---

Let the experts in Infrastructure and Operations Security consulting assist you in moving your security posture to the next level and gain a sustainable competitive advantage. The RSA Security Practice of EMC Consulting is a global leader, offering comprehensive services that are tailored to your specific requirement.

### About EMC Consulting

EMC Consulting enables the full realization of the inherent power of information. We create complete information environments that are reliable, efficient and secure. The result is information that reveals its potential. With EMC Consulting, people and organizations can bring the power of information to life...information that illuminates what's possible and that can move the world forward.

### About RSA

RSA, The Security Division of EMC, is the expert in information-centric security, enabling the protection of information throughout its lifecycle. RSA enables customers to cost-effectively secure critical information assets and online identities wherever they live and at every step of the way, and manage security information and events to ease the burden of compliance.

For more information, please visit [www.RSA.com](http://www.RSA.com) and [www.EMC.com](http://www.EMC.com).



The Security Division of EMC

[www.rsa.com](http://www.rsa.com)

EMC, RSA, RSA Security and the RSA logo are registered trademarks or trademarks EMC Corporation in the U.S. and/or other countries. All other trademarks mentioned herein are the properties of their respective owners.