Index

**Version A09**

Please let us know if you find any errors in the index. Also, reach out if you have suggestions to improve the index (e.g. keywords that should be added, removed, or have page references added or removed). The easiest way to submit these improvements is to email [511@contextsecurity.com](mailto:511@contextsecurity.com).

Seth Misenar and Eric Conrad

# Index

|  |  |
| --- | --- |
| $HOME\_NET | 2:79, 3:86, 3:130 |
| $TRUSTED | 2:77-78 |
| .dll | 4:143, 5:82 |
| .evt | 5:43-44, 5:128, 5:131 |
| .evtx | 5:43-44, 5:128, 5:131 |
| .exe | 3:121, 4:63, 5:104-105 |
| .jar | 2:118, 3:49, 5:40 |
| Abnormal | 1:140, 1:160, 2:34, 2:36, 2:41, 3:53, 3:154 |
| Access token | 1:112, 2:24, 2:139, 3:175, 4:130, 4:150, 4:152-153, 4:155, 4:159 |
| ACT, Application Compatibility Toolkit | 4:127-128 |
| ActiveX | 1:90, 1:93 |
| Administrative accounts | 2:139, 4:3, 4:94, 4:96-98, 4:100, 4:123, 4:135, 5:28, 5:133, 5:143, 5:155, 5:157, 5:159, 5:184 |
| Adobe Reader | 1:90, 1:96, 4:28 |
| ADS, Alternate Data Stream | 4:68-69 |
| Adversary Deception | 2:3, 2:134-135 |
| Adversary success | 1:20, 3:20 |
| Alert data | 1:27, 3:64, 3:82, 3:93 |
| Alexa | 2:38, 3:173, 3:175, 5:88 |
| Analysis Methodology | 3:3, 3:57, 3:60 |
| Anomaly | 2:43, 3:38, 3:43, 3:50-53, 3:81, 3:122, 3:127-130, 3:145, 5:87 |
| Anomaly Detection | 2:34, 2:112, 3:50, 3:52-53, 3:128, 3:130, 3:145, 4:49, 5:28 |
| Antimalware | 1:52, 1:142, 2:110, 2:157, 4:4, 4:18, 4:169-170 |
| Antivirus | 2:157, 3:21, 3:46-48, 3:55, 3:63, 3:73, 3:115, 3:125, 4:169-170, 5:102 |
| Anubis | 2:160 |
| APK | 2:160 |
| AppArmor | 4:85 |
| Application Inspection | 2:95-96, 2:98-99 |
| Application Monitoring | 4:48 |
| Application Whitelisting | 4:48, 4:61-62, 4:70, 4:76, 4:84, 4:86-87, 4:91, 4:93, 4:180, 5:50 |
| Application Whitelisting, Bypass | 4:82 |
| Application Whitelisting, Phase 0: Whitelist Building | 4:56, 4:71-75 |
| Application Whitelisting, Phase 1: Targeted Detection | 4:76-78 |
| Application Whitelisting, Phase 2: Strict Enforcement | 4:79-80 |
| Applocker | 4:86-90, 5:132, 5:161-162 |
| APT | 2:39, 3:169, 4:162, 5:78, 5:104 |
| argus | 3:77, 3:93 |
| ASD Top 35 | 5:25, 5:38 |
| ASD Top 4 | 5:26-28, 5:38 |
| ASEPs | 4:112 |
| ASEPs, Auto-Start Extensibility Points | 1:133, 4:3, 4:112-113, 4:115 |
| ASEPs, Registry | 4:112, 5:177-182 |
| Asset Inventory | 5:52, 5:54, 5:58-59, 5:108 |
| Authentication | 4:4, 4:130-131, 4:141-143, 4:150-152, 4:157, 4:160, 4:166-167, 5:36, 5:84, 5:96, 5:154 |
| Authentication Policy Silos | 4:166 |
| Autoruns | 1:133, 4:3, 4:113, 4:115 |
| awk | 3:40, 3:157 |
| Backdoor | 1:47-48, 1:107 |
| Base64 | 3:147, 4:143 |
| Baseline Configuration | 4:3, 4:31-34, 4:37-39, 4:41, 4:74, 4:93, 5:75 |
| Baselining | 4:42, 4:113, 4:181, 5:51 |
| Behavior | 2:10, 2:107-109, 3:49-50, 3:136, 5:104 |
| Bejtlich | 1:27, 1:55, 3:9, 3:11, 3:16, 3:20, 5:5, 5:9 |
| BITS, Background Intelligents Transfer Service | 4:27, 4:29 |
| Blacklist | 1:97, 2:44, 2:53-54, 2:56-57, 2:117, 3:44, 3:46, 3:155, 4:165, 4:186, 5:102 |
| Blue Team | 3:29 |
| Bogon | 2:53-54 |
| Botnet | 1:49, 3:5, 3:137, 5:89, 5:106, 5:109 |
| Bro | 3:30, 3:38-40, 3:43, 3:69, 3:74, 3:89, 3:93, 3:152, 3:155-156, 3:172-173, 3:175-176 |
| Browser | 1:82, 1:90-94, 2:18, 2:114-115, 3:151-153, 3:172 |
| Browser attacks | 1:92-93 |
| C2 | 1:47-48, 1:107, 1:130-131, 1:136, 2:23, 2:26, 2:44-45, 3:3, 3:107, 3:134, 3:141, 5:88-89, 5:176 |
| C2, HTTP | 3:148-149 |
| C2, HTTPS | 1:119, 1:141, 2:97, 3:3, 3:141, 3:159-160, 3:162, 3:166, 3:175 |
| C2, HTTPS and X.509 | 3:55, 3:131-132, 3:162, 3:165, 3:169-175 |
| C2, ICMP | 3:143-144 |
| C2, non-HTTPS SSL | 3:162, 3:164-165 |
| C2, Persistent Connections | 3:138-139 |
| C2, Tor | 3:167 |
| Cached Credentials | 4:150-151 |
| CAPEX | 1:58, 1:153 |
| Carving | 3:3, 3:69-70, 3:74, 3:89 |
| CDM, Continuous Diagnostics and Miticgation | 1:24, 5:6, 5:10-13, 5:23 |
| Centralized Logging, Windows | 4:173-174, 5:114 |
| Change Detection | 4:41-42, 5:96-98 |
| Change Monitoring | 4:41-42, 4:181 |
| Ciphertext | 3:131 |
| CIS, Center for Internet Security | 4:34-35, 4:37, 4:39, 5:124 |
| Cleartext | 1:141, 4:101, 4:130, 4:143-144, 4:148, 4:160 |
| Client-Side | 1:28, 1:60, 1:71-75, 1:77, 1:90, 1:96, 2:17-18, 2:22, 2:26, 2:76, 2:82, 2:90, 3:108 |
| Content Filter | 1:54, 2:116-118, 2:120, 2:122, 2:156, 3:140 |
| Content-Type | 2:118-119 |
| Correlated Data | 1:27, 3:64, 3:87 |
| Cost per record | 1:11 |
| Critical Controls, 1 | 3:123, 3:135, 4:18, 4:60, 4:95, 5:47, 5:52, 5:74, 5:87, 5:101, 5:108, 5:148 |
| Critical Controls, 10 | 4:18 |
| Critical Controls, 13 | 3:135 |
| Critical Controls, 14 | 5:108 |
| Critical Controls, 19 | 3:123 |
| Critical Controls, 2 | 3:123, 3:135, 4:16, 4:60, 5:52, 5:74, 5:101, 5:108, 5:148 |
| Critical Controls, 20 | 4:7-8 |
| Critical Controls, 3 | 3:135, 5:47, 5:52, 5:148 |
| Critical Controls, 5 | 4:8, 4:16, 4:95 |
| Critical Controls, 8 | 4:60 |
| Critical Controls, 9 | 3:135 |
| Critical Controls, First Five Quick Wins | 4:7-8, 4:16, 4:60, 4:95, 4:192, 5:50-51 |
| Critical Security Controls | 1:34, 1:37-40, 1:122, 3:162, 4:7-8, 4:16, 4:88, 4:93, 5:23-24, 5:148, 5:184 |
| Cuckoo | 2:108-109, 2:140 |
| CyberScope | 5:18 |
| Daemonlogger | 3:68 |
| Data Breach | 1:9-11, 3:19, 4:178 |
| Data Classification | 5:32, 5:34 |
| Data compromise | 1:69, 1:163, 2:36, 5:34 |
| Daylight Savings Time | 2:58-59, 3:85 |
| DBIR | 1:9-10, 1:12-15, 2:125, 3:19 |
| DDoS | 1:48-49, 1:67, 1:100 |
| Debug Programs | 4:99, 4:103, 4:110, 4:191 |
| Deception Devices | 2:3, 2:134-137 |
| Deduction | 3:58 |
| Default Deny | 1:142, 2:51, 2:55, 2:57, 2:60, 5:107 |
| Defensible Network | 1:2, 1:26, 2:163, 3:16, 3:123-125, 3:127-128, 3:138, 3:160, 5:20, 5:30-31, 5:39-40 |
| Detection-Oriented | 1:116-117, 2:74, 4:180 |
| DIACAP | 3:8, 5:7-8, 5:18 |
| diff | 4:42, 4:113, 5:59, 5:96 |
| Dirty Word List | 2:152, 2:154-155, 3:61 |
| Display filters | 3:111, 3:119-122, 3:132, 3:167 |
| DITSCAP | 3:8, 5:7-8 |
| DLL | 2:160, 3:52, 3:87, 3:130, 4:50, 4:55, 4:83, 4:91, 4:143, 4:183, 5:82, 5:161-162 |
| DNS, failed-dns-query | 5:93 |
| DNS, Logging | 5:86-87, 5:90-93, 5:184 |
| DNS, long-dns-query | 5:93, 5:184 |
| DNS, NXDOMAIN | 5:93 |
| DOCX | 1:79, 1:97, 2:118, 2:160, 3:44, 3:86, 3:130, 3:163 |
| DoS, Denial of Service | 1:46, 1:48, 2:102, 3:33, 3:117-118 |
| dumpcap | 3:68 |
| Dynamic Analysis | 2:108-109, 2:118, 2:160 |
| Egress | 1:3, 1:142-143, 1:166, 2:39, 2:42, 2:44, 2:47, 2:49, 2:55, 2:57, 2:60, 2:97, 2:113, 2:122, 2:162, 4:172-174, 4:180 |
| ELSA | 1:3, 1:166, 3:30, 3:41 |
| Emerging Threats | 3:44, 3:83, 3:86-87, 3:130, 3:136 |
| EMET, Enhanced Mitigation Experience Toolkit | 4:3, 4:44-46 |
| Enable-PSRemoting | 5:173 |
| Entropy | 3:34, 3:52, 3:124, 3:127, 3:131-132, 3:163, 3:167, 5:88, 5:104-105, 5:135, 5:138, 5:156, 5:181 |
| Event ID 1056, RDP Self-Signed Cert | 5:147, 5:162 |
| Event ID 1102, Event Log Cleared | 5:145, 5:162 |
| Event ID 2003, Firewall Disabled | 5:151, 5:162 |
| Event ID 2005, Firewall Rule | 5:103, 5:152 |
| Event ID 4624, Logon | 5:153, 5:155 |
| Event ID 4720, User Creation | 5:44, 5:142, 5:162 |
| Event ID 4722, User Enabled | 5:44, 5:142, 5:162 |
| Event ID 4724, Password Reset | 5:142, 5:162 |
| Event ID 4732, User Added to Group | 5:44, 5:144, 5:162 |
| Event ID 4738, Account Changed | 5:142, 5:162 |
| Event ID 7030, Interactive Service Error | 5:21, 5:139-140, 5:162 |
| Event ID 7045, Service Creation | 5:21, 5:135, 5:138, 5:140, 5:149, 5:162 |
| Event IDs, Applocker | 4:89-90, 5:161-162 |
| Event IDs, Removable Media | 5:149 |
| Event Logs, Critical Windows Events | 5:3, 5:127, 5:134, 5:140-141, 5:143, 5:145-146, 5:148-150, 5:153, 5:161, 5:184 |
| Event Logs, Damaged | 5:129 |
| Event Logs, Windows | 5:19, 5:123, 5:129, 5:131, 5:133, 5:164 |
| Event Query, Windows | 5:121 |
| Event Viewer | 5:120, 5:128-131, 5:142, 5:144, 5:147, 5:149, 5:151 |
| eventvwr | 5:120, 5:128, 5:130 |
| EXE | 2:160, 3:3, 3:33, 3:52, 3:61, 3:63, 3:73, 3:87, 3:107, 3:116-117, 3:121-122, 3:130, 3:178, 5:105, 5:162 |
| EXE, MZ | 3:72, 3:118-120, 3:130 |
| EXE, PE | 3:73, 3:87, 3:118, 3:120, 3:130 |
| EXE, This program cannot be run in DOS mode | 3:33, 3:117-119 |
| EXE, This program must be run under Win32 | 3:118, 3:120 |
| EXE, This program must be run under Win64 | 3:118 |
| EXE, Transfer | 3:3, 3:125, 3:127, 3:130, 3:178 |
| Executable | 1:79, 3:116, 3:125, 3:127, 4:65-68, 4:71, 4:74-75, 4:77, 4:83, 5:102 |
| Exfiltration | 1:101, 1:131, 1:141, 1:143, 2:15, 2:25, 2:36, 2:42-45, 2:58-61, 2:68-69, 2:81, 2:83, 2:89-90, 2:94, 2:100-102, 2:110, 2:122 |
| Exploitation | 1:44-45, 1:70, 1:75, 1:93, 1:99, 1:107, 1:118, 1:127, 1:131, 2:15, 2:22, 2:90, 2:137, 4:93, 4:111, 4:130 |
| Extracted data | 3:64, 3:69 |
| False Negative | 3:125 |
| False Positive | 2:66, 2:81, 2:86, 2:102, 2:140, 3:24, 3:52, 3:129-130, 4:76-78, 4:184, 5:40 |
| File Analysis | 2:157, 2:160 |
| File Carving | 3:70, 3:74 |
| File Integrity Monitoring | 4:42, 4:62, 4:177, 4:181 |
| File-format | 1:90, 1:96-97, 3:65, 3:115, 4:185 |
| FIPS 199 | 5:33 |
| Firewalls | 1:54, 2:64, 2:74, 2:87, 2:92-95, 2:97-102, 2:116, 2:146, 2:156, 2:162 |
| Flash | 1:90, 1:93-94, 4:26, 5:26 |
| Flow Data | 1:26, 2:30-33, 2:41, 2:143, 2:162, 3:77 |
| Forensics | 1:155, 2:107, 2:125, 2:154, 3:34, 3:61, 4:42, 4:72, 4:83, 4:183-184, 5:129 |
| Forward Proxy | 2:116, 2:122-123 |
| Framework | 1:37, 1:94, 1:111, 1:122, 2:96, 2:152, 3:39, 4:186, 5:8, 5:174 |
| GeoIP | 2:33, 2:40, 2:53-54, 2:56 |
| Get-WinEvent | 5:21, 5:43-44, 5:140, 5:142, 5:144-145, 5:147, 5:149, 5:151, 5:162 |
| grep | 3:5, 3:30, 3:37, 3:75-76, 3:152, 3:154, 3:156-157, 3:176, 5:68-69, 5:92 |
| Group Policy | 4:24, 4:38, 4:86-87, 4:108, 4:124, 4:137, 4:173, 5:114-115, 5:123 |
| Hanlon's Razor | 3:49, 5:40 |
| HIDS, Host Intrusion Detection System | 1:9, 4:170, 4:177-182 |
| HIPS, Host Intrusion Prevention System | 4:170, 4:177-180, 4:182, 5:36 |
| HKLM\Security\Policies\Secrets | 4:103 |
| HoneyAdmins | 2:139 |
| Honeyclients | 2:140 |
| Honeynets | 2:135, 2:137 |
| Honeypots | 2:3, 2:134-139 |
| HoneyRobots.txt | 2:139 |
| HoneySAT | 2:139 |
| HoneyTable | 2:139 |
| HoneyTokens | 2:4, 2:165 |
| HoneyUsers | 2:139 |
| HTTP GET | 3:36, 3:109, 5:105 |
| HTTP POST | 1:135-136, 3:147-148 |
| Hunt team | 1:31, 1:117, 1:163, 2:8-10, 2:126-127, 2:130-131, 3:7, 3:11-13, 3:178, 4:186 |
| Hunt Teams | 1:31, 1:84, 1:117, 1:163, 2:8-10, 2:39, 2:126-127, 2:130-131, 3:7, 3:11-13, 3:178, 4:186 |
| Hypothesis Management | 3:60 |
| ICMP | 1:141, 2:32, 2:48-50, 3:52, 3:110, 3:138, 3:141-145 |
| ICMP 0:0, Echo Reply | 3:144 |
| ICMP 8:0, Echo Request | 3:52, 3:142, 3:145 |
| IDS Frontends | 1:60, 1:62-64, 3:3, 3:30-34, 3:66, 3:83, 3:113 |
| Impersonation Level | 4:152-155, 4:159 |
| Inbound Filtering | 2:29, 2:53 |
| Incident Response | 1:8-9, 1:39, 1:155, 1:157, 3:13, 3:103, 3:138, 3:140, 4:42, 4:184 |
| Indicator Identification | 2:152 |
| Indicators | 1:129-130, 2:151-155 |
| Indicators of Compromise | 2:155, 4:184 |
| Interactive Logon | 4:151, 4:157, 4:167, 5:155 |
| Internal SI Firewalls | 2:146, 2:162 |
| Inventory, Active Scanning | 5:52, 5:54-58, 5:64, 5:108 |
| Inventory, Passive Discovery | 3:30, 3:93, 5:54, 5:63-64, 5:66-69 |
| Invisibility | 2:78 |
| IPFIX | 2:30-32, 2:41, 2:143, 2:162, 3:77 |
| IRC | 1:102, 1:128, 2:48, 2:52, 2:70, 2:77, 2:97, 2:101, 3:39, 3:53, 3:67, 3:73, 3:141, 4:82, 4:86 |
| IRC C2 | 2:97, 2:101, 3:141 |
| ISCM, Information Security Continuous Monitoring | 5:6, 5:8, 5:14-16 |
| JAR | 2:106, 2:118, 2:160, 3:49, 5:40 |
| Java | 1:90, 1:93-95, 2:114, 2:118, 2:160, 4:22, 4:26, 4:28, 4:46, 5:26, 5:78 |
| JavaScript | 1:93, 2:114, 2:160 |
| Joe Sandbox | 2:160 |
| Kansa | 4:186-187 |
| Kill Chain | 1:129-130, 2:151-152, 2:154 |
| LanMan Hash | 4:137-138 |
| Layer 3 | 1:56, 1:121, 2:30, 2:33, 2:53, 2:55-57, 2:93, 2:95, 2:97-98, 2:144, 3:108, 3:127 |
| Layer 4 | 1:56, 2:30, 2:33, 2:55, 2:57, 2:93, 2:95, 2:97, 3:108 |
| Layer 7 | 1:33, 1:56, 1:121, 2:33, 2:43-45, 2:50, 2:93, 2:95, 2:98-99, 2:101, 3:65, 3:79, 3:108, 5:100 |
| LiveSSP | 4:145, 4:148, 4:160, 4:166 |
| Log data | 1:27, 2:43, 3:64, 5:19, 5:129 |
| Log files | 3:8, 5:5, 5:129 |
| Log Monitoring | 4:39, 4:181, 5:112, 5:127, 5:132 |
| Log Review | 1:9, 4:177 |
| Log Settings, Windows | 5:122, 5:124 |
| Logon Types, Type 10 | 4:151, 5:155 |
| Logon Types, Type 11 | 4:150-151 |
| Logon Types, Type 2 | 4:151, 4:155, 4:157, 4:167, 5:155 |
| Logon Types, Type 3 | 2:50, 4:109, 4:151, 5:156, 5:159-160 |
| Logon Types, Type 4 | 4:151 |
| Logon Types, Type 7 | 4:145, 4:151 |
| Long Tail Analysis | 4:186-187, 5:41-44, 5:167, 5:181, 5:184 |
| LSA Secrets | 4:103 |
| lsass.exe | 4:63 |
| LUA Buglight | 4:128 |
| M-Trends | 1:8, 1:14-15, 1:84, 1:126, 1:135, 1:138, 2:125, 4:161 |
| Malvertising | 1:77, 1:83 |
| Malware Detonation Devices | 1:26, 1:54, 2:3, 2:64, 2:106-107, 2:140, 3:125 |
| MBSA, Microsoft Baseline Security Analyzer | 5:79-82 |
| Memory Analysis | 4:183-184, 4:186 |
| Metadata | 1:27, 3:64, 3:79, 3:87, 4:56, 5:129 |
| Metasploit | 1:111, 1:138-139, 3:47, 3:132, 3:165, 4:161, 5:136, 5:138-139, 5:146, 5:157-158 |
| Meterpreter | 1:111-112, 3:117, 3:164-165, 4:159, 5:133, 5:141, 5:145-146, 5:157 |
| Microsoft Account | 4:142, 4:145-148 |
| Microsoft Office | 1:90, 1:96-97, 4:34-35, 5:26 |
| Mimikatz | 4:48, 4:91, 4:148, 4:158-166 |
| Minnow | 1:87-88 |
| Mobile application | 2:95 |
| Mobile device | 1:38, 1:44, 1:86-88, 2:10, 2:114, 3:110, 4:6, 4:13, 4:21 |
| ModSecurity | 2:3, 2:72 |
| MSSP | 1:9, 1:148, 1:153-155, 1:159 |
| NAT | 2:33-34 |
| Nation-State | 1:68 |
| ndiff | 5:59 |
| NetFlow | 1:26, 2:30-33, 2:41, 2:143, 2:162, 3:77 |
| netsniff-ng | 3:30, 3:66, 3:68 |
| Network Logon | 4:109, 4:151, 5:156, 5:159-160 |
| NGFW | 1:26, 1:54, 2:3, 2:64, 2:74, 2:87, 2:92-95, 2:97-102, 2:116, 2:156, 3:108, 5:89, 5:107 |
| ngrep | 3:30, 3:37, 3:75-76 |
| NIDS | 2:3, 2:74-77, 2:80-84, 2:86-87, 3:15, 3:17, 3:30-31, 3:38, 3:43, 3:51, 3:93, 4:177 |
| NIPS | 2:3, 2:74, 2:86-90, 4:177 |
| nmap | 2:38, 3:30, 3:145, 5:56, 5:58-59 |
| Non-Encrypted HTTPS | 3:160-161 |
| NSRL RDS | 4:56, 4:71-75 |
| NT Hash | 4:134, 4:136, 4:138-139, 4:141-142, 4:157, 5:156 |
| NTFS Permissions | 4:98-99, 4:106-108 |
| Obfuscation | 2:160, 3:147 |
| Offense informs defense | 2:149, 5:24 |
| OpenAppId | 2:3, 2:96-97, 2:104 |
| OpenVAS | 5:76 |
| OPEX | 1:58, 1:153 |
| OSSEC | 3:93, 4:181 |
| Outbound connections | 2:35-36, 2:38, 2:41, 5:106 |
| Outbound Filtering | 2:29, 2:55-57 |
| Outsource | 1:148, 1:152-155, 1:159, 2:67 |
| p0f | 5:3, 5:64-65, 5:71 |
| PAC | 2:114-115 |
| Packet capture, Full | 1:62-63, 2:30, 3:32, 3:66-68, 3:93 |
| Packet Data | 1:62-63, 1:112, 2:30, 2:130-132, 3:32, 3:66-68, 3:93 |
| PADS, Passive Asset Database | 3:93, 5:64 |
| Pass the pass | 4:160 |
| Pass-the-Hash | 4:134, 4:137, 4:157, 4:159, 5:155-160 |
| Password Hashes | 4:130, 4:133-134, 4:139, 4:155, 4:159, 5:96 |
| Passwords Hashes, Ntds.dit | 4:139 |
| Passwords Hashes, SAM | 4:137, 4:139 |
| Patching | 1:75, 2:64, 2:66, 2:68, 4:15-17, 4:21-23, 4:26, 4:31, 4:65, 4:93, 5:31, 5:51, 5:78, 5:184 |
| PDF | 1:72, 1:74, 1:79, 1:97, 2:119, 2:160, 3:108, 5:26 |
| Perfect Solution Fallacy | 3:55, 3:155 |
| Perimeter SI Firewall | 2:3, 2:47, 2:58 |
| Persistence | 1:108, 1:110, 1:112, 1:116, 1:131, 1:133, 2:121, 4:4, 4:111-112, 4:182-183, 4:189, 5:176 |
| Persistence, registry | 5:176 |
| Persistence, service | 4:112 |
| persistent.pl | 3:139-140, 5:106 |
| Phish | 1:12, 1:72-74, 1:80-81, 1:87, 2:152 |
| Phishing | 1:12, 1:72-74, 1:80-81, 1:87, 2:152 |
| Pivoting | 1:102, 1:127, 1:137, 5:153, 5:155, 5:160 |
| Plugin | 1:93-94, 4:159 |
| Ponemon | 1:11 |
| Port Scan | 5:58 |
| Post-Exploitation | 1:99, 1:107, 1:118, 1:127, 1:131, 2:15, 2:23, 2:137, 4:130, 4:182 |
| PowerShell Remoting | 4:186, 5:173-174 |
| PPT | 1:85, 1:97, 2:160, 4:138 |
| PPTX | 1:85, 1:97, 2:160 |
| PRADS | 3:30, 5:64, 5:66-69 |
| PRADS, Passive Real-Time Asset Database | 3:30, 5:64, 5:66-69 |
| Prevention-Oriented | 1:54, 2:74 |
| Privilege escalation | 1:112, 3:13, 3:93, 4:107, 5:46 |
| Process Monitor | 4:125-126 |
| Protected Users | 4:166, 5:160 |
| Protocol Behavior | 3:43, 3:49 |
| Proxies | 2:57, 2:112-114, 2:116, 2:121-123, 2:140, 3:139, 3:147, 5:100-106 |
| PSExec | 1:138-139, 3:132, 4:158, 5:133-139, 5:157-159 |
| Rainbow Tables | 4:134 |
| Red Team | 1:39, 3:29 |
| Redline | 4:184-185 |
| Registry keys | 3:8, 4:125, 5:5, 5:41, 5:167, 5:176, 5:179, 5:181 |
| Remote Interactive | 4:151, 5:155 |
| Reputation | 2:41, 2:45, 2:56, 2:98, 2:120-122, 3:50-51, 4:161 |
| Response-Driven | 1:120 |
| Restricted Admin Mode RDP | 4:166 |
| Reverse HTTP | 1:112, 3:139, 5:106 |
| Reverse HTTPS | 1:112, 5:106 |
| RFC 1918 | 2:53-54 |
| Risk Informed | 1:122 |
| Risk Management | 1:37, 1:122, 5:8, 5:14, 5:18 |
| RMF, Risk Management Framework | 5:9 |
| Router | 1:38, 2:29-30, 2:34, 2:41-45, 2:47, 2:143, 5:97-98 |
| RTF | 1:79, 1:97 |
| Salts | 4:101, 4:134-136, 4:138, 4:157, 5:156-157 |
| SANCP | 3:93 |
| Sandbox | 1:26, 2:108-109, 2:118, 2:140 |
| SCAP, Security Content Automation Protocol | 4:39, 5:18, 5:74-76 |
| SCCM, System Center Configuration Manager | 4:27-29, 4:67 |
| Scheduled Tasks | 4:112 |
| SCM, Security Compliance Manager | 4:38 |
| SCUP, System Center Updates Publisher | 4:28-29 |
| Security Onion | 1:60-61, 3:28-30, 3:93, 3:99, 3:178, 5:66 |
| SeDebugPrivilge | 4:99, 4:103, 4:110, 4:163, 4:191 |
| Sensor Placement | 3:100-102 |
| Sensor, Design | 3:91, 3:93 |
| Sensor, DMZ | 2:75, 3:102 |
| Sensor, External | 3:102 |
| Sensor, NSM | 3:92, 3:99-100 |
| Sensor, Security Onion | 3:30, 3:93, 3:99, 3:178 |
| Sensor, Umbrella | 3:101-102 |
| Service Accounts | 4:102-103, 5:155 |
| Service Logon | 4:151 |
| Service-side | 1:44-45, 1:70, 1:75, 3:110 |
| Set-ExecutionPolicy | 5:170-171 |
| sFlow | 2:30 |
| Sguil | 1:60, 1:62-64, 3:3, 3:30-34, 3:66, 3:83, 3:113 |
| Shell | 1:48, 1:64, 1:107, 1:111, 5:84, 5:101, 5:118-119, 5:133, 5:141 |
| Shellcode | 1:135, 3:32, 3:34, 4:44 |
| SI Firewall | 2:3, 2:47-48, 2:58-61, 2:92-95, 2:97-99, 2:146-147, 2:162 |
| SID | 4:152 |
| SIEM | 1:26, 1:54, 1:147, 2:3, 2:125-128, 2:132, 3:30, 3:41, 3:63, 4:49-50, 4:56, 4:181, 5:109 |
| Signature Evasion | 3:47 |
| Signature Matching | 3:43-44, 3:46, 3:131 |
| SiLK | 3:77 |
| Situational Awareness | 1:29, 5:46 |
| Sniffing | 1:67, 3:92-94, 3:97, 3:99, 5:56, 5:64 |
| Sniffing, Hubs | 3:95 |
| Sniffing, Port Mirror/SPAN Port | 3:94-96, 3:98, 3:101, 3:128, 3:178 |
| Sniffing, Port Overload | 3:97-98 |
| Sniffing, Taps | 3:94-95, 3:97-98 |
| Sniffing, Virtual | 3:94, 3:99 |
| Snorby | 3:30-31 |
| Snort | 2:3, 2:78-79, 2:96, 2:104, 3:30, 3:38, 3:40, 3:43, 3:68, 3:80, 3:84-85, 3:145 |
| Snort Frontends | 1:60, 1:62-64, 3:3, 3:30-34, 3:66, 3:83, 3:113 |
| SOC | 1:145-161, 4:10, 4:91 |
| Social Engineering | 1:12, 1:71, 1:77, 2:17, 4:111 |
| SP 800-117 | 5:75 |
| SP 800-137 | 5:8, 5:14-17, 5:23 |
| SP 800-37 | 5:8 |
| Spam | 1:46, 1:67, 2:67, 3:86, 5:103, 5:109-110 |
| Splash Proxy | 2:121 |
| Splunk | 3:30, 3:41 |
| Spoofed | 2:41 |
| SQL Injection | 2:10, 2:14-16 |
| SRP, Software Restiction Policies | 4:86-87 |
| SSH | 1:141, 2:95, 2:101, 3:39, 3:139-140, 3:144, 5:84 |
| SSL | 1:112, 2:39, 3:39, 3:159-167, 3:173, 3:175, 4:67, 5:147 |
| SSO, Single Sign-On | 4:133, 4:141-143, 4:145, 5:156 |
| SSP, Security Service Provider | 1:148, 4:4, 4:141-143, 4:145, 4:160 |
| Stage 2 | 1:133, 3:3, 3:13, 3:107, 3:115-118, 3:128-129, 5:27 |
| Statistical Data | 3:64, 3:81 |
| STIGs, Security Technical Implementation Guides | 4:39-40 |
| Strategic Web Compromise | 1:84 |
| String data | 3:64, 3:75-76, 3:89 |
| strings, command | 3:5, 3:61, 3:75-76, 3:89, 3:117, 3:152, 3:154, 3:157 |
| Suricata | 3:30, 3:38, 3:40, 3:43, 3:145 |
| Sysmon | 4:3, 4:49-56, 4:58 |
| Sysmon, syntax and configuration | 4:3, 4:49, 4:51-55 |
| Tagged data | 3:84-86 |
| Target Breach | 1:13, 2:26, 3:21-25, 3:142, 4:178 |
| TCP/21, FTP | 2:93, 2:95, 3:22-23, 3:39, 3:79, 4:67, 5:101 |
| TCP/22, SSH | 1:141, 2:95, 2:101, 3:39, 3:139-140, 3:144, 5:84 |
| TCP/3389, RDP | 4:150, 4:155, 4:166, 5:110, 5:132-133, 5:146-147, 5:152, 5:162 |
| TCP/443, HTTPS | 1:112, 2:39, 3:39, 3:159-167, 3:173, 3:175, 4:67, 5:147 |
| TCP/6667, IRC | 2:97, 2:101, 3:39, 3:53, 3:141 |
| TCP/80, HTTP | 1:45, 1:112, 1:121, 1:135-136, 2:39, 2:42, 2:95, 3:39, 3:44, 3:79, 3:138, 3:141, 3:147-148, 3:154, 3:159-167, 3:175, 4:67, 4:143 |
| tcpflow | 3:77 |
| Teensy | 1:85 |
| Threat Intelligence | 1:128, 2:4, 2:98, 2:106, 2:120, 2:149-150, 2:153, 2:157, 4:183 |
| ThreatExpert | 2:160 |
| ThreatTrack | 2:160 |
| Time synchronization | 2:57, 3:91, 3:103-104 |
| Time Zone | 3:104 |
| TLS | 1:112, 3:13, 3:117, 3:160, 3:162-165, 3:167, 3:169 |
| True Positive | 3:24, 3:130, 4:76-77 |
| tshark | 3:35, 3:37, 3:77-78, 3:80, 3:152, 3:175 |
| tspkg | 4:160 |
| TTPs | 1:128, 2:150 |
| Tunnel | 1:141, 2:53, 3:139-141, 3:143-144, 3:162, 3:166, 5:40, 5:102, 5:106 |
| Two-Factor Authentication | 4:131, 4:167 |
| UAC, User Account Control | 4:118-119, 4:121-125, 5:182 |
| UDP/123, NTP | 2:57, 3:91, 3:103 |
| UDP/53, DNS | 2:13, 2:39, 2:51, 2:115, 3:52, 3:141, 4:67, 5:86-90, 5:93, 5:184 |
| UDP/69, TFTP | 4:67 |
| URL Analysis | 2:156, 2:159-160 |
| USB | 1:77, 1:85, 1:141, 3:110, 4:67, 5:43, 5:129, 5:148-149, 5:162, 5:172, 5:180 |
| User Rights, Windows | 4:98-99, 4:106, 4:109, 4:152, 4:191 |
| User Visibility | 2:98 |
| User-Agent | 3:3, 3:40, 3:107, 3:151-155, 3:157, 3:178 |
| UTC | 1:9, 1:129, 3:103-104 |
| Virtual Patching | 2:64, 2:66, 2:68 |
| VirusTotal | 2:157-159, 4:50, 4:56, 4:113, 4:164 |
| Visibility | 1:121, 1:132-133, 1:160, 2:44-45, 2:78, 2:90, 2:98, 2:101, 2:142, 3:178, 4:178, 5:15 |
| VLAN ACLs | 2:142, 2:144-146, 4:178 |
| VNC | 1:112, 4:155, 5:139 |
| VPN | 1:34, 1:65, 1:141, 2:35, 3:135, 3:138-139, 3:162, 5:40, 5:47, 5:61, 5:102, 5:108, 5:185 |
| Vulnerability assessment | 1:38, 3:8, 5:82 |
| Vulnerability Scanning | 2:16, 4:20, 5:3, 5:47, 5:58, 5:73-74, 5:76 |
| Watering Hole | 1:77, 1:84, 2:17-22, 4:119 |
| WDigest | 4:143-145, 4:148, 4:160, 4:163, 4:166 |
| Web Application Firewall | 1:26, 2:3, 2:63-64, 2:66-70 |
| wecutil | 5:119 |
| Wepawet | 2:160 |
| wevutil | 5:128 |
| WFAS, Windows Firewall with Advanced Security | 4:173-175, 5:132, 5:150-151, 5:162 |
| Whitelist Integrity | 4:64 |
| Windows Event Collector | 5:119 |
| Windows Remoting | 5:118, 5:173 |
| winrm | 5:118, 5:173 |
| Wireshark | 1:60, 1:63-64, 3:32, 3:35-36, 3:65, 3:68, 3:70, 3:81, 3:119-122, 3:132, 3:143, 3:161, 3:164, 3:167 |
| WMF | 1:79, 1:97 |
| WPAD | 2:114-115 |
| WSUS, Window Server Update Services | 3:124, 4:23-29 |
| X.509 | 3:55, 3:131-132, 3:162, 3:165, 3:169-175 |
| XLS | 1:97, 2:160, 4:69 |
| XLSX | 1:97, 2:160, 4:69 |
| XOR | 1:135, 3:147 |
| Zero-copy | 3:68 |
| Zero-day | 5:78 |
| Zone.Identifier | 4:68-69 |