Armis Centrix™ & NIS 2

See, Protect and Manage
Your Entire Attack Surface

Luca Bacchi–
Coherentia Srl
Luca.bacchi@coherentia.it

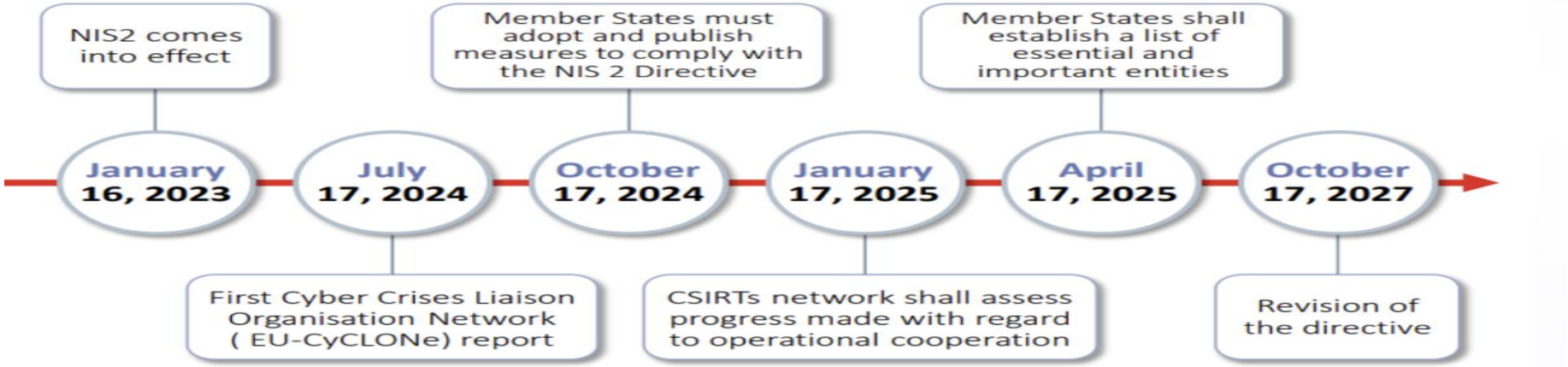
COHERENTIA

NIS 2: una breve introduzione

Nel Gennaio 2023 gli stati membri dell' EU hanno emanato una revisione della direttiva della sicurezza e reti informatiche del 2016 (NIS Network & Information System).

(Perché) in risposta ai nuovi attacchi ed ai nuovi scenari di guerra ibrida.

(Obiettivo) Rafforzare i requisiti di sicurezza, razionalizzare gli obblighi di reportistica, introduzione di misure di controllo e supervisione più rigide.



NIS 2: Aziende Coinvolte

NIS 2 identifica come Aziende Target «Entità critiche» che sono divise in 2 categorie:

- ❑ Essenziali
- ❑ Importanti

Stessi obblighi, ma le sanzioni per le categorie «essenziali» sono più rigorose

Impatti:

(1) Sulle aziende già coinvolte NIS, che potrebbero essere costrette a rivedere i loro criteri/programmi di compliance

(2) Che sulle organizzazioni che per la prima volta devono approcciare la nuova direttiva

NIS 2: Organizzazione impattate

Entità Critiche **Essenziali** (già presenti in NIS1) :

- Sanità
- Infrastruttura Digitale
- Trasporti
- Approvvigionamento Idrico
- Provider servizi digitali
- Settore Bancario
- Infrastrutture mercato finanziario
- Energia

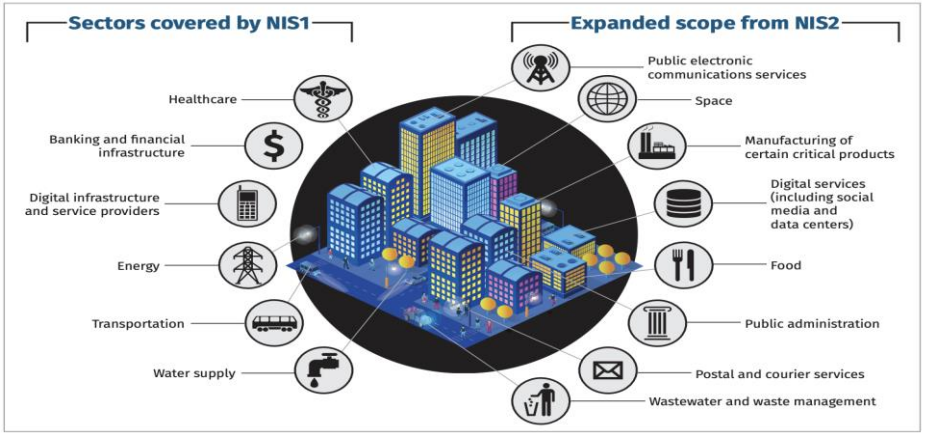
Nuove

- **Acque Reflue**
- **Salute (farmaci, R&S, dispositivi medici criti**
- **Spaziale**
- **Amministrazione Pubblica**

Nuove

Entità Critiche **Importanti** (NIS2):

- Provider comunicazione elettronica pubblica
- Prodotti Chimici
- Produzione, trattamento, distribuzione alimentare
- Fabbricazione prodotti critici (veicoli, pc, medicali)
- Provider digitali (social network, motori ricerca)
- Servizi Postali, corriere espresso



NIS 2: riferimenti

NIS 2 è una direttiva Europea che dovrà essere tradotta in legge italiana

- https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32022L2555&from=EN

L 333/80 IT Gazzetta ufficiale dell'Unione europea 27.12.2022

DIRETTIVE

DIRETTIVA (UE) 2022/2555 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO

del 14 dicembre 2022

relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148 (direttiva NIS 2)

NIS 2: gli elementi essenziali – Preambolo 51

Gli Stati membri dovrebbero incoraggiare l'uso di ogni **tecnologia innovativa**, compresa l'**intelligenza artificiale,** il cui utilizzo potrebbe **migliorare l'individuazione e la prevenzione** degli attacchi informatici, consentendo di destinare in modo più efficace risorse per affrontare gli attacchi informatici. Gli Stati membri dovrebbero pertanto incoraggiare, nelle loro strategie nazionali per la cybersicurezza, le attività di ricerca e sviluppo volte a facilitare l'uso di tali tecnologie, in particolare quelle relative agli **strumenti automatizzati o semiautomatizzati** nella cybersicurezza, e, se del caso, la condivisione dei dati necessari per formare gli utenti di tali tecnologie e migliorarle. L'utilizzo di tutte le tecnologie innovative, compresa l'intelligenza artificiale, dovrebbe rispettare il diritto dell'Unione in materia di protezione dei dati, compresi i principi di protezione dei dati con riguardo all'accuratezza, alla minimizzazione dei dati, all'equità e alla trasparenza, nonché alla sicurezza dei dati, come la più recente crittografia**. I requisiti di protezione dei dati fin dalla progettazione e predefiniti di cui al regolamento (UE) 2016/679 dovrebbero essere pienamente rispettati.**

NIS 2: gli elementi essenziali – Preambolo 58

Poiché lo sfruttamento delle **vulnerabilità nei sistemi informatici** e di rete può causare perturbazioni e danni significativi, **la rapida individuazione e correzione di tali vulnerabilità** è un fattore importante per la riduzione dei rischi. I soggetti che sviluppano o amministrano tali sistemi informatici e di rete dovrebbero pertanto stabilire procedure adeguate per gestire **le vulnerabilità nel momento in cui vengono scoperte**. Poiché le vulnerabilità sono spesso rilevate e divulgate da terzi, il fabbricante o fornitore di prodotti TIC o servizi TIC dovrebbe anche mettere in atto le procedure necessarie per ricevere informazioni sulla vulnerabilità da terzi. A tale riguardo, le norme internazionali ISO/IEC 30111 e ISO/IEC 29147 forniscono orientamenti sulla gestione delle vulnerabilità e sulla divulgazione delle vulnerabilità. Al fine di facilitare il contesto della divulgazione volontaria delle vulnerabilità, è particolarmente importante rafforzare il coordinamento tra persone fisiche e giuridiche segnalanti e i fabbricanti o fornitori di prodotti o servizi TIC. La divulgazione coordinata delle vulnerabilità consiste in un processo strutturato attraverso il quale le vulnerabilità sono segnalate al fabbricante o al fornitore dei prodotti TIC o dei servizi TIC potenzialmente vulnerabili, in modo tale da consentire loro di diagnosticarle ed eliminarle prima che informazioni dettagliate in merito siano divulgate a terzi o al pubblico. La divulgazione coordinata delle vulnerabilità dovrebbe comprendere anche il coordinamento tra la persona fisica o giuridica segnalante e il fabbricante o il fornitore di prodotti TIC o servizi TIC potenzialmente vulnerabili, per quanto riguarda i tempi per la risoluzione e la pubblicazione delle vulnerabilità.

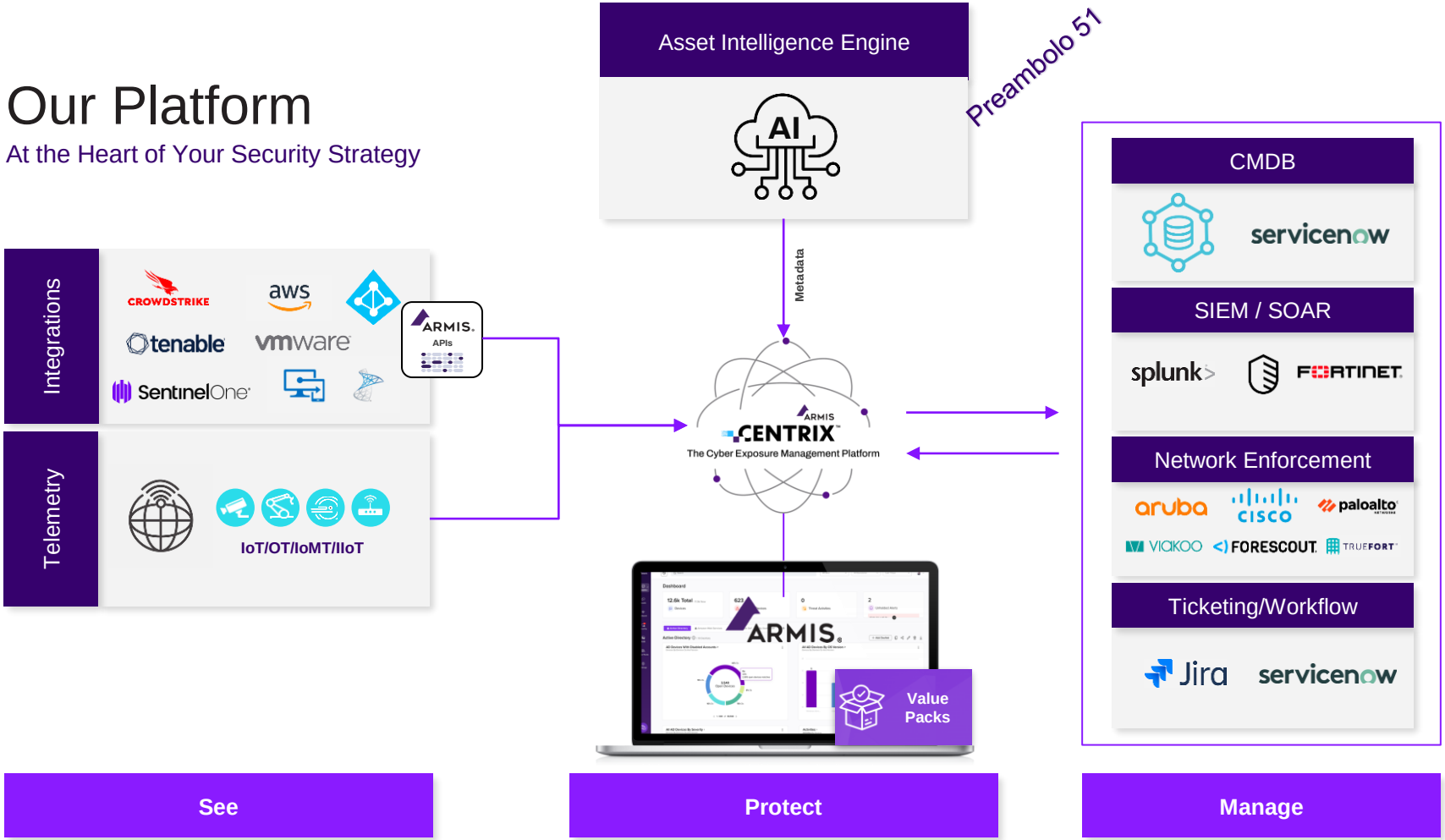
NIS 2: gli elementi essenziali – Articolo 21

Le misure di cui al paragrafo 1 sono basate su un **approccio multirischio** mirante **a proteggere i sistemi informatici e di rete e il loro ambiente** fisico da incidenti e comprendono almeno gli elementi seguenti:

- ✓ policy sull'**analisi dei rischi** e sulla **sicurezza dei sistemi informativi;**
- ✓ sistemi di **gestione degli incidenti**;
- ✓ sistemi di **business continuity**, come la gestione dei backup e il **disaster recovery**, e la gestione delle crisi;
- ✓ misure di gestione della **sicurezza della supply chain**;
- ✓ la sicurezza nell'acquisizione, nello sviluppo e nella manutenzione di reti e sistemi informativi, compresa la **gestione** e la **divulgazione delle vulnerabilità**;
- ✓ policy e procedure per **valutare l'efficacia delle misure di gestione del rischio di cybersecurity**;
- ✓ pratiche di **igiene informatica di base** [i.e., regole fondamentali per garantire la cybersecurity] e formazione in materia di sicurezza informatica;
- ✓ policy e procedure relative all'uso della **crittografia** e, se del caso, della cifratura crittografia;
- ✓ misure sulla sicurezza delle **risorse umane**, le politiche di controllo degli accessi e la gestione degli asset; e
- ✓ l'uso di **soluzioni di autenticazione a più fattori** [i.e., la c.d. multi-factor authentication] o di autenticazione continua, di comunicazioni vocali, video e di testo protette e di sistemi di comunicazione di emergenza protetti all'interno dell'entità, ove opportuno.

Our Platform

At the Heart of Your Security Strategy



Armis products

A Modular Approach to Address Key Security Challenges

Asset Management and Security

Complete asset inventory of all asset types allowing any organization to see and secure their attack surface

OT/IOT Security

Protect and manage OT/IOT networks and physical assets, ensure uptime and build an effective & comprehensive security strategy

Medical Device Security

Complete visibility and security for all medical devices, clinical assets and the entire healthcare ecosystem - with zero disruption to patient care

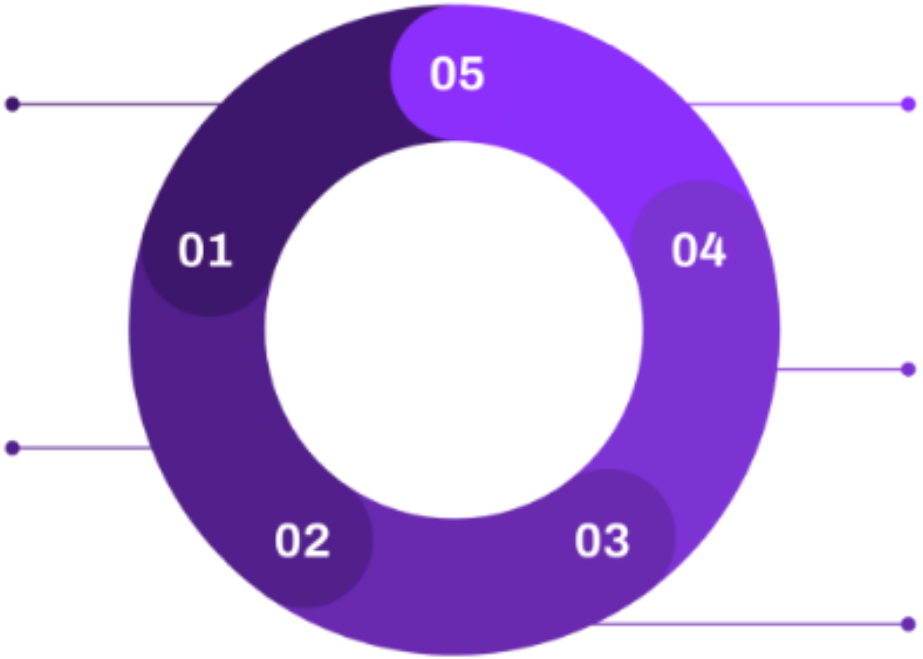
Vulnerability Prioritization and Remediation

Consolidate, prioritize and remediate all vulnerabilities; improve MTTR with automatic remediation and ticketing workflows

Preambolo 58

Armis Centrix: ViPR

Elimina il gap, attraverso una visione unica di tutte le vulnerabilità e dei dispositivi associati



Traccia e gestisci gli step di avanzamento e i progressi

Remediation: tramite connessione con tool esistenti e workflows – migliorando MTTR

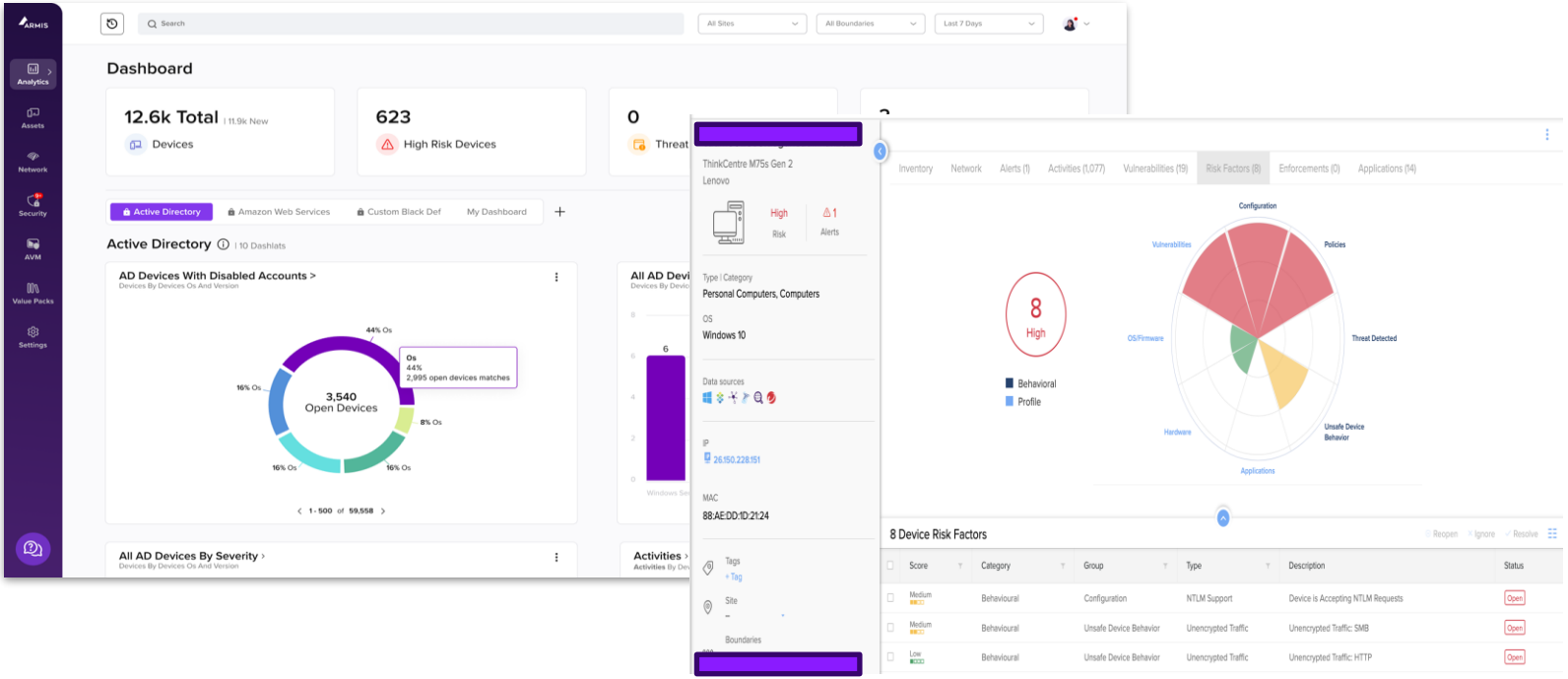
Arricchisci con informazioni di contesto sul device

Prioritizza le vulnerabilità

DEMO

Analisi del rischio e sicurezza

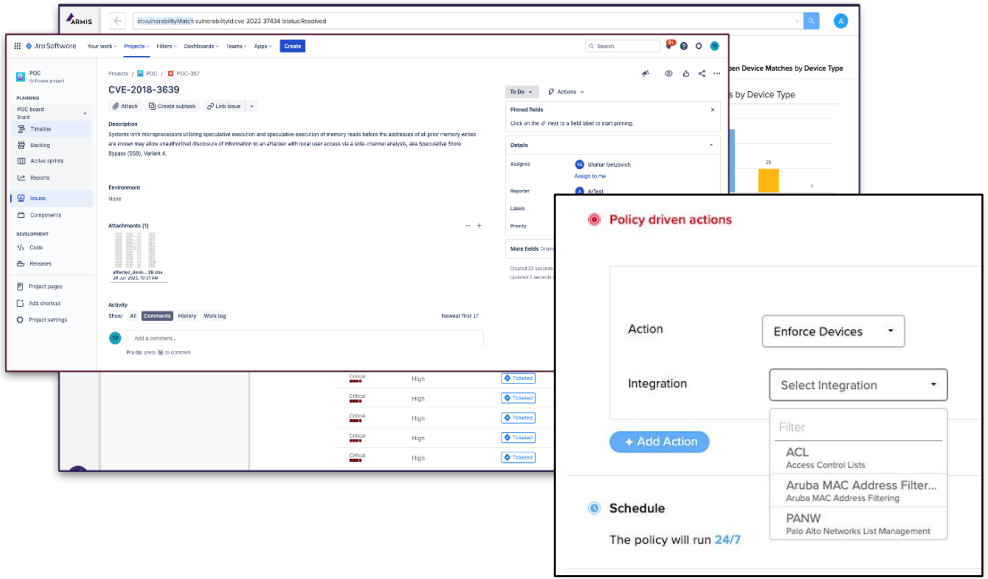
Un asset inventory completo e dettagliato che identifichi e classifichi ogni tipologia di device è il primo step per una analisi del rischio esaustiva.



Gestione degli incidenti

Connessione automatica con altri tool e sistemi di workflow – Migliorare il Mean Time To Resolution (MTTR)

- Generare e condividere informazioni di contesto con altri tool IT, sicurezza, SOC
- Creazione **automatica** o **manuale** di ticketing
- Azioni di remediation e mitigazione in generale (sfruttando sistemi esistenti)



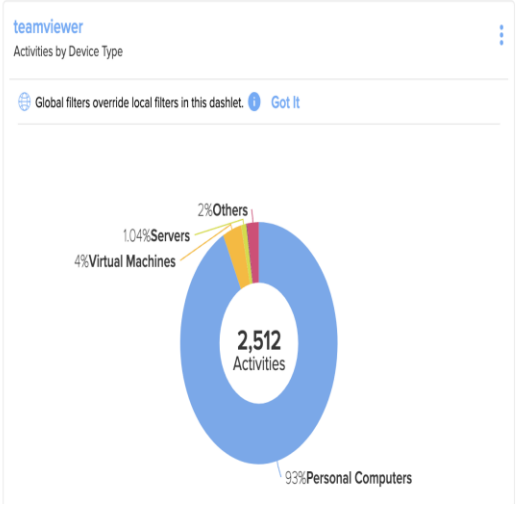
Altri item della Direttiva

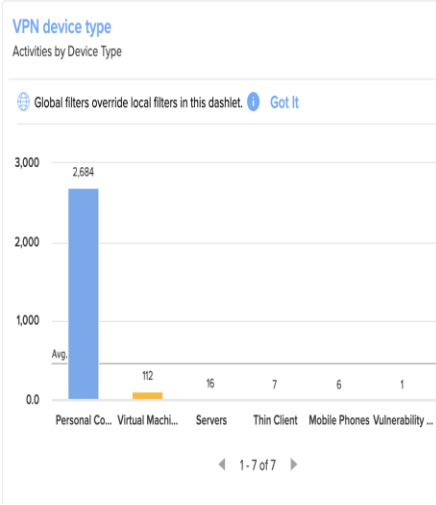
- manutenzione sistemi informatici di rete compresa gestione vulnerabilità (apparati End of Support, End of Sale, Hardware/Software fuori manutenzione)

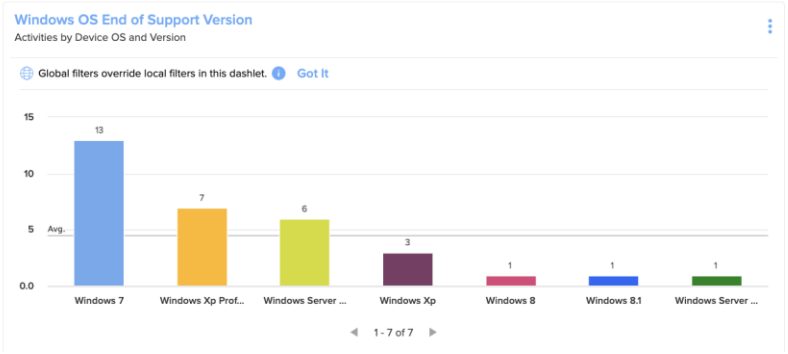
- Politiche e procedure uso crittografia

(protocolli, credenziali in chiaro, utilizzo SSLv3, TLSv1/1.x)

- Rapporti con diretti fornitori (chi accede da remoto, cosa fa sui che device)



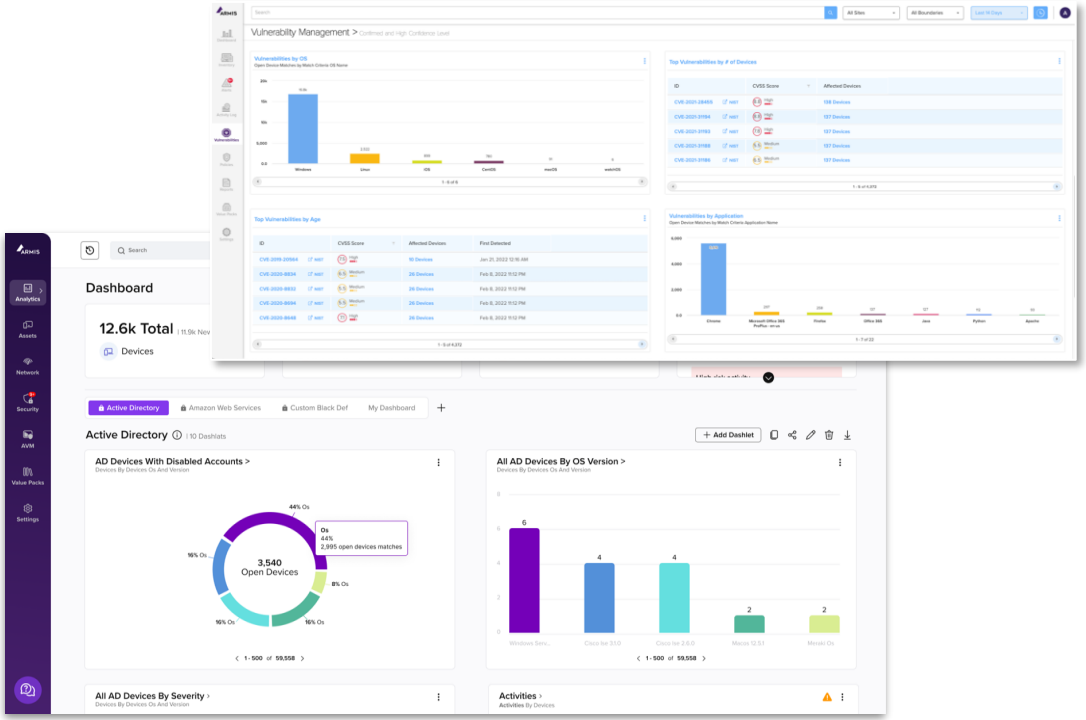




Tracciamento e gestione degli step implementativi di miglioramento

Customizable Dashboard and Reports

- Reports and dashboards suitable for every level in the organization
- Track SLAs, demonstrate progress on exposure reduction



Summary - Tabella

	Articolo 21	Armis Support
2.	Le misure di cui al paragrafo 1 sono basate su un approccio multirischio mirante a proteggere i sistemi informatici e di rete e il loro ambiente fisico da incidenti e comprendono almeno gli elementi seguenti:	
a)	politiche di analisi dei rischi e di sicurezza dei sistemi informatici;	Si esamindando il fattore di rischio di ogni dispositivo in base allo stato e al comportamento
b)	gestione degli incidenti;	Si tramite dashboard, workflow ed integrazioi con sistemi terzi
c)	continuità operativa, come la gestione del backup e il ripristino in caso di disastro, e gestione delle crisi;	Si attraverso la rappresentazione della mappatura dei device, del network mapping, del modello purdue (ambiente OT) è possibile avere una idea di come i sistemi per la BC siano interfacciati al resto della rete
d)	sicurezza della catena di approvvigionamento, compresi aspetti relativi alla sicurezza riguardanti i rapporti tra ciascun soggetto e i suoi diretti fornitori o fornitori di servizi;	Si tramite l'analisi del traffico da e verso i dispositivi e tramite l'analisi operativa dei device (ad es. EoS)
e)	sicurezza dell'acquisizione, dello sviluppo e della manutenzione dei sistemi informatici e di rete, compresa la gestione e la divulgazione delle vulnerabilità;	Si tramite il modulo ViPR per la gestione e la prioritizzazione delle vulnerabilità
f)	strategie e procedure per valutare l'efficacia delle misure di gestione dei rischi di cibersicurezza;	Si tramite l'analisi e dashboard incrementali sullo stato di sicurezza e di rischio dei device
g)	pratiche di igiene informatica di base e formazione in materia di cibersicurezza;	N.A
h)	politiche e procedure relative all'uso della crittografia e, se del caso, della cifratura;	Si, tramite l'analisi del traffico ed evidenziando l'utilizzo di procolli cifrati e/o metodi di encryption deboli/obsoleti
i)	sicurezza delle risorse umane, strategie di controllo dell'accesso e gestione degli attivi;	NA
j)	uso di soluzioni di autenticazione a più fattori o di autenticazione continua, di comunicazioni vocali, video e testuali protette e di sistemi di comunicazione di emergenza protetti da parte del soggetto al proprio interno, se del caso	NA

