LDR551 – Building & Leading Security Operations Centers

Topics

SOC Design & Operational Planning

Introduction	551.1–7-20
SOC Planning	551.1–21-40
SOC Functions	551.1–43-55
Team Creation, Hiring & Training	551.1–58-92
Cyber Threat Intelligence	551.1–95-118
Building the SOC	551.1–121-134

SOC Telemetry & Analysis

Cyber Def Theory & Mental Models	551.2–8-28
SOC Tools & Technology	551.2–31-41
SOC Data Collection	551.2–42-68
MITRE ATT&CK to Plan Collection	551.2–69-78
Capacity Planning	551.2–81-103
Protecting SOC Data/Capabilities	551.2–106-125

Attack Detection, Threat Hunting & Triage

Analytic Frameworks & Tools	551.3–6-19
Detection & Analytic Design	551.3–20-36
Efficient Alert Triage	551.3–39-55
Detection Engineering	551.3–56-75
SOC-Assisted Use Cases	551.3–78-106
Threat Hunting	551.3–107-130
Active Defense	551.3–133-147

Investigation & Response

Incident Response Planning & Prep.	551.4–6-27
Identification & Coordintion	551.4–30-50
Forensic Analysis & IR Tools	551.4–53-70
Containment & Eradication	551.4–71-78
Incident Response in the Cloud	551.4–79-87
Investigation	551.4–88-111
Recovery, Post Incident & Practice	551.4–114-132

Metrics, Automation, Continuous Improvement

Staff Retention & Burnout Prevention	551.5–6-24
Building Your SOC Culture	551.5–25-35
Metrics, Goals & Effective Execution	551.5–36-67
Measurements & Prioritization Issues	551.5–70-92
Automation in Security Operations	551.5–93-108
Analytic Test & Adversary Emulat°	551.5–109-128
SOC Capability Assessment	551.5–131-140
The Lean SOC	551.5–141-152

Categories

Essentials

Attack Tree	551.W–53
Average SOC	551.1–13-14
Capacity Planning	551.W–84-85
CI/CD Pipeline Data Sources	551.3–83
Constituency Definition	551.1–34
Continuous Learning	551.1–86
CTI Producers & Consumers	551.1–103
Cyber Kill Chain	551.1–111
	551.2–13-14
DAIR Model	551.2–19
Dedicated Internal SOC	551.1–23
Detection Maturity Model	551.3–74
DevOps Monitoring	551.3–82
Diamond Model	551.1–111
Duty Roles	551.1–65-67
EASY Framework	551.1–108
F3EAD Cycle	551.1–111
FMEA Process	551.W–225
GQM Process	551.W–185-187
IMS	551.2–35
Incident Response Cycle	551.2–18-19
Indicator Relationships	551.1–114
Investigation Review Questions List	551.W–175
Log Collection	551.2–44-46
MITRE ATT&CK	551.1–51
Modern Defense Mindset	551.2–11
MTS Goal Hierarchy (IR)	551.4–24-25
	551.W–151
OCTAVE	551.W–28-30
OODA Loop	551.2–20-21
PICERL Model	551.2–18
PIR Process	551.W–37-43
Purple Team Methodology	551.5–118-120
Pyramid of Pain	551.2–15
Relationship Tracking	551.1–39
Sampling with AQL Tables	551.W–168-172
SIEM	551.2–33
SOC – Auxiliary Functions	551.1–60-63
SOC – Core	551.1–48-54
SOC – Functions	551.1–46
SOC – High Level	551.1–45
SOC – Room Layout	551.1–124
SOC – Tiered VS Tierless	551.1–64
Speed of Intel Use	551.1–113
STIX	551.1–114
TaHiTI Methodology	551.W–138-139
Technology Selection	551.2–37-39
Threat Data VS Info VS Intel	551.1–98
Threat Hunting Process	551.3–116
Threat Intel Levels	551.1–100-101
Threat Profile	551.W–50
TIP	551.2–34
Use Case Database Interactions	551.3–66
Workforce	551.1–89

Labs

ATT&CK Navigator for Prioritization	551.2–80
	551.2–64-80
Attack Modeling & Data Src Assessment	551.2–30
	551.W–52-63
Capacity Planning	551.2–105
	551.W–81-93
Creating, Classifying, and Communicating Your Metrics	551.5–69
	551.W–184-200
Critical Asset Mapping	551.1–57

- 551.W–28-30
- Cyber42 Simulation Instructions 551.W–236-245
- Detection Rule Management, Measurement and Visualization 551.3–38
  - 551.W–94-112
- Developing & Implementing Playbooks 551.4–52
  - 551.W–154-166
- Improving Quality and Resilience 551.5–152
  - 551.W–225-235
- Incident Response Goals and Teamwork 551.4–29
  - 551.W–147-153
- Investigation Quality Review 551.4–113
  - 551.W–167-183
- Planning a Threat Hunt 551.3–132
  - 551.W–138-146
- Priority Intel Requirements 551.1–120
  - 551.W–37-43
- Purple Team Assessment Planning, Execution, and Tracking 551.5–130
  - 551.W–201-224
- SOC Charter & Mission 551.1–42
  - 551.W–22-27
- SOC Roles 551.1–94
  - 551.W–31-36
- Structuring, Documenting, and Organizing Use Cases 551.3–77
  - 551.W–113-137
- Threat Actor Assessment 551.2–7
  - 551.W–44-51

Tools

- ADAz 551.3–18
- Amazon CloudTrail 551.3–85
- Armitage 551.5–113
- Atomic Red Team 551.3–18
  - 551.5–113
- Autopsy 551.4–57
- BAS 551.5–113, 123-127
- Beats 551.3–85
- BT3 551.5–113
- Bulk Extractor 551.4–57
- CAPE 551.4–68
- ChatGPT 551.5–106
- Cobalt Strike 551.5–113
- Covenant 551.5–113
- CrowdStrike 551.4–64
- CSV 551.5–113
- Cuckoo 551.4–68
- DarkTrace 551.4–65
- DeTT&CT 551.2–77
- Draw.io 551.W–55, 57
- EnCase 551.4–57
- ExtraHop 551.4–65
- Feedly 551.W–43
- Fidelis 551.4–65
- FireEye 551.4–64
- FLARE 551.2–114
  - 551.4–57
- FLOSS 551.4–68
- Fluentd 551.3–85
- FTK 551.4–57
- Git 551.W–100-109
- Grafana 551.W–195
- Graphite 551.W–195
- Hybrid Analysis 551.4–68
- Infection Monkey 551.5–113
- JA4+ 551.2–62
- Jira 551.3–65, 68
- Joe Sandbox 551.4–68
- Jupyter 551.3–8, 16
- Kibana 551.W–195
- MaGMa UCF 551.3–71
- MDO 551.3–50-51
- Metasploit 551.5–113
- Metta 551.5–113
- Microsoft Defender 551.4–64
- MISP 551.1–117
  - 551.3–11
  - 551.W–43, 47
- MITRE ATT&CK Navigator 551.2–73-74
  - 551.3–12
  - 551.5–128
  - 551.W–64-80, 215
- MITRE CALDERA 551.3–18
  - 551.5–113
- MITRE CAR 551.3–72
- MITRE D3FEND 551.3–9
- MITRE Engage 551.3–9, 140-144
- MITRE Shield 551.3–9
- MITRE TRAM 551.5–105
  - 551.W–78
- NXLog 551.2–53
  - 551.3–85
- OpenBAS 551.4–129
- OSQuery 551.3–72
  - 551.4–57
- Palantir ADS 551.3–69
- PowerBI 551.W–195
- PowerShell Empire 551.5–113
- Prometheus 551.W–195
- Purple Team ATT&CK Automation 551.5–113
- Redline 551.4–57
- Redmine 551.3–65, 68
  - 551.W–114
- REMnux 551.4–57
- RTA 551.5–113
- Sandboxie 551.4–68
- Scikit Learn 551.5–105
- Sentinel 551.3–16
- SIFT 551.4–57
- SleuthKit 551.4–57
- Snort 551.3–28
- Splunk 551.3–17
- Splunk Attack Range 551.3–18
- Suricata 551.2–59
- Syslog-ng 551.3–85

Sysmon 551.2–58
 551.3–72, 118
 551.4–57
Tableau 551.W–195
TheHive 551.4–42
 551.W–158-164, 178-181
VECTR 551.5–121-122
 551.W–202-222
Vectra 551.4–65
Vega 551.W–195
Velociraptor 551.4–57
VirusTotal 551.4–68
Wazuh 551.4–64
Zeek 551.2–59, 62

Books
 11 Strategies of a World-Class Cybersecurity Operations Center (2022) 551.2–125
 Analysis of Alternatives (AoA) Handbook (2017) 551.2–38
 Applied Incident Response (2020) 551.4–70
 Blue Team Handbook: Incident Response Edition (2014) 551.4–70
 Blue Team Handbook: SOC, SIEM, and Threat Hunting V1.02 (2019) 551.2–78
 BTFM: Blue Team Field Manual (2017) 551.4–70
 CSIRT Effectiveness and Social Maturity (2016) 551.4–22
 Drive: The Surprising Truth About What Motivates Us (2009) 551.5–7
 Flow: The Psychology of Optimal Experience (2008) 551.5–20
 How to Measure Anything in Cybersecurity Risk (2023) 551.5–48
 Intelligence-Driven Incident Response (2017) 551.1–104
 Measure What Matters: How Google, Bono, and the Gates Foundation Rock the World with OKRs (2018) 551.5–39
 Peak: Secrets from the New Science of Expertise (2017) 551.5–20
 Psychology of Intelligence Analysis (1999) 551.4–98
 Reinventing Jobs: A 4-Step Approach for Applying Automation to Work (2018) 551.5–98
 Security Metrics: Replacing Fear, Uncertainty, and Doubt (2007) 551.5–50
 Statistical Process Control for Managers (2017) 551.W–182
 The 4 Disciplines of Execution: Achieving Your Wildly Important Goals (2021) 551.5–39
 The Career Architect Development Planner (1996) 551.1–84
 The Essential Drucker (2008) 551.2–22
 The Hard Thing About Hard Things (2014) 551.5–30
 The Infinite Game (2019) 551.2–23
 The One Thing: The Simple Truth Behind Extraordinary Results (2018) 551.5–60
 The Tyranny of Metrics (2018) 551.5–83
 The Visual Display of Quantitative Information (2001) 551.W–196
 What You Do Is Who You Are (2019) 551.5–26

Other Courses
 FOR500 - Windows Forensics 551.4–70
 FOR508 - Digital Forensics 551.4–70
 FOR509 - Cloud Forensics 551.4–80
 FOR518 - Mac & iOS Forensics 551.4–70
 FOR572 - Network Forensics 551.4–70
 FOR610 - Reverse Engineering 551.2–114
  551.4–68, 70
 LDR553 - Cyber Incident Response 551.4–46, 126
 SEC450 - Blue Team Fundamentals 551.1–8, 52
  551.5–156
 SEC503 - Intrusion Detection 551.4–70
 SEC504 - Incident Handling 551.2–18
  551.4–70
 SEC511 - Continuous Monitoring 551.2–11
 SEC530 - Defensible Architecture 551.4–27
 SEC540 - Secure DevOps 551.3–83
 SEC547 - Defending Supply Chain 551.3–90
 SEC555 - Tactical SIEM 551.2–50
 SEC599 - Purple Team Tactics 551.5–116
 SEC699 - Advanced Purple Teaming 551.5–116

A

Acceptable Use Policies 551.3–105
Acceptance 551.3–83
Account Tagging 551.3–50
Accountability 551.5–58
 Cadence 551.5–65, 83
Accuracy 551.1–106
ACH 551.4–89, 98, 100-103
 Example 551.4–101
 Methodology 551.4–100
ACM 551.4–43
ACSC System Configuration Guides 551.4–12
Action Priority 551.W–229-230
Active Defense 551.3–134-147
 Example 551.3–138, 142
 Frameworks 551.3–140
 Goals 551.3–135-139
 Mistakes 551.3–146
 Summary 551.3–147
 When 551.3–145
Activity 551.5–146
Adaptive Case Management → ACM
Additional Logging 551.4–120
Advanced Attacks 551.3–35
Adversarial Simulation 551.3–60
Adversary Emulation 551.5–114, 116-117, 128
Adversary Engagement 551.3–9, 140
 Techniques 551.3–144
Adversary Vulnerabilities 551.3–9

LDR551 – Building & Leading Security Operations Centers

- Agentless 551.4–61
- Agents 551.W–195
- Alert 551.2–82
  - Aggregation 551.3–35
  - Context 551.3–53
  - Count 551.2–83, 89-93
    - Complicating Factors 551.2–90
    - Dependencies 551.3–36
    - Estimation 551.2–88
  - Dashboard 551.2–92
  - Disposition 551.3–30-33
  - Enrichment 551.5–104
  - Fatigue 551.3–27
  - Generation 551.2–85
  - High Volume 551.3–33
  - Important 551.3–48
  - Management 551.5–103
  - Non-Actionable 551.3–34
  - Playbook Trigger 551.4–42
  - Prioritization 551.5–77
  - Priority 551.3–33, 44
  - Queue 551.3–42-43
  - Volume 551.3–27
- Alerting 551.2–33
  - Real-Time 551.4–63
  - Threshold 551.3–26
- Alexiou Principle 551.4–91
- Alignment Matrix 551.1–39
- Alternatives Analysis 551.2–37
- Always-On Communication Channels 551.1–132
- Amazon CloudTrail 551.3–85
- Analysis of Competing Hypotheses → ACH
- Analysis Placebo 551.5–74
  - Effect 551.5–85
- Analysis Writeup Example 551.4–92
- Analyst Core Toolset 551.2–32
- Analytic 551.3–19
  - Accuracy 551.3–29
  - Classification 551.3–61
  - Scope 551.3–22
  - Testing 551.5–110-113, 128
    - Continuous 551.5–111
    - Methodology 551.5–112
    - Tools 551.3–17 551.5–113
  - Types 551.2–15
- Analytics Downstream 551.3–28
- Android 551.2–65
- Anomaly Detection 551.3–61 551.4–84
- Anomaly Investigation 551.3–124
- Anomaly-Based Network Intrusion Detection 551.4–65
- ANSI Tables → AQL Tables
- Antivirus 551.4–75
- AoA Process 551.2–37-39
- API 551.W–194
- Application Domain 551.4–86
- Applied Incident Response 551.4–70
- APT Modeling 551.2–13
- AQL (QRadar) 551.3–14
- AQL Tables 551.W–168-172
- Armitage 551.5–113
- Artifacts Analysis 551.4–56
- Assessment 551.1–60-61
  - Point-In-Time 551.5–123
  - Real-Time 551.5–123
- Asset Management System 551.4–35
- Assets Tracking 551.4–35
- Assignable Cause 551.W–182
- At-Risk Users 551.3–91-92
- Atomic Red Team 551.3–18, 129 551.5–113
- Atomic Testing 551.5–114
- Attack Chains 551.5–117
- Attack Modeling 551.W–52-63
- Attack Path 551.5–120
- Attack Simulation 551.3–18
- Attack Surface 551.3–87
- Attack Tactics 551.3–49
- Attack Technique Prioritization 551.W–64-80
- Attack Tree 551.2–40 551.W–53, 61
  - Methodology 551.W–52-61
- Attacker Loop 551.2–21
- Audit Policy 551.2–44-48
  - Flexibilty 551.2–51
- Auditd 551.2–58
- Australian Signals Directorate 551.4–12
- Authentication Events 551.2–58
- Authentication Methods 551.2–121
- Authentication Systems 551.2–113
- Authenticator 551.2–121
- Automated Analysis 551.4–67
- Automated Lab Environments 551.3–18
- Automatic Technique Extraction 551.W–78
- Automation 551.5–10, 14-15, 94-108
  - 4-Steps Approach 551.5–98-102
  - Evolution 551.5–95
  - Keys to Success 551.5–108
  - Risks 551.5–107
  - Types 551.5–97
- Autonomic Security Operations 551.5–96
- Autonomous Systems 551.5–95
- Autoruns 551.3–72 551.4–63
- AWS 551.2–67
- AWS Lambda 551.4–85
- Azure 551.2–67
- Azure Functions 551.4–85

B

- Backdoor 551.3–126
- Balance of Skills 551.1–133
- Bandwidth 551.5–148, 150
- BAS 551.5–113, 123-127

- Baselines 551.4–14
- BCP 551.4–19
- Beats 551.3–85
- BEC 551.3–91, 93-100
  - Prevention 551.3–96, 99
  - Summary 551.3–100
- Behavioral Engineering Model → BEM
- Bell Curve 551.2–100
- BEM 551.5–23
- Beta Distribution 551.2–100
- Bias 551.1–80-81
  - 551.4–96-97
- BinderHub 551.3–8
- Binomial Distribution 551.2–93
- Blocking 551.4–74
- Blue Team 551.3–8
  - 551.5–115
  - 551.W–210, 215
- BLUEPRINT 551.5–156
- Bottleneck 551.5–61
- Box Checking Exercise 551.2–39
- Brainstorming 551.4–98
  - 551.W–230
- Breach Detection 551.3–137
- BT3 551.5–113
- Budget 551.5–16
- Burnout 551.5–8
  - Mitigation 551.5–18-19
    - Summary 551.5–24
- Business Email Compromise → BEC
- Business Intelligence Tools 551.W–195

C

- C2 Infrastructure 551.4–72
- Calibrated Probability Assessment 551.5–87
- Campaign View 551.3–51
- Canaries 551.3–134
- Candidate Personality Characteristics 551.1–77
- Capabilities 551.W–39
- Capability Assessment 551.5–132-140
  - Summary 551.5–140
- Capacity Planning 551.2–86-87
  - 551.W–81-93
  - Core Variables 551.2–102
  - Summary 551.2–103
  - Worksheet 551.W–84
- Case Management 551.4–43
  - 551.5–103
- Case Review 551.4–109-110
- Case Templates 551.4–42
- Categorization 551.2–56
- Causality Bias 551.4–97
- Causes Assignment 551.W–182
- Centralized Events 551.3–22
- CEO Fraud 551.3–94
- Certifications 551.1–91
- Chain of Custody 551.4–77
- Chart Types 551.W–196-198
- Chat Bot 551.5–97, 104
- ChatGPT 551.5–106
- Cherry Picking 551.5–18
- Chokepoint 551.3–73
- Chronological Attack Models 551.2–13
- CI/CD 551.3–18, 81
  - Pipeline 551.3–83-86
- CIA 551.4–26
  - 551.W–30
- CIS Benchmarks 551.4–11
- CIS Controls 551.4–13
- CIS RAM 551.1–32
- CIS Top 20 Controls 551.4–119
- Cisco 551.4–66
- CISO 551.1–100
  - 551.3–140
- Client Hello 551.2–61-62
- Cloud Logs 551.2–67
- Cloud Native Tools 551.4–85
- Cloud Network Visibility 551.2–67
- Cloudflare 551.2–64-65
- CMMC 551.4–12
- CMMI 551.5–133
- CMS 551.2–32, 34-35
- Cobalt Strike 551.5–113
- COBIT 551.5–133
- Cognitive Automation 551.5–97
  - Example 551.5–105-106
- Collaboration 551.1–97
  - Real-Time 551.4–48
- Collection 551.1–49
  - Diagram 551.2–117
  - Goals 551.2–49
  - Issues 551.2–48
  - Plan (Intel) → Intel Collection Plan
  - Policy 551.2–49
  - Protection 551.2–116
  - Strategies 551.2–50
  - Summary 551.2–68
  - System 551.2–44-46
    - 551.3–22
  - Topics 551.2–43
- Collection Plan (Intel) 551.1–108
- Command Execution 551.2–72
- Commit 551.3–83
- Commodity Malware 551.4–76
- Common Cause 551.W–182
- Communication 551.4–46-47
- Community 551.1–97
- Completeness 551.1–106
- Compliance 551.5–123
- Compliance Assessment 551.4–36
- Compliance Frameworks 551.1–29
- Compliance Requirements 551.4–36
- Compromised Assets 551.4–49
- Concept of Operations 551.1–36
- Confidence Interval 551.5–89

Confirmation Bias 551.4–96, 98, 111
Consent Grant Attacks 551.3–96
Consider ROI for Automation 551.5–101
Conslusion Testing 551.4–107
Constant Operations 551.1–65-66
Constant Value 551.5–101
Constituency 551.1–34
  Steering 551.1–37
Containment 551.4–18, 72, 86
  Actions 551.4–74
  Procedures 551.4–73
  Strategies 551.4–72
  Summary 551.4–78
Context 551.1–106
Contextualization 551.1–100
Conti 551.W–45
Continuous Coverage in One Location 551.1–66
Continuous Improvement 551.1–54
  551.2–27
  551.4–124
  551.5–19
Continuous Learning Model 551.1–86
  551.5–11
Continuous Security Model 551.5–133
Continuous Security Monitoring → CSM
Control Frameworks 551.1–31
Conversation Hijacking 551.3–94
Conversational Automation 551.5–97
Coordination → Cross-Team Coordination
Correlation 551.2–33
  551.3–28
Counter-Factual Thinking 551.4–124
Countermeasures 551.3–9
Covenant 551.5–113
Coverage Check 551.3–66
Coverage of Operations 551.1–66-68
Covering 24/7 551.1–66
COVID-19 551.1–128
Creativity 551.5–9-10, 13, 19
Credential Theft Prevention 551.3–96
Credentials 551.4–59, 62
  Protection 551.4–60
CREST Maturity Assessment 551.5–138
Critical Assets 551.W–28
  Mapping Methodology 551.W–28
Critical Infrastructure 551.3–48
Criticality 551.4–75
Cross-Team Coordination 551.4–24-25
Cross-Training 551.4–125
CrowdStrike 551.4–64
CSF (NIST) 551.5–133-135, 139
CSM 551.2–47
  551.4–32
CSP 551.4–80, 87
CSV 551.5–113
CTI 551.1–96-118
  → Threat Intelligence
Culture 551.5–24, 26-35
  Breaking 551.5–28-29
  Common Mistakes 551.5–29
  Improvement 551.5–27
  Problems 551.5–28
  Summary 551.5–35
Customer Requirements 551.5–53
CVE 551.3–28
CVSS 551.5–71, 78-82
  Attack Vector 551.5–88
Cyber Analytics Repository 551.2–75
Cyber Kill Chain 551.1–51, 111
  551.2–13-14
  551.3–71, 122
  551.4–44, 92
  551.5–122, 124
  551.W–206, 208
Cyber Resilience Review IG 551.4–117

D

D&R Pipeline 551.1–48
Daily Operations 551.5–40
  Monitoring 551.5–42
DAIR 551.2–19
DarkTrace 551.4–65
Data Classification 551.3–49, 54
Data Destruction 551.3–49
Data Enrichment 551.2–57
Data Exfiltration 551.3–126
Data Privacy 551.4–48
Data Quality 551.3–114
Data Sets 551.3–17
Data Sources 551.2–72, 77
  551.3–83-86, 90, 104
  Assessment 551.W–52, 62
  Intentional 551.4–35
  Robust 551.4–63
  Unintentional 551.4–35
  Visualization 551.W–195-197
Deception 551.3–9, 134
Decision Tree 551.5–88
Decomposition 551.4–90-92
  551.5–100
Deconstruct Task for Automation 551.5–100
Dedicated SOC 551.1–23
Deep Work 551.5–21-22
Defects 551.5–147
Defense in Depth 551.2–14
  551.4–13
Defensible Network Architecture 551.4–27
Defensive Planning 551.2–40
Deliberate Practice 551.5–20
Denial Of Service 551.3–49
Detection 551.1–50, 60
  551.3–41
  Capability Ranking 551.2–76-77
  Coverage 551.3–66
  Fidelity 551.W–78

- Key Data Sources 551.2–58-59, 78
- Reliable 551.3–24
- Rule Management 551.W–94
- System 551.3–22-23
- Testing 551.5–116

Detection as Code 551.3–58, 74
Detection Engineering 551.3–57
- Concepts 551.3–59
- Maturity Models 551.3–74
- Prioritization 551.3–73

Detection Maturity Model → DML
Detection-Oriented Defense 551.2–11
DeTT&CT 551.2–77
Development Pipeline 551.3–82
DevOps 551.3–81-86
- Monitoring Goals 551.3–82

DevSecOps 551.3–80
DGA 551.3–120
DHCP Lease 551.4–35
Diamond Model 551.1–111
551.4–92
Diavol 551.W–45
Digital Media Analysis 551.4–56
Digital Transformation 551.1–38
Direct Feedback 551.5–33
DISA 551.4–12
Disconfirmation 551.4–95
Disgruntled Employee 551.3–102
Distal Goal 551.W–147, 149
DKIM 551.3–96
DLP 551.3–104
DMARC 551.3–96
DML 551.3–74
DNS Lookup 551.5–103
DoH 551.2–64-65
DoT 551.2–65
Dream Team 551.1–73

E

EASY Framework 551.1–108
ECH 551.2–61
ECSF 551.1–89
EDR 551.2–32
551.4–39, 57, 60, 64
551.5–95
- Alert 551.2–99

Education 551.1–86
Effective Visualization 551.W–196
Effects Analysis 551.W–225, 227
Eisenhower Matrix 551.5–59
ElasticSearch 551.W–97
Electronic Frontier Foundation 551.1–27
Email Forwarding 551.3–96
Email Protection 551.3–96
- Testing 551.3–98

Email Triage 551.3–50
Emotet 551.2–62
Empowerment 551.5–9, 12-13
Encrypted Traffic Monitoring 551.4–65
Engagement Matrix 551.W–148, 151
Engineering-First Approach 551.5–96
ENISA 551.1–89
- CSIRT Maturity Framework 551.5–137

Enrichment 551.2–57
551.3–28
551.5–103-104
Enterprise SOC 551.1–15
Enterprise Training 551.4–126
Entra ID 551.2–123
Enumeration 551.5–103
Environment 551.1–86
Ephemerality 551.4–86
EPSS 551.5–81
Eradication 551.4–18, 75, 86
- Plan 551.4–73
- Strategies 551.4–75
- Summary 551.4–78

EternalBlue 551.4–101
Evaluate Impact of Automation 551.5–102
Event ID 4624 551.3–118
Event Matrix Diagram 551.4–103, 105
Event Recording Vocabulary 551.4–37
Evidence 551.4–77
- Disconfirmation / Disproval 551.4–95
- Evaluation Bias 551.4–97
- Handling 551.4–85
- Organization 551.4–103
- Preservation 551.4–77
- Review 551.4–121

Evidence-Focused Analysis 551.4–98
Execution 551.5–58
- Disciplines 🕮 551.5–39, 58-66
  - Why This Works 551.5–66
- Summary 551.5–67

Exercise (IR) 551.4–127-131
- Common Mistakes 551.4–130
- Deliverables 551.4–131
- Participants 551.4–128
- Planning 551.4–127

Exfiltration 551.3–49
Exotic Lily 551.W–45
Experience 551.1–86
551.5–83, 91
Expertise 551.5–83, 91
Exploit Availability 551.5–81
Exploit Prediction 551.5–81
Exploitability 551.5–78
Exposure 551.1–86
External Factors 551.5–23
Externalization 551.4–90, 93, 103
ExtraHop 551.4–65

F

F3EAD Cycle 551.1–111

Failure Mode 551.W–225, 227
FAIR 551.1–32
Fake Attorney 551.3–94
False Invoice 551.3–94
False Negatives 551.1–105
  551.2–82
  551.3–25-26
False Positives 551.2–82
  551.3–25-26, 145
  Assessment 551.3–29
  Testing 551.3–69
  Tuning 551.3–31
Familiarity Principle 551.5–85-86
FI-ISAC 551.3–71
  551.W–138
Fidelis 551.4–65
FIDO 551.2–121
File Detection Analytics 551.3–19
File Modification 551.2–72
Finite Games 551.2–23-26
Finite Strategy 551.2–25
FireEye 551.4–64, 66, 68
Firefighting 551.5–58
Firefox 551.2–62, 64-65
FIRST 551.5–81
  551.5–137
FISMA 551.4–36
Flake 551.5–28
FLOSS 551.4–68
Flow Channel 551.5–20-21
Fluentd 551.3–85
FMEA 551.5–152
  Process 551.W–225-231
Focus on Enemy 551.1–11-12
Follow-the-Sun 551.1–67
Foothold 551.4–73
Forensic Analysis 551.4–32, 39, 54-58
  Considerations 551.4–58
  Tools 551.4–64-69
  Training 551.4–70
  Types 551.4–55
Formal Training 551.1–84
Four-DX (4DX) 551.1–133
  551.5–58-66
FS_THREAT_INDEX 551.W–205-207
Full Packet Capture 551.4–54
Funcions-as-a-Service 551.4–85
Functional Impact 551.4–37
Functional Testing 551.3–83
Fuzzy Hashing 551.1–117

G

Gaming 551.5–83
Gap Analysis 551.3–13
GCP 551.2–67
GDPR 551.1–29
Githubification 551.3–58
GLBA 551.1–30
Goals 551.3–9
  551.5–45, 47-48
  Hiearchy 551.4–24
  Metrics Derivation Process 551.5–46-56
  Summary 551.5–67
  Top-Down Alignment 551.5–49
  Top-Level 551.W–24
Goodhart's Law 551.5–83, 91
Google Cloud Functions 551.4–85
Google SRE 🕮 551.5–95-96
GPO 551.1–49
GQIM 551.W–186
GQM 551.5–49
  Process 551.W–185-187
Graph Types 551.W–195-197
Grounded Theory 551.5–8
Growth 551.5–9-11, 18-19
  Optimal Tasks 551.5–20

H

Hardening Requirements 551.4–11-12
Hardening Resources 551.4–12
Hardware Token 551.2–121
HBR 551.1–131-133
Heretic 551.5–28
HIDS 551.2–58
  551.4–64
High-Fidelity Rules 551.2–57
High-Priority Alerts 551.3–44
High-Risk Accounts 551.3–50
High-Visibility Users → At-Risk Users
Highly Protected Subnet 551.3–48
HIPAA 551.1–29
  551.4–11, 36
Hiring → Recruitment
Historical Data 551.2–88
Historical Trending 551.W–214
HITRUST 551.4–12
Honey Documents 551.3–139
Honeypots 551.3–134
Host Logs 551.2–58
Host-Based Firewall 551.4–74
HTTP2/3 551.2–66
Human Analysis 551.1–98
Human Capital Management 551.5–7-13, 24
Human Capital Model 🕮 551.5–8-14
Human-Like Interactions 551.5–97
Hybrid Collection 551.2–50
Hybrid Model 551.3–43-44
Hypothesis Refutation 551.4–98, 100

I

IaaS 551.3–81
Ideal Hunter 551.3–112

- Identity Protection 551.3–96
- IdP 551.2–123
- Immediate Training 551.1–86, 88
- Importance 551.5–59
- Improvement Initiatives 551.5–40
- Improvement Opportunities 551.5–139
- IMS 551.2–32, 34-35
  - 551.3–30, 46
  - 551.4–42-43, 92
- Incident 551.4–31-32
  - Awareness 551.4–49
  - Categorization 551.4–38
  - Data Tracking 551.4–38, 44
  - History 551.4–40
  - Identification 551.4–31
    - Summary 551.4–50
  - Lead 551.4–33-34
  - Management 551.4–26, 130
    - Maturity 551.5–137
    - Summary 551.4–132
  - Report 551.4–117
  - Response 551.1–53, 60
    - 551.4–26
    - Automation 551.5–103
    - Cloud 551.4–80-87
    - Communication 551.4–46-47
    - Cycle 551.2–18-19
    - Exercise → Exercise (IR)
    - Findings 551.4–103
    - First Actions 551.4–72
    - Goals 551.4–8
    - 551.W–147-153
    - Governance 551.4–15
    - Maturity 551.5–138
    - Plan 551.4–17, 40, 69
    - Policy 551.4–16
    - Procedures 551.4–18-19
    - Roles 551.4–33-34
    - Secondary Goal 551.4–119
    - Team 551.4–20-25
    - Toolset 551.4–57
- Incremental Value 551.5–101
- Indicators 551.W–186
- Infection Monkey 551.5–113
- Infinite Games 551.2–23-25
- Infinite Strategy 551.2–25, 27
- Informal Training 551.1–84
- Information Domain 551.3–72
- Information Impact 551.4–37
- Infrastructure Domain 551.4–86
- Initial Access Vector 551.W–39
- Initial Compromise 551.4–45
- Initial Point of Entry/Infection 551.4–39
- Initiatives 551.5–55, 57
- Input-Driven Log Centralization 551.2–50
- Insider Threat 551.3–79, 101-105
  - Best Practices 551.3–105
  - Data Sources 551.3–104
  - Monitoring Goals 551.3–103
- Integrated Automation 551.5–97
- Intel Collection Plan 551.1–108
  - 551.W–37, 41
  - Example 551.W–41
- Intel Drivers 551.W–38
- Intel Provider 551.W–42
- Intel Requirements 551.W–38
- Intel-Driven D&R 551.3–74
- Intel-Driven IR 551.4–7
- Intentional Evidence 551.4–35
- Interaction Diagram 551.4–25
- Interactive Logons 551.4–59
- Interactive Tasks 551.5–100
- Intermediate Training 551.1–86, 88
- Internal Data Request 551.3–94
- Internal Factors 551.5–23
- Internet Connections 551.2–119
- Interval 551.5–72-73
- Interview – Should Not Do 551.1–80
- Interview Key Items 551.1–81
- Interviewing → Recruitment
- Intrinsic Motivation 551.5–7
- Intruders in the House 551.3–73
- Intrusion Detection Console 551.3–46
- Inventory 551.4–84
- Inventory Management System 551.4–35
- Investigation 551.1–52
  - 551.3–41
  - 551.4–39, 85
  - Bias 551.4–95-98
  - Mindset 551.4–94
  - Quality 551.4–106, 109-110
    - Review 551.4–111
    - 551.W–167-183
  - Tactics 551.4–90-93
  - Wrong Way 551.1–52
- Investigative Playbook Automation 551.5–106
- IOC 551.1–100, 103, 113
  - 551.2–15
  - 551.4–118
  - Definition 551.1–104
  - List 551.4–117
  - Lookup 551.2–34
- (ISC)² 551.1–91
- ISO27001 551.1–31
  - 551.4–11
  - 551.5–133
- ISO27005 551.1–32
- ISO2859-1 551.W–168
- Isolation 551.4–74

J

- JA4+ 551.2–62
- JARM 551.2–62
- Jerk 551.5–28
- Job Advertisement/Post 551.1–72-73

Job Hopping 551.1–77
Job Rotation 551.3–105
 551.4–125
Joint Publication 2-0 (Joint Intel) 551.1–99
Judgement 551.5–83, 91
  Simulation 551.5–106
Jupyter 551.3–8
  Notebooks 551.3–16

K

Kerberos TGT 551.4–59-60
Key Results 551.5–55
Key to Success 551.1–97
 551.2–20, 120
 551.3–28, 33, 41, 47, 54, 75
 551.4–27, 50, 99, 117, 124
 551.5–40, 51, 108
KMS 551.2–32, 36
Knowledge Base → SOC Knowledge Base
KPI 551.5–42, 45
 551.W–185
  Continuous Monitoring 551.5–56
  Identification 551.5–53
  Interaction 551.5–44
  Summary 551.5–67
KSA 551.1–89
 551.4–69, 80
 551.W–31-35

L

LAPS 551.4–60
Latency 551.5–148-149
Lateral Movement 551.2–108, 117
 551.3–48, 126
 551.W–216
  Protocols 551.2–59
Law Enforcement 551.4–128
Lazarus Group 551.4–101
 551.W–45
  Threat Profile 551.W–50
Leadership 551.2–22
Lean Manufacturing 551.5–146-147
Lean SOC 551.5–142-152
Least Privilege 551.3–105
Legal Approval 551.3–139
Lessons Learned 551.3–60
 551.4–122
Liaison 551.4–34
Life Safety Assessment 551.4–36
Link Analysis Diagram 551.4–103-105
Live Response 551.4–54
Local Accounts Used Over the Network 551.3–126
Local Admin Group 551.4–60
Location Logging 551.3–139
Log Centralization Strategies 551.2–50
Log Detection Analytics 551.3–19
Log Enrichment 551.2–57
Log-Normal Distribution 551.2–100
 551.W–88
Logistic Regression 551.5–105
Long-Tail Analysis 551.3–124
Lookalike Domain 551.3–96
Loss Exceedance Curves 551.5–89-90
Lures 551.3–142

M

MaGMa UCF 551.3–71
  Identifiers 551.W–142
Malicious Email 551.5–125
Maltego 551.4–93
  Casefile 551.4–103
Malware Analysis 551.4–67-68
  Tools 551.4–68
  Workstations 551.2–114
Malware Configurations 551.1–116
Malware Persistence 551.2–58
Malware Traffic 551.5–124-125
Management 551.2–22
Management Debt 551.5–30, 35
Managerial Models 551.2–10
Mandiant Attack Cycle 551.2–13
 551.3–122
Manual Analysis 551.4–67
Mass Malware 551.4–76
MDO 551.3–50-51
Measure Anything in Cybersecurity 🕮 551.5–85, 87
Measurement → Measures
Measures 551.4–119
 551.5–52, 62
  Design Recommendations 551.5–87-91
  Lag 551.5–63-64
  Lead 551.5–63-64
  Levels 551.5–72
   Operations 551.5–73
  Problems 551.5–84
   Summary 551.5–92
  Scale 551.5–87
Memory Forensics 551.4–39
Mere-Exposure Effect 551.5–85-86
Metasploit 551.5–113
Metrics 551.5–16-17
  Bad 551.5–17
  Classification 551.W–192-193
  Collection Tools 551.W–194-195
  Creation 551.W–184-200
  Definition 551.5–41
  Derivation Process 551.5–46-56
  Display Tools 551.W–195
  Example 551.W–191
  Fixation 551.5–83
  Good 551.5–17, 50-51
  Interaction 551.5–44
  Mapping to Goals 551.5–49

  - Measurement 551.5–52, 62
    - Design Recommendations 551.5–87-91
  - Motivation 551.5–37
  - Operational 551.5–54
  - Prioritization 551.W–193
  - Problem 551.5–84-85
  - Projects 551.5–67
  - Rate 551.5–51
  - Selection 551.W–184-200
  - Summary 551.5–67
- Metta 551.5–113
- Microsoft 551.4–66
  - Defender 551.4–64
- Missing Information 551.4–97
- Mission & Goals 551.1–26
- Mission Statement 551.1–26, 36
  551.W–25
- MITRE 551.3–9
  - 11 Strategies of World-Class SOC 551.5–156
  - ATT&CK 551.1–51
    551.2–16-17, 70-76
    551.3–121-123
    551.4–38, 92
    551.5–105, 122, 124
    - Cloud Matrix 551.4–82
    - Data Source Planning 551.2–70
    - Mapping 551.3–141
    - Matrix 551.2–16
      551.4–118
    - Object Types 551.2–71
    - Tactic Detection Capability 551.2–76
  - Cyber Analytics Repository 551.2–75
  - Engage Matrix 551.3–141
- Modern Defense Mindset 551.2–11
- Momentum 551.4–123
- Monitoring Goals 551.3–82, 89, 103
- Monte Carlo Analysis 551.2–102
  551.5–89-90
  551.W–88
- Mordor 551.3–17
- Morphological Matrix 551.4–99
- MSSP 551.1–15, 23, 68-70
  551.3–43-44
  551.5–53
  - Hybrid Model 551.3–43-44
  - Onboarding 551.1–69
- MTS Goal Hierarchy 551.W–148
  - Example 551.W–150
- Multi-Team Systems 551.4–22-25
  551.W–147

N

- NDA 551.3–105
- NDR 551.4–57, 65
- Negative Incentives 551.5–29
- Negative Value 551.5–101
- NETBIOS Lookup 551.5–103
- NetFlow 551.2–59-60
- Network Anomalies 551.2–99
- Network Logs 551.2–59
- Network Security Monitoring → NSM
- NICCS 551.W–36
- NICE Framework (NIST) 551.1–89-90
  551.W–31
  - Job Roles 551.W–32
- NIDS 551.2–59
- NIST National Checklist Program 551.4–12
- NIST SP 800-123 551.4–12
- NIST SP 800-171 551.1–29
- NIST SP 800-181 551.1–89
- NIST SP 800-30 551.1–32
- NIST SP 800-37 551.1–32
- NIST SP 800-39 551.1–32
- NIST SP 800-53 551.1–31
  551.4–119
- NIST SP 800-61 551.2–18
  551.4–18, 37
- Noise 551.3–34
- Nominal 551.5–72-73
- Non-Assignable Cause 551.W–182
- Non-Critical Systems 551.4–72
- Non-Default Events 551.4–80
- Noninteractive Logons 551.4–59
- Normal Distribution 551.2–100
- Normalization 551.2–56
  551.4–82
- NSG Flow Logs 551.2–67
- NSM 551.2–47
  551.4–32, 65
  - Challenge 551.2–60
  - Cloud 551.2–67
- NXLog 551.2–53
  551.3–85

O

- Objectives 551.5–55
- Observable Aggregator 551.1–104
- OCSF 551.4–82
- OCTAVE 551.W–28-30
- Offense Informs Defense 551.4–13
- Offense Magnitude 551.5–77
- OKR 551.5–42-43, 45, 59
  - Continuous Monitoring 551.5–56
  - Creation 551.5–55
  - Interaction 551.5–44
  - Metrics Derivation Process 551.5–46-56
  - Summary 551.5–67
  - System 551.5–39
- On-The-Job Training 551.1–84
- Onboarding → Service Provider
- OODA Loop 551.2–20-21
  551.3–136
  551.5–51
- OpenBAS 551.4–129

Operational Efficiency 551.5–14-16
Operations 551.3–83
Opportunity for Automation 551.5–99
OPSEC 551.3–144
.... 551.4–48, 68, 72, 76
Orchestration 551.5–97
Ordinal 551.5–72-73, 75-76, 78, 81
  Drop Numbers 551.5–88
  Mapping 551.5–88
  Problem 551.5–84
OSCD 551.3–12
OSQuery 551.3–72
.... 551.4–57
Output-Driven Log Centralization 551.2–50
Overconfidence 551.4–107
OWASP 551.3–86

P

Packet Mirroring 551.2–67
Pairing Employees 551.1–130
Palantir ADS 551.3–69
Palo Alto 551.4–66
PAP 551.W–166
Parsing 551.2–55
Pass-the-Hash 551.4–60
Pass-the-Ticket 551.4–60
Passkeys 551.2–121
Password Hash 551.4–59
Passwordless 551.2–121
Patching 551.5–82
  Prioritization 551.5–78-80
    Fixed 551.5–88
PCAP 551.3–17
PCI-DSS 551.1–29
.... 551.4–11, 36
Peer Review 551.4–106
.... 551.5–12
Penetration Testing 551.5–116
Perception 551.5–16
  Bias 551.4–97
Perfect Forward Secrecy → PFS ....
Performance Management 551.5–33
Perimeter Model 551.2–122
Periodic Review 551.4–110
.... 551.5–15
Permissible Actions Protocol → PAP ....
Permissions 551.W–24
Persistence Mechanisms 551.3–126
.... 551.4–61
Personality Types 551.5–28
PFS 551.2–61
Phishing Alert 551.2–99
PICERL 551.2–18-19
.... 551.4–72
PII 551.3–99
Pipeline 551.3–59
PIR 551.1–120
  Periodicity 551.W–42
  Process 551.W–37-43
Plan 551.4–15
Playbook 551.4–40-43
.... 551.5–97
  Development 551.W–154-166
  Example 551.4–41
  Workflow 551.W–157
Poisson Distribution 551.2–93-97
.... 551.W–87
Policies 551.1–33
Policy 551.4–15
Portability 551.4–86
Positive Team Culture → Culture ....
Post Enrichment 551.3–28
Post-Exploitation 551.3–48, 126
  Focus 551.2–11
Post-Incident Activity 551.4–18, 116
  Tracking 551.4–123
Post-Recovery 551.4–116
PowerShell 551.4–54, 57
  Empire 551.5–113
  Remoting 551.2–59
.... 551.4–60-61
Pre-Commit 551.3–83
Pre-Response Briefing 551.4–124
Pre-Screening 551.1–82
Prediction 551.4–107
  Exploit 551.5–81
Predictive Analysis 551.5–105
Premortem Analysis 551.4–107
Preparation 551.4–7, 10, 18, 80
  Summary 551.4–27
Presumption of Compromise 551.2–11
.... 551.3–113
Preventative Controls 551.4–14
Prevention 551.4–10
  Testing 551.5–116
Prioritization 551.2–16
.... 551.4–83
  Alert 551.5–77
  Importance 551.5–71
  Issues 551.5–74-82
    Summary 551.5–92
  Patching 551.5–78-80
Priority Account 551.3–50
Priority Threat Group Profile 551.W–46
  Example 551.W–48
Privacy Shield 551.1–29
Privileged Accounts 551.2–109-112
  Usage 551.3–126
Proactive Detection 551.2–11
Probabilistic Modeling 551.2–97, 100
Probability 551.2–88, 93-96
.... 551.5–89
  Calibrated Assessment 551.5–87
  Estimation Bias 551.4–97
Procedure 551.4–15

- Process Creation 551.2–72
- Processes 551.5–57
  - Failures 551.W–229
  - In Control 551.W–183
  - Out of Control 551.W–183
- Product Agnostic Analytics 551.3–72
- Production 551.3–83
- Program Frameworks 551.1–31
- Prophet of Rage 551.5–28
- Proximal Goal 551.W–147
- Pseudocode 551.3–72
- PsExec 551.4–59, 62
- Purple Team 551.5–115
  - ATT&CK Automation 551.5–113
- Purple Teaming 551.3–60
  - 551.4–83
  - 551.5–114
  - Assessment 551.W–201-224
    - Metrics 551.W–213
  - Campaign 551.W–206
  - Methodology 551.5–118-120
  - Tracking Tools 551.5–121
- Pyramid of Pain 551.2–15
- Python Script 551.5–95

Q

- Qualitative Labels 551.5–84, 88
- Quality 551.5–148, 151
  - Improvement 551.W–225-231
  - Requirements 551.1–109
- Quality Review 551.4–111
- Quantitative Risk Analysis 551.5–89-90
- Quarantine 551.3–51
  - Zone 551.2–114
- QUIC 551.2–60

R

- Ransomware 551.2–123
  - 551.5–90
- Ratio 551.5–72-73
- RDP 551.4–59-60
- Rebuild 551.4–75
- Recorded Future 551.1–99
- Recoverability Effort 551.4–37
- Recovery 551.4–18
  - Activities 551.4–115
- Recruitment 551.1–71-82
  - Hiring 551.1–74-75
  - Interviewing 551.1–76-82
    - Should Not Do 551.1–80
    - Technical Tests 551.1–78
- Red Team 551.3–49, 98
  - 551.5–115
  - 551.W–209
  - Testing 551.W–78
- Red Teaming 551.5–114
- Redacted Version 551.4–117
- Redmine 551.3–65, 68
- Reflection 551.5–14-15
- Registry Run Keys 551.3–121
  - 551.4–61
- Relationship Management 551.1–39
- Relative Likelihood 551.4–100
- Relevance Period 551.2–15
- Remote Command Execution 551.4–62
- Remote Credential Guard 551.4–60
- Remote File Share 551.4–59
- Remote Team Management 551.1–131
- Removal 551.4–75
- Repetitive Tasks 551.5–97, 100
- Report Processing 551.5–105
- Response 551.4–39
- Response-Driven Teams 551.2–11
- Restricted Admin Mode 551.4–60
- Retention 551.1–64, 67
  - Strategy 551.4–85
- Revision of Plans and Procedures 551.4–121
- Rewarding 551.5–83
- Rework 551.5–146
- RFC Specification 551.3–34
- Risk Assessment Methodology 551.W–28
- Risk Based Scoring 551.3–35
- Risk Frameworks 551.1–31-32
- Risk Matrices 551.5–74-75, 89
- Risk of Exploitation 551.5–81
- Risk Register 551.W–229
- Risk-Informed Strategy 551.2–11
- Rogue DNS Server 551.2–60, 64
- Room Layout 551.1–124
- Root Causes 551.4–117
- Rotating Duty 551.3–42
- RPA 551.5–97
- RPN 551.W–229-230
- RTA 551.5–113
- RunAs 551.4–59

S

- Sample Size 551.W–169-172
- Sampling 551.4–111
- Scheduled Tasks 551.4–61
- Scikit Learn 551.5–105
- Scoreboard 551.5–58, 64-65
- Scribe 551.4–34
- SCRM 551.3–88
- Second-Order Effects 551.2–25
- Secrepo 551.3–17
- Secure Configurations 551.4–14
- Security Director 551.1–62
- Security Metrics 🕮 551.5–50
- Security Monitoring 551.3–83, 88, 115
- Security Policy Templates (SANS) 551.1–33
- Security Requirements 551.W–30

- Security Scanning ... 551.3–83
- Segregation of Duties ... 551.3–105
- Selective Attention Test ... 551.4–97
- Self-Review ... 551.4–106
- Seniority ... 551.5–33
- Sensitive Information ... 551.3–48
- Sentinel
  - Notebooks ... 551.3–16
- Separation of Accounts ... 551.2–109-112
- Service Domain ... 551.4–86
- Service Provider ... 551.1–68-70
  - Onboarding ... 551.1–69
- Shallow Work ... 551.5–22
- Shared Mindset ... 551.1–133
- Sharing ... 551.1–117
- Shift ... 551.1–65, 67
- SIEM ... 551.2–32-35, 54
  - Agent ... 551.2–53
- Sigma ... 551.3–8, 11-15
  - Example ... 551.W–95-96
  - Rule Format ... 551.3–13
- SIM3 Model ... 551.5–137
- Similar To Me (Bias) ... 551.1–80
- Simon Sinek ... 551.2–23-27
- Simulation Platform ... 551.4–129
- SIR ... 551.W–40
- Site Reliability Engineering → Google SRE ...
- Situational Awareness ... 551.3–81, 83
- Skills ... 551.5–9, 11, 18
  - Assessment ... 551.W–34
- SKUE ... 551.4–125
- SLA ... 551.1–68
  - ... 551.4–69
  - ... 551.5–53
- SMB ... 551.3–118
  - ... 551.4–60
- SME ... 551.4–26, 34, 47
- SNI ... 551.2–61
- SOAR ... 551.2–32, 35
  - ... 551.4–39, 41-42
  - ... 551.5–95
  - Categories ... 551.5–103
- SOC ... 551.1–9-10
  - Analyst Activities ... 551.W–83
  - As Production Line ... 551.5–142
  - Assessment ... 551.1–31
    - ... 551.5–110
    - Summary ... 551.5–128
  - Average ... 551.1–13-14
  - Breakdown ... 551.1–13
  - Building ... 551.1–122-134
  - Capability Assessment ... 551.5–132-140
    - Summary ... 551.5–140
  - Challenges ... 551.1–17
  - Charter ... 551.1–36
    - ... 551.5–136
    - Components ... 551.W–24
    - Examples ... 551.W–27
  - Cloud Data ... 551.2–120
  - Detection Capabilities ... 551.2–75
  - Duty ... 551.1–65
  - Enclave ... 551.2–118, 120
  - Functions ... 551.1–44, 46
    - Auxiliary ... 551.1–47-48, 60-62
    - Core ... 551.1–47-48
    - Summary ... 551.1–55
  - High-Level View ... 551.1–45
  - Internal VS External ... 551.1–23
  - Knowledge Base ... 551.2–32, 36
    - ... 551.4–125
  - Loop ... 551.2–21
  - Manager ... 551.1–62
  - Maturity ... 551.1–14-16
  - Measurement ... 551.5–62
  - Members & Data ... 551.2–107-124
    - Summary ... 551.2–125
  - Models (Mental) ... 551.2–10-28
  - Models (Org) ... 551.1–60-64
  - Operations ... 551.2–9, 26
  - Planning ... 551.1–25
    - Summary ... 551.1–40
  - Reference Systems ... 551.2–32
  - Requirements ... 551.1–28
  - Scale ... 551.1–23
  - Services & Capabilities ... 551.1–35
  - Survey ... 551.1–67, 129
  - Team Creation ... 551.1–59
    - Summary ... 551.1–92
  - Technology ... 551.2–41
    - Selection ... 551.2–37-39
  - Tiered VS Tierless ... 551.1–63-64
  - Virtual ... 551.1–128, 130-131
    - Onboarding ... 551.1–130
- SOC As a Peer ... 551.1–62
- SOC-CMM ... 551.1–31
  - ... 551.5–133-136, 139
  - Assessment Tool ... 551.5–136
  - Maturity Measurement ... 551.5–134-135
- Social Engineering ... 551.3–79
  - Toolkit ... 551.3–138
- SOMM ... 551.1–14
- Sources of Truth ... 551.4–14
- SOX ... 551.1–30
  - ... 551.4–11
- SpectreOps ... 551.3–73
- Speed of Intel Use ... 551.1–113
- SPF ... 551.3–96
- SPL (Splunk) ... 551.3–14
- Splunk ... 551.3–17
  - Attack Range ... 551.3–18
- Spoofed Email ... 551.3–96
- Stack Ranking ... 551.3–124
- Staff Retention ... 551.5–8-24
  - Summary ... 551.5–8-24
- Stakeholder Requirements ... 551.5–53
- Standardization ... 551.3–8

- Start Value 551.5–43
- Steering Committee 551.1–37
  551.W–38
- STIG 551.4–12
- STIX 551.1–114
  551.2–71
- Stop the Bleeding 551.4–72-73
- Strategic Drivers 551.W–28
- Strategic Planning 551.3–140
  551.5–132, 140
- Strategies of a World-Class SOC 🕮 551.5–47
- Strong Requirements 551.W–37
- Strong Structure 551.1–133
- Structured Self-Critique 551.4–108
- Study Plan 551.2–39
- Submission Explorer 551.3–51
- Success Factors 551.W–24, 28, 185
- Supervised Learning 551.5–105
- Supply Chain 551.3–79, 87-90
  - Data Sources 551.3–90
  - Monitoring Goals 551.3–89
  - Risk Management 551.3–88
- Support 551.1–60
- Supportive Context 551.1–133
- Surgical Removal 551.4–75
- Suricata 551.2–59
- Survey 551.2–88, 97, 100
- Sysinternals Suite 551.4–62
- Syslog Daemon 551.2–53
- Syslog-ng 551.3–85
- Sysmon → **Tools**
- Systems 551.4–9

T

- Tactical Log Collection 551.2–50
- Tagging 551.2–56
  551.3–50
- TaHiTI Methodology 551.W–138-139
- Target Value 551.5–42, 53
- Targeted Attack 551.3–48
- Targeted Malware 551.4–76
- Taskwork 551.4–23
- TAXII 551.1–114
- Taxonomy 551.4–82
- TCP/853 551.2–65
- Team 4-D 551.1–133
- Team Coordination → Cross-Team Coordination
- Team Feedback 551.4–124
- Teamwork 551.4–23
  551.5–27
- Technical Capability 551.5–133
- Technical Depth Probing 551.1–79
- Technical Models 551.2–10
- Telemetry 551.4–87
- Telnet 551.4–62
- Temporal Score 551.5–81-82
- Theory of Constraints 551.5–61
- Threat 551.3–109
  - Actor 551.5–116
    551.W–39
    - Assessment 551.W–44-51, 155
  - Detection 551.4–84
    - Analytics 551.5–12
    - Open Standard 551.4–82
  - Explorer 551.3–51
  - Group 551.W–44-46
    - Layers 551.W–73
    - Priority 551.W–64
  - Hunting 551.1–50
    551.3–108-130
    - Example 551.3–118
    - How 551.3–115-117
    - Options 551.3–125
    - Planning 551.W–138-146
    - Process 551.3–116
    - Reference Guides 551.3–129
    - Summary 551.3–130
    - Tools 551.4–64
    - Value 551.3–127
    - What 551.3–109
    - When 551.3–113
    - Where 551.3–126
    - Who 551.3–112
    - Why 551.3–111
  - Intelligence 551.1–60-62, 96-118
    551.3–90
    551.5–118
    - Bias 551.4–98
    - Data VS Info VS Intel 551.1–98
    - Feedback 551.4–116, 118
    - In The SOC 551.1–101
    - Levels 551.1–100-101
    - Measurement 551.1–105-107
    - Mental Models 551.1–111-112
    - Platform 551.1–115-117
    - Producers & Consumers 551.1–103
    - Production 551.1–108
    - Questions 551.1–110
    - Sources 551.1–102
    - Speed of Use 551.1–113
    - Transport 551.1–114
  - Landscape 551.1–100
    551.W–39
  - Model 551.3–49
    551.4–38
  - Modeling 551.1–27
    551.W–28
  - Protection 551.3–51
  - Report 551.5–105
  - Scenarios 551.W–30
- Threat-Informed Defense 551.2–40
- Ticket Lifetime 551.4–60
- Tiering 551.1–63-64
  551.3–42
- Timeline 551.4–44-45, 105, 117

Review 551.4–121
Timeliness 551.1–106
TIMWOOD 551.5–147
TIP 551.1–103, 115
.... 551.2–32, 34-35
.... 551.3–68
.... 551.W–47
Remark 551.1–104
TLS 551.2–60-63
Fingerprinting 551.2–62
Top-Down Derived Metrics 551.5–49
Tor 551.2–62
Traceability Matrix 551.5–139
Traffic Capture 551.2–67
Traffic Mirroring 551.2–67
Training 551.1–83-92
Plan 551.1–88
Transactive Memory 551.4–125
Transitional Training 551.1–86, 88
Triage 551.1–51
.... 551.2–85
.... 551.3–41
Optimization 551.3–51
Place 551.3–46
Queue 551.3–30
Requirements 551.3–45
Software & Features 551.3–47
Tripwires 551.3–134
True Positives 551.3–25
Testing 551.3–69
Trust 551.5–12
TTP 551.1–100
.... 551.3–19, 140
.... 551.4–38, 44, 75
.... 551.5–115, 117-118
TTP-Focused Attack Models 551.2–16
Two in the Box 551.5–31

U

UEBA 551.3–104
Unexpected Protocols Outbound 551.3–126
Unintentional Evidence 551.4–35
Unit Test 551.3–72
Unknown Unknowns 551.3–111
Unstructured Data 551.5–97, 106
Unstructured Documents 551.2–36
Urgency 551.5–59
US DoD 8140 .... 551.1–88
Use Case 551.3–33-34, 62-71
Attributes 551.W–115
Database 551.3–64-69
Development 551.3–67, 75
Example 551.3–70
Management 551.W–113-137
SOC-Assisted 551.3–79, 106
Tracking 551.3–63
User Account Activity 551.4–84

V

Value 551.5–146
Vendor Lock-In 551.3–12
.... 551.W–95
VERIS Framework 551.4–37-38
.... 551.5–54
Virtual Interview 551.1–82
Virtual Network Tap 551.2–67
Virtual Team Work 551.1–133
Virtual Work 551.1–129
Visibility 551.3–115
.... 551.5–119
VMWare 551.4–66
VNC 551.4–59
Volatile Evidence 551.4–39
VPC Flow Logs 551.2–67
Vulnerability 551.3–48
Management System 551.4–35

W

WannaCry 551.4–101
Waste 551.5–146
Types 551.5–147
Watch & Learn 551.4–75-76
Wazuh 551.4–64
Web-Bugged Email 551.3–139
Webhooks 551.W–194
Website Clone 551.3–138
WIG 551.5–58-59, 66
Windows 10 .... 551.4–60
Windows 7 / Server 2008 R2 .... 551.4–60
Windows Defender 551.4–60
Windows DNS 551.2–64
Windows Event Forwarding 551.2–53
Windows Logs 551.1–49
WinRM 551.4–61
Wiping 551.4–75
WMF 551.4–61
WMI 551.4–54, 57, 63
Workflow 551.5–97
Workload Estimation 551.2–88

X

XDR 551.2–32
.... 551.4–57, 66

Y

YAML 551.3–13
YARA 551.3–8, 10
.... 551.4–68

Z

Zero Trust 551.2–122-123
.... 551.3–89