



# At a Glance

---

## **Part I Introduction to SIEM: Threat Intelligence for IT Systems**

---

1	Business Models .....	3
2	Threat Models .....	19
3	Regulatory Compliance .....	35

## **Part II IT Threat Intelligence Using SIEM Systems**

---

4	SIEM Concepts: Components for Small and Medium-size Businesses .....	53
5	The Anatomy of a SIEM .....	77
6	Incident Response .....	93
7	Using SIEM for Business Intelligence .....	115

**Part III SIEM Tools**

8	AlienVault OSSIM Implementation . . . . .	139
9	AlienVault OSSIM Operation . . . . .	169
10	Cisco Security: MARS Implementation . . . . .	197
11	Cisco MARS Advanced Techniques . . . . .	225
12	Q1 Labs QRadar Implementation . . . . .	261
13	Q1 Labs QRadar Advanced Techniques . . . . .	289
14	ArcSight ESM v4.5 Implementation . . . . .	329
15	ArcSight ESM v4.5 Advanced Techniques . . . . .	355
	Appendix: The Ways and Means of the Security Analyst . . . . .	383
	Index . . . . .	415

# Contents

Foreword .....	xxi
Acknowledgments .....	xxiii
Introduction .....	xxv

## Part I

### Introduction to SIEM: Threat Intelligence for IT Systems

<b>1 Business Models .....</b>	<b>3</b>
What Are IT Business Models? .....	4
What You Have to Worry About .....	5
Overview of CIA .....	9
Government .....	10
Military .....	10
Three-Letter Agencies .....	12
Social Services Infrastructure .....	13
Commercial Entities .....	14
Retail Services .....	14
Manufacturing/Production .....	15
Banking .....	15
Universities .....	16
How Does Your Company's Business Model Affect You? .....	18

<b>2 Threat Models</b> .....	<b>19</b>
The Bad Things That Could Happen .....	21
Vulnerabilities .....	21
Malicious Intent .....	23
Recognizing Attacks on the IT Systems .....	25
Scanning or Reconnaissance .....	26
Exploits .....	26
Entrenchment .....	29
Phoning Home .....	30
Control .....	31
After That... .....	32
Summary .....	33
<b>3 Regulatory Compliance</b> .....	<b>35</b>
Compliance Regulations .....	38
Sarbanes-Oxley Act (2002) - SOX .....	38
Gramm-Leach-Bliley Act (1999) - GLBA .....	38
Healthcare Insurance Portability and Accountability Act (1996) - HIPAA .....	39
Payment Card Industry Data Security Standard - PCI DSS .....	39
California Senate Bill 1386 (2003) - CA SB1386 .....	40
Federal Information Security Management Act (2002) - FISMA .....	40
Cyber Security Act of 2009 (SB 773) .....	40
Recommended Best Practices .....	41
Prudent Security .....	42
Summary .....	49

**Part II**

**IT Threat Intelligence Using SIEM Systems**

<b>4 SIEM Concepts: Components for Small and Medium-size Businesses</b> .....	<b>53</b>
The Homegrown SIEM .....	54
Log Management .....	55
Syslog .....	56
Alerts .....	56
Flow Data .....	56
Vulnerability Assessment Data .....	57
Let the Collection Begin .....	57
Logging Solutions .....	60

Event Correlation .....	63
Event Normalization .....	64
Correlation Rules .....	65
Commercial SIEM for SME .....	65
Endpoint Security .....	67
Securing the Endpoints .....	67
Protecting the Network from the Endpoints .....	70
IT Regulatory Compliance .....	71
Compliance Tools .....	73
Implementation Methodology .....	74
Tools Reference .....	75
Summary .....	76
<b>5 The Anatomy of a SIEM .....</b>	<b>77</b>
Source Device .....	78
Operating Systems .....	79
Appliances .....	79
Applications .....	79
Determining Needed Logs .....	80
Determining Needed SIEM Resources .....	80
Log Collection .....	81
Push Log Collection .....	82
Pull Log Collection .....	82
Prebuilt Log Collection .....	83
Custom Log Collection .....	83
Mixed Environments .....	83
Parsing/Normalization of Logs .....	84
Rule Engine/Correlation Engine .....	86
Correlation Engine .....	87
Log Storage .....	90
Database .....	90
Flat Text File .....	90
Binary File .....	91
Monitoring .....	91
Summary .....	92
<b>6 Incident Response .....</b>	<b>93</b>
What Is an Incident Response Program? .....	94
Grown from the Security Program .....	94
Where the IR Program Fits In .....	96
How to Build an Incident Response Program .....	97
The IR Team .....	97
Useful Tools for the IR Team .....	99

Socio/Political Aspects .....	100
The Price Tag .....	100
Security Incidents and a Guide to Incident Response .....	101
A Typical Escalation Flow to Security Incident .....	101
Finally! An Incident .....	102
Incident Response Procedures .....	104
Automated Response .....	111
Automated Response—a Good Thing .....	112
Automated Response—a Bad Thing .....	113
Summary .....	114
<b>7 Using SIEM for Business Intelligence .....</b>	<b>115</b>
What Is Business Intelligence .....	116
Business Intelligence Terminology .....	117
Common Business Intelligence Questions .....	119
Answers to the Common Business Intelligence Questions .....	119
Developing Business Intelligence Strategies Using SIEM .....	130
How to Utilize SIEM for Your BI Objectives .....	131
Using the Data that Your Organization Currently Possesses .....	132
What Other Companies Are Doing with SIEM and BI .....	134
Summary .....	135

### Part III

#### SIEM Tools

<b>8 AlienVault OSSIM Implementation .....</b>	<b>139</b>
Background .....	140
Concept .....	140
Open Source Tools .....	140
Functionality .....	142
Commercial Version .....	146
Design .....	147
Architecture .....	147
Deployment Considerations .....	149
Implementation .....	149
Requirements .....	150
Installation Process .....	151
Profiles .....	165
Modifications After Installation .....	165
Web Console .....	166
Dashboards .....	166

Incidents .....	166
Analysis .....	167
Reports .....	167
Assets .....	167
Monitors .....	167
Intelligence .....	167
Configuration .....	168
Tools .....	168
Summary .....	168
<b>9 AlienVault OSSIM Operation .....</b>	<b>169</b>
Interface .....	170
Dashboards .....	170
Incidents .....	174
Analysis .....	178
Assets .....	181
Intelligence .....	182
Monitors .....	184
Analysis of a Basic Attack .....	185
Analysis of a Sophisticated Attack .....	190
Summary .....	195
<b>10 Cisco Security: MARS Implementation .....</b>	<b>197</b>
Introduction to MARS .....	198
Topology, Sessions, and Incidents .....	199
Scaling a MARS Deployment .....	201
Analyze Requirements .....	202
Objectives .....	202
Unique Threat Concerns .....	203
Infrastructure Inventory .....	204
Design .....	205
Resources and Requirements .....	205
Roles and Responsibilities .....	206
Deployment .....	206
Installing the Device and Connect to Network .....	206
Configuring the Web Interface .....	208
Assigning MARS User Accounts .....	208
Adding Monitored Devices .....	209
Integrating Flow Data .....	212
Generating Topology .....	212
Operation: Queries, Rules, and Reports .....	216
Queries .....	217
System Rules .....	218

User Inspection Rules .....	220
Reports .....	221
Limitations .....	223
Summary .....	223
<b>11 Cisco MARS Advanced Techniques .....</b>	<b>225</b>
Using the MARS Dashboard .....	226
Summary Page .....	228
Incidents Page .....	233
Query/Reports Page .....	234
Rules Page .....	235
Management Page .....	238
Admin Page .....	240
Adding Unsupported Devices to MARS .....	243
Importing Device Support Packages .....	244
Building Your Own Custom Parsers .....	246
A Typical Day in the Life of a MARS Operator .....	252
Limitations .....	259
Summary .....	259
<b>12 Q1 Labs QRadar Implementation .....</b>	<b>261</b>
QRadar Architecture Overview .....	262
Q1 Labs Terms to Know .....	266
Planning .....	267
Know Your Network .....	267
Plan Your QRadar SIEM Deployment .....	268
Initial Installation .....	270
Configuring the Underlying CentOS System .....	270
The QRadar Administrative Interface .....	271
Getting Flow and Event Data into QRadar .....	285
Event Sources and Data .....	286
Flow Sources and Data .....	287
Summary .....	287
<b>13 Q1 Labs QRadar Advanced Techniques .....</b>	<b>289</b>
Using the QRadar Dashboard .....	291
QRadar Dashboard Default Views .....	292
QRadar Views .....	292
Custom Views .....	295
The Equation Editor .....	296
QRadar Sentries .....	299
QRadar Sentry Components .....	300
QRadar Sentry Types .....	300



QRadar Rules	301
QRadar Rule Types	302
QRadar Rule Components	302
QRadar Custom Rules Wizard	303
The Offense Manager	307
Searching QRadar Offenses	308
QRadar Tuning	309
QRadar False Positive Wizard	309
QRadar DSMs and Custom DSMs	311
Replacing the QRadar SSL Certificates	314
Stepping Through the Process	317
Analyzing Events	317
Summary	327
<b>14 ArcSight ESM v4.5 Implementation</b>	<b>329</b>
ArcSight Terminology and Concepts	330
Overview of ArcSight Products	331
ArcSight ESM v4.5	332
ArcSight SmartConnectors	335
ArcSight Express	336
ArcSight Logger	336
ArcSight ESM v4.5 Architecture Overview	337
Planning Your Deployment	340
Determine Goals	340
Manage Assets	341
Determine ArcSight Hardware Requirements	341
Initial Installation	342
Mount and Cable Servers	343
Install and Configure Operating System	343
Install ArcSight ESM v4.5 Database Software and Oracle Database	344
Install ArcSight ESM v4.5 Manager	348
Configure ArcSight Partition Archiver	350
Install ArcSight SmartConnector	351
Install ArcSight Console	353
Summary	354
<b>15 ArcSight ESM v4.5 Advanced Techniques</b>	<b>355</b>
Operations: Dealing with Data	356
Filters	356
Rules	357
Lists	360
Trending	360

Active Channels .....	361
Notifications .....	363
Cases .....	364
Exporting Information .....	364
Managing Assets and Networks .....	365
The ArcSight SmartConnector .....	365
The ArcSight Asset Model .....	366
The ArcSight Network Model .....	367
Management and Troubleshooting .....	368
Log and Configuration Files .....	368
Database .....	373
System Patching and Upgrades .....	376
Tips and Tricks .....	379
Summary .....	381
<b>Appendix: The Ways and Means of the Security Analyst ...</b>	<b>383</b>
<b>Index .....</b>	<b>415</b>