

Essential tools...

...for essential security controls

Tutorial days INFN – F. M. Taurino – 12/10/22

Documento con licenza CC-BY-SA

CIS Critical Security Controls

- **Linee guida** sulle misure da implementare per **prevenire e mitigare** i più comuni e diffusi **attacchi contro reti e sistemi informatici**
- Versione 8 rilasciata nel 2021
- Mappatura dei controlli verso **NIST, ISO27001, GDPR** e altri
- **18 controlli**, con specifiche **“difese”** per tre gruppi di utenti
 - IG1 - Piccole imprese, senza IT dedicato
 - IG2 - Medie imprese, con reparto IT
 - IG3 - Grandi aziende, o realtà soggette a controlli normativi e di conformità

CIS Controls

Version 7

01	Inventory of Hardware
02	Inventory of Software
03	Continuous Vulnerability Management
04	Control of Admin Privileges
05	Secure Configuration
06	Maintenance and Analysis of Logs
07	Email and Browser Protections
08	Malware Defenses
09	Limitation of Ports and Protocols
10	Data Recovery
11	Secure Configuration of Network Devices
12	Boundary Defense
13	Data Protection
14	Controlled Access Based on Need to Know
15	Wireless Access Control
16	Account Monitoring and Control
17	Security Awareness Training
18	Application Security
19	Incident Management
20	Penetration Testing



CIS Controls

Version 8

01	Inventory and Control of Enterprise Assets
02	Inventory and Control of Software Assets
03	Data Protection
04	Secure Configuration of Enterprise Assets and
05	Account Management
06	Access Control Management
07	Continuous Vulnerability Management
08	Audit Log Management
09	Email and Web Browser Protections
10	Malware Defenses
11	Data Recovery
12	Network Infrastructure Management
13	Network Monitoring and Defense
14	Security Awareness and Skills Training
15	Service Provider Management
16	Application Software Security
17	Incident Response Management
18	Penetration Testing



Perchè questa presentazione?

- Elenco **validissimo**, in uso in realtà differenti, in tutto il mondo
- E' la base delle "**Misure minime di sicurezza ICT per la PA**"
- ...ma non parla MAI di **prodotti !!!**

Limitare i costi...

- Per molti punti, indicheremo alcuni tool utilizzati per lo scopo, preferibilmente open source, altrimenti free, cercando di evitare il più possibile quelli a pagamento
- Alternativeto.net è nostro amico...

CSC1 e CSC2 - intro

Gestione degli asset, hw e sw

- Inventario di pc, server on prem e in cloud, apparati, dispositivi, account, programmi e licenze
- Dal file ods/xls, passando per **Snipe-IT**, **PDQ Inventory**, fino a **osquery/fleet** (*test in corso*)

Snipe-IT – LAMP stack + API

The screenshot displays the Snipe-IT Asset Management dashboard. At the top, there is a search bar labeled "lookup by Asset Tag" and a "Create New" button. The dashboard features six summary cards: 144 assets, 363 licenses, 0 accessories, 0 consumables, 79 components, and 47 people. Below these are two main sections: "Recent Activity" and "Assets by Status".

Recent Activity

Date	Admin	Action	Item	Target
10/10/2022 13:29	Francesco	update	[Redacted]	Vostro 3500
10/10/2022 13:29	Francesco	checkout	[Redacted]	Vostro 3500 Caterina [Redacted]
08/10/2022 18:05	Francesco	create new	FS SFP 1G Base T 100m	
08/10/2022 18:05	Francesco	create new	FS SFP 10G Base T 30m	
06/10/2022 21:23	Francesco	update	GrandStream GXP1625	
06/10/2022 21:22	Francesco	update	Sennheiser PC8 USB	

[View All](#)

Assets by Status

Ready to deploy (7) | Archived (2) | Assigned (137)

The donut chart illustrates the distribution of assets across three status categories. The largest segment is "Assigned" with 137 assets, represented in blue. "Ready to deploy" accounts for 7 assets in green, and "Archived" accounts for 2 assets in red.

PDQ Inventory – free per Windows

PDQ Inventory 19.3.350.0 Free Mode

File Edit View Collection Computer Report Tools Options Help

Scan Tools Add Computers Scan Profiles New Scanner Collection Library New Dynamic Collection New Static Collection Print Preview New Report Cut Copy Paste Delete Buy Start Trial Help

Type to filter

Welcome to PDQ Inventory

- All Computers (442)
- Auto Reports
- Reports
- Scan Profiles
- Collection Library
- Tools
- sanmichele.local
 - Computers (110)
 - Dipartimenti (0)
 - Amministrazione (24)
 - Reparti (280)
 - RisparmioEnergético (2)
 - Segreteria (21)
 - SoloWsus (1)
 - Domain Controllers (3)
 - Allow Scan (433)
 - Disallow Scan (9)
 - Internet Explorer (303)
 - Memory (303)
 - Microsoft .NET Framework 4.6.2+
 - Microsoft Office (128)
 - Non-Standard Shares (171)
 - Online Systems (95)
 - PowerShell (303)
 - Reboot Required (192)
 - Reboot Timeline
 - Requires .NET to Scan (4)
 - Servers (15)
 - Systems with Smart Card Readers (0)
 - Workstations (416)
 - New Collection (383)

Allow Scan
Computers that will be scanned

Name	Online	Host Name	IP Address	Scan Status	O/S	O/S Version	SP / Release	Uptime	Current User	Successful Scan Date	Manufacturer
PC-28-89	Yes	PC-28-89	192.168.		11	10.0.22000.795	21H2	18 days 5 hours	enzio	08/10/2022 11:31	Dell Inc.
PC-29-134	No	PC-29-134	192.168.		11	10.0.22000.527	21H2		otta	08/10/2022 11:30	Dell Inc.
PC-29-14	Yes	PC-29-14	192.168.		11	10.0.22000.527	21H2	10 days 6 hours	otta (locke...	08/10/2022 11:30	Dell Inc.
PC-29-15	No	PC-29-15	192.168.		11	10.0.22000.527	21H2		bio	08/10/2022 11:30	Dell Inc.
PC-29-32	No	PC-29-32	192.168.		11	10.0.22000.978	21H2		astro	08/10/2022 11:30	Dell Inc.
PC-29-55	No	PC-29-55	192.168.		11	10.0.22000.493	21H2		agrino	08/10/2022 11:31	Dell Inc.
PC-29-86	Yes	PC-29-86	192.168.		11	10.0.22000.556	21H2	10 days 1 hour	pre (locked)	08/10/2022 11:29	Dell Inc.
PC-29-88	Yes	PC-29-88	192.168.		11	10.0.22000.527	21H2	138 days 10 hours	zza	08/10/2022 11:29	Dell Inc.
PC-29-89	Yes	PC-29-89	192.168.		11	10.0.22000.613	21H2	50 days 10 hours	cone (disc...	08/10/2022 11:29	Dell Inc.
PC-41-18	Yes	PC-41-18	192.168.		10	10.0.19043.1586	21H1	141 days 23 hours	vese	08/10/2022 11:29	Dell Inc.
PC-41-19	Yes	PC-41-19	192.168.		10	10.0.19043.1645	21H1	30 days 9 hours	(locked)	08/10/2022 11:30	Dell Inc.
PC-41-21	Yes	PC-41-21	192.168.		10	10.0.19043.1566	21H1	107 days 13 hours	zza	08/10/2022 11:29	Dell Inc.
PC-41-22	Yes	PC-41-22	192.168.		10	10.0.19042.1526	20H2	96 days 12 hours	ecurti	08/10/2022 11:30	Dell Inc.
PC-41-25	Yes	PC-41-25	192.168.		10	10.0.19042.1586	20H2	90 days 9 hours	vese	08/10/2022 11:30	Dell Inc.
PC-28-73	No	PC-28-73	192.168.		11	10.0.22000.739	21H2	28 days 6 hours	io	08/10/2022 11:28	Dell Inc.
PC-29-13	No	PC-29-13	192.168.		11	10.0.22000.556	21H2		agala	08/10/2022 11:29	Dell Inc.
PC-29-143	No	PC-29-143	192.168.		11	10.0.22000.556	21H2		azzuoli	08/10/2022 11:29	Dell Inc.
PC-29-19	Yes	PC-29-19	192.168.		11	10.0.22000.556	21H2	42 days 11 hours	avalle	08/10/2022 11:30	Dell Inc.
PC-29-195	No	PC-29-195	192.168.		11	10.0.22000.556	21H2		etta (locked)	08/10/2022 11:30	Dell Inc.
PC-29-197	Yes	PC-29-197	192.168.		11	10.0.22000.556	21H2	4 days 5 hours	ta	08/10/2022 11:30	Dell Inc.
PC-29-221	Yes	PC-29-221	192.168.		11	10.0.22000.556	21H2	9 days 11 hours	vese	08/10/2022 11:29	Dell Inc.
PC-29-38	Yes	PC-29-38	192.168.		11	10.0.22000.613	21H2	19 days 12 hours	avalle	08/10/2022 11:31	Dell Inc.
PC-40-173	No	PC-40-173	192.168.		10	10.0.19043.1586	21H1		esco	08/10/2022 11:30	Dell Inc.
PC-40-232	Yes	PC-40-232	192.168.		10	10.0.19044.1706	21H2	93 days 2 hours	otta (locke...	08/10/2022 11:30	Dell Inc.
PC-28-125	Yes	PC-28-125	192.168.		11	10.0.22000.556	21H2	10 days 6 hours	io	08/10/2022 11:30	Dell Inc.
PC-28-188	Yes	PC-28-188	192.168.		11	10.0.22000.593	21H2	23 days 8 hours	niello	08/10/2022 11:30	Dell Inc.
PC-29-106	Yes	PC-29-106	192.168.		11	10.0.22000.556	21H2	10 days 6 hours	zza	08/10/2022 11:29	Dell Inc.
PC-29-25	Yes	PC-29-25	192.168.		11	10.0.22000.556	21H2	9 days 12 hours	etta	08/10/2022 11:28	Dell Inc.
PC-29-41	Yes	PC-29-41	192.168.		11	10.0.22000.556	21H2	37 days 7 hours	zza (locked)	08/10/2022 11:31	Dell Inc.
PC-29-64	Yes	PC-29-64	192.168.		11	10.0.22000.593	21H2	10 days 6 hours	ecurti	08/10/2022 11:30	Dell Inc.
PC-29-65	Yes	PC-29-65	192.168.		11	10.0.22000.613	21H2	7 days 12 hours	nte	08/10/2022 11:28	Dell Inc.
PC-29-67	Yes	PC-29-67	192.168.		11	10.0.22000.613	21H2	10 days 5 hours	io	08/10/2022 11:30	Dell Inc.

433 Computers (1 selected)

0 Computers Scanning Upgrade Your License

PDQ – HW di un pc

PC-29-88 - Computer [29 of 433]

File Edit View Computer Tools Options Help

Scan Tools Print Preview Prev Computer Next Computer Cut Copy Paste Help

Computer

- Active Directory Groups
- Applications
- Collections
- CPU
- Custom Fields
- Deployments
- Disk Drives
- Displays
- Environment
- Files & Directories
- Hardware
- Hot Fixes
- Local Groups
- Local Users
- Memory Modules
- NICs
- PowerShell
- Printers (local)
- Processes
- Product Keys
- Registry

PC-29-88

General

Name	PC-29-88
Description	
Host Name	PC-29-88
Added	05/03/2022 12:43
Online	<input checked="" type="checkbox"/> Yes
Uptime	138 days 10 hours
Boot Time	25/05/2022 09:23
Current User	[redacted]ozza
Display Name	[redacted]
IP Address	192.168.[redacted]
MAC Address	30:D0:42:[redacted]
Time Zone	(UTC+01:00) Amsterdam, Berlino, Berna, Roma, Stoccolma, Vienna

Operating System

O/S	11
Name	Microsoft Windows 11 Pro
Version	10.0.22000.527
SP / Release	21H2
Installed	23/02/2022 20:27:22
Serial Number	00355-60684-14279-AAOEM
System Drive	C
PowerShell Version	5.1.22000.1
SMBv1 Server Enabled	Yes

Active Directory

Parent Path	Dipartimenti/Reparti
Description	[redacted]
Domain	[redacted]
Domain Controller	Controller di dominio: \cms03.[redacted]
Location	
Last Logon	03/10/2022 03:07
Created	23/02/2022 11:50

System

Manufacturer	Dell Inc.
Model	OptiPlex 7490 AIO
Memory	16 GB
Processor	16-Core 2,9 GHz Intel Core i7-10700 CPU @ 2.90GHz
Chassis	All in One
Serial Number	J[redacted]
BIOS Version	1.6.0
BIOS Manufacturer	Dell Inc.
BIOS Asset Tag	
Family	OptiPlex
Version	
SKU	0A46

Scanning

Allow Scan	Yes
------------	-----

PDQ – SW di un pc

The screenshot displays the PDQ Engine interface for a computer named 'PC-29-88'. The main window shows a list of installed software with columns for Name, Version, Publisher, Install Date & Time, Uninstall, Registry Hive, and Registry Path. The left sidebar contains a navigation tree with categories like Computer, Applications, Collections, CPU, Custom Fields, Deployments, Disk Drives, Displays, Environment, Files & Directories, Hardware, Hot Fixes, Local Groups, Local Users, Memory Modules, NICs, PowerShell, Printers (local), Processes, Product Keys, and Registry. The top menu includes File, Edit, View, Computer, Tools, Options, and Help. The toolbar contains icons for Scan, Tools, Print Preview, Prev Computer, Next Computer, Cut, Copy, Paste, and Help.

Name	Version	Publisher	Install Date & Time	Uninstall	Registry Hive	Registry Path
7-Zip 21.07 (x64 edition)	21.07.00.0	Igor Pavlov	23/02/2022 11:59		HKEY_LOCAL_MAC...	SOFTWARE
Adobe Acrobat Reader DC - Italiano	22.002.20212	Adobe Systems Inc...	14/09/2022 12:33		HKEY_LOCAL_MAC...	SOFTWARE
Dell Peripheral Manager	1.5.0	Dell Inc.	23/02/2022 20:00		HKEY_LOCAL_MAC...	SOFTWARE
Google Chrome	99.0.4844.51	Google LLC	23/02/2022 00:00		HKEY_LOCAL_MAC...	SOFTWARE
Java 7 Update 80	7.0.800	Oracle	23/02/2022 12:04		HKEY_LOCAL_MAC...	SOFTWARE
Java SE Development Kit 7 Update 80	1.7.0.800	Oracle	23/02/2022 12:04		HKEY_LOCAL_MAC...	SOFTWARE
Kaspersky Endpoint Security for Windows	11.6.0.394	AO Kaspersky Lab	23/02/2022 12:32		HKEY_LOCAL_MAC...	SOFTWARE
Kaspersky Security Center Network Agent	13.0.0.11247	Kaspersky	23/02/2022 12:30		HKEY_LOCAL_MAC...	SOFTWARE
LibreOffice 7.2 Help Pack (Italian)	7.2.5.2	The Document Fou...	23/02/2022 12:01		HKEY_LOCAL_MAC...	SOFTWARE
LibreOffice 7.2.5.2	7.2.5.2	The Document Fou...	23/02/2022 12:01		HKEY_LOCAL_MAC...	SOFTWARE
Microsoft Edge	99.0.1150.30	Microsoft Corporat...	05/03/2022 07:12		HKEY_LOCAL_MAC...	SOFTWARE
Microsoft Edge Update	1.3.155.77		23/02/2022 20:07		HKEY_LOCAL_MAC...	SOFTWARE
Microsoft Edge WebView2 Runtime	99.0.1150.30	Microsoft Corporat...	06/03/2022 23:12		HKEY_LOCAL_MAC...	SOFTWARE
Microsoft OneDrive	22.033.0213.0002	Microsoft Corporat...	08/03/2022 09:57		HKEY_USERS	S-1-5-21-
Microsoft OneDrive	22.191.0911.0001	Microsoft Corporat...	01/10/2022 11:03		HKEY_USERS	S-1-5-21-
Microsoft OneDrive	22.196.0918.0001	Microsoft Corporat...	08/10/2022 08:39		HKEY_USERS	S-1-5-21-
Microsoft Update Health Tools	4.65.0.0	Microsoft Corporat...	23/02/2022 11:12		HKEY_LOCAL_MAC...	SOFTWARE
Microsoft Visual C++ 2005 Redistributable	8.0.56336	Microsoft Corporat...	23/02/2022 12:05		HKEY_LOCAL_MAC...	SOFTWARE
Mozilla Firefox ESR (x64 it)	91.6.0	Mozilla	23/02/2022 11:59		HKEY_LOCAL_MAC...	SOFTWARE
Mozilla Maintenance Service	91.6.0	Mozilla	23/02/2022 11:59		HKEY_LOCAL_MAC...	SOFTWARE
Notepad++ (64-bit x64)	8.2	Notepad++ Team	23/02/2022 12:01		HKEY_LOCAL_MAC...	SOFTWARE
TightVNC	2.8.63.0	GlavSoft LLC.	23/02/2022 11:57		HKEY_LOCAL_MAC...	SOFTWARE

CSC1 – difese e tool

- **arpwatch/arpalert**, su vm con una scheda in ogni vlan, in modo passivo
- **arp-scan**, per il discovery attivo, a intervalli regolari
- Tabelle arp/fdb da firewall/router/sw e dai sistemi di monitoraggio
- Log dei server DHCP

CSC2 – difese e tool

- Di base, utenti con bassi privilegi che non possano apportare modifiche, installare (o compilare...) programmi
- Software Restriction Policies e Applocker su Windows
- Fapolicyd su Linux (recente)

CSC3 - intro

Protezione dei dati

- Inventario, classificazione (per es. “pubblico”, “riservato”, “sensibile”), uso sicuro, conservazione e dismissione
- Accesso solo a dispositivi e provider autorizzati
- Liste controllo accessi

CSC3 – difese e tool - 1

- ACL su filesystem e condivisioni, con audit degli accessi e delle operazioni
 - Samba vfs_full_audit (facile sui NAS)
 - Audit su share Windows
- Cifratura
 - Bitlocker/Vault/dm-crypt o **VeraCrypt**

CSC3 – difese e tool - 2

- Cifratura dati in transito con ssl, tls, ssh
- **Projectsend** al posto di WeTransfer
- **NextCloud** al posto di Dropbox
- **Rclone** per cifrare dati inviati a cloud esterni
- Archivi **7-zip** con cifratura AES
- Distruzione sicura con **shred, wipe, dban**
 - E il trapano...

CSC4 – intro

Configurazione sicura degli asset e del sw

- Golden image e procedure di installazione sicure secondo framework noti, con revisione annuale
- Verifica firmware e versioni, cambio password di default e gestione su vlan separata per gli apparati di rete

CSC4 – difese e tool

- Blocco sessioni dopo 15 minuti
- Firewall su server e client
- Accesso con protocolli sicuri (ssh/https)
- Verificare se possibile disabilitare gli account di default (root/administrator)
- Rimuovere o disabilitare programmi o servizi inutili

CSC4 – difese e tool - 2

- Utilizzo di server DNS aziendali o noti
 - limitare porte 53 e 853 verso server affidabili
 - verificare blocchi per DoH
- Lockout dopo alcuni tentativi di autenticazione falliti
 - **fail2ban/lfld** (da **csf**)
 - Gpo account lockout policy
- Remote wiping – find my device
 - **Miradore MDM** – piano gratuito in valutazione

CSC5 - intro

Gestione degli account

- Inventario account aziendali
 - Classificazione e revisione trimestrale
 - Procedure di roll in e roll out, anche via ticket
- Password complesse
 - Minimo 8 caratteri con 2fa
 - 14 caratteri dove non possibile

CSC5 – difese e tool

- Disabilitare account non utilizzati
 - **AdTidy free** o query ldap su AD/Samba4
 - **Lastlog** su server Linux
- Utilizzare account senza privilegi amministrativi
- Elenco account di servizio
- Gestione centralizzata degli account
 - **AAI/AD/Samba4/FreeIPA**

CSC6 - intro

Gestione del controllo accessi

- Procedure per concessione o rimozione accessi
 - Almeno via ticket
- MFA per applicazioni esterne e accesso remoto
 - **Pfsense con openvpn + totp**
- MFA per accesso amministrativo ove possibile

CSC6 – difese e tool

- Inventario dei sistemi di autenticazione e autorizzazione, locali e remoti
- Centralizzare il controllo accessi
- Gestione e manutenzione controllo accessi basato sui ruoli
 - Revisione almeno annuale

CSC7 - intro

Gestione continua delle vulnerabilità

- Procedura per valutare, monitorare e gestire le vulnerabilità degli asset
- Procedura di correzione, basata su analisi del rischio
- Aggiornamento automatico dei sistemi operativi
 - **unattended-upgrade/yum-cron**, solo security
 - Windows update (defer feature updates)
 - MacOS security update

CSC7 – difese e tool

- Aggiornamento automatico delle applicazioni
 - Linux: **ansible**/unattended-upgrades/yum-cron
 - Win: **ansible/winget/choco/wapt/pdq** deploy
 - Mac: **ansible/brew** (con i cask)/munki

CSC7 – difese e tool

- Scansioni vulnerabilità
 - Interne ogni 3 mesi, esterne ogni mese
 - Strumenti SCAP
 - **OpenVas, nmap -sV o -A + plugin vulscan**
- Correzione delle vulnerabilità rilevate
 - Secondo le procedure

CSC8 - intro

Gestione dei log

- Procedure, per quali apparati e servizi, retention
- Raccolta log locali agli asset, con spazio adeguato
- Sincronizzazione orari
 - **ntp/nettime/gpo**
- Raccolta log query DNS (privacy???)
 - “rndc querylog” per bind

CSC8 – difese e tool

- Raccolta log richieste URL (privacy???)
 - Log di squid/squidguard
- Centralizzare i log
 - **Rsyslog/graylog** (con **winlogbeat**)
- Retention di almeno 90 giorni (dpo?)
- Revisione e controllo dei log, almeno su base settimanale
- Raccolta log dai fornitori di servizi
 - Anche dalla console ESET

CSC9 - intro

Protezione posta elettronica e browser

- Browser e client mail sempre aggiornati (CSC2 e 7!)
- Servizi di filtro DNS
 - Solo server sicuri (es. **1.1.1.2**), blocklist (**pi-hole+firebog**)
- Servizi di filtro URL
 - **Squidguard + blocklist Univ. Di Tolosa / Watchguard WebBlocker**
- Filtro ip e subnet malevole
 - **PfBlockerNG + firehol_level1 / Watchguard RED**

CSC9 – difese e tool

- Limitare estensioni in browser e client di posta
 - Gpo con admx per Chrome/Firefox
- sui server di posta **SPF/DMARC/DKIM** e antimalware
 - Proxmox Mail Gateway, clamav + signature aggiuntive
 - NethServer, rspamd, clamav + signature aggiuntive
 - Blocco estensioni per file dannosi

CSC10 - intro

Difesa dai malware

- Antimalware su tutti gli asset
 - Con aggiornamento automatico
 - Preferire la gestione centralizzata
 - Negli ultimi anni, Eset e KSP
- Disattivare esecuzione automatica e abilitare scansione automatica per i dispositivi mobili
- Abilitare le funzioni anti exploit

CSC11 – intro

Recupero dei dati

- Procedura per il recupero dei dati, con classificazione, priorità e sicurezza
- Eseguire backup automatizzati
 - **Proxmox Backup Server/Veeam**
 - **Rsync + sanoid** (retention snapshot zfs) + **syncoid** (replica)
 - **BackupPC** (via smb/sftp)/**UrBackup**

CSC11 – difese e tool

- **Rclone con crypt** verso storage esterni
- Versioni dei backup anche offsite o offline
 - Sync su PBS o storage ZFS remoto
 - Rclone verso storage a oggetti/servizi cloud
 - I NAS dei marchi più noti hanno tool simili
- Eseguire regolarmente test di ripristino
 - Almeno trimestrali

CSC12 – intro

Gestione infrastruttura di rete

- Hardware e versione dei firmware supportati
- Segmentazione della rete, vlan per tipologia traffico
- Gestione sicura degli apparati via https/ssh
- Creazione diagramma dell'infrastruttura
- AAA – radius/packetfence/captive portal
- Anche per le VPN
- Tool: **LibreNMS/Oxidized**

CSC13 – intro

Monitoraggio e difesa della rete

- Centralizzare analisi log e gestione eventi
 - SIEM come **Wazuh/Ossim/SecurityOnion**
- HIDS
 - **AIDE** (ma anche "rpm -V" o "debsums" per i pacchetti)
 - **Samhain**, anche su Windows via CygWin (ma anche "sfc /scannow" + "dism /online /cleanup-image /restorehealth")
 - Via **osquery file integrity monitoring pack**

CSC13 – difese e tool

- NIDS (anche NIPS quando integrati nei fw)
 - **Snort** con firme almeno VRT free (delay 30gg)
 - Integrato in **PfSense**
 - Educational 29,99\$/anno - Business 399\$/anno
 - Emerging Threats Open o Pro (prezzo non pubblico)
 - **Suricata**
 - Integrato in **PfSense**
 - Integrato in **OpnSense**, con firme ET Pro incluse SE si condivide con Proofpoint la telemetria (privacy???)

CSC13 – difese e tool - 2

- Filtro traffico fra vlan e segmenti di rete
- Verifica della sicurezza degli asset che si collegano in vpn
 - **Eset** centralizzato invia informazioni su stato update e av
 - Oppure richiamare **osquery** nel file di configurazione OpenVPN
- Salvare log dei flussi di traffico di rete (privacy???)
- Controllo accessi sulle porte lan (mac o meglio 802.1x)
- Filtri a livello di applicazione e tuning soglie degli avvisi
 - **OpenAppID in Snort**

CSC14 – intro

Formazione sulla sicurezza informatica

- Programma di sensibilizzazione sulla sicurezza
- Riconoscimento attacchi di social engineering
- Tecniche di autenticazione e di gestione dati
- Esposizione involontaria dei dati e segnalazione incidenti
- Necessità degli aggiornamenti e pericoli legati al lavoro se connessi a reti non sicure
- Formazione specifica per ruolo (dirigenti/amm/dev/etc)

CSC15 – intro

Gestione dei service provider

- Inventario dei service provider, con classificazione dei dati trattati e procedure di gestione
- Assicurarsi che implementino sistemi e framework di sicurezza, anche con controlli periodici (e nel dark web)
- Disattivazione sicura
 - Cancellazione e verifica eventuali flussi automatici

CSC16 – intro

Sicurezza degli applicativi

- Procedura di sviluppo secure by design
- Gestione e risoluzione delle vulnerabilità
 - Livelli di gravità, analisi e correzione
- Inventario software e librerie di terze parti, anche per verificare se aggiornati o non più supportati
 - Per esempio, “composer” o “npm” per i progetti web
- Hardening dell’infrastruttura

CSC16 – 2

- Separazione ambienti dev e prod
- Formazione degli sviluppatori sulle tematiche della sicurezza
- Utilizzare algoritmi di cifratura e moduli di autenticazione o log standard (tipo AES, LDAP, syslog)
- Strumenti di analisi statica del codice
- Penetration test applicativi

CSC17 – intro

Gestione e risposta agli incidenti

- Documentazione, procedure, ruoli e responsabilità
- Designazione del team (IT, legal, PR, HR, dirigenti), con almeno un membro interno se affidato a terzi, e inventario dei contatti a cui segnalare l'accaduto
- Procedura di segnalazione, informazioni minime e mezzi alternativi di comunicazione, procedure di risposta
- Esercitazioni e revisioni post-incidente

CSC18 – intro

Penetration test

- Programma di PT su reti, applicazioni, web, api, valutazione frequenza, tempi ed esclusioni
- Eseguire PT su sistemi esposti e sistemi interni almeno una volta l'anno
- Mitigazione e remediation
- Alcuni tool: **Metasploit, Burp suite**



That's all Folks!