



Confidence in a connected world.

Security Management

Considerations Regarding
Implementing Security Operations
Centers

Presentation Agenda

1 Key SOC Considerations

2 SOC Options

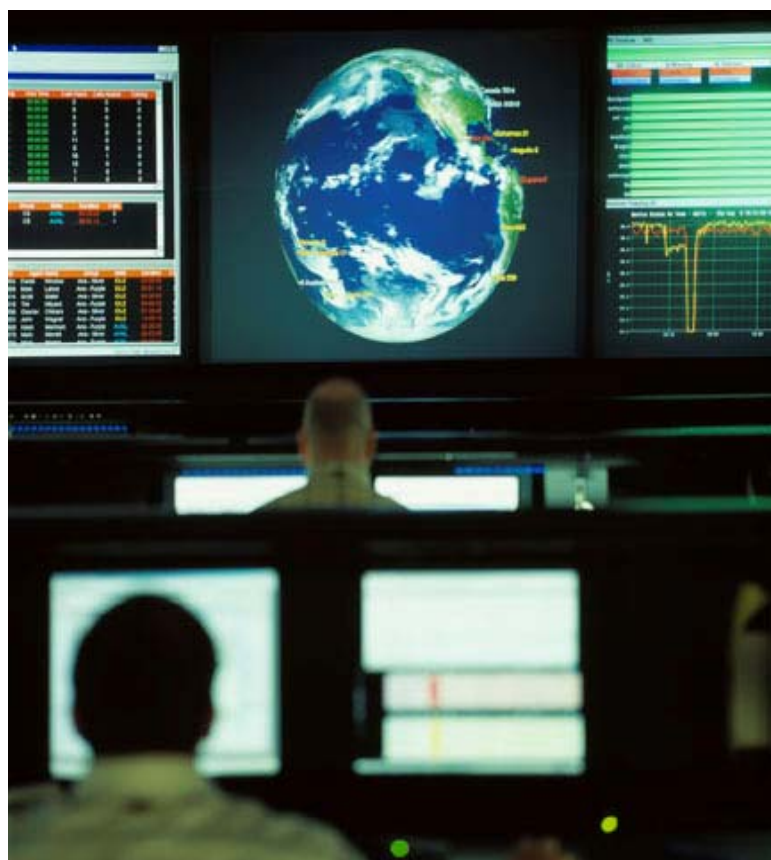
3 Summary

Driving Motivation for a SOC



- Identify security threats that impact business assets
 - Detect exposure of confidential information
 - Prevent a disruption in service
 - Increase employee productivity
- Gain Knowledge of security risks to:
 - Improve asset control - systems being targeted
 - Understand global threat activity
 - Prioritize incident response (patching, virus definitions, IPS signatures)
- Provide Reporting of security posture to executive management
 - A security dashboard for executive view

Security Operation Centers – Key Requirements



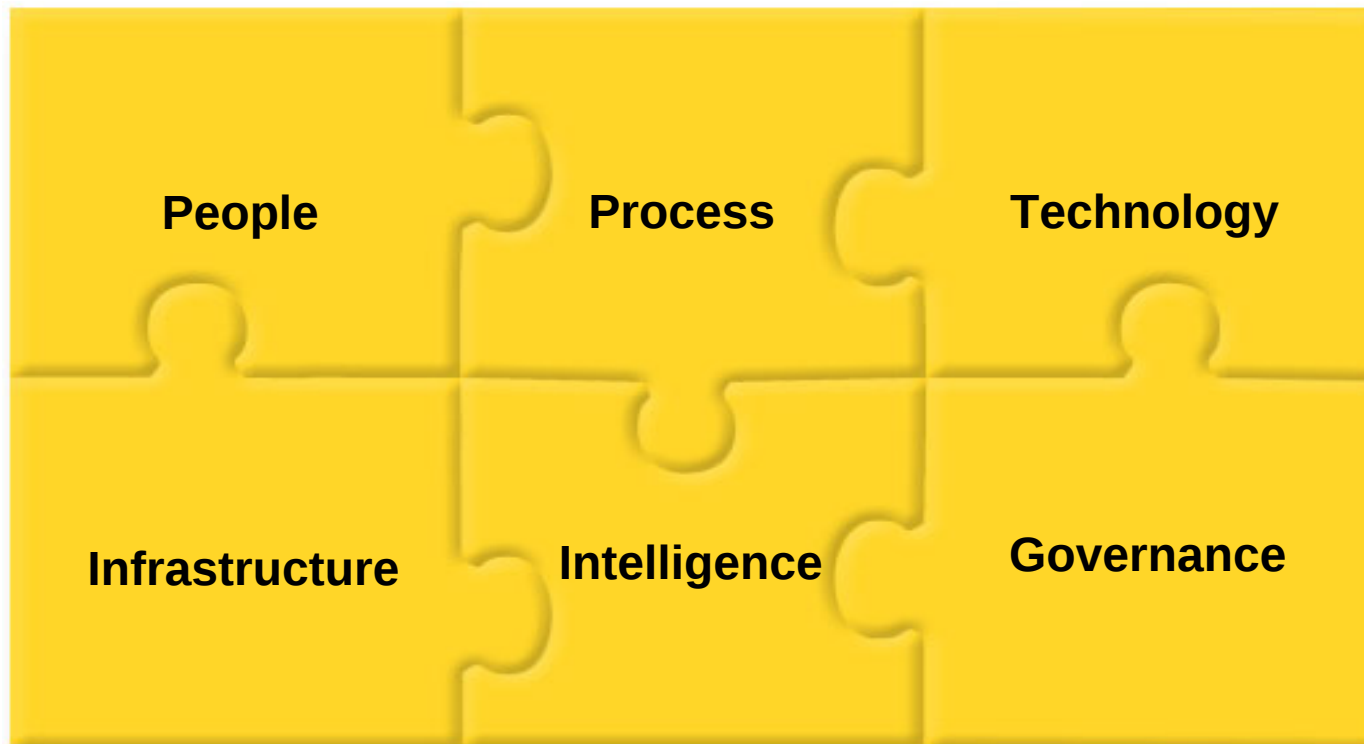
1. Gather *all* security information into one aggregation point
2. Report security posture at corporate/agency level. A dashboard for executive view
3. View security information by event/incident
4. Take immediate action for remediation
5. Protect security data (either trusted source or may not leave organization)
6. Manage threats happening around the world around the clock
7. Satisfy regulatory requirements (HIPAA, SOX, NERC, BASEL..)
8. Retain and retrieve data for investigation purposes
9. Obtain global, local, and personalized intelligence

Key SOC Functionality



- Centralized data logging
- Comprehensive vulnerability scanning program
- Global threat intelligence
- Forensics capabilities
- Incident analysis
- Incident response
- Best practices implementation
- Governance
- Remediation Capabilities
- Report Generation

SOC Delivery Consideration



- **Regardless of approach these elements are always costs to be considered**

People, Process and Technology Considerations



- People – How do you:
 - Find staff with the analysis skill set required?
 - Implement training to keep staff informed?
 - Measure the performance of the staff to insure QoS?
- Process – How do you:
 - Implement a consistent operation procedure?
 - Implement a process to test the procedures you have in place?
- Technology – How do you:
 - Implement a technology that can scale as your organization grows?
 - Implement a technology that supports a variety of technologies from various vendors?
 - Implement a technology that gives you the security insight required?

People, Process and Technology Considerations



- Infrastructure – How do you:
 - Implement a redundant infrastructure to insure a continuity of operations?
 - Implement and test a DR/BCP plan?
 - Stage a data center environment that gives you the space to grow as your business grows?
- Intelligence – How do you:
 - Get information on the global threat landscape and not just threats that are impacting your environment?
 - Correlate the global intelligence data with in house security data to try to predict an attack?
- Governance – How do you:
 - Implement an auditable process to demonstrate consistency and accuracy of the monitoring program?
 - Implement a security program that doesn't impact business delivery?

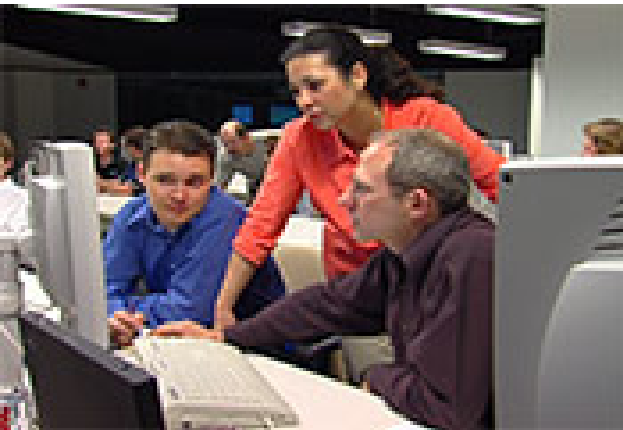


Confidence in a connected world.



SOC Options

Business Model Approaches



- Outsourced
 - Outsource to MSSP
 - Utilize MSSP staff and technology to minimize impact to existing operations
 - Utilize consulting to help transition to MSSP
- In-Sourced/Co-Sourced
 - Build your own
 - Utilize existing staff or use trained consultants to augment existing staff
 - Implement 3rd party SIM solution to generate events
 - Leverage MSSP to generate events and escalate them to an internal incident response team for analysis and remediation



Confidence in a connected world.



Outsourced

Outsourced SOC – Choosing a Partner



- Technical
 - Does the MSSP have the technical skills to do what is needed?
- Business
 - Does the company have the correct business relationships to maintain relevance for you?
- People/Process
 - Does the company have the correct resources and processes to execute on your needs?





Confidence in a connected world.



In-Sourced/Co-Sourced SOC

Co-Sourced SOC – Leveraging MSSP and Consulting



- Leverage expertise of MSSP
- Virtual SOC Extension
- Dedicated staff to
 - Prioritize incident response
 - Create custom reports
 - Extend support to additional capabilities
 - Vulnerability management
 - Patch management
 - AV
 - Email
 - Incident response
 - Deep analysis
 - Highly customize



In-Sourced SOC- Leveraging SIM Technology and Consulting



- Assess
 - Advisory Services to assess security operations requirements
- Design
 - Advisory Services to design security operations center
- Implement
 - Enablement services for installation of systems, custom software, 3rd party devices
- Manage
 - Residency Services to augment security staff



Confidence in a connected world.



Summary and Q&A