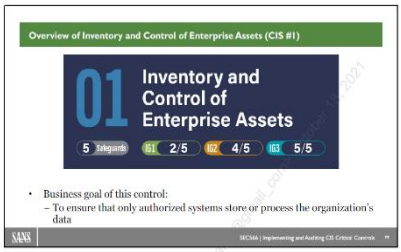
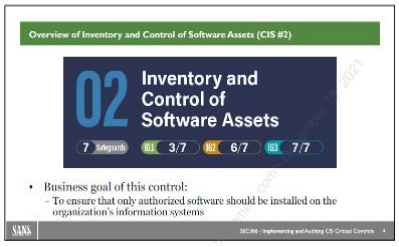
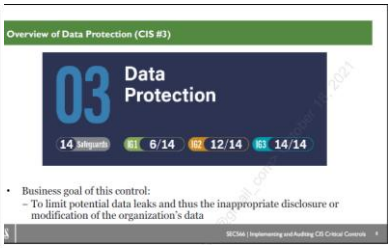
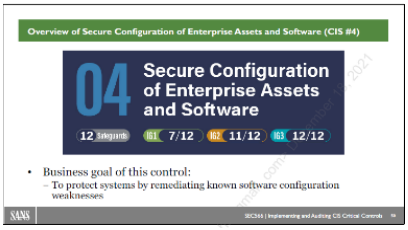
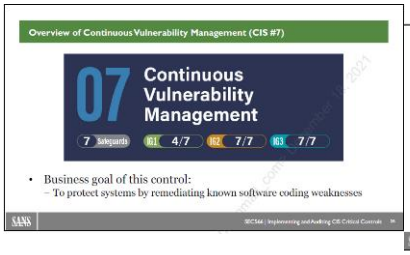
Implementing and Auditing the Critical Security Controls Index

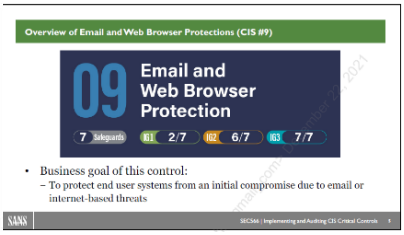


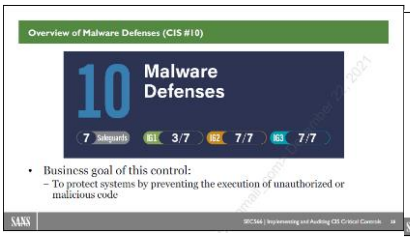


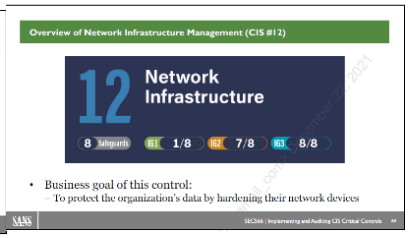


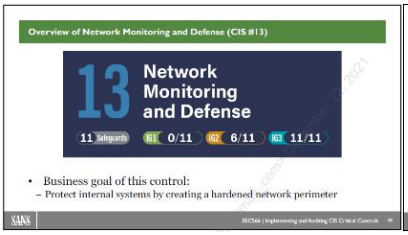


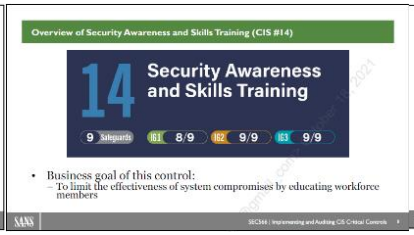


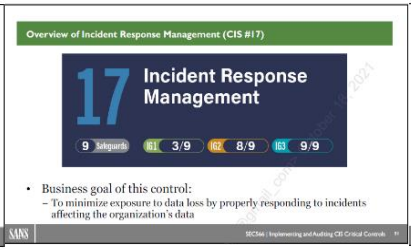


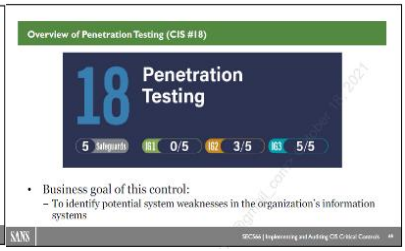












#8

800-171 *[b1/p42]* Protecting controlled

800-30 *[b1/p42]* Guide for conducting RA

800-37 *[b1/p42]* Guide for applying RA

800-39 *[b1/p42]* Managing information security Risk

800-53 *[b1/p42]* Security and Privacy control

802.1X C#12.6 *[b4/p64]* secure network communication protocols

Aa

AAA C#12.5 *[b4/p64]*

Access Auditor (SCC) C#5 *[b2/p42]* Commercial Tool

Access Auditor (SCC) C#6 *[b2/p62]* Commercial Tool

Access cntrol lists (ACL)C#3.3 *[b2/p9]*

Accessing administrative interfaces C#4.6 *[b3/p54]* TO managing configuration

Active Directory Group Policies (Microsoft) C#4 *[b3/p63]* Commercial Tool

AD Audit Plus (ManageEngine) C#6 *[b2/p62]* Commercial Tool

AD Audit Plus C#6 *[b2/p61]* Sample tool. Active Directory auditing and Compliance compnent useful for regulated industries such as insurance , banking and & healthcare. AD Audit Plus User Account Report details the user account name, client hostname , logon time, the failure reason the failure type and Microsoft SID identifier

AD Reports (MaxPowerSoft) C#6 *[b2/p62]* Commercial Tool

ADSI Queries C#6 *[b2/p63]* Free Tool

AlienVault Unified Security Management (AT&T) C#8 *[b2/p85]* Commercial Tool

Amanda C#11 *[b4/p54]* Free Tool

Apple FileVault C#3.6 *[b2/p10]* Data encryption

Application layer firewall C#13.10 *[b4/p87]* application layer filtering

Application-layer encryption C#3.11 *[b2/p11]* client-side encryption

AppLocker (Microsoft) C#2 *[b3/p19]* Free Tool

Archer SmartSuite tool C#17 *[b5/p62]* has the ability to analyze and manage each of the following areas: 1- Policy Management 2- Threat Management 3- Asset Management 4- Risk Management 5- Business Continuity

Areca C#11 *[b4/p54]* Free Tool

Arkime (Moloch) C#13 *[b4/p97]* Free Tool

Armitage C#1 *[b1/p80]* Is an attack tool that provide graphical front end to many common attack tools, most important to "Metasploit"

ARP cache tables on switches *[b1/p84]* Passive inventory tools

ARP cache tables on Wireless access points C#1.5 *[b1/p84]* Passive inventory tools

ARP Caches C#1 *[b1/p88]* Passive Scan

Attachment scanning C#9.7 *[b4/p9]* It's email server anti-malware protections

Attestation of Compliance (AoĆ) C#15.5 *[b5/p24]* Standardiżed assessment reports for service providers

Audit logs C#8 *[b2/p73-74]* can help us reliably observe what has happened on our systems, and, collectively, on our networks. Configured correctly, they can help us prevent or detect violations of confidentiality, integrity, and availability.

AuditScript CIS Control Assessment Tool *[b1/p25]* Security control-centric view of risk assessment and scores the organizaton , it's self-assessment tool, based in CIS Control project , NIST 800-53 ISO27002:2013

AuditScript CIS Control Assessment Tool Visualized *[b1/p26]* Manually measures progress until the sensors deployed to automate the collection of information

Australian ACIS Essential Eight *[b1/p39]* Mitigate incident by prioritization list of mitigation strategies, 1- Application Whitelisting 2- Patch Application 3- Configure Microsoft Office Macro Settings 4- Using Application Hardening 5- Restrict Administrative Privileges 6- Patch Operating Systems 7- Multi-Factor Authentication 8 - Daily Backups

Authentication systems C#5 *[b2/p40]* To production systems and Standard and administrative user accounts

Automated Patch Management C#7.3 and 4 *[b3/p32]* Perform OS and application updates

Bb

BackupExec (Symantec) C#11 *[b4/p53]* Commercial Tool

Backups C#11 *[b4/p46]* should include the operating system binaries, application software binaries, and the data located on each machine.

Bacula C#11 *[b4/p54]* Free Tool

Black Hills Information Security (BHIS) *[b1/p45]*

Blackhole Exploit Toolkit C#2 *[b3/p6]* attack tool. installed on web server & pre-confgiured to attack out of date code running on the machine

Block lists C#9.3 *[b4/p8]* to limit an enterprise asset from connecting to potentially malicious or unapproved websites.

Blue Coat URL Filtering C#9 *[b4/p15]* Commercial Tool

BlueCat IPAM C#1 *[b1/p92]* Commercial Tool

Cc

Cat C#6 *[b2/p63]* Free Tool

Cat/Diff C#5 *[b2/p43]* Free Tool

Category-based filtering C#9.3 *[b4/p8]* Network-based URL filters

CB Protection (Carbon Black) C#2 *[b3/p18]* Commercial Tool

Center for Internet Security(CIS) *[b1/p12]* Maintain community efforts EX:(sec benchmark, sec metrics, CIS controls, MS-ISAC)

Change Auditor (Dell Quest) C#5 *[b2/p42]* Commercial Tool

Change Auditor (Quest) C#6 *[b2/p62]* Commercial Tool

Chef Server (Chef) C#4 *[b3/p63]* Commercial Tool

CIS Goal *[b1/p7]* Defending system as part of community RA model

CIS-Implementation Groups *[b1/p18]* These tags is to help orgaizations to understand which control most applicable. Three types: 1- limited, 2-moderate, 3- significant.

Cisco Adaptive Security Appliance (ASA) C#13 *[b4/p96]* Commercial Tool

Cisco Firepower Firewall (Cisco) C#13 *[b4/p96]* Commercial Tool

Cisco OpenDNS (208.67.222.222, 208.67.220.220) C#9 *[b4/p16]* Free Tool

Cisco Prime (Cisco) C#12 *[b4/p72]* Commercial Tool

ClamAV C#10 *[b4/p35]* Free Tool + Automation Script

Clear-EventLog C#8 *[b2/p75]* Commands in Microsoft PowerShell . compromised the system owner, clear logs, limit owner ability to perform incident handling.

Clonezilla C#11 *[b4/p54]* Free Tool

Cloud service provider (CSP) C#13.3 *[b4/p85]*

Cloudflare DNS (1.1.1.2, 1.1.1.3) C#9 *[b4/p16]* Free Tool

Code Green TrueDLP C#3 *[b2/p19]* Commercial Tool

Code scanning tools C#16 *[b5/p37]* To validate that there are no weaknesses in the code they are developing, against both production and development systems

Collect audit logs C#8.2 *[b2/p77]*

Collective risk model *[b1/p44]* practical approach to risk management, useable approach, ack limitation of quantitative model

Collective threat model Open Threat Taxonomy (OTT) *[b1/p50]* catalog all potential threats. focus in threat action. help standardize RA. community RA methodology.

collectives control catalog (CCC) *[b1/p51]* analyze control from 35+ standards. normalize 2000 control to 400.

Collectives Risk Model (CRM) *[b1/p51]*

Collectives Security Control Catalog *[b1/p52 - 55]* 1-inventory 2-normalize and mapping 3-coverage 4-prioritization and tagging

Collectives Threat Model (CTM) *[b1/p50]* also formerly Known as OTT

Compete Security Suite (Sophos) C#10 *[b4/p34]* Commercial Tool

Configuration Manager (LANDesk) C#4 *[b3/p63]* Commercial Tool

Configuration Profile C#4.12 *[b3/p56]* Apple , to seprate enterprise applications and data from personal applications and data.

Configuration Profile maxFailedAttempts C#4.10 *[b3/p56]* Apple ,for automatic device lockout

Control Compliance Suite Vulnerability Scanner (Symantec) C#7 *[b3/p40]* Commercial Tool

Controls, Measure, Metric, Maturity *[b1/p28]*

Cryptograph C#11 *[b4/p52]* Sample tool. is an audit tool by Enclave Forensics used to examin data streams, store files, to determine frequency count of characters used in a file. quick view to check if the file is encrypted or not

CryptoLocker C#11 *[b4/p47]* It's Attack code, has been known to attack both live and backup data sets

CS Maturity Model Certification (CMMC) *[b1/p43]* manage (DIB), approved private sector, based on NIST SP 800-171 with additional control

CSVDE C#6 *[b2/p63]* Free Tool

Customized questionnaires C#15.5 *[b5/p24]* Standardiżed assessment reports for service providers

CyberSecurity control standards *[b1/p36]* CIS, NIST SP 800-171, CMMC, NIST CS FRAMEWORK, ISO 27002:2013, ACIS, CAT, PCI DSS

Cybersecurity Standards *[b1/p35]* The goal to clarify what defenses available for organization to be ableto defend itself

Dd

Data Classification scheme C#3.7 *[b2/p10]* Sensitive , Confidential and Public

Data Disposal C#3.5 *[b2/p10]*

Data encryption C#3 *[b2/p10]*

Data Execution Prevention (DEP) C#10.5 *[b4/p29]* Microsoft® ,anti-exploitation features

Data Loss Prevention (DLP) C#3 *[b2/p5]*

Data Protector (HP) C#11 *[b4/p53]* Commercial Tool

Data Retention C#3.4 *[b2/p10]* Must include both minimum and maxmum timelines

Database logs C#8 *[b2/p73]* can record when data manipulation commands were executed on data tables and which accounts executed those commands.

Default configuration C#4 *[b3/p50]*

Defender Exploit Guard (WDEG) C#10.5 *[b4/p29]* Windows® anti-exploitation features

Defense Industrial Base (DIB) *[b1/p43]*

Device logs from IDS/IPS systems *[b1/p84]* Passive inventory tools

Device logs from packet capture tools C#1.5 *[b1/p84]* Passive inventory tools

DHCP Logs C#1.5 *[b1/p84]* Passive inventory tools

Directory C#5.6 *[b2/p35]* To centralize account management

Directory Servise C#6.7 *[b2/p56]* To centralize access control

DMARC policy C#9.5 *[b4/p9]* To lower the chance of spoofed or modified emails from valid domains

DNS filtering services C#9.1 *[b4/p8]* to block access to Known malicious domains

DNS query logging C#10 *[b4/p29]* to identify where known command and control domains or malicious domains have been accessed. This will help incident handlers to more quickly identify the scope of an incident and identify those machines that have executed specific malicious binaries.

DNSExfiltrator C#13 *[b4/p83]* attack tool , used to move data covertly over DNS

Document Contributors *[b1/p13]* 1- International Contributors 2- US Contributors

Domain-level administrator account C#5 *[b2/p29]* In Microsoft Windows environments

DomainKeys Identified Mail (DKIM) standards C#9.5 *[b4/p9]*

Dormant account C#5.3 *[b2/p34]* Delete or disable after 45 days

DREAD Program C#16 *[b5/p41]* Threat modeling process for prioritizing the severity of the weakness so development efforts can also be prioritized

Ee

ELK/Logstash C#8 *[b2/p86]* Free Tool

Enclave DAD/LASSIE *[b2/p86]* Free Tool

Enclave Security / AuditScripts *[b1/p45]*

Encryption methods C#3.11 *[b2/p11]* 1- Storage-layer encryption 2- Application-layer encryption

Endpoint Detection and Response (EDR) clien C#13.7 *[b4/p86]* host-based intrusion prevention solution

Endpoint Security (Tanium) C#10 *[b4/p34]* Commercial Tool

Endpoint Security (Triumfant) C#10 *[b4/p34]* Commercial Tool

Enterprise Security for Endpoints (Trend Micro) C#10 *[b4/p34]* Commercial Tool

Enterprise Security Manager (HP Arcsight) C#8 *[b2/p85]* Commercial Tool

ePolicy Orchestrator (EPO) C#10 *[b4/p33]* sample tool. traditional anti-malware consoles ,to stop the potential infection of systems by malicious code.

ERD *[b1/p23-24]* One of the 14 types of UML(Structure), referred to as Class Diagram, it's useful during implementaion and evaluate.

ESM/NitroSecurity C#13 *[b4/p95]* ability to gather more information about unusual traffic

Event Correlation (Infogressive) C#8 *[b2/p85]* Commercial Tool

Event logs C#8 *[b2/p73]* can record what applications or processes started or stopped, who started and stopped them, and when

Ff

File Integrity Assessment tools (FIA) C#4 *[b3/p55]* TO detect and respoond unauthorized chages to systems.

Filtering proxy C#13.10 *[b4/p87]* application layer filtering

FireEye Network IPS C#13 *[b4/p96]* Commercial Tool

FireMon C#12 *[b4/p72]* Commercial Tool

Firewall Analyzer and FireFlow (AlgoSec) C#12 *[b4/p72]* Commercial Tool

Firewall Assurance (Skybox Security) C#12 *[b4/p72]* Commercial Tool

Firewall on Servers C#4.4 *[b3/p54]*

Firewall Security Manager (SolarWinds) C#12 *[b4/p72]* Commercial Tool

Forcepoint C#9 *[b4/p14]* Sample tool

Forcepoint/Websense Triton URL Filtering C#9 *[b4/p15]* Commercial Tool

Fortinet FortiGate C#13 *[b4/p96]* Commercial Tool

Fortinet FortiGate C#3 *[b2/p19]* Commercial Tool

Gg

Gatekeeper C#10.5 *[b4/p29]* anti-exploitation features

Gateway C#13.10 *[b4/p87]* application layer filtering

Get-Eventlog C#8 *[b2/p87]* Automation Script

Get-EventLog/Get-WinEvent C#8 *[b2/p86]* Free Tool

Get-LocalGroupMember C#5 *[b2/p44]* Automation scripts

Get-WMIObject / Get-CIMInstance C#2 *[b3/p19]* Free Tool

Get-WMIObject/Get-CIMInstance C#4 *[b3/p64]* Free tool

Get-WMIObject/Get-CIMInstance C#5 *[b2/p43]* Free Tool

Get-WMIObject/Get-CIMInstance C#6 *[b2/p63]* Free Tool

Governance Program Domains *[b1/p61]*

Granting access C#6.1 *[b2/p55]*

Graylog C#8 *[b2/p86]* Free Tool

Group memberships C#5 *[b2/p40]* To managed user accounts

Guiding Principles *[b1/p15]* 5 Guiding Principles : 1-Address most common attack(not academic but real) 2-Ensure consistent control 3- Automated measurement 4- Address current attack (technical) 5- Measure the effectiveness of sec measurement

Hh

HEAT / Lumension C#2 *[b3/p18]* Commercial Tool

Host-based Data Loss Prevention (DLP) tools C#3.13 *[b2/p12]*

Host-based firewall C#4.5 *[b3/p54]* on end user devices

Host-based intrusion detection C#13.2 *[b4/p85]*

Host-based IPS agent C#13.7 *[b4/p86]* host-based intrusion prevention solution

Ii

Identity service C#5.6 *[b2/p35]* To centralize account management

Information Security Management System (ISMS) *[b1/p40]*

Initial Compromise C#9 *[b4/p5]* 1- Spear phising attack (email based) 2- watering hole attack (web based) 3- web application server attack (server based)

InsightVM / Nexpose (Rapid7) C#4 *[b3/p63]* Commercial Tool

InsightVM / Nexpose (Rapid7) C#7 *[b3/p40]* Commercial Tool

Institute of Applied Network Security (IANS) *[b1/p45]*

Intune Device lock C#4.10 *[b3/p56]* Microsoft ,for automatic device lockout

Invincea Enterprise C#9 *[b4/p15]* Commercial Tool

IP Address Management (IPAM) tools C#1.5 *[b1/p84]* Passive inventory tools

IP360 (Tripwire nCircle) C#7 *[b3/p40]* Commercial Tool

IronPort WSA/ESA (Cisco) C#9 *[b4/p15]* Commercial Tool

ISO 27002:2013 *[b1/p40]* Paired with ISMS, focus on governance, operational, software development

Jj

Jamf Pro/Casper (Jamf) C#4 *[b3/p63]* Commercial Tool

John the Ripper C#4 *[b3/p51]* Attack tool. ability to crack password hashes provided to it given enough time and CPU Cycle to work.

Kk

Key Performance Indicators (KPIs) *[b1/p28]*

Kiwi CatTools C#12 *[b4/p73]* Free Tool

Ll

LANMAN Hash C#4 *[b3/p51]* Unsalted

LANSurveyor (SolarWinds) C#1 *[b1/p92]* Commercial Tool

Lansweeper C#1 *[b1/p92]* Commercial Tool

Lansweeper C#2 *[b3/p18]* Commercial Tool

LDAP C#5 *[b2/p29]* To extend the privileges in Unix/Linux

Linux dm-crypt C#3.6 *[b2/p10]* Data encryption

Local Administrator Password Solution (Microsoft LAPS) C#5 *[b2/p43]* Free Tool

Log Correlation Engine (Tenable) C#8 *[b2/p85]* Commercial Tool

Log management systems C#5 *[b2/p40]* To logged administrative access to systems

Log management systems C#6 *[b2/p60]* Generate user account and access reports for management

LogParser (Microsoft) C#8 *[b2/p86]* Free Tool

LogParser C#9 *[b4/p16 +17]* Free tool + automation script

Lynis C#2 *[b3/p19]* Free Tool

Lynis C#4 *[b3/p64 + 65]* Free tool + automation script

Mm

ManageEngine OpUtils C#1 *[b1/p92]* Commercial Tool

Maturity Model Score *[b1/p27]* 5 Levels: L1: Documentation, L2: Implement 1-5 ,L3: Fully implemented, L4: Automated , L5: Reported

McAfee DLP C#3 *[b2/p19]* Commercial Tool

McAfee End Point Protection (McAfee) C#10 *[b4/p34]* Commercial Tool

Metasploit C#18 *[b5/p78]* Pentest sample tool. allow system admin to perform PT against the boundary system they are protecting , run exploit code against vulnerable system

Metasploit C#7 *[b3/p29]* CIS 7 attack tool. writen by HD Moore, ability to allow attackers to easily execute exploit code against target system. Meterpreter module : (run arp_scanner..etc)

MFA C#5.2 *[b2/p34]* 8-character password for account using MFA, 14-character password for account not using MFA

Microsoft Baseline Security Analyzer C#4 *[b3/p64]* Free tool

Microsoft Office365 Email Filtering C#9 *[b4/p15]* Commercial Tool

Microsoft PowerShell Get-WMIObject C#6 *[b2/p64]* automation scripts

Microsoft RunAs tool C#5 *[b2/p35]* to use administrative or elevated accounts

Microsoft's STRIDE Program C#16 *[b5/p41]* Threat modeling process for prioritizing the severity of the weakness so development efforts can also be prioritized

Mimecast Email Filtering C#9 *[b4/p15]* Commercial Tool

Mimikats C#5 *[b2/p32]* attack tool. tool to retrieving a system credentials, read data from memory , DLL, LSASS , Sekurlsa.dll

MITRE ATT&CK Model *[b1/p11]* Attack lifecycle:1-Recon 2-weaponize 3-deliver 4- exploit 5-control 6-excute 7- maintain

MS-ISAC *[b1/p12]* Multi-State Information Sharing and Analysis Center

Multi-Factor Authentication Tools (Various) C#5 *[b2/p42]* Commercial Tool

Nn

Nemesis/Hping3 C#3 *[b2/p20]* Free Tool

NET/WMIC C#6 *[b2/p63]* Free Tool

NetBackup (Symantec) C#11 *[b4/p53]* Commercial Tool

NetFlow Analyzer C#3 *[b2/p18]* monitoring and network forensics tool. how is talking to who? EX: Firewall

NetFlow Protocol C#13 *[b4/p86]* To track and record the flow of traffic entering and leaving the network

NetVault (Dell) C#11 *[b4/p53]* Commercial Tool

Network Advisor (RedSeal) C#12 *[b4/p72]* Commercial Tool

Network Configuration Manager (SolarWinds) C#12 *[b4/p72]* Commercial Tool

Network Instruments Observer C#3 *[b2/p19]* Commercial Tool

Network Intrusion Detection System (NIDS) C#13.3 *[b4/p85]*

Network Intrusion Detection Systems (Various) C#10 *[b4/p34]* Commercial Tool

Network Intrusion Detection Systems (Various) C#3 *[b2/p19]* Commercial Tool

Network Intrusion Prevention System (NIPS) C#13.8 *[b4/p87]* network intrusion prevention solution

Network Miner C#13 *[b4/p97]* Free Tool

Network Sniffing C#1 *[b1/p88]* passive scan

Network Storage Server (FalconStor) C#11 *[b4/p53]* Commercial Tool

Network-based Data Loss Prevention (DLP) tools C#3.13 *[b2/p12]* to detect and block attempts to exfiltrate data from the organization

Network-based URL filters C#9.3 *[b4/p8]* To limit an enterprise asset from connecting to potentially malicious or unapproved websites.

NEWT Professional (Komodo) C#2 *[b3/p18]* Commercial Tool

NEWT Professional C#2 *[b3/p16]* sample tool. Network scanning tool ,information about the system: CPU, BIOS, Serial,...etc. create qucik visual network diagrams

Next Generation Firewall (Intel Security) C#13 *[b4/p96]* Commercial Tool

Ngrep C#3 *[b2/p20+21]* Free Tool + Automation Script

Nipper C#12 *[b4/p73 +74]* Free Tool + Automation Script

Nipper Studio (Titania) C#12 *[b4/p72]* Commercial Tool

Nipper-NG C#12 *[b4/p73]* Free Tool

NIS C#5 *[b2/p29]* To extend the privileges in Unix/Linux

NIS+ C#5 *[b2/p29]* To extend the privileges in Unix/Linux

NIST CSF *[b1/p41]* defend critical infrastructure. five core area: identify, protect, detect, respond, recover

NIST SP 800-171 *[b1/p42]* Framework for protection controlled unclassified info. (CUI) in non-federal system. taken from NIST SP 800-53. defines tech infrastructure, some GOV. and Operations controls

Nmap C#1 *[b1/p93-94]* Free Tool + Automation Script

Nmap NSE C#7 *[b3/p42]* Automation script

Nmap Scripting Engine C#7 *[b3/p41]* Free Tool

NTLMv2 C#4 *[b3/p51]* Salted

Oo

Open Log Management (LogLogic) C#8 *[b2/p85]* Commercial Tool

Open Log Management (LogLogic) C#8 *[b2/p85]* Commercial Tool

Open Secure Shell (OpenSSH) C#3.10 *[b2/p11]* Encrypt sensitive data in transit

OpenDLP C#3 *[b2/p20]* Free Tool

OpenDNS (Cisco) C#9 *[b4/p15]* Commercial Tool

OpenVAS C#7 *[b3/p39+41]* sample tool. Open Vulnerability Assessment System & network Security Scanner with graphical user front end. NVTs , GNU GPL, fork Nessus + Free Tool

Operational Security Domains *[b1/p62]*

OWASP TOP 10 vulnerability awarness C#14.9 *[b5/p9]*

Pp

Palo Alto Networks Firewall C#13 *[b4/p96]* Commercial Tool

Palo Alto Networks URL Filtering C#9 *[b4/p15]* Commercial Tool

Patch Management System C#7 *[b3/p38]* Applies software updates to production systems

Payment Card Industry (PCI) C#15.5 *[b5/p24]* Standardiżed assessment reports for service providers

phpIPAM C#1 *[b1/p93]* Free Tool

Pi-hole C#9 *[b4/p16]* Free Tool

Poison Ivy Remote Access Trojan C#10 *[b4/p26]* Attack tool. graphical tool gives attacker ability to customize malicious code with simple Microsoft Windows. Ability to start services,chnage registry key, start network sniffer...etc. organization should detect binaries of it to stop it

Port-filtering tools C#4.5 *[b3/p54]* on end user devices

Port-level access control C#13.9 *[b4/p87]* utilizes 802.1x

PowerBroker (BeyondTrust) C#5 *[b2/p42]* Commercial Tool

PrivecyRights.org *[b1/p10]* Maintain chronology of data breaches, searchable DB, by year/cause/industry

Privilege Guard (Avecto) C#2 *[b3/p18]* Commercial Tool

Privilege Guard (Avecto) C#5 *[b2/p42]* Commercial Tool

Privileged Account Security Solution (CyberArk) C#5 *[b2/p42]* Commercial Tool

Privileged Password Manager (Dell Quest) C#5 *[b2/p42]* Commercial Tool

Production data sets C#6 *[b2/p60]* User accounts must have permissions set in it

Production systems C#6 *[b2/p60]* To managed user accounts

Proofpoint Email Filtering C#9 *[b4/p15]* Commercial Tool

Protect (Cylance) C#10 *[b4/p34]* Commercial Tool

Puppet Enterprise (Puppet Labs) C#4 *[b3/p63]* Commercial Tool

Qq

Qradar (IBM) C#8 *[b2/p85]* Commercial Tool

Quad9 (9.9.9.9) C#9 *[b4/p16]* Free Tool

Qualys Cloud Platform (QualysGuard) C#1 *[b1/p92]* Commercial Tool

QualysGuard (Qualys) C#7 *[b3/p40]* Commercial Tool

QualysGuard C#4 *[b3/p62 +63]* Sample tool. QualysGuard Vulnerability Managment automates the life cycle of the network & Vulnerability management across the enterprise , comprehensive reports , security level, time to fix and impact in the business. SaaS (software-as-a-Service) no infrastructure to deploy or manage , Commercial Tool

Rr

RANCID C#12 *[b4/p73]* Free Tool

Rapid7 C#7 + C#4 *[b3/p40 + 63]* Commercial Tool

Rapid7 InsightVM (Nexpose) C#1 *[b1/p92]* Commercial Tool

Redo C#11 *[b4/p54]* Free Tool

Remove-EventLog C#8 *[b2/p75]* Commands in Microsoft PowerShell . compromised the system owner, clear logs, limit owner ability to perform incident handling.

Reputation-based filtering C#9.3 *[b4/p8]* network-based URL filters

Retain audit logs C#8.10 *[b2/p79]* For minimum of 90 days

Retina (BeyondTrust) C#7 *[b3/p40]* Commercial Tool

Revision History *[b1/p31]*

Revoking access C#6.2 *[b2/p55]*

Risk Management Categories *[b1/p46]* 1- purpose of control: identify list of control(what control to implement) . 2- purpose of gap analysis: implement appropriate control (how mature).)

Risk management maturity levels *[b1/p48]* 1- inetial 2-managed 3-defined 4-quantitatively defined 5- optimized

Risk Management Process Steps *[b1/p47]* 1- threat inventory 2-threat modeling 3-control inventory 4-map threats to control 5-control prioritization 6-asset classification 7-control implementation 8-control validation 9-risk reporting 10-risk respond

rm C#8 *[b2/p75]* Commands in linux. compromised the system owner, clear logs, limit owner ability to perform incident handling.

Role-based access control C#6.8 *[b2/p57]*

RouterSploit C#12 *[b4/p61]* attack tool. ability to pair specific router of firewall vulnerabilities with payloads to make the process of compromising a perimeter facing system easier

RSA Archer C#17 *[b5/p62]* Sample tool. incident response management.

RSA/Tablus DLP C#3 *[b2/p19]* Commercial Tool

Ss

SAINT and SAINTmanager (SAINT) C#7 *[b3/p40]* Commercial Tool

SamSam (MSIL) Ransomware C#11 *[b4/p44]* attack tool.

Sandboxing C#9.7 *[b4/p9]* It's email server anti-malware protections

SANS Institute *[b1/p45]*

Scapy C#3 *[b2/p20]* Free Tool

SecureID (RSA) C#6 *[b2/p62]* Commercial Tool

Security awareness website C#14 *[b5/p15]* Sample tool

Security Blanket (IBM) C#4 *[b3/p64]* Free tool

Security Compliance Corp (SCC) Access Auditor C#5 *[b2/p41]* sample tool, privileges management suite

Security Content Automation Protocol (SCAP) C#7 *[b3/p31]* To scan information systems in a standard way to detect the weaknesses or vulnerabilities that might be present on those systems.The two SCAP protocols most often used for this measurement purpose are: 1- The Common Vulnerability Scoring System (CYSS) 2 -The Common Configuration Scoring System (CCSS)

Security Governance Controls *[b1/p59 - 60]*

Security Onion C#13 *[b4/p97]* Free Tool

Security Policy Orchestration Solution (Tufin) C#12 *[b4/p72]* Commercial Tool

Sender Policy Framework (SPF) C#9.5 *[b4/p9]*

Service Organization Control 2 (SOC 2) C#15.5 *[b5/p24]* Standardiżed assessment reports for service providers

Service provider data flows C#3.8 *[b2/p11]* Data flow documentation

ServiceNow Discovery C#1 *[b1/p92]* Commercial Tool

SIEM C#13.1 *[b4/p85]* To Centralize security event alerting across enterprise assets for log correlation and analysis

SIEM Correlation Server (CorreLog) C#8 *[b2/p85]* Commercial Tool

SIEM platform C#6 *[b2/p57]*

Simpana (Commvault) C#11 *[b4/p53]* Commercial Tool

Six Sigma *[b1/p29]* Quality Management program, define thresholds for maturity, standard for acceptable risk, percentage . used in metrics phase.

Skybox Secure solution (Skybox security) C#7 *[b3/p40]* Commercial Tool

SMP Connections C#7 *[b3/p32]* Windows systems use local administrator credentials

Social Engineering Toolkit (SET) C#9 *[b4/p6]* sample attack tool , penetration testing and proof of concept tool to facilitate email and web-based attack. Integrate with Rapid7 Metasploit framework.

SolarWinds IP Address Tracker C#1 *[b1/p91]* (Zenmap ,Nmap) This tool has a Scan feature that monitors the network for new devices , changes and unkonwn systems , also configurd to alert security analysts

SolarWinds IP Address Tracker C#1 *[b1/p93]* Free Tool

SolarWinds IPAM C#1 *[b1/p92]* Commercial Tool

Sourcefire IPS (Cisco) C#13 *[b4/p96]* Commercial Tool

Sourcefire Snort C#13 *[b4/p97]* Free Tool

Spiceworks C#1 *[b1/p93]* Free Tool

Spiceworks C#2 *[b3/p19]* Free Tool

Splunk C#8 *[b2/p84]* sample tool. Key indicators for securital information in dashboard. escalation decision easy.

Splunk Enterprise (Splunk) C#8 *[b2/p85]* Commercial Tool

SSH Service C#7 *[b3/p32]* Unix Systems use SSH credentials

SSO provider C#6.7 *[b2/p56]* To centralize access control

Standards focus on *[b1/p37]* 1- GOV controls, 2-operation controls, 3- technical infrastructure control, 4-software dev control, 5-consumer privacy control

StealthWatch (Lancope) C#13 *[b4/p96]* Commercial Tool

Storage-layer encryption C#3.11 *[b2/p11]* Server- side encryption

Subterfuge MITM C#6 *[b2/p53]* attack tool. is an all-purpose man in the middle attack tool, act as proxy , LAN layer 2 attacks (ARP poisoning) , IP impersonation, social engineering, HTTP injection, DNS Spoofing, credential harvesting , deliver false software update.

Sudo C#5 *[b2/p43]* Free Tool

Supporting Documents *[b1/p17]*

Symantec Endpoint Protection (Symantec) C#10 *[b4/p34]* Commercial Tool

Symantec/Vontu DLP *[b2/p19]* Commercial Tool

Synchronization C#8.4 *[b2/p77]* at least two synchronized time, can performed by standard log formats or log aggregators

Syslog-NG C#8 *[b2/p86]* Free Tool

System Center (Microsoft) C#6 *[b2/p62]* Commercial Tool

System Center (Microsoft) C#2 *[b3/p18]* Commercial Tool

System Center and Active Directory (Microsoft) C#5 *[b2/p42]* Commercial Tool

System Integrity Protection (SIP) C#10.5 *[b4/p29]* Apple® anti-exploitation features

Tt

Tenable Nessus (Tenable.io) C#1 *[b1/p92]* Commercial Tool

Tenable.io / Nessus (Tenable) C#4 *[b3/p63]* Commercial Tool

Tenable.io/Nessus (Tenable) C#7 *[b3/p40]* Commercial Tool

Titania Nipper C#12 *[b4/p71]* Sample tool. Parse the configuration file in order to evaluate a proper security settings: Bay network, Checkpoint, Cisco.

Titus DLP *[b2/p19]* Commercial Tool

Traffic filtering C#13.4 *[b4/p86]* between network segments

Transport Layer Security (TLS) C#3.10 *[b2/p11]* Encrypt sensitive data in transit

Tripwire Enterprise C#12 *[b4/p72]* Commercial Tool

Tripwire Enterprise C#4 *[b3/p63]* Commercial Tool

Tripwire Enterprise C#5 *[b2/p42]* Commercial Tool

Tripwire Enterprise Viewfinity (CyberArk) C#2 *[b3/p18]* Commercial Tool

True Image (Acronis) C#11 *[b4/p53]* Commercial Tool

Trusted Access (Duo) C#6 *[b2/p62]* Commercial Tool

TShark/Tcpdump C#13 *[b4/p97 + 98]* Free Tool + Automation Script

Tshark/TCPDump C#3 *[b2/p20]* Free Tool

Uu

UML Diagrams *[b1/p21-22]* Unfied Modeling Language , 14 types, 3 categories(1- Structure, 2-Behavior 3-Interaction) , Combines elements: data, business and object modeling , helps developrs

Unix Sudo/Su tools C#5 *[b2/p35]* To use administrative or elevated accounts

USB Rubber Ducky C#3 *[b2/p7]* Physical tool like an authenticate token & storage device. Write their code using batch-like scripting language. Ways to remediation: disable usage of removable media

Vv

V7.1 CIS control defenses *[b2/p96 -99]*

Varonis Data Classification Engine C#3 *[b2/p19]* Commercial Tool

Veeam Backup and Replication (Veeam) C#11 *[b4/p53]* Commercial Tool

Version-controlled-infrastructure-as-code C#4.6 *[b3/p54]* TO managing configuration

Version-controlled-infrastrure-as-code C#12.3 *[b4/p63]* Securly manage network infrastrure.

Vulnerability handling policy C#16.2 *[b5/p36]* identifies reporting process

Vulnerability Managemant Systems (VMS) C#7 *[b3/p38]*

Vulnerability tracking system C#16.2 *[b5/p36]* includes severity ratings, and metrics for measuring timing for identification, analysis, and remediation of vulnerabilities.

Ww

Web Application Firewalls (WAF) C#16 *[b5/p36]* To filter all traffic destined for the web application

Websense Triton C#9 *[b4/p14]* sample tool, used to URL monitoring and logging for authenticated proxy at boundary network

Wi-Fi Protected Access 2 (WPA2) C#12.6 *[b4/p64]* secure network communication protocols

Windows BitLocker C#3.6 *[b2/p10]* Data encryption

Windows Defender (Microsoft) C#10 *[b4/p34]* Commercial Tool

Wireshark C#13 *[b4/p97]* Free Tool

Wireshark C#3 *[b2/p20]* Free Tool

WMIC C#2 *[b3/p19 +20]* Free Tool + Automation Script

WMIC C#4 *[b3/p64]* Free tool

WMIC/NET C#5 *[b2/p43]* Free Tool

Work Profile C#4.12 *[b3/p56]* Android, to seprate enterprise applications and data from personal applications and data.

Xx

xDSCResourceDesigner (Microsoft PowerShell) C#4 *[b3/p64]* Free tool

Yy

Yubikey (Yubico) C#6 *[b2/p62]* Commercial Tool

Zz

Zeke (Bro) IDS C#13 *[b4/p97]* Free Tool