| **Title** | **Bk** | **Page** | **Description** |
| --- | --- | --- | --- |
| 13 "Sensitive" privileges | 4 | 105 | SeTcbPrivilege SeBackupPrivilege SeCreateTokenPrivilege SeDebuPrivilege SeEnableDelegationPrivilege SeAuditPrivilege SeImpersonatePrivilege SeLoadDriverPrivilege SeLoadDriverPrivilege SeSecurityPrivilege SeSystemEnvironemtPrivilege SeAssignPrimaryTokenPrivilege SeResrorePrivilege SeTakeOwnershipPrivilege |
| Active interception - ZAP by OWASP | 2 | 80 |  |
| Active scanning | 5 | 48 | Host, port , service discovery. Test before prod scan |
| Active TLS interception | 2 | 78 | uses TLS proxies |
| AIP | 5 | 27 | Azure Information Protection  IP - Key used to encrypt policy - then signed with priv key |
| Amazon CloudWatch | 1 | 164 | Real-time monitoring resources |
| Amazon Detective | 1 | 181 | Faster security investigations. |
| Amazon GuardDuty | 1 | 179 | Threat intelligence |
| Amazon Inspector | 1 | 183 | Automating security posture assessment |
| Amazon Macie | 1 | 186 | Discover sensitive and regulated data in S3 |
| Amazon VPC | 1 | 174 |  |
| AppArmor Linux | 4 | 83 | App control/whitelisting. Path based |
| Application control | 4 | 62-68 | Block binaries. Malware might already be present in baseline |
| AppLocker | 4 | 84 | Allow known good / block known bad.  event ID 8003 - Audit Mode |
| AppLocker - enforce mode | 4 | 87 | event id 8007 for enforce mode |
| ASEPs | 4 | 107 | Auto Start Extensibility Points - well known ASEPs: HKLM\..\CurrentVersion\Run HKCU\..\CurrentVersion\Run , services, startmenu\program\startup |
| ASLR | 1 | 184 | Address space layout randomization (ASLR) is a technique that is used to increase the difficulty of performing a buffer overflow attack |
| ASR: Defender for Endpoint | 4 | 39 | Attach surface reduction - protection / detection of suspicious process operations or behaviours deemed risky |
| Asset inventory | 5 | 47 | Both active and passive scanning + DHCP logs or the switch CAM tables |
| autorunsc.exe | 4 | 108 | Analyses different ASEPs |
| AWS - VXLAN | 3 | 80 | traffic mirroring AWS |
| AWS cloudtrail | 1 | 156 | user, role, service actions monitor |
| AWS CloudTrail events: Mgmnt vs Data | 1 | 159 |  |
| AWS config | 1 | 188 | Cont monitoring |
| AWS Firewall Manager | 1 | 168 | configure and manage rules and security groups |
| AWS IAM | 1 | 153 | Manage access |
| AWS network firewall | 1 | 169 | Stateless + stateful / IDS and IPS capabilities |
| AWS Security Hub | 1 | 151 | Assess security posture |
| AWS VPC flow logging | 3 | 77 | L3 / L4 visibility. AWS doesn't want you to be looking at L2. DNS to Amazon DNS, DHCP, traffic to vpc router is not logged |
| AWS WAF and Shield | 1 | 172 |  |
| Azure authentication methods | 4 | 147 | MFA, passwords, password less -> windows hello, authenticator and fido2 security key |
| Azure Automatic State config | 4 | 24 | Centralized cloud based DSC mgmnt and monitoring of both cloud and on-prem |
| Azure Network Watcher | 3 | 80 | provide layer 7 visibility |
| Azure NSG | 3 | 85 | Composed of security rules |
| Baseline config | 4 | 11 | Reduce the business impact and time to recovery of a fielded system. Prevent unneeded software. Derive it from an industry proven config.  Ensure that the configuration can be predictably deployed |
| Baseline monitoring | 4 | 17 | Ensure org is operating under correct security posture assump Observe configuration changes and impacts to the security posture |
| Beats | 3 | 40 | Lightweight, (similar to UFs) |
| BitLocker | 4 | 18 | Encrypts all data |
| C2 - Malleable | 3 | 197 | C2 beacons via http/s, or DNS |
| C2 Protocols | 3 | 142 |  |
| CDM | 5 | 10 | Continuous diagnostics and mitigation |
| Certificate Pinning - decrypt traffic | 2 | 92 |  |
| Change Detection | 5 | 97 | Built-in - report changes in real-time Differential - compare current config to prev |
| CIS benchmarks | 4 | 12 |  |
| CIS Hardened images | 4 | 20 |  |
| Client-side exploit | 2 | 21-30 |  |
| Cloud deployment models | 1 | 135 | Public, private, hybrid - Multicloud |
| Cloud service delivery models | 1 | 136 |  |
| Cloud Service Delivery Models | 1 | 136 | IaaS, PaaS, SaaS |
| CloudTrail Insights | 1 | 160 | Raise issue (after baseline) |
| Code Integrity | 4 | 18 | Validates integrity of driver or system file each time loaded into memory |
| Cortex | 5 | 191 | Hive's analysis engine - queries online resources like virustotal, dshield shodan and many others |
| Cost of a data breach | 1 | 35 | Ponemon Institute |
| Credential Compromise | 1 | 36 | camouflauge as legitimate traffic |
| Credential Stuffing | 4 | 124 | Common passwords and credentials compromised by attackers are used against corporate accounts to try and gain access |
| CryptoLocker | 1 | 57-58 |  |
| CSM - focus | 5 | 5 | Focussed on Vulnerabilities and data at rest |
| Data Classification | 5 | 24 | focuses on identifying critical data/systems |
| Data exfiltration | 1 | 87 |  |
| Debug Programs | 4 | 98 | LSA Secrets - decrypt secrets |
| DeepBlueCLI | 5 | 159 | Threat hunting via win event logs |
| DEP |  |  | Data execution prevention (DEP) is a security feature within operating system that prevents applications from executing code from a non-executable memory location. |
| Device Health Attestation (DHA) | 4 | 18 | Allow/deny conditional access |
| DISA STIGS | 4 | 15 | Security Technical Impl Guides |
| DNS over TLS (DoT) | 2 | 170 | TCP port 853 |
| DNS Tunnels | 5 | 81 | ideal c2 channel |
| dnscat2 | 5 | 85 | DNS Tunnel - encrypts all data and then converts to hex before sending over network, CANT TUNNEL IPv4 |
| DNSSEC | 2 | 174 | only encrypts the header |
| DoH | 2 | 171 | 443 - like normal https |
| DSC (desired state config) | 4 | 23 | Powershell based config management platform. define n deploy baseline configs, push/pull state config updates, monitor drift in config state |
| ECH | 3 | 192 | Encrypted Client Hello -- JA3 FAIL |
| ELAM |  |  | Protects computer on start up and before 3rd party drivers initialize |
| Entropy | 3 | 104 | Randomly generated strings |
| Entropy - DGAs | 3 | 116 | Domain generation algos |
| EternalBlue | 4 | 8 | SMB1 exploit |
| Event ID 2003 | 5 | 136 | Firewall enable/disable |
| Event ID 2005 | 5 | 137 | RDP enabled but is common for benign actions |
| Event ID 4672 | 4 | 105 | Any of 13 sensitive provided during logon |
| Event ID 4720 and 4738 | 5 | 126 | User account created/changed |
| Event ID 4735 4737 4755 | 5 | 129 | Changes to domain groups |
| Event ID 7045 | 5 | 122 | Service was installed in the system |
| Event ID 8003 | 4 | 84 | AppLocker audit mode |
| Event ID 8007 | 4 | 87 | AppLocker Enforce mode |
| Event ID Summary | 5 | 147 |  |
| Event IDs 7048 and 4697 | 5 | 119 | Service created |
| file command | 3 | 62 | detemines type of file |
| Forward proxy | 2 | 96 | Detect c2, monitor egress, filter content that violates policy |
| freq.py | 3 | 112 | Detect randomly generated stringsn |
| Full data capture tools | 3 | 58 | Wireshark, tcpdump, netsniff-ng.  Netsniff-ng is designed for high speed networks |
| GeoIP | 2 | 47-48 | Consider legitimate traffic locations |
| Goal of traditional security architecture | 1 | 60 | Prevention oriented |
| Goal Oriented Defense | 1 | 47 | Prevent adversaries achieve goals |
| Hash Bypass | 4 | 81 | Inject executable/dll content into memory |
| Hash storage | 4 | 131 | windows password hashes - c\windows\system32\config\SAM, (only local accounts). Domain hashes reside in active directory. Domain hashes reside in c:\ntds\ntds.dit on domain controllers |
| HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run | 4 | 107 | Maintain persistence |
| Honeypots - Tactical | 2 | 149 |  |
| Honeypots/ honeynets | 2 | 145 | Adversary deception |
| Host based firewall capabilities | 4 | 32 |  |
| HTTP 2 | 2 | 72 | binary protocol - better compression push promise, multiplexed, HPACK |
| HTTP user agent strings | 3 | 155 | OS versions associated with user agents |
| HTTPS - malicious | 3 | 167 | client hello should be frame 4 |
| HTTPS TLS handshake | 2 | 70 |  |
| Hunt Team | 1 | 100 | Presumption of compromise, Focus post exploit detection |
| IaC security issues | 1 | 142 | Fast ! = Secure |
| ICMP | 3 | 143 | ping |
| ICMP SSH Tunnel | 3 | 145 | SSH Banner |
| IDS Alerts | 1 | 72 | Has only a fraction of packets |
| IMPHASH | 4 | 53 | Hashes an executables function or API imports from DLLs. Hashes the dlls in the order they were loaded |
| Infrastructure as code | 1 | 140 | Automation in cloud, supports CI, CD |
| Iodine | 5 | 87 | Offers true routable tunnel via DNS |
| IPFix | 2 | 34-36 | Session flow info: timestamp, src, dest,  icmp, udp/tcp ports, tcp flags, bytes |
| ISCM | 5 | 12 | Info sec continuous monitoring |
| Kibana | 3 | 41 | UI to search the data |
| LANMAN Hash | 4 | 128 | password less than 8 characters |
| LAPS | 4 | 96 | Local Administrator Password solution - sets a random pwd for common local admin account on every computer in the domain |
| Lateral Movement | 1 | 127 |  |
| Layer 3 inbound filtering | 2 | 47 |  |
| Layer 7 aware | 1 | 105 |  |
| LM | 4 | 128 | LAN manager -MS legacy password hash - only supports uppercase, no salts and so on |
| Lockheed Martin: Cyber Kill Chain | 1 | 111 | Post exploit categorization is limited |
| Log on types | 4 | 162 | 2 - interactice, 5 - service, 3 - network |
| LogStash | 3 | 39 | Server-side data processing pipeline (Like HFs) |
| Long Tail Analysis | 5 | 32 | Focus on least frequent occurrences |
| Long tail analysis | 5 | 157 | Inspect the least frequent |
| LSA secrets | 4 | 98 | passwords are stored in HKLM\Security\Policies\Secrets - can be read by accounts that have Debug Programs user privilege |
| LUA Buglight | 4 | 119 |  |
| Magic local admin RID 500 | 4 | 117 |  |
| Magnificent Seven | 4 | 104 | most imp privileges - debug programs, impersonate a client, act as a part of the OS and so on |
| Malware detonation devices | 2 | 139 |  |
| Mandiant M-Trends | 1 | 32 | Recompromise |
| MBSA | 5 | 64 | MS Baseline Security Analyzer - doesn't exist now |
| Microsoft Defender : Application guard | 4 | 33 | Leverages hyper V to instantiate isolated containers separate from underlying OS |
| Microsoft SCT | 4 | 14 | Security Compliance Toolkit, security benchmarks and implementation -- contains tools and scripts |
| MIME / Magic Bytes | 2 | 102 | Content type blocking / alerting. Type of file |
| Mirror ports (Span Ports cisco) | 3 | 96 | Doesn’t forward malformed frames or VLAN tags |
| Mitre attack framework | 1 | 112-113 |  |
| Modern Adversaries |  |  | Web-app + client site attack |
| Modern adversaries goals | 1 | 94 | Hiding and persistence |
| Modern Cyber defense | 1 | 99 | Post exploitation, early detection, Presumption |
| Modern Cyber defense - Response Driven | 1 | 104 | Rapid detection + Response |
| MSSP | 5 | 183 | Monitor 24\*7 |
| ndiff | 5 | 51 | Discover host changes over time |
| NetFlow | 2 | 34-36 | Session flow info: timestamp, src, dest,  icmp, udp/tcp ports, tcp flags, bytes |
| Netwrok Tap + Buffer | 3 | 97-98 | caches frames on overload. captures malformed frames |
| New Security Padadigm | 1 | 48 | Quickly Detect & Respond |
| Next gen firewalls | 2 | 127 | look at data, do reputation checks,  real time user awareness  Block FB chat for particular users |
| ngrep | 3 | 66 | "-q prints matching headers and payloads" "-I uses pcap as input" "MZ OR JOIN" -- String to search Text display packets containing the string |
| NIDS - detection wins | 2 | 116 | C2 detection |
| NIDS - Placement | 2 | 109 |  |
| NIDS Anomaly Detection | 3 | 50 | Learning mode, alert mode |
| NIDS Protocol Behaviour | 3 | 49 | Alert for non-standard protocol usage. False positives for apps not conforming to RFC |
| NIPS - IPS | 2 | 120 | Prevention devices, can inflict DOS |
| NIST 800-137 | 5 | 13 | Define, establish, Implement, Analyze, Respond, Review and update |
| Nmap | 5 | 50 | Command line nmap plus GUI Zenmap |
| NotPetya | 3 | 11 | Uses Mimikatz to steal creds, move laterally via psexec and wmic (windows mgmnt instrumentation console) |
| NSM Sensors | 3 | 94 | full packet capture remains local |
| NSRL | 4 | 70 | National Software Reference Library |
| NT | 4 | 130 | Password hashed but no salts |
| NTFS permissions | 4 | 93 |  |
| OpenAppId | 2 | 130 | identifies web and client-side apps Verify traffic stream contains allowed app data |
| OpenVAS | 5 | 60 | Open source version of nessus |
| p0f version 3 | 5 | 57 | Passively identify OS and some apps too |
| PAC | 2 | 98 | Proxy auto config - Forward proxy IP will be associated |
| Pass-the-hash | 4 | 169-170 | Force uniq passwords for local admins |
| PAT | 4 | 14 | Microsoft Policy Analyzer Tool - assess and compare sec config against policies |
| pcap | 3 | 57 | pcapng - next gen - many tools can't handle its format |
| pcap - Flow data (netflow data) | 3 | 67 | Flow data are summary data, showing socket pairs, protocols, IP addresses, ports, and bytes transferred between hosts |
| Perfect forward secrecy | 2 | 86 |  |
| Perimeter SI Firewall | 2 | 43 | IP based layer 3-4 filtering. Eg. Filter outbound SMTP traffic except from a few mail servers |
| Pivot | 2 | 21-30 |  |
| Ponemon Institute | 1 | 35 | Cost of a data breach |
| Powershell | 4 | 47 |  |
| Powershell - GetMissingUpdates | 5 | 65 | Find missing patches |
| promiscuous network access | 3 | 95 | required for sniffing |
| PSExec | 1 | 128 | Run commands on compromised system Execute without preinstall or physical access |
| QUIC - HTTP 3 | 2 | 74 | Uses port 443, 80. |
| Rainbow tables | 4 | 126 | Windows hash don’t use salt and prone to attacks |
| Ransomware Intro | 1 | 56 |  |
| RDAP -- domain stats - DNS | 5 | 93 | Outputs in JSON - see expiration, registration and update times for various DNS names like sans.org |
| reg query - Remote registry querying | 5 | 155 | HKEY\_CURRENT\_USER (HKCU) is accessed via "HKU" and requires that ".DEFAULT" be added to the path Remote registry start |
| RestrictedAdmin - RDP | 4 | 183 | No delegation token with RDP |
| Reverse Proxy | 2 | 96 | Internet to internal servers |
| RID 500 | 4 | 117 | Built-in local admin account |
| RITA | 2 | 189 | Good tool to detect beaconing |
| RMF 800-37 | 5 | 8 | Categorize, Select, Implement, Assess, Authorize, Monitor |
| Routers | 2 | 33,37 | First and last opportunity. Notify changes via syslog Detects persistent connections over HTTP |
| RPZ | 2 | 165-166 | DNS Firewall - don't resolve this names |
| Safelist | 4 | 63 |  |
| Salts - Windows | 4 | 126 | No salts used for calculating password hashes |
| SAT | 4 | 163 | Security access tokens |
| SCAP | 5 | 60 | CVE, CPE - communicate software flaws |
| Secure Boot | 4 | 18 | Ensure device boots using only trusted manu S/w |
| Security Onion | 3 | 17-23 | Standalone mode for POCs |
| Security Onion - Alert menu - Hunt Menu | 1 | 72-73 |  |
| SeDebugPrivilege | 4 | 105 | Clear text passwords |
| Server-side attack | 2 | 21-30 | 1. Exploiting a vulnerable application on a laptop 2. SQL commands entered into a web form 3. uses a listening port to deliver an attack to the vulnerable device |
| Session-based data | 2 | 34-36 | Data captured from router, srcip, destip, sport, dport, packets, bytes, flags |
| SI Firewall | 2 | 45 | Block rules are essential. Default deny outbound |
| SIEM | 3 | 31 |  |
| Signature matching / based | 3 | 48 | high entropy strings will avoid detection |
| SOC Focus | 5 | 179 | Detecting breaches |
| SOC Technical and business goals OR Purpose of SOC | 5 | 179 | Bussiness goal: reduced disruption resulting from security incidents/issues and reduced impact associated with compromise |
| Software inventory | 5 | 45 |  |
| Splash proxy | 2 | 104 | first time block by default |
| SSL/TLS without HTTPS | 3 | 164 | Common encrypted c2 channel |
| SSPI | 4 | 154 | Allow apps to interface with Microsoft authentication packages for single sign-on via the Windows API |
| Stateful firewalls | 2 | 44 |  |
| String data | 3 | 65 | Sequence of printatble characters |
| Sysmon | 4 | 49 | Generate hashes of all binaries. Capture full command line. Identify application making the request |
| Test before Scan | 5 | 49 |  |
| TheHive | 5 | 190 | Open source platform for SOC and incident response |
| Threat Intelligence | 1 | 115 | TTP - study adversary tactics |
| TLS Decryption - passive | 2 | 81 | Server's RSA priv key OR  client pre-master secret |
| Token Impersonation levels | 4 | 164 |  |
| Tor C2 | 3 | 169 | Onion router |
| TPM | 4 | 18 |  |
| Traditional attacker | 1 | 54 | Infect large numbers |
| Traditional cyber defense architecture | 1 | 63 | Layer 3 and 4 |
| Traditional Malware | 1 | 53 |  |
| Traditional security architecture | 1 | 64 | Devices dependend (perimeter), focus on Decreasing operating costs |
| Transaction Data | 3 | 69 | Flow data + layer 7 content  eg http headers - host, method, content-type, user agent |
| tshark | 3 | 25 | access to display filters. Eg. Display only http post methods in pcap |
| UAC | 4 | 113 | User Account Control |
| VACLs | 2 | 153 | VLAN Access Control Lists |
| Verizon and Mandiant reports |  |  | 3rd party notification of breach |
| Virtual Patching | 2 | 58 | WAF |
| VPC detection and Monitoring -- Flow logs | 1 | 177 | L3/ L4 network details |
| Vulnerability scanning | 5 | 58 |  |
| VulnWhisper | 5 | 61 | Aggregates and correlates info from a wide range of vul scanning tools |
| WAF - placement | 2 | 60 | front of the web app |
| Watering hole | 2 | 21-30 | Client site exploit |
| WDFAS OR WFAS | 4 | 30 | Windows Defender firewall with Advanced Security - managed via group policy, egress filtering, n/w loc aware, stateful packet filtering, local logging Log file location: C:\Windows\System32\LogFiles\Firewall\pfirewall.log |
| WDigest | 4 | 156 | Clear text passwords in memory |
| Web application attack scenario | 2 | 16-20 |  |
| Web application firewall | 2 | 57 | TLS termination + Virtual Patching |
| Window update agent WUA | 5 | 64 | Scan a system for deviations from the expected updates. |
| Windows Hello | 4 | 133 | Pin or biometric verification used on personal device |
| Windows Versions in User Agent Strings | 3 | 155 |  |
| Wow6432node | 3 | 107 | 32 bit on 64 bit os |
| Wow6432node | 5 | 154 | 32bit on 64 bit windows |
| WPAD - config clients to use proxy | 2 | 98-99 | web proxy auto-discovery protocol. NULL record return to prevent MITM |
| WSUS server | 3 | 51 | Windows Server Update Services |
| X.509 | 3 | 174-178 | short issuer field is suspect + missing O& C |
| Zeek | 3 | 27-28 | carve exe from pcap.  zeek-cut simple carves out the fields to view. |
| zeek - wierd.log | 3 | 70 | provides transaction data that doesn't conform to the standard (RFC) |
| Zeek-cut | 5 | 88 | Specify fields to show |
| Zenmap | 5 | 50 | GUI nmap |
| Zero Trust | 2 | 7 |  |
| Zone.Identifier ADS | 4 | 66 | Indicates the network zone (Alternate data stream). 3 is from internet, 2 is from trusted site |