

HCCA's 12TH ANNUAL COMPLIANCE INSTITUTE

APRIL 13-16, 2008 | NEW ORLEANS, LA | HILTON RIVERSIDE NEW ORLEANS

Sustaining Security Operations

John Curin,
Senior Managing Consultant
Burwood Group, Inc.



www.hcca-info.org | 888-580-8373



Information Security Overview

Information Security

Strategic prioritization of goals, and definition of objectives

Effective technology adoption

Optimized Security operations to support company's mission

Strategy & Architecture

- Guiding principles, operational strategy
- Risk prioritization and remediation planning
- Road-map definition
- Architectural design process

Technology Integration

- Security infrastructure integration
- Implementation & tuning of tools
- Network controls
- Implementation of monitoring systems
- Technical expertise

Operations

- Support, monitoring, & response processes
- Security monitoring and management
- Continued audit and compliance processes
- Vulnerability and infrastructure assessment



www.hcca-info.org | 888-580-8373

2

Starting with Policy

- Define Guiding Principles
 - Regulatory guides
 - Standards based guides
- Define Control Objectives and Assets
 - What do we have?
 - What are we protecting?
- Develop Policy
 - Define 'acceptable use'
 - Mandate procedure inline with guiding principles
- User Training
 - New Employee Orientation
 - Cyclical Training and Education
 - Awareness Program
- Design an Operations Framework to Manage Security
 - Security Event Management
 - Incident Response
 - Audit Trail



www.hcca-info.org | 888-580-8373

3

Developing the Operational Framework

- Who defines the security budget?
- Who executes the security budget?
- Who owns implementation/integration?
- How is the analyst role fulfilled?
- Who quantifies 'risk' within the organization? Outside the organization?
- Who owns event management and monitoring?
- How is incident response initiated and escalated?



www.hcca-info.org | 888-580-8373

4

Security Operations – Event Management



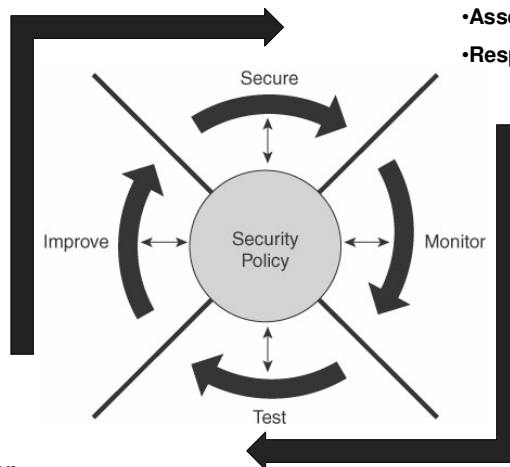
www.hcca-info.org | 888-580-8373

5

Securing the Network

Strategy:

- Architecture
- Engineering
- Implementation



Operations:

- Monitoring
- Assessment
- Response



www.hcca-info.org | 888-580-8373

6

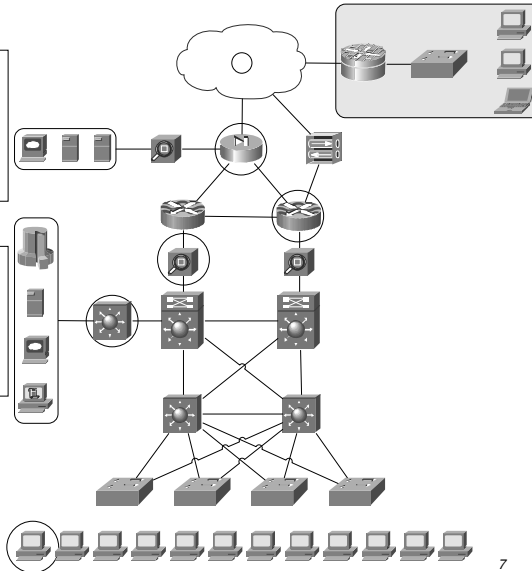
Typical Security Monitoring

Most Environments:

- Firewall
- IDS / IPS
- VPN Concentrators
- Host based (AV, HIPS, agents)

Example:

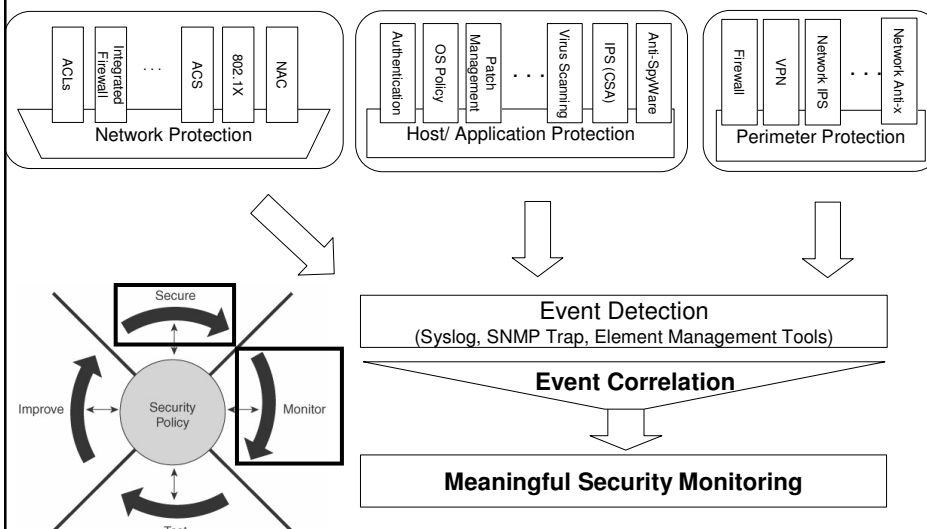
- Firewall log
- IPS log
- Host based solutions, mgmt consoles, native log formats



www.hcca-info.org | 888-580-8373

7

Event Management



www.hcca-info.org | 888-580-8373

8

8

The Dashboard – 24 Hour Summary

Page Refresh Rate
15 minutes

24 Hour Events

Netflow	760,538
Events	859,976
Sessions	798,097
Data Reduction	7%

24 Hour Incidents

High	9	2%
Medium	151	47%
Low	158	49%
Total	318	100%

All False Positives

To be confirmed	504	0%
System determined	847	0%
Logged	2,997,183	99%
Dropped	0	0%
User confirmed	3,822	0%
Total	3,002,356	100%

To-do List

- C:173021 (Assigned) Large spike in LCS L...
- C:144172 (New) Sami Traffic Spike o...
- C:129486 (Assigned) Pix Route Lookup Fai...

Determines how frequently page updates.

Discrete flows received from network devices
Number of discrete *events* received
Number of *sessions* created from *events*

```

graph TD
    A[Receive events  
(SNMP, syslog, etc)] --> B[Correlate events into sessions]
    B --> C[Compare session to rules]
    C --> D[Create an Incident]
    
```

HCCA
HEALTH CARE
COMPLIANCE
ASSOCIATION

www.hcca-info.org | 888-580-8373

9

Security Operations – Assessment and Audit

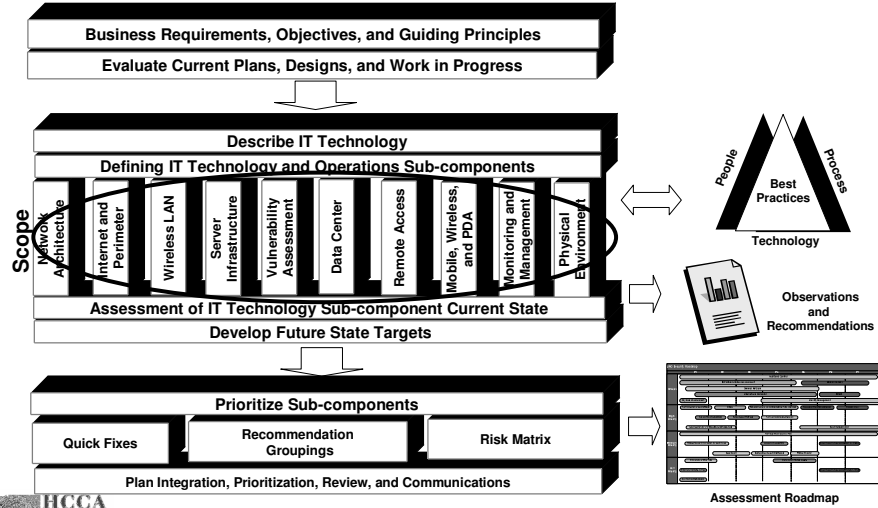
HCCA
HEALTH CARE
COMPLIANCE
ASSOCIATION

www.hcca-info.org | 888-580-8373

10

Assessment and Audit Approach

Assessment Phase Transitioning through to Strategy:



www.hcca-info.org | 888-580-8373

Risk Matrix: Business Risk

Higher Business Risk	28 observations	16 observations
Lower Business Risk	14 observations	8 observations
	Lower Probability of Occurrence	Higher Probability of Occurrence



www.hcca-info.org | 888-580-8373

Transitioning into Strategy: Example Security Assessment Mitigation Roadmap

