Inhalt

Geleitwort ..... **IX**

Vorwort ..... **XI**

1 Über dieses Buch **1**

1.1 Orientierung und Motivation 1

1.2 Ziel des Buches 2

1.3 Wer soll das Buch lesen? 4

1.4 Was erwartet Sie in diesem Buch? 6

1.5 Wie ist das Buch aufgebaut 7

1.6 Was Sie noch wissen sollten 8

1.7 Etwas zur verwendeten Sprache und Gendergerechtigkeit 10

2 Grundlagen der Netzwerküberwachung **11**

2.1 Herausforderungen und Trends 11

2.2 Was ist ein SIEM? 13

2.3 Warum ein SOAR einsetzen? 16

2.3.1 Was unterscheiden SOAR und SIEM? 16

2.3.2 Die Kernfunktionen eines SOAR 18

2.4 Die Cyber Kill Chain 20

2.4.1 Warum sollte ich sie kennen? 20

2.4.2 Bedeutung und Phasen der Cyber Kill Chain 21

2.5 Das MITRE ATT&CK Framework 23

2.5.1 Entstehung und Hintergrund 23

2.5.2 Die MITRE ATT&CK-Matrix 25
2.5.3 Wie wird das MITRE ATT&CK Framework in SIEM und SOAR eingesetzt? 30
2.6 Das MISP-Projekt 32
2.6.1 Wer steckt dahinter? 32
2.6.2 Wie ist die MISP aufgebaut? 32
2.6.3 Wer nutzt MISP und welche Vorteile hat es? 33
2.6.4 Wie kann ich MISP installieren? 34
2.6.5 Wie richte ich Feeds ein und rufe Informationen ab? 36
2.7 Was ist ein Security-Operation-Center (SOC)? 38
2.8 Kontrollfragen zu Kapitel 2 39

3 Eine eigene Testumgebung aufbauen 41
3.1 Proxmox VE 42
3.1.1 Proxmox VE installieren 43
3.1.2 Proxmox für den Einsatz vorbereiten 45
3.1.3 Virtuelle Maschinen erstellen 46
3.2 Virtualisierung mit XCP-ng 64
3.2.1 Design und Komponenten von XCP-ng 64
3.2.2 XCP-ng und Xen Orchestra installieren 66
3.2.3 Virtuelle Maschinen mit Xen Orchestra erstellen 69
3.3 Virtualisierung mit Unraid 72
3.3.1 Wie ist Unraid aufgebaut? 73
3.3.2 Unraid installieren 74
3.3.3 Festplatten für den Einsatz vorbereiten 75
3.3.4 Erste Schritte in Unraid 77
3.3.5 Virtuelle Maschinen in Unraid einrichten 78
3.3.6 Docker-Container in Unraid einrichten 80
3.4 Lokaler Server oder Cloud-Lösung? 82
3.5 Eigenes Testnetzwerk für Wazuh 83
3.6 Kontrollfragen zu Kapitel 3 85

4 Netzwerkmonitoring mit Wazuh 87
4.1 Wazuh-Aufbau und -Komponenten 88
4.2 Wazuh installieren 90

4.3 Konfigurationsdateien in Wazuh 93
4.3.1 Was sind eigentlich Decoder? 95
4.3.2 Warum gibt es Wazuh-Rulesets? 96
4.4 Agenten einrichten 97
4.4.1 Agenten auf einem Windows-System einrichten 98
4.4.2 Agenten auf einem Linux-System einrichten 99
4.4.3 Agenten auf einem Mac einrichten 101
4.5 Agentenloses Monitoring in Wazuh 103
4.5.1 Agentenloses Monitoring über SSH 103
4.5.2 Logdaten über das Syslog-Protokoll übertragen 108
4.6 Das Wazuh-Dashboard 112
4.6.1 Bereiche „Agent Summary“ und „Last 24 Hours Alerts“ 113
4.6.2 Bereich „Endpoint Security“ 113
4.6.3 Bereich „Threat Intelligence“ 121
4.6.4 Bereich „Security Operations“ 128
4.6.5 Bereich „Cloud Security“ 131
4.7 Kontrollfragen zu Kapitel 4 134

5 Anwendungsfälle 137
5.1 Wazuh konfigurieren und anpassen 138
5.1.1 Agentengruppen erstellen 142
5.1.2 Eigene Regeln und Decoder erstellen 147
5.1.3 Überwachung von Docker-Containern mit Wazuh 164
5.1.4 OPNsense-Firewall überwachen 171
5.1.5 Benutzerdefinierte Compliance-Prüfungen erstellen 176
5.1.6 Alerts per E-Mail empfangen 182
5.1.7 Wazuh aktualisieren 186
5.1.8 Wazuh deaktivieren und löschen 191
5.1.9 Kontrollfragen zu Abschnitt 5.1 195
5.2 Threat Intelligence mit Wazuh 196
5.2.1 Mit Wazuh Schwachstellen erkennen 196
5.2.2 Malware auf einem Linux-System erkennen 202
5.2.3 Mit Wazuh Windows-Defender-Protokolle sammeln und darstellen 207
5.2.4 Malware mithilfe von YARA erkennen 211

5.2.5 Malware mithilfe von VirusTotal erkennen 226
5.2.6 Kontrollfragen zu Abschnitt 5.2 231
5.3 Angriffe erkennen 233
5.3.1 Brute-Force-Angriffe erkennen und stoppen 234
5.3.2 SQL-Injection-Angriffe erkennen 241
5.3.3 USB-Schnittstelle auf Windows-PC überwachen 246
5.3.4 Metasploit Backdoor erkennen 255
5.3.5 Living-off-the-Land-Angriffe erkennen 262
5.3.6 Command and Control (C&C) Server erkennen 270
5.3.7 Kontrollfragen zu Abschnitt 5.3 277

6 Effiziente Reaktion durch Automatisierung 279
6.1 Die Vor- und Nachteile der Automatisierung 280
6.2 Automatisierung mit Open-Source-Tools 281
6.2.1 Die Schaltzentrale – TheHive 283
6.2.2 Cortex – das Gehirn 284
6.2.3 Installation von TheHive, Cortex und MISP in Docker 285
6.2.4 Die Zusammenarbeit von TheHive und Wazuh konfigurieren 299
6.3 Automatisierung mit Shuffle und IRIS 302
6.3.1 Hauptmerkmale von Shuffle 302
6.3.2 Shuffle installieren und kennenlernen 304
6.3.3 Hauptmerkmale von DFIR-IRIS 306
6.3.4 IRIS installieren und einrichten 308
6.3.5 Shuffle-Workflow anhand eines praktischen Beispiels 311
6.4 Kontrollfragen zu Kapitel 6 325

7 Lösungen zu den Kontrollfragen 327
7.1 Lösungen zu Kontrollfragen in Kapitel 2 327
7.2 Lösungen zu Kontrollfragen in Kapitel 3 329
7.3 Lösungen zu Kontrollfragen in Kapitel 4 332
7.4 Lösungen zu Kontrollfragen in Abschnitt 5.1 336
7.5 Lösungen zu Kontrollfragen in Abschnitt 5.2 338
7.6 Lösungen zu Kontrollfragen in Abschnitt 5.3 340
7.7 Auflösung des Szenarios in Abschnitt 5.3.6 342
7.8 Lösungen zu Kontrollfragen in Kapitel 6 346

Stichwortverzeichnis 349