Building a Security Operations Center (SOC)

Ben Rothke, CISSP CISM

Wyndham Worldwide Corp.

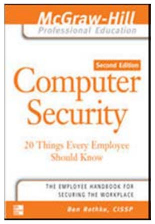
Session ID: TECH-203

Session Classification: Advanced

RSACONFERENCE2012

About me…

- Ben Rothke, CISSP, CISM, CISA
- Manager - Information Security - Wyndham Worldwide Corp.
  - All content in this presentation reflect my views exclusively and **not** that of Wyndham Worldwide
- Author - *Computer Security: 20 Things Every Employee Should Know* (McGraw-Hill)

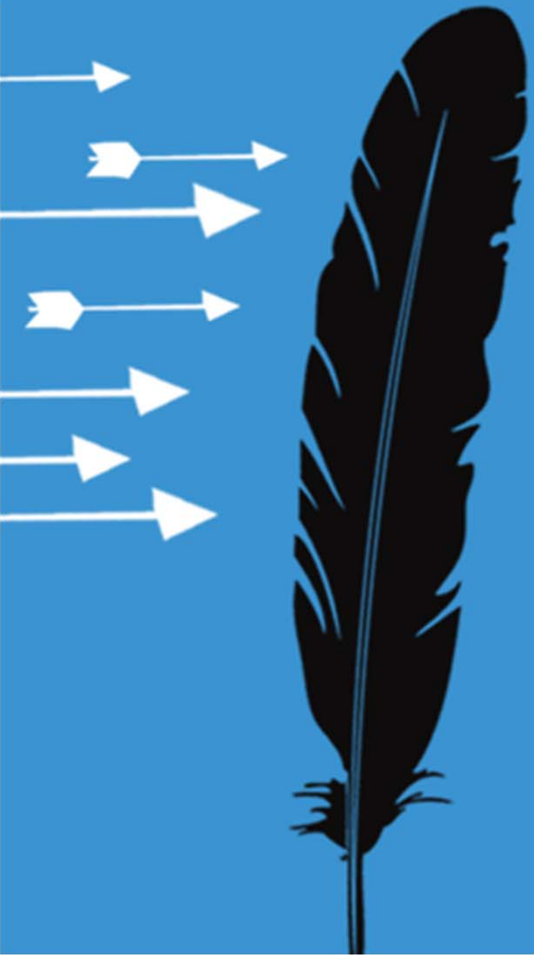


McGraw-Hill
Professional Education
Second Edition
Computer Security
20 Things Every Employee Should Know
THE EMPLOYEE HANDBOOK FOR SECURING THE WORKPLACE
Ben Rothke, CISSP

- Write the Security Reading Room blog
  - https://365.rsaconference.com/blogs/securityreading

Agenda

- Introduction
- Need for a Security Operations Center (SOC)
- Components of an effective SOC
- Deciding to insource or outsource the SOC
  - Outsourced SOC = MSSP
- SOC requirements
- Q/A



Building a Security Operations Center (SOC)

Current information security challenges

- Onslaught of security data from disparate systems, platforms and applications
- numerous point solutions (AV, firewalls, IDS/IPS, ERP, access control, IdM, SSO, etc.)
- millions / billions of messages daily
- attacks becoming more frequent / sophisticated
- regulatory compliance issues place increasing burden on systems and network administrators

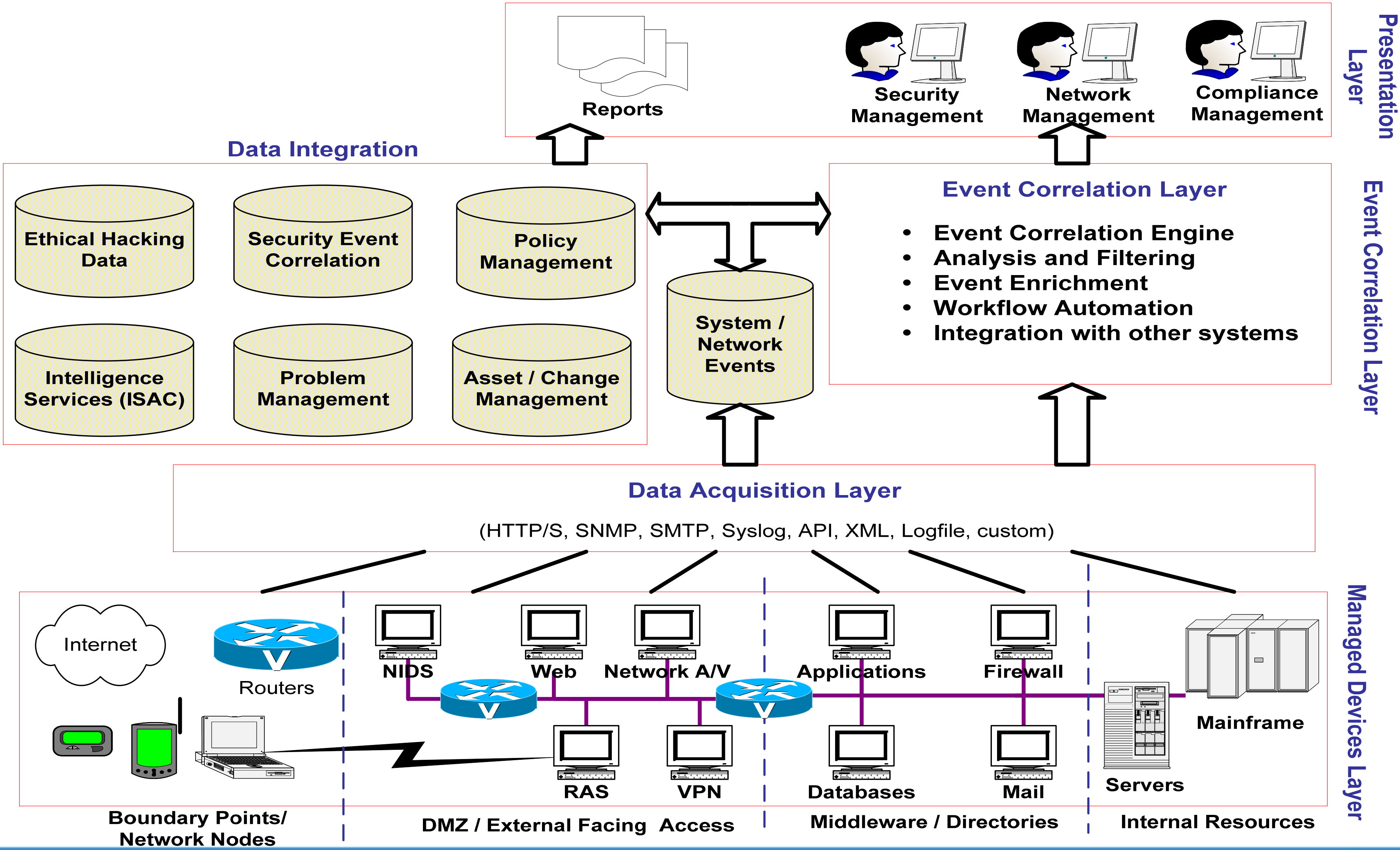
Why do you need a SOC?

- because a firewall and IDS are not enough
- nucleus of all information security operations
- provides
  - continuous prevention
  - protection
  - detection
  - response capabilities against threats, remotely exploitable vulnerabilities and real-time incidents on your networks
- works with CIRT to create comprehensive infrastructure for managing security operations

SOC benefits

- speed of response time
  - malware can spread throughout the Internet in minutes or even seconds, potentially knocking out your network or slowing traffic to a crawl
- consequently, every second counts in identifying these attacks and negating them before they can cause damage
- ability to recover from a DDoS attack in a reasonable amount of time

Integrated SOC



Presentation Layer

Reports

Security Management

Network Management

Compliance Management

Data Integration

Ethical Hacking Data

Security Event Correlation

Policy Management

Intelligence Services (ISAC)

Problem Management

Asset / Change Management

System / Network Events

Event Correlation Layer

- Event Correlation Engine
- Analysis and Filtering
- Event Enrichment
- Workflow Automation
- Integration with other systems

Data Acquisition Layer

(HTTP/S, SNMP, SMTP, Syslog, API, XML, Logfile, custom)

Managed Devices Layer

Boundary Points/ Network Nodes

DMZ / External Facing Access

Middleware / Directories

Internal Resources

SOC functions

- Real-time monitoring / management
  - aggregate logs
  - aggregate data
  - coordinate response and remediation
- Reporting
  - executives
  - auditors
  - security staff
- Post-incident analysis
  - forensics
  - investigation

SOC planning

- full audit of existing procedures, including informal and ad-hoc
- planning of location, resources, training programs, etc.
- plans change; don’t try to prepare everything ahead of time
  - sometimes best approach is not clear until you have actually started
  - build it like aircraft carrier - change built into design

SIM/SIEM/SEM tools

- Many SOC benefits come from good SIM tool
  - consolidates all data and analyzes it intelligently
  - provides visualization into environment

- Choose SIM that's flexible and agile, plus:
  - track and escalate according to threat level
  - priority determination
  - real-time correlation
  - cross-device correlation
  - audit and compliance

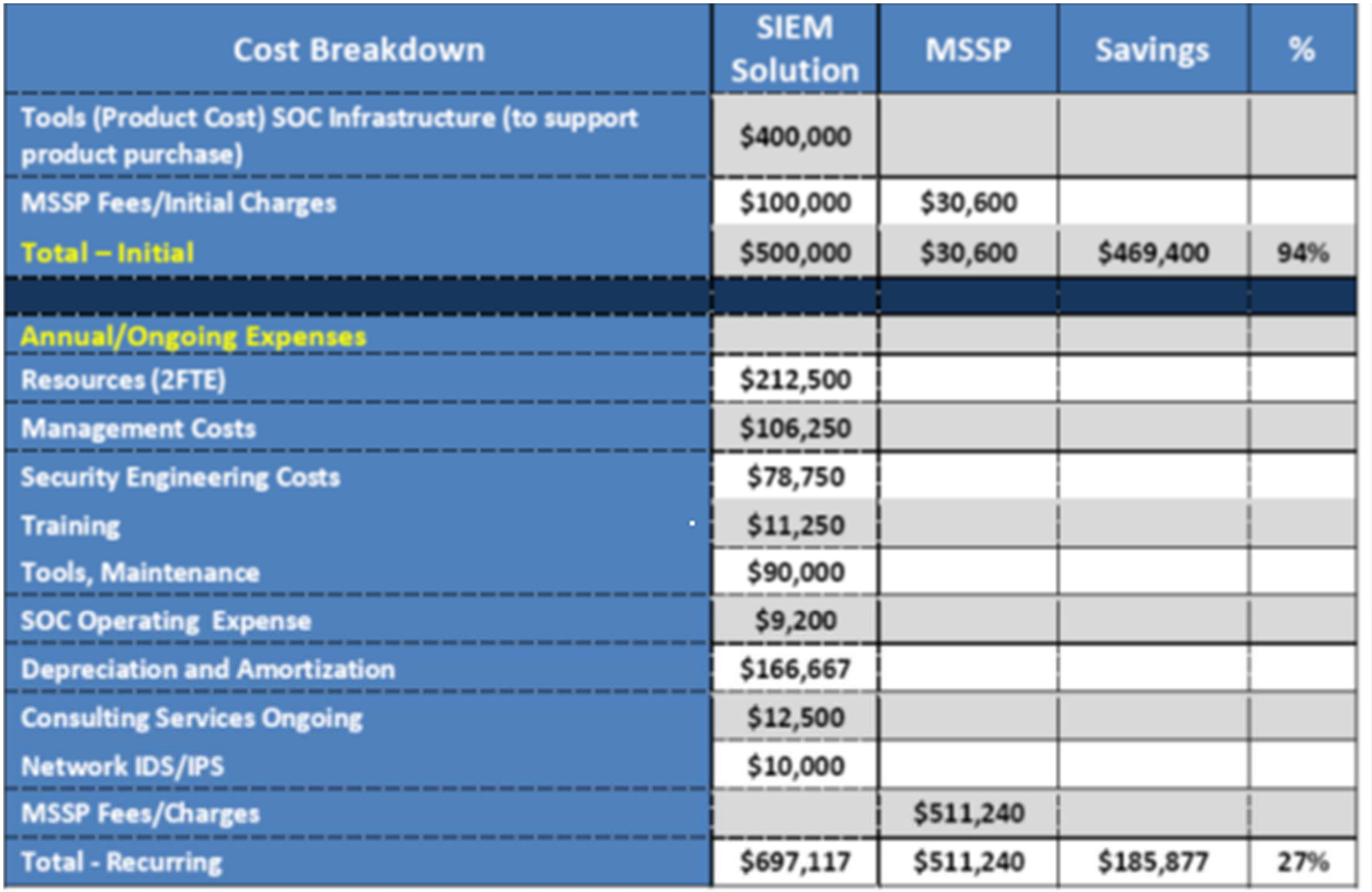
Challenge of SIM & automation

- A well-configured SIM can automate much of the SOC process. But…
- *“The more advanced a control system is, so the more crucial may be the contribution of the human operator”*
  - Ironies of Automation - Lisanne Bainbridge
    - discusses ways in which automation of industrial processes may expand rather than eliminate problems with the human operator
- don’t get caught in the hype that a SIM can replace good SOC analysts
  - no secret that they can’t

Which SOC?

- Outsourced
  - Symantec, SecureWorks (Dell), Solutionary, WiPro, Tata, CenturyLink (Savvis, Qwest), McAfee, Verizon (Cybertrust / Ubizen), Orange, Integralis, Sprint, EDS, AT&T, Unisys, VeriSign, BT Managed Security Solutions (Counterpane), NetCom Systems and more
- Centralized group within enterprise
  - Corporate SOC

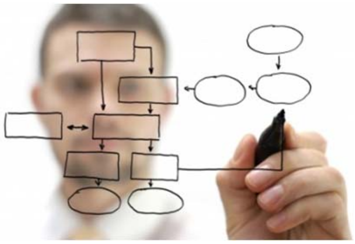
In-house SOC vs. outsourced MSSP



Cost Breakdown	SIEM Solution	MSSP	Savings	%
Tools (Product Cost) SOC Infrastructure (to support product purchase)	$400,000			
MSSP Fees/Initial Charges	$100,000	$30,600		
Total – Initial	$500,000	$30,600	$469,400	94%
Annual/Ongoing Expenses				
Resources (2FTE)	$212,500			
Management Costs	$106,250			
Security Engineering Costs	$78,750			
Training	$11,250			
Tools, Maintenance	$90,000			
SOC Operating Expense	$9,200			
Depreciation and Amortization	$166,667			
Consulting Services Ongoing	$12,500			
Network IDS/IPS	$10,000			
MSSP Fees/Charges		$511,240		
Total - Recurring	$697,117	$511,240	$185,877	27%

The Business Case for Managed Security Services Managed Security Services Providers vs. SIEM Product Solutions
http://www.solutionary.com/dms/solutionary/Files/whitepapers/MSSP_vs_SIEM.pdf

Define the SOC requirements



- define specific needs for the SOC within the organization
- what specific tasks will be assigned to the SOC?
    - detecting external attacks, compliance monitoring, checking for insider abuse, incident management, etc.
- who will use the data collected and analyzed by the SOC?
    - what are their requirements?
- who will own and manage the SOC?
- types of security events will be fed into the SOC

Internal SOC

Advantages	Disadvantages
▪ dedicated staff ▪ knows environment better than a third-party ▪ solutions are generally easier to customize ▪ potential to be most efficient ▪ most likely to notice correlations between internal groups ▪ logs stored locally	• larger up-front investment • higher pressure to show ROI quickly • higher potential for collusion between analyst and attacker • less likely to recognize large-scale, subtle patterns that include multiple groups • can be hard to find competent SOC analysts

Internal SOC - Questions

1. does your staff have the competencies (skills and knowledge) to manage a SOC?
2. how do you plan to assess if they really do have those competencies?
3. are you willing to take the time to document all of the SOC processes and procedures?
4. who's going to develop a training program?
5. who's going to design the physical SOC site?
6. can you hire and maintain adequate staff levels?

Internal SOC success factors

1. Trained staff
2. good SOC management
3. adequate budget
4. good processes
5. integration into incident response
    - If your organization can’t commit to these five factors, **do not** build an internal SOC – it will fail
        - will waste money and time and create false sense of security

- if you need a SOC but can’t commit to these factors, strongly consider outsourcing

Outsourced SOC

Advantages	Disadvantages
▪ avoid capital expenses – it’s their hardware & software ▪ exposure to multiple customers in similar industry segment ▪ often cheaper than in-house ▪ less potential for collusion between monitoring team and attacker ▪ good security people are difficult to find ▪ unbiased ▪ potential to be very scalable & flexible ▪ expertise in monitoring and SIM tools ▪ SLA	• contractors will never know your environment like internal employees • sending jobs outside the organization can lower morale • lack of dedicated staff to a single client • lack of capital retention • risk of external data mishandling • log data not always archived • log data stored off-premises • lack of customization • MSSP standardize services to gain economies of scale in providing security services to myriad clients

Outsourced SOC – general questions

1. **Can I see your operations manual?**
2. what is its reputation?
3. who are its customers?
4. does it already service customers in my industry?
5. does it service customers my size?
6. how long have its customers been with it?
7. what is its cancellation/non-renew rate?
8. how do they protect data and what is the level of security at their SOC?

Outsourced SOC – staffing questions

1. what is the experience of its staff?
2. does it hire reformed hackers?
3. are background checks performed on all new employees?
4. does it use contractors for any of its services?
5. are personnel held to strict confidentiality agreements?
6. what is the ratio of senior engineers to managed clients?
7. what certifications are held by senior/junior staff?
8. what is its employee turnover rate?

Outsourced SOC – stability questions

1. Is it stable?
2. does it have a viable business plan?
3. how long has it been in business?
4. positive signs of growth from major clients?
5. consistent large account wins / growing revenue?
6. what is its client turnover rate?
7. what are its revenue numbers?
   - If private and unwilling to share this information, ask for percentages rather than actual numbers
8. will it provide documentation on its internal security policies and procedures?

Outsourced SOC - sizing / costs

- should provide services for less than in-house solution
- can spread out investment in analysts, hardware, software, facilities over several clients
- how many systems will be monitored?
- how much bandwidth is needed?
- potential tax savings
  - Convert variable costs (in-house) to fixed costs (services)

Outsourced SOC – performance metrics

- must provide client with an interface providing detailed information
  - services being delivered
  - how their security posture relates to overall industry trends
- provide multiple views into the organization
- various technical, management and executive reports
- complete trouble ticket work logs and notes

Outsourced SOC – SLA's

- well-defined SLA's are critical
  - processes and time periods within which they will respond to any security need.
  - SLA should include specific steps to be taken
  - procedures the company takes to assure that the same system intrusions do not happen again
  - guarantee of protection against emerging threats
  - recovers losses in the event service doesn't deliver as promised
  - commitments for initial device deployment, incident response/protection, requests for security policy & configuration changes, acknowledgement of requests

Outsourced SOC - Transitioning

- ensure adequate knowledge transfer
- create formal service level performance metrics
  - establish a baseline for all negotiated service levels
  - measure from the baseline, track against it, adjusting as necessary.
- create internal CIRT
  - identify key events and plan the response
- hold regular transition & performance reviews
- be flexible
  - schedule formal review to adjust SLA's after 6 months of service operation and periodically thereafter

Outsourced SOC – Termination

- all outsourcing contracts must anticipate the eventual termination at the end of the contract
- plan for an orderly in-house transition or a transition to another provider
- develop an exit strategy
  - define key resources, assets and process requirements for continued, effective delivery of the services formerly provided by the outgoing provider

Outsourcing: don’t just trust - verify

- Call Saturday night 2AM
  - Who’s answering? Do they sound competent?
- Reports
  - Are they to your liking? Can they create complex reports?
- Set off a few alarms
  - Are they calling/alerting you in a timely manner?
- True process for real-time threat analysis?
  - Or simply a glorified reporting portal that looks impressive

Mike Rothman on MSSP

- We have no illusions about the amount of effort required to get a security management platform up and running, or what it takes to keep one current and useful.
- Many organizations have neither the time nor the resources to implement technology to help automate some of these key functions.
- So they are trapped on the hamster wheel of pain, reacting without sufficient visibility, but without time to invest in gaining that much-needed visibility into threats without diving deep into raw log files.
- A suboptimal situation for sure, and one that usually triggers discussions of managed services in the first place.

http://securosis.com/blog/managed-services-in-a-security-management-2.0-world November 2011

SOC analysts

- Good SOC analysts hard to find, hard to keep
  - Have combination of technical knowledge and technical aptitude
- hire experienced SOC analysts
  - pay them well
  - you get what you pay for

SOC analyst – skill sets

- O/S proficiency
- network protocols
- chain of custody issues
- ethics
- corporate policy
- services
- multiple hardware platforms
- attacks
- directories
- routers/switches/firewall
- programming
- forensics
- databases
- IDS
- investigative processes
- applications
- and much more

SOC analyst - qualities

- extremely curious
  - ability to find answers to difficult problems / situations
- abstract thinker
  - can correlate IDS incidents and alerts in real-time
- ethical
- deals with low-level details while keeping big-picture view of situation
- can communicate to various groups that have very different requirements
- responds well to frustrating situations

SOC analyst burnout

- SOC analysts can burnout
- have a plan to address this
  - extensive training
  - bonuses
  - promotions
  - management opportunities
  - job rotation

SOC management

- management and supervision of a SOC is a key factor to ensure its efficiency
- while analysts, other staff, hardware and software are key elements, a SOC's ultimate success is dependent on a competent SOC manager.
- inadequate/poor management has significant consequences
  - from process performance decrements, to incidents being missed or incorrectly handled

SOC processes and procedures

- SOC heavily process-driven
- processes work best when documented in advance
- usability and workflow critical
- documentation
  - adequate time must be given to properly document many different SOC functions
  - corporate networks and SOC are far too complex to be supported in an ad-hoc manner
  - documentation makes all the difference

Sample SOC runbook table of contents

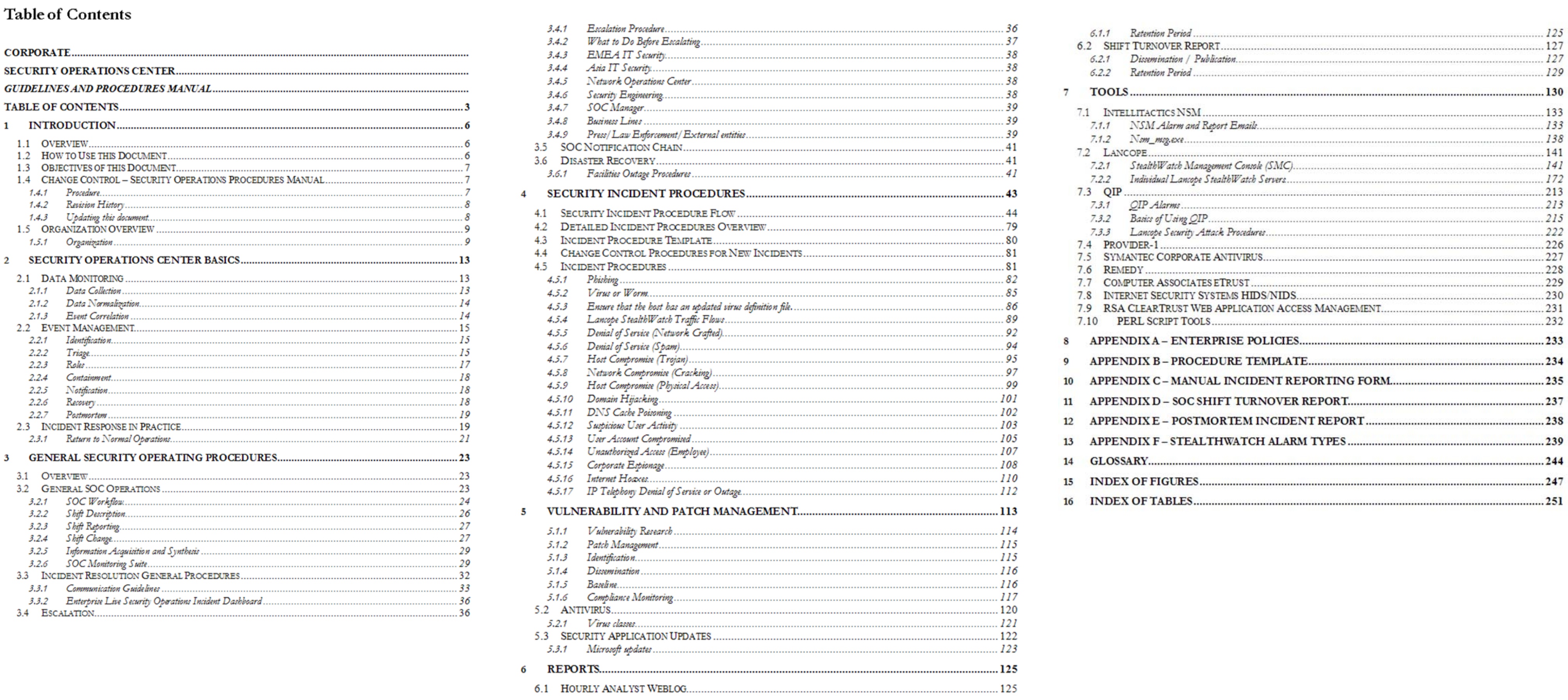
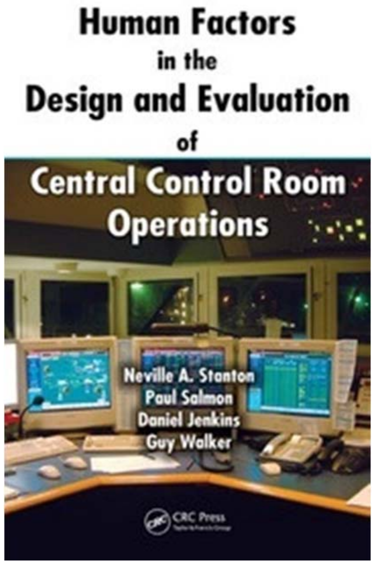


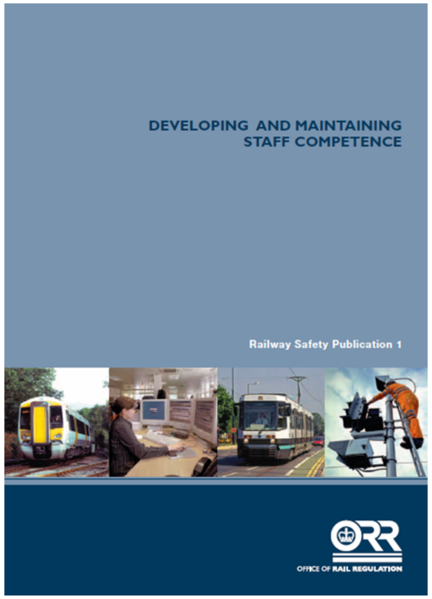
Table of Contents

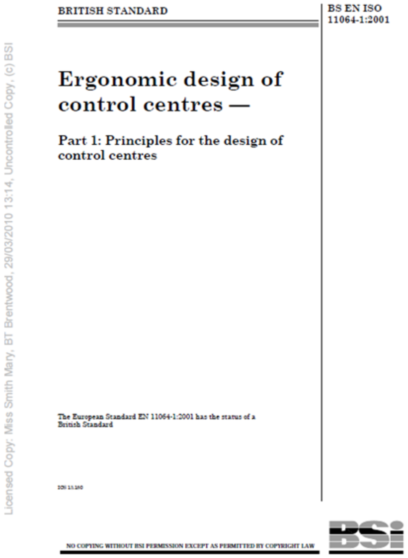
SOC metrics

- measured by how quickly incidents are:
  - identified
  - addressed
  - handled
- must be used judiciously
- don’t measure base performance of an analyst simply on the number of events analyzed or recommendations written

Additional references




DEVELOPING AND MAINTAINING
STAFF COMPETENCE
Railway Safety Publication 1
ORR
OFFICE OF RAIL REGULATION



BRITISH STANDARD

BS EN ISO
11064-1:2001

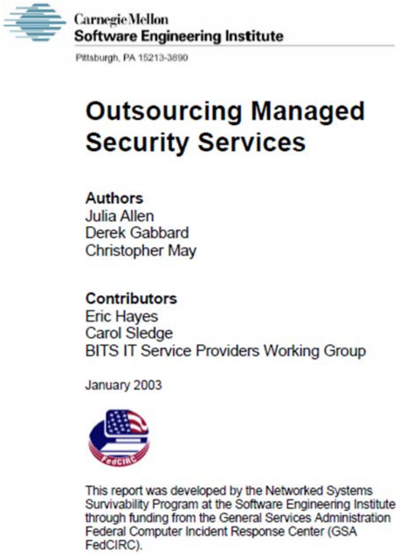
Ergonomic design of control centres —

Part 1: Principles for the design of control centres

The European Standard EN 11064-1:2001 has the status of a British Standard

ICS 13.180

BSI


Carnegie Mellon
Software Engineering Institute
Pittsburgh, PA 15213-3890

Outsourcing Managed Security Services

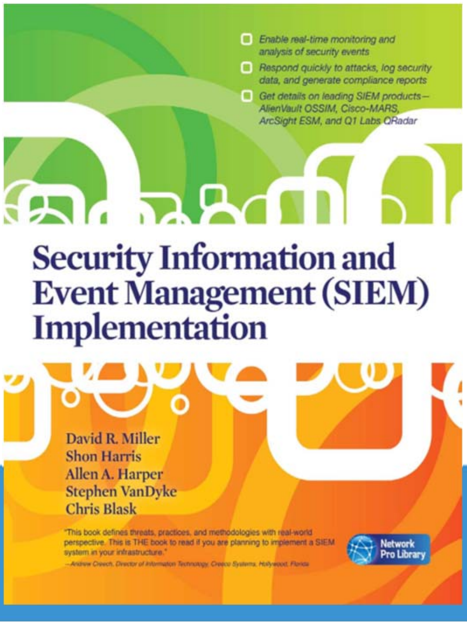
Authors
Julia Allen
Derek Gabbard
Christopher May

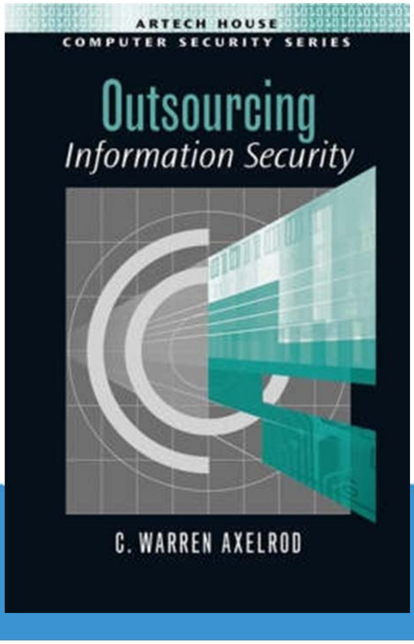
Contributors
Eric Hayes
Carol Sledge
BITS IT Service Providers Working Group

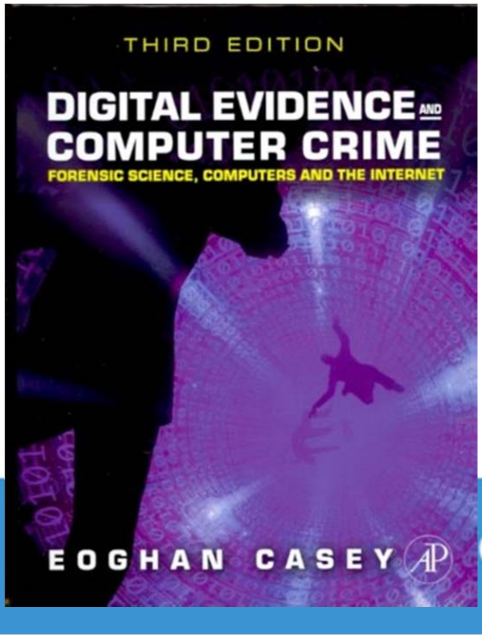
January 2003

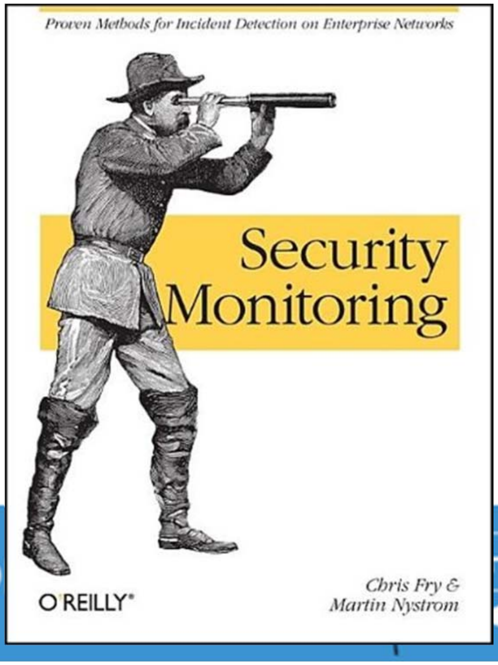
FedCIRC

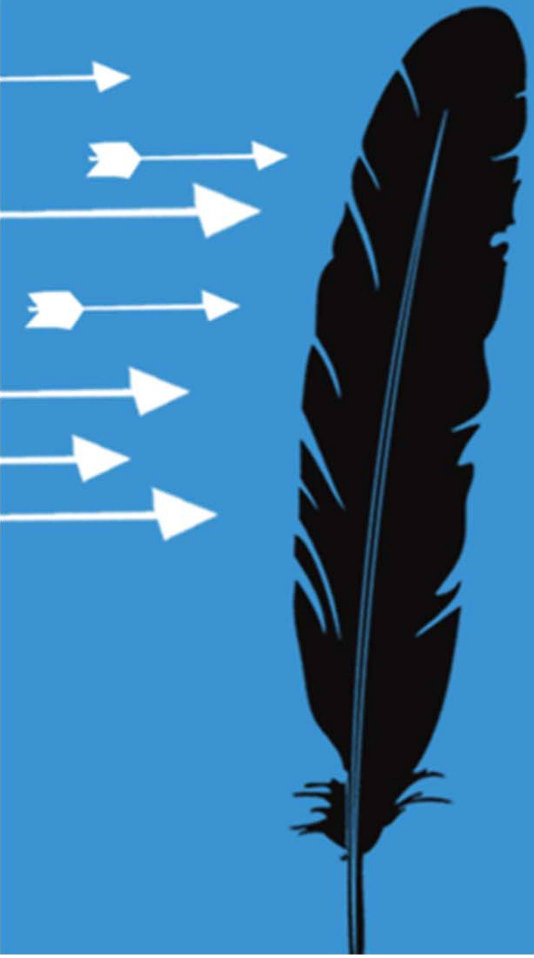
This report was developed by the Networked Systems Survivability Program at the Software Engineering Institute through funding from the General Services Administration Federal Computer Incident Response Center (GSA FedCIRC).


Enable real-time monitoring and analysis of security events
Respond quickly to attacks, log security data, and generate compliance reports
Get details on leading SIEM products—AlienVault OSSIM, Cisco-MARS, ArcSight ESM, and Q1 Labs QRadar
Security Information and Event Management (SIEM) Implementation
David R. Miller
Shon Harris
Allen A. Harper
Stephen VanDyke
Chris Blask
"This book defines threats, practices, and methodologies with real-world perspective. This is THE book to read if you are planning to implement a SIEM system in your infrastructure."
—Andrew Creech, Director of Information Technology, Crescent Systems, Hollywood, Florida
Network Pro Library






Proven Methods for Incident Detection on Enterprise Networks
Security
Monitoring
O'REILLY
Chris Fry &
Martin Nystrom



Apply

Apply

- obtain management commitment to a SOC
  - ensuring adequate staffing and budget
- define your SOC requirements
- decide to have SOC in-house or outsourced
  - *in-house* – create detailed and customized processes
  - *outsourced* – ensure their process meets your requirements
- create process to ensure SOC is effective and providing security benefits to the firm

Ben Rothke, CISSP CISM
Manager – Information Security
Wyndham Worldwide Corporation

www.linkedin.com/in/benrothke
www.twitter.com/benrothke
www.slideshare.net/benrothke