

# SANS SEC566 – Implementing & Auditing CSC In Depth

---

## Topics

## Categories

**Background & Philosophy of CSC** .... 566.1–5-45

**Auditing Principles & Philosophies** .. 566.1–46-61

### Critical Security Controls

- #1 Inventory of (Un)Authorized Devices  
566.1–62-89
- #2 Inventory of (Un)Authorized Software  
566.1–90-115
- #3 Secure Configurations for HW & SW  
566.2–3-30
- #4 Cont Vulnerability Assessment & Remediation  
566.2–31-55
- #5 Controlled Use of Admin Privileges  
566.2–56-82
- #6 Maint, Monitoring & Analysis of Audit Logs  
566.2–83-112
- #7 Email & Web Browser Protection  
566.3–3-28
- #8 Malware Defenses  
566.3–29-50
- #9 Limitation & Control of Network Ports  
566.3–51-73
- #10 Data Recovery Capability  
566.3–74-91
- #11 Secure Config for Network Devices  
566.3–92-121
- #12 Boundary Defense  
566.4–3-31
- #13 Data Protection  
566.4–32-61
- #14 Controlled Access Based on Need-to-Know  
566.4–62-84
- #15 Wireless Access Control  
566.4–85-111
- #16 Account Monitoring & Control  
566.5–3-28
- #17 Security Skills Assessment & Training  
566.5–29-47
- #18 Application Software Security  
566.5–48-72
- #19 Incident Response & Management  
566.5–73-92
- #20 Penetration Tests & Red Team Exercises  
566.5–93-115

**Conclusion & Next Steps** ..... 566.5–116-141

**CIS for Effective Cyber Defense v6.1** . 566.6–1-92

**NIST SP 800-53 Rev 4 – Recommended  
Security Controls** ..... 566.7–1-462

**NIST SP 800-53A Rev 4 – Guide for Assessing  
Security Controls** ..... 566.8–1-487

### Baselines for Automation

- #1-2 ..... 566.1–71, 98
- #3-6 ..... 566.2–12, 42, 67, 93
- #7-11 ..... 566.3–12, 38, 59, 81, 101
- #12-15 ..... 566.4–13, 42, 71, 95
- #16-20 ..... 566.5–14, 37, 57, 81, 102

### Breach Case Studies

- Barracuda ..... 566.2–62
- Carbon Black (Bit9) ..... 566.1–66
- ClixSense ..... 566.1–10
- Community Health Systems ..... 566.3–96
- DBIR (Verizon) ..... 566.1–9
- Disney Consumer Products ..... 566.1–10
- eHarmony ..... 566.2–6
- Elex / Clash of Kings ..... 566.1–10
- Facebook ..... 566.1–94
- Foursquare ..... 566.1–10
- Google ..... 566.2–35
- LexisNexis ..... 566.2–88
- LinkedIn ..... 566.2–6
- Lockheed Martin (F-35) ..... 566.4–6
- Los Angeles Times ..... 566.5–32
- MySpace ..... 566.1–10
- New York Times ..... 566.4–66
- PFC Manning ..... 566.4–36
- RSA ..... 566.3–33
- Snapchat ..... 566.5–52
- Sony ..... 566.5–76
- State of South Carolina ..... 566.5–6
- TJX ..... 566.4–89
- Ubiquiti ..... 566.3–6
- Virginia.gov ..... 566.3–77
- vTech Learning Lodge ..... 566.3–55
- Weebly ..... 566.1–10
- WikiLeaks ..... 566.4–36
- WSJ ..... 566.4–66
- Yahoo ..... 566.1–10

### Defenses

- #1-2 ..... 566.1–67-69, 95-96
- #3-6 ..... 566.2–7-10, 36-40, 63-65, 89-91
- #7-11 ..... 566.3–7-10, 34-36, 56-57, 78-79, 97-99
- #12-15 ..... 566.4–7-11, 37-40, 67-69, 90-93
- #16-20 .... 566.5–7-12, 33-35, 53-55, 77-79, 97-100

### Entity Relationship Diagrams

- #1-2 ..... 566.1–72, 99
- #3-6 ..... 566.2–13, 43, 68, 94
- #7-11 ..... 566.3–13, 39, 60, 82, 102
- #12-15 ..... 566.4–14, 43, 72, 96
- #16-20 ..... 566.5–15, 38, 58, 82, 103

### Evaluation & Testing

- #1-2 ..... 566.1–79-82, 106-108
- #3-6 ..... 566.2–19-22, 48-50, 73-76, 99-102
- #7-11 ... 566.3–18-20, 44-46, 65-67, 86-90, 107-110

# SANS SEC566 – Implementing & Auditing CSC In Depth

---

#12-15 ..... 566.4–20-24, 49-53, 77-79, 101-104  
#16-20 . 566.5–20-22, 41-45, 65-67, 85-90, 108-113

## Labs

Lab Setup Instructions ..... 566.1–E2  
Performing Gap Analysis w/ AuditScripts Scoring  
Tool.....566.1–E3  
#1 Automating Device Inventory w/ Nmap &  
Ndiff.....566.1–E4  
#2 Whitelisting w/ AppLocker.....566.1–E5  
#3 Linux Config Analysis w/ Lynis .. . 566.2–E2  
#4 Vulnerability Mgt w/ OpenVAS .. . 566.2–E3  
#7 Phishing Campaigns w/ GoPhish... 566.3–E2  
#9 Parsing Nmap Output w/ PowerShell 566.3–E3  
#11 Network Device Configuration Analysis w/  
Nipper.....566.3–E4  
#12 Traffic Analysis w/ Wireshark.....566.4–E2  
#13 Encrypting Files w/ VeraCrypt .. . 566.4–E3  
#15 WiFi Analysis w/ NetSpot .... . 566.4–E4  
#16 Analyzing User Accounts w/ PowerShell &  
WMI..... 566.5–E2  
Writing a Personal Action Plan.....566.5–E3

## Minimum Control Sensors

#1-2 ..... 566.1–70, 97  
#3-6 ..... 566.2–11, 41, 66, 92  
#7-11 ..... 566.3–11, 37, 58, 80, 100  
#12-15 ..... 566.4–12, 41, 70, 94  
#16-20 ..... 566.5–13, 36, 56, 80, 101

## Root Cause Analysis

#1-2 ..... 566.1–83-86, 109-111  
#3-6 ..... 566.2–23-27, 51-52, 77-80, 103-109  
#7-9,11 ..... 566.3–21-25, 47-49, 68-70, 111-117  
#12-15 ..... 566.4–25-28, 54-59, 80-81, 105-107  
#16,18 ..... 566.5–23-25, 68-70

## Sample Automation Scripts

#1 Nmap & Ndiff ..... 566.1–78  
#2 WMIC 🌐 ..... 566.1–105  
#3 Lynis 🌐 ..... 566.2–18  
#4 MBSACLI 🌐 ..... 566.2–47  
#5 WMIC 🌐 ..... 566.2–72  
#6 PowerShell 🌐 (Get-Eventlog) ..... 566.2–98  
#7 LogParser 🌐 ..... 566.3–17  
#8 ClamScan ..... 566.3–43  
#9 Nmap ..... 566.3–64  
#11 Nipper 🌐 ..... 566.3–106  
#12 Tshark ..... 566.4–19  
#13 Ngrep 🌐 ..... 566.4–19  
#14 PowerShell 🌐 (Get-ACL) ..... 566.4–76  
#15 OpenVAS ..... 566.4–100  
#16 PowerShell 🌐 (Get-WMIObject) ... 566.5–19  
#18 W3AF ..... 566.5–62-64

## Standard Mappings

#1-2 ..... 566.1–87-88, 112-113  
#3-6 ..... 566.2–28-29, 53-54, 81-82, 110-111  
#7-11 ..... 566.3–26-27, 50, 71-72, 91, 118-119

#12-15 ..... 566.4–29-30, 60-61, 82-83, 108-109  
#16-20 . 566.5–26-27, 46-47, 71-72, 91-92, 114-115

## Tools

Access Auditor ..... 566.5–17, 566.2–70  
AccessEnum ..... 566.4–73, 75  
Active Directory 🌐 ..... 566.1–36  
..... 566.2–70  
..... 566.4–74  
Certificate Services ..... 566.1–76  
Group Policies ..... 566.2–16  
AD Audit Plus ..... 566.5–16-17  
AD Reports ..... 566.5–17  
ADSI Queries ..... 566.5–18  
Aircrack ..... 566.4–88  
Akamai Kona ..... 566.5–60  
Amanda ..... 566.3–85  
Application Security Manager ..... 566.5–60  
AppLocker 🌐 ..... 566.1–E5, 104  
AppScan ..... 566.5–59-60  
APT1 Recon Batch ..... 566.4–65  
Areca ..... 566.3–85  
Armitage 🌐 ..... 566.1–65  
..... 566.5–107  
AuditScripts Scoring Tool ..... 566.1–E3  
Aveska IAM ..... 566.4–73  
BackupExec ..... 566.3–84  
Bacula ..... 566.3–85  
BeEF ..... 566.5–51  
BET ..... 566.1–93  
Blackhole Exploit Toolkit ..... 566.1–93  
BLAST ..... 566.5–61  
BlueCoat URL Filtering ..... 566.3–15  
Bro IDS ..... 566.4–18  
CACE AirPcap TX/Pilot ..... 566.4–98  
CACE Pilot ..... 566.4–97  
CANVAS ..... 566.5–106  
Casper ..... 566.2–16  
Cat 🌐 ..... 566.2–71  
..... 566.5–18  
CB Protect ..... 566.1–103  
Cenzic Enterprise ..... 566.5–60  
Change Auditor ..... 566.2–70  
..... 566.5–17  
Chef Server ..... 566.2–16  
CIS-CAT ..... 566.2–16  
Cisco Adaptive Security Appliance ..... 566.4–17  
Cisco Firepower Firewall ..... 566.4–17  
Cisco Prime ..... 566.3–104  
..... 566.4–74  
ClamAV ..... 566.3–42-43  
Clear Pass ..... 566.1–76  
Clonezilla ..... 566.3–85  
CloudFlare Enterprise ..... 566.5–60  
Cobalt Strike ..... 566.5–106  
Code Advisor ..... 566.5–60  
Code Green TrueDLP ..... 566.4–46  
Compete Security Suite ..... 566.3–41

# SANS SEC566 – Implementing & Auditing CSC In Depth

---

Configuration Manager .....	566.2–16	LAPS 	566.2–71
Control Now GFI MailEssentials .....	566.3–15	LASSIE .....	566.2–97
Core Impact Pro .....	566.5–106	Log Correlation Engine .....	566.2–96
CounterAct .....	566.1–76	LogParser 	566.2–97
Courion AAS .....	566.4–73	.....	566.3–16–17
Cryptograph .....	566.3–83	Logstash .....	566.2–97
CSI .....	566.1–103	Lsof 	566.3–63
CSVDE .....	566.5–18	Lurker .....	566.2–78
DansGuardian .....	566.3–16	Lynis 	566.1–104
Data Protector .....	566.3–84	.....	566.2–E2, 17–18
Diff 	566.2–71	MailScanner .....	566.3–16
ELK .....	566.2–97	MBSA 	566.2–17, 47
Enclave DAD .....	566.2–97	McAfee DLP .....	566.4–46
Enterprise Security for Endpoints .....	566.3–41	McAfee Endpoint Protection .....	566.3–41
Enterprise Security Manager ..	566.4–16, 566.2–96	McAfee ePolicy Orchestrator .....	566.3–40
Event Correlation .....	566.2–96	Meraki .....	566.4–98
Event Data Warehouse .....	566.2–96	Metasploit 	566.1–65
EX Email Security .....	566.3–15	.....	566.2–34, 108
FindBugs .....	566.5–61	.....	566.5–105–107
FireEye Network IPS .....	566.4–17	Microsoft Windows Advanced Firewall 	566.3–63
FireFlow .....	566.3–104	Mimikatz .....	566.2–61
FireMon .....	566.3–104	Moloch .....	566.4–18
FirePAC .....	566.3–104	Ndiff .....	566.1–E4
Firewall Analyzer .....	566.3–104	.....	566.2–107
Firewall Assurance .....	566.3–104	Nemesis .....	566.4–47
ForcePoint .....	566.3–14–15	Nessus .....	566.1–36
Forefront 	566.3–41	.....	566.2–45
Fortify 360 .....	566.5–60	.....	566.3–62
Fortinet Fortigate .....	566.4–17, 46	NetBackup .....	566.3–84
FxCop .....	566.5–61	NetBrain .....	566.3–62
Google Apps Email Filtering .....	566.3–15	Netcat .....	566.2–107, 109
GoPhish .....	566.3–E2	NetFlow Analyzer .....	566.4–45
Graylog .....	566.2–97	NetSpot .....	566.4–E4, 99
HEAT .....	566.1–103	Netstat .....	566.3–63
HiveOS .....	566.4–98	NetVault .....	566.3–84
Hping .....	566.4–47	Network Advisor .....	566.3–104
HTTPtunnel .....	566.4–5	Network Configuration Manager .....	566.3–104
Identity IQ .....	566.4–74	.....	566.4–74
InSSIDer .....	566.4–99	Network Instruments Observer .....	566.4–46
Invincea .....	566.3–15	Network Miner .....	566.4–18
IP360 .....	566.2–45	Network Storage Server .....	566.3–84
.....	566.3–62	Network Topology Mapper 	566.1–75
Ipchains .....	566.3–63	NEWT Professional .....	566.1–101, 103
iPost .....	566.1–32–36	.....	566.3–111
Iptables 	566.3–63	NeXpose .....	566.2–45
IronPort WSA/ESA .....	566.3–15	.....	566.3–62
ISE .....	566.1–76	Next Generation Firewall .....	566.4–17
Jamf Pro .....	566.2–16	Ngrep .....	566.4–47–48
John the Ripper .....	566.2–5	Nipper .....	566.3–E4, 103, 105–106
Juniper Netscreen Firewall .....	566.4–17	Nipper Studio 	566.3–104
Kali 	566.5–107	NitroSecurity .....	566.4–16
KeyPass .....	566.3–111	Nmap .....	566.1–E4, 77–78
Kismet .....	566.4–99	.....	566.2–106–108
Kiwi Syslog Generator .....	566.2–109	.....	566.3–63–64
KiwiCatTools .....	566.3–105	.....	566.4–99
LANSurveyor .....	566.1–76	Script Engine .....	566.2–46
.....	566.3–111	Okta Online SSO .....	566.4–73
LANsweeper .....	566.1–76, 103	OneLogin Online SSO .....	566.4–73


# SANS SEC566 – Implementing & Auditing CSC In Depth

---

Open Log Management .....	566.2–96	Security Blanket .....	566.2–17
OpenDLP .....	566.4–47	Security Onion .....	566.4–18
OpenDNS .....	566.3–15	Security Policy Orchestration Solution .	566.3–104
OpenNAC .....	566.1–77	SET .....	566.3–5
OpenVAS .....	566.2–E3, 44, 46	ShareEnum .....	566.4–75
.....	566.3–63	SIEM Correlation Server .....	566.2–96
.....	566.4–99–100	Simpana .....	566.3–84
OpenWRT .....	566.4–99	Skybox Secure Solution .....	566.2–45
OSCS Inventory 🍷 .....	566.1–104	.....	566.3–62
OSSIM .....	566.1–77	Snort .....	566.4–18
Ounce Labs Core .....	566.5–59–60	SourceFire IPS .....	566.4–17
OWASP Live CD .....	566.2–79	Spiceworks .....	566.1–77, 104
PacketFence .....	566.1–77	Splunk .....	566.2–95–96
Palo Alto Networks Firewall .....	566.4–17	Sqlmap .....	566.3–54
Palo Alto Networks URL Filtering .....	566.3–15	Squid .....	566.3–16
Paros .....	566.5–61	SRR Lite .....	566.2–26
PhlashDance .....	566.3–95	StealthWatch .....	566.4–17
Poison Ivy RAT .....	566.3–32	Subterfuge MitM .....	566.5–5
PowerBroker .....	566.2–70	Sudo 🐼 .....	566.2–71
PowerShell 🍷 .....	566.1–104	Symantec DLP .....	566.4–46
.....	566.2–17, 71, 87, 97–98	Symantec Endpoint Protection .....	566.3–41
.....	566.3–E3	Syslog Sender .....	566.2–109
.....	566.4–75–76	Syslog-NG .....	566.2–97
.....	566.5–E2, 18–19	Tablus DLP .....	566.4–46
Privilege Guard .....	566.1–103	Tanium Endpoint Security .....	566.3–41
.....	566.2–70	TCPDump .....	566.4–18, 47
Privileged Account Security Solution ....	566.2–70	Tripwire .....	566.1–103
Privileged Password Manager .....	566.2–70	.....	566.2–14, 16, 70
Process Explorer 🍷 .....	566.3–63	.....	566.3–104
Process Hacker 🍷 .....	566.3–61–62	.....	566.4–74
ProofPoint Email Filtering .....	566.3–15	Triumphant Endpoint Security .....	566.3–41
Protect .....	566.3–41	True Image .....	566.3–84
Puppet .....	566.2–16	Trusted Access .....	566.5–17
Qradar .....	566.2–96	Tshark .....	566.4–18–19, 47
QualysGuard .....	566.2–15, 45	Unified Security Management .....	566.2–96
.....	566.3–62	USB-Rubber-Ducky .....	566.4–35
RadialNet .....	566.2–107	Veeam Backup & Replication .....	566.3–84
RANCID .....	566.3–105	VeraCrypt .....	566.4–E3, 566.4–75
Redo .....	566.3–85	ViewFinity .....	566.1–103
Retina .....	566.2–45	Vontu DLP .....	566.4–46
.....	566.3–62	vSentry .....	566.3–41
RF Protect .....	566.4–98	W3AF .....	566.5–62–64
RouterSploit 🍷 .....	566.3–95	WebInspect .....	566.5–60
RSA Archer .....	566.5–84	WebScarab .....	566.5–61
RSA DLP .....	566.4–46	WebSense Triton .....	566.3–14–15
SAINT .....	566.2–45	WiFi Analyzer .....	566.4–98
.....	566.3–62	Wikto .....	566.5–61
Saint Security Suite .....	566.5–106	Wireless IPS .....	566.4–98
Scapy .....	566.4–47	Wireshark .....	566.4–E2, 18, 47
SCC Access Auditor .....	566.2–69	WMIC 🍷 .....	566.1–104–105
SCCM 🍷 .....	566.1–36, 76, 103	.....	566.2–17, 71–72
.....	566.2–70	.....	566.5–E2, 18
.....	566.3–41	xDSCResourceDesigner .....	566.2–17
.....	566.4–74	Yubikey .....	566.5–17
.....	566.5–17	Zenmap .....	566.1–75
SecureFusion .....	566.2–45	Zone Defense .....	566.4–98
.....	566.3–62		
SecureID .....	566.5–17		

# SANS SEC566 – Implementing & Auditing CSC In Depth

## A

AAA .....	566.3–114
.....	566.4–20
Access Control Policy .....	566.4–25
Access Point .....	566.4–102
Account → CSC #5,16 .....	
Account Housekeeping .....	566.5–24
Account Lockout .....	566.5–9
ACE .....	566.3–114
ACL .....	566.3–108
.....	566.4–68
Active Scanner .....	566.1–99, 106
.....	566.2–14
.....	566.3–60
Active Tools .....	566.1–67
ActiveX .....	566.3–8
Administrative Access .....	566.2–68
Administrative Privileges .....	566.2–58, 63
Administrative Tasks .....	566.2–65
.....	566.3–99
Administrator .....	566.2–58
AES .....	566.4–92, 105
Aggressive Scan .....	566.2–108
Air-gapped Systems .....	566.1–96
.....	566.4–36
AirPCap .....	566.4–97
Alert Signatures .....	566.2–93
Alert System .....	566.1–100, 106
Anomaly Reports .....	566.2–107
Anti-Malware .....	566.3–34, 36–37
Policy .....	566.3–47
Application Audit .....	566.1–86
Application Firewall .....	566.3–57–58
.....	566.5–53
Application Proxy .....	566.4–15
Application Security → CSC #18 .....	
Application Whitelisting .....	566.1–95
.....	566.3–7
AppLocker  .....	566.1–95
Approved Software Application Inventory .....	566.1–98
APT .....	566.4–65
Archived Data .....	566.4–69
ARF .....	566.1–31
ASLR .....	566.3–35
Asset Inventory .....	566.1–67–68, 71
.....	566.3–81
.....	566.4–42, 71
System .....	566.1–70
Asset Management Database .....	566.1–85
Attack Lifecycle Model (Mandiant) .....	566.1–11
Attack Mitigation Scores (NSA) .....	566.1–20
Attacker Activities .....	566.1–15
Audit .....	566.1–48–50
Audit Interview Technique .....	566.2–77
Audit Log .....	566.2–85
Audit Logistics .....	566.3–117
Audit Trail .....	566.4–26
Australian Top 35 Mitigation Strategies ..	566.1–37–38

Authentication System .....	566.2–66, 68
.....	566.3–100
.....	566.4–12
Authorized Devices .....	566.1–64
Authorized Software .....	566.1–92, 95
Awareness Websites .....	566.5–40

## B

B2B .....	566.3–115
Back Channel .....	566.4–10, 28
Back-out Procedure .....	566.1–111
Backdoor .....	566.4–28
Backup .....	566.3–78–80, 82
→ CSC #10 .....	
Media Encryption .....	566.3–89
Banner .....	566.4–25
BioMeasures .....	566.2–64
Bluetooth .....	566.4–87, 105
Botnet .....	566.2–19, 88
Boundary → CSC #12 .....	
Browser Configuration .....	566.3–9
Business Continuity .....	566.3–87
BYOD .....	566.4–93

## C

Cain & Abel .....	566.4–97
CAPEC .....	566.1–19
CCE / CPE / CVE .....	566.1–31
.....	566.2–36
CCSS / CMSS / CVSS .....	566.1–31
.....	566.2–36
CEO Fraud .....	566.3–6
CERT .....	566.5–83
Change Management .....	566.1–85
.....	566.3–116
Checklist .....	566.2–26, 109
.....	566.3–65
CIP .....	566.1–51
Cisco Works .....	566.3–70
CISecurity .....	566.1–12
Claim .....	566.4–68
Classification → CSC #14 .....	
Classification Level .....	566.4–67
Classification Policy .....	566.1–110
Cleanup Cost .....	566.4–20
CNCI .....	566.1–6
COBIT .....	566.1–25
Code Analysis Tool .....	566.5–65
Command Injection .....	566.5–69
Conficker .....	566.2–48
Configuration Baseline .....	566.2–11
.....	566.3–60, 101
→ CSC #3 .....	
Configuration Management .....	566.1–85
.....	566.2–7
Consensus Audit Guidelines .....	566.2–79

# SANS SEC566 – Implementing & Auditing CSC In Depth

---

Controllers of Data .....	566.4–54
Core Evaluation Tests .....	566.1–53-54
Council on CyberSecurity .....	566.1–12
Critical Governance Controls .....	566.1–24
Critical Security Controls .....	566.1–6, 12, 22
Contributors .....	566.1–13-14
Course Outline per Control .....	566.1–59-60
Documents .....	566.1–26
Families .....	566.1–20
Focus .....	566.1–28
Philosophy 🍷 .....	566.1–17
Principles .....	566.1–16-18
CryptoLocker .....	566.3–79

## D

Data at Endpoints .....	566.4–56
Data at Rest .....	566.4–56, 69
Data Classification .....	566.4–71
Data Exfiltration .....	566.4–36
Data in Motion .....	566.4–56
Data Leakage .....	566.4–34
Protection .....	566.4–54
Sources .....	566.4–56
Data Plane .....	566.4–28
Data Protection Strategy .....	566.4–59
Data Recovery .....	566.3–76, 87
.....	566.4–34
→ CSC #10 .....	.....
DBIR .....	566.1–9
Dedicated Administration System .....	566.2–66
.....	566.3–100
Default Passwords .....	566.2–63
Defense-in-Depth .....	566.3–48
.....	566.4–15
Defenses .....	566.1–15
DEP .....	566.3–35
Development Artifact .....	566.5–55
Device ACL & Authorization .....	566.3–113
Device Discovery System .....	566.1–70
Devices → CSC #1 .....	.....
DHCP .....	566.1–67
DIACAP .....	566.1–51
DIDS .....	566.4–27
Directory Traversal .....	566.5–69
Disaster Recovery .....	566.3–87
Disk Imaging .....	566.2–19
DLP .....	566.4–34
→ CSC #13 .....	.....
Host-Based .....	566.4–40-41, 70
Network-Based .....	566.4–39, 41
DMZ .....	566.4–10, 27-28
DNS .....	566.2–104
.....	566.3–36, 57
Domain Administrators .....	566.2–64
Dormant Account .....	566.5–8
DoS .....	566.4–28
Driver Signing .....	566.1–111

Duty to Take Special Care .....	566.4–57
---------------------------------	----------

## E

EAP .....	566.4–92, 105
Effectiveness Measures .....	566.1–55
Egress ACL .....	566.4–28
Eicar .....	566.3–44-45, 49
Email → CSC #7 .....	.....
Email Attachments .....	566.3–10
Email Exfiltration Website .....	566.4–40, 53
Email Filtering Proxy .....	566.3–11
EMET .....	566.3–35, 38
Encryption .....	566.3–83
.....	566.4–39, 41, 43
→ CSC #13 .....	.....
Policy .....	566.4–54, 59
System .....	566.4–70
Endpoint Protection .....	566.3–37
.....	566.4–41
ENUM .....	566.3–44-45
Environment Separation .....	566.5–55
ERD .....	566.1–42-45
Consolidated .....	566.1–45
Error Checking .....	566.5–54
Error Handling .....	566.3–55
Existing Vulnerabilities .....	566.2–39
External Communications Policy .....	566.3–115
External Devices .....	566.3–35
External Third-Parties .....	566.4–57

## F

Fail Closed .....	566.4–21
FBI .....	566.1–8
FDCC .....	566.2–26
FIA .....	566.2–9, 11, 14
File Integrity .....	566.2–14
File Transfer Website .....	566.4–40, 53
Firewall Leak Tests .....	566.4–58
Firewalls .....	566.3–116
FISMA .....	566.1–6, 51
Flash .....	566.3–8, 33
Frequency Analysis .....	566.3–83
FTP .....	566.4–27
Full Disk Encryption .....	566.1–85

## G

Gap Analysis .....	566.5–33, 566.1–45
GLBA .....	566.1–50-51
Gold Version .....	566.2–23
Golden Ticket .....	566.2–58
GRC .....	566.1–70, 97
.....	566.2–11, 41, 66, 92
.....	566.3–11, 37, 58, 80, 100
.....	566.4–12, 41, 94
Grouping of Baseline Resources .....	566.2–25

# SANS SEC566 – Implementing & Auditing CSC In Depth

---

## H

Hard Drive Encryption .....	566.4–37
Hardened Device .....	566.3–102
Hardened Email Client .....	566.3–12
Hardened Web Browser .....	566.3–12
Hardened Wireless Device .....	566.4–101
Hardening Configuration Templates .....	566.5–55
Hardware Lifecycle Management .....	566.1–84
Hash Baseline .....	566.2–12
Heartbleed .....	566.3–96
HIDS .....	566.4–27
HIPAA .....	566.1–50–51
HIPS .....	566.3–47–48
Host-Based Firewall .....	566.3–56, 58–59, 67
HTTP .....	566.4–27
HTTP Tunneling .....	566.4–5

## I

ICMP .....	566.2–101
Identity & Access Management .....	566.2–66
IDS / IPS .....	566.4–8, 22, 27
→ CSC #12 .....	
Impact Analysis .....	566.3–87
In-House-Developed Application .....	566.5–54
Incident Handling .....	566.5–83
Incident Response → CSC #19 .....	
Information Assurance Program .....	566.5–43
Information Disclosure .....	566.4–34, 57
Information Flow .....	566.3–113
Information Security Lifecycle .....	566.2–23
Information Security Policy .....	566.4–54
Information Security Standards .....	566.1–51–52
Infrared .....	566.4–87
Ingress ACL .....	566.4–28
Insider Threat .....	566.5–20
Installation Policy .....	566.1–109
Integrity Checking .....	566.2–8–9
Integrity Checking Policy .....	566.1–111
Internal Network .....	566.4–10
Internal Systems .....	566.4–4, 23
Intrusion Monitoring .....	566.4–25
Inventory Database/Baseline .....	566.1–99–100, 106
IP Spoofing .....	566.4–21
iPost .....	566.1–32–36
Risk Measurement Components .....	566.1–36
IPSec .....	566.2–8
ISDN .....	566.2–104
ITIL .....	566.1–25

## J

JavaScript .....	566.3–8
------------------	---------

## K

Key Management .....	566.3–88
Known Vulnerability .....	566.2–51

## L

LANMAN .....	566.2–5
LDAP .....	566.2–58
Less-Trusted Networks .....	566.4–67
Level of Trust .....	566.2–51
Log Analysis → CSC #6 .....	
Logs .....	566.2–39
Archiving .....	566.2–90
Baseline .....	566.2–93
Format .....	566.2–89
Level .....	566.2–108
Management .....	566.2–105
Retention .....	566.2–93
LSASS .....	566.2–61

## M

Maintenance → CSC #6 .....	
Malicious IP .....	566.4–7
Malicious Software .....	566.3–31
Malware → CSC #8 .....	
Man-in-the-Browser .....	566.2–19
Man-in-the-Middle .....	566.2–19
Mandiant .....	566.1–11
MD5 .....	566.2–6
.....	566.3–55
Meterpreter .....	566.2–34
Mimikatz .....	566.1–11
.....	566.2–60–61
Misconfigured System .....	566.2–7
Mission-Critical Role .....	566.5–35
MITRE .....	566.1–19
MMC .....	566.2–26
Monitoring → CSC #6 .....	
Monitoring Policy .....	566.4–25
Most Critical Programming Errors .....	566.5–66
Multi-Factor Authentication .....	566.4–105
.....	566.5–11

## N

NAC .....	566.1–79
.....	566.3–48
NAT .....	566.3–116
National Security .....	566.4–34
Need-to-Know .....	566.4–64
→ CSC #14 .....	
NERC .....	566.1–51
NetFlow .....	566.4–11, 13, 42
Network Assessment .....	566.3–117
Network Device Configuration .....	566.3–97–98
.....	566.4–12
→ CSC #11 .....	
Network Device Management System .....	566.3–100
.....	566.4–70, 94



# SANS SEC566 – Implementing & Auditing CSC In Depth

---

Network Filtering .....	566.3–116
Network Monitoring .....	566.4–58
Network Perimeter .....	566.4–23, 37, 44
Network Security Testing .....	566.2–49
Network Segmentation .....	566.4–27, 67
→ CSC #14 .....	
Network Share .....	566.4–68
Network Topology .....	566.4–27
Network Traffic Baseline .....	566.3–38, 101
NIDS .....	566.2–101
.....	566.4–26–27
NIS .....	566.2–58
NIST .....	566.1–27–28, 51
IR 7511 .....	566.1–30
SP 800-117 .....	566.1–30
SP 800-126 .....	566.1–30
SP 800-18 .....	566.2–26
SP 800-40 .....	566.2–26
SP 800-42 .....	566.2–49
SP 800-53 .....	566.1–27–28
SP 800-53 → <b>Standard Mappings</b> .....	
NLA .....	566.1–70, 81
.....	566.4–94
Non-Disclosure Agreement .....	566.4–57
NTLM .....	566.2–5
NTP .....	566.2–92, 99
NVD .....	566.1–32

## O

OCIL / OCRL .....	566.1–31
Offline Media .....	566.4–44
OpenNet .....	566.1–32
Operation Aurora .....	566.2–35
Opportunistic Malware .....	566.3–48
OTP .....	566.2–64
OTT .....	566.1–19
Outbound Traffic .....	566.4–39
OVAL .....	566.1–31
OWASP .....	566.2–79

## P

Packet Inspection .....	566.4–7
Passive Tools .....	566.1–67
Password .....	566.2–65
.....	566.5–11
→ CSC #5 .....	
File .....	566.2–75
Policy .....	566.2–80
Patch Management .....	566.2–23, 26, 38
System .....	566.2–41
Patching Timeline .....	566.2–40
PCI .....	566.1–51
PDA .....	566.4–107
PEAP .....	566.4–105
Peer-to-Peer .....	566.4–92, 105
Penetration Testing .....	566.2–108

→ CSC #20 .....	
Perimeter Traffic .....	566.4–14
Periodic Scans .....	566.4–38
Persistent Connection .....	566.4–50
Phishing .....	566.2–78
.....	566.3–19
Phishing 🚩 .....	566.1–11
PII .....	566.4–44, 49–50
Ping Sweep .....	566.3–116
PKI .....	566.1–70
.....	566.3–114
.....	566.4–94
PMS .....	566.2–43
Poison Ivy .....	566.3–32–33
Policy .....	566.1–84
Ponemon .....	566.1–9
Port → CSC #9 .....	
Port Scan .....	566.3–56
Principle of Least Privilege .....	566.2–64
PrivacyRights.org .....	566.1–10
Privilege → CSC #5 .....	
Provisioning Tools .....	566.3–70
Proxy .....	566.4–9, 12
→ CSC #12 .....	
Public Locations .....	566.4–56

## Q

Quizz .....	566.5–38–39
-------------	-------------

## R

RADIUS .....	566.3–114
RAT .....	566.3–32
RDP .....	566.2–8
Recovery Posture .....	566.3–87
Red Team Exercises .....	566.1–86
→ CSC #20 .....	
Release Management .....	566.3–116
Remediation .....	566.2–33
Remote Administration .....	566.2–8
Removable Device Policy .....	566.4–54
Removable Media Control .....	566.3–37
Risk Rating .....	566.2–40
Rlogin .....	566.4–28
Rogue Devices .....	566.2–107
Rogue Wireless Devices .....	566.4–101
Rootkit .....	566.3–48
Ruleset Review .....	566.3–70
RunAs .....	566.2–65

## S

SaaS .....	566.2–15
Sandboxing .....	566.3–46
SBU .....	566.1–32
SCAP .....	566.1–30–31, 76
.....	566.2–10–11, 36, 41
.....	566.3–58



# SANS SEC566 – Implementing & Auditing CSC In Depth

---

.....	566.4–94
Vulnerability Score .....	566.2–50
Scope .....	566.3–117
Screen Lock .....	566.5–8
SDLC .....	566.5–68
Secondary Evaluation Methodologies .....	566.1–56
Secure Access Control .....	566.4–20
Secure Code .....	566.5–55
Secure Configuration .....	566.2–7, 12, 19
→ CSC #3 .....	
Secured System Images .....	566.2–13
SecurID .....	566.3–114
Security Assessment .....	566.3–69
Security Awareness .....	566.5–34, 566.5–43
Security Benchmark .....	566.2–26
Security Configuration Snap-in .....	566.2–26
Security Flaws .....	566.5–65
Security Measures .....	566.2–52
Security Profile .....	566.4–90
Security Templates .....	566.2–26
Segregation of Duties .....	566.2–80
Sekurlsa .....	566.2–61
Sender Policy Framework .....	566.3–10
Sensitive Information .....	566.4–37-38
→ CSC #13 .....	
Sensitive Network Traffic .....	566.4–43
Service → CSC #9 .....	
Service Inventory .....	566.3–59
Service Separation .....	566.3–57
Session Tracking .....	566.4–11
SHA1 .....	566.2–6
SIEM .....	566.1–70, 79, 97
.....	566.2–11, 41, 66, 92
.....	566.3–11, 37, 58, 80, 100
.....	566.4–12, 41, 94
Deployment .....	566.2–91, 95
Signature Update .....	566.3–34
Skills → CSC #17 .....	
Smart Cards .....	566.2–64
SMB .....	566.2–37
Smurf Attack .....	566.4–21
SNMP .....	566.4–107
Social Engineering .....	566.2–80
.....	566.3–33
.....	566.5–43
Social Networking .....	566.4–58
Software → CSC #2 .....	
Software Inventory .....	566.1–95-96, 106
.....	566.2–12
System .....	566.1–97
Source Control .....	566.1–111
SOX .....	566.1–50-51
Spear Phishing .....	566.3–4
SPF .....	566.3–10
DNS Record .....	566.3–11
Spycar .....	566.3–44-45
SQL Injection .....	566.3–55
.....	566.5–69

SRR Lite .....	566.2–26
SSH .....	566.2–37, 62
.....	27
SSID .....	566.4–103
SSL .....	566.2–8
.....	566.3–55
.....	566.4–27
STIG .....	566.2–26
.....	566.3–65
Strategy .....	566.1–84
Sudo .....	566.2–65
Super User Account Baseline .....	566.2–67
SYN Flood .....	566.3–116
Synchronized Time Sources .....	566.2–89
Syslog Server .....	566.3–113
System Configuration Enforcement System ..	566.2–11
.....	566.3–11
.....	566.4–12, 94
System Events .....	566.2–85
System Hardening .....	566.2–26
System Logging .....	566.5–24
System Procurement Policy .....	566.2–24

## T

TACACS .....	566.3–114
Targeted Malware .....	566.3–48
TCP Sessions .....	566.4–27
Technical Assessment .....	566.1–85
Telnet .....	566.2–8
.....	566.4–28
Test Scenarios .....	566.2–107
Third-Party RFI .....	566.4–58
Third-Party-Procured Application .....	566.5–54
Time-of-Day Access .....	566.5–10
TLS .....	566.2–8
.....	566.3–55
.....	566.4–27, 92
Top 35 Mitigation Strategies .....	566.1–37-38
Topology Map .....	566.4–26
Towtruck .....	566.3–44-45
Traffic Flow Inventory .....	566.4–25
Training .....	566.5–38-39
→ CSC #17 .....	
Scenario-Based .....	566.5–43
Trojan .....	566.2–19
Two-Factor Authentication .....	566.3–98, 109, 114
.....	566.4–9, 14, 23

## U

UML .....	566.1–39-41
Unauthenticated Scan .....	566.2–37
Unauthorized Access .....	566.4–64, 77, 87, 101
Unauthorized Browser .....	566.3–7, 18
Unauthorized Code .....	566.3–31
Unauthorized Configuration .....	566.2–20, 22

# SANS SEC566 – Implementing & Auditing CSC In Depth

---

Unauthorized Devices .....	566.1–80-81	.....	566.4–90
Unauthorized Elevated Accounts .....	566.2–75	.....	566.5–65
Unauthorized Email .....	566.3–18		
Unauthorized Network Device .....	566.3–108		
Unauthorized Service .....	566.3–66-67		
Unauthorized Software .....	566.1–108, 111		
Unauthorized Traffic .....	566.4–23		
Undocumented Account .....	566.2–62		
Undocumented Backdoor .....	566.2–62		
Undocumented Changes .....	566.1–109		
Unusual Services .....	566.2–108		
URL Categorization Services .....	566.3–9		
URL Filtering Proxy .....	566.3–11		
URL Whitelisting .....	566.3–7		
USB .....	566.4–38		
Devices Inventory .....	566.4–38		
Token .....	566.4–52		
User Token .....	566.3–114		

## V

Vendor Management Policy .....	566.2–24
Virtual Machines .....	566.1–96-97
Virtualization System .....	566.1–97
VLAN .....	566.3–57, 99
.....	566.4–23, 68, 93
VMS .....	566.2–43
VNC .....	566.2–8
VPN .....	566.2–104
Vulnerability → CSC #4 .....	
Vulnerability Assessment .....	566.2–33, 51
Vulnerability Intelligence .....	566.2–38
Vulnerability Management .....	566.2–11, 23, 26-27, 51
Vulnerability Scanner .....	566.1–85
.....	566.2–37

## W

WAF .....	566.5–58, 68
Watering Hole .....	566.3–4
Watering Hole 🚩 .....	566.1–11
Web Application Attack .....	566.3–4
Web Browser → CSC #7 .....	
Whitelisting .....	566.1–97
WIDS .....	566.4–91, 94, 101, 103
WiFi .....	566.4–87
WinDump .....	566.4–97
WinPCap .....	566.4–97
WIPS .....	566.4–101, 103
Wireless .....	566.4–87
→ CSC #15 .....	
Access Baseline .....	566.4–94
Configuration .....	566.4–90
Hardware .....	566.4–91
Wireshark .....	566.4–97
WLSE .....	566.4–106
WPA .....	566.4–92, 105

## X

XCCDF .....	566.1–31
XSS .....	566.5–69

## Z

Zombie .....	566.2–19
--------------	----------