

SEC530 – Defensible Security Architecture and Engineering: Implementing Zero Trust for the Hybrid Enterprise

Topics

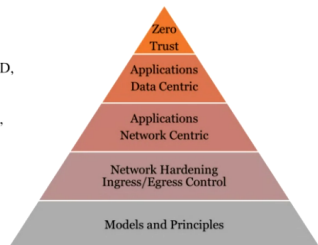
Section 5 – ZT principles and practical architectures with NAC, SASE, SIEM, EDR, Tripwires, and Red Herrings

Section 4 – L7 data centric: WAF, DB, encryption, AD, Cloud, DB, DLP, MDM, CASB, and Containers

Section 3 – L7 network security: NGFW, NSM, TLS, remote access, jump boxes, and anti DDoS

Section 2 – Hardening Layers 3-4, IPv6, DNS, controlling ingress/egress, FWs, segmentation, and proxies

Section 1 – Fundamentals, DARIOM, intelligence-driven architectures, and hardening Layers 1-2



Defensible Network Architecture:

Monitored, Inventoried, Controlled, Claimed,
Minimized, Assessed, Current

Defensible Security Architecture Life Cycle:

Discover & Assess, Redesign,
Implement, Operate & Monitor

Mindset: *Build it once, build it right.*

Failed mindsets:

Inside == trusted, outside == untrusted

All-Prevent Defense

Compliance-Driven Security

Shiny object syndrome

1 – Journey Towards Zero Trust

Course Overview	530.1-4-17
Defensible Security Architecture	530.1-18-23
Network Flow	530.1-137-152
Physical Security	530.1-78-89
Private VLANs	530.1-126-136
Security Models	530.1-51-63
Threat, Vuln, Data Flow Analysis	530.1-64-75
Traditional SecArch Deficiencies	530.1-24-36
Winning Defensible Sec Strategies	530.1-37-48
Wireless	530.1-90-105

2 – Network Sec Architecture and Engineering

Blackholes and Darknets	530.2-62-67
Bogon Filtering	530.2-57-61
IPv6	530.2-70-95
Layer 3 Attacks and Mitigation	530.2-4-13
Securing IPv6	530.2-96-115
Securing NTP	530.2-51-56
Securing SNMP	530.2-44-50
Segmentation	530.2-118-134
SMTP Proxy	530.2-159-173
Switch and Router Best Practices	530.2-14-41
Web Proxy	530.2-135-158

3 – Network-Centric AppSec Architecture

Distributed DoS (DDoS) Protection	530.3-137-153
Malware Detection	530.3-89-107
Network Encryption	530.3-154-173
Network Intrusion Detection (NIDS)	530.3-65-85

Network Security Monitoring (NSM)	530.3-24-62
Next-Generation Firewall (NGFW)	530.3-4-23
Remote Access	530.3-108-136

4 – Data-Centric AppSec Architecture

Access Controls	530.4-50-59
Containers	530.4-169-180
Data Encryption	530.4-60-73
Data Loss Prevention (DLP)	530.4-94-105
Data-Centric Security	530.4-4-9
Database Monitoring and Controls	530.4-34-49
Enterprise Data Control	530.4-106-125
File Classification	530.4-74-91
Mobile Device Mgt (MDM)	530.4-126-139
Private Cloud Security	530.4-140-159
Public Cloud Challenges	530.4-160-168
Web Application Firewalls (WAF)	530.4-10-32

5 – Zero-Trust Architecture: Addressing the Adversaries Already in Our Networks

Audit Policies	530.5-119-138
Credential Rotation	530.5-19-30
Host-Based Firewalls	530.5-52-57
Log Collection	530.5-96-118
MITRE ATT&CK Content Engr	530.5-139-162
Network Access Control (NAC)	530.5-58-74
Securing Traffic	530.5-31-49
Security Info and Event Mgt (SIEM)	530.5-87-93
Segmentation Gateways	530.5-75-86
Tripwires and Red Herring Def	530.5-165-184
Zero Trust Architecture	530.5-4-18

Categories

Labs

Advanced Defense Strategies	530.W-324-339
Architecting for Flow Data	530.W-79-96
Architecting for NSM	530.W-174-197
Auditing Router Security	530.W-97-122
Cloud Monitoring and Asset Tracking	530.W-402-424
Discovering Sensitive Data	530.W-251-262, 530.W-425-442
Egress Analysis	530.W-36-52
Encryption Considerations	530.W-214-237
Intelligence-Drive Architectures	530.W-340-366
IPv6	530.W-140-163
Layer 2 Attacks	530.W-53-78
Mutual Authentication	530.W-276-293
Network Isolation	530.W-276-293
Network Security Monitoring	530.W-198-213
Practical Threat Modeling with MITRE ATT&CK	530.W-8-35
Proxy Power	530.W-164-173
Remediating Web Vulnerabilities	530.W-367-401
Router SNMP Security	530.W-123-139
Secure Virtualization	530.W-263-275

SEC530 – Defensible Security Architecture and Engineering: Implementing Zero Trust for the Hybrid Enterprise

Securing Web Applications	530.W-238-250
Setup	530.W-4-7
SIEM Analysis and Tactical Detection	530.W-293-311
Sigma Generic Signatures	530.W-313-323
VirusTotal Enterprise	530.W-340-366

Tools

Any Run 🐧	530.3-99
auditctl 🐧	530.5-136
auditd 🐧	530.5-134
auditpol 🌈	530.5-123
ausyscall 🐧	530.5-137
Auto Secure (Cisco)	530.2-30-31
BloodHound	530.3-127
Bro 🐧	530.3-49
Samples	530.3-56-57
bro-cut 🐧	530.3-56
bro-pkg 🐧	530.3-59
Cain and Abel	530.1-119
chmod 🐧	530.4-57
CIS-CAT Pro 🟡	530.2-38
Cisco IOS (any)	530.2-34
Cisco IOS (router)	530.1-119, 123, 143
.....	530.2-10-11, 16, 19-20, 30-31, 61, 110, 126
Cisco IOS (switch)	530.1-114-115, 119, 133
.....	530.2-17-19, 21-23, 111
copy 🌈	530.4-55
Cuckoo Sandbox	530.3-100
curl 🐧	530.5-64
dig	530.3-148
dnstwist	530.2-169
Docker 🐧	530.4-172, 176, 179
domain_stats	530.3-37
dsniff 🐧	530.1-112
Ettercap	530.1-119
EveBox	530.3-84
Evil Foca	530.2-72
find 🐧	530.4-57
fprobe 🐧	530.1-143
freq	530.3-37
.....	530.5-92
fwknop	530.5-47
getfacl 🐧	530.4-56
Guacamole	530.3-117
hping	530.2-13
ifconfig 🍏	530.2-91
ip 🐧	530.2-89, 91, 102
ip6tables 🐧	530.2-99
ipconfig 🌈	530.2-87
iptables 🐧	530.2-128-129
John The Ripper	530.2-48
Kibana	530.3-83
Kon-Boot	530.4-66
macof 🐧	530.1-112
masscan	530.2-101
Metasploit	530.2-46, 102-103, 113
ModSecurity	530.4-16

MRTG	530.2-66
net group 🌈	530.5-181
netsh 🌈	530.1-118
.....	530.2-91, 102
netstat 🐧 🍏	530.2-102
.....	530.3-29
NFdump	530.1-150
NfSen NetFlow Analyzer	530.1-150
nftables 🐧	530.2-99
Nipper Studio 🟡	530.2-38
Nipper-ng	530.2-38-40
Nmap	530.2-46-47, 56, 101
ntopng	530.1-149, 151
Ntpdc	530.2-55-56
ocr.ps1 📄	530.4-82
PfSense	530.2-127
ping	530.2-13
ping6 🐧 🍏	530.2-100, 102
ProxyCannon	530.3-116
pulledpork	530.3-76-77
radv	530.2-95
radvdump 🍏	530.2-92
Rumble Network Discovery (RND)	530.2-104
Security Onion 🐧	530.3-33
setfacl 🐧	530.4-56
Sigma2attack	530.5-161
sigmac	530.5-148-149, 157, 159
Snort	530.2-108-109
.....	530.3-68-72
Squid	530.2-154-155
sslstrip	530.3-161
streams 🌈	530.4-80
Suricata	530.1-146-147
.....	530.3-73-74
sysctl 🐧 🍏	530.2-88, 92
Sysmon	530.5-127-129
Ubee 🐧	530.2-100
VeraCrypt	530.4-67
viewssld	530.3-167
vssadmin 🌈	530.4-55
Wireshark	530.2-109
.....	530.3-167
zcat	530.2-105
Zeek 🐧	530.3-36-61

Commands (Cisco IOS)

access-list	530.2-49, 126
auto secure	530.2-30
banner login	530.2-25
crypto key generate	530.2-17, 36
enable algorithm-type	530.2-23
ip access-list	530.2-61
ip arp inspection trust	530.1-119
ip authentication	530.2-11
ip dhcp snooping	530.1-123
ip domain-name	530.2-17
ip flow-export	530.1-143
ip flow	530.1-143

SEC530 – Defensible Security Architecture and Engineering: Implementing Zero Trust for the Hybrid Enterprise

ip ssh	530.2–17, 36
ipv6 nd rguard	530.2–111
key chain	530.2–10
logging	530.2–19
no cdp enable	530.2–18
no ip bootp server	530.2–18
no ip http server	530.2–18
no service config	530.2–18
private-vlan	530.1–133-134
service password-encryption	530.2–21
service password	530.2–34
snmp-server community	530.2–49
snmp-server group	530.2–50
switchport private-vlan	530.1–135




Zero Trust Principles

Access Continuously Verified	530.5–77
Access Determined By Network Agent ..	530.5–76
All Traffic Secured	530.5–12
Assets Scanned, Hardened & Rotated ...	530.5–12
Assume Breach	530.5–6
Central Control & Automation	530.5–77-78
Connect To Authorized Systems Only ...	530.5–53
Data Flows Known & Controlled	530.5–12
Data-Centric Focus	530.5–6
Every Flow Must Be Proven	530.5–6
Identity Determined By User & Device ..	530.5–76
Internal Network Not Trusted	530.5–6
Least Privilege Enforced	530.5–12
Log & Inspect All Traffic	530.5–6, 12
Passwords Rotated & Audited	530.5–30
Threats Always Present	530.5–6
Traffic Authenticated & Encrypted ..	530.5–48, 59
Variable Trust	530.5–13

A

Abnormal Conditions	530.5–85
Abnormal Event	530.3–37
Access Control	530.1–63, 101
.....	530.2–120-121
.....	530.4–51-57
MAC-Based	530.1–104
Monitoring	530.4–58
Summary	530.4–59
Access Management	530.5–124
Access Requirements Example	530.4–110
Access-Denied Assistance	530.4–108
Account Lockout	530.4–26
ACL	530.1–27, 104, 119
Inbound/Outbound	530.2–126
Standard/Extended	530.2–126
Active Defense	530.5–167
Active Directory	530.1–101
.....	530.3–14
.....	530.4–68
.....	530.5–27, 82
Administrative Center	530.4–79, 112
.....	530.5–23
Management	530.3–128
Rights Management	530.4–85
Acunetix	530.4–24
Add-KdsRootKey	530.5–29
Admin Password Reset	530.2–16
Administrative Workstation	530.2–131
.....	530.3–130
ADS	530.4–80, 86
Adversary Vulnerabilities	530.5–167
AES	530.1–104
.....	530.2–50
AFRINIC	530.2–84
Agent-Based Flow	530.1–139
AH	530.5–44
AIP	530.4–85-86, 89
Air Marshal (Meraki)	530.1–94
Alert	530.5–140
Anomaly-Centric	530.5–142
Automated	530.5–144
Engine	530.5–90
Real-Time	530.5–162
Signature-Centric	530.5–142
Alert-Driven Workflows	530.3–26
Alexa	530.5–92
All-Prevent Defense	530.1–32
Always On VPN	530.3–122-124
Amazon	530.1–139, 145
Amplification Factor	530.2–55
Analytics	530.3–39
Analytics Reuse & Sharing	530.5–148
Anomaly	530.5–142-143
Detection	530.5–144, 162
Anomaly-Based IDS	530.1–140
.....	530.3–66
Antivirus Database	530.3–92

SEC530 – Defensible Security Architecture and Engineering: Implementing Zero Trust for the Hybrid Enterprise

AntiVMDetection	530.3–104
API	530.3–21
Hooking	530.3–96
APNIC	530.2–84
App Any Run (Interactive Malware Analysis)	530.3–99
AppArmor	530.4–174
Apple System Logger 	530.5–131
Application Attack (DDoS)	530.3–148
Mitigation	530.3–149
Application Awareness	530.4–46
Application Container	530.4–133
Application Control	530.3–7-8
.....	530.4–8
Application Layer Security	530.2–136
Application Proxy → Proxy	
Application Rules	530.3–19
Application Streaming	530.3–131
Application-Level Inspection	530.3–5
APT	530.1–40
29	530.1–59
41	530.1–43
.....	530.2–6
ARIN	530.2–84
ARP	530.1–30, 116-117
Cache Poisoning	530.1–116, 118
Mitigation	530.1–119-121
Cache Settings	530.1–118
Spoofing	530.1–116, 119
Mitigation	530.1–119
ARPANET	530.1–19, 26
.....	530.2–16
ASEP	530.5–116
ASN	530.3–102
Asset Discovery	530.3–25
Asset Tracking	530.3–51
Assume Breach	530.5–5-6, 166
Attack Surface Analysis	530.1–66, 68-69
Attacker Reconnaissance Auditing	530.5–181
Attacks (ARP)	530.1–116
Attacks (DHCP)	530.1–120-123
Attacks (IPv6)	530.2–72
Attacks (routers)	530.2–6
Attacks (switches)	530.1–108
Audit Example 	530.5–135
Audit File System	530.5–125
Audit Object Access	530.4–54
Audit Policy	530.5–120-121
Advanced	530.5–121-122
Summary	530.5–138
Windows	530.5–121
Audit Process Creation	530.5–126
audit.rules	530.5–136
Auditd 	530.5–134, 179
Capabilities	530.5–134
Configuration	530.5–136
AUID	530.5–135
Authenticated Internet Access	530.3–18
Authentication & Encryption	530.3–34

Authentication Factors	530.3–118
Authentication Retries	530.2–16-17
Automated Build Image	530.4–177
Automatic Boot	530.4–69
Automatic Classification Rules	530.4–81
Automatic Enrollment	530.5–40-41
Automatic Submission	530.3–96
AUX port	530.2–16
AV Storm	530.4–157
AWS S3 Bucket	530.4–166
Azure	530.2–132
.....	530.4–134
Information Protection → AIP	
Key Vault	530.4–161
Rights Management Connector	530.4–89
vTAP	530.4–162

B

Backdoor	530.5–22
Backup Files & Directories	530.4–53
Bad Checksums	530.3–49
Banners	530.2–25
Baseline	530.1–74
Bayesian Analysis	530.2–162
BCP	530.1–47, 66
Bcrypt	530.2–24
Beaconing Detection	530.3–40, 61
Behavior Monitoring	530.3–91-93
.....	530.4–44
.....	530.5–142
Behavioral Anomaly	530.5–85
BGP	530.1–142
.....	530.3–150
BIOS	530.4–66
BitLocker	530.4–68, 122
Network Unlock	530.4–70
To Go	530.4–68, 122
Blackhole	530.2–63
Blind Spot	530.1–71
BloodHound	530.3–127
Bluetooth	530.1–91
Bogon	530.2–58-59
Filter	530.2–60-61
Bootkit Attack	530.4–65-66
BOOTP	530.2–18
Botnet Tunneling	530.3–115
BPF	530.1–144
Filtering	530.1–147
Breakout Point	530.1–59
Bro	530.1–144
.....	530.3–35, 38
Package Manager	530.3–59
Scripting	530.3–45, 50-54
Bruteforce Attack	530.4–113
BSSID	530.1–94
Business Impact	530.2–125
Business Outcome-Focused Architecture	530.1–38

SEC530 – Defensible Security Architecture and Engineering: Implementing Zero Trust for the Hybrid Enterprise

BYOAP	530.1–93
BYOD	530.4–127-130, 137
Bypass List	530.2–150

C

CA	530.5–38
Types	530.5–40
CAA	530.3–164
Caching Accelerator	530.3–147
CAM	530.1–112
.....	530.2–101
Overflow	530.1–112-113, 116
Mitigation	530.1–113
Table	530.1–111-113
Canarytoken	530.5–178, 182
CapMe	530.3–83
CAPTCHA	530.4–23, 26
Captive Portal	530.5–60, 68
CASB	530.2–139
.....	530.4–167
CDN	530.3–16
CDP	530.1–30, 72
.....	530.2–18
Hardening	530.1–109
Central Access Policy	530.4–118
Central Management Lockdown	530.4–153
Centralized Control	530.5–78
Centralized Logging	530.2–19
.....	530.5–83
Centralized Protection	530.5–84
Cert Spotter	530.3–163
Certbot	530.3–159
Certificate Enrollment	530.5–38
Certificate Transparency Monitoring	530.3–163
cFlow/cPacket	530.3–43
CGroup	530.4–176
Chain (FW rules)	530.2–128
Chaining (IPv6 Extension Headers)	530.2–78
Challenge-Response	530.1–105
Change Monitoring	530.5–124
Change Tracking	530.4–36
Channel Binding Token	530.5–110
Chrome (Google)	530.1–67
Chroot	530.4–171
Cipher Suites	530.3–165
CIS	530.2–35-38
SecureSuite Membership	530.2–38
CIS Critical Control 1	530.5–59, 74
Cisco	530.1–79, 141
AutoSecure	530.2–30-31
Best Practices	530.2–29
Default Password Type	530.2–21
Default RSA Key Size	530.2–16
Default SSH Version	530.2–16
IOS Benchmark	530.2–36-37
Logging	530.2–19
Nexus	530.1–133

Passwords	530.2–21-22, 34
Smart Install	530.2–26
CiscoParse	530.2–38
Claims	530.4–112-113
ClamAV	530.2–154
Classification Levels	530.2–121
Clean Source Principle → CSP	
Client Access Network	530.1–71
Client Certificate	530.5–37
Client Hello	530.5–36
Client-to-Client Pivot	530.1–46
Cloud	530.2–153
Connection Point	530.4–167
Encryption	530.4–71
Environment	530.1–139
Isolation	530.4–164
CNSA	530.1–102
COBIT	530.1–38, 54
COMINT	530.1–140
Command and Control	530.2–150
.....	530.3–32, 39, 56-57, 157
Community Port	530.1–127, 131-132
.....	530.2–123
Configuration	530.1–135
Compensating Controls	530.2–131
Compliance	530.1–32, 35
Checks	530.5–61
Compound Authentication	530.4–113
Computer Certificate	530.5–65
Conditional Access	530.4–110-111, 115
Auditing	530.4–116
Time Restriction	530.4–119-120
Conficker (worm)	530.1–29
Console Access	530.4–154
Console port	530.2–16
Container	530.4–170-171
Auditing & Logging	530.4–179
Escape	530.4–174-175
Impact	530.4–173
Secrets	530.4–178
Summary	530.4–180
Content Discovery	530.4–39-40
Content Filtering	530.2–144, 156
Bypass	530.2–145
Content Inspection	530.4–99
Content-Based Classification Rules	530.4–81
Context (alerts)	530.3–25-26, 35, 74
Control Gate	530.2–121
Control Plane	530.5–77
Controlled Authentication	530.3–133
Controlled Network Authentication	530.3–127
Core Routing	530.5–78
Corporate Workspace	530.4–132
Cousin Domain	530.2–168-169
.....	530.3–37
Cozy Bear	530.1–59
Credential Rotation	530.5–20-22
Automatic	530.5–26

SEC530 – Defensible Security Architecture and Engineering: Implementing Zero Trust for the Hybrid Enterprise


Summary	530.5–30
Critical Assets	530.1–47
.....	530.2–124-125
Cryptanalysis	530.1–140
Crypto Suite Support	530.3–165
CSC	530.1–38, 54
CSF (NIST)	530.1–38, 54
CSP	530.3–128
Cuckoo	530.3–100
Custom Applications	530.4–8, 11
CVE-2010-2568	530.4–155
CVE-2017-8905	530.4–149
CVE-2018-0171	530.2–26
CVE-2018-6981	530.4–149
CVE-2019-0887	530.4–149
Cyber Kill Chain	530.1–57-59
Countermeasures	530.1–58
Cyber Prep (MITRE)	530.1–41

D

DAC	530.4–79, 109, 115
DAD	530.2–90
DAI	530.1–119
DAM	530.4–42, 47-48
Application Awareness	530.4–46
Deployment	530.4–43
User Context Awareness	530.4–45
DARIOM (model)	530.1–65, 79
Discover and Assess	530.1–66, 80, 107, 156
.....	530.2–5, 71, 177
Operate and Monitor	530.1–75, 159
.....	179
Redesign and Implement	530.1–73-74, 89, 157-158
.....	530.2–67, 115, 178
Darknet	530.2–63-66
Dashboard	530.3–39, 41
Data At Rest/In Motion	530.1–75
.....	530.4–61, 95
Data Cleanup	530.4–101
Data Diode	530.5–107
Data Encryption	530.4–61
Summary	530.4–72
Data Expiration	530.4–83
Data Governance	530.4–75
Summary	530.4–138
Data Leakage	530.4–99
Data Masking	530.4–41
Data Plane	530.5–77
Data Policy	530.4–107
Protection	530.4–124
Summary	530.4–125
Data Protection	530.4–51
Data Remanence	530.4–164
Data Restriction Policy	530.4–107
Data Stubbing	530.4–101
Data-Centric Defenses	530.4–6
Data-Driven Workflows	530.3–26

Database Encryption	530.4–63
Database Logging	530.4–36
Database Monitoring	530.4–35-36
Summary	530.4–48
Database Security	530.4–37
Issue	530.4–38
DBF(W)	530.4–42, 48
Application Awareness	530.4–46
Deployment	530.4–43
User Context Awareness	530.4–45
DBIR	530.1–32
.....	530.4–12
DCEPT	530.5–180
DDoS	530.3–138
Attack Types	530.3–140
Application	530.3–148
HTTP	530.3–146
Protocol	530.3–143
Volumetric	530.3–140
Mitigation	530.3–142, 147, 149, 151
Protection (ISP)	530.3–142
Scrubbing	530.3–150
Summary	530.3–152
De-perimetrization	530.1–30
Deauthentication	530.1–96
Deceptive Security	530.5–166
Deep-Packet Inspection	530.3–5-7, 13
Default Credentials	530.3–139
Default Gateway	530.1–131-132
.....	530.2–95
Default Logging	530.5–120
Defense-In-Depth	530.1–32
.....	530.2–37
Defensible Networks	530.1–21-23
Delivery Optimization	530.1–129-130
Denial-of-Service	530.1–111, 140
.....	530.2–55-56, 58, 111
.....	530.4–176
Distributed	530.3–138
DES	530.2–50
Detailed Tracking	530.5–126
DeTT&CT (MITRE)	530.1–44
Device Certificate	530.5–41
Device Claim	530.4–111, 117
DGA	530.3–56
DHCP	530.1–30
.....	530.4–70
Fingerprinting	530.5–61, 63-64, 71
Database	530.5–64
Options	530.5–63
Rogue Server	530.1–119-122
Mitigation	530.1–123
Snooping	530.1–119, 123
Starvation	530.1–119-120
DHCPv6	530.2–85, 87, 95
Dictionary Attack	530.3–115
Diffie-Hellman	530.3–168
.....	530.5–44

SEC530 – Defensible Security Architecture and Engineering: Implementing Zero Trust for the Hybrid Enterprise

Digital Certificate	530.1–101, 103
.....	530.2–143
.....	530.3–56
Digital Signature	530.2–165
DirectAccess	530.3–124
DISA	530.2–28, 32–34
.....	530.5–8–11
Disassociation	530.1–96
Discover and Assess → DARIOM (model)	
Disk Encryption	530.4–65, 67
Diversion	530.5–184
DKIM	530.2–165–168
DLP	530.2–139, 142
.....	530.3–6
.....	530.4–77
Agent	530.4–102
Bypass	530.4–103
Cloud-Based	530.4–100
Definition	530.4–95
Network-Based	530.4–96–99, 121
Limitations	530.4–99
Summary	530.4–104
DMA Attack	530.4–69
DMARC	530.2–167–168
DMZ	530.1–127
.....	530.2–122–125, 152–153
Design	530.2–123
DNS	530.2–150, 163, 165, 167
.....	530.3–8–9
Amplification Attack	530.3–148–149
Round Robin	530.2–53
Tunnel	530.2–150
Detection	530.3–61
DNS Recursion	530.3–149
Docker	530.4–170–172
Compose	530.4–178
Container	530.3–55
Content Trust	530.4–177
Hub	530.4–177
Swarm	530.4–178
Dockerfile	530.4–175, 177
Domain Admins	530.5–124, 181
Domain Isolation 	530.5–43
Domain Registrar	530.2–145
Domain Validation	530.3–164
Downgrade Attack (HTTPS)	530.3–161
Dridex	530.3–60
Drive Mapping	530.4–129
Drive-By Malware	530.2–141
Duplicate Address Detection → DAD	
Dynamic Access	530.5–71–72, 88
Dynamic Authorization	530.5–85
Dynamic Data Mask	530.4–41

E

EAP-TLS	530.1–103
ECDH	530.1–102–103

ECDSA	530.1–102–103
EDNS0	530.3–148
EDR	530.5–146
Effective Access	530.4–117
EFS	530.4–64
EGP	530.2–9
Egress Analysis	530.1–70
EIGRP	530.2–9–11, 37
EKM	530.4–63
Elastic Stack	530.3–41
ElasticSearch	530.3–55
.....	530.5–159
Electric Fence (Concept)	530.5–72, 89
Elliptic Curve	530.5–44
Email Data Control	530.4–123
Email Spoofing	530.2–165, 168
Emergency Admin Account	530.2–33
Encrypted Container	530.4–67
Encrypted Data	530.4–62
Encryption & Authentication	530.3–34
End-to-End Encryption	530.5–34
Endpoint Visibility	530.3–41
Engagement Activities	530.5–167
Enterprise Admins	530.5–124
Enterprise CA	530.5–40–41
EQL	530.5–146
ESP	530.5–44
EternalBlue	530.1–29
EUI-64	530.2–86
Evasion	530.3–90
Event ID 4625	530.5–180
Event ID 4662	530.5–181
Event Log Readers (Group)	530.5–114
Evil Twin	530.1–94
EVT(X)	530.5–104, 111
Executable-Based Lock Down	530.5–55
Exfiltration	530.2–150
.....	530.3–9, 39
Analysis	530.1–70
Explicit Permissions	530.4–52
Export-ImageText	530.4–82
Exposure	530.1–59
External-Facing Sensor	530.3–32
EXTERNAL_NET	530.3–70

F

F5 Irule	530.5–173
Facility Codes	530.5–101
Fake Account	530.5–180, 183
Fake DHCPv6	530.2–72
Fake Email Accounts	530.2–171
FakeDNS	530.3–102
False Positives/Negatives	530.1–60
.....	530.3–14, 78
.....	530.5–88, 140, 162
Reduction	530.3–80
FAST	530.4–113

SEC530 – Defensible Security Architecture and Engineering: Implementing Zero Trust for the Hybrid Enterprise

FC00::/7	530.2–93
FCI	530.4–78, 83–85
Integration	530.4–84–85, 89
FD00::/8	530.2–93
FDE	530.4–65–66
FDFE:	530.2–87
FE80::	530.2–86–87
Federation Services	530.5–76
FF02::1	530.2–94, 113
FF02::2	530.2–94
Field Normalization	530.5–147
File Auditing	530.5–125, 179
File Carving	530.3–98
File Classification	530.4–77, 80, 82, 84–85, 88
Copy	530.4–84
Example	530.4–87
Move	530.4–84
Summary	530.4–90
File Monitoring	530.5–137
File Permissions	530.4–53
File Properties	530.4–79
File Relocation	530.4–101
FilesNotToSnapshot	530.4–55
FIN4	530.1–43
Fingerbank	530.5–64
Fingerd	530.2–18
FIPS 140-2	530.2–34
Firewall	530.1–26
Architecture	530.2–122
Policy (guidelines)	530.2–122
FireWire	530.4–69
Flare	530.3–61
Flat Network	530.1–27
Flexible Authentication Secure Tunneling → FAST ...	
Flow Components	530.1–149
Flow Logs	530.4–162
Flowbits	530.3–77
FlowSet	530.1–142
Fluentd	530.5–109, 113
FMX	530.1–42
Forest Functional Level	530.4–79
Forward Web Proxy	530.5–173
ForwardedEvents.evtx	530.5–111
FQDN Blocking	530.3–112
Fragmentation	530.1–23
Frequency Analysis	530.3–37
Frequency Anomaly	530.5–85
FSRM (Windows Server Role)	530.4–78
FUD	530.5–5
Full Stack Security	530.4–7
Full Tunneling (VPN)	530.3–121–122
Fullbogon	530.2–58–59
FWaaS	530.2–139
Fwknop	530.5–47

G

GCM	530.5–44
-----------	----------

GCMP	530.1–102
GDPR	530.1–66
Geographic Detection	530.3–51
Geographical Anomaly	530.5–85
Geolocation	530.3–11
Blocking	530.3–16
Malware Behavior	530.3–102
Get-Content	530.4–87
Get-WinEvent	530.5–104
Getfacl	530.4–56
Global Unicast Address	530.2–82–84, 87, 111
GMAC	530.5–44
gMSA	530.5–29
Gold Image	530.5–26
Google Auth	530.3–120
GoToMyPC	530.3–111, 113
Granular Rules	530.5–57
Gratuitous ARP	530.1–118
GRC	530.1–53, 66
GRE	530.1–142
.....	530.3–150
Tunnel	530.2–13, 107
Group Policy	530.4–53
GRSEC	530.4–180
GUA → Global Unicast Address	
Guacamole (Apache)	530.3–117, 120
Guest Management	530.1–97
.....	530.5–68

H

HALO	530.5–183
Hardcoded MAC Address	530.1–113–114
Hardening	530.1–109
Hardware Implant	530.1–85
Health Monitoring	530.5–70
Heartbleed	530.3–114
Hexatier	530.4–43
HIDS	530.4–162
Hierarchy of Needs	530.1–61
HIPAA	530.1–66
.....	530.4–165
HITRUST	530.4–165
HMAC	530.1–102
.....	530.2–10
.....	530.3–119
Honeypot	530.5–175–177
Honeytoken	530.5–178, 180
Hop Limit	530.2–77
Host-Based Firewall	530.5–53, 79
Capabilities	530.5–54
Inbound Access	530.5–55
Logging	530.5–57
Outbound Access	530.5–56
HOTP	530.3–119
HP WebInspect	530.4–24
HSM	530.4–63, 161
HSTS	530.3–160–162

SEC530 – Defensible Security Architecture and Engineering: Implementing Zero Trust for the Hybrid Enterprise

Preloading	530.3–162
HTTP Attack (DDoS)	530.3–146
Mitigation	530.3–147
Hunting Solution	530.1–60
Hurricane Electric	530.2–114
Hyper-Converged Storage	530.4–154
Hypervisor	530.4–141, 171
Hardening	530.4–152
Migration	530.4–144
Networking	530.4–142
Security	530.4–148–152
Hypervisor-Based Endpoint Security	530.4–157
Hypponen (law)	530.1–33

I

IaaS	530.1–127, 152
.....	530.4–162
IAM	530.3–127, 134
IBM AppScan	530.4–24
ICAP	530.2–154–156
.....	530.4–96
ICMP Flooding	530.3–141
ICS	530.1–69
Identity Management	530.5–76, 80
IDS	530.3–73–74
.....	530.4–97
Default Configuration	530.3–78
Evasion	530.2–107
IEEE 802.11	530.1–91
n/ac/w	530.1–95–96
IEEE 802.15.4	530.1–104
IEEE 802.1X	530.1–88, 101–102, 113
.....	530.2–33
.....	530.5–34, 41, 62, 67
Port Authentication	530.5–61
IGP	530.2–9
Impact Assessment	530.1–38
Imperva	530.4–43
Inbound Access	530.5–55
Inbound Rules	530.3–20
InetSim	530.3–102
Ingress Analysis	530.1–70
Inherited Permissions	530.4–52
Inline Analysis	530.3–96
Inline Visibility	530.3–27
Intermediate CA	530.5–39
Internal Monitoring	530.3–32
Internal Pivoting	530.3–70, 81
Internet Zone	530.4–80
Intrusion Prevention	530.3–5–7
Inventory Automation	530.5–82
IOC	530.3–100
IoT	530.1–33, 69
.....	530.3–138–139
IPS	530.3–27
Bypass	530.2–78, 107
IPSec	530.5–34, 41–43

Support	530.5–42
Windows	530.5–44–45
Iptables	530.2–99, 128–129
.....	530.5–53–54
IPv4	530.2–73, 74
Headers	530.2–76
IPv5	530.2–75
IPv6	530.1–67, 142
.....	530.2–71–115
Addresses	530.2–80–95
Assignment	530.2–95
Format	530.2–83
Multicast	530.2–94, 101
Types	530.2–82
Discovery	530.2–102–106
Encapsulation	530.2–107
Firewall Support	530.2–99
Growth	530.2–74
Headers	530.2–76–79
Rogue Router Attack	530.2–112–113
Router Advertisement	530.2–111–113
Scanning	530.2–101
Security Issues	530.2–98
Subnet	530.2–81
Tunneling	530.2–107–110
IS-IS	530.2–9
ISATAP	530.2–107
ISO27001	530.1–38, 54
Isolated Port	530.1–127, 131–132
.....	530.2–123
Configuration	530.1–135
ISP	530.3–142

J

JA3	530.3–58–60
Jammer	530.1–105
Jump Box	530.2–131
.....	530.3–127, 131–133
Just-In-Time	530.2–132

K

KDC	530.4–113
KDS Root Key	530.5–29
Kerberos	530.2–52
.....	530.5–44
Kerberos Armoring	530.4–111, 113
Support	530.4–113–114
Key Chain	530.2–10–11
Key Management	530.1–96, 101
Key Recovery	530.4–64, 68
Keylogger	530.4–130
Kibana	530.3–41
Kon-Boot	530.4–66, 103
Kubernetes	530.3–55
.....	530.4–178

L

SEC530 – Defensible Security Architecture and Engineering: Implementing Zero Trust for the Hybrid Enterprise

LACNIC	530.2–84
LAPS	530.5–27
Lateral Movement	530.3–129
.....	530.5–180
Law	530.1–33
Layer 1	530.1–85–88
Attacks	530.1–85–86
Mitigations	530.1–88
Layer 2	530.1–107–123
Attacks	530.1–108
Audit Tools	530.2–28
Benchmarks	530.2–33–34
Mitigations	530.1–109, 113–115, 119, 123
Layer 3	530.2–5–13
Attacks	530.2–6–8
Audit Tools	530.2–28, 38
Benchmarks	530.2–35
Mitigations	530.2–12
Layer 4	530.3–5
Layer 7	530.2–136
.....	530.3–5–8, 66
Inspection	530.5–80
Layer 8	530.1–84
.....	530.2–168
LDAP	530.1–101
.....	530.3–14
LDAPS	530.5–41
Least Privilege	530.1–63
.....	530.2–131
.....	530.5–17
Legacy Protocols	530.2–18
Let’s Encrypt	530.3–159
Liability	530.1–97
Libpcap	530.3–45
Link Aggregation Group	530.1–127
Link-Local Address (fe80)	530.2–82, 104
Linux Containers → LXC	
Linux Logs	530.5–130
Audit Example	530.5–135
Linux Permissions	530.4–56–57
LLDP	530.1–72
Hardening	530.1–109
LLMNR	530.2–94
LM	530.2–23
Load Balancer	530.2–138
.....	530.3–151
Local Admin Account	530.2–131
.....	530.5–26
Local Administrator	530.4–64
Local Virtualization	530.3–132
Location-Based Classification Rules	530.4–81
Lockdown Mode	530.4–151
Log Agent	530.5–104–108, 146
Features	530.5–107–108
Modern	530.5–109
Third-Party	530.5–111–112
Capabilities (Open-Source)	530.5–113
Types	530.5–105

Log Aggregator	530.5–90
Log Broker	530.5–90
Log Collection	530.5–97
Agentless	530.5–114
Summary	530.5–118
Log Collector	530.5–90
Log Enrichment	530.5–91–92
Log Extraction (Traditional VS Network) ...	530.5–117
Log Field Parsing	530.5–103
Log Inspection	530.5–91
Logging	530.2–19
LogMeIn	530.3–113
Loopback Interface	530.2–20
LSA Secrets	530.3–129
LXC	530.4–170–171

M

MAC	530.5–62
Address Filtering	530.1–88
Authentication	530.5–62
Limiting	530.1–115
Spoofing	530.1–111, 116
Mitigation	530.1–113
Machine Learning	530.2–162
Machine-In-The-Middle	530.5–43, 110
Malformed Frames	530.3–28, 30
Malicious Image	530.4–177
Malware Detonation	530.3–91–106
Cloud Services Issue	530.3–94
Network Access	530.3–102
Summary	530.3–106
Workflow	530.3–92
Malware Hash Registry	530.3–52
Man-In-The-Middle	530.1–94, 116, 121
.....	530.2–8, 10, 12, 54
.....	530.3–161
.....	530.4–113
Managed Service Account → MSA	
Management Network	530.4–142, 148
Management Server	530.4–150–151
Management Traffic	530.2–20
Mangle Table	530.2–128
Master Key	530.4–69
MCAP	530.5–79, 81–82
MD4	530.2–23
MD5	530.2–11
MDM	530.4–123, 131–137
Example	530.4–136
Policy	530.4–135
Security	530.4–137
Meltdown	530.4–163
Memory Analysis	530.3–93
Metadata Logging	530.3–74
Metasploit Browser Autopwn	530.5–173
Meterpreter	530.5–25
MFA	530.2–120, 132
.....	530.3–113

SEC530 – Defensible Security Architecture and Engineering: Implementing Zero Trust for the Hybrid Enterprise

.....	530.4–23, 69, 129
MHN	530.5–176
MIB	530.2–105
Microsoft Intune	530.4–134
Microsoft Update	530.2–136
.....	530.3–8-9
.....	530.5–110
Migration Network	530.4–142
MIME	530.2–142
.....	530.3–7
Mimikatz	530.1–29
.....	530.3–129
.....	530.5–180
MimikatzHoneyToken	530.5–180
Mirai	530.3–139
Mirror Port → Port Mirroring	
SSL Decrypt	530.3–170
Misconfigured Asset	530.3–37
MITRE	530.1–41-42, 44, 59
ATT&CK	530.1–42, 59
.....	530.5–146-147
Mapping to Engage	530.5–167
Matrix	530.5–145
Navigator	530.1–44
Engage	530.5–167
Shield	530.5–167
MLD	530.2–103
Mobile Devices	530.2–153
ModSecurity	530.4–16
Monlist	530.2–55-56
MOP	530.2–18
Morris (worm)	530.1–26
MotD	530.2–25
MPLS	530.1–142
MS08-067	530.1–29
MS14-025	530.5–27
MS17-010	530.1–29
MSA	530.5–28
MSS	530.1–23
MSSP	530.1–32
mTLS	530.5–36
MTU	530.5–102
Multicast Address	530.2–94, 101
Multifactor Authentication	530.3–118
Multitenancy	530.4–163
Mutual Authentication	530.5–37, 41

N

NAC	530.1–63, 88, 113
.....	530.5–46, 59
Agent	530.5–70
Capabilities	530.5–61
Deployment	530.5–60, 66-67
Inline	530.5–66-67
Out-of-Band	530.5–66-67
Example	530.5–65
Problems	530.5–73

Summary	530.5–74
Name Server	530.2–150
Namespace	530.4–174-175
NAS	530.4–142-143
NAT	530.2–128
.....	530.3–32
NCP	530.2–16
NDP Host Solicitation	530.2–103
Neighbor Advertisement Spoofing	530.2–72
Neighbor Authentication	530.2–10-11
Neighbor Solicitation	530.2–103
NetFlow	530.1–141
Components	530.1–149
Exporter (configuration)	530.1–143
Template	530.1–141
V9	530.1–141-142
Network ACL	530.5–59
Network Agent	530.5–76, 81
Network Antivirus	530.3–14
Network Closets	530.1–84
.....	530.2–16
Network Control	530.2–120
Network Encryption	530.3–155-156
Issues	530.3–157
Summary	530.3–172
Network Flows	530.1–138-152
Advantages	530.1–140
Components	530.1–149
Data Sources	530.1–139
Design	530.1–152
Filtering	530.1–147-148
Planning	530.1–144
Standard (NetFlow V9) → NetFlow	
Network Key	530.4–70
Network Metadata	530.3–37
Network Sensor	530.3–81
Network Share Auditing	530.5–125
Network Storage	530.4–143
Network Tap	530.1–146
.....	530.3–27, 30-31
Network Unlock	530.4–70
Network Visibility	530.3–27, 38
Analysis	530.1–71
Public Cloud	530.4–162
Network-Centric Architecture	530.1–34
Network-Centric Defenses	530.4–6
Nftables	530.2–99
NGFW	530.3–5-22
.....	530.4–98, 121
.....	530.5–78, 80
Capabilities	530.3–6
Rule Implementation	530.3–11-12
NGFWaaS	530.2–139
NIDS	530.3–25, 66-84
NIST	530.1–38, 62
.....	530.2–97
Special Publication [X] → SP [X]	
Non-Repudiation	530.3–156

SEC530 – Defensible Security Architecture and Engineering: Implementing Zero Trust for the Hybrid Enterprise

Notification	530.2–132
NotPetya	530.1–29
Nprobe	530.1–151
NPS	530.5–70
NRO	530.2–60
NSA	530.5–8
NSE	530.2–102
NSM	530.1–146, 152
.....	530.2–66
.....	530.3–25-61, 73-74
Behavioral-Based	530.3–35
Sensor	530.3–32
Summary	530.3–85
NTA	530.3–38-39
NTFS	530.4–64, 80, 84
Ntop	530.1–149
NTP	530.2–52-56
Amplification Attack	530.2–55
.....	530.3–149
Design	530.2–53
NXLog	530.5–109, 113

O

O-ESA	530.1–53
O-ISM3	530.1–54
OAuth	530.5–76
Object Access	530.5–125
OCR	530.4–82
OODA (loop)	530.1–59
OpenSPF	530.2–164
OpenVPN	530.3–110
Operate and Monitor → DARIOM (model)	
Orangeworm	530.1–43
OSA	530.1–53
OSPF	530.2–9, 37, 94
OSquery	530.5–146
OUI	530.1–93
.....	530.5–61
Out-of-Band Visibility	530.3–27
Outbound Access	530.5–56
OWASP Top-10	530.4–12

P

PAC	530.4–111
Packet Captures	530.3–34
Packet Vacuum	530.2–66
PacketBeats	530.1–139
Packetfence	530.5–64
PAD	530.1–79
.....	530.2–18
Pafish	530.3–103
PAM	530.3–120
PAM (Linux)	530.5–23-24
Parameter Request List	530.5–63
Pass-thru Authentication	530.4–38

Passive Sniffing	530.3–167
Passive SSL/TLS Decryption	530.3–167
Password Age	530.5–28
Password Auditing	530.5–25
Password Guessing	530.3–115
Password Policy	530.5–23
Third-Party	530.5–24
Password Security	530.2–21-24
Cracking Speed	530.2–24
Password Spraying	530.3–115
Pattern Matching	530.4–81
.....	530.5–103
Payload Inspection Issues	530.3–90
PBKDF2	530.2–21-23
PCAP	530.3–33
PCI	530.1–66
.....	530.4–77
DSS	530.1–35
PDR (formula)	530.1–55
Peer-to-Peer	530.1–129
.....	530.5–69
Patching	530.1–130
Perimeter Security	530.5–5
Persistence	530.3–93
PF_RING	530.3–43, 45
PFS	530.3–167-168
PfSense Console	530.2–127
PGP Key Site	530.5–183
Phishing	530.1–34
.....	530.2–141, 160, 170
Physical Security	530.1–79
.....	530.2–16
Threats	530.1–83
PID	530.1–87
PII	530.2–125
PIM	530.2–132
Ping Sweep	530.2–101
Pivot	530.1–46, 138
.....	530.2–123
.....	530.3–32
Detection	530.3–81
Mitigation	530.1–127
PKI	530.4–64
.....	530.5–38-39
Plug and Play Monitoring	530.5–126
PMF	530.1–95-96
PMK	530.1–103
Poison PDF	530.1–34
Policy Violation	530.4–101-103
Port Authentication	530.5–61
Port Knocking	530.5–47
Port Locking	530.3–15
Port Mirroring	530.1–146
.....	530.3–27-29
.....	530.4–43
Overload	530.3–29
Virtual Switch	530.4–147
Port Scanning	530.5–71

SEC530 – Defensible Security Architecture and Engineering: Implementing Zero Trust for the Hybrid Enterprise

Port Security	530.1–113-115, 119
Post-Authentication Checks	530.3–110, 125
.....	530.5–71, 83
Powershell Remoting	530.5–146
PPP	530.2–25
PPTP	530.3–113
Pre-Master Key	530.5–36
Preferred Lifetime	530.2–91-92
Presumption of Compromise	530.1–40, 70
PRI	530.5–100
Privacy Extension Address	530.2–86, 88-90, 101
Private Botnet	530.3–116
Private Cloud	530.4–141
Summary	530.4–158
Private Port	530.1–127
Privilege Escalation	530.4–174
Privileged Identity Management	530.2–132
Process Analysis	530.3–93
Process Monitoring	530.5–126-127
Productivity Applications	530.3–132
Promiscuous Mode	530.4–146, 162
Promiscuous Port	530.1–127, 131-132
.....	530.2–123
Configuration	530.1–135
Protocol Analysis	530.3–68
Protocol Attack (DDoS)	530.3–143
Protocol Security	530.1–30
Protocol Translation	530.4–114
Protocol Visibility Analysis	530.1–72
Proxy	530.2–137-173
Application	530.2–137
Authenticated	530.2–151
Modes	530.2–148
Explicit	530.2–148-153
Transparent	530.2–148-149
SMTP	530.2–160-165, 169-170, 173
Capabilities	530.2–161
Types	530.2–138
Forward	530.2–138, 148
Reverse	530.2–138-140, 148
.....	530.3–147, 151
.....	530.4–13
Web	530.2–138, 141-148, 156-157
.....	530.3–6
Access Options	530.2–153
Alternatives	530.2–147
Capabilities	530.2–142
ProxyCannon	530.3–116
PSExec	530.1–29
PSK → WPA2-PSK	
Public Cloud	530.4–161
Due Diligence	530.4–165
Summary	530.4–168
Purple Teaming	530.1–41-42
PVLAN	530.1–127-136
.....	530.2–123
Configuration	530.1–135
Issues	530.1–129

Ports	530.1–131-132
-------------	---------------

Q

Quarantine	530.5–69
Query Log	530.4–36
QUIC	530.1–67

R

RA	530.2–111
Guard	530.2–111, 113
RADIUS	530.1–101-103
.....	530.5–60
Ransomware	530.4–53, 55
RAT	530.2–38, 41
Rate Limiting	530.2–172
RCE	530.2–26
RDNSS	530.2–95
RDP	530.3–111
RDP-SSH	530.3–109
Real-Time Detection	530.1–60
Real-Time Device Inventory	530.5–83
Recovery Agent	530.4–64
Recovery Key	530.4–64, 69
Red Herring	530.5–166
Red Teaming	530.1–66
Scenario	530.1–81-83
.....	530.2–6-7, 72
Redesign and Implement → DARIOM (model)	
Registry Key Auditing	530.5–125
Registry Key Monitoring	530.3–93
Reject Forged Transmits	530.4–145
Reject MAC Address Change	530.4–145
Remote Access	530.3–109
Applications	530.3–111
Risk Tolerance	530.3–113-114
Summary	530.3–135
Remote Desktop	530.3–113, 117, 131
Removeable Media	530.4–122
Replay Attacks	530.1–96, 105
Reputation Database	530.3–92
Resource Exhaustion Attack	530.3–146
Restore Files & Directories	530.4–53
Reverse Proxy	530.3–147, 149, 151
.....	530.5–171
→ Proxy	
Definition	530.4–13
Reverse Tunneling	530.3–111
RFC 137	530.2–16
RFC 1796	530.1–141
RFC 1918	530.2–58
.....	530.3–70
RFC 2460	530.2–79
RFC 3164	530.5–98, 102
RFC 3587	530.2–83
RFC 3954	530.1–141-142

SEC530 – Defensible Security Architecture and Engineering: Implementing Zero Trust for the Hybrid Enterprise

RFC 4191	530.2–113
RFC 4193	530.2–83-84
RFC 4380	530.2–109
RFC 4941	530.2–90
RFC 5424	530.5–98
RFC 6106	530.2–95
RFC 6113	530.4–113
RFC 6844	530.3–164
RFC 7059	530.2–107
RFC 791	530.2–77
RFID	530.1–91, 105
RIP	530.2–9
RIPE NCC	530.2–84
RIR	530.2–60, 84
Risk Analysis	530.1–66
Risk Appetite	530.1–38
.....	530.2–124
Risk Management	530.1–38
Risk Tolerance	530.4–130
Risk-Driven Architecture	530.1–38
RITA	530.3–40, 61
RMS	530.4–85
robots.txt	530.4–28
Rogue Access Point	530.1–94
Rolling Codes	530.1–105
Root CA	530.5–39-40
Router Advertisement Daemon	530.2–95
Routers (common issues)	530.2–5
ACL	530.2–126
Threats	530.2–6
Routing Protocols	530.2–9-10
RPC	530.4–149
RRDtool	530.1–150
RSA	530.1–103
Rsyslog	530.5–131
Rubber Ducky	530.1–85-86
Rule Chaining	530.5–54
Rule Implementation Suggestions	530.3–11
Rule Management	530.3–75-76
Priorities	530.3–79
Rule Staging	530.4–116

S

S4U2Self	530.4–114
SABSA	530.1–53, 65
Salted MD5	530.2–21-22
SAML	530.5–76
SAN	530.4–142-143
Sandboxing	530.3–6, 91, 95
Virtual Machines	530.3–100-101
SASE	530.2–139-140
SAT	530.5–180
Scan Storm	530.4–157
SCCM	530.4–134
.....	530.5–26
Scheduled Task	530.5–29
Screen Scraping	530.4–130

Script Collection	530.5–115-116
Scripting	530.3–21
Scrubbing	530.3–150
Scrutinizer	530.1–149
SCRYPT	530.2–21-23
SCT	530.3–163
SD-WAN	530.2–139-140
SDK	530.3–21
SDN	530.1–148
.....	530.5–78
SDP	530.2–139
.....	530.3–126
Secondary Account	530.2–131
SecRule	530.4–18-19
Secure Data Deletion	530.4–164
Secured Traffic	530.5–32
Methods	530.5–34
Summary	530.5–48
Security Architect	530.1–8
Security Architecture	530.1–6
Defensible	530.1–21-23
Life Cycle	530.1–65
Winning Mindset	530.1–79
Frameworks	530.1–53
Security Onion	530.1–144
.....	530.2–66, 105
.....	530.3–33, 41
Security Violation Counter	530.1–115
Security Zones	530.2–124
Segmentation	530.1–27, 46
.....	530.2–119-122, 152
Issue	530.2–130
Login	530.2–131
Principles	530.2–121
Segmentation Gateway	530.5–78-80, 83
Summary	530.5–86
Self-Signed Certificates	530.3–58
.....	530.4–64
SELinux	530.4–174
Sender Authentication	530.2–168
Sender Verification	530.2–163
Sensitive Data	530.3–94
.....	530.4–39, 76
AD Group	530.5–124
Preprocessor	530.4–97
Sensor Placement	530.3–32
Server Hello	530.5–36
ServerTokens	530.5–170
Service Account	530.4–38
.....	530.5–26
Special	530.5–28
Service Banner	530.5–169-172
Service Information	530.5–170-171
Session Key	530.4–70, 113
.....	530.5–36
Setfacl	530.4–56
SGID	530.4–57, 175
Sguil	530.3–82

SEC530 – Defensible Security Architecture and Engineering: Implementing Zero Trust for the Hybrid Enterprise

Shadow Copy	530.4–55	Header	530.3–69
.....	530.5–25	Options	530.3–71
Shadow IT	530.3–112	Preprocessors/Decoders	530.3–72
ShadowServer	530.2–27	SNTP	530.2–52
Shell Detection	530.3–51	SOC Report	530.4–165
Shiny Object Syndrome	530.1–36	SOC Zones	530.1–48
SIEM	530.1–123, 145	Social Engineering	530.1–85
.....	530.2–19	SOCKS	530.2–137
.....	530.3–38, 40	Software Change Detection	530.3–51
.....	530.5–83	Software-Based Flow Logs	530.1–146, 148
Components	530.5–90	Software-Defined Perimeter	530.2–139
Integration	530.3–83	SoH	530.5–70–71
.....	530.4–47	SOHO	530.1–100
Rules	530.5–142	530.2–37, 100
Summary	530.5–118	530.3–28
What Is It Used For?	530.5–89	SolarWinds	530.1–149
SIGINT	530.1–140	Breach	530.5–8
Sigma	530.5–148–150, 160–161	SOX	530.1–66
Rule Format	530.5–152–156	SP 800-119	530.2–97, 115
ElasticSearch Query Conversion	530.5–159	SP 800-141	530.2–122
Splunk Query Conversion	530.5–157	SP 800-207	530.1–62
Supported Outputs	530.5–151	530.5–8
Signature	530.5–143	SP 800-53	530.1–38
Categories	530.3–67	SP 800-63B	530.5–20–21
Signature-Based Detection	530.3–67	SP 800-88	530.4–164
Evasion	530.3–90	SPA	530.5–34, 46–47
Simple Packet Authorization → SPA		Spam Appliance	530.2–160
Sinkholing	530.3–112	SPAN	530.3–28
Site Categories	530.2–144–145	Special Guest	530.1–97
SLAAC	530.2–85–88, 95, 101	Spectre	530.4–163
Attack	530.2–72	SPF	530.2–163–164, 167–168
Privacy	530.2–88	Split Tunneling (VPN)	530.3–121
SLIP	530.2–25	Spoofed Router Advertisement	530.2–103, 113
Slowloris	530.3–146	Spoofing Attacks	530.1–96
Smart Card	530.5–40–41	SQLi Detection	530.3–52
Smart Install	530.2–26	Squert	530.3–82
SMB	530.1–29	SquidGuard	530.2–155
.....	530.2–130	SSDP	530.2–94
.....	530.5–56	SSH	530.2–16
Smurf Attack	530.2–6	530.3–109
SNMP	530.2–18, 45	530.5–71
Attack	530.2–46–48	Inspection	530.3–6, 13
Community Strings	530.2–34, 45, 49	SSID	530.1–94
Wordlist	530.2–46	SSL	530.3–58–59
Hardening	530.2–49	Certificate Analysis	530.2–143
Trap	530.1–115	Certificate Validation	530.3–51
.....	530.2–19	Decrypt Mirroring	530.3–170–171
.....	530.5–67, 97	Inspection	530.2–143, 154
V2c	530.2–49	530.3–6, 13, 169
V3	530.2–34, 49	Offloading	530.4–14
.....	530.5–71	Spoofing	530.4–130
Levels of Access	530.2–50	SSL Labs (Qualys)	530.3–166
Recommendations	530.2–37	SSL Termination	530.3–117
Snort	530.1–144	SSL/TLS Passive Decryption	530.3–167
.....	530.3–33, 68	SSO	530.3–134
Rules	530.2–108–109	530.4–38
.....	530.3–69–73, 75	530.5–76
Flowbits	530.3–77	SSRS	530.4–38, 45

SEC530 – Defensible Security Architecture and Engineering: Implementing Zero Trust for the Hybrid Enterprise

Standalone CA	530.5–40
Statement of Health → SoH	
Station Isolation	530.1–98-100, 127
Sticky Bit	530.4–57
Sticky MAC Address	530.1–113, 115
STIG	530.2–28, 32-34
Storage Network	530.4–142
Stored Procedure	530.5–182
Stratum (NTP)	530.2–54
Subordinate CA	530.5–39
SUID	530.4–57, 175
Suricata	530.1–139, 144, 146-147
.....	530.3–33, 40, 60, 84
SWG	530.2–140
Switched Port ANalyzer → SPAN	
Switches (common issues)	530.1–107
Logs	530.1–123
Threats	530.1–108
SYN Cookie	530.3–144-145
SYN Flood	530.3–143
Protection	530.3–144
SYN Sequence Number	530.3–145
Syslog	530.1–123
.....	530.2–19
.....	530.5–97-102, 130
Agent 🧑	530.5–131
Agent 🏠	530.5–109
Configuration	530.5–131
Example	530.5–132-133
Devices	530.5–99
Drawback	530.5–103
Example	530.5–100
Message Limitations	530.5–102
Syslog-NG	530.5–131
Syslogd	530.5–131
Sysmon 🏠	530.1–139
.....	530.3–38
Capabilities	530.5–127
Configuration	530.5–129
Example	530.5–128
System & Organization Controls → SOC Report	
System Call Monitoring	530.5–136

T

T-Pot	530.5–176
Take Ownership	530.4–53
TBS	530.1–55-56, 59
TCO	530.1–32
TCP Flooding	530.3–141
TCP/3389	530.3–111
TCP/445	530.2–130
TCP/465	530.3–15
TCP/4786	530.2–26-27
TCP/514	530.5–98, 133
TCP/5985	530.2–130
TCP/993	530.3–15
TCP/995	530.3–15

Team Cymru	530.2–58-61, 65
TeamViewer	530.3–113
Teensy Attack	530.1–86
Telnet	530.2–16
Temporal Anomaly	530.5–85
Temporary Address	530.2–87-88, 91-92
Lifetime	530.2–91-92
Teredo	530.2–107, 109
Terms and Conditions	530.1–97
.....	530.2–147, 156
.....	530.5–68
Threat Actor	530.1–43, 45
Threat Hunting	530.1–40
.....	530.5–144, 162
Threat Modeling	530.1–41, 45, 66
Threat-Focused Models	530.1–54
Threats	530.1–83, 108
Tiering Firewall	530.5–78
Tiers	530.2–125
TIFF	530.4–82
Time Restrictions	530.2–132
Time-Based Security → TBS	
TLS	530.3–58-60
.....	530.5–34, 41
TOGAF	530.1–53
Tokens	530.3–119
TOTP	530.3–119
TPM	530.4–65, 69-70
Traceroute Detection	530.3–51
Traditional Communication	530.5–33
Traffic Analysis	530.1–140
Traffic Mirroring	530.4–145, 162
Trigger Log	530.4–36
Tripwire	530.5–184
Trust Calculation	530.5–81
Trust Over Time	530.5–14
Trusted Certificate Authority	530.2–143
.....	530.3–169
Trusted Interfaces	530.1–123
TTL	530.2–77
TTP	530.1–42, 44
Two-Legged FW Ruleset (example)	530.2–129
Tyrell Corporation (case study)	530.1–28, 136
.....	530.2–134, 158
.....	530.3–3, 23, 62, 86, 107, 136, 153, 173, 176-177
.....	530.4–9, 31, 49, 73, 91, 105, 139, 159, 183-184
.....	530.5–18, 49, 93

U

U2F	530.3–119
UDP Flooding	530.3–141
UDP/123	530.2–52
UDP/3544	530.2–109-110
UDP/514	530.5–98, 132
UEFI	530.4–70
UFW	530.5–53
ULA → Unique Local Address	

SEC530 – Defensible Security Architecture and Engineering: Implementing Zero Trust for the Hybrid Enterprise

Unauthenticated VLAN	530.5–60
Unauthorized Access Point	530.1–93
Unauthorized Asset	530.3–37
Unauthorized Change	530.5–124
Unauthorized Router Advertisement	530.2–111–112
Mitigation	530.2–111
Unauthorized Routing Update	530.2–10
Unauthorized Tunnel	530.2–12
Unique Local Address (fd00)	530.2–82, 93
Unknown Unknowns	530.1–67
Untrusted Interfaces	530.1–123
Unused Port	530.1–114
Unused Services	530.2–18
Update-FrmClassificationPropertyDefinition	530.4–79
Uplink Port	530.1–127
URL Filtering	530.3–6–7, 11
USB Keyboard Attack	530.1–86–87
User Certificate	530.5–41
User Claim	530.4–111, 114, 117
User Context Awareness	530.4–45
User-Agent	530.5–173

V

Valid Lifetime	530.2–91–92
Variable Trust	530.5–13, 89
Varnish	530.3–147
VDI	530.3–131
Veil Framework	530.3–99
VeraCrypt	530.4–67
VID	530.1–87
View (DB)	530.4–37
Vigenere Cipher	530.2–21
Virtual Desktop Infrastructure → VDI	
Virtual Patching	530.4–15, 24–25
Virtual Sensor	530.4–147
Virtual Switch Security	530.4–145
Virtual Tap	530.4–147, 162
VirtualBox	530.3–132
Visibility	530.1–60
.....	530.3–27
Virtual Network	530.4–146
VLAN	530.1–27, 46, 127
Disabled	530.1–88
Primary/Secondary	530.1–133, 135
Private → PVLAN	
VM Escape	530.3–132
.....	530.4–149, 156
VM Identification	530.3–103
VM Interaction	530.4–155
VM Masking	530.3–104
VM Migration	530.4–144
VM to VM Traffic	530.4–147
VM Tools	530.4–156
VMCloak	530.3–104
VMWare Endpoint Security	530.4–157
VMWare vCenter	530.4–151
VMWare Workstation	530.3–132

VNC	530.3–117
Volume Master Key	530.4–69
Volume Shadow Copy Service → VSS	
Volumetric Attack (DDoS)	530.3–141–142
VPC	530.1–139, 145
Traffic Mirroring	530.4–162
VPN	530.2–139, 153
.....	530.3–109
Always On	530.3–122–124
Full Tunnel	530.3–121
Split Tunnel	530.3–121
TLS-Based	530.3–110
VSS	530.4–55
VTP	530.1–133–134
Transparent Mode	530.1–134
VTY	530.2–17, 19
Vulnerability Identification	530.3–25
Vulnerability Scan	530.5–61, 71
Vulnerable Software Detection	530.3–51

W

WAF	530.2–138, 148
.....	530.3–147, 151
Allow List	530.4–22
Capabilities	530.4–15
Centralized Protection	530.4–23
Challenges	530.4–17
Content Routing	530.4–27
Definition	530.4–11
Deployment	530.4–21
Detection	530.4–29
Evasion	530.4–18
Focus	530.4–12
Key Advantage	530.4–23
Management Platform	530.4–153
Normalization	530.4–19
Protocols Support	530.4–20
Summary	530.4–30
WAN Optimization	530.3–122–123
WarBerryPi	530.1–85
Watering Hole	530.2–141
WDS	530.4–70
Weak Password	530.5–21, 23–24
Web Proxy → Proxy	
Web Vulnerability Scanner	530.4–24
.....	530.5–171
WebLabyrinth	530.4–28
Website Allow List	530.2–146
WebSockets	530.4–20
WFAS	530.5–53
Whitecap Rules	530.3–80
WHOIS	530.5–92
Whois Creation Data Lookup	530.3–37
WiFi (4/5/6)	530.1–95
WinAuth	530.3–120
Windows 10	530.1–129–130
Windows Always On VPN	530.3–124

SEC530 – Defensible Security Architecture and Engineering: Implementing Zero Trust for the Hybrid Enterprise

Windows Auditing	530.4–54
Windows Authorization Manager	530.5–124
Windows Defender Firewall	530.5–53
Windows Event	530.5–104
Collector	530.5–111
Forwarding	530.5–110, 146
Log	530.5–102
Example	530.5–105–106
Viewer	530.5–104, 111
Windows Firewall	530.5–44
Windows Hyper-V	530.4–151
Windows Permissions & Rights	530.4–52
Windows Remote Management	530.5–110
Windows Sysinternals	530.4–80
.....	530.5–127
Windows Task Scheduler	530.5–111
Windows Update → Microsoft Update	
Wine	530.3–103
WinRM	530.2–130
WIP	530.4–134
WIPS	530.1–93–94
Wireless	530.1–91
Risk	530.1–92
Witty (worm)	530.2–65
WMI	530.5–71
WMIC	530.1–29
Working Hours	530.4–119
Wormhole Attack	530.2–12–13
Mitigation	530.2–12
WPA2 Personal/Enterprise	530.1–101
WPA2-PSK	530.1–97, 101
WPA3 Enterprise	530.1–102–103

X

X-Forwarded-For	530.2–141
X-Powered-By	530.5–171
X.25	530.1–79
X.509	530.3–56, 163
.....	530.5–61
XFF	530.2–141

Y

YAML	530.5–152
YARA	530.3–100
.....	530.5–148

Z

Z-Wave	530.1–91
Zeek	530.1–139
.....	530.2–105
.....	530.3–33, 35–61, 40
Architecture	530.3–43–45
Bad Checksums	530.3–49
CLI	530.3–49
Configuration	530.3–46–48
Docker	530.3–55
File Extraction	530.3–98
Logs	530.3–36, 165
.....	530.4–47
Scripting	530.3–50–54
Use Cases	530.3–56–61
Zero Trust	530.5–6–7
Credentials	530.5–20
Mandates	530.5–12
Model	530.1–62–63
Need	530.5–5
Pillars & Capabilities	530.5–10–11
Roadmap	530.5–16
Scenario	530.5–15
Summary	530.5–17
Zero Trust Model	530.2–139–140
Zeus	530.3–56
Zigbee	530.1–91, 104
Zoning	530.1–48
.....	530.2–121, 123–124
ZTNA	530.2–139–140
.....	530.3–126