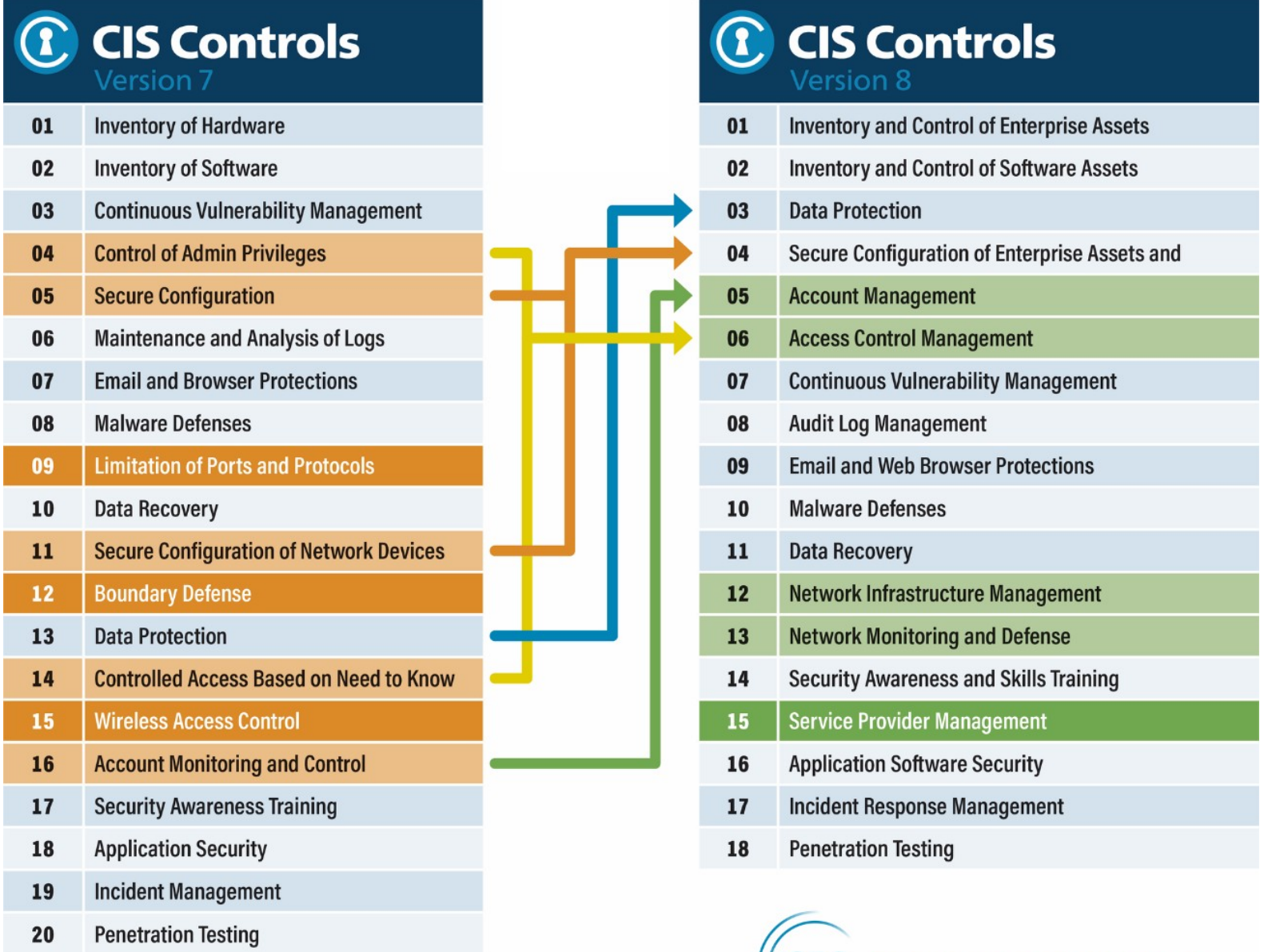
Essential tools...

...for essential security controls

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

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…

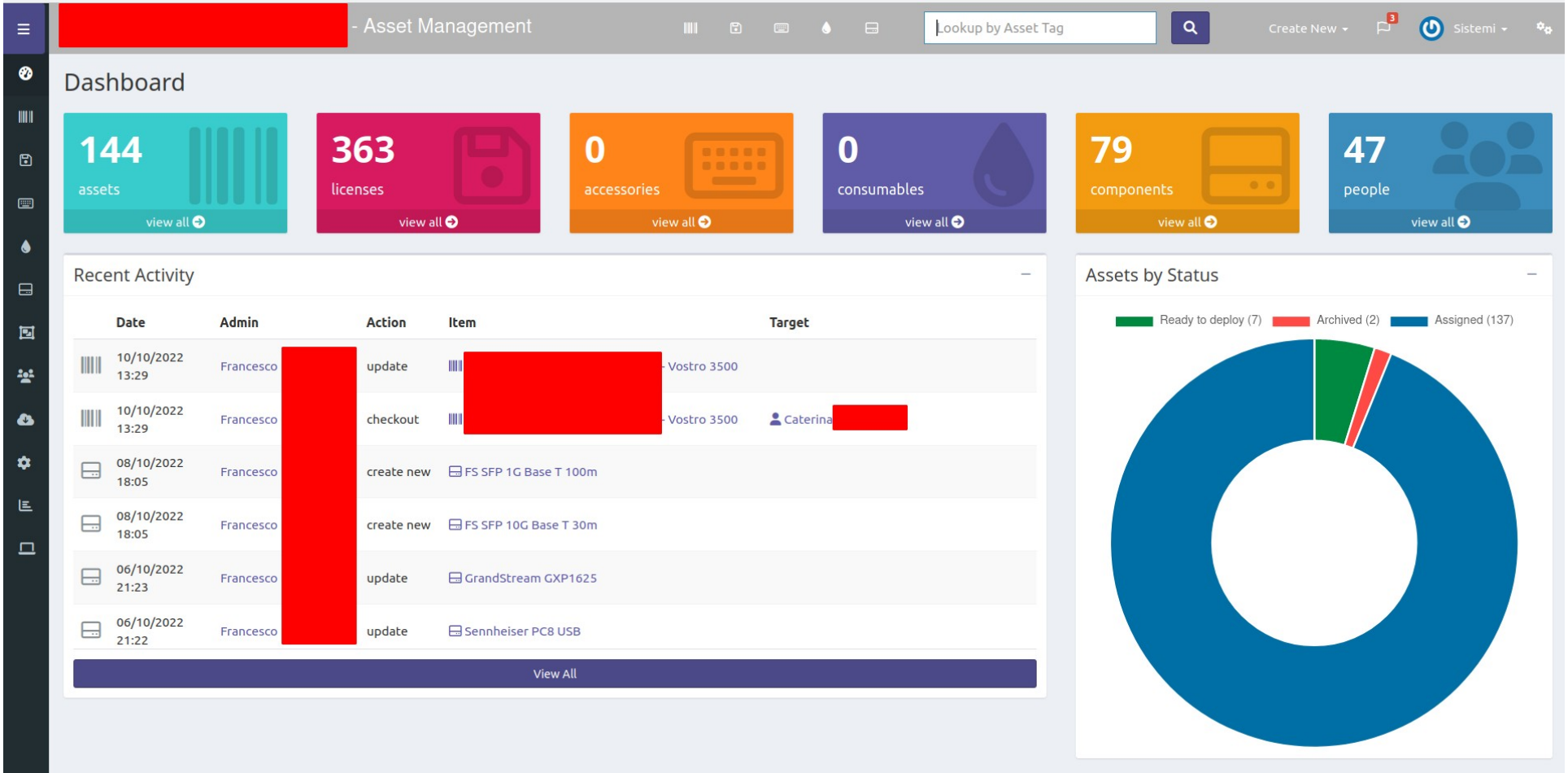
- Per molti punti, indicheremo alcuni tool utilizzati per lo scopo, preferibilmente open source, altrimenti free, cercando di evitare il più possibile quelli a pagamento
- Alternativeto.net è nostro amico…

CSC1 e CSC2 - intro

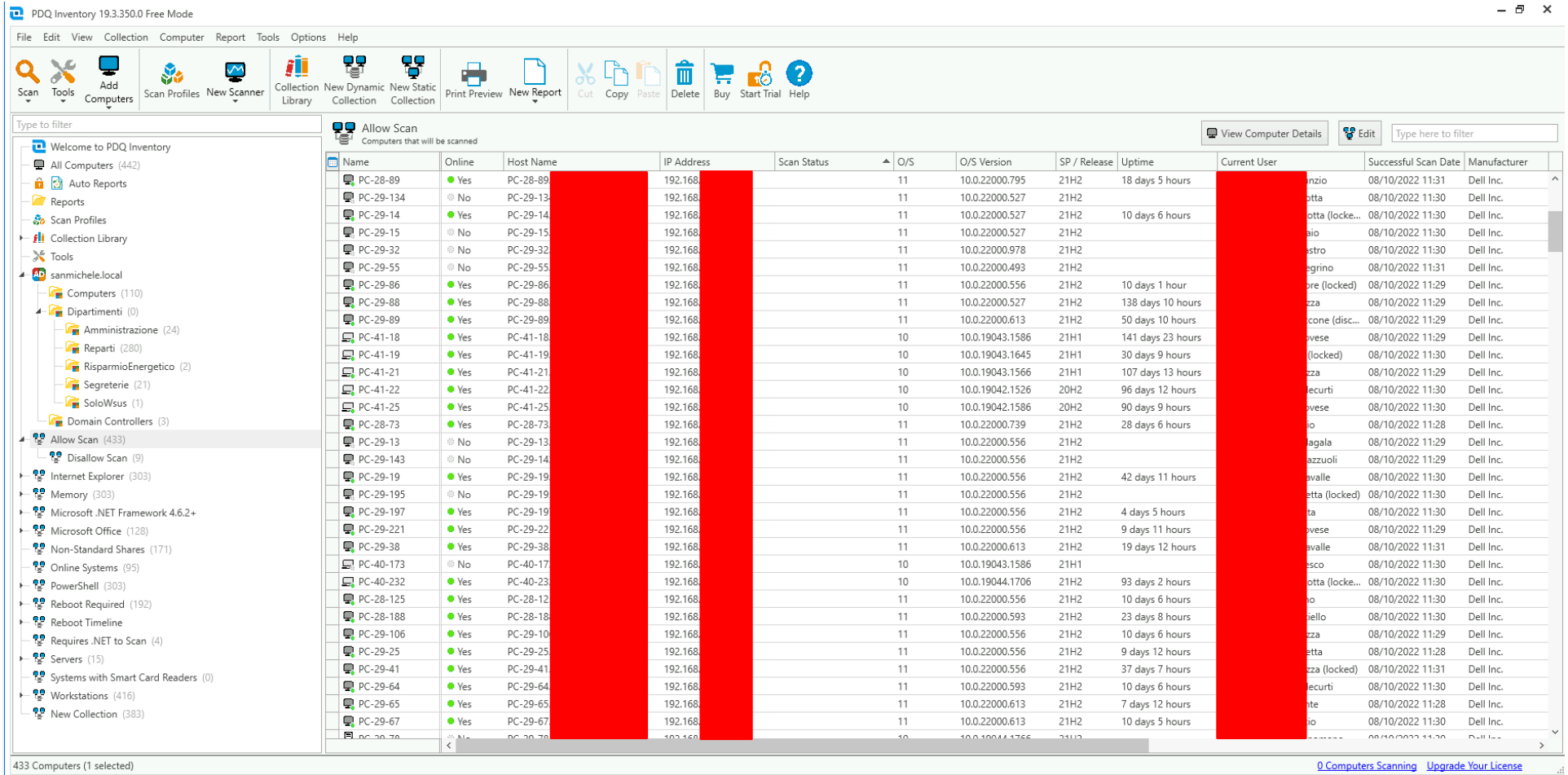
Gestione degli asset, hw e sw

- 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*)

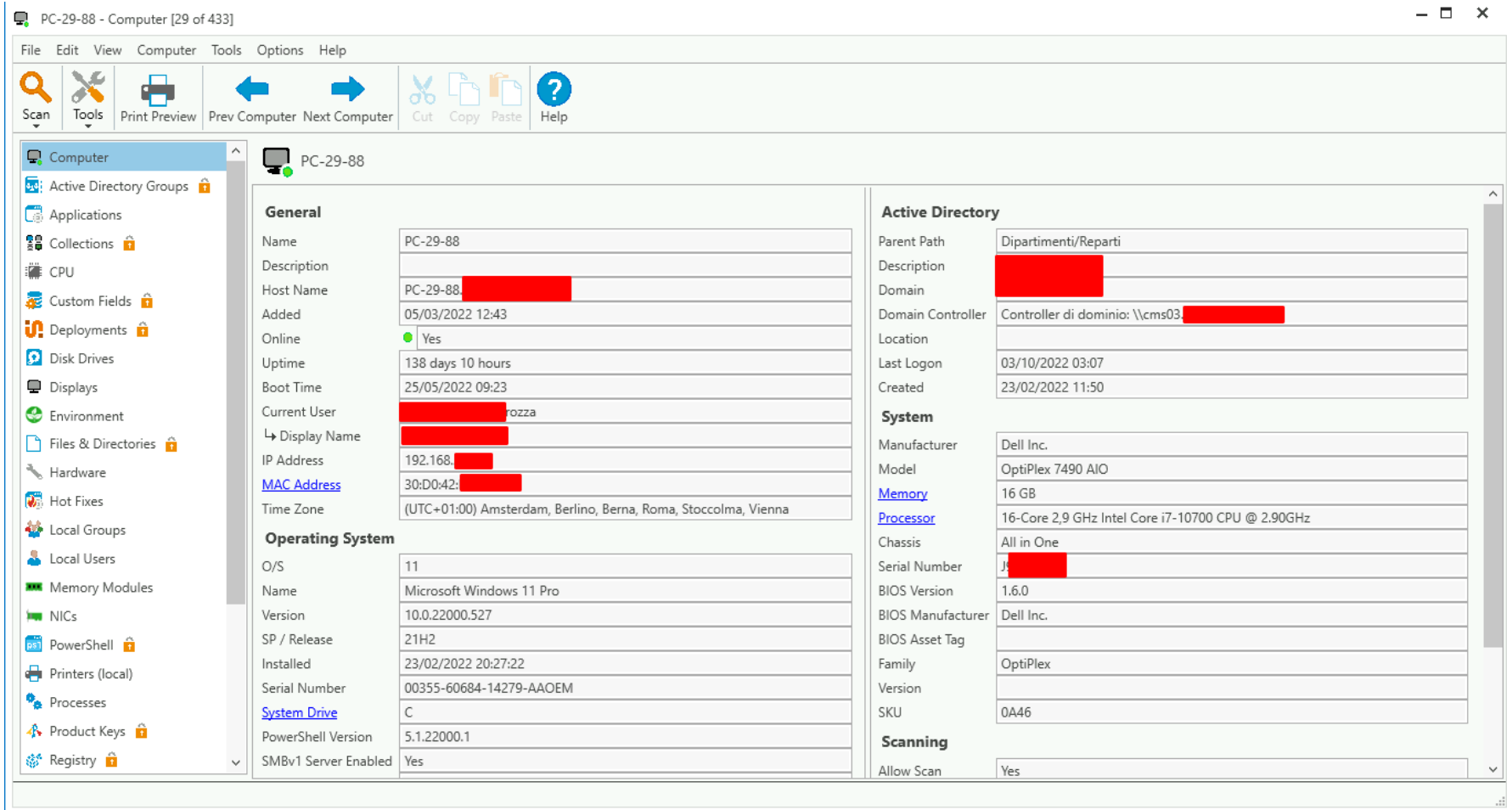
Snipe-IT – LAMP stack + API



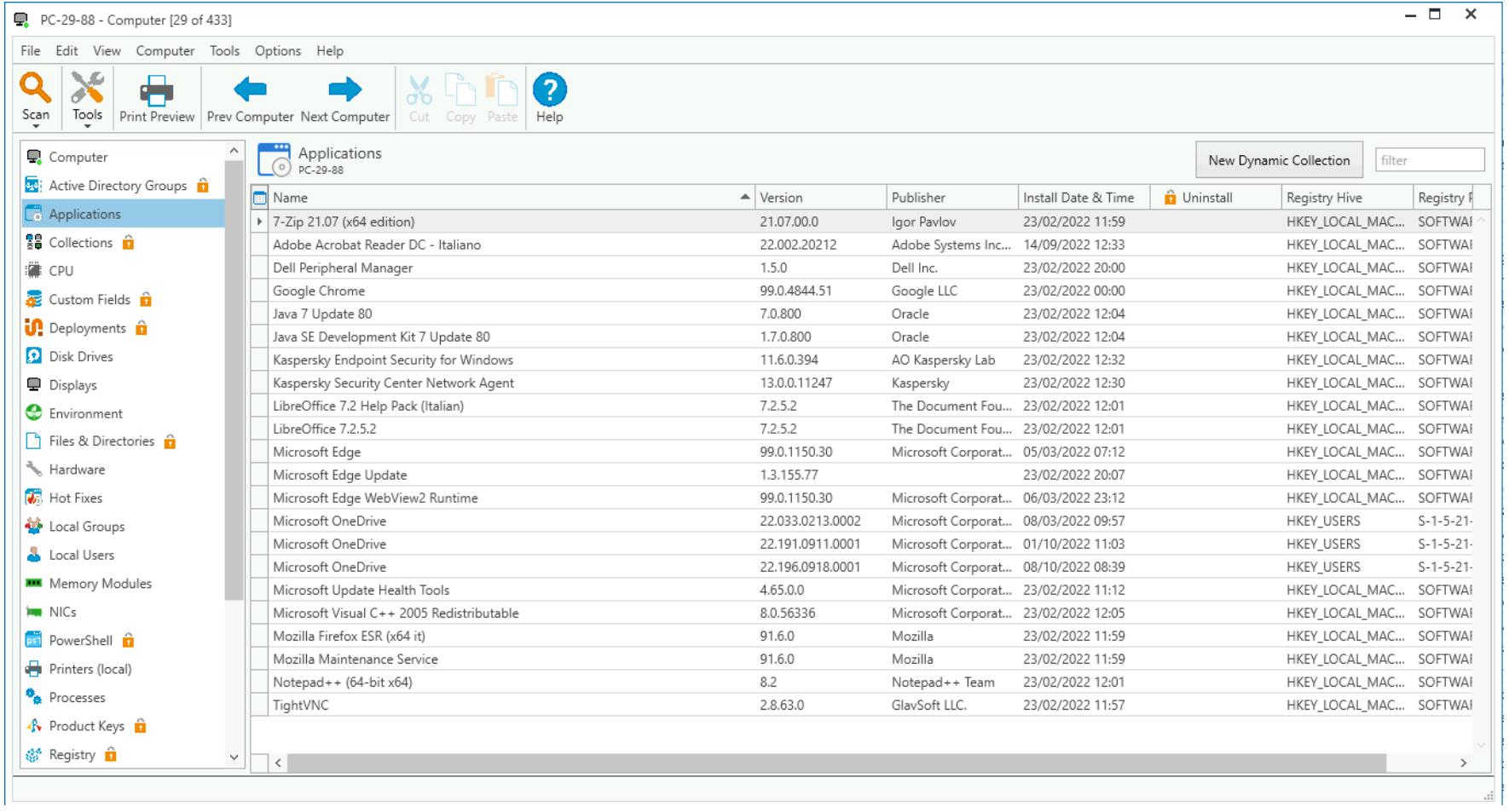
PDQ Inventory – free per Windows



PDQ – HW di un pc



PDQ – SW di un pc



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 disabilitaregli 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/lfd** (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!