



**SECURITY**

# Security Operations Center

Building, Operating, and Maintaining Your SOC

[ciscopress.com](http://ciscopress.com)

Joseph Muniz  
Gary McIntyre

Nadhem AlFardan, CCIE No. 20519

**FREE SAMPLE CHAPTER**



SHARE WITH OTHERS

# Security Operations Center

---

Joseph Muniz

Gary McIntyre

Nadhem AlFardan

**Cisco Press**

800 East 96th Street

Indianapolis, Indiana 46240 USA

## **Security Operations Center**

Joseph Muniz, Gary McIntyre, Nadhem AlFardan

Copyright© 2016 Cisco Systems, Inc.

Published by:

Cisco Press

800 East 96th Street

Indianapolis, IN 46240 USA

All rights reserved. No part of this book may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or by any information storage and retrieval system, without written permission from the publisher, except for the inclusion of brief quotations in a review.

Printed in the United States of America

First Printing November 2015

Library of Congress Control Number: 2015950793

ISBN-13: 978-0-13-405201-4

ISBN-10: 0-13-405201-3

## **Warning and Disclaimer**

This book is designed to provide information about building and running a security operations center (SOC). Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied.

The information is provided on an “as is” basis. The authors, Cisco Press, and Cisco Systems, Inc. shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book or from the use of the discs or programs that may accompany it.

The opinions expressed in this book belong to the author and are not necessarily those of Cisco Systems, Inc.

## **Trademark Acknowledgments**

All terms mentioned in this book that are known to be trademarks or service marks have been appropriately capitalized. Cisco Press or Cisco Systems, Inc., cannot attest to the accuracy of this information. Use of a term in this book should not be regarded as affecting the validity of any trademark or service mark.

## **Special Sales**

For information about buying this title in bulk quantities, or for special sales opportunities (which may include electronic versions; custom cover designs; and content particular to your business, training goals, marketing focus, or branding interests), please contact our corporate sales department at [corpsales@pearsoned.com](mailto:corpsales@pearsoned.com) or (800) 382-3419.

For government sales inquiries, please contact [governmentsales@pearsoned.com](mailto:governmentsales@pearsoned.com).

For questions about sales outside the U.S., please contact [international@pearsoned.com](mailto:international@pearsoned.com).

## Feedback Information

At Cisco Press, our goal is to create in-depth technical books of the highest quality and value. Each book is crafted with care and precision, undergoing rigorous development that involves the unique expertise of members from the professional technical community.

Readers' feedback is a natural continuation of this process. If you have any comments regarding how we could improve the quality of this book, or otherwise alter it to better suit your needs, you can contact us through email at [feedback@ciscopress.com](mailto:feedback@ciscopress.com). Please make sure to include the book title and ISBN in your message.

We greatly appreciate your assistance.

**Publisher:** Paul Boger

**Associate Publisher:** Dave Dusthimer

**Business Operation Manager, Cisco Press:** Jan Cornelssen

**Acquisitions Editor:** Denise Lincoln

**Managing Editor:** Sandra Schroeder

**Senior Development Editor:** Christopher Cleveland

**Senior Project Editor:** Tonya Simpson

**Copy Editor:** Keith Cline

**Technical Editors:** Dr. Fred Mpala, Matthew Waters

**Editorial Assistant:** Vanessa Evans

**Cover Designer:** Mark Shirar

**Composition:** codeMantra

**Indexer:** WordWise Publishing Services

**Proofreader:** Sarah Kearns




**Americas Headquarters**  
Cisco Systems, Inc.  
San Jose, CA

**Asia Pacific Headquarters**  
Cisco Systems (USA) Pte. Ltd.  
Singapore

**Europe Headquarters**  
Cisco Systems International BV  
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).

 CCDE, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0812R)

## About the Authors

**Joseph Muniz** is a consultant at Cisco Systems and security researcher. Joseph started his career in software development and later managed networks as a contracted technical resource. Joseph moved into consulting and found a passion for security while meeting with a variety of customers. He has been involved with the design and implementation of multiple projects, ranging from Fortune 500 corporations to large federal networks. Joseph is the author of and contributor to several books and is a speaker for popular security conferences. Check out his blog, <http://www.thesecurityblogger.com>, which showcases the latest security events, research, and technologies.

**Gary McIntyre** is a seasoned information security professional focusing on the development and operation of large-scale information security programs. As an architect, manager, and consultant, he has worked with a wide range of public and private sector organizations around the world to design, build, and maintain small to large security operations teams. He currently holds a Masters degree from the University of Toronto and has also been a long-time (ISC)<sup>2</sup> instructor.

**Dr. Nadhem AlFardan** has more than 15 years of experience in the area of information security and holds a Ph.D. in Information Security from Royal Holloway, University of London. Nadhem is a senior security solution architect working for Cisco Systems. Before joining Cisco, he worked for Schlumberger and HSBC. Nadhem is CISSP certified and is an ISO 27001 lead auditor. He is also CCIE Security certified. In his Ph.D. research, Nadhem published a number of papers in prestige conferences, such as IEEE S&P and USENIX Security, mainly around cryptoanalysis topics. His work involved him working with organizations such as Google, Microsoft, Cisco, Mozilla, OpenSSL, and many others, mainly to help them assess and fix major findings in the Transport Layer Security/Secure Sockets Layer (TLS/SSL) protocol. His work is referenced in a number of IETF standards.

## About the Technical Reviewers

**Dr. Fred Mpala** is a security professional with broad experience in security and risk management.

**Matthew Waters** is a seasoned security professional and chief information security officer within the financial sector, specializing in large-scale transformation programs.

## Dedications

**Joseph Muniz:** I would like to give a huge “thank you” to my friends and family for supporting me for this and my other crazy projects. This book goes out to Irene Muniz, Ray Muniz, Alex Muniz, Raylin Muniz, Ning Xu, my friends at Cisco, and the many other great people in my life.

**Gary McIntyre:** For Candice and Winston, who paid the highest price to see this through.

## Acknowledgments

**Joseph Muniz:** I will start by thanking Gary McIntyre and Nadhem AlFardan for including me on this project. I really enjoyed collaborating on the material and hope that they do not mind my input. If they do, it is probably too late by now anyway.

I had help with validating my content and would like to recognize Jeff Williams and Aamir Lakhani. Jeff is the NetFlow ninja and assisted with reviewing my Lancopé contributions. Aamir is my good friend and co-authored two books with me prior to this project. I let Aamir beat up all my drafts and appreciate both his and Jeff's time on this project.

I also want to thank Jamey Heary for helping me line up this opportunity. Jamey is a brilliant engineer and the author of *Cisco ISE for BYOD and Secure Unified Access* (Cisco Press, 2013). I would not have been involved with this project without him.

Finally, I would like to thank Denise Lincoln and the rest of the Cisco Press team for their support while we determined and then polished the final content for this book. They are a very professional group and a pleasure to work with.

**Gary McIntyre:** As with any book like this, it's hard to acknowledge everyone who might deserve it. Thankfully, a book about security encourages a bit of obfuscation, silence, and mystery.

To Dean T., who first taught me about correlations using Cheap Trick and Queen. For Bev T., for never being boring. For Leslie C., for teaching me not to bore others. For Beth, who could not stay to see this. For my parents, who likely still don't understand what I do for a living and love me anyway. Finally, for all the customers, colleagues, and students I've had over my career: your fingerprints are all over this thing. Thank you.



## Contents at a Glance

Introduction xx

### **Part I: SOC Basics**

Chapter 1 Introduction to Security Operations and the SOC 1

Chapter 2 Overview of SOC Technologies 35

### **Part II: The Plan Phase**

Chapter 3 Assessing Security Operations Capabilities 69

Chapter 4 SOC Strategy 91

### **Part III: The Design Phase**

Chapter 5 The SOC Infrastructure 103

Chapter 6 Security Event Generation and Collection 123

Chapter 7 Vulnerability Management 189

Chapter 8 People and Processes 215

### **Part IV: The Build Phase**

Chapter 9 The Technology 245

Chapter 10 Preparing to Operate 319

### **Part V: The Operate Phase**

Chapter 11 Reacting to Events and Incidents 347

Chapter 12 Maintain, Review, and Improve 365

Index 397

# Contents

Introduction xx

## Part I SOC Basics

### Chapter 1 Introduction to Security Operations and the SOC 1

Cybersecurity Challenges	1
Threat Landscape	4
Business Challenges	7
<i>The Cloud</i>	8
<i>Compliance</i>	9
<i>Privacy and Data Protection</i>	9
Introduction to Information Assurance	10
Introduction to Risk Management	11
Information Security Incident Response	14
Incident Detection	15
Incident Triage	16
<i>Incident Categories</i>	17
<i>Incident Severity</i>	17
Incident Resolution	18
Incident Closure	19
Post-Incident	20
SOC Generations	21
First-Generation SOC	22
Second-Generation SOC	22
Third-Generation SOC	23
Fourth-Generation SOC	24
Characteristics of an Effective SOC	24
Introduction to Maturity Models	27
Applying Maturity Models to SOC	29
Phases of Building a SOC	31
Challenges and Obstacles	32
Summary	32
References	33

### Chapter 2 Overview of SOC Technologies 35

Data Collection and Analysis	35
Data Sources	37

Data Collection	38
<i>The Syslog Protocol</i>	39
<i>Telemetry Data: Network Flows</i>	45
<i>Telemetry Data: Packet Capture</i>	48
Parsing and Normalization	49
Security Analysis	52
<i>Alternatives to Rule-Based Correlation</i>	55
<i>Data Enrichment</i>	56
<i>Big Data Platforms for Security</i>	57
Vulnerability Management	58
Vulnerability Announcements	60
Threat Intelligence	62
Compliance	64
Ticketing and Case Management	64
Collaboration	65
SOC Conceptual Architecture	66
Summary	67
References	67

## **Part II: The Plan Phase**

### **Chapter 3 Assessing Security Operations Capabilities 69**

Assessment Methodology	69
Step 1: Identify Business and IT Goals	71
Step 2: Assessing Capabilities	73
<i>Assessing IT Processes</i>	75
Step 3: Collect Information	82
Step 4: Analyze Maturity Levels	84
Step 5: Formalize Findings	87
<i>The Organization's Vision and Strategy</i>	87
<i>The Department's Vision and Strategy</i>	87
<i>External and Internal Compliance Requirements</i>	87
<i>Organization's Threat Landscape</i>	88
<i>History of Previous Information Security Incidents</i>	88
<i>SOC Sponsorship</i>	89
<i>Allocated Budget</i>	89
<i>Presenting Data</i>	89

*Closing* 90

Summary 90

References 90

## **Chapter 4 SOC Strategy 91**

Strategy Elements 91

Who Is Involved? 92

SOC Mission 92

SOC Scope 93

Example 1: A Military Organization 94

*Mission Statement* 94

*SOC Scope Statement* 95

Example 2: A Financial Organization 95

*Mission Statement* 95

*SOC Scope Statement* 95

SOC Model of Operation 95

In-House and Virtual SOC 96

SOC Services 98

SOC Capabilities Roadmap 99

Summary 101

## **Part III: The Design Phase**

### **Chapter 5 The SOC Infrastructure 103**

Design Considerations 103

Model of Operation 104

Facilities 105

SOC Internal Layout 106

*Lighting* 107

*Acoustics* 107

Physical Security 108

Video Wall 108

SOC Analyst Services 109

Active Infrastructure 110

Network 111

*Access to Systems* 112

Security 112

Compute 115

*Dedicated Versus Virtualized Environment* 116

*Choice of Operating Systems* 118

Storage 118

*Capacity Planning* 119

Collaboration 119

*Ticketing* 120

Summary 120

References 120

## **Chapter 6 Security Event Generation and Collection 123**

Data Collection 123

Calculating EPS 124

*Ubuntu Syslog Server* 124

Network Time Protocol 129

*Deploying NTP* 130

Data-Collection Tools 134

*Company* 135

*Product Options and Architecture* 136

*Installation and Maintenance* 136

*User Interface and Experience* 136

*Compliance Requirements* 137

Firewalls 137

*Stateless/Stateful Firewalls* 137

*Cisco Adaptive Security Appliance ASA* 138

*Application Firewalls* 142

*Cisco FirePOWER Services* 142

Cloud Security 152

Cisco Meraki 153

*Exporting Logs from Meraki* 154

Virtual Firewalls 155

*Cisco Virtual Firewalls* 156

*Host Firewalls* 157

Intrusion Detection and Prevention Systems 157

Cisco FirePOWER IPS 160

Meraki IPS 161

Snort 162

Host-Based Intrusion Prevention 162

Routers and Switches	163
Host Systems	166
Mobile Devices	167
Breach Detection	168
Cisco Advanced Malware Prevention	168
Web Proxies	169
<i>Cisco Web Security Appliance</i>	170
Cloud Proxies	172
<i>Cisco Cloud Web Security</i>	172
DNS Servers	173
Exporting DNS	174
Network Telemetry with Network Flow Monitoring	174
NetFlow Tools	175
<i>StealthWatch</i>	177
<i>Exporting Data from StealthWatch</i>	179
NetFlow from Routers and Switches	182
NetFlow from Security Products	184
NetFlow in the Data Center	186
Summary	187
References	188

## **Chapter 7    Vulnerability Management    189**

Identifying Vulnerabilities	190
Security Services	191
Vulnerability Tools	193
Handling Vulnerabilities	195
OWASP Risk Rating Methodology	197
<i>Threat Agent Factors</i>	198
<i>Vulnerability Factors</i>	198
<i>Technical Impact Factors</i>	200
<i>Business Impact Factors</i>	200
The Vulnerability Management Lifecycle	202
Automating Vulnerability Management	205
Inventory Assessment Tools	205
Information Management Tools	206
Risk-Assessment Tools	206
Vulnerability-Assessment Tools	206

Report and Remediate Tools	206
Responding Tools	207
Threat Intelligence	208
Attack Signatures	209
Threat Feeds	210
Other Threat Intelligence Sources	211
Summary	213
References	214

## **Chapter 8 People and Processes 215**

Key Challenges	215
Wanted: Rock Stars, Leaders, and Grunts	216
The Weight of Process	216
The Upper and Lower Bounds of Technology	217
Designing and Building the SOC Team	218
Starting with the Mission	218
Focusing on Services	219
<i>Security Monitoring Service Example</i>	220
Determining the Required SOC Roles	223
<i>Leadership Roles</i>	224
<i>Analyst Roles</i>	224
<i>Engineering Roles</i>	224
<i>Operations Roles</i>	224
<i>Other Support Roles</i>	224
Working with HR	225
<i>Job Role Analysis</i>	225
<i>Market Analysis</i>	225
<i>Organizational Structure</i>	226
<i>Calculating Team Numbers</i>	227
Deciding on Your Resourcing Strategy	228
<i>Building Your Own: The Art of Recruiting SOC Personnel</i>	229
<i>Working with Contractors and Service Bureaus</i>	229
<i>Working with Outsourcing and Managed Service Providers</i>	230
Working with Processes and Procedures	231
Processes Versus Procedures	231
Working with Enterprise Service Management Processes	232
<i>Event Management</i>	232

<i>Incident Management</i>	233
<i>Problem Management</i>	233
<i>Vulnerability Management</i>	233
<i>Other IT Management Processes</i>	233
The Positives and Perils of Process	234
Examples of SOC Processes and Procedures	236
<i>Security Service Management</i>	236
<i>Security Service Engineering</i>	237
<i>Security Service Operations</i>	238
<i>Security Monitoring</i>	239
<i>Security Incident Investigation and Response</i>	239
<i>Security Log Management</i>	240
<i>Security Vulnerability Management</i>	241
<i>Security Intelligence</i>	241
<i>Security Analytics and Reporting</i>	242
<i>Breach Discovery and Remediation</i>	242
Summary	243

## **Part IV: The Build Phase**

### **Chapter 9 The Technology 245**

In-House Versus Virtual SOC	245
Network	246
Segmentation	247
VPN	251
High Availability	253
Support Contracts	254
Security	255
Network Access Control	255
Authentication	257
On-Network Security	258
Encryption	259
Systems	260
Operating Systems	261
Hardening Endpoints	262
Endpoint Breach Detection	263
Mobile Devices	264
Servers	264



Storage	265
Data-Loss Protection	266
Cloud Storage	270
Collaboration	271
Collaboration for Pandemic Events	272
Technologies to Consider During SOC Design	273
Firewalls	273
<i>Firewall Modes</i>	273
<i>Firewall Clustering</i>	276
<i>Firewall High Availability</i>	276
<i>Firewall Architecture</i>	277
Routers and Switches	279
<i>Securing Network Devices</i>	280
<i>Hardening Network Devices</i>	280
Network Access Control	281
<i>Deploying NAC</i>	282
<i>NAC Posture</i>	284
<i>Architecting NAC</i>	285
Web Proxies	290
<i>Reputation Security</i>	290
<i>Proxy Architecture</i>	292
Intrusion Detection/Prevention	295
<i>IDS IPS Architecture</i>	295
<i>Evaluating IDS IPS Technology</i>	296
<i>Tuning IDS/IPS</i>	298
Breach Detection	300
Honeypots	301
Sandboxes	302
Endpoint Breach Detection	303
Network Telemetry	306
<i>Enabling NetFlow</i>	308
<i>Architecting Network Telemetry Solutions</i>	310
Network Forensics	312
<i>Digital Forensics Tools</i>	313
Final SOC Architecture	314
Summary	317
References	318

## **Chapter 10 Preparing to Operate 319**

Key Challenges	319
People Challenges	319
Process Challenges	320
Technology Challenges	321
Managing Challenges Through a Well-Managed Transition	321
Elements of an Effective Service Transition Plan	322
Determining Success Criteria and Managing to Success	322
<i>Deploying Against Attainable Service Levels</i>	323
<i>Focusing on Defined Use Cases</i>	325
Managing Project Resources Effectively	328
Marching to Clear and Attainable Requirements	329
<i>Staffing Requirements for Go-Live</i>	329
<i>Process Requirements for Go-Live</i>	330
<i>Technology Requirements for Go-Live</i>	331
Using Simple Checks to Verify That the SOC Is Ready	332
<i>People Checks</i>	332
<i>Process Checks</i>	336
<i>Technology Checks</i>	340
Summary	346

## **Part V: The Operate Phase**

### **Chapter 11 Reacting to Events and Incidents 347**

A Word About Events	348
Event Intake, Enrichment, Monitoring, and Handling	348
Events in the SIEM	349
Events in the Security Log Management Solution	350
Events in Their Original Habitats	350
Events Through Communications and Collaboration Platforms	350
Working with Events: The Malware Scenario	351
Handling and Investigating the Incident Report	353
Creating and Managing Cases	354
<i>Working as a Team</i>	355
<i>Working with Other Parts of the Organization</i>	357
<i>Working with Third Parties</i>	359

Closing and Reporting on the Case 362

Summary 363

## **Chapter 12 Maintain, Review, and Improve 365**

Reviewing and Assessing the SOC 366

Determining Scope 366

*Examining the Services* 367

*Personnel/Staffing* 369

*Processes, Procedures, and Other Operational Documentation* 371

*Technology* 372

Scheduled and Ad Hoc Reviews 373

Internal Versus External Assessments 374

*Internal Assessments* 374

*External Assessments* 374

Assessment Methodologies 375

*Maturity Model Approaches* 375

*Services-Oriented Approaches* 376

*Post-Incident Reviews* 378

Maintaining and Improving the SOC 381

Maintaining and Improving Services 381

Maintain and Improving Your Team 383

*Improving Staff Recruitment* 383

*Improving Team Training and Development* 384

*Improving Team Retention* 386

Maintaining and Improving the SOC Technology Stack 387

*Improving Threat, Anomaly, and Breach-Detection Systems* 388

*Improving Case and Investigation Management Systems* 391

*Improving Analytics and Reporting* 392

*Improving Technology Integration* 392

*Improving Security Testing and Simulation Systems* 393

*Improving Automated Remediation* 394

Conclusions 395

Index 397

## Command Syntax Conventions

The conventions used to present command syntax in this book are the same conventions used in the IOS Command Reference. The Command Reference describes these conventions as follows:

- **Boldface** indicates commands and keywords that are entered literally as shown. In actual configuration examples and output (not general command syntax), boldface indicates commands that are manually input by the user (such as a **show** command).
- *Italic* indicates arguments for which you supply actual values.
- Vertical bars (|) separate alternative, mutually exclusive elements.
- Square brackets ([ ]) indicate an optional element.
- Braces ({ }) indicate a required choice.
- Braces within brackets ({ [ ] }) indicate a required choice within an optional element.

## Introduction

Many security books are available, but they focus on either products or on very high-level security best practices. We could not find a book about developing a security operations center. This lack of coverage meant that people interested in this topic would have to take the literature available from security books and interview existing SOC leaders to learn how it should be done. We identified this gap and decided to write this book.

In this book, we use a blend of industry experience and best practices of many of our customers to create a guide for those interested in how a SOC should be developed and managed. This book presents the collective view of its three authors (each a consultant at Cisco Systems). We have worked with hundreds of customers, ranging from Fortune 500 companies to large military organizations, giving us a broad and deep understanding about how SOCs are developed and run in the real world. We hope that our research and experience assists you with your existing SOC or with future security operations projects.

## Who Should Read This Book?

This book is written for anybody interested in learning how to develop, manage, or improve a SOC. This book, which is based on a blend of our industry experience and best practices, can serve as a guide for those interested in creating and managing a SOC. A background in network security, network management, and network operations would be helpful, but it is not required to benefit from this book.

## How This Book Is Organized

**Chapter 1, “Introduction to Security Operations and the SOC”:** This first chapter provides an introduction to security operations. First, we examine challenges that organizations face that justify the investment in a SOC. This chapter also covers high-level SOC topics such as vulnerability management, threat intelligence, digital investigation, and data collection and analysis, thus setting the stage for the rest of the book.

**Chapter 2, “Overview of SOC Technologies”:** This chapter explains how to deploy and customize SOC technologies. The goal is to gain a basic understanding of technology and services found in most modern SOC environments. Topics include data collection, data processing, vulnerability management, and case management.

**Chapter 3, “Assessing Security Operations Capabilities”:** This chapter describes a methodology for developing SOC requirements and assessing security operations capabilities against those requirements. The purpose is to help define a SOC strategy and create a supporting roadmap.

**Chapter 4, “SOC Strategy”:** This chapter explains how to develop a strategy and roadmap for SOC capabilities using results from tactics learned in Chapter 3. These can be used as a benchmark to validate progress and justify future investment in the SOC.

**Chapter 5, “The SOC Infrastructure”:** This chapter covers design considerations for a SOC infrastructure. Topics include the SOC facility, analyst environment, and various technology considerations.

**Chapter 6, “Security Event Generation and Collection”:** Most SOC environments focus heavily on collecting and analyzing data. This chapter describes common tools found in a SOC environment that are used to produce and collect such data.

**Chapter 7, “Vulnerability Management”:** This chapter explains how a SOC can create and deliver a vulnerability management practice. Topics covered include identifying and managing vulnerabilities, calculating risk, and ranking threats to properly prioritize which vulnerabilities to address first.

**Chapter 8, “People and Processes”:** This chapter focuses on developing an appropriate governance and staffing model based on the range of services the SOC will provide. The goal is to not only recruit the right team but also to retain those valuable resources. The chapter also explains how to leverage outsourcing or managed service providers when the situation calls for such resources.

**Chapter 9, “The Technology”:** SOC technologies were briefly discussed in earlier chapters, but this chapter covers how common technologies found in the SOC fit into a SOC architecture. The focus is on design considerations for SOC network, security, collaboration, and storage technologies.

**Chapter 10, “Preparing to Operate”:** This chapter walks you through common steps required to transition a SOC to a fully operational state. Topics include challenges faced before going live, transition plan development, and the impact of proper project management.

**Chapter 11, “Reacting to Events and Incidents”:** In this chapter, you learn how the people, processes, and technology parts of an effective SOC come together to react to events and incidents. This chapter includes a storyline that walks you through how an effective SOC would react to an identified security incident.

**Chapter 12, “Maintain, Review, and Improve”:** The final chapter of this book wraps things up by explaining how to review and maintain the SOC and its services. This chapter also covers how to continuously improve the SOC services to guide its evolution. Improvement topics include how to identify issues with the SOC so that they can be remediated to improve SOC service.

*This page intentionally left blank*

## Overview of SOC Technologies

*“If all you have is a hammer, everything looks like a nail.”—Abraham Maslow*

Chapter 1, “Introduction to Security Operations and the SOC,” provided a general overview of security operations center (SOC) concepts and referenced a number of technologies that offer SOC services such as vulnerability management, threat intelligence, digital investigation, and data collection and analysis. This chapter covers the details of these technologies using a generic and product-agnostic approach. This will give the fundamental understanding of how the technologies function so that these concepts can be related to products covered later in this book. This chapter also covers data collection and analysis, such as how a security information and event management (SIEM) collects and processes log data.

In this chapter, we continue to reference open source code deployments and industry-recognized architectures whenever applicable to illustrate how to deploy and customize SOC technologies. These technologies are used to develop a conceptual architecture that integrates the different SOC technologies and services. After reading this chapter, you should understand the technology and service expectations for most modern SOC environments.

Let’s start by introducing the most fundamental responsibility for a SOC: collecting and analyzing data.

### Data Collection and Analysis

You need to first acquire relevant data before performing any sort of useful analysis. In the context of security monitoring, data from various sources and in different formats can be collected for the purposes of security analysis, auditing, and compliance. Data of special interest includes event logs, network packets, and network flows. You might also want sometimes to actively probe or collect content such as the static content of a web page or the hash value of a file.



Generating and capturing event logs is crucial to security operation. Events can directly or indirectly contribute to the detection of security incidents. For example, a high-priority event generated by a properly tuned intrusion detection system would indicate an attack attempt. However, a high-link-utilization event generated by a router might not be a security event by definition but could indicate a security incident when correlated with other events such as a denial-of-service (DoS) attack or a compromised host scanning your network.

Every organization operates its own unique and continuously evolving list of services and systems. However, the basic questions related to data collection and analysis remain similar across all organizations:

- Which elements should you monitor?
- What data should you collect and in what format?
- What level of logging should you enable on each element?
- What protocols should you use to collect data from the various elements?
- Do you need to store the data you collect and for how long?
- Which data should you parse and analyze?
- How much system and network overhead does data collection introduce?
- How do you associate data-collection requirements with capacity management?
- How do you evaluate and optimize your data-collection capability?

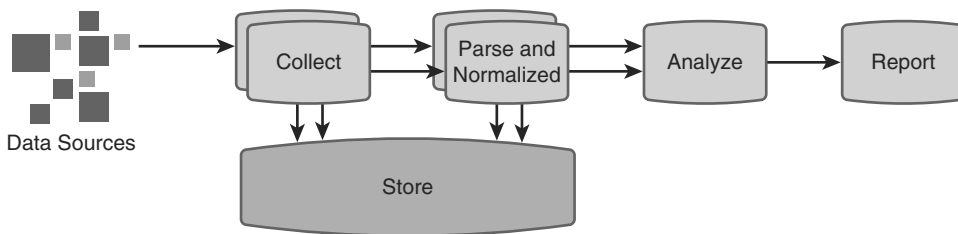
Chapter 7, “Vulnerability Management,” and Chapter 9, “The Technology,” address many of these questions. The fundamental idea is not to monitor everything for the sake of monitoring, but rather to design your data-collection capability so that your technical and compliance objectives are met within the boundaries you are responsible for monitoring. For example, depending on your network topology and the elements you want to collect data from, you might want to distribute your data collectors and centralize your monitoring dashboard so that you have multiple visibility points feeding into one place to monitor all events. Another example is comparing the cost and return of investing in collecting and storing packets versus leveraging NetFlow in existing network assets for security forensic requirements.

Regardless of the technology and design that is selected, the key is that the final product not provide too much or little data. We find many failures experienced by a SOC results from poor data-collection practices. This could be caused by many factors, from blind spots based on how data is collected, to not correlating the right data such as identifying vulnerable systems that do not exist on the network. Sometimes the proper tools are enabled but their clocks are not properly synchronized, causing confusion when troubleshooting. We address these and other best practices for collecting data later in this chapter under logging recommendations.

In principle, the type of data to acquire and what the data originator supports determine the collection mechanism to deploy. For example, most enterprise-level network devices

natively support the syslog protocol for the purpose of remote event logging, whereas other systems require the installation of an agent to perform a similar function.

Understanding your exact environment and identifying the elements that you acquire useful data from are the initial steps in the process of building a data-collection capability. The conceptual steps shown in Figure 2-1 represent this process. Data can be stored in a flat file, a relational database, or over a distributed file system such as the Hadoop Distributed File System (HDFS). The analyze step can use various techniques, such as statistical-based anomaly detection, deploying event correlation rules, or applying machine learning on data. Starting from the SOC design phase, you should formalize and document all processes and procedures, including your choices of technology.



**Figure 2-1** *Basic Data Management Workflow*

After data has been collected, you can decide whether to store it, parse it, or both. Although storing data in its original format can be beneficial for the purposes of digital investigations, out-of-band security analytics, and meeting compliance requirements, it is important to note that data at this point is regarded as being unstructured, meaning the exact structure is still unknown or has not been validated. To understand the structure of the data, parsing is required to extract the different fields of an event. For the data to have any use to the organization, be aware that when storing original data, regardless of the form, you must have a repository that can accept it and tools that can later query, retrieve, and analyze it. Many factors can determine what type and how much data the SOC should store, such as legal and regulatory factors, cost to manage the stored data, and so on. Let's look at the different types of data sources.

## Data Sources

Logging messages are considered the most useful data type to acquire. Logging messages summarize an action or an activity that took place on a system, containing information related to an associated event. Depending on your environment, you might want to consider collecting logging messages from various forms of security, network, and application products. Examples of physical and virtual devices that could provide valuable logging messages include the following:

- Security elements such as firewalls, intrusion detection and prevention systems, antivirus solutions, web proxies, and malware analysis tools
- Network elements such as routers, switches, and wireless access points and controllers

- Operating systems such as the different releases of Microsoft Windows, UNIX, Linux, and OS X
- Virtualization platforms such as Virtual-Box, Kernel-based Virtual Machine (KVM), Microsoft Hyper-V, and VMware ESX
- Applications such as web servers, Domain Name System (DNS) servers, e-mail gateways, billing applications, voice gateways, and mobile device management (MDM) tools
- Databases
- Physical security elements such as security cameras, door access-control devices, and tracking systems
- Systems used in process and control networks, such as supervisory control and data acquisition (SCADA) and distributed control system (DCS)

In addition to logging messages, you might want to collect, store, and possibly analyze other forms of data. Examples include collecting network packets, NetFlow, and the content of files such as configuration files, hash values, and HTML files. Each of these data sources provides unique value, but each has its own associated costs to consider before investing in methods to collect and analyze the data. For example, storing network packets typically has a higher cost for collecting and storage but can provide more granular detail on events than NetFlow. Some industry regulations require storage of packet-level data, making capturing packets a must-have feature. For customers looking for similar forensic data at a lower price, collecting NetFlow can be a less-expensive alternative, depending on factors such as existing hardware, network design, and so on.

To better understand the cost and value of collecting data, let's look deeper at how data can be collected.

## Data Collection

After you have an idea about the data you want to collect, you must figure out how to collect it. This section reviews the different protocols and mechanisms that you can use to collect data from various sources. Depending on what the data source supports, data can be pulled from the source to the collector or pushed by the source to the collector.

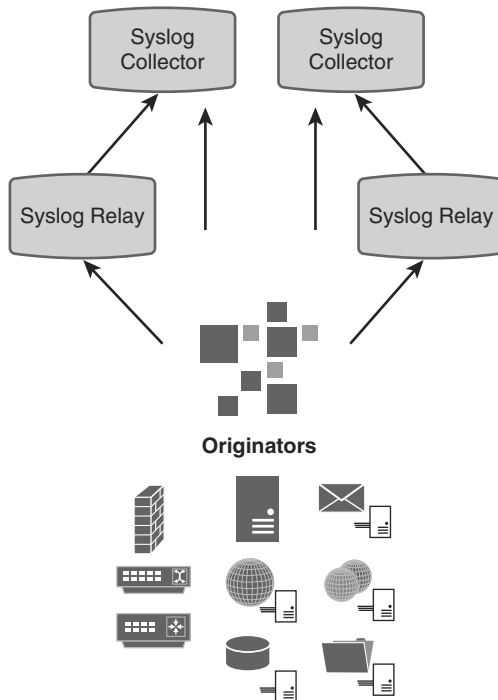
It is important to emphasize the need for time synchronization when collecting data. Capturing logs without proper time stamping could cause confusion when evaluating events and could corrupt results. The most common way a SOC enforces time synchronization across the network is by leveraging a central timing server using the Network Time Protocol (NTP). Best practice is to have all services and systems, including those that generate, collect, and analyze data, synchronize their clocks with a trusted central time server. Chapter 6, "Security Event Generation and Collection," discusses how to best design your NTP implementation for your SOC.

## The Syslog Protocol

The syslog protocol, as defined in IETF RFC 5424,<sup>1</sup> provides a message format that enables vendor-specific extensions to be provided in a structured way, in addition to conveying event notification messages from a syslog client (originator) to a syslog destination (relay or collector). The syslog protocol supports three roles:

- **Originator:** Generates syslog content to be carried in a message
- **Collector:** Gathers syslog messages
- **Relay:** Forwards messages, accepting messages from originators or other relays and sending them to collectors or other relays

Figure 2-2 shows the different communication paths between the three syslog roles, noting that a syslog client can be configured with multiple syslog relays and collectors.



**Figure 2-2** *Syslog Collection Design*

Implementations of syslog use User Datagram Protocol (UDP) with port number 514 to forward events. It is also possible to implement the protocol over a reliable transport protocol, for example, Transfer Control Protocol (TCP), as per IETF RFC 3195.<sup>2</sup> Syslog does not natively provide security protection in terms of confidentiality, integrity, and authenticity. However, these security features can be delivered by running syslog over a secure network protocol, such as Transport Layer Security (TLS) and Datagram Transport

Layer Security (DTLS), as described in RFCs 5425 and 6012, respectively. These approaches might be more secure, but typically at a cost of additional overhead and the risk that some systems might not offer support for these protocols. It is recommended to review the product’s configuration guide to verify possible performance impacts and capabilities before implementing certain features.

Syslog is generally supported by network and security solutions for the purpose of event logging. UNIX and UNIX-like operating systems support syslog through the use of an agent such as rsyslog and syslog-ng. Similarly, Microsoft Windows platforms require the installation of an agent to forward events in syslog format.

Regardless of the syslog client, you need to configure at least the following parameters:

- **Logging destinations:** The collector, relay IP addresses, or hostnames. Depending on the implementation, the originator can forward syslog messages to one or more destinations.
- **Protocol and port:** Typically these are set to UDP and port 514 by default. The option of changing this setting is implementation dependent.
- **Logging severity level:** Can be a value ranging from 0 to 7, as shown in Table 2-1.
- **Logging facility:** A value between 0 and 23 that could be used to indicate the program or system that generated the message. The default value assigned to syslog messages is implementation specific. For example, you can assign logging facility values to categorize your events. Table 2-2 shows an example of assigning facility values to asset categories. Other approaches could be designed based on your environment and requirements. The severity and logging facility values could be combined to calculate a priority value of an event, influencing the post-event actions to take.

**Table 2-1** *Logging Severity Levels*

Level	Severity
0	Emergency: System is unusable.
1	Alert: Action must be taken immediately.
2	Critical: Critical conditions.
3	Error: Error conditions.
4	Warning: Warning conditions.
5	Notice: Normal but significant condition.
6	Informational: Informational messages.
7	Debug: Debug-level messages.

Depending on your setup and requirements, configuring other parameters beyond this list might be required. For example, the SOC may want more granular data by selecting which operating system or application events to log and forward.

**Table 2-2** *Example of Mapping Facility Values to Categories*

Facility Value	Role
Local0	Databases
Local1	Core network devices (routers, switches, wireless controllers, and so on)
Local2	Other network devices
Local3	Operating system
Local4	Core applications
Local5	Not used
Local6	Not used
Local7	Other elements

Let's look at a few examples that demonstrate how to configure a syslog client. Example 2-1 shows how to configure a Cisco IOS-based router to forward events by specifying the logging destinations, level, and facility. Note that there are many other parameters available for syslog beyond what we used for these examples. You can find many comprehensive sources available on the Internet that provide a list of available parameters, such as <http://www.iana.org/assignments/syslog-parameters/syslog-parameters.xhtml>.

**Example 2-1** *Configuring a Cisco IOS Router for Syslog*

```
Router# configure terminal
Router(config)# logging host1
Router(config)# logging host2
Router(config)# logging trap level
Router(config)# logging facility facility_type
```

With the configuration in Example 2-1, the router would generate sample messages similar to what is shown in Example 2-2. The log messages in Example 2-2 are for CPU and link status updates. Some administrators would consider these messages easy to read at an individual level. Now imagine receiving thousands or even millions of such messages per day from various network device types, each with a unique message structure and content. A firewall is a good example of a network security device that would typically generate a large number of logging messages, overwhelming a security administrator who operates a basic log collection tool.

**Example 2-2** *Sample Syslog Messages Generated by a Cisco IOS Router*

```
Sep 9 03:34:57 ROUTER 23772: Sep 9 03:34:53.911: %SYS-3-CPUHOG: Task ran for 18428
msec (22/9), process = IP SNMP, PC = 32976EC.Sep 19 10:25:32 ROUTER 77: Jun 19
10:25:31.093: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial4/0, changed
state to up
Sep 19 10:26:02 ROUTER 78: Sep 19 10:26:01.093: %LINEPROTO-5-UPDOWN: Line protocol
on Interface Serial4/0, changed state to down
```

Next, let's look at remote logging of Linux distribution messages. Remote logging of these events can be achieved by running syslog daemons. Examples are the syslogd and the use of commercial and open source logging daemons such as rsyslog or syslog-ng. In the case of Linux, most operating system log files, such as the ones shown in Example 2-3, are located in the `/var/log/` directory. For CentOS (Community ENTERprise Operating System) using rsyslog, the, syslog configuration is maintained in `/etc/rsyslog.conf`, shown in Example 2-4. Once again, these logs might be able to be interpreted individually, but sorting through a large number of these types of log events would prove cumbersome for most administrators.

**Example 2-3** *Linux Common Log Files and Directories*

```
messages : General message and system related stuff
auth.log : Authentication logs
kern.log : Kernel logs
cron.log : Crond logs (cron job)
maillog : Mail server logs
httpd/ : Apache access and error logs directory
boot.log : System boot log
secure : Access logs from the sshd process
```

**Example 2-4** *rsyslog.conf Sample Configuration*

```
# Forward all messages, generated by rsyslog using any facility and
# priority values, to a remote syslog server using UDP.
# By adding this line and keeping the default configuration, the logs
# will be stored on the client machine and forwarded to the log
# server. To limit the log messages sent by rsyslog, you can specify
# facility and priority values.
# Remote host as name/ip:port, e.g. 192.168.0.1:514, port optional
*. * @log_serever

# You can use @@ for TCP remote logging instead of UDP
# *. * @@log_serever
```

Example 2-5 shows sample Secure Shell (SSH) access log messages for the user *root*. Note that, for many environments, allowing root to gain remote login access using SSH is not recommended.

**Example 2-5** *Sample Linux Syslog Messages for SSH Access*

```
Sep  7 14:36:01 CentOS6 sshd[3140]: Accepted password for root from x.x.x.x
port 65314 ssh2
Sep  7 14:36:02 CentOS6 sshd[3140]: pam_unix(sshd:session): session opened for user
root by (uid=0)
```

**Tip** Pay attention to the log rotation settings for syslog files that are maintained locally on your system. In the case of CentOS, for example, the log rotation settings are maintained in the `/etc/logrotate.d` directory.

A syslog relay or collector must be ready to receive and optionally process (for example, parse, redirect, and/or enrich) logging messages as required. Your choice of the logging server is driven by a number of factors, such as your technical requirements, skill set, scalability of the platform, vendor support, and of course, cost of acquisition and operation. In addition to commercial log management tools such as Splunk and HP Arcsight ESM, a growing number of open-source code implementations are available, such as graylog<sup>23</sup> and logstash<sup>4</sup> (part of the Elasticsearch ELK stack<sup>5</sup>).

Although some SIEM products manage security events, they might not be made for long-term event storage and retrieval. The reason why is that some SIEMs' performance and scalability are limited when compared to dedicated log management platforms such as Splunk or Logstash, especially as the amount of data they store and process increases. This is due to how legacy SIEM tools store and query events, which in most cases means the use of a relational database infrastructure. Note that some SIEM vendors are evolving their approach of managing events and deploying big data platforms for their data repository. SIEM vendors that have not made this move are sometimes referred to as *legacy*.

## Logging Recommendations

Enabling logging features on a product can prove useful but also have an associated cost on performance and functionality. Some settings should be required before enabling logging, such as time synchronization and local logging as a backup repository when the centralized logging solution fails. When designing and configuring your syslog implementation, consider the following best practices before enabling logging:

- In the context of security operation, log events that are of business, technical, or compliance value.
- Configure your clients and servers for NTP, and confirm that clocks are continuously being synchronized.
- Time stamp your log messages and include the time zone in each message.
- Categorize your events by assigning logging facility values. This will add further context to event analysis.



- Limit the number of collectors for which a client is configured to the minimum required. Use syslog relays when you require the same message to be forwarded to multiple collectors. Syslog relays can be configured to replicate and forward the same syslog message to multiple destinations. This scenario is common when you have multiple monitoring platforms performing different tasks such as security, problem management, and system and network health monitoring.
- Baseline and monitor the CPU, memory, and network usage overhead introduced by the syslog service.
- Have a limited local logging facility, in file or memory, so that logs are not completely lost if the syslog collector is unavailable, such as in the case of network failure.
- On a regular basis, test that logging is functioning properly.
- Protect your syslog implementation based on evaluating the risk associated with syslog not providing confidentiality, integrity, or authenticity services.
- Ensure that log rotation and retention policies are properly set.
- Protect files where logs are stored: Restrict access to the system, assign proper files access permissions, and enable file encryption if needed. Read access to log files must be granted only to authorized users and processes. Write access to log files must be granted only to the syslog service. Standard system hardening procedures could be applied to operating systems hosting your logging server.

### Logging Infrastructure

There are other elements to consider when designing a logging infrastructure. These include the type of data being received, expected storage, security requirements, and so on. Here are some factors that will influence how you should design your logging infrastructure:

- The logging level for which your systems are configured. Remember, configuring higher severity levels results in generating more logging messages. For example, configuring a firewall for severity level 6 (information) would result in the firewall generating multiple events per permitted connection: connection establishment, termination, and possibly network address translation.
- The amount of system resources available to the syslog client and server in comparison to the number of logging messages being generated and collected. An environment that generates a large amount of logging data might require multiple logging servers to handle the volume of events.
- The per-device and aggregate events per second (EPS) rates. This is closely related to the device type, available resources, logging level, security conditions, and the placement of the device in the network. You must consider the expected EPS rate in normal and peak conditions usually seen during attacks. Chapter 6 provides best practices for calculating EPS rates.

- The average size (in bytes) of logging messages.
- The amount of usable network bandwidth available between the logging client and the logging server.
- Protecting syslog messages using secure network protocols such as TLS and DTLS introduces additional load that must be accounted for.
- The scalability requirements of the logging infrastructure, which ideally should be linked to capacity planning.
- Consider collecting logging messages using an out-of-band physical or logical network. Separating your management plane—for example, by using a separate management virtual LAN (VLAN) or a Multiprotocol Label Switching (MPLS) virtual private network (VPN)—is a good network and system management practice that applies to most devices and systems. You might, however, encounter cases in which a system does not support having a separate physical or logical management interface, forcing you to forward logging messages in-band.

The preceding factors should influence your design decision related to the logging model: centralized, distributed, or semi-centralized.

## Telemetry Data: Network Flows

Every network connection attempt is transported by one or more physical or virtual network devices, presenting you with an opportunity to gain vital visibility and awareness of traffic and usage patterns. All that is needed is a way to harvest this information from existing network devices such as routers, switches, virtual networking, and access points. This essentially is enabling additional visibility capabilities from common network equipment depending on how the network traffic is collected and processed. An example is looking at traffic on switches to identify malware behavior, such as a system passing a file that attempts to spread across multiple devices using uncommon ports, giving the administrator additional security threat awareness about the environment.

In many cases, capturing and transferring network packets is not required, desired, or even feasible. Reasons could include the cost for storage of the data being captured, skill sets required to use the data, or hardware costs for tools that can capture the data. This can be the case especially when multiple remote locations are connected by a wide-area network (WAN). The alternative to capturing packets is to collect contextual information about network connections in the form of network flow.

The IP Flow Information eXport (IPFIX) protocol, specified in a number of RFCs, including 7011,<sup>6</sup> is a standard that defines the export of unidirectional IP flow information from routers, probes, and other devices. Note that IPFIX was based on Cisco NetFlow Version 9. The standard ports that an IPFIX service listens to, as defined by IANA, are udp/4379 and tcp/4379.

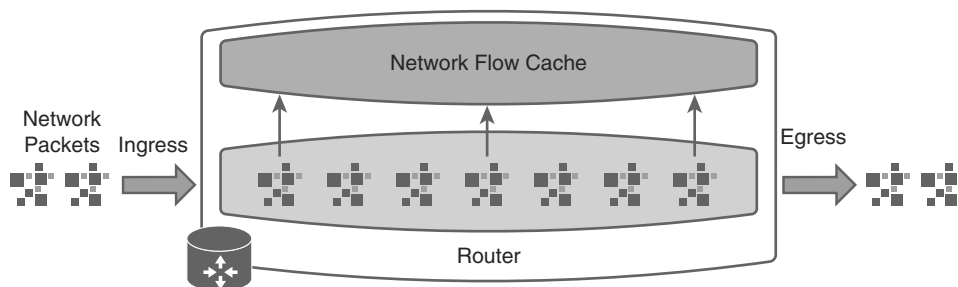
A flow, according to the IPFIX standard, consists of network packets that share the same arbitrary number of packet fields within a timeframe (for example, sharing the same source IP address, destination IP address, protocol, source port, and destination port).

IPFIX enables you to define your own list of packet fields to match. In IPFIX, network flow information is exported (pushed) using two types of records: flow data and template. The template record is sent infrequently and is used to describe the structure of the data records.

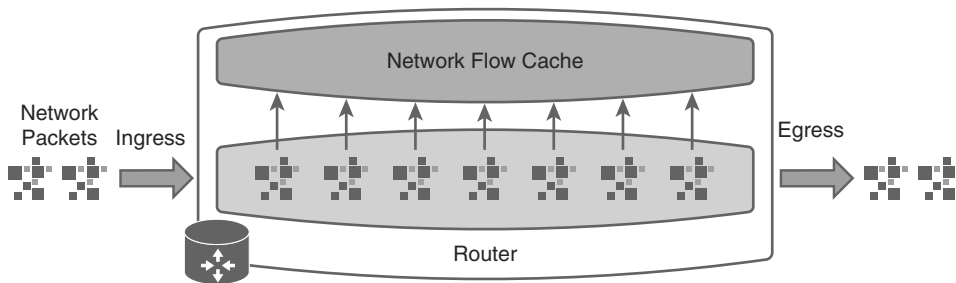
Routers and high-end network switches are the most common devices that can capture, maintain, and update flow records using their cache. These devices can export a record when they believe that a flow has completed or based on fixed time intervals. Keep in mind that capturing, maintaining, and exporting network flow information could impact the system's overall performance depending on the platform being used. Best practice is working through a capacity-planning exercise and consulting with your network vendor on the impact of enabling the feature. Network device vendors generally maintain testing results per platform and are happy to share test results with their customers.

In addition to routers and switches, there is the option of using dedicated hardware appliances that can convert information collected from captured packets into network flow records that can then be exported. Similar to syslog, you can implement a distributed solution with relays that accept, replicate, and forward network flow information to various destinations such as SIEM tools and network flow analyzers. Some vendors, such as Lancope, offer sensor appliances that can add additional attributes while converting raw packets to NetFlow, such as application layer data that typically would not be included in a flow record.

Depending on your platform, a router (or any other flow-collection device) can support sampled/unsampled flow collection, as shown in Figure 2-3 and Figure 2-4, respectively. In the case of sampled flow collection, to update its flow records, the router looks at every  $n$ th packet (for example, 1 in every 128) rather than at every packet that traverses it. This behavior introduces probabilistic security threat detection, meaning some flows might be missed. In addition, relying on sampled flows would result in unreliable digital investigation, assuming network flows are part of your investigation artifacts. For these and other reasons, it is recommended to use only sampled flow collection if no other options are available. An analogy of comparing sampled and unsampled flow is knowing somebody has entered your house within the past few hours versus knowing a user entered your house a few minutes ago and currently is sitting in your living room. Unsampled details are much more valuable, and best practice is using the most current version if possible.



**Figure 2-3** *Sampled Flow Collection*



**Figure 2-4** *Unsampled Flow Collection*

One major benefit of using flow-based detection for security is having “the canary in the coal mine” approach for identifying network breaches, meaning detecting unusual behavior that is not linked to an attack signature. An example is a trusted user performing network reconnaissance followed by connecting to sensitive systems that the user has never accessed before. Most common security products, such as firewalls and intrusion prevention system (IPS) technology, would probably ignore this behavior. A flow-based security product, however, could identify the user as being authorized to perform these actions but still flag the unusual behavior as an indication of compromise.

Another benefit of flow-based security is enabling the entire network as a sensor versus limiting visibility to security products. Typically, this also reduces investment cost in new products by leveraging capabilities within existing equipment. Security products may have limitations as to what they can see, because of traffic being encrypted or where they are placed on the network, thus causing security blind spots. It also might not be feasible to deploy security products at multiple remote locations. These and other scenarios are great use cases for using network flow for security analytics.

Let’s look at a few examples of how to enable NetFlow on devices. Example 2-6 shows the steps to configure NetFlow v9 on a Cisco IOS-based router.

**Example 2-6** *Configuring NetFlow v9 on a Cisco IOS-Based Router*

```
! Configure the NetFlow collector IP address and port
Router(config)# ip flow-export destination {ip_address | hostname} udp_port

! Configure the router to use NetFlow version 9
Router(config)# ip flow-export version 9

! Specifies the interface that to enable NetFlow on
Router(config)# interface type number

! Enables NetFlow on the interface:
! ingress: Captures traffic that is being received by the interface
! egress: Captures traffic that is being transmitted by the interface
Router(config)# ip flow {ingress | egress}
```

With IPFIX and NetFlow v9, you can do much more than what is shown in Example 2-6. On a Cisco IOS-based router, you can customize your flow records and define what to match and what data to export. Example 2-7 shows an example of this configuration.

**Example 2-7** *Configuring NetFlow v9 on an IOS-Based Router with a Customized Record*

```
! Create a flow record that matches specific criteria and collect
! specific information
Router(config)# flow record MY_RECORD
Router(config-flow-record)# match ipv4 source_address
Router(config-flow-record)# match ipv4 destination address
Router(config-flow-record)# match transport source-port
Router(config-flow-record)# match transport destination-port
Router(config-flow-record)# match interface input
Router(config-flow-record)# collect counter packets
Router(config-flow-record)# collect counter bytes

! Configure your export settings
Router(config)# flow exporter MY_EXPORTER
Router(config-flow-exporter)# destination {ip_address | hostname}
Router(config-flow-exporter)# export-protocol netflow-v9
Router(config-flow-exporter)# transport udp udp_port

! Enabling flow monitor
Router(config)# flow monitor MY_MONITOR
Router(config-flow-monitor)# record record_name
Router(config-flow-monitor)# exporter exporter_name
Router(config-flow-monitor)# cache {entries number | timeout {active | inactive |
update} seconds | type {immediate | normal | permanent}}
```

Chapter 6 delves deeper into NetFlow-based technologies. Now let's look at a different way to monitor the network using packet-capture technology.

## Telemetry Data: Packet Capture

There are cases in which you need to go beyond collecting logging messages and network flow information. An example is the need for deep forensic capabilities to meeting strict regulation requirements for capturing raw network packets. Network traffic can be captured and forwarded to an intrusion detection system (IDS), a deep packet inspection engine (DPI), or simply to a repository where captured packets are stored for future use. Your choice of the packet capturing technology is influenced by the network and media type to monitor.

In the case of Ethernet, you can consider two techniques to capture network packets, each with its pros and cons:

- **Port mirroring:** This approach uses network switches to mirror traffic seen on ports or VLANs to other local or remote ports. This is a basic feature supported by most of today's enterprise-level network switches. The local Switched Port Analyzer (SPAN) configuration for Cisco switches can be used to mirror traffic locally, meaning within the same switch. The remote SPAN (RSPAN and ERSPAN) configuration for Cisco switches can extend this feature by allowing remote mirroring of traffic across multiple switches if they are all configured for RSPAN. Note that based on the number of captured packets and state of your network, copying packets to a remote switch can have implications on the overall performance of the network. In addition, it is important to consider how much oversubscription you would allow when copying traffic. For example, you might not want to mirror traffic from multiple 10-Gbps interfaces on a switch to a single 1-Gbps interface. Best practice is carefully selecting the sources and destinations for port mirroring.
- **Network taps:** Another approach is connecting out-of-band devices in the form of network taps to monitor and capture packets from point-to-point links. Network taps capture and copy network packets without involving the active network components, making them suitable for most environments. Network taps, however, cannot capture some traffic, such as packets that are exchanged locally within a switch. It is also financially infeasible to connect taps to all network links. You would generally connect them to the most important locations in your network, such as your Internet gateways and data centers. Network taps are also ideal for on-demand troubleshooting.

**Note** Whether continuous or on demand, capturing packets is an expensive operation in terms of the amount of data to collect, transfer, analyze, and eventually store. The cost associated with capturing packets can be determined by the amount of data to acquire; the location in your network; and the network, system, and storage resources available for this purpose.

Capturing syslogs, network flows, and packets is not very useful if an administrator is manually shuffling through thousands of events. Even the most trained professionals could miss an important alert or not be able to associate events that look trivial as individual alerts but map out to a larger threat if pieced together. This is where centralized collection solutions show the most value, by parsing and normalizing data so that it can be used later for security analysis that helps administrators identify the most important events to focus on.

## Parsing and Normalization

Data that requires further processing and analysis must be first parsed and normalized. *Parsing* refers to the process of taking raw input in string format and traversing the

different fields based on a predefined schema, and *normalization* refers to the process of allowing similar extracted events from multiple sources to be uniformly stored or consumed by subsequent processing steps.

Let's look at an example of parsing a message generated by iptables (Linux host-based firewall) for dropped packets on a CentOS Linux host. Example 2-8 shows the original message saved to the local `/etc/var/kernel.log` file and the version of the same message represented in JavaScript Object Notation (JSON) format. The JSON form was created after being forwarded to and parsed by the log management platform Logstash. Notice that in this example the received syslog message is parsed, but this example does not extend parsing to extract the content of the iptables drop message. This means that in this example, we did not retrieve data such as the action, source and destination IP addresses, TCP ports, TCP headers, interface where the packet was dropped, and so on. This can be achieved by creating a parser that refers to the iptables logging message schema.

### Example 2-8 Event Generated by iptables and Processed by Logstash

```
# Original logging message generated by iptables
DROP: IN=eth1 OUT= MAC= x:x:x:x:x:x:x:x:x:x SRC=10.x.x.28 DST=10.x.x.155
LEN=48 TOS=0x10 PREC=0x00 TTL=55 ID=40590 DF PROTO=TCP SPT=61716 DPT=4433 WIN-
DOW=65535 RES=0x00 SYN URGP=0

# Syslog message stored in /etc/var/kernel.log and received by the
# log collector (Logstash)
Sep 15 13:23:10 CentOS6 kernel: DROP: IN=eth1 OUT= MAC= x:x:x:x:x:x:x:x:x:x
SRC=10.x.x.28 DST=10.x.x.155 LEN=48 TOS=0x10 PREC=0x00 TTL=55 ID=40590 DF
PROTO=TCP SPT=61716 DPT=4433 WINDOW=65535 RES=0x00 SYN URGP=0

# The parsed syslog message, with fields shown in JSON format
{
  "_index": "logstash-2014.09.15",
  "_type": "syslog",
  "_id": "GDbzh5zJQw6VaWWO5CQAMg",
  "_score": null,
  "_source": {
    "message": "Sep 15 13:23:10 CentOS6 kernel: DROP: IN=eth1 OUT= MAC=
      x:x:x:x:x:x:x:x:x:x SRC=10.x.x.28 DST=10.x.x.155 LEN=48 TOS=0x10
      PREC=0x00 TTL=55 ID=40590 DF PROTO=TCP SPT=61716 DPT=4433 WINDOW=65535 RES=0x00
      SYN URGP=0 ",
    "@version": "1",
    "@timestamp": "2014-09-15T12:23:10.000Z",
    "type": "syslog",
    "file": "/var/log/kern.log",
    "host": "CentOS6.5",
    "offset": "1463891",
```

```

    "syslog_timestamp": "Sep 15 13:23:10",
    "syslog_hostname": "CentOS6",
    "syslog_program": "kernel",
    "syslog_message": "DROP: IN=eth1 OUT= MAC=x:x:x:x:x:x:x:x:x:x:x:x
      SRC=10.x.x.28 DST=10.x.x.155 LEN=48 TOS=0x10 PREC=0x00 TTL=55 ID=40590 DF
      PROTO=TCP SPT=61716 DPT=4433 WINDOW=65535 RES=0x00 SYN URGP=0 ",
    "received_at": "2014-09-15 12:23:06 UTC",
    "received_from": "CentOS6.5",
    "syslog_severity_code": 5,
    "syslog_facility_code": 1,
    "syslog_facility": "user-level",
    "syslog_severity": "notice"
  },
  "sort": [
    1410783790000,
    1410783790000
  ]
}

```

Parsing of messages such as event logs can make use of regular expressions also known as regex. Regex are patterns that you can use to extract information from some text input. A pattern can be expressed by a combination of alphanumeric characters and operators in a syntax that is understood by regex processors. An example is matching the string *root*, which is not case sensitive. This can be expressed using one of the regex patterns shown in Example 2-9. Both statements will match all possible lowercase and uppercase combinations of the string root (for example, rooting, -Root!-, or simply RooT).

Regex is commonly used for creating intrusion detection/prevention signatures, where you can quickly create custom regex-based signatures that match patterns of your choice. This allows you to alert and protect against attacks that try to exploit unpatched systems or alert and protect systems that could not be easily patched. An example is protecting legacy applications or devices used in process control networks.

**Example 2-9** *Regex Pattern to Match the Non-Case-Sensitive String root*

```

[rR] [oO] [oO] [tT]
OR
[rR] [oO] {2} [tT]

```

Similarly, SIEM tools make use of regex. The schema or exact structure of the message must be known beforehand. SIEM tools must maintain a current schema library for all the different events they can process. In addition, the tools should allow creating custom parsers as required. Failing to properly parse and normalize a message could result in being unable to analyze the data.

Many regex cheat sheets are available online, such as <http://tinyurl.com/RgExCheatSheet>, which you can use to reference regex commands.



Security Analysis

*Security analysis* refers to the process of researching data for the purpose of uncovering potential known and unknown threats. The complexity of the task varies from performing basic incident mapping to advanced mathematical modeling used to discover unknown threats. Revealing relationships between events within a context is achieved using machine learning-based techniques or knowledge-based techniques, such as rule-based matching and statistical anomaly detection.

Event correlation is the most known and used form of data analysis. *Security event correlation* refers to the task of creating a context within which revealing relationships between disparate events received from various sources for the purposes of identifying and reporting on threats. A context can be bound by time, heuristics, and asset value.

Correlation rules are packaged in SIEM tools. The vendors usually offer the option of performing regular updates to the rule sets as part of a paid support service. These rules can be tuned, or you can create your own rules; however, it is important to first know the use cases you are looking to address. Most correlation rules offered by SIEM vendors are based on experience they gain from their install bases and internal research teams, meaning that most likely they have developed rules for your business requirements. Examples of out-of-box correlation rules include flagging excessive failed logins, malware infection, unauthorized outbound connections, and DoS attempts. It is a good practice to have the SIEM vendor run through your business scenarios during a proof of concept to validate their correlation and reporting capabilities.

It is common practice to tune the out-of-the-box rules or create your own rules that meet your business requirements. Table 2-3 shows some of the use cases shipped with the Splunk SIEM application, referred to as Splunk Enterprise Security Application. Note that the thresholds are listed that you can adjust for each use case.

Table 2-3 Splunk Enterprise Security Correlation Rules

Correlation Search	Description	Default
Endpoint - Active Unremediated Malware Infection	Number of days that the device was unable to clean the infection	3
Endpoint - Anomalous New Services	Number of new services	9
Endpoint - Anomalous New Processes	Number of new processes	9
Endpoint - Anomalous User Account Creation	Number of new processes in a 24-hour period	3
Access - Brute-Force Access Behavior Detected	Number of failures	6
Access - Excessive Failed Logins	Number of authentication attempts	6
Endpoint - High Number of Infected Hosts	Number of infected hosts	100

**Table 2-3** *continued*

<b>Correlation Search</b>	<b>Description</b>	<b>Default</b>
Endpoint - Host with Excessive Number of Listening Ports	Number of listening ports	20
Endpoint - Host with Excessive Number of Processes	Number of running processes	200
Endpoint - Host with Excessive Number of Services	Number of running services	100
Endpoint - Host with Multiple Infections	Total number of infections per host	> 1
Endpoint - Old Malware Infection	Number of days host had infection	30 days
Endpoint - Recurring Malware Infection	Number of days that the device was re-infected	3 days
Network - Substantial Increase in an Event	Number of events (self-baselines based on average)	3 St Dev.
Network - Substantial Increase in Port Activity (by Destination)	Number of targets (self-baselines based on average)	3 St Dev.
Network - Vulnerability Scanner Detection (by Event)	Number of unique events	25
Network - Vulnerability Scanner Detection (by Targets)	Number of unique targets	25

Correlation rules are meant to detect and report on threat scenarios, also referred to as use cases. Before you formalize a use case, you want to answer the following questions:

- What methodology should you use to come up with a use case?
- For a use case, what logging messages should you collect and from which devices?
- Can you achieve the requirements of a use case using existing security controls (for example, by using an existing intrusion detection/prevention system or a firewall)?
- How complex is the task of creating or tuning correlation rules?
- How do you associate use cases with your risk-assessment program?
- How complicated is the use case, and what impact will it have on the performance of your SIEM tool?
- Will the rule created for a use case result in an increase in false positives?

The exact use case and your choice of tools impact the complexity associated with creating or customizing correlation rules. For example, creating a rule that alerts on detecting the use of a clear-text management protocol such as Telnet could be straightforward compared to more complex rules that involve multiple sources, messages, and time periods.

Also, it is important to consider the performance impact on the SIEM as your rules grow in size and complexity along with management for customized functions.

Let's look at the example use case to create a correlation rule that triggers an alert when the same account was used to log in to more than ten data center servers, followed by one or more of these servers establishing one or more outbound TCP connections to external IP addresses within 5 minutes after the ten login attempts. The idea of using this example is to demonstrate how complex creating correlation rules can be for use cases that might sound simple. You can express this use case as a nested statement made of a combination of events (content) and operators such as **AND**, **OR**, **NOT**, and **FOLLOWED BY** (stateful context). In this use case, a context is nothing but an arbitrary set of parameters that describe a particular event of sequence of events. This nested statement to meet this use case is shown in Example 2-10.

**Example 2-10** *High-Level Correlation Rule Statement*

```
[
    (More than ten successful login events)
    AND
    (Events are for the same user ID)
    AND
    (Events generated by servers tagged as data center)
    AND
    (Events received within a one-minute sliding window)
]
FOLLOWED BY
[
    (TCP connection event)
    AND
    (Source IP address belongs to the data center IP address range)
    AND
    (Destination IP address does NOT belong to the internal IP
    address range)
    AND
    (Protocol is TCP)
    AND
    (Events received within fives minutes)
]
```

After a custom statement has been created, the next step is to convert the statement to a rule following the syntax used by your SIEM tool of choice. Commercial SIEM tools provide a graphical interface for you to complete this task. An alternative is outsourcing rule creation to a third-party consultant or to the SIEM vendor's professional services. We recommend first verifying with the SIEM vendor that there is not an existing rule or rules that meet your needs before investing time and money into creating customized correlation rules.

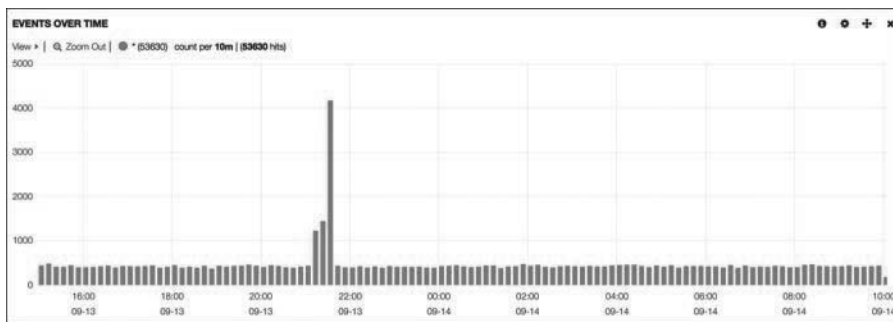
Despite the fact that a use case might look simple, converting it to a rule might not be so easy. Even if you were to convert the previous example into a correlation rule, how about the more complicated ones? In addition, how much can you grow your rule base, and what impact on performance would it have on your tool? Let's look at some alternatives to creating correlation-based rules.

## Alternatives to Rule-Based Correlation

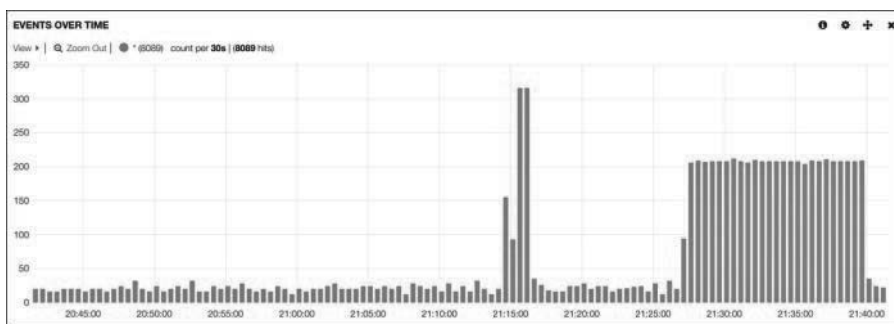
Anomaly-based correlation is another approach that can be combined with rule-based correlation. Detecting anomalies relies on first statically profiling your environment to establish a baseline. After you have a baseline, the SIEM can identify activity patterns that deviate from the baseline, alerting on potential security incidents. Profiling an environment typically generates multiple baselines, such as the following:

- Traffic rate baseline such as average EPS and peak EPS per day of the week
- Network baseline looking at protocol and port usage per day of the week
- System baseline monitoring average and peak CPU and memory usage, average number of running services, user login attempts per day of the week

When it comes to profiling peaks, it is important to record not only the highest values reached but also the durations in which noticeable increase of usage were observed, thus adding statefulness to your profiling process. Figure 2-5 is a histogram that shows the distribution of syslog messages sent from Linux hosts in the past 24 hours. The distribution of events shows a spike in the number of events lasting for around 30 minutes. This type of event would generally trigger the interest of a security analyst. Figure 2-6 shows zooming in to this data to identify two different periods of high syslog activities corresponding to what was shown in Figure 2-5. In this specific example, the first period is short and corresponds to the installation of system patches on a number of hosts, and the second (and longer-lasting) period corresponds to a wider remote system compliance check. These might not have been malicious events; however, using anomaly detection can help administrators be more aware of changes in their environment. This proves useful for a response if users complain that the network is running slowly during the spike time periods.



**Figure 2-5** *Event Distribution Histogram Showing Two Different Peak Shapes*



**Figure 2-6** Event Distribution Histogram Showing Two Different Peak Shapes: Zoom

Another approach that could also be combined with rule-based correlation is risk-based correlation, also referred to as algorithmic. The basic idea is to calculate a risk score for an event based on the content and context of an event. Risk scores can be based on asset value, source IP address reputation, geolocation, reported user role (for example, a Lightweight Directory Access Protocol [LDAP] group), and so on. This approach is useful when you do not have much visibility on the use cases you require or when configuring correlation rules is complex. The challenge to this approach is the work required to design the risk formula and assigning values to input types that are being considered.

**Note** Risk scores do not include probability values. You learn how to calculate risk in Chapter 7, “Vulnerability Management.”

There are other methods to improve network awareness beyond correlating events. Let’s look at additional ways to improve data through data-enrichment sources.

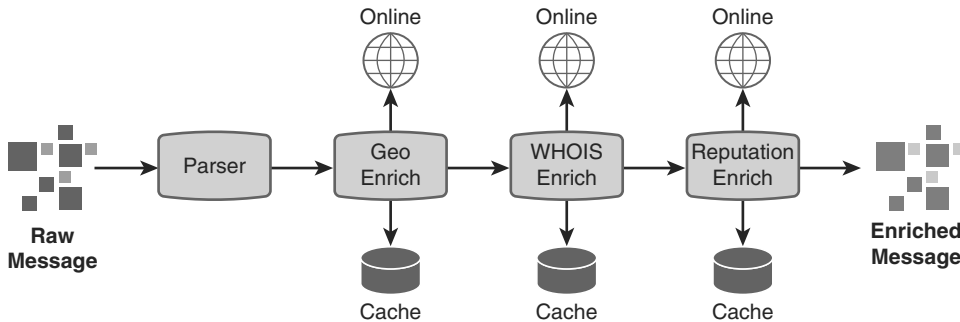
## Data Enrichment

*Data enrichment* refers to the practice of adding additional context to the data that you receive. Common examples of enrichment sources include the following:

- Geo information, allowing you to map IP addresses to geographical locations
- WHOIS information, allowing you to tap into further contextual information on IP addresses
- Reputation information on domain names, IP addresses and e-mail senders, file hash values, and so on
- Domain age information

This overlay knowledge you gain helps you make more informative decisions, increasing the accuracy of your threat-detection processes and tools.

Typically, enrichment is applied to post-parsed messages just before data is stored or processed in real time or off line. This can sometimes help security products save process power by blocking known attacks, such as sources with negative reputation, at a preprocess stage. Figure 2-7 shows a sample enrichment process. The figure also shows that enrichment information can be acquired in real time or from an existing cache.



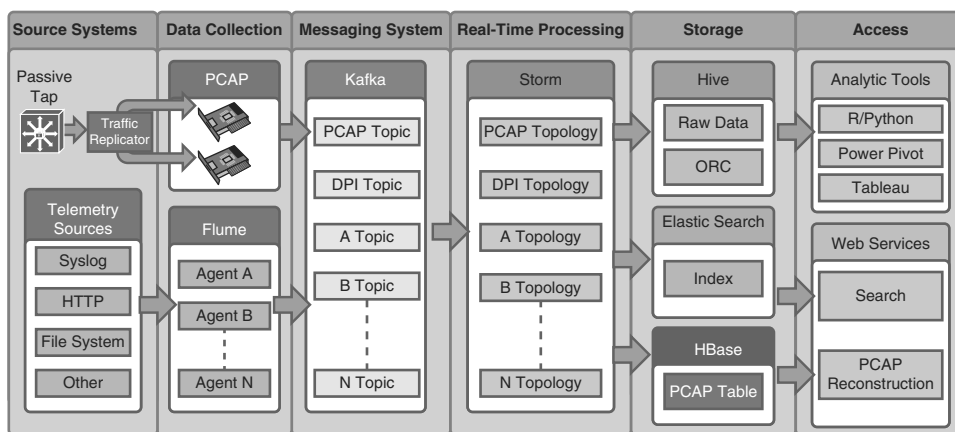
**Figure 2-7** *Sample Enrichment Process*

## Big Data Platforms for Security

Using relational databases to store and query data does not scale well and is becoming a huge problem for organizations as information requirements continue to increase. The solution is to use big data platforms that can accept, store, and process large amounts of data. In the context of security, big data platforms should not only be scalable in terms of storing and retrieving large amounts data but also support services offered by traditional log management and SIEM tools. This hybrid of capabilities and storage is critical for storing, processing, and analyzing big data in real time or on demand.

Most of today's big data platforms are based on Apache Hadoop. This framework allows for the distributed processing of large data sets across clusters of computers using HDFS, MapReduce, and YARN to form the core of Apache Hadoop. At the heart of the platform is the Hadoop Distributed File System (HDFS) distributed storage system. YARN is a framework for job scheduling and cluster resource management. MapReduce is a YARN-based system for parallel processing of large data sets. In addition, many Hadoop-related projects deliver services on top of Hadoop's core services.

Open source-based log management and processing tools are starting to present themselves as viable replacements to legacy the SIEM tools. This is not only the case of storage and offline processing of data but also for real-time processing using (for example, Apache Storm<sup>7</sup>). Figure 2-8 shows the architecture of the Cisco OpenSOC platform, which is based largely on a number of Apache projects, allowing data of various format to be collected, stored, processed (on-line and off-line), and reported.



**Figure 2-8** *The Cisco OpenSOC Platform Architecture*

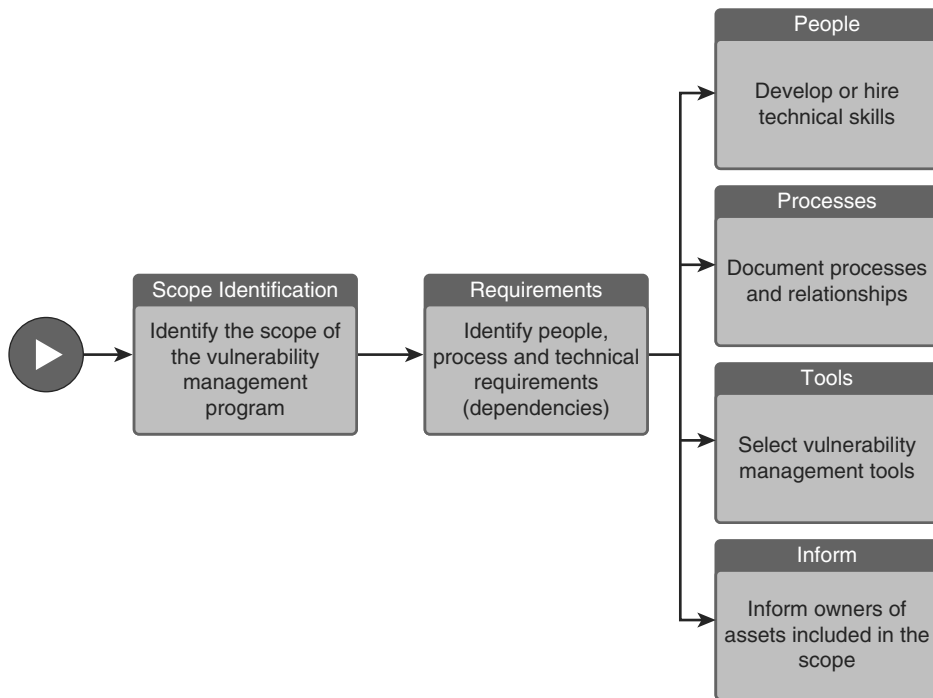
## Vulnerability Management

*Vulnerability management* refers to the process of discovering, confirming, classifying, prioritizing, assigning, remediating, and tracking vulnerabilities. Do not confuse vulnerability management with vulnerability scanning, the latter being part of the vulnerability management process, with emphasis on the discovery phase. It is also important to understand that risk management deals with all associated risks, whereas vulnerability management targets technology.

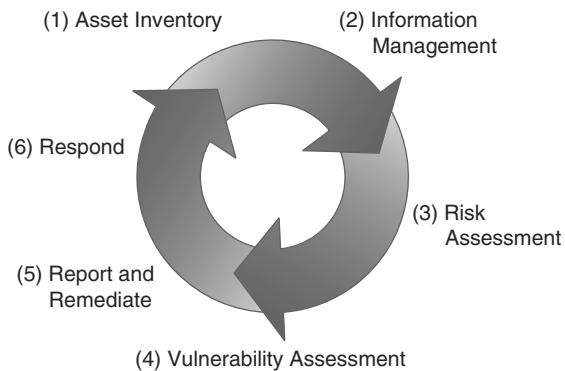
Vulnerabilities can be perceived as weaknesses in people, process, and technology. Vulnerability management in the context of SOC focuses on known technical weaknesses introduced in software and firmware. It is worth highlighting that the existence of a technical vulnerability could be the result of weaknesses in people and process such as the lack of a proper software quality assurance process.

Organizations with a mature security program integrate the closely linked vulnerability management and risk management practices. Sometimes this can be accomplished using tools that can automate this integration. Figure 2-9 shows the initial steps you would typically undertake to identify the scope and prepare your vulnerability management program. We will look deeper into preparing the SOC in Chapter 10.

The most critical element of vulnerability management is being faster at protecting the vulnerable asset before the weakness is exploited. This is accomplished by continuously applying a series of steps to identify, assess, and remediate the risk associated with the vulnerability. A good reference model that can be followed as a guideline for handling risk is the SANS Vulnerability Management Model shown in Figure 2-10. The details of each step are covered in Chapter 7.



**Figure 2-9** *Preparing a Vulnerability Management Program*



**Figure 2-10** *SANS Vulnerability Management Model*

One of the most common methods to identify when a system is vulnerable is by monitoring for vulnerability announcements in products found within your organization. Let's look more into how this information is released.



## Vulnerability Announcements

Vulnerabilities in open and closed source code are announced on a daily basis. Identifiers are associated with vulnerability announcements so that they can be globally referenced, ensuring interoperability. One commonly used standard to reference vulnerabilities is the Common Vulnerabilities and Exposures (CVE), which is a dictionary of publicly known information security vulnerabilities and exposures. CVE's common identifiers make it easier to share data across separate network security databases and tools. If a report from one of your security tools incorporates CVE identifiers, the administrator can quickly and accurately access and fix information in one or more separate CVE-compatible databases to remediate the problem. Each CVE identifier contains the following:

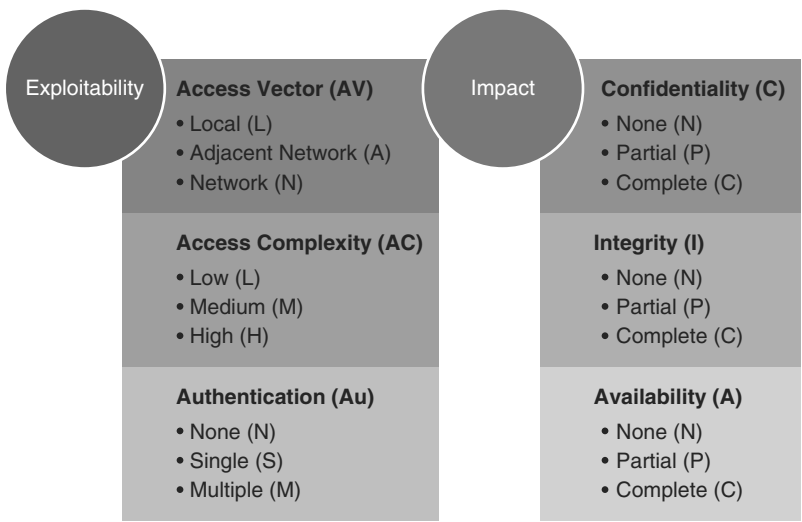
- CVE identifier (CVE-ID) number in the form of CVE prefix + Year + Arbitrary Digits
- Brief description of the security vulnerability or exposure
- Other related material

The list of products that use CVE for referencing vulnerabilities is maintained by MITRE.<sup>8</sup>

The CVE identifier does not provide vulnerability context such as exploitability complexity and potential impact on confidentiality, integrity, and availability. These are provided by the Vulnerability Scoring System (CVSS), maintained by NIST. According to NIST, CVSS defines a vulnerability as a bug, flaw, weakness, or exposure of an application, system device, or service that could lead to a failure of confidentiality, integrity, or availability.

The CVSS enables users to understand a standardized set of characteristics about vulnerabilities. These characteristics are conveyed in the form of a vector composed of three separate metric groups: *base*, *environmental*, and *temporal*. The base metric group is composed of six metrics: Access Vector (AV), Access Complexity (AC), Authentication (Au), Confidentiality (C), Integrity (I), and Availability (A). The base score, ranging from 0 to 10, derives from an equation specified within the CVSS. AV, AC, and Au are often referred to as exploit metrics, and C, I, and A are referred to as impact metrics. Figure 2-11 shows the base metrics used in CVSS (source: NIST CVSS Implementation Guidance). The vector template syntax for the base score is AV:[L,A,N]/AC:[H,M,L]/Au:[M,S,N]/C:[N,P,C]/I:[N,P,C]/A:[N,P,C].

CVSS is a quantitative model that ensures a repeatable accurate measurement while enabling users to see the underlying vulnerability characteristics that were used to generate the scores. Thus, CVSS is well suited as a standard measurement system for industries, organizations, and governments that need accurate and consistent vulnerability impact scores. Example 2-11 shows the information included in the vulnerability announcement labeled CVE-2014-4111 including the CVSS score of (AV:N/AC:M/Au:N/C:C/I:C/A:C).



**Figure 2-11** CVSS Base Metrics (Source: NIST CVSS Implementation Guidance)

**Example 2-11** Vulnerability Announcement CVE-2014-4111

**Original release date:** 09/09/2014

**Last revised:** 09/10/2014

**Source:** US-CERT/NIST

**Overview**

Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability."

**Impact**

**CVSS Severity (version 2.0):**

**CVSS v2 Base Score:** 9.3 (HIGH) (AV:N/AC:M/Au:N/C:C/I:C/A:C)

**Impact Subscore:** 10.0

**Exploitability Subscore:** 8.6

**CVSS Version 2 Metrics:**

**Access Vector:** Network exploitable; Victim must voluntarily interact with attack mechanism

**Access Complexity:** Medium

**Authentication:** Not required to exploit

**Impact Type:** Allows unauthorized disclosure of information; Allows unauthorized modification; Allows disruption of service

**External Source:** MS

**Name:** MS14-052**Type:** Advisory; Patch Information**Hyperlink:** <http://technet.microsoft.com/security/bulletin/MS14-052>

## Threat Intelligence

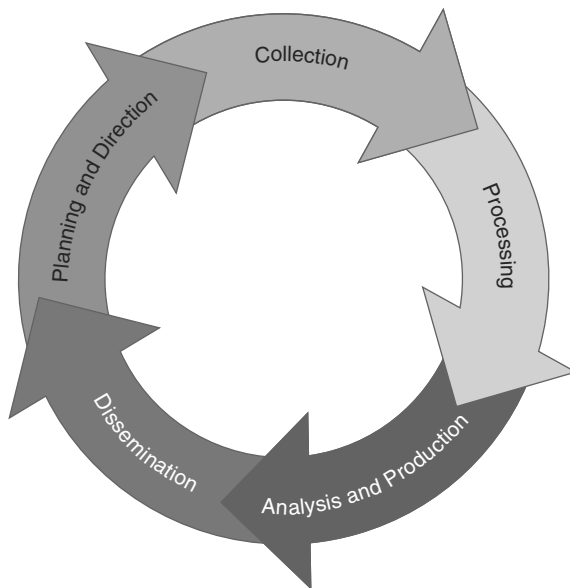
The market's understanding of threat intelligence is evolving. According to Gartner, "Threat intelligence is evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice, about an existing or emerging menace or hazard to assets that you can use to inform decisions regarding the subject's response to that menace or hazard." Forrester defines threat intelligence as "details of the motivations, intent, and capabilities of internal and external threat actors. Threat intelligence includes specifics on the tactics, techniques, and procedures of these adversaries. Threat intelligence's primary purpose is to inform business decisions regarding the risks and implications associated with threats."

Converting these definitions into common language could translate to threat intelligence being evidence-based knowledge of the capabilities of internal and external threat actors. How can this type of data benefit the SOC? The idea is extending security awareness beyond the internal network by consuming intelligence from other sources Internet-wide related to possible threats to your organization. For example, you might hear about a threat that has impacted multiple organizations, and so you can proactively prepare rather than react once the threat is seen against your network. Do not confuse threat intelligence with enrichment data discussed earlier in this chapter. Providing an enrichment data feed is one service that threat intelligence platforms would typically provide.

Forrester defines a five-step threat intelligence cycle, shown in Figure 2-12, for evaluating threat intelligence sources: planning and direction, collection, processing, analysis, and production and dissemination.

In many cases, you will be the consumer for one or more intelligence feeds. A number of threat intelligence platforms that you might want to consider include the following:

- **Cyber Squad ThreatConnect:**<sup>9</sup> An on-premises, private, or public cloud solution offering threat data collection, analysis, collaboration, and expertise in a single platform. Learn more at <http://www.threatconnect.com/>.
- **BAE Detica CyberReveal:** A multithreat monitoring, analytics, investigation, and response product. CyberReveal brings together BAE Systems Detica's heritage in network intelligence, big data analytics, and cyberthreat research. CyberReveal consist of three core components: platform, analytics, and investigator. Learn more at <http://www.baesystems.com/>.
- **Lockheed Martin Palisade:** Supports comprehensive threat collection, analysis, collaboration, and expertise in a single platform. Learn more at <http://www.lockheedmartin.com/>.
- **MITRE CRITs:** Collaborative Research Into Threats (CRITs) is an open source feed for threat data. Learn more at <https://crits.github.io/>.



**Figure 2-12** *Threat Intelligence Cycle According to Forrester*

In addition, a number of standards of schemas are being developed for disseminating threat intelligence information, including the following:

- **Structured Threat Information eXpression (STIX):** An express language designed for sharing of cyberattack information. STIX details can contain data such as the IP address of command-and-control servers (CnC), malware hashes, and so on. Learn more at <http://stix.mitre.org/>.
- **Open Indicators Of Compromise (OpenIOC):** Open framework for sharing threat intelligence in a machine-digestible format. Learn more at <http://www.openioc.org/>.
- **Cyber Observable eXpression (CybOX):** A free standardized schema for specification, capture, characterization, and communication of events of stateful properties that are observable in the operational domain. Learn more at <https://cybox.mitre.org/>.

Transport mechanisms, such as Trusted Automated eXchange of Indicator Information (TAXII), are used to exchange cyberthreat information represented by the previously discussed schemas.

You should define what threat intelligence is best for your security operation. Evaluation criteria could include the benefits it brings, do you plan to consume it, and how threat intelligence will integrate with your SOC technologies and processes, including the automation of this integration. Also, it is important to note that there are many open source and non-security-focused sources that can be leveraged for threat intelligence as well. Some examples are social media sources, forums, blogs, vendor websites, and so on.

## Compliance

Monitoring the compliance of your systems against reference configuration templates or standard system builds gives you an opportunity to detect changes and existing configuration problems that could lead to a possible breach. Sometimes, these issues cannot be seen by common security tools such as vulnerability scanners unless the configuration problem is exploited, which is not the best time to identify the problem. There are also cases in which you might have a policy that forces you to follow some good security practices, such as continuously evaluating against benchmarks set by the Center of Internet Security (CIS) or meeting PCI DSS 2.0.

Many of today's vulnerability scanning tools, such as Qualys, Nessus, and Nexpose, include a compliance module that enables them to remotely log in to a system, collect its configuration, and then analyze that against a reference benchmark. You can also develop your own programs or scripts that can perform the same function.

Automating the system compliance process and then linking it to your risk management and incident response practices are key steps in any successful security operation. An example of including this in your practice is incorporating system compliance as part of the risk assessment and vulnerability assessment steps of the SANS Vulnerability Management Model shown earlier in Figure 2-10.

## Ticketing and Case Management

The SOC team is expected to track potential incidents reported by tools or people. A case must be created, assigned, and tracked until closure to ensure that the incident is properly managed. This activity should be backed up by both, having the right tools, authority, and integration with incident response and case management processes.

SIEM, vulnerability management, and other SOC tools should either support built-in local case management or preferably integrate with your existing IT ticketing system such as BMC Remedy or CA Service Desk Manager, for central management and reporting of trouble tickets. You should work with the help desk team to create new ticket categories with meaningful and relevant security incident ticket fields and attributers.

A key point to consider is that remediation for some events may require resources outside the SOC analysts for business or other technical support. This is why assigning responsibilities that are sponsored by the proper authority is critical for the success of case management. The Responsibility, Accountable, Consulted, and Informed (RACI) matrix can be used as a model for identifying roles and responsibilities during an organization change process. Table 2-4 represents an example RACI chart, where R = Responsible, A = Accountable, C = Consult, and I = Inform.

**Table 2-4** *RACI Matrix Example*

Function	Project Sponsor	Business Analyst	Project Manager	Software Developer
Initiate project	C		AR	
Establish project plan	I	C	AR	C
Gather user requirements	I	R	A	I
Develop technical requirements	I	R	A	I
Develop software tools	I	C	A	R
Test software	I	R	A	C
Deploy software	C	R	A	C

Typical steps to build a RACI matrix are as follows:

- Step 1.** Identify all the processes or activities known as functions on the left side of the matrix.
- Step 2.** List all the roles at the top of the matrix.
- Step 3.** Create values to reference, such as AR, C, I, and R, that will be assigned.
- Step 4.** Verify every process has an R and that there is only one R to avoid conflicts. If there must be more than one R, break up the function until there is only one R per function.

When multiple teams are involved, such as what could end up on your RACI matrix, collaboration between teams becomes mission critical. Let's look at how the SOC can leverage collaboration technologies.

## Collaboration

The SOC should be equipped with a collaboration platform that allows the SOC team to centrally store, manage, and access documents, including system manuals, documented processes, incident response procedures, and so on. The platform can be based on commercial products such as Microsoft SharePoint, or can be a customized web-based platform that is developed to fit your exact needs. The platform should support role-based access control (RBAC) so that you can facilitate for various user-access requirements.

Communication is also important within the SOC and with external resources. Most likely, these tools already exist within the organization, such as e-mail, internal websites, conference products, and mailing lists that can be customized for specific purposes such as bringing together a tiger team when a high-priority incident is seen. An example is the Cisco Emergency Responder 9.0 architecture made up of voice, video, and web collaboration products and customized for incident response situations.

## SOC Conceptual Architecture

To get the best out of your investment, you should operate the various SOC technologies under a cohesive architecture. The architecture should formalize the operation model of SOC in terms of components and relationships.

We propose a reference conceptual architecture in Figure 2-13. The proposed reference architecture formalizes the following:

- The input to the SOC in terms of categorized sources
- The output of the SOC in terms of alerts and actions
- The SOC’s technologies
- The relationship between the technologies
- The areas where measurements can be collected in terms of type, value, and frequency

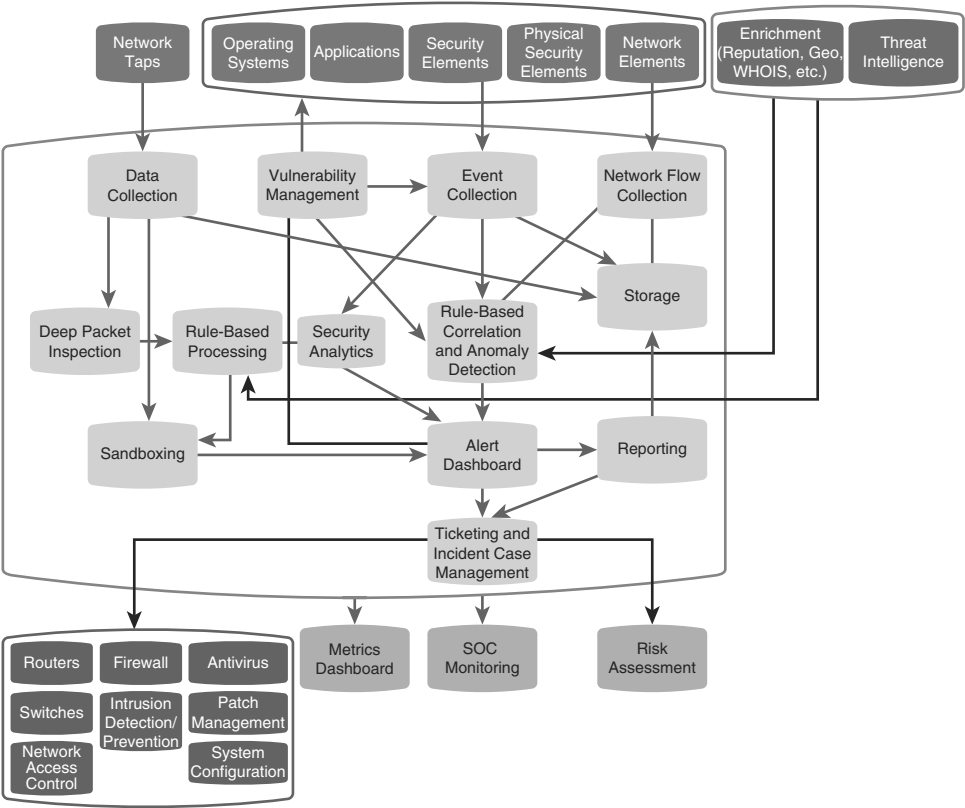


Figure 2-13 SOC’s Conceptual Architecture

We will refer to this architecture and detail its different blocks in various chapters of this book. One other architecture to consider is looking at how SOC responsibilities could be outsourced to a managed service provider. Figure 2-14 represents the Cisco architecture for managed threat defense services targeting customers looking to outsource some or all of their SOC responsibilities.



**Figure 2-14** *Cisco Managed Threat Defense Architecture*

## Summary

This chapter focused on the technology and services associated with most modern SOC environments. The chapter provided an overview of best practices for data collection that covered different data sources, such as syslogs, network telemetry, and packet capturing. The chapter then reviewed how data is processed so that it can be used for security analysis. We included different techniques that can also complement captured data, such as using data enrichment. The next topic covered was vulnerability management, following steps from the SANS Vulnerability Management Model. The chapter concluded with some operation recommendations, such as how to handle case management and collaboration between teams.

Now that you have a good idea about the technologies and services found in a SOC, it is time to look at how these can work together. Next up is Chapter 3, “Assessing Security Operations Capabilities,” which focuses on assessing SOC operational capabilities.

## References

1. The syslog protocol, <http://tools.ietf.org/html/rfc5424>
2. Reliable delivery for syslog, <https://www.ietf.org/rfc/rfc3195.txt>
3. Graylog2, <http://www.graylog2.org>



4. Logstash, <http://www.logstash.net>
5. Elasticsearch ELK, <http://www.elasticsearch.org/overview>
6. Specification of the IP Flow Information Export (IPFIX) Protocol for the Exchange of Flow Information, <http://tools.ietf.org/html/rfc7011>
7. Apache Storm, <https://storm.incubator.apache.org>
8. CVE-IDs - Products & Services by Product Category, [https://cve.mitre.org/compatible/product\\_type.html](https://cve.mitre.org/compatible/product_type.html)
9. ThreatConnect, <http://www.threatconnect.com>

*This page intentionally left blank*

# Index

## A

---

AAA (authentication, authorization, and accounting), 112, 280

acceptances, 196

access. *See also* security

    Cisco Meraki, 154

    control policies, 146

    to data/systems, 25

    facilities, 108

    RDP (Remote Desktop Protocol), 253

    segmentation, 256

    SSH (Secure Shell), 43

    to systems, 112

    type synchronization, 134

access control lists. *See* ACLs

ACLs (access control lists), 165, 249, 260

acoustics, facilities, 107

ACS (annualized cost of safeguard), 197

Act on the Protection of Personal Information (APPI), Japan, 10

Act step (OODA Loop), 2

actions and objectives (Phase 6, cyber kill chain), 3

Active Directory. *See* AD

active infrastructure, 110-120

    collaboration, 119-120

    compute, 116-118

    networks, 111-112

    security, 112-115

    storage, 118

AD (Active Directory), 257, 391

ad hoc reviews, 373

adding debug log messages, 140

Address Resolution Protocol.  
*See* ARP

addresses, MAC (media access control), 256

advanced forensic services, 360

Advanced Malware Protection.  
*See* AMP

advanced persistent threats.  
*See* APTs

alarms, NetFlow, 175

ALE (annualized loss expectancy), 196

**alerts**

AMP (Advanced Malware Protection), configuring, 151

Cisco FirePOWER, 145

discovery rules, 149

Impact Flag Alerting, 148

**AMP (Advanced Malware Protection), 143, 168-169, 258**

alerts, configuring, 151

files, tracking, 150

**analysis, 52-57**

events, 80

incidents, 79

job role, 225

market, 225

maturity level analysis (step 4), 84-86

**analysts**

roles, 224

services, facilities, 109-110

**analytics, 242**

optimization, 392

security, 223

**announcements of vulnerabilities, 60-62**

**annualized cost of safeguard. *See* ACS**

**annualized loss expectancy. *See* ALE**

**annualized rate of occurrence. *See* ARO**

**anomalies**

anomaly-based correlation, 55

system optimization, 388

**antivirus software, 262**

**AnyConnect, 252**

**Apache Hadoop, 57**

**APIs (application programming interfaces), 173**

**application programming interfaces. *See* APIs**

**Application Visibility & Control. *See* AVC**

**applications**

firewalls, 142

infrastructure, 110. *See also* infrastructure

nano configuration utility, 125

**applying maturity models, 29-30**

**APTs (advanced persistent threats), 393-394**

**architecture, 314-317**

Cisco Emergency Responder 9.0, 66

conceptual, 66-67

firewalls, 277-279

managed threat defense, 67

NAC (network access control), 285

networks, 247

proxies, 292

telemetry, 310

**ARO (annualized rate of occurrence), 196**

**ARP (Address Resolution Protocol), 205**

**ASA (Cisco Adaptive Security Appliance), 126, 138-141, 258**

**assessments, 69, 366-381**

budgets, 89

capabilities (step 2), 73-82

configuration, 192

documentation, 84

external, 374-375

formalization of findings (step 5), 87-90

goals, identifying (step 1), 71-73

information collection (step 3), 82-84

- internal, 374
  - inventories, 205
  - maturity level analysis (step 4), 84-86
  - methodologies, 69-90, 375-381
    - maturity models*, 375-376
    - post-incident reviews*, 378-381
    - services-oriented approaches*, 376-378
  - OpenVAS (Open Vulnerability Assessment System), 194
  - presentations, 89
  - risks, 11, 203
  - scope, determining, 366-374
  - threats, 88
  - tools, 206
  - vulnerabilities, 81, 192, 203
- assets**
- information, 390
  - inventories, 203
  - owners, working with, 357
  - value. *See* AV
- assignment, 16**
- attackers**
- skill level of, 198
  - types of, 198
- attacks**
- DoS (denial-of-service), 5, 350
  - incident category (2), 17
  - signatures, 209-210
- attempted access, incident category (4), 17**
- audits, 191-192, 358**
- authentication, 257-258**
- authentication, authorization, and accounting. *See* AAA**
- automation**
- remediation, 394
  - scanning, 192
  - vulnerability management, 205-208
- AutoPlay, disabling, 262**
- AutoRun, disabling, 262**
- autoshutdown, 262**
- AV (asset value), 196**
- availability, HA (high availability), 253-254**
- AVC (Application Visibility & Control), 143**
- average escalation fidelity, 376**
- average incident responses, 376**
- avoiding risk, 196**
- 
- B**
- backups, power failures, 111**
- BAE Detica CyberReveal, 63**
- big data, security, 57**
- Bit9, 258**
- blacklists, 298**
- BMC Remedy, 64**
- Boyd, John, 2**
- breach detection, 5, 168-173**
- design, 300-314
  - discovery services, 223, 242-243
  - endpoints, 263, 303
  - honeypots, 301
  - networks
    - forensics*, 312
    - telemetry*, 306
  - sandboxes, 302
  - system optimization, 388
- bring your own device (BYOD), 7**
- broadcast mode, NTP (Network Time Protocol), 131**

**budgets, 25**  
     assessments, 89  
     capacity planning, 104  
     SOCs (security operations centers), 2  
     strategies, 94  
**buffered logging, 163**  
**building phases, 31**  
**burst capacity, 361**  
**business challenges, cybersecurity, 7-10**  
**business impact factors, 200**  
**BYOD (bring your own device), 7**

## C

---

**CA Service Desk Manager, 64**  
**caches, WCCP (Web Cache Communication Protocol), 292**  
**calculations**  
     EPS (events per second), 124-129  
     maturity levels, 86  
     team numbers, 227-228  
**cameras, CCTV, 108**  
**capabilities, 100**  
     assessments, 69. *See also* assessments  
     development roadmaps, 91, 99-101  
**Capability Maturity Model. *See* CMM**  
**capacity**  
     burst, 361  
     planning, 104, 119  
**capturing**  
     packets, 48-49, 258  
     syslog protocol, 49  
**careers, 386-387. *See also* staffing; teams**

**Carnegie Mellon Software Engineering Institute. *See* SEI**  
**Carnegie Mellon University, 12**  
**case management, 64-65**  
     closing/reporting cases, 362-363  
     incidents, 354-362  
     optimization, 391-392  
**categories of incidents, 17**  
**CCTV cameras, 108**  
**Center of Internet Security. *See* CIS**  
**certification**  
     evaluation, 78  
     JITC (Joint Interoperability Certification), 137  
**Chambers, John, 1**  
**changes, 388. *See also* maintenance**  
**ChangeWave Research, 8**  
**checks to ensure readiness, 332-345**  
**chief information officers (CIOs), 8**  
**CIS (Center of Internet Security), 64**  
     Security Benchmarks for Windows and Macs, 262  
**Cisco Adaptive Security Appliance. *See* ASA**  
**Cisco Cloud Web Security. *See* CWS**  
**Cisco Email Security Appliance. *See* ESA**  
**Cisco Emergency Responder, 66, 272**  
**Cisco FirePOWER, 142-152, 258**  
     exporting from, 144-152  
     IPSs (intrusion prevention systems), 160-161  
     Management Center, configuring, 133  
**Cisco Firepower Management Center. *See* FMC**

Cisco Identity Services Engine. *See* ISE

Cisco Meraki, 153-155, 161-162

Cisco Next-Generation Intrusion Prevention System. *See* NGIPS

Cisco Security Manager. *See* CSM

Cisco WSA (Web Security Appliance), 170-172

classification, initial, 16

clientless VPNs, 252

clients

AnyConnect, 252

NTP (Network Time Protocol), 130

closing

cases, 362-363

incidents, 19-20, 79

cloud

proxies, 172

security, 152-157

*Cisco Meraki, 153-155*

*VMs (virtual firewalls), 155-157*

services, 8

storage, 270-271

clustering firewalls, 276

CMDB (configuration management database), 390

CMM (Capability Maturity Model), 27

CMMI Institute, 27

CnC (command and control), 211

Phase 6, cyber kill chain, 3

COBIT (Control Objectives for Information and related Technology), 27, 71

dependencies, 74

goals, 72

collaboration, 25, 271-273

evaluation, 82

events through, 350-351

infrastructure, 119-120

for pandemic events, 272-273

platforms, 65

TLS (Transport Layer Security), 120

Collaborative Research Into Threats. *See* CRITs

collection, events, 80, 123-152

calculating EPS, 124-129

firewalls, 137-152

NTP (Network Time Protocol), 129-134

tools, 134-137

command and control. *See* CnC

commands

ACLs (access control lists), 260

show logging buffered, 134

Common Vulnerabilities and Exposures. *See* CVEs

communications, 65, 358

events through, 350-351

comparisons of in-house SOC models, 245-246

compliance, 9, 191-192

event collection tools, 137

monitoring, 64

requirements, 87

strategies, 94

components

infrastructure, facilities, 105-110

reference conceptual architecture, 66-67

services, 219-220

compute, 116-118

Computer Incident Response Team (Lockheed Martin), 3

computer rooms, internal layouts of, 106

**Computer Security Incident Response.** *See* CSIRT

conceptual architecture, 66-67

configuration

alerts, 145

AMP (Advanced Malware Protection), 151

assessments, 192

Cisco FirePOWER Management Center, 133

devices to report on syslog/TCP, 165

encryption, performance, 260

nano configuration utility, 125

NetFlow v9, 47-48

NTP (Network Time Protocol), 130-134

syslog protocol

*Cisco IOS routers for, 41*

*Cisco Meraki, 154*

*parameters, 40*

syslog.conf sample configuration, 42

Ubuntu syslog servers, 125

VPs (virtual firewalls), 155-157

configuration management database. *See* CMDB

conformance, incidents, 377

connections, ISPs (Internet service providers), 111

connectivity requirements, 104

console logging, 163

consultants, 83

contractors, working with, 359

contracts, support, 254

control, evaluation, 81

Control Objectives for Information and related Technology. *See* COBIT

coordinated universal time. *See* UTC

Core Impact, 195

correlation

events, 80

rules

*alternatives to, 55-56*

*high-level correlation rule statements, 54*

*Splunk Enterprise Security, 52*

countermeasures, 6

coverage

requirements, 297

services, 221

CRITs (Collaborative Research Into Threats), 63

CSIRT (Computer Security Incident Response), 203, 352

CSM (Cisco Security Manager), 139

custodians, working with, 357

CVEs (Common Vulnerabilities and Exposures), 60, 190, 209

CVSS (Vulnerability Scoring System), 60

CWS (Cisco Cloud Web Security), 172

cyber kill chain, 3

Cyber Observable eXpression. *See* CybOX

Cyber Squad ThreatConnect, 63

cybersecurity

business challenges, 7-10

challenges of, 1-10

threat landscapes, 4-7

cyberthreats, 2

CybOX (Cyber Observable eXpression), 63

cycles of threat intelligence, 63



## D

---

DAPs (dynamic access policies), 253  
 Darknet, 7  
 Data Breach Investigation Report (DBIR), 5  
 data center traffic, 155  
 data centers, NetFlow in, 186-187  
 data collection, 35-51  
 data enrichment, 56  
 data protection, 9-10  
 Data Protection Act 1998 (United Kingdom), 10  
 data sources, 37  
 data-in-motion DLP, 268  
 data-loss protection. *See* DLP  
 data-recovery locations, 105.  
   *See also* facilities  
 databases  
   administrators, 357  
   CMDB (configuration management database), 390  
 DDoS (distributed DoS), 97  
 debug log messages, adding, 140  
 Decide step (OODA Loop), 2  
 decryption, SSL (Secure Sockets Layer), 142  
 dedicated environments, 116-117  
 deep packet inspection engines. *See* DPI engines  
 Delivery (Phase 3, cyber kill chain), 3  
 demilitarize zone. *See* DMZ  
 denial-of-service. *See* DoS attacks  
 dependencies, goals/processes, 73  
 deployment  
   DLP (data-loss protection), 269  
   model of operation, 104

  NAC (network access control), 282  
   web proxies, 294  
 depth, 389  
 design, 273-300  
   breach detection, 300-314  
   firewalls, 273-279  
   infrastructure, 103-104  
   NAC (network access control), 281-289  
   routers/switches, 279-281  
   SCIF (Sensitive Compartmented Information Facility), 108  
   services, 368  
   teams, 218-231  
   technologies  
     *IDSs (intrusion detection systems)*, 295-300  
     *IPSs (intrusion prevention systems)*, 295-300  
   Web proxies, 290-295  
   workstations, 110  
 detection  
   anomalies, 55  
   breach, 168-173. *See also* breach detection  
   endpoints, 263  
 development  
   employee development programs, 369  
   roadmaps, 91, 99-101  
   strategies, 91  
   teams, 384  
 devices, 37  
   hardening, 280  
   mobile, 167-168, 264  
   security, 280  
   USB memory, 14

**DHCP (Dynamic Host Configuration Protocol)**, 205, 391

**digital forensic tools**, 313

**directory information**, 391

**disabling**

AutoPlay, 262

AutoRun, 262

services, 262

**discovery**

breach discovery services, 242-243

rules, 149

time, 5

VDS (vulnerability discovery service), 222

vulnerabilities, 80

**distributed DoS. *See* DDoS**

**DLP (data-loss protection)**, 73, 266-270

**DMVPN (Dynamic Multipoint VPN)**, 251

**DMZ (demilitarize zone)**, 247, 292

**DNS (Domain Name System)**, 24, 173-174, 205, 391

**documentation**

assessments, 84

incidents, 15

processes, 234-235

services, 370-372

strategies, 92

**DoD Risk Management Framework (RMF)**, 11

**Domain Name System. *See* DNS**

**door access control equipment**, 108

**DoS (denial-of-service) attacks**, 5, 17, 350

**DPI (deep packet inspection) engines**, 49

**dynamic access policies. *See* DAPs**

**Dynamic Host Configuration Protocol. *See* DHCP**

**Dynamic Multipoint VPN. *See* DMVPN**

## E

---

**eastern standard time. *See* EST**

**Easy VPN**, 251

**Economist Intelligence Unit report (2014)**, 348

**education, management of**, 384-385

**EF (exposure factor)**, 196

**elements of strategies**, 91-95

**e-mail**, 74

DLP (data-loss protection), 267

ESA (Cisco Email Security Appliance), 268

**emergency response services**, 360

**employee development programs**, 369

**enabling**

logging, 164

NetFlow, 177, 308

**encryption**, 259-260

**Endgame Systems**, 7

**endpoints**

breach detection, 263, 303

DLP (data-loss protection), 267

hardening, 262

management, 167

**end-user support**, 357

**enforcement**, 3

**engineering**

roles, 224

security, 361

SSE (security services engineering), 237-238

enrichment (data), 56, 390-391  
 enterprise service management processes, 232-234  
 entries, removing Registry, 262  
 EPS (events per second), 44, 117, 124, 349  
     calculating, 124-129  
 ESA (Cisco Email Security Appliance), 73, 268  
 escalation, average fidelity, 376  
 EST (eastern standard time), 131  
 evaluation. *See also* assessments  
     collaboration, 82  
     control, 81  
     events, 80  
     governance, 77  
     incidents  
         *analysis*, 79  
         *closure*, 79  
         *reporting*, 79  
         *triage*, 79  
     IT processes, 75, 84-86  
     log management, 81  
     monitoring, 81  
     network readiness, 80  
     people, 76  
     post-incident activities, 79  
     processes, 78  
     SOC experience, 77  
     structures, 77  
     technologies, 80  
     ticketing, 82  
     training, 78  
     vulnerabilities  
         *assessment*, 81  
         *discovery*, 80

*remediation*, 80

*tracking*, 80-81

## events

case management, 354-362  
 collaboration, 350-351  
 collection, 80, 123-152  
     *calculating EPS*, 124-129  
     *firewalls*, 137-152  
     *NTP (Network Time Protocol)*, 129-134  
     *tools*, 134-137  
 communications, 350-351  
 generating, 123  
 logging, syslog protocols, 40  
 malware, 351-352  
 management, 232  
 in original habitats, 350  
 overview of, 348  
 reporting, 353-354  
 responses, 347  
 in security log management service, 350  
 in SIEM (security information and event management), 349  
 sources, 391

events per second. *See* EPS

executive sponsorship, 24

## exercises

incident category (0), 17  
 teams, 385-386

existing controls, risk assessments, 12

expected loads, 221

experience, 25

Exploitation (Phase 4, cyber kill chain), 3

**exporting**

- ASA data, 139
- from Cisco FirePOWER, 144-152
- data from Stealthwatch, 179-182
- DNS (Domain Name System), 174
- logs, 154-155, 171
- syslog messages, 157

**exposure factor.** *See* EF

**external assessments,** 374-375

## F

---

**facilities, 105-110**

- acoustics, 107
- analyst services, 109-110
- lighting, 107
- physical security, 108
- SOC internal layouts, 106-108
- video walls, 108-109

**failover,** 254

**FC (Fiber Channel),** 118

**Federal Data Protection Act (Germany),** 10

**feeds**

- reputation, 391
- threats, 210-211

**Fiber Channel.** *See* FC

**fidelity, average escalation,** 376

**files**

- log, Linux, 42
- permissions, 262
- tracking, 150

**filtering URLs,** 143

**financial constraints of services,** 221

**financial organization strategies,** 95

**FireEye,** 258

**FirePower (Cisco).** *See* Cisco FirePOWER

**firewalls, 113, 255**

- applications, 142
- architecture, 277-279
- ASA (Cisco Adaptive Security Appliance), 126, 138-141
- Cisco FirePOWER, 142-152
- clustering, 276
- design, 273-279
- event collection, 137-152
- HA (high availability), 276
- host, 157
- modes, 273-276
- stateful, 137-140
- stateless, 137-140
- VMs (virtual firewalls), 155-157

**flooring, internal layouts (facilities),** 106

**flows, networks,** 45-48

**FMC (Cisco Firepower Management Center),** 113, 143

- access control policies, 146
- alerts, configuring, 145
- discovery rules, 149

**forensics**

- networks, 312
- services, 360

**form factors,** 297

**formalization of findings (step 5),** 87-90

**formulas,** 128. *See also* calculations

**FQDN (fully qualified domain name),** 131, 173

**front-line SOC monitoring,** 360

**FTP (File Transfer Protocol),** 280

**fully qualified domain name.** *See* FQDN

## G

---

generating events, 123  
generations of SOCs (security operations centers), 21-24  
generic routing encapsulation. *See* GRE  
Germany, Federal Data Protection Act, 10  
GET-VPN, 251  
goals  
    COBIT (Control Objectives for Information and related Technology), 72  
    identifying (step 1), 71-73  
    strategies, 91  
governance, 25, 77  
GRE (generic routing encapsulation), 251

## H

---

HA (high availability), 253-254, 276  
habitats, events in original, 350  
hacking, 1  
Hadoop Distributed File System. *See* HDFS  
handling  
    incident reports, 353-354  
    vulnerabilities, 195-204  
hardening  
    devices, 280  
    endpoints, 262  
hardware  
    ISE (Cisco Identity Services Engine), 285  
    requirements, 104

HDFS (Hadoop Distributed File System), 37  
heat maps, 13  
help desks, 83, 358  
Hidden Wiki, 7  
high availability. *See* HA  
high-level correlation rule statements, 54  
histories of previous information security incidents, 89  
honeypots, 301  
hosts  
    firewalls, 157  
    host-based intrusion prevention, 162  
    host-based VPNs, 252  
    systems, 166  
HR (human resources), 225-228, 358

## I

---

IA (information assurance), 10-11  
identifying  
    risks, 196  
    security services, 191-193  
    vulnerabilities, 190-191  
IDSs (intrusion detection systems), 49, 113, 157-162  
    design, 295-300  
Impact Flag Alerting, 148  
impact of risk assessments, 12  
incidents. *See also* events  
    analysis, 79  
    case management, 354-362  
    categories, 17  
    closure, 19-20, 79  
    conformance, 377

- CSIRT (Computer Security Incident Response), 203
- detection, 15
- history of previous information security, 89
- incident response. *See* IR
- management, 233
- post-incident
  - activities*, 79
  - reviews*, 20, 378-381
- reporting, 79, 353-354
- resolutions, 18-19
- responses, 347
- RTIR (Request Tracker for Incident Response), 353
- severity of, 17-18
- SIIR (security incident investigation and response service), 239-240
- triage, 16, 79
- indicators of compromise (IOC)**, 14, 388
- information assurance.** *See* IA
- information collection (step 3)**, 82-84
- information management**, 203
  - tools, 206
- information security management systems.** *See* ISMSs
- Information Technology Infrastructure Library.** *See* ITIL
- infrastructure**, 103
  - active, 110-120
  - collaboration, 119-120
  - compute, 116-118
  - design, 103-104
  - facilities, 105-110
    - analyst services*, 109-110
    - physical security*, 108
    - video walls*, 108-109
  - logging, 44-45
  - model of operation, 104-105
  - networks, 111-112
  - readiness, 80
  - security, 112-115
  - storage, 118-104
- in-house SOC models**, 96-98, 245-246
- initial classification**, 16
- installation**
  - event collection tools, 136
  - Phase 5, cyber kill chain, 3
  - Ubuntu syslog servers, 125
- integration**
  - IDS/IPS systems, 113
  - technologies, 392
- intelligence**
  - platforms, 211-213
  - security, 241-242
  - threats, 62-63, 208-213, 360, 391
  - vulnerabilities, 360, 391
- interfaces**
  - APIs (application programming interfaces), 173
  - event collection tools, 136
  - Tor browsers, 7
- internal assessments**, 374
- internal layouts (facilities)**, 106-108
  - computer rooms, 106
  - flooring, 106
  - management offices, 106
  - war rooms, 106
- Internet service providers.** *See* ISPs
- intrusion detection systems.** *See* IDSs
- intrusion prevention systems.** *See* IPSs

**inventories**

assessments, 205

assets, 203

**investigations**incidents. *See also* incidents*category (5), 17**reports, 353-354*

optimization, 391-392

SIIR (security incident investigation and response service), 239-240

**investments, model of operation, 104****IP Flow Information eXport. *See* IPFIX****IP Security. *See* IPSec****IPFIX (IP Flow Information eXport), 45****IPSec (IP Security), 251****IPSs (intrusion prevention systems), 12, 113, 157-162, 192**

Cisco FirePOWER, 160-161

Cisco Meraki, 161-162

subscriptions, 143

**IR (incident response), 14-21**

detection, 15

**ISE (Cisco Identity Services Engine), 205, 257, 285****ISMSs (information security management systems), 9, 236, 381****ISO/IEC 27001:2013, 9****ISO/IEC 27005:2010, ISO/IEC 31000:2009, 11****ISPs (Internet service providers), 111****IT (information technology). *See also* assessments**active infrastructure, 110-120. *See also* active infrastructure

dependencies, 73

management processes, 233

process evaluation, 84-86

**ITIL (Information Technology Infrastructure Library), 367, 382**

---

**J****Japan, Act on the Protection of Personal Information (APPI), 10****JITC (Joint Interoperability Certification), 137, 191**job role analysis, 225. *See also* staffing**Joint Interoperability Certification. *See* JITC**

---

**K****Kali Linux, 194**

key cards, 256

key challenges, people, 215-217

key performance indicators. *See* KPIs

known-unknown zero-day vulnerabilities, 7

KPIs (key performance indicators), 91, 382

---

**L****Lancope StealthWatch, 114**

landscapes, threat, 4-7

layers of segmentation, 248

layouts of internal (facilities), 106-108

**LDAP (Lightweight Directory Access Protocol), 56, 120, 177**

leadership roles, 224

leakage, VLAN, 249

learning, management of, 384-385

**legal, working with, 358**

**levels**

logging

*security, 40*

*values, 126*

services, 221

**lifecycles**

PDCA (plan, do, check and act), 381

vulnerability management, 202-204

**lighting, facilities, 107**

**Lightweight Directory Access Protocol. *See* LDAP**

**Linux, log files, 42**

**location strategies, 93**

**Lockheed Martin**

Computer Incident Response Team,  
3

Palisade, 63

**log files**

Linux, 42

security log management, 240-241

**log management, 81**

**logging, 36**

buffered, 163

console, 163

debug log messages, adding, 140

enabling, 164

events, syslog protocols, 40

infrastructure, 44-45

levels, values, 126

messages, 22, 37

options, 138, 163

recommendations, 43

security levels, 40

syslog servers, 164

terminal, 163

**Logstash, 50-51**

**LOIC (Low Orbit Ion Cannon), 5**

**Low Orbit Ion Cannon (LOIC), 5**

## M

---

**M2M (machine-to-machine), 7**

**MAC addresses, 256**

**machine-to-machine. *See* M2M**

**maintenance, 365, 381-395**

event collection tools, 136

monitoring, 388

services, 381-383

teams, 383-387

technologies, 387-395

**malicious code, incident category (3),  
17**

**malware, 168-169, 351-352**

**managed service providers, working  
with, 360**

**managed threat defense architecture,  
67**

**management**

case, 64-65

CMDDB (configuration management  
database), 390

endpoint, 167

events, 232

incidents, 233, 354-362

information, 203

MDM (Mobile Device  
Management), 167-168

offices, 106

problem, 233

requirements, 297

risk, 11-13, 357

SANS Vulnerability Management  
Model, 64, 202, 207

security log, 240-241



- skills, 384-385
- SSM (security services management), 221, 236-237
- strategies, 92
- teams, 355-357
- transitions, 321-345
  - checks to ensure readiness, 332-345*
  - planning, 322*
  - project resources, 328-329*
  - requirements, 329-332*
  - success criteria, 322-328*
- vulnerabilities, 24, 58-62, 189-190, 233, 241
  - automating, 205-208*
  - handling, 195-204*
  - identifying, 190-191*
  - lifecycles, 202-204*
  - OWASP Risk Rating Methodology, 197-202*
  - security services, 191-193*
  - tools, 193-195*
- maps, risk heat, 202
- market analysis, 225
- matrices, RACI, 64-65, 83
- maturity level analysis (step 4), 84-86
- maturity models, 27-28, 71
  - applying, 29-30
  - assessments, 375-376
  - scoring, 86
- MDM (Mobile Device Management), 167-168, 264
- measurements, EPS on Ubuntu syslog servers, 124-129
- memory, USB devices, 14
- messages
  - debug log, adding, 140
  - logging, 22, 37
  - parsing, 51
- SNMP (Simple Management Network Protocol), 256
- SSH (Secure Shell), 43
- syslog, 42, 125, 157
- Metasploit, 194**
- methodologies, assessments, 69-90, 375-381
- metrics, ITIL (Information Technology Infrastructure Library), 382
- Microsoft Active Directory, 22
- migrations, 388-389
- military organization strategies, 94
- mirroring ports, 49
- mission statements, 91-92, 218-219
- mitigation, 196
- MITRE, 60, 63
- Mobile Device Management. *See* MDM
- mobile devices, 167-168, 264
- models
  - in-house SOC, 96-98
  - infrastructure, 104-105
  - maturity, 27-28
  - of operations, 91, 94-98
  - SANS Vulnerability Management Model, 202, 207
  - technologies, 246
  - virtual SOC, 96-98
- modes, firewalls, 273-276
- monitoring, 3, 9, 36
  - compliance, 64
  - evaluation, 81
  - front-line SOC, 360
  - maintenance, 388
  - networks, 246
  - security, 220, 239

## N

---

**NAC (network access control)**, 205, 255-257, 394

architecture, 285

deployment, 282

design, 281-289

posture, 284

**nano configuration utility**, 125

**NAP (network access protection)**, 262

**NAS (network-attached storage)**, 118

**NAT (Network Address Translation)**, 128, 138, 259

**National Institute of Standards and Technology**. *See* NIST

**Nessus**, 64, 194

**NetFlow**

configuring, 47-48

in data centers, 186-187

enabling, 308

routers/switches, 182-184

from security products, 184-186

StealthWatch, 177-182

tools, 175-182

**Netragard**, 7

**network access control**. *See* NAC

**network access protection**. *See* NAP

**Network Address Translation**. *See* NAT

**network administrators**, 357

**network-attached storage**. *See* NAS

**Network and Information Security**. *See* NIS

**network operations center**. *See* NOC

**Network Time Protocol**. *See* NTP

**networks**, 246-254

active infrastructure, 111-112

architecture, 247

DLP (data-loss protection), 267

flows, 45-48

forensics, 312

HA (high availability), 253-254

overhead, 36

readiness, 80

SANs (storage-area networks), 118

segmentation, 247-250

strategies, 93

support contracts, 254

taps, 49

telemetry, 306, 310

VPNs (virtual private networks), 248, 251-253

WANs (wide-area networks), 45

**Networkworld.com**, 6

**Nexpose**, 64

**NGIPS (Cisco Next-Generation Intrusion Prevention System)**, 210

**NIS (Network and Information Security)**, 137

**NIST (National Institute of Standards and Technology)**, 10-11

NIST 800-70, 262

**NIST SP 800-39**, 11

**Nmap**, 194

**NOC (network operations center)**, 105

**normalization**, 49-51, 349. *See also* events

**North American Electric Reliability Corporation Critical Information Protection (NERC CIP)**, 118

**NSA Security Configuration Guide**, 262

**NTP (Network Time Protocol)**, 38, 129-134

**numbers, calculating teams**, 227-228

## O

---

Observe step (OODA Loop), 12  
 offices, 106. *See also* facilities  
 on-network security, 258-259  
 OODA Loop, 2, 4  
 Open Indicators Of Compromise. *See* OpenIOC  
 Open Vulnerability Assessment System. *See* OpenVAS  
 Open Web Application Security Project. *See* OWASP Risk Rating Methodology  
 OpenIOC (Open Indicators Of Compromise), 63  
 OpenVAS (Open Vulnerability Assessment System), 194  
 operating systems, 118, 261  
 Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE), 12  
 operations, 319  
   documentation, 370-372  
   key challenges, 319-321  
     *people*, 319-320  
     *processes*, 320  
     *technologies*, 321  
   models of, 91, 94-98  
   roles, 224  
   services, 369  
   transition management, 321-345  
 opportunities, 198  
 optimization, 365, 381-395  
   analytics, 392  
   careers, 386-387  
   case management, 391-392  
   data collection, 36  
   enrichment (data), 390-391

  investigations, 391-392  
   remediation, automating, 394  
   reporting, 392  
   services, 381-383  
   simulation systems, 393-394  
   teams, 383-387  
   technologies, 387-395  
   testing, 393-394  
 options, logging, 138, 163  
 organization strategies, 94  
 organizational structures, 226  
 Orient step (OODA Loop), 2  
 outsourcing, 104-105, 359  
 overhead, 36  
 OWASP Risk Rating Methodology, 11, 197-202  
 ownership strategies, 93

## P

---

P2M (person-to-machine), 7  
 P2P (person-to-person), 7  
 packets  
   capturing, 48-49, 258  
   stateful packet inspection, 138  
 pandemic events, collaboration, 272-273  
 parameters, configuring syslog protocol, 40  
 parsing, 36, 49-51  
 passphrases, 262  
 passwords, 262  
 PAT (Port Address Translation), 138  
 patching systems, 262  
 patterns, regex, 51  
 PCI DSS (Payment Card Industry Data Security Standard), 9, 137, 191

**PCI SSC (PCI Security Standards Council), 9**

**PDCA (plan, do, check and act) lifecycles, 9, 381**

**peak EPS, accommodating, 128**

**penetration tests, 192-193**

**people, 215. *See also* staffing**  
checking for transition readiness, 332-336

evaluation, 76

HR (human resources), 225-228

key challenges, 215-217

operation challenges, 319-320

resource strategies, 228-231

roles, 223-225

teams, building, 218-231

**performance**

encryption, 260

requirements, 296

**permissions, 262**

**person-to-machine. *See* P2M**

**person-to-person. *See* P2P**

**personnel/staffing, 369-370**

**phases**

building, 31

of cyber kill chains, 3

incident detection, 15

**physical devices, 37**

**physical security of facilities, 108**

**PIN codes, 256**

**plan, do, check and act lifecycles. *See* PDCA lifecycles**

**planning**

capacity, 104, 119

transitions, 322

**platforms**

big data, 57

collaboration, 65

threat intelligence, 84, 211-213

**PMO (project management office), 83**

**policies**

access control, 146

software restriction, 262

**Port Address Translation. *See* PAT**

**ports**

mirroring, 49

security, 256

SPAN (Switched Port Analyzer), 174

**post-incident. *See also* incidents**

activities, 79

reviews, 20, 378-381

**posture, NAC (network access control), 284**

**power failures, 111**

**presentations of assessments, 89**

**prevention, malware, 168-169**

**privacy, 9-10**

**probabilities, risk assessments, 12**

**probes, incident category (4), 17**

**problem management, 233**

**procedures, 25, 231-243**

documentation, 370-372

examples of, 236-243

**processes, 25, 215, 231-243**

documentation, 234-235, 370-372

enterprise service management, 232-234

evaluation, 78

examples of, 236-243

impact of, 217

IT evaluation, 84-86

operation challenges, 320

transition readiness, checking for, 336-340

weight of, 216-217

Product Security Incident Response Team. *See* PSIRT

programs, operating as, 25

project management office. *See* PMO

project resource management, 328-329

protection (data), 9-10

protocols, 36

- ARP (Address Resolution Protocol), 205
- DHCP (Dynamic Host Configuration Protocol), 205, 391
- FTP (File Transfer Protocol), 280
- IPFIX (IP Flow Information eXport), 45
- LDAP (Lightweight Directory Access Protocol), 56, 120, 177
- NTP (Network Time Protocol), 38, 129-134
- RADIUS (Remote Authentication Dial-In User Service), 112
- RDP (Remote Desktop Protocol), 253
- SCP (Security Copy Protocol), 280
- SMTP (Simple Mail Transfer Protocol), 141
- SNMP (Simple Management Network Protocol), 22, 141, 256
- SNTP (Simple Network Time Protocol), 129
- syslog, 39-43
- TACACS (Terminal Access Controller Access Control System), 112
- TCP (Transmission Control Protocol), 165
- UDP (User Datagram Protocol), 40, 130
- WCCP (Web Cache Communication Protocol), 292

provisioning, 252

proxies

- architecture, 292
- cloud, 172
- Web, 169-170, 290-295

PSIRT (Product Security Incident Response Team), 209

## Q

---

Qualys, 64

queue backlogs, ticketing, 377

## R

---

RACI (Responsibility, Accountable, Consulted and Informed) matrix, 64-65, 83, 368

RADIUS (Remote Authentication Dial-In User Service), 112

rates, EPS (events per second), 44

ratings, OWASP Risk Rating Methodology, 197-202

RBAC (role-based access control), 65

RDP (Remote Desktop Protocol), 253

readiness

- checks to ensure, 332-345
- networks, 80

recommendations, logging, 43

Reconnaissance (Phase 1, cyber kill chain), 3

recruitment, staff, 383-384. *See also* staffing

reference conceptual architecture, 66-67

regex patterns, 51

Registry, removing entries, 262

**relationships, reference conceptual architecture, 66-67**

**remediation, 204, 242-243**

automating, 394

tools, 206

vulnerabilities, 80

**Remote Authentication Dial-In User Service. *See* RADIUS**

**Remote Desktop Protocol. *See* RDP**

**remote SPAN. *See* RSPAN**

**removing Registry entries, 262**

**reporting, 204, 242**

access control policies, 146

cases, 362-363

Economist Intelligence Unit report (2014), 348

events, 353-354

incidents, 79

optimization, 392

requirements, 297

services, 223

tools, 206

**reputation**

feeds, 391

security, 290

**Request Tracker for Incident Response. *See* RTIR**

**requirements**

compliance, 87

connectivity, 104

data collection, 36

event collection tools, 137

hardware, 104

management, 297

performance, 296

reporting, 297

transition management, 329-332

**resolution of incidents, 18-19**

**resources, 198**

strategies, 94, 228-231

**responses, 204**

average incident, 376

CSIRT (Computer Security Incident Response), 203

emergency response services, 360

events, 347

incidents, 347

IR (incident response), 14-21

RTIR (Request Tracker for Incident Response), 353

SIIR (security incident investigation and response service), 239-240

tools, 207

**Responsibility, Accountable, Consulted and Informed matrix. *See* RACI matrix**

**retention, teams, 386**

**retrospection, 389**

**reviews, 365-381. *See also* assessments**

ad hoc, 373

post-incident, 20, 378-381

scheduling, 373

scope, determining, 366-374

services

*continuous improvement, 369*

*design, 368*

*documentation, 370-372*

*examining, 367*

*operations, 369*

*personnel/staffing, 369-370*

*strategies, 367*

*technologies, 372-373*

*transitions, 368*

**ReVuln, 7****risks**

- assessments, 203
- heat maps, 13, 202
- identifying, 196
- management, 11-13, 357
- OWASP Risk Rating Methodology, 197-202
- tools, 206
- VLANs (virtual LANs), 249

**roadmaps**

- design, 103-104
- development, 91, 99-101

**role-based access control. *See* RBAC****roles**

- of strategy builders, 92
- of syslog protocols, 39
- teams, 223-225

**rotation settings, log, 43****routers, 163-166**

- design, 279-281
- NetFlow, 47-48, 182-184

**RSPAN (remote SPAN), 49****rsyslog.con sample configuration, 42****RTIR (Request Tracker for Incident Response), 353****rules**

- correlation, alternatives to, 55-56
- discovery, 149
- firewalls, 113
- high-level correlation rule statements, 54
- IPs (intrusion prevention systems), 113
- segmentation, 113
- Splunk Enterprise Security correlation, 52

---

**S**

---

**SaaS (Software as a Service), 136, 152****safeguard value. *See* SV****sandboxes, 6, 167, 302****SANs (storage-area networks), 118**

- SANS Vulnerability Management Model, 64, 202, 207

**Sarbanes-Oxley (SOX), 118****SCADA (supervisory control and data acquisition), 38****scanning, 192**

- incident category (4), 17

**scheduling reviews, 373****SCIF (Sensitive Compartmented Information Facility), 108****scope, 91, 93-94**

- determining, 366-374
- widening, 389

**scoring maturity models, 86****SCP (Security Copy Protocol), 280****screen lock timers, 262****Secure Shell. *See* SSH****Secure Sockets Layer. *See* SSL****Secure Sockets Layer/Transport Layer Security. *See* SSL/TLS****security, 255-260**

- analytics, 223
- authentication, 257-258
- big data, 57
- cloud, 152-157
  - Cisco Meraki*, 153-155
  - VMs (virtual firewalls)*, 155-157
- CSIRT (Computer Security Incident Response), 203
- devices, 280

- encryption, 259-260
- engineering, 361
- facilities, 108
- firewalls, 255
- infrastructure, 112-115
- intelligence, 241-242
- logging
  - level values*, 126
  - levels*, 40
  - management*, 240-241
- monitoring, 220, 239
- NAC (network access control), 255-257
- on-network, 258-259
- operations, 361
- ports, 256
- products, NetFlow from, 184-186
- reputation, 290
- services, 191-193
- teams, 357
- Security Copy Protocol.** *See* SCP
- security group tags.** *See* SGTs
- security incident investigation and response service.** *See* SIIR
- security information and event management.** *See* SIEM
- security information management.** *See* SIM
- security log management service.** *See* SLMS
- security services engineering.** *See* SSE
- security services management.** *See* SSM
- security services operations.** *See* SSO
- segmentation**
  - access, 256
  - networks, 111, 247-250
  - rules, 113
- SEI (Carnegie Mellon Software Engineering Institute), 27**
- selecting operating systems, 118**
- SEM function, 23**
- Sensitive Compartmented Information Facility.** *See* SCIF
- servers, 264-265**
  - DLP (data-loss protection), 267
  - DNS (Domain Name System), 173-174
  - FQDN (fully qualified domain name), 131, 173
  - NTP (Network Time Protocol), 130
  - SNMP (Simple Management Network Protocol), 164
  - syslog, logging, 164
  - Ubuntu syslog, 124-129
- service level agreements.** *See* SLAs
- services, 36, 98-99**
  - AAA (authentication, authorization, and accounting), 112
  - analysts, facilities, 109-110
  - breach discovery, 223, 242-243
  - cloud, 8
  - components, 219-220
  - continuous improvement, 369
  - coverage, 221
  - design, 368
  - disabling, 262
  - documentation, 370-372
  - emergency response, 360
  - focus on (team building), 219-223
  - forensic, 360
  - levels, 221
  - maintenance, 381-383
  - model of operation, 104
  - operations, 369
  - outsourcing, 104-105



- personnel/staffing, 369-370
- remediation, 242-243
- reporting, 223
- reviewing, 367
- security, 191-193
- SIIR (security incident investigation and response service), 222
- SLMS (security log management service), 222
- SSE (security services engineering), 222, 237-238
- SSM (security services management), 221, 236-237
- SSO (security services operations), 222, 238
- strategies, 91, 367
- technologies, 372-373
- transitions, 368
- TVIS (threat and vulnerability intelligence service), 223
- VDS (vulnerability discovery service), 222
- VINES (Virtual Integrated Network Service), 129
- services-oriented assessments, 376-378
- severity of incidents, 17-18
- SGTs (security group tags), 112
- show logging buffered command, 134
- SIEM (security information and event management), 22-23, 31, 114, 134, 349
- signatures, attacks, 209-210
- SIIR (security incident investigation and response service), 222, 239-240
- SIM (security information management), 23
- Simple Mail Transfer Protocol. *See* SMTP
- Simple Management Network Protocol. *See* SNMP
- Simple Network Time Protocol. *See* SNTP
- simulation systems, optimization, 393-394
- single loss expectancy. *See* SLE
- skills
  - level of attackers, 198
  - management, 384-385
  - sets, 25
- SLAs (service level agreements), 79, 95
- SLE (single loss expectancy), 196
- SLMS (security log management service), 222
- SMTP (Simple Mail Transfer Protocol), 141
- SNMP (Simple Management Network Protocol), 22, 141, 164, 256
- Snort, 162
- SNTP (Simple Network Time Protocol), 129
- SOCs (security operations centers)
  - budgets, 2
  - building phases, 31
  - characteristics of, 24-26
  - generations, 21-24
- Software as a Service. *See* SaaS
- Software Engineering Institute (SEI), 12
- software restriction policies, 262
- SPAN (Switched Port Analyzer), 174
- Splunk
  - Enterprise Security correlation rules, 52
  - recommended configurations, 117

sponsorship, 89

SSE (security services engineering),  
222, 237-238

SSH (Secure Shell), 43, 112, 280

SSL (Secure Sockets Layer), 112, 142

SSL/TLS (Secure Sockets Layer/  
Transport Layer Security), 259

SSM (security services management),  
221, 236-237

SSO (security services operations),  
222, 238

staffing, 369-370, 383-387. *See also*  
teams

stakeholders, 71-72

standards, IPFIX (IP Flow  
Information eXport), 45

stateful firewalls, 137-140

stateless firewalls, 137-140

statements

high-level correlation rule, 54  
mission, 218-219

StealthWatch, 114, 177-182

steps of OODA Loops, 2

sticky MAC, switches, 256

STIX (Structured Threat Information  
eXpression), 63

storage, 265-271

cloud, 270-271

data collection, 36

DLP (data-loss protection), 266-270  
infrastructure, 118

storage-area networks. *See* SANs

strategies, 91

elements of, 91-95

OODA Loop, 2, 4

resources, 228-231

services, 367

structure evaluation, 77

Structured Threat Information  
eXpression. *See* STIX

subscriptions, 143

AMP (Advanced Malware  
Protection), 143

success criteria of transition manage-  
ment, 322-328

supervisory control and data acqui-  
sition. *See* SCADA

support

contracts, 254

end-user, 357

requirements, 297

roles, 224

SV (safeguard value), 197

Switched Port Analyzer. *See* SPAN

switches, 163-166

design, 279-281

NetFlow, 182-184

sticky MAC, 256

symmetric active/passive mode, NTP,  
130

synchronization of NTP, 130-134

syslog protocol, 39-43

alerts, configuring, 146

capturing, 49

messages, 125

messages, exporting, 157

syslog servers

devices, configuring to report on,  
165

logging, 164

systems, 260-265

access to, 112

administrators, 357

endpoint breach detection, 263

hardening endpoints, 262

mobile devices, 264

operating systems, 261

overhead, 36

servers, 264-265

## T

---

TACACS (Terminal Access  
Controller Access Control  
System), 112

taps, networks, 49

TAXII (Trusted Automated eXchange  
of Indicator Information), 63

TCP (Transmission Control Protocol),  
165

teams, 215. *See also* people

building, 218-231

exercises, 385-386

HR (human resources), 225-228

maintenance, 383-387

management, 355-357

numbers, calculating, 227-228

personnel/staffing, 369-370

retention, 386

roles, 223-225

security, 357

training, 384

technical impact factors, 200

technologies, 245

analysis, 52-57

architecture, 314-317

checking for transition readiness,  
340-345

collaboration, 271-273

data collection, 39-51

data sources, 37

design, 273-300

*breach detection*, 300-314

*firewalls*, 273-279

*IDSs (intrusion detection  
systems)*, 295-300

*IPSs (intrusion prevention  
systems)*, 295-300

*NAC (network access control)*,  
281-289

*routers/switches*, 279-281

*Web proxies*, 290-295

evaluation, 80

in-house *versus* virtual SOC's,  
245-246

integration, 392

maintenance, 387-395

networks, 246-254

*HA (high availability)*, 253-254

*segmentation*, 247-250

*support contracts*, 254

*VPNs (virtual private  
networks)*, 251-253

normalization, 49-51

operational challenges, 321

for pandemic events, 272-273

parsing, 49-51

reviews, 372-373

security, 255-260

*authentication*, 257-258

*encryption*, 259-260

*firewalls*, 255

*NAC (network access control)*,  
255-257

*on-network*, 258-259

storage, 265-271

*cloud*, 270-271

*DLP (data-loss protection)*,  
266-270

strategies, 94

systems, 260-265

*endpoint breach detection*, 263

- hardening endpoints*, 262
- mobile devices*, 264
- operating systems*, 261
- servers*, 264-265
- telemetry, networks**, 45-48, 306
  - packet capture, 48-49
- Terminal Access Controller Access Control System**. *See* TACACS
- terminal logging**, 163
- testing**
  - optimization, 393-394
  - penetration, 192-193
- third parties, working with**, 359-362
- threat and vulnerability intelligence service**. *See* TVIS
- threats**, 2
  - agent factors, 198
  - assessments, 88
  - attack signatures, 209-210
  - descriptions of risk assessments, 12
  - feeds, 210-211
  - intelligence, 62-63, 208-213, 360, 391
  - landscapes, 4-7
  - managed threat defense architecture, 67
  - platforms, 211-213
  - system optimization, 388
- ticketing**, 64-65, 120
  - evaluation, 82
  - queue backlogs, 377
- time**
  - periods, strategies, 93
  - zones, 131
- timelines**
  - IR (incident response), 15
  - strategies, 94
- TLS (Transport Layer Security)**, 112, 120
- tools**, 198
  - Core Impact, 195
  - digital forensic, 313
  - event collection, 134-137
  - information management, 206
  - inventory assessments, 205
  - Kali Linux, 194
  - Metasploit, 194
  - nano configuration utility, 125
  - Nessus, 194
  - NetFlow, 175-182
  - Nmap, 194
  - OpenVAS (Open Vulnerability Assessment System), 194
  - remediation, 206
  - reporting, 206
  - responses, 207
  - risk assessments, 206
  - vulnerabilities, 193-195, 206
- Tor browsers**, 7
- tracking**
  - files, 150
  - RTIR (Request Tracker for Incident Response), 353
  - vulnerabilities, 80-81
- traffic, data center**, 155
- training**
  - evaluation, 78
  - teams, 384
- transfers**, 196
- transitions**
  - management, 321-345
    - checks to ensure readiness*, 332-345
    - planning*, 322

- project resources*, 328-329
- requirements*, 329-332
- success criteria*, 322-328
- services, 368
- Transmission Control Protocol. *See* TCP
- Transport Layer Security. *See* TLS
- triage, incidents, 16, 79
- Trojans, 263
- troubleshooting debug log messages, 140
- Trusted Automated eXchange of Indicator Information. *See* TAXII
- tuning, 379-389
- TVIS (threat and vulnerability intelligence service), 223
- type synchronization, access, 134
- types
  - of attack signatures, 209-210
  - of attackers, 198

## U

---

- Ubuntu syslog servers, measuring EPS, 124-129
- UCS (Unified Computing System), 187
- UDP (User Datagram Protocol), 40, 130
- unauthorized access, incident category (1), 17
- Unified Computing System. *See* UCS
- United Kingdom
  - Data Protection Act 1998, 10
  - IA (information assurance), 10
- upgrades, 388-389
- URLs (uniform resource locators), filtering, 143

- U.S. Department of Defense (DoD), 137
  - Directive 8500.01E, 10
- US-EU Safe Harbor on Data Protection directive, 9
- USB memory devices, 14
- User Datagram Protocol. *See* UDP
- user interfaces, event collection tools, 136
- UTC (coordinated universal time), 131

## V

---

- values, logging levels, 126
- VBIR (2015 Verizon Breach Investigation Report), 190
- VDS (vulnerability discovery service), 222
- verification, 16
- Verizon 2015 Data Breach Investigation Report (DBIR), 5
- versions, NetFlow, 308
- VFs (virtual firewalls), 155-157
- video
  - collaboration, 272
  - walls in facilities, 108-109
- VINES (Virtual Integrated Network Service), 129
- virtual devices, 37
- virtual environments, 116-117
- virtual firewalls. *See* VFs
- Virtual Integrated Network Service. *See* VINES
- virtual LANs. *See* VLANs
- virtual private networks. *See* VPNs
- virtual SOC models, 96-98, 245-246

**VLANs (virtual LANs), 110, 113**

segmentation, 247-250

**VoIP (Voice over IP), 272**

**VPNs (virtual private networks), 248, 251-253**

**vulnerabilities**

announcements, 60-62

assessments, 81, 192, 203

discovery, 80

factors of, 198-200

handling, 195-204

identifying, 190-191

intelligence, 360, 391

known-unknown zero-day, 7

management, 24, 58-62, 189-190, 233, 241

*automating, 205-208*

*lifecycles, 202-204*

OWASP Risk Rating Methodology, 197-202

remediation, 80

risk assessments, 12

SANS Vulnerability Management Model, 64, 202, 207

security services, 191-193

tools, 193-195, 206

tracking, 80-81

**vulnerability discovery service. *See* VDS**

**Vulnerability Scoring System. *See* CVSS**

**VUPEN Security, 7**

## W

---

**WANs (wide-area networks), 45**

war rooms, internal layouts (facilities), 106

**WCCP (Web Cache Communication Protocol), 292**

**Weaponization (Phase 2, cyber kill chain), 3**

**Web Cache Communication Protocol. *See* WCCP**

**Web proxies, 169-170, 290-295**

**Web Security Appliance. *See* WSA whitelists, 298**

**wide-area networks. *See* WANs**

**widening scope, 389**

**Windows Server Update Services. *See* WSUS**

**workspaces, 105. *See also* facilities**

**workstation design, 110**

**World Economic Forum (2014), 8**

**WSA (Web Security Appliance), 170-172, 213, 259**

**WSUS (Windows Server Update Services), 261**

## Y

---

**YARN, 57**

## Z

---

**zones, time, 131**