



SECURITY

Security Operations Center

Building, Operating, and Maintaining Your SOC

Security Operations Center

Joseph Muniz

Gary McIntyre

Nadhem AlFardan

Cisco Press

800 East 96th Street

Indianapolis, Indiana 46240 USA

Security Operations Center: Building, Operating, and Maintaining your SOC

Table of Contents

Contents

Introduction

Part I: SOC Basics

Chapter 1 Introduction to Security Operations and the SOC

- Cybersecurity Challenges

- Threat Landscape

- Business Challenges

 - The Cloud

 - Compliance

 - Privacy and Data Protection

- Introduction to Information Assurance

- Introduction to Risk Management

- Information Security Incident Response

 - Incident Detection

 - Incident Triage

 - Incident Categories

 - Incident Severity

 - Incident Resolution

 - Incident Closure

 - Post-Incident

- SOC Generations

 - First-Generation SOC

 - Second-Generation SOC

 - Third-Generation SOC

 - Fourth-Generation SOC

Table of Contents

Characteristics of an Effective SOC

Introduction to Maturity Models

Applying Maturity Models to SOC

Phases of Building a SOC

Challenges and Obstacles

Summary

References

Chapter 2 Overview of SOC Technologies

Data Collection and Analysis

Data Sources

Data Collection

The Syslog Protocol

Telemetry Data: Network Flows

Telemetry Data: Packet Capture

Parsing and Normalization

Security Analysis

Alternatives to Rule-Based Correlation

Data Enrichment

Big Data Platforms for Security

Vulnerability Management

Vulnerability Announcements

Threat Intelligence

Compliance

Ticketing and Case Management

Collaboration

SOC Conceptual Architecture

Summary

References

Part II: The Plan Phase

Chapter 3 Assessing Security Operations Capabilities

Table of Contents

Assessment Methodology

Step 1: Identify Business and IT Goals

Step 2: Assessing Capabilities

Assessing IT Processes

Step 3: Collect Information

Step 4: Analyze Maturity Levels

Step 5: Formalize Findings

The Organizations Vision and Strategy

The Departments Vision and Strategy

External and Internal Compliance Requirements

Organizations Threat Landscape

History of Previous Information Security Incidents

SOC Sponsorship

Allocated Budget

Presenting Data

Closing

Summary

References

Chapter 4 SOC Strategy

Strategy Elements

Who Is Involved?

SOC Mission

SOC Scope

Example 1: A Military Organization

Mission Statement

SOC Scope Statement

Example 2: A Financial Organization

Mission Statement

SOC Scope Statement

SOC Model of Operation

In-House and Virtual SOC

SOC Services

SOC Capabilities Roadmap

Table of Contents

Summary

Part III: The Design Phase

Chapter 5 The SOC Infrastructure

Design Considerations

Model of Operation

Facilities

SOC Internal Layout

Lighting

Acoustics

Physical Security

Video Wall

SOC Analyst Services

Active Infrastructure

Network

Access to Systems

Security

Compute

Dedicated Versus Virtualized Environment

Choice of Operating Systems

Storage

Capacity Planning

Collaboration

Ticketing

Summary

References

Chapter 6 Security Event Generation and Collection

Data Collection

Calculating EPS

Ubuntu Syslog Server

Network Time Protocol

Deploying NTP

Data-Collection Tools

Table of Contents

Company

Product Options and Architecture

Installation and Maintenance

User Interface and Experience

Compliance Requirements

Firewalls

Stateless/Stateful Firewalls

Cisco Adaptive Security Appliance ASA

Application Firewalls

Cisco FirePOWER Services

Cloud Security

Cisco Meraki

Exporting Logs from Meraki

Virtual Firewalls

Cisco Virtual Firewalls

Host Firewalls

Intrusion Detection and Prevention Systems

Cisco FirePOWER IPS

Meraki IPS

Snort

Host-Based Intrusion Prevention

Routers and Switches

Host Systems

Mobile Devices

Breach Detection

Cisco Advanced Malware Prevention

Web Proxies

Cisco Web Security Appliance

Cloud Proxies

Cisco Cloud Web Security

DNS Servers

Exporting DNS

Network Telemetry with Network Flow Monitoring

Table of Contents

NetFlow Tools

StealthWatch

Exporting Data from StealthWatch

NetFlow from Routers and Switches

NetFlow from Security Products

NetFlow in the Data Center

Summary

References

Chapter 7 Vulnerability Management

Identifying Vulnerabilities

Security Services

Vulnerability Tools

Handling Vulnerabilities

OWASP Risk Rating Methodology

Threat Agent Factors

Vulnerability Factors

Technical Impact Factors

Business Impact Factors

The Vulnerability Management Lifecycle

Automating Vulnerability Management

Inventory Assessment Tools

Information Management Tools

Risk-Assessment Tools

Vulnerability-Assessment Tools

Report and Remediate Tools

Responding Tools

Threat Intelligence

Attack Signatures

Threat Feeds

Other Threat Intelligence Sources

Summary

References

Table of Contents

Chapter 8 People and Processes

Key Challenges

Wanted: Rock Stars, Leaders, and Grunts

The Weight of Process

The Upper and Lower Bounds of Technology

Designing and Building the SOC Team

Starting with the Mission

Focusing on Services

Security Monitoring Service Example

Determining the Required SOC Roles

Leadership Roles

Analyst Roles

Engineering Roles

Operations Roles

Other Support Roles

Working with HR

Job Role Analysis

Market Analysis

Organizational Structure

Calculating Team Numbers

Deciding on Your Resourcing Strategy

Building Your Own: The Art of Recruiting SOC Personnel

Working with Contractors and Service Bureaus

Working with Outsourcing and Managed Service Providers

Working with Processes and Procedures

Processes Versus Procedures

Working with Enterprise Service Management Processes

Event Management

Incident Management

Problem Management

Vulnerability Management

Other IT Management Processes

The Positives and Perils of Process

Table of Contents

Examples of SOC Processes and Procedures

Security Service Management

Security Service Engineering

Security Service Operations

Security Monitoring

Security Incident Investigation and Response

Security Log Management

Security Vulnerability Management

Security Intelligence

Security Analytics and Reporting

Breach Discovery and Remediation

Summary

Part IV: The Build Phase

Chapter 9 The Technology

In-House Versus Virtual SOC

Network

Segmentation

VPN

High Availability

Support Contracts

Security

Network Access Control

Authentication

On-Network Security

Encryption

Systems

Operating Systems

Hardening Endpoints

Endpoint Breach Detection

Mobile Devices

Servers

Storage

Table of Contents

Data-Loss Protection

Cloud Storage

Collaboration

Collaboration for Pandemic Events

Technologies to Consider During SOC Design

Firewalls

Firewall Modes

Firewall Clustering

Firewall High Availability

Firewall Architecture

Routers and Switches

Securing Network Devices

Hardening Network Devices

Network Access Control

Deploying NAC

NAC Posture

Architecting NAC

Web Proxies

Reputation Security

Proxy Architecture

Intrusion Detection/Prevention

IDS IPS Architecture

Evaluating IDS IPS Technology

Tuning IDS/IPS

Breach Detection

Honeypots

Sandboxes

Endpoint Breach Detection

Network Telemetry

Enabling NetFlow

Architecting Network Telemetry Solutions

Network Forensics

Digital Forensics Tools

Table of Contents

Final SOC Architecture

Summary

References

Chapter 10 Preparing to Operate

Key Challenges

People Challenges

Process Challenges

Technology Challenges

Managing Challenges Through a Well-Managed Transition

Elements of an Effective Service Transition Plan

Determining Success Criteria and Managing to Success

Deploying Against Attainable Service Levels

Focusing on Defined Use Cases

Managing Project Resources Effectively

Marching to Clear and Attainable Requirements

Staffing Requirements for Go-Live

Process Requirements for Go-Live

Technology Requirements for Go-Live

Using Simple Checks to Verify That the SOC Is Ready

People Checks

Process Checks

Technology Checks

Summary

Part V: The Operate Phase

Chapter 11 Reacting to Events and Incidents

A Word About Events

Event Intake, Enrichment, Monitoring, and Handling

Events in the SIEM

Events in the Security Log Management Solution

Events in Their Original Habitats

Events Through Communications and Collaboration Platforms

Table of Contents

Working with Events: The Malware Scenario

Handling and Investigating the Incident Report

Creating and Managing Cases

Working as a Team

Working with Other Parts of the Organization

Working with Third Parties

Closing and Reporting on the Case

Summary

Chapter 12 Maintain, Review, and Improve

Reviewing and Assessing the SOC

Determining Scope

Examining the Services

Personnel/Staffing

Processes, Procedures, and Other Operational Documentation

Technology

Scheduled and Ad Hoc Reviews

Internal Versus External Assessments

Internal Assessments

External Assessments

Assessment Methodologies

Maturity Model Approaches

Services-Oriented Approaches

Post-Incident Reviews

Maintaining and Improving the SOC

Maintaining and Improving Services

Maintain and Improving Your Team

Improving Staff Recruitment

Improving Team Training and Development

Improving Team Retention

Maintaining and Improving the SOC Technology Stack

Improving Threat, Anomaly, and Breach-Detection Systems

Improving Case and Investigation Management Systems

Improving Analytics and Reporting

Table of Contents

Improving Technology Integration

Improving Security Testing and Simulation Systems

Improving Automated Remediation

Conclusions

Index