

# SEC450 – Blue Team Fundamentals: Security Operations and Analysis



This work is licensed under a Creative Commons Attribution 4.0 International License, by A. D'Hondt  
Template available at <https://github.com/academic-templates/tex-course-index-template>

## Topics

### Learning Objectives ..... 450.1-16

### Sec Ops Teams, Tools and Mission

SOC Foundations .....	450.1-18-28
SOC Organization & Functions .....	450.1-30-41
SOC Data Collection .....	450.1-43-55
Introduction to SIEM .....	450.1-57-68
Building SIEM Queries .....	450.1-72-84
SIEM Visualizations & Dashboards ..	450.1-88-100
Know Your Enemy .....	450.1-104-114
Threat Intelligence Platforms .....	450.1-116-128
Alert Generation & Processing .....	450.1-132-144
IMS & SOAR Platforms .....	450.1-146-162

### Network Traffic Analysis

Network Architecture .....	450.2-6-16
Traffic Capture & Analysis .....	450.2-18-28
Understanding DNS .....	450.2-30-50
DNS Analysis & Attacks .....	450.2-54-82
Understanding HTTP .....	450.2-86-101
HTTP(S) Analysis & Attacks .....	450.2-105-121
HTTP/2 & HTTP/3 .....	450.2-123-130
Spotting Malicious Encrypted Traffic ..	450.2-134-143
Common Protocols for Post-Exploitation ..	450.2-145-159

### Endpoint Defense, Security Logging & Malware Identification

Endpoint Attack Tactics .....	450.3-6-29
Endpoint Defense In Depth .....	450.3-31-54
How Windows Logging Works .....	450.3-56-68
How Linux Logging Works .....	450.3-70-80
Interpreting Important Events .....	450.3-82-113
Log Collection, Parsing & Normalization ..	450.3-117-129
File Contents & Identification .....	450.3-133-147
Identifying & Handling Suspicious Files ..	450.3-149-171

### Efficient Alert Triage & Email Analysis

Alert Triage & Prioritization .....	450.3-6-22
Structure Analytical Techniques .....	450.3-26-53
Models & Concepts for Infosec .....	450.3-55-84
Incident Closing & Quality Review ..	450.3-88-97
Analysis OPSEC .....	450.3-101-118
Email Header Analysis .....	450.3-120-149
Email Content Analysis .....	450.3-151-163

### Continuous Improvement, Analytics & Automation

Improving Life in the SOC .....	450.3-6-27
Analytic Features & Enrichment .....	450.3-29-48
New Analytic Design, Testing & Sharing ..	450.3-50-76
Tuning & False Positive Reduction ..	450.3-78-98
Automation & Orchestration .....	450.3-102-119
Improving Operational Efficiency & Workflow ..	450.3-121-131
Containing Identified Instructions ..	450.3-135-158
Skill & Career Development .....	450.3-162-175

### Workbook

Advanced SIEM Log Search with SQL ..	450.W-25-41
Alert Triage & Prioritization ..	450.W-258-289
Alert Tuning & False Positive Reduction ..	450.W-366-385
Analyzing Malicious DNS .....	450.W-138-146
Analyzing Phishing Email Headers	450.W-353-365
Analyzing TLS Traffic Without Decryption ..	450.W-185-197
Collecting & Documenting Incident Information ..	450.W-315-352
Crafting SIEM Visualizations and Dashboards for Threat Hunting .....	450.W-42-70
CTF Instructions .....	450.W-420-422
Dissecting Common Malware File Types ..	450.W-235-257
DNS Requests, Traffic & Analysis ..	450.W-114-137
HTTP/2 & HTTP/3 Traffic Analysis ..	450.W-167-184
Incident Management Systems - Playbooks, Workflow, Automation .....	450.W-92-113
Log Enrichment & Visualization ..	450.W-221-234
SOC Automation - File Analysis ..	450.W-386-402
SOC Automation - Incident Containment ..	450.W-403-419
Structured Analysis Challenge ..	450.W-290-314
Threat Hunting with a SIEM in Windows Logs ..	450.W-198-220
Using a SIEM for Log Analysis .....	450.W-4-24
Using MISP Threat Intel Platform ..	450.W-71-91
Wireshark & HTTP/1.1 Analysis ..	450.W-147-166



# SEC450 – Blue Team Fundamentals: Security Operations and Analysis

## Categories

### Key Takeaways

Attack Surface Reduction Rules .....	450.3–38
Blue Team Truth .....	450.1–27–28
Blue Team’s Mission .....	450.1–15, 20
Cyber Security Operations .....	450.1–12–13, 19
Defense Mindset .....	450.1–14
DNS Lookup .....	450.2–33
DoH & DNSSEC .....	450.2–46–47
Domain-to-IP Safe Mapping .....	450.2–57
Endpoints Defense in Depth .....	450.3–31
Enemy & Attack Types .....	450.1–108, 114
Events, Alerts & Incidents .....	450.1–133, 136, 140
Host vs Network Firewall .....	450.3–40
HTTP/1.1 vs HTTP/2 .....	450.2–125
Incident Management System .....	450.1–148, 154
Linux Log Path .....	450.3–76
Log Collection Pipeline .....	450.3–118
Log Ingestion Pipeline .....	450.3–129
Log Life Cycle .....	450.3–127
Models for Information Security .....	450.4–55
Monitoring .....	450.1–44, 52, 55
PCAP Collection .....	450.2–22, 25
Protocol Tunneling .....	450.2–153
Risk Appetite .....	450.1–23
SIEM .....	450.1–61, 63, 68
Visualization .....	450.1–89, 100
Workflow .....	450.1–73, 84
Sigma Signatures & Queries .....	450.5–71–75
SOC Charter .....	450.1–22
SOC Human Capital Model .....	450.5–22
SOC Organization .....	450.1–31, 34, 36, 38
SOC Tools Together .....	450.1–160
Threat Intelligence Platform .....	450.1–118, 121, 128
TLS Decryption .....	450.2–136
URI Decoding .....	450.2–87
Visibility Points .....	450.2–10
When Each Model of InfoSec Applies .....	450.4–81
Windows Log Path .....	450.3–58
Zero Trust Architecture .....	450.2–13
Zones & Traffic Flows .....	450.2–8

### Common Attack Patterns

Contact To A Sinkholed Domain .....	450.4–15
Data Exfiltration Through TFTP .....	450.4–15–16
DNS Tunneling .....	450.2–70–74
DNS-Based .....	450.2–64
Domain Shadowing .....	450.2–68
Exploit Attempt In Perimeter .....	450.4–17–18
Exploit Kit Delivered To User’s Browser .....	450.4–18
Homoglyph .....	450.2–78–79
Malware Delivery Through HTTP .....	450.4–16
Malware Delivery Through SMTP .....	450.4–15
Microsoft Office Documents .....	450.3–155
Phishing Served Over HTTP/3 .....	450.W–183
Phishing With IDN .....	450.2–81
Request To A Suspicious Website .....	450.4–15
Rogue Device .....	450.2–146
SMB Attacks .....	450.2–151

Spear Phishing .....	450.4–19
Weaponized USB Stick .....	450.4–18
Worm .....	450.2–14
ZeroLogon Attack .....	450.4–18

### Tools

AlienVault OTX .....	450.W–131
Arkime .....	450.W–259, 263–269
Search .....	450.W–266–269
AuditD 🐍 .....	450.3–79, 89
Output Example .....	450.3–90
Starter Rules .....	450.3–90
aureport 🐍 .....	450.3–89
Autofill .....	450.5–121, 123
AutoIt .....	450.5–130
Chrome Smart Keywords .....	450.5–126
CyberChef .....	450.W–242
dhclient 🐍 .....	450.W–114
dig 🐍 .....	450.2–58
..... 450.W–117–122, 356, 403–404	
domain_stats2 .....	450.2–62
eslogger 🍏 .....	450.3–92
file .....	450.3–134–135
..... 450.W–237, 255	
Firefox Smart Keywords .....	450.5–125
Greasemonkey .....	450.5–121, 129
hexdump .....	450.3–133–134
..... 450.W–255	
Ipconfig 📈 .....	450.2–31
journalctl 🐍 .....	450.3–78
lnkinfo 🐍 .....	450.3–158
..... 450.W–247	
LnkParse3 .....	450.3–158
logger 🐍 .....	450.3–79
Logstash .....	450.1–66
..... 450.W–224–230	
MailHog .....	450.W–398–400
Maltego 🟡 .....	450.4–42
MISP .....	450.1–123–127
Correlation Graph .....	450.W–87–89
Event .....	450.W–80–82
Freetext .....	450.W–83–86
Homepage .....	450.W–74
Threat Intel Context .....	450.W–75–79
Node-RED .....	450.5–113
..... 450.W–386–397, 404–419	
nslookup .....	450.2–58
OneNoteAnalyzer 📈 .....	450.3–158
..... 450.W–256	
OpenSearch .....	450.1–66, 81
..... 450.W–198–219	
Alerts by Category .....	450.W–371, 379
Alerts Tags per Signature .....	450.W–369, 378
Available Tables .....	450.W–29
Dashboards .....	450.W–61–65
Suricata Alerts .....	450.W–368–384
Panels .....	450.W–5–9
Reference Queries .....	450.W–22
Visualizations .....	450.W–43–44, 54–56



# SEC450 – Blue Team Fundamentals: Security Operations and Analysis

---

Outlook Quick Parts .....	450.5–124
PassiveTotal (RiskIQ) 🛡️ .....	450.4–111
Pulsedive OSINT Extension .....	450.5–127
Regex101 🛡️ .....	450.5–58
Regepx 🛡️ .....	450.5–58
<b>sigcheck.exe</b> .....	450.3–165
Sigma2MISP .....	450.5–75
Sputnik OSINT Extension .....	450.5–127
Tampermonkey .....	450.5–121, 129
tcpdump .....	450.W–115
TextExpander .....	450.5–121
TheHive .....	450.1–153–154
Alert Handling .....	450.W–95–98
Case .....	450.W–99
Create Case From Selection .....	450.W–286–288
Credential Expose Template .....	450.W–328
Main Interface .....	450.W–94
Playbook .....	450.W–100
Playbook Completion .....	450.W–328–351
Related Alerts .....	450.W–273
Similar Cases .....	450.W–273
Triage .....	450.W–259–260, 272–277
Workflow .....	450.1–154
Tshark .....	450.W–196–197
URLQuery.net 🛡️ .....	450.4–155
URLScan.io 🛡️ .....	450.4–109
Virustotal 🛡️ .....	450.4–107
.....	450.W–131, 252, 280
Scan vs Search .....	450.4–109
whois 🗣️ .....	450.2–62
Wireshark .....	450.2–26
Conversations 📱 .....	450.W–149–150
DNS Analysis .....	450.W–124–129
DoH .....	450.2–48–49
Analysis .....	450.W–132–134
Example Display Filters .....	450.2–27
Export Objects 📁 .....	450.W–160–161
HTTP/2 .....	450.2–128
Export Packet Bytes 📁 .....	450.2–128
.....	450.W–176–177, 182
Follow HTTP Stream 📱 .....	450.W–156–157
HTTP/2 .....	450.2–127
Follow HTTP/2 Stream .....	450.W–171
HTTP Display Filters .....	450.W–164–165
HTTP/2 .....	450.2–127
Carving Support .....	450.2–100, 128
HTTP/3 Support .....	450.2–129
.....	450.W–179
Protocol Hierarchy 📱 .....	450.W–148
TLS/SSL Keylog File .....	450.W–167, 179
User Interface .....	450.2–26
yEd .....	450.4–42
Zeek .....	450.2–23–24
.....	450.W–194–196
zeek-cut .....	450.W–195–196
<b>Summaries</b>	
Alert Triage Prioritization .....	450.4–22
Analysis OPSEC .....	450.4–118
Analytic Design, Testing & Sharing .....	450.5–76
Analytic Features & Enrichment .....	450.5–48
Automation & Orchestration .....	450.5–119
Containing Identified Intrusions .....	450.5–158
DNS Analysis & Attacks .....	450.2–82
Email Authentication Methods .....	450.4–141
Email Content Analysis .....	450.4–163
Email Header Analysis .....	450.4–149
Endpoint Attack Tactics .....	450.3–29
Endpoint Defense-in-Depth .....	450.3–54
Events, Alerts & Incidents .....	450.1–144
File Content & Identification .....	450.3–147
How Linux Logging Works .....	450.3–80
How Windows Logging Works .....	450.3–68
HTTP/2 & HTTP/3 Traffic Analysis .....	450.2–130
Identifying & Handling Suspicious Files .....	450.3–171
Improving Life in the SOC .....	450.5–27
Improving Ops Efficiency & Workflow .....	450.5–119
IMS & SOAR Platforms .....	450.1–162
Incident Closing & Quality Review .....	450.4–97
Interpreting Important Events .....	450.3–113
Know Your Enemy .....	450.1–114
Log Collection, Parsing, Normalization .....	450.3–129
Models & Concepts for InfoSec .....	450.4–55, 84
Network Architecture .....	450.2–16
Network Traffic Analysis .....	450.2–161
SIEM - Build Queries .....	450.1–84
SIEM - Introduction .....	450.1–68
SOC .....	450.1–41
Spotting Malicious Encrypted Traffic .....	450.2–143
Structured Analytical Techniques .....	450.4–53
Threat Intelligence Platforms .....	450.1–128
Traffic Capture & Analysis .....	450.2–28
Tuning & False Positive Reduction .....	450.5–98
Understanding DNS .....	450.2–50
Understanding HTTP .....	450.2–101

## References

<i>Analysis of Competing Hypothesis</i> 📱 .....	450.4–46
<i>Crafting The InfoSec Playbook</i> 📱 .....	450.5–68
FOR578 - Cyber Threat Intelligence .....	450.4–66
FOR610 - Reverse Engineering Malware .....	450.2–109
.....	450.3–137
LDR551 - Building and Leading Security Operations Center .....	450.1–40
<i>On The Failure to Eliminate Hypotheses in a Conceptual Task</i> 📱 .....	450.4–45
<i>Psychology of Intelligence Analysis</i> 📱 .....	450.4–27, 36
SEC511 - Advanced Threat Detection and Monitoring .....	450.3–61
.....	450.5–156
SEC555 - SIEM Tactical Analytics .....	450.W–230
SEC595 - Applied Data Science & Machine Learning for Cybersecurity Professionals .....	450.5–59
<i>Site Reliability Engineering</i> 📱 .....	450.5–117–118
<i>Structured Analysis Techniques for Intelligence Analysis</i> 📱 .....	450.4–37
<i>Thinking Fast &amp; Slow</i> 📱 .....	450.4–34



# SEC450 – Blue Team Fundamentals: Security Operations and Analysis

---

## A

A/AAAA Record	450.2–35, 38
Accidental Block	450.5–109
Account Domain	450.3–82
Account Name \$	450.3–83, 110–111
Accuracy (Data Tables)	450.W–27
ACH → Analysis of Competing Hypothesis	.....
ACL	450.2–7
Active Directory	450.2–44
.....	450.3–82–83
.....	450.5–45
Active Intrusion Discovery	450.5–139
Active Scanning	450.3–32
Actor Characterization	450.1–151
Administrative Account Usage Location	450.5–91
Advanced Security	450.3–66
Adversary	450.4–72
Adware	450.1–108
.....	450.5–88
Agent-Based Deployment	450.3–50, 119
Aggregation	450.1–77–78, 81
SQL Functions	450.W–34
Air-Gapped Networks	450.5–142
Alert	450.1–133
Cherry-Picking	450.5–25, 83
Disabling	450.5–83
Fatigue	450.5–83, 90
Fidelity	450.5–36–37, 79
High	450.5–42, 79
Increase	450.5–91
Low	450.5–86–87
Frequency	450.5–90
Generation	450.5–81
Maximum	450.5–82
Low Priority	450.4–21
.....	450.5–88, 98
Non-Actionable	450.5–89
Pattern-Based	450.5–53
Poor Types	450.5–85
Queries From Signatures	450.5–74
Queue	450.1–137–138, 154
.....	450.5–81–82
Reduction	450.5–95
Selection	450.5–94
Threshold-Based	450.5–64
Timestamp Issue	450.W–260
Triage	450.1–137, 148
.....	450.4–15, 18–19
.....	450.5–81
.....	450.W–261–271
Tuning	450.1–95
.....	450.5–79
Down From Default	450.5–84, 89
Up From Zero	450.5–84, 89
Types	450.1–141
Unique	450.4–20
Volume	450.5–79
High	450.5–90
Typical vs Ideal	450.5–78

Workflow	.....	450.1–139
Alexiou Principle	.....	450.4–57
Allow List	.....	450.5–61–63
Pseudo	.....	450.5–66
ALPHV	.....	450.1–105
Ambiguity	.....	450.4–58
Analysis Desktop	.....	450.4–112
Analysis of Competing Hypothesis	.....	450.4–46
Example: WannaCry Attribution	.....	450.4–51
Lessons	.....	450.4–52
Matrix	.....	450.4–49
Example	.....	450.W–303
Steps	.....	450.4–47
Template	.....	450.W–313
Tips for Success	.....	450.4–50
Analyst Empowerment	.....	450.5–136
Analytic Thinking	.....	450.4–34
Analytics	.....	450.5–36
High Quality	.....	450.5–42
Machine Learning-Based	.....	450.5–59
Metadata-Based	.....	450.5–53
Sharing	.....	450.5–70–71
Automation	.....	450.5–75
Simple Is Best	.....	450.5–68
Strategy	.....	450.5–84
Analyzers	.....	450.1–153
.....	.....	450.W–104
Angler Exploit Kit	.....	450.2–93
Anomalous Login Attempts	450.W–198, 206, 209–212	
Anomaly Detection	.....	
.....	.....	450.2–159
.....	.....	450.3–52
.....	.....	450.5–91
Anomaly Hunting	.....	450.2–21
Anomaly-Based Alert	.....	450.1–141–143
Anonymous IP Source Address	.....	450.3–102
Anti-Exploitation	.....	450.2–15
.....	.....	450.3–35
Antispam Header	.....	450.4–145
Antivirus	.....	450.3–41
Deny List-Based	.....	450.5–63
Apache Logs	.....	450.3–77
AppArmor	.....	450.3–43
Application Behavior	.....	450.2–11
Application Control	.....	450.3–43–45
Alerts	.....	450.3–66
Bypass	.....	450.3–44–45
Rules	.....	450.3–104
Violations	.....	450.3–66
Application Guard for Office	.....	450.4–153
Application Layer Logs	.....	450.2–23
Application Logs	.....	450.3–66, 77
Application Monitoring	.....	450.1–49, 55
Application Protocols	.....	450.5–148
AppLocker	.....	450.3–43, 66, 104
.....	.....	450.5–157
Allow List-Based	.....	450.5–63
Approved Protocols List	.....	450.5–91
APT	.....	450.1–110
Attack Steps	.....	450.4–9



# SEC450 – Blue Team Fundamentals: Security Operations and Analysis

Model .....	450.4–61	Integration .....	450.1–149
Naming .....	450.1–111	Paradox .....	450.5–116
APT1 .....	450.1–105	Preconditions .....	450.5–19
APT19 .....	450.2–115	Should Use ? .....	450.5–104
APT28 .....	450.1–111	AutoOpen .....	450.W–247–248
AQL .....	450.1–81	Autoruns  .....	450.3–47
ARC .....	450.4–131, 143	AWS .....	450.1–50
Archive .....	450.3–126	Lambda Function .....	450.1–51
ArcSight .....	450.W–225	Azure  .....	450.1–50
Arkime  .....	450.2–22, 25	Active Directory .....	450.3–101
Artificial Intelligence .....	450.5–115	Log Analytics .....	450.1–65
ASCII .....	450.3–139	Sec Ops Guide .....	450.3–101–102
Table .....	450.3–141	Sentinel .....	450.1–82
ASEP .....	450.3–47		
ASLR .....	450.3–35		
ASN .....	450.5–43		
ASR → Attack Surface Reduction .....			
Asset Database .....	450.5–45	Backdoor .....	450.3–46
Asset-Centric Security .....	450.2–13	Backstab  .....	450.3–19–20
Assumption of Compromise .....	450.2–14	Bad Stress .....	450.5–10
ATC .....	450.1–156	Bandwidth Limitation .....	450.2–10
Attack Group Naming .....	450.1–111	Base64 .....	450.2–110, 114–115
Attack Method Identification .....	450.1–152	Bash Bunny  .....	450.3–98
Attack Surface Reduction .....	450.3–36, 66, 103	BDNS → Blockchain DNS .....	
.....	450.4–153	BEACON .....	450.2–121
Rules .....	450.3–38	Beaconing .....	450.2–110, 115
Attack Trees .....	450.4–73, 81	Beats .....	450.W–225
Attacker Infrastructure Interaction .....	450.4–111	BEC .....	450.4–151
Attacks General Types .....	450.1–108	Detection .....	450.4–159
L7 .....	450.4–56	BeyondCorp (Google) .....	450.2–13
Attribution of Attacks .....	450.1–105	Bias .....	450.4–28
.....	450.4–51, 67, 91	Confirmation .....	450.4–31, 33, 45
Audit Mode .....	450.3–43	Fighting With ACH .....	450.4–46
.....	450.5–154	Bidirectional Flow .....	450.5–21
Audit Other Object Access Events  .....	450.3–97	Big Endian .....	450.3–143
Audit PNP Activity .....	450.3–98	BIMI .....	450.4–144
Audit Policies .....	450.3–53, 59, 87, 96–98	Binary File .....	450.3–141
Audit Security System Extension  .....	450.3–96	Black Basta  .....	450.1–105
Audit Trail .....	450.4–46	BlackCat  .....	450.1–105
Auditbeat  .....	450.3–87	Block Mode .....	450.3–43
Auditd  .....	450.3–79, 89	Blockchain DNS .....	450.2–75
AuKill  .....	450.3–19	Blue Team .....	450.1–13
Authenticated Scanning .....	450.3–33	Checklist .....	450.4–80
Authentication Logs  .....	450.3–75, 77, 85	Fundamentals .....	450.1–7
Authentication Server .....	450.3–106	Truths .....	450.1–27–28
Authentication-Results .....	450.4–140	Botnets .....	450.1–108
Authenticity .....	450.3–164	Flow Logs Example .....	450.2–20
Authenticode .....	450.3–164	Bottlenecks .....	450.5–19, 22
Authoritative Nameserver .....	450.2–31–33	Boyd .....	450.4–58
Auto-Categorization .....	450.5–88	Brainstorming .....	450.4–40
Automated Actions .....	450.1–148	Browser Extension .....	450.3–47
Automation .....	450.5–17, 98, 102–107	OSINT .....	450.5–121, 127
.....	450.5–130	Brute Force Attack Detection .....	450.5–65
Benefits .....	450.5–20	Brute Force Login Attempt .....	450.1–75
Candidate ? .....	450.5–105	.....	450.W–212
Framework .....	450.5–113	BSD .....	450.3–72
Full .....	450.5–116	Bucketing .....	450.W–141
Future in SecOps .....	450.5–117	Buffer Overflow .....	450.3–35
Human Capital Model .....	450.5–102	Burnout .....	450.5–9–11
.....	450.5–17	Mitigation .....	450.5–17



# SEC450 – Blue Team Fundamentals: Security Operations and Analysis

---

Business Reality .....	450.1–25
Business-Critical Tool .....	450.5–109
BYOVD .....	450.3–19
Byte Order .....	450.3–143
ByteSecLabs .....	450.W–193

## C

CAA Record .....	450.W–135
Cached Credentials .....	450.3–82
Caching Server .....	450.2–31, 55
Calculation .....	450.1–80–81
CAM Table .....	450.5–142
Campaign Analysis .....	450.4–62
Campaign Tracking .....	450.4–67
Canonicalization .....	450.4–136
Capability .....	450.4–72
CapTipper ✎ .....	450.2–25
Case .....	450.1–154
Closure .....	450.W–351
Management .....	450.5–107, 111
Summary .....	450.W–350
Template .....	450.1–153–154
.....	450.W–94–95
CEO Fraud .....	450.1–108
.....	450.4–159
Certificate Authority .....	450.2–135
.....	450.3–164
.....	450.W–135
Certificate Exchange .....	450.2–142
Challenge Analysis .....	450.4–38, 92
ChatGPT .....	450.5–115
Christmas Tree Scan .....	450.5–89
cipher ✎ .....	450.4–12
CIS Critical Controls .....	450.3–34
CIS Top 20 .....	450.5–61
CIS Top-10 .....	450.3–45
Classification of Closed Case .....	450.4–91
Client Master Key .....	450.3–107
Client-Side Exploit .....	450.3–10
Cloud .....	450.2–8
Cloud Logs 📈 .....	450.3–101
Cloud Monitoring .....	450.1–50–51
Cloud Sign-In Failure Logs 📈 .....	450.3–101
CNAME Record .....	450.2–42
Tunneling .....	450.2–71
Co-Creation .....	450.5–20
Cobalt Strike ✎ .....	450.2–121
Code Database .....	450.1–161
Code Execution .....	450.3–12
Code Injection .....	450.3–44
Code Integrity .....	450.3–66
Code Points .....	450.3–139
Code Signing .....	450.3–164
Cold Storage .....	450.3–126
Collection .....	450.1–34
.....	450.3–25
Cloud-Based .....	450.3–66
Intelligence Cycle .....	450.4–68

Command & Control .....	450.1–159
.....	450.4–9
Command Line Logging 🔍 .....	450.3–79
Common Information/Event Model .....	450.3–124
Common Language for Analytics .....	450.5–71
Communication Plan .....	450.1–39
Community ID .....	450.W–262–266, 278–279
Compensating Control .....	450.1–25
Completeness .....	450.4–90
Composite Identification .....	450.4–147
Compressed Archive With Password .....	450.4–11
Compromise .....	450.1–27
Computer Account .....	450.3–82–83
Concept of Operations .....	450.1–22
Condition Detection .....	450.5–31
Confluence .....	450.1–161
conn.log .....	450.2–24
CONNECT .....	450.2–135
Constituency .....	450.1–22
Containment .....	450.1–156
.....	450.4–64
.....	450.5–109
.....	450.W–100
Decision .....	450.5–135–136
DNS-Based Blocking .....	450.5–144
Email-Based Blocking .....	450.5–153
File-Based .....	450.5–157
Host-Based .....	450.5–157
IOC-Based Blocking .....	450.5–140
IPS-Based Blocking .....	450.5–155
L2 .....	450.5–143
L3 .....	450.5–144, 155
L4 .....	450.5–146, 155
L7 .....	450.5–155
Mobile Device .....	450.5–143
NGFW-Based Blocking .....	450.5–155
PowerShell-Based Firewall .....	450.5–147
Proxy-Based Blocking .....	450.5–155
RPZ Blocking .....	450.5–149
Tasks .....	450.W–328
Content-Type .....	450.2–95
Context .....	450.1–148
Conti Playbook 💯 .....	450.1–112–113
.....	450.2–158
Continuous Improvement .....	450.1–34
Continuous Security Monitoring .....	450.1–49
Continuous Vulnerability Management .....	450.3–34
Cookies .....	450.2–113
Corelight .....	450.2–22
.....	450.W–262
Correlation .....	450.1–60
Cortex Engine .....	450.1–153
Example .....	450.W–101–106
Courses of Action .....	450.4–61–62
Creativity .....	450.5–16
Killer .....	450.5–19
Credential Dumping .....	450.3–21
Credential Guard 📈 .....	450.3–37
Credential Theft .....	450.2–13



# SEC450 – Blue Team Fundamentals: Security Operations and Analysis

---

Attacks .....	450.3–37
From Backup .....	450.3–49
In Memory .....	450.3–49
Investigation .....	450.4–160
CredGuard *	450.3–19
Critical Assets .....	450.1–39
Cron .....	450.1–134
Cross-Fertilization of Ideas .....	450.4–40
Cross-Sector Dependency .....	450.1–151
CrowdStrike .....	450.4–44, 78
Crypto-Mining .....	450.1–51 ..... 450.5–88
CSIRT .....	450.1–13
CSM → Continuous Security Monitoring .....	
CSV .....	450.3–121
CTPH .....	450.3–162
Cyber Attack Life Cycle .....	450.4–9–10
Cyber Awareness .....	450.4–159
Cyber Kill Chain .....	450.2–105 ..... 450.3–7, 27 ..... 450.4–9, 61, 81, 90
Alerts At Same Stage .....	450.4–17
Step Visible in Logs .....	450.4–90
Cyber Security Operations .....	450.1–12
Center .....	450.1–13
Cybersecurity Skills Gap .....	450.1–9

## D

DART .....	450.1–13
Dashboards .....	450.1–94–95 ..... 450.W–206–209
Dashboards Query Language .....	450.W–21
Reference Queries .....	450.W–22
Data At Rest .....	450.1–49
Data Collection .....	450.1–32, 43 ..... 450.3–128 ..... 450.4–36
Data Destruction Detection .....	450.4–12
Data Exfiltration .....	450.1–92 ..... 450.2–152 ..... 450.4–8
Detection .....	450.4–11 ..... 450.5–64
Example .....	450.W–268–271
Data Flow Diagram .....	450.1–39
Data In Motion .....	450.1–46
Data Organization .....	450.4–38
Data Storage .....	450.3–128
Data Theft .....	450.3–26
Data Usage .....	450.3–128
Database Export .....	450.3–25
DBIR .....	450.1–10
DCID .....	450.2–129
De-Fanged Indicators .....	450.1–122
Dealing With Uncertainty .....	450.4–58
Deception .....	450.3–54
Decomposition .....	450.4–35, 41, 57, 83
Defense Evasion .....	450.3–19

Defense-In-Depth .....	450.3–49 ..... 450.4–61, 63	
Defensible Network .....	450.1–55	
Defensive Strategy .....	450.4–81	
Deferred Judgment .....	450.4–40	
Definition of Dangerous .....	450.4–7	
Delivery Stage .....	450.5–154	
Denial of Service .....	450.5–34	
Deny List .....	450.5–61–63	
Deobfuscation .....	450.W–248–250	
DEP .....	450.3–35	
Destination Blackholing .....	450.5–144	
Destover *	450.4–12	
Detection .....	450.1–34 ..... 450.4–63	
Coverage .....	450.5–63	
Engineering .....	450.1–31	
Outcomes .....	450.5–29	
DeviceIoControl .....	450.3–20	
Devices .....	450.1–21	
DGA .....	450.2–63, 69	
DHCP .....	450.2–146–148 Reservation .....	450.5–143
Scopes .....	450.5–142	
Diagnosticity .....	450.4–47, 50 Evaluation .....	450.W–302–311
Diamond Model .....	450.4–72	
Difficulty of SOC Work .....	450.1–8	
DigitalShadows .....	450.4–51	
Direction .....	450.4–68	
Directors Intelligence Level .....	450.4–67	
Dirty Pipe .....	450.3–18	
Discover & Visualize (UI) .....	450.W–37	
Discovery .....	450.3–14	
Dissemination .....	450.4–68	
Dissenting Role .....	450.4–94	
DKIM .....	450.2–41 ..... 450.4–131, 135 Checks .....	450.W–358, 363
Header Components .....	450.4–136–137	
DLL .....	450.W–251	
DLP .....	450.1–49, 107 ..... 450.3–51	
Event of Interest .....	450.W–217	
DMARC .....	450.4–131, 138–139, 144 Checks .....	450.W–359–360, 363
DNS .....	450.2–30 Attack Scenarios .....	450.2–64
Block List .....	450.5–152	
Cache 📁 .....	450.2–31	
Connecting Domain to IP .....	450.2–57	
Danger of Misunderstanding .....	450.2–39	
Delegation .....	450.2–45	
Dynamic .....	450.5–152	
Firewall .....	450.5–149	
Lookup .....	450.2–33	
Reputation .....	450.2–61	
Malicious Traffic Detection .....	450.2–59–60	
Mapping .....	450.2–38	



# SEC450 – Blue Team Fundamentals: Security Operations and Analysis

---

Over HTTPS .....	450.2–46-49, 65, 134
Over TLS .....	450.2–46
Port .....	450.2–49
Passive Data .....	450.2–57, 136 .....450.W–130-131
Record Modification Attack .....	450.2–68
Record Types .....	450.2–34-45 .....450.W–135
Research Sites .....	450.2–62
Rogue .....	450.2–49
Server & Client Types .....	450.2–31
Suspicious Request .....	450.2–66
Traffic Analysis .....	450.2–55
Tunneling .....	450.2–41, 63, 70-74 .....450.4–11 .....450.W–144-145
Characteristics .....	450.W–145
Detection .....	450.2–74 .....450.W–146
Visibility .....	450.2–55
DNS-Based Blocking .....	450.5–144
DnsCat2 ❌ .....	450.2–71
DNSSEC .....	450.2–46
Documentation Level .....	450.4–89
Documentation Quality Checklist .....	450.4–89
DoH → DNS over HTTPS .....	
Domain Admin .....	450.3–15
Domain Age .....	450.2–62 .....450.5–53
Domain Controller .....	450.3–106-107
Domain Impersonation .....	450.4–146
Domain Ownership Proof .....	450.2–68
Domain Randomness .....	450.2–63 .....450.5–53
Domain Reputation .....	450.2–61 .....450.5–43
Domain Shadowing .....	450.2–68 .....450.4–155
DoT → DNS over TLS .....	
Downgrade Attack .....	450.2–142
DQL → Dashboards Query Language .....	
Drive-by Download .....	450.1–109 .....450.3–48
Dropbox .....	450.4–156
Dual-Home Machine .....	450.2–152
Dwell Time .....	450.1–11, 152
Dynamic Analysis .....	450.3–145
Dynamic Delivery .....	450.5–153
Dynamic Ports (>49152) .....	450.W–216
DynDNS .....	450.5–152
E	
E3 License 📈 .....	450.3–36, 38
E5 License 📈 .....	450.3–36, 38
ECH → Encrypted Client Hello .....	
EDR .....	450.1–48
.....	450.3–50
.....	450.5–157
Failed .....	450.1–53
EFF .....	450.4–76
Elastic Stack .....	450.1–66
ElasticSearch .....	450.W–225
EldoS .....	450.4–12
Elliptic Curve .....	450.2–140
Email .....	450.4–123
Authentication .....	450.4–135
Methods .....	450.4–141
Content Order .....	450.4–125
Delivery .....	450.4–120-121
Forwarding .....	450.4–143
Headers & Source .....	450.4–124-125
Example .....	450.W–354, 361
Order .....	450.4–142
Intra-Organization .....	450.4–147-148
Junk .....	450.4–146
Malicious Attachments .....	450.4–153
Rejected .....	450.4–141, 143
Self-to-Self .....	450.4–147-148
Source Verification .....	450.4–131
Spoofed .....	450.4–130, 147-148
Email Template .....	450.5–121
Email-Based Attacks .....	450.4–151
Email-Based Blocking .....	450.5–153
Embed Object Functionality .....	450.3–155
EmerDNS .....	450.2–75
EMET 🖼 .....	450.2–15 .....450.3–35
.....	450.5–157
Emotet 🎯 .....	450.2–140 .....450.5–38
Empowerment .....	450.5–15
Encapsulation .....	450.4–56
Encoding .....	450.3–139, 143
Encrypted Client Hello .....	450.2–137, 142
Endpoint Data .....	450.1–54
Endpoint Monitoring .....	450.1–44, 48-49, 55
Endpoint or Network Monitoring ? .....	450.1–52
Endpoint-Centric Attack Steps .....	450.3–6
Endpoints Defense .....	450.3–31
Enduring Value .....	450.5–118
Engineering .....	450.5–117
Enrichment .....	450.1–159 .....450.5–35-36, 42-47, 107-108 .....450.W–229
Asset-Based .....	450.5–45
Capabilities .....	450.5–44
Example .....	450.5–46-47
Feature Addition .....	450.5–43
User-Based .....	450.5–45
Enter-PSSession ✎ .....	450.2–155
Entra ID Audit Logs 📈 .....	450.3–102
Entra ID Privileged Accounts Logs 📈 .....	450.3–101
Entra ID Sign-In Logs 📈 .....	450.3–101
Entra ID User Account Logs 📈 .....	450.3–102
Enumeration .....	450.3–14



# SEC450 – Blue Team Fundamentals: Security Operations and Analysis

.....	450.5–107–108
Ephemeral Key	450.2–142
EPSS → Exploit Prediction Scoring System	.....
Eradication	450.4–64
EternalBlue 	450.2–14, 151 ..... 450.4–17
Evaluation Mode	450.5–154
eve.json	450.W–222
Event	450.1–133
Collection	450.1–134–135
Log Flow	450.1–136
Logging	450.3–53, 57–58, 70
Severity Levels	450.3–60, 70, 75
Event Matrix	450.4–43
Event Viewer 	450.3–57–58
EventID 1 (Sysmon)	450.3–88
EventID 1006/1116	450.3–103 ..... 450.W–219
EventID 1115	450.3–103
EventID 1121/1122	450.3–38, 450.3–103
EventID 1125/1126	450.3–103
EventID 4104	450.3–105
EventID 4624/4625	450.1–81–82 ..... 450.3–60, 112 ..... 450.W–198–199, 202–204
Example	450.3–61–62
Interpretation	450.3–82–83
Template	450.3–63
EventID 4648	450.3–84
EventID 4657/4660/4663	450.3–95
EventID 4688	450.3–88 ..... 450.W–200–201, 299–301
EventID 4697/7045	450.3–96
EventID 4698	450.3–97
EventID 4720	450.3–100
EventID 4728/4732	450.3–100
EventID 4768/4769/4770	450.3–109–111
EventID 4771	450.3–110
EventID 5152/5154/5156	450.W–212–216
EventID 6416	450.3–98 ..... 450.W–217
EventID 7036	450.5–73
EventID 7045	450.5–73
EventID 8003/8004/8006/8007	450.3–104
Evidence	450.4–49
Bad	450.4–50
Checking	450.W–295–301
Gathering	450.W–294
Source Reliability	450.4–94
Volatility	450.5–140
EVTX	450.3–57–58 ..... 450.5–41
Exchange ActiveSync	450.4–122
Exchange Online Protection	450.4–147
Executables	450.3–153
Malicious File	450.W–238
Malware Alert	450.W–274
Packing	450.4–16
Short Name Alert	450.W–261, 277–283
vs Scripts (Attachments)	450.4–151
Executives Intelligence Level	450.4–67
Execve System Call	450.3–89–90
Exfiltration	..... 450.3–26
Example	450.3–27–28
Expel	450.4–159
Explicit Proxy	450.2–135
Exploit Guard 	450.3–35–36
Exploit Prediction Scoring System	450.3–34
Exploit Prevention	450.3–39
Exploit Protection	450.3–36
Exploitation	..... 450.4–9
Extended Validation Certificates	450.4–144
Externalization	450.4–35, 41, 83
Extortion	450.1–105, 108
Case Study	450.1–112–113

## F

F3EAD Cycle	450.4–70
FaaS	450.1–50
Facility 	450.3–70, 75
Failed Login	450.1–81–82 ..... 450.3–82, 86
Fake Response	450.5–150
False Negative	450.5–29, 69
High	450.5–34
Zero	450.5–33
False Positive	450.1–139, 142 ..... 450.3–14 ..... 450.4–20 ..... 450.5–29–30, 78, 93 ..... 450.W–277
High	450.5–33
Prevention	450.5–43
Solution	450.5–35
Zero	450.5–34
Fast Lane	450.5–97
Fast Search	450.3–126
Fast Track Process	450.5–97
Features	450.5–37
High	450.5–38
Low	450.5–39
Positive/Negative	450.5–52
Ranking	450.5–56
Field Analysis	450.5–93
File Contents	450.3–133
Dangerousness	450.3–152
Identification	450.3–134
Signatures	450.3–136
Vulnerabilities	450.3–159
File Extraction (PCAP)	450.2–100 ..... 450.W–159–162, 175–177, 181–183
File Integrity Monitoring	450.3–46, 49
File Permissions	450.3–16, 44
Auditing	450.3–49
File Reputation	450.3–42
File Watch	450.W–387–389
File-Based Containment	450.5–157



# SEC450 – Blue Team Fundamentals: Security Operations and Analysis

---

Filtering	450.1–75, 81
FIM → File Integrity Monitoring	
Fingerprint	450.3–162
Firewall 🔥	450.3–94
Firewall 🖥️	450.3–93
First Contact Rule	450.5–66
FISMA	450.1–151
Flat Network	450.2–14–15
Flatline Rule	450.5–64
Flow Logs	450.2–18–19
→ Network Flow	
Opportunities	450.2–21
Fluentd	450.W–225
Folder Access	450.3–36
Foothold	450.4–10
Forensics	450.1–31–33, 36
Forensics Tasks	450.5–110
Form Auto-Fill	450.5–121–123
Form Contents Caching	450.5–128
Form History Control	450.5–128
Formal Training	450.5–14
Forwarding Server	450.2–31, 33, 55
Four A's	450.1–150
Four-Eyes Rule	450.5–109, 137
FQDN	450.2–43
Frames	450.2–123
Free TLD	450.2–60
Free-For-All	450.5–91
Frequency Rule	450.5–64
FSG ✕	450.4–16
FTP	450.2–156
Full Automation	450.5–116
Full Duplex	450.2–10
Full Packet Capture	450.2–25
Full Text Search	450.3–122–123
Functional Impact	450.1–151
Fuzzy Hashing	450.3–162

## G

Gatekeeper 🍏	450.3–43
GCP	450.1–50
Generic Language for Analytics	450.5–71
GeoIP Information	450.5–43
Get-WinEvent ↗	450.3–58, 63
GhostPack	450.3–19
Gmail	450.4–124
Good Stress	450.5–10
Government-Backed Groups	450.1–105
GQM System	450.1–40
Graph Thinking	450.4–73–74
Grounded Theory	450.5–11
Group Management Logs 📈	450.3–100
Grouping	450.1–77–78, 81
Growth	450.5–13

## H

Hackers-for-Hire	450.1–107
------------------	-----------

HackMD ✕	450.1–161
Hacktivism	450.1–106
Hash Lookup	450.3–161, 167
...	450.5–110
Hashing	450.3–162
Collision	450.3–162, 166
Header Injection	450.5–153
Health Attestation	450.3–48
Help Desk Access	450.5–91–92
HermeticWiper 💀	450.3–166
Heuristic Detection	450.3–102
HGS	450.3–48
Hibernate	450.5–142
HIDS/HIPS	450.3–46
...	450.5–157
Successor	450.3–50
Highest Quality Data	450.5–36
HIPAA	450.3–51
Hive 💀	450.1–105
Homoglyph	450.2–78
Honeypot Kernel	450.W–226
Host Firewall	450.3–39–40
...	450.5–146
Logs	450.3–77, 93–94
Host IPS	450.1–58
Host-Based Containment	450.5–157
Host-Centric Attack Steps	450.3–6–7
Hostname	450.2–146
HPACK	450.2–127
HTA	450.W–247
HTTP	450.2–86–87
Analysis Methods	450.2–106
Evil Usage	450.2–105
File Analysis	450.2–116
Host Header	450.W–151–154
Inbound Attacks Blocking	450.5–156
Methods	450.2–88–90
Proxy	450.2–135
Request Headers	450.2–91–94, 106
Analysis	450.2–98, 106, 110
Response Codes	450.2–96
Response Headers	450.2–95–99
Analysis	450.2–99, 106, 110
Suspicious Activity	450.2–117–121
HTTP/1.1 vs HTTP/2	450.2–124
HTTP/2	450.2–123–124
File Extraction	450.2–128
Frame Types	450.2–123–124
Most Important	450.W–168, 173
Session	450.2–126
Stream ID	450.W–169–170, 174
Streams	450.2–125
TLS Decryption	450.W–167
HTTP/3	450.2–129
Why Blocking	450.W–183
Human Capital Theory	450.5–11
Human-in-the-Loop	450.5–106
Hypothesis	450.4–49
Disproven	450.4–50



# SEC450 – Blue Team Fundamentals: Security Operations and Analysis

Example .....	450.W-311
Generation .....	450.4-38
Example .....	450.W-294
Exercise .....	450.4-39
Likelihood .....	450.4-50
Unproven .....	450.4-50
Hypothesis Testing .....	450.4-38

## I

IaaS .....	450.1-50
IBM .....	450.5-113
ICANN .....	450.2-75
ICMP .....	450.2-157
Identification .....	450.4-64
Identity Protection  .....	450.3-102
Identity-Centric Security .....	450.2-13
IDN → International Domain Name .....	
IDS .....	450.1-143
IEEE 802.1X .....	450.2-7, 9
IMAP .....	450.4-122
IMS → Incident Management System .....	
In-Memory Malware Scanning .....	450.3-41
Inadequate Compensation .....	450.5-25
Inbound Deny .....	450.3-39
Incident .....	450.1-133
Categorization .....	450.1-150
Success .....	450.1-152
Event Chart .....	450.4-43
Factors .....	450.1-151
Notification .....	450.1-150
Reporting .....	450.1-150
Scoring .....	450.1-151
Threat Intel-Centric View .....	450.4-72
Tracking Framework .....	450.4-91
Type .....	450.4-91
Incident Management System .....	450.1-121, 137, 147
Enrichment to SOAR .....	450.5-111
Features .....	450.1-149
Overview .....	450.1-148
Incident Response .....	450.1-32, 34
Cycle .....	450.4-64-65
Model .....	450.4-81
Plan .....	450.1-39
SOAR .....	450.5-107
Techniques .....	450.1-156
Tracking .....	450.4-44
Indexing .....	450.3-122
.....	450.5-41
Indicator Database .....	450.1-149
Indicator of Attack .....	450.4-78-79
Infection Chain Example .....	450.W-251
Information Collection .....	450.4-36
Information Impact .....	450.1-151
Initial Compromise .....	450.4-10
Initial Detection .....	450.4-91
Initial Exploitation .....	450.3-8
Initial Investigation .....	450.1-159
Installation Phase .....	450.3-41

Intelligence Cycle .....	450.4-68
Intelligence-Driven Network Defense .....	450.4-61
Inter-Group Cooperation .....	450.5-25
Interactive Login .....	450.3-82
Internal Firewall .....	450.5-91-92
International Domain Name .....	450.2-78-81
Internet Noise .....	450.4-21
Intrusion .....	450.3-82
Analysis Model: Diamond Model .....	450.4-72
APT Model: Cyber Kill Chain .....	450.4-61
Motivation .....	450.5-139
Nature .....	450.5-139
Intuitive Thinking .....	450.4-34
Investigation .....	450.1-32, 34
Anonymity .....	450.4-116
Passive Sources .....	450.4-111
Startup Principle .....	450.4-57
Tasks .....	450.W-328
IOA vs IOC .....	450.4-78-79
IOC .....	450.1-148, 153-154
.....	450.5-51
Blocking .....	450.5-140
Extraction .....	450.3-157
Intelligence Level .....	450.4-67
Public Submission .....	450.4-110
IOC-less Search .....	450.4-81
Iodine ✎ .....	450.2-71-73
IoT .....	450.2-8
IP Allow List .....	450.4-146
IP Anonymization .....	450.4-113
IP Reputation .....	450.W-194
IPS Mode .....	450.5-34
IPS-Based Blocking .....	450.5-155
Iptables 🔪 .....	450.3-94
ISAC/ISAO .....	450.1-121
→ Info Sharing Analysis Center/Organization .....	
IsDebuggerPresent API Call 🖲️ .....	450.W-261, 274, 277
ISO .....	450.W-245
Malicious File .....	450.W-244-246
ISOC .....	450.1-13
Isolated VLAN .....	450.5-143
ITIL .....	450.1-133

## J

JA3(S) .....	450.2-140
.....	450.W-191-193
Creator .....	450.W-193
JARM .....	450.2-140
JavaScript .....	450.5-129
journalctl 🔪 .....	450.3-78
JSON .....	450.3-121
.....	450.W-27
Log Example .....	450.W-222
Jump Box .....	450.2-152
.....	450.5-91-92
Jump Server .....	450.3-48

## K

# SEC450 – Blue Team Fundamentals: Security Operations and Analysis

KDC → Key Distribution Center .....	450.3–44
Kerberos Authentication  .....	450.3–106–107
Failed .....	450.3–110
Negotiate .....	450.3–112
Kernel Exploitation .....	450.3–18
Kernel Messages  .....	450.3–75
Kernel Mode .....	450.3–66
KEV → Known Exploited Vulnerabilities .....	450.3–121
Key Distribution Center .....	450.3–106–107
Key Length Field .....	450.3–112
Key Logging .....	450.3–25
Key-Value Pairs .....	450.3–121
Log Example .....	450.W–224
Killing a Process .....	450.5–147
Knowledge Database .....	450.1–149
Known Bad/Good Domain .....	450.5–149–150
Known Bad/Good Enumeration .....	450.5–61
Known Bad/Good IP .....	450.5–149, 151
Known Exploited Vulnerabilities .....	450.3–34
KQL → Kusto Query Language .....	450.1–81–83
..... Advanced Query: WDAC Events .....	450.W–21 450.3–104
Example Query .....	450.1–82
Project .....	450.1–83

## L

L3 Anonimization .....	450.4–113
L7 (Non-)Anonimization .....	450.4–113
L7 Attacks .....	450.4–56
L7 Metadata .....	450.2–23
Lack of Confidence .....	450.5–14
LAN Turtle  .....	450.3–98
Latency .....	450.1–140
Lateral Movement .....	450.2–10, 21 ..... 450.3–23–25, 84, 97
Prevention .....	450.3–39
Lazarus Group .....	450.2–116
Leaked Passwords .....	450.3–102
Learning Curve .....	450.1–161
Least Privilege .....	450.2–9, 11–12 ..... 450.5–15
Legal Context .....	450.1–21
Lessons Learned .....	450.4–65
LetsEncrypt .....	450.2–134
Libpcap  .....	450.2–25
LightDM  .....	450.3–86
Link Analysis .....	450.4–41
Tools .....	450.4–42–43
Link Shortening Service .....	450.4–154, 157, 162
Linux Auditing .....	450.3–79
Linux Logging .....	450.3–70
New Way .....	450.3–78
Linux Logins .....	450.3–85
Failures .....	450.3–86
List Thinking .....	450.4–74
Listening Port .....	450.3–9
Little Endian .....	450.3–143

Living Off The Land .....	450.3–44, 97
LLM .....	450.5–115
LNK .....	450.3–158
Malicious File .....	450.W–237–238, 247
Vulnerability .....	450.3–159
Local Account .....	450.3–82
LockBit  .....	450.1–105 ..... 450.3–19
Log Agents .....	450.W–224–225
Log Aggregator .....	450.3–119 ..... 450.W–225
Log Attributes .....	450.5–37
Alerting .....	450.5–50
Matching to Threat Intel .....	450.5–51–52
Log Channels  .....	450.3–57–58
Attributes .....	450.3–60
Most Interesting .....	450.3–66
Log Collection .....	450.3–56
Agent vs Agentless .....	450.3–119
Easy .....	450.3–93
Methods .....	450.3–119
Most Interesting  .....	450.3–77, 87, 89–91
Most Interesting  .....	450.3–66, 87–88
Pipeline .....	450.3–118
Structured Formats .....	450.3–121–122
Unstructured Formats .....	450.3–120
Log Flow Diagram .....	450.1–39
Log Format Selection .....	450.5–41
Log Life Cycle .....	450.3–127
Log Normalization .....	450.3–124–125 ..... 450.W–228
Log Path  .....	450.3–76
Log Path  .....	450.3–58
Log Source .....	450.3–119
Log Storage .....	450.3–126
Log Types .....	450.1–58
Log4j .....	450.2–119
Logging Tools .....	450.1–58
Login Screen  .....	450.3–86
Logokit  .....	450.4–158
LogRhythm .....	450.W–225
Long-Tail Analysis .....	450.4–20
Lookalike Domain .....	450.4–154, 162
Loss Prevention .....	450.1–28
Low-Cardinality Fields .....	450.5–61
LSA .....	450.3–37
lsass.exe .....	450.3–37–38

## M

MAC .....	450.2–146
Machine Learning .....	450.5–59, 64, 450.3–102
Macro .....	450.5–121
Magic Bytes .....	450.3–136
Malicious Attachments .....	450.4–153
Malicious C2 Server Fingerprinting .....	450.2–140
Malicious DNS .....	450.2–65
Malicious File Handling .....	450.3–150–151
Malicious File Hosting .....	450.4–156



SEC450 – Blue Team Fundamentals: Security Operations and Analysis

Malicious Insider .....	450.1–107
.....	450.3–51
Malicious Outsider .....	450.3–51
Malicious Redirect .....	450.5–55
Malicious Script Detection .....	450.3–168
Malicious Subdomains .....	450.W–136
MalVirt  .....	450.3–19
Malware	
Detection Alert .....	450.3–103
DNS .....	450.2–65
Most Interesting .....	450.3–41–42
Man-In-The-Middle .....	450.2–13
Management Plane .....	450.1–50–51
Management Traffic .....	450.W–68–69
Managers Intelligence Level .....	450.4–67
Mandiant M-Trends .....	450.1–11
Manifest Template .....	450.3–65
Material Impact .....	450.1–164
MDA .....	450.4–120
MDE  .....	450.3–66, 104
Medusa  .....	450.3–19
Memory Forensics .....	450.5–142
Mental Model .....	450.4–28, 55
Importance .....	450.4–83
Toolbox .....	450.4–59
When Applies .....	450.4–81
Merlin C2 .....	450.W–183
Metadata Analysis .....	450.5–50
Metadata Collector .....	450.2–22
Metasploit  .....	450.2–137
.....	450.3–40
Metrics .....	450.1–40
.....	450.5–17, 22
Adjustment .....	450.5–23
MFA .....	450.4–159
Fraud Alert  .....	450.3–101
Micro-Automation .....	450.5–121
Micro-Segmentation .....	450.2–8, 14
Microsoft 365  .....	450.4–145
Safe Attachments Policies .....	450.4–153
Microsoft Graph API  .....	450.3–101
MIME Type .....	450.2–95
Mimikatz  .....	450.3–22–23
.....	450.5–91
Mindset .....	450.1–14
Mirror Port .....	450.2–10
MISP .....	450.1–123–128, 160
.....	450.5–51, 75
Terminology .....	450.1–124
Mission Questions .....	450.1–20
MITRE ATT&CK .....	450.3–11
.....	450.4–80–81
.....	450.5–72
Modern Defense .....	450.1–14
MPSSVC .....	450.3–67
MTA/MUA .....	450.4–120, 122
Mutually Exclusive Hypotheses .....	450.4–47
MX Record .....	450.2–43
.....	450.4–120
MySQL Logs .....	450.3–77
<b>N</b>	
NAC .....	450.5–142–143
NAC → Network Access Control .....	
Naked IP Address .....	450.2–118
.....	450.5–57
Namecheap .....	450.2–68
Need-To-Know .....	450.4–105
Nested Files .....	450.3–137
NetFlow Collector .....	450.2–19
Network Access Control .....	450.2–146
Network Architecture .....	450.2–6
Network Connectivity .....	450.5–143
Network Data Capture Formats .....	450.2–18
Network Defense .....	450.4–61
Network Diagram .....	450.1–39
Network Firewall .....	450.3–40
.....	450.5–146
Network Flow .....	450.1–61
.....	450.2–9, 19, 67
Ports .....	450.2–19
Network IPS .....	450.1–58
Network Layers .....	450.5–141
Network Logon .....	450.3–82
Network Monitoring .....	450.1–44–45, 55
Network or Endpoint Monitoring ? .....	450.1–52
Network Protection .....	450.3–36, 103
Network Scanning .....	450.3–32
Network Security Monitoring .....	450.1–46–47
Network Segmentation .....	450.2–159
Network Stack .....	450.5–141
Network Tap .....	450.2–10, 23
Network Traffic Blocking .....	450.5–157
Network Zone .....	450.2–8
Network-Centric Attack Steps .....	450.3–7
NetworkMiner  .....	450.2–25
New Country Sign-Ins .....	450.3–102
New Device Logs  .....	450.3–101
New Term Rule .....	450.5–66
New User Creation Logs  .....	450.3–100
New-NetFirewallRule  .....	450.5–147
Next-Gen Firewall .....	450.2–11–12
NGFW-Based Blocking .....	450.5–155
NIST SP800-61 .....	450.1–133, 151
.....	450.4–64
Nmap  .....	450.3–32
Noise .....	450.3–105
.....	450.5–89
Filtering .....	450.W–371
Reduction .....	450.3–41, 43
Non-Authenticated Protocols .....	450.2–13
Non-Malicious Insider .....	450.3–51
Non-Routable IP .....	450.5–143
NotPetya  .....	450.2–14
Novel Scenarios .....	450.5–16
NS Record .....	450.2–45
NSA .....	450.4–51



# SEC450 – Blue Team Fundamentals: Security Operations and Analysis

---

NSM → Network Security Monitoring .....
NTLM  ..... 450.3–112
..... 450.W–205
NtLoadDriver ..... 450.3–20
NULL Record ..... 450.2–72
Null Routing ..... 450.5–144
NXLog ..... 450.W–225

## O

Obfuscator ..... 450.3–168
Object Access Auditing  ..... 450.3–95
Observables ..... 450.1–153–154
..... 450.W–97, 102–105, 342–349
Automated Analysis ..... 450.W–104–105
Observed Activity ..... 450.1–151
Octet-Stream ..... 450.2–97, 99
Office Documents ..... 450.3–155
Office Macros ..... 450.3–38
Olevba  ..... 450.3–155–156
OneDrive  ..... 450.4–156
OneNote  ..... 450.1–161
File ..... 450.3–158
Magic Bytes ..... 450.W–255
OODA ..... 450.4–58–60
Open Redirects ..... 450.4–158
OpenDNS ..... 450.2–31
OpenNIC ..... 450.2–75
OpenSearch ..... 450.1–66, 96
Query Language ..... 450.1–67
SQL Query ..... 450.1–81
Operating System Permissions ..... 450.3–16–17
Operational Efficiency ..... 450.5–17, 21
Operations Tempo ..... 450.4–81
Opportunistic Attacks ..... 450.1–108–109
..... 450.3–45
..... 450.4–102, 161
OPSEC ..... 450.4–101
..... 450.5–140
Failures ..... 450.4–110–111, 115, 117
Ideal ..... 450.4–107
Link Expansion ..... 450.4–157
NATO Definition ..... 450.4–102
Open Redirect ..... 450.4–158
Tools ..... 450.4–108
Types ..... 450.4–104
Orchestration ..... 450.5–103
Ordering ..... 450.1–80
Organizational Goals ..... 450.1–21
Organized Crime ..... 450.1–105
OSINT Tools ..... 450.4–108
Scan vs Search ..... 450.4–109
OSSIM ..... 450.1–96
OUI ..... 450.2–146
Outbound Deny ..... 450.3–39
Outlook ..... 450.4–124
Over-Specification ..... 450.5–69
Over-Tuning ..... 450.5–50, 67
Overconfidence ..... 450.4–93

## P

PaaS ..... 450.1–50
Package Name Field ..... 450.3–112
Packet Capture ..... 450.2–18
PAM → Pluggable Authentication Module .....
PAP → Permissible Actions Protocol .....
Pareto Principle ..... 450.5–94–96
..... 450.W–371
Parsing ..... 450.5–41
Pass-the-Hash ..... 450.3–37
Pass-the-Ticket ..... 450.3–37
Passive DNS ..... 450.2–57
..... 450.W–130–131
Hunt ..... 450.W–136
Passive Scanning ..... 450.3–32
Passive Search ..... 450.4–107
Password Resets ..... 450.5–140
Password Spray Attack ..... 450.1–92, 97
Password Spray Attacks ..... 450.3–102
Passwords Theft Attack ..... 450.2–68
Patching ..... 450.3–34
Pattern Matching ..... 450.5–50, 53
PAWS ..... 450.3–48
PCAP ..... 450.1–39, 58
..... 450.2–25
Collector ..... 450.2–22
Downside ..... 450.2–18
.pcapng ..... 450.2–25
PDF ..... 450.3–157
PE Format ..... 450.3–153
Malicious File ..... 450.W–238
Peer-Led On-The-Job Training ..... 450.5–14
Pen Testing ..... 450.1–31–33, 36
People ..... 450.1–19
Perception ..... 450.4–29–31
Issues ..... 450.4–33
Perfect Forward Secrecy ..... 450.2–142
Perfect Rule ..... 450.5–30
Performance (Data Tables) ..... 450.W–27
Perimeter ..... 450.2–7–8
Periodic Review ..... 450.4–96
Permissible Actions Protocol ..... 450.4–106, 111
Permission Request Process ..... 450.5–138
Permissions  ..... 450.3–49
Persistence ..... 450.2–158
..... 450.3–13, 47, 97
Pew Pew Map  ..... 450.1–95
pfirewall.log  ..... 450.3–93
Phishing ..... 450.1–159
Alert Example ..... 450.W–96–97
Attempts ..... 450.1–152
Common Tactics ..... 450.4–154
Hosted on Hacked Site ..... 450.4–155
Investigation Anonymization ..... 450.4–116
Mistake ..... 450.4–117
Logs Example ..... 450.W–335–338
Prevention ..... 450.3–48
Priority ..... 450.4–161
Tactics Combination ..... 450.4–162



# SEC450 – Blue Team Fundamentals: Security Operations and Analysis

Physical Attacks .....	450.3–98	.....	450.3–24, 38
Physical Isolation .....	450.5–142	PSRP .....	450.2–155
PICERL .....	450.4–64–65, 70, 81	PTR Record .....	450.2–37–38, 40
Pivot .....	450.3–82	.....	450.4–128
PKI .....	450.3–164	Punycode .....	450.2–78–79
Plaintext File .....	450.3–141	PUP .....	450.5–88
Playbook .....	450.1–149, 153–156	Purple Teaming .....	450.5–14
.....	450.5–105	Pyramid of Pain .....	450.4–78
Breakdown .....	450.1–156		
Completion .....	450.W–328–351		
Creation .....	450.1–156		
Example .....	450.1–155		
Execution .....	450.W–100		
Planning .....	450.1–156		
Pluggable Authentication Module .....	450.3–85		
Policy Alerts .....	450.1–143	QPACK .....	450.2–129
Policy Change .....	450.3–67	.....	450.W–179
Policy for Raising Fidelity .....	450.5–91	QRadar .....	450.1–81
Polyglots .....	450.3–138	.....	450.W–225
Example .....	450.W–247, 251	Quality .....	450.4–96
Polymorphic Malware .....	450.5–157	Consistence .....	450.4–88
Poor Process Cost Documentation .....	450.5–138	Quarantine .....	450.4–139, 145, 153
Port Scan .....	450.1–97	.....	450.5–153
.....	450.W–213	Query Workbench .....	450.W–28, 37
External .....	450.4–21	QUIC .....	450.2–129
Positive Feedback Loop .....	450.5–12, 21	Why Blocking .....	450.W–183
Post-Exploitation .....	450.3–11, 29	Quick Parts .....	450.5–124
Favorites .....	450.2–4		
Potential Impact .....	450.1–151		
PowerShell Logs .....	450.3–105	R	
PowerShell Remoting .....	450.2–155		
.....	450.3–24		
Pre-Classification .....	450.4–13	Randomness Measure .....	450.5–43, 53
Pre-Exploitation .....	450.3–29	Ransomware .....	450.1–10–11, 105, 108
Premature Block .....	450.4–115	Case Study .....	450.1–112–113
Premortem Analysis .....	450.4–93–94	Ransomware Prevention .....	450.3–36
Preparation .....	450.4–64	RAT .....	450.2–158
Prevention .....	450.4–63	Raw Logs .....	450.1–65
PrivescCheck .....	450.3–17	RDP .....	450.2–154
Privilege Escalation .....	450.3–15–16	.....	450.3–24
Local .....	450.3–18	Logon Event .....	450.3–82
Prevention .....	450.3–49	Tunneling .....	450.2–153
Privileges 📈 .....	450.3–49	RE&CT .....	450.1–156
Problem Modeling .....	450.4–35	Real-Time Collaborative Editing .....	450.1–161
proc_create Rule 🔥 .....	450.3–89	Received Headers .....	450.4–127–128
Procedure Review .....	450.5–19	Reconnaissance .....	450.4–9
Process .....	450.1–19	Recoverability .....	450.1–151
Improvement .....	450.5–25	Recovery .....	450.4–65
Process Creation Logs .....	450.3–87–89	Recursive Server .....	450.2–31, 33
Process Explorer .....	450.3–19	Red Hat .....	450.3–77
Processing of Intelligence Data .....	450.4–68	Red Team .....	450.1–31–33, 36
ProcExp ✎ .....	450.3–20	Red Teaming .....	450.5–14
Product ID .....	450.3–98	Reddit .....	450.5–26
Proof of Domain Ownership .....	450.2–41	Redirection .....	450.4–154
Protocols Safety .....	450.2–159	Referer .....	450.2–91, 94
Proxy Authentication .....	450.2–96	.....	450.W–295, 324
Proxy Logs .....	450.4–11	Reflection .....	450.5–19
Proxy-Based Blocking .....	450.5–155	Registry Key .....	450.3–13
PSEExec ✎ .....	450.2–151	Registry Value Modified 📈 .....	450.3–95
		Regular Expression .....	450.5–50, 53–54
		Testing .....	450.5–58
		Relationship Building .....	450.5–138
		Relative Likelihood .....	450.4–50
		Relayed Email Invalidiation .....	450.4–141



# SEC450 – Blue Team Fundamentals: Security Operations and Analysis

---

Remediation .....	450.1–159	Salesforce .....	450.W–193
Remote Access .....	450.5–91–92	Samba 🐾 .....	450.2–149
Remote Login .....	450.2–149	Sandboxing .....	450.2–109 ..... 450.3–145, 161, 167 ..... 450.4–153
Responder .....	450.W–96	Scalability .....	450.5–106
Response .....	450.4–63	Scapy .....	450.2–157
Tasks .....	450.W–341	Scheduled Task .....	450.3–13, 47, 97
Retention Period .....	450.3–126, 128	SCL .....	450.4–145–146
Return-Path Field .....	450.4–132, 135	Scope .....	450.1–22
REvil 🦊 .....	450.1–105	Scoped Search .....	450.3–123
RFC 821 - SMTP .....	450.4–129	Script Block Logs .....	450.3–105
RFC 974 -DNS/MX .....	450.2–43	Scripting .....	450.5–130 DIY .....
RFC 1464 - DNS/TXT .....	450.2–41	Scripting.FileSystemObject .....	450.W–249–250
RFC 1912 - DNS .....	450.2–37	Scripts .....	450.3–154 vs Executables (Attachments) .....
RFC 2317 - DNS/PTR .....	450.2–37	sdelete ✎ .....	450.4–12
RFC 2616 - HTTP/1.1 .....	450.2–90	SE_PRIVILEGED_ENABLED .....	450.3–20
RFC 3164 - BSD Syslog .....	450.3–72–73	Search Processing Language .....	450.1–81 ..... 450.W–21
RFC 3195 - Syslog over TCP .....	450.3–73	Seatbelt ✎ .....	450.3–19
RFC 3954 - NetFlow .....	450.2–19	Security ID .....	450.3–64
RFC 5322 - IMF .....	450.4–123	Security Logs 📈 .....	450.3–59–60
RFC 5424 - Syslog .....	450.3–72–73	Security Mitigations .....	450.3–66
RFC 5425 - Syslog over TLS .....	450.3–73	Security Relevant Data .....	450.5–40
RFC 5426 - Syslog over UDP .....	450.3–73	Security Strategy .....	450.4–67
RFC 5427 - Syslog Conventions .....	450.3–75	Security-Relevant Logs .....	450.1–135
RFC 5484 - Signed Syslog .....	450.3–73	SecurityOnion .....	450.1–96
RFC 6012 - Syslog over Encrypted UDP .....	450.3–73	Sekurlsa .....	450.3–22
RFC 6376 - DKIM .....	450.4–137	Selection .....	450.1–75, 81
RFC 7001 - SMTP Message Authentication .....	450.4–134	Self-Assessment .....	450.1–32–33
RFC 7208 - SPF .....	450.4–132–134	Self-Critique .....	450.4–94
RFC 8446 - TLS1.3 .....	450.2–142	Self-Extracting Archives .....	450.3–153
RFC 8601 - Authentication-Results .....	450.4–140	Self-Measurement .....	450.5–22
RIG Exploit Kit 🦊 .....	450.5–55–56	Self-Signed Certificate .....	450.W–189–191
Risk Acceptance .....	450.1–26	SELinux .....	450.3–43
Risk Appetite .....	450.1–23	Sender Policy Framework .....	450.2–41
Risk Assessment .....	450.4–67	Sense of Accomplishment .....	450.5–13
RiskIQ .....	450.4–111	Sensitive Hosts/Users/Data .....	450.4–13
Risky Sign-Ins 📈 .....	450.3–102	Sensitive Lookups .....	450.4–108
Rogue Device .....	450.2–146	Sensitivity .....	450.5–30 High .....
Rogue DNS .....	450.2–49	..... 450.5–33	
ROI .....	450.1–40	Medium .....	450.5–32
Root Nameserver .....	450.2–33	Problem .....	450.5–50
Router .....	450.2–7	Sentinel 📈 .....	450.1–81–83 ..... 450.W–21, 30
Router ACL .....	450.5–144	Available Tables .....	450.W–30
RPZ Blocking .....	450.5–149	Sequence-Based Rule .....	450.5–67
Domain-Based .....	450.5–150, 157	Server .....	450.2–8
Rsyslog 🐾 .....	450.3–71, 74	Server Name Indication .....	450.2–142 ..... 450.W–139
Rubber Ducky ✎ .....	450.3–98	TLS Extension .....	450.W–185
Rule Examination .....	450.5–96	Server-Side Exploit .....	450.3–9
Rule Fired .....	450.3–103	Service Creation .....	450.3–96
Rule Generic Format .....	450.5–72	Service Logs .....	450.2–18
Rule Logic .....	450.5–60	Service Name/ID .....	450.3–111
Rule Tuning .....	450.5–35	Service Tickets .....	450.3–107, 109
RunAs Login 📈 .....	450.3–84	SFTP .....	450.2–152
Runbook .....	450.5–105		
rundll32.exe .....	450.3–44		

## S

SaaS .....	450.1–50
Safe Attachments .....	450.5–153



# SEC450 – Blue Team Fundamentals: Security Operations and Analysis

---

SFTY .....	450.4–145
Shamoon 🚧 .....	450.4–12
Short-Term Memory .....	450.4–32
Solution .....	450.4–35
shred ✖ .....	450.4–12
Shutdown .....	450.5–142
SIEM .....	450.1–59, 148, 160
Alerts .....	450.1–137
Choice .....	450.1–88
Cloud-Native .....	450.1–64
Engineer Questions .....	450.3–128
Enrichment Capabilities .....	450.5–44
Features .....	450.1–63
Log Collection .....	450.1–61
Log Storage .....	450.1–65
Most Important Tasks .....	450.5–42
Products .....	450.1–62
Quiz .....	450.1–97
Search Approach .....	450.1–74
Summary .....	450.1–68, 100
TIP Workflow .....	450.1–121
Workflow .....	450.1–73
Sigma .....	450.3–101
.....	450.5–71–75
Alert Queries .....	450.5–74
Rule Format .....	450.5–72
Signature .....	450.3–87, 161, 164–166
Verification .....	450.3–165
.....	450.4–135
Signature-Based Alert .....	450.1–141–143
Single Port Mirror .....	450.2–10
Single Sign-On .....	450.3–22
SIRT .....	450.1–13
Skills .....	450.5–14
SLAT .....	450.3–37
SLO .....	450.5–117
Slow Attack Progression .....	450.2–14
Slow Search .....	450.3–126
Smart Keywords .....	450.5–125–126
SmartConnectors .....	450.W–225
SmartScreen .....	450.3–36
SMB 📂 .....	450.2–149–151
Connection Event .....	450.3–82
Versions .....	450.2–150
SMTP .....	450.4–120, 123
Message Components .....	450.4–125–126
Response .....	450.5–154
Spoofing .....	450.4–129–130
Snapchat .....	450.4–158
Snapshot .....	450.3–150
Snare .....	450.W–225
SNI → Server Name Indication .....	
Snoopy 🐾 .....	450.3–87
Snort ✖ .....	450.4–15
.....	450.5–40, 71
SOAP .....	450.2–155
SOAR .....	450.1–137, 148, 157, 160
Case Management .....	450.5–107, 111
Categories .....	450.5–107
Enrichment .....	450.5–108
Platforms .....	450.1–158
Product Considerations .....	450.5–106
Response .....	450.5–109–110
TIP Workflow .....	450.1–121
What ? .....	450.5–105
SOC .....	450.1–13, 19
Adjacent Functions .....	450.1–31
Analysts' Intelligence Level .....	450.4–67
Charter .....	450.1–22
Common Issues .....	450.5–25
Components .....	450.1–19
Core Activities .....	450.1–32
Critical Information .....	450.1–39
Human Capital Model .....	450.5–12–16
Automation .....	450.5–102
Ideal vs Reality .....	450.5–6–7
Mission .....	450.1–15
Operating Environment .....	450.1–21
Organization .....	450.1–31
Process .....	450.1–32, 34
Summary .....	450.1–41
Tangential Capabilities .....	450.1–32
Technology .....	450.1–32
Tiered VS Tierless .....	450.1–38
Tiers .....	450.1–37
Tools Overview .....	450.1–160
SOCKS Proxy .....	450.2–135
Software Inventory .....	450.3–32
SolarWinds Supply Chain Attack .....	450.W–136
Source Blackholing .....	450.5–144
Spam .....	450.1–108, 159
Filtering .....	450.4–145–146
Identification .....	450.5–153
Prevention .....	450.2–41
Report .....	450.5–154
SPAN .....	450.2–10
→ Switch Port ANalyzer .....	
Spear Phishing .....	450.4–19, 162
Specific Field Match .....	450.5–50
Specificity .....	450.5–30, 67
Medium .....	450.5–32
SPF .....	450.4–131–134
Checks .....	450.W–358, 362
Results .....	450.4–133–134
SPF → Sender Policy Framework .....	
Spike Rule .....	450.5–64
Spinning Disk .....	450.3–126
SPL → Search Processing Language .....	
Splunk .....	450.1–81
.....	450.W–21
Free Tier .....	450.1–96
Universal Forwarder .....	450.W–224
Spoofed Email Injection .....	450.4–130
Spoofing Check Failures .....	450.5–153
SQL .....	450.1–81, 88
.....	450.W–26–41
Query Format .....	450.W–32–33
SQL Injection Attack Detection .....	450.5–65



# SEC450 – Blue Team Fundamentals: Security Operations and Analysis

SRE .....	450.5–117
srm ✖ .....	450.4–12
SRV Record .....	450.2–44
SSD .....	450.3–126
Ssdeep .....	450.3–162
SSH .....	450.2–152–153
Login With Key .....	450.3–85
Scan .....	450.W–233
SSL Certificate .....	450.2–138–139
ssl.log .....	450.W–195–196
Staging Malware .....	450.3–24
Static Analysis .....	450.3–161
Steering Committee .....	450.1–22
Steganography .....	450.3–169
Streams .....	450.2–123
Stress Types .....	450.5–10
STRIDE .....	450.4–76
Strings .....	450.3–141
Example .....	450.3–142
Extraction .....	450.3–145
Structured Analysis .....	450.4–37–38
Structured Logs .....	450.3–121
Stub Resolver .....	450.2–31, 33
Stuxnet 🚀 .....	450.3–45, 159
SubjectUserID .....	450.3–64
Superficial Briefing .....	450.5–25
Supplied Realm Name .....	450.3–110
Suricata ✖ .....	450.2–18
.....	450.5–40
.....	450.W–97
Suspect File .....	450.3–149
Suspicious Behavior .....	450.3–103
Suspicious Browser Usage .....	450.3–102
Suspicious Inbox Forwarding .....	450.3–102
Suspicious Inbox Rules .....	450.4–159
Switch .....	450.2–9–10
SYN .....	450.5–89
Sysdig 📈 .....	450.3–87
Sysinternals ✖ .....	450.3–47, 165
.....	450.4–12
Syslog 📈 .....	450.3–70–71, 85
Daemons .....	450.3–74, 76
Example .....	450.3–72
.....	450.W–223
Fix Pain .....	450.3–78
Format .....	450.3–72
Management .....	450.3–75
Network Protocol .....	450.3–73
Size Limit .....	450.3–73
TLS .....	450.3–73
Priority .....	450.3–75
Similarity to System Logs 📈 .....	450.3–77
Unstructured Logs .....	450.3–120
Sysmon 📈 .....	450.3–79
Sysmon 📈 .....	450.3–59, 66–67, 87
Extra Information .....	450.3–88
Sysmon-like 🍏 .....	450.3–92
System Administration .....	450.1–31
System Logs .....	450.3–66, 77

Systemd Journal .....	450.3–78
Systems of Judgment .....	450.4–34

## T

Table-Top Exercises .....	450.5–14	
Tagging .....	450.3–125	
Targeted Attacks .....	450.1–108, 110 ..... 450.4–9, 102, 161	
Active Intrusion Discovery .....	450.5–139	
Automated Blocking .....	450.5–116	
Identification Opportunities .....	450.4–14	
Reaction .....	450.5–140	
TCP Handshake .....	450.5–89	
Tcpdump ✖ .....	450.2–25	
Technology .....	450.1–19	
TGS → Ticket Granting Service .....		
TGT → Ticket Granting Ticket .....		
The Onion Router .....	450.4–113	
TheHive ✖ .....	450.1–137, 153–154, 160 Workflow .....	450.1–154
Threat Hunt .....	450.1–73	
Advanced .....	450.3–104	
Model .....	450.4–81	
Workflow .....	450.1–73	
Threat Intelligence .....	450.1–31–33, 36, 116–117 ..... 450.3–102 ..... 450.4–66 Context .....	450.1–117
Cycle .....	450.4–68	
Feed Effectiveness .....	450.1–120	
Levels .....	450.4–66–67	
Matching .....	450.5–61	
Log Attributes .....	450.5–51	
Model .....	450.4–81	
Platforms .....	450.1–118–119	
Considerations .....	450.W–79	
Summary .....	450.1–128	
Workflow .....	450.1–121	
Sources .....	450.1–120	
ThreatCrowd .....	450.W–393	
Threats .....	450.1–21	
Modeling .....	450.4–76, 81	
Summary .....	450.1–114	
Threshold .....	450.1–152 ..... 450.5–50, 53, 64	
Thumbnail Pictures .....	450.W–251	
Ticket Granting Service .....	450.3–106	
Ticket Granting Ticket .....	450.3–107	
Ticketing Solution .....	450.1–147	
TIFF Exploit 📸 .....	450.4–152	
TIP → Threat Intelligence Platforms .....		
TLD .....	450.2–60 Zone File .....	450.2–45
TLP → Traffic Light Protocol .....		
TLS Certificate .....	450.2–138–139 ..... 450.W–187–191	
Check .....	450.2–41	
TLS Fingerprints .....	450.2–140	



# SEC450 – Blue Team Fundamentals: Security Operations and Analysis

---

TLS Handshake .....	450.W–186-187, 192
TLS Traffic Decryption .....	450.2–46-47, 65, 136-137
.....	450.4–56
TLS1.2 .....	450.2–138
TLS1.3 .....	450.2–134, 138, 142
Certificate Transfer .....	450.W–187
TLSH .....	450.3–162
Toil .....	450.5–118
Elimination .....	450.5–117
TOR → The Onion Router .....	
Trace Headers .....	450.4–125, 134
Trademark Verification .....	450.4–144
Traffic Capture .....	450.1–61
Traffic Duplication .....	450.2–10
Traffic Flow .....	450.2–8
Traffic Interception .....	450.2–68
Traffic Light Protocol .....	450.4–105
Traffic Mirror .....	450.2–9-10
Traffic Size .....	450.5–53
Transcription Logging .....	450.3–105
Transparent Proxy .....	450.2–135
Travels Block .....	450.5–146
Triage .....	450.1–32, 34
.....	450.4–6
Exploit Alerts .....	450.4–18-19
FTP Alert .....	450.W–260-261
IDS Alerts .....	450.4–15
.....	450.W–273
Login Alert .....	450.W–137-318
Model .....	450.4–81
Trojans .....	450.1–108
True Negative .....	450.5–29
True Positive .....	450.1–142
.....	450.5–29, 78
Trust .....	450.5–136
Strategies for Building .....	450.5–137
Trusted Hyper-V .....	450.3–48
Trusted Platform Module .....	450.3–37
Trusted Publishers Certificate Store .....	450.3–164
Tshark ✎ .....	450.2–20, 25
TTL .....	450.2–33, 35
TTP .....	450.4–78
TXT Record .....	450.2–41
.....	450.4–132, 135-136, 139, 144
Tunneling .....	450.2–71-72

## U

UBA .....	450.1–49, 58, 107
.....	450.3–52
UEBA .....	450.3–52
UFW .....	450.3–77
Log Example .....	450.W–224, 226-232
Unattributed Connection .....	450.4–112
Unauthenticated Scanning .....	450.3–33
Uncategorized Websites .....	450.1–97
Uncommon TLD .....	450.2–60
Unicode .....	450.3–139
Unstructured Data .....	450.1–161

Unstructured Logs .....	450.3–120
Unusual Ports .....	450.5–146
URI .....	450.2–87
URL Reputation Check .....	450.2–107
Tools .....	450.2–108
US-CERT .....	450.1–150
USB Plug & Play Logs .....	450.3–98
.....	450.W–217
User Awareness .....	450.4–159
User Devices .....	450.2–8
User Identity .....	450.2–11
User Impersonation .....	450.4–146
User Mode .....	450.3–66
User-Agent .....	450.2–91-92
Analysis .....	450.2–111-112
Users .....	450.1–21
UTF .....	450.3–139, 143

## V

VBA Script .....	450.W–247-248
Vendor ID .....	450.3–98
Ventura 🍏 .....	450.3–92
Verified Mark Certificate .....	450.4–144
VERIS .....	450.1–150
.....	450.4–91
Verizon .....	450.1–10, 150
Vhash .....	450.3–162
Vicious Cycle .....	450.5–12
Vidar 💯 .....	450.5–55-56
Video Capture .....	450.3–25
Virtual Secure Mode .....	450.3–37
Virtualization-Based Security .....	450.3–37
Virtuous Cycle .....	450.5–12
Virus Detection .....	450.1–159
Virus Samples Collection .....	450.5–110
Visibility .....	450.1–39, 44
.....	450.3–50-51
Visibility Points .....	450.2–10
Visualization .....	450.1–60, 88
Creation Process .....	450.1–89
Quiz .....	450.1–92-93
Summary .....	450.1–99
Types .....	450.1–90-91
VLAN .....	450.2–9
VNC .....	450.2–154
.....	450.3–24
Vulnerability Information .....	450.5–43, 45
Vulnerability Management .....	450.1–31-33
Vulnerability Scanning .....	450.3–33
.....	450.5–45
Vulnerable Drivers .....	450.3–38

## W

Wacatac 💯 .....	450.W–252
WAF .....	450.1–49
.....	450.5–156
WAN .....	450.2–8



# SEC450 – Blue Team Fundamentals: Security Operations and Analysis

---

WannaCry 🎯	450.2–14
	450.4–51
WDAC 📡	450.3–43, 104
	450.5–157
Weak Correlation	450.1–142
Weaponization	450.4–9
Web Exploit	450.1–159
Web Shell	450.3–46
Webpage Modification	450.5–129
Webserver	450.2–86
Weighted Mean	450.1–151
WFAS 🌐	450.3–93
What-If? Analysis	450.4–95
Win32 API Calls	450.3–38
WinCollect	450.W–225
Windows Defender	450.3–103
Application Control	450.3–104
Windows DNS Logs	450.5–41
Windows Event Logs	450.3–57–58
Descriptions	450.3–64
Templates	450.3–63
Windows Exploit Guard	450.2–15
Windows Logins	450.3–82, 84
Failures	450.3–82
Windows Vista	450.2–155
Winlogbeat	450.W–213
Winpcap 📡	450.2–25
WinRM	450.2–155
wipe ✖	450.4–12
Wireshark ✖	450.2–25–26
WMI	450.3–24
Event Subscription	450.3–38
Workflow Customization	450.1–149
Worklogs	450.1–153–154
	450.W–108–109
Worm	450.2–14
WScript.Shell	450.W–249–250
WSMV	450.2–155
X	
X-Forwarded-For	450.2–91
X.509	450.W–195
X11 Forwarding	450.2–152
	450.3–24
x509.log	450.W–195
XDR	450.1–48
	450.3–50
XML	450.3–61–65
EventData	450.3–62, 65
Nested	450.3–97
System	450.3–65
Y	
YAML	450.5–72
YARA	450.5–71
Z	
Zeek ✖	450.2–18, 23
Output Example	450.2–24
Zero Coding Skill	450.5–115
Zero Trust	450.2–8, 12
Architecture	450.2–13
ZIP	450.3–155
Zone	450.2–8