MIDGARD

CYBER VALHALLA PROTECTION

> *«Il tuo regno, protetto dalla forza degli antichi e dalla precisione del futuro.»*

Piattaforma on-premise per l'inventario degli asset, la gestione delle vulnerabilità e la misurazione continua della conformità alla Direttiva NIS2 (D.Lgs. 138/2024).

FORTEZZA ON-PREMISE
MOTORE COMPLIANCE NIS2
ASSET INTELLIGENCE

WWW.MIDGARDSEC.IT

IN VIGORE DAL 16.10.2024

LA NIS2 È LEGGE ITALIANA

Il D.Lgs. 138/2024 recepisce la Direttiva (UE) 2022/2555. Soggetti essenziali e importanti – e con essi le rispettive catene di fornitura – devono registrarsi presso l'ACN, adottare misure di gestione del rischio proporzionate e notificare gli incidenti significativi al CSIRT Italia.

Gli organi di amministrazione e direttivi rispondono direttamente dell'adeguatezza delle misure adottate e dell'assolvimento degli obblighi formativi.

CALENDARIO DEGLI OBBLIGHI

- **16 OTTOBRE 2024**
  Entrata in vigore del decreto: perimetro dei soggetti obbligati definito.
- **1 GENNAIO — 28 FEBBRAIO**
  Finestra annuale di registrazione e aggiornamento dei dati sulla piattaforma ACN.
- **ADEGUAMENTO PROGRESSIVO**
  Attuazione delle misure di sicurezza di base secondo le determinazioni ACN, nei termini previsti per ciascuna categoria.
- **OBBLIGO PERMANENTE**
  Notifica degli incidenti significativi: preallarme entro 24 h, notifica entro 72 h, relazione finale entro un mese.

10 M€ / 2%
SANZIONE MASSIMA SOGGETTI ESSENZIALI

7 M€ / 1,4%
SANZIONE MASSIMA SOGGETTI IMPORTANTI

24 h
PREALLARME AL CSIRT ITALIA DALLA CONOSCENZA DELL'INCIDENTE

LA FORTEZZA ON-PREMISE

Midgard risiede interamente nella vostra infrastruttura: nessun dato di scansione, inventario o vulnerabilità lascia il perimetro aziendale. La scelta progettuale garantisce sovranità del dato e piena compatibilità con i requisiti di data residency.

Il sistema opera anche in reti isolate: l'aggiornamento dei database CVE può avvenire tramite un unico canale controllato.

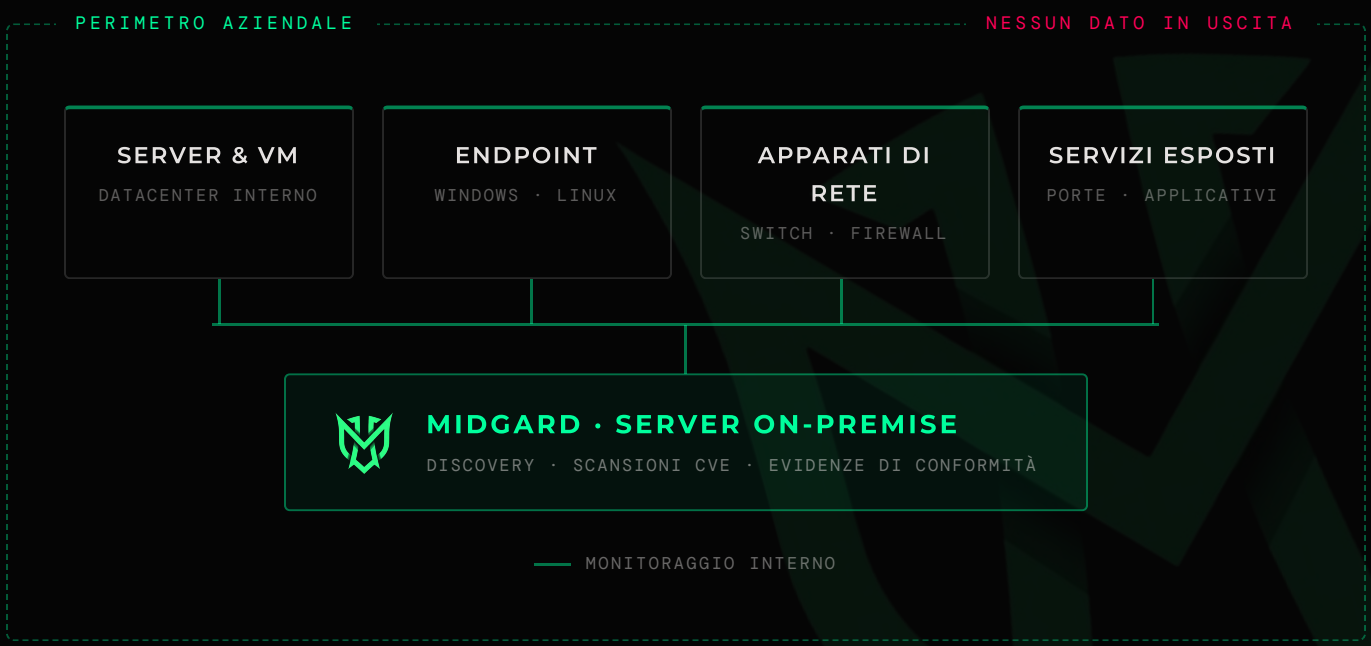
- SOVRANITÀ DEI DATI
- ISOLAMENTO DI RETE
- NESSUNA DIPENDENZA DA TERZE PARTI
- DEPLOYMENT SU VM O LXC CONTAINER

1 GIORNO

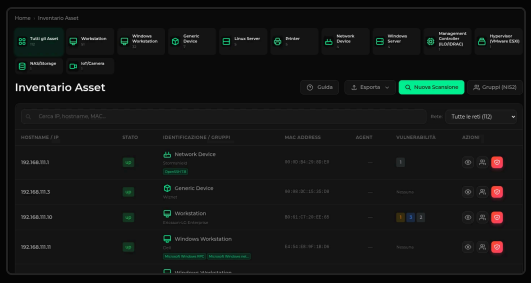
TEMPO TIPICO DI INSTALLAZIONE E PRIMO INVENTARIO

PERCHÉ CONTA

Il valore di un programma di gestione delle vulnerabilità dipende dalla continuità. Un'installazione rapida riduce il tempo che separa la decisione dalla prima evidenza utile per l'audit.



CAPACITÀ DI DIFESA 01

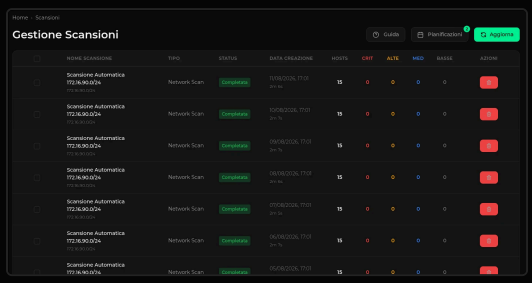


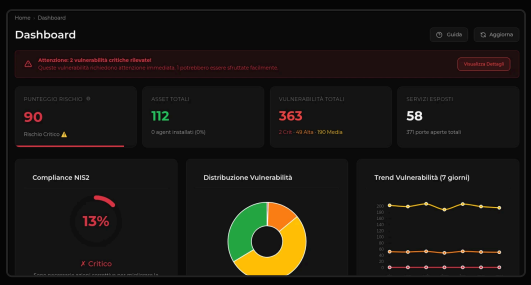
INVENTARIO ASSET

Discovery automatico e continuo dei dispositivi in rete, con rilevazione di sistema operativo, servizi esposti e criticità. La base di evidenza richiesta da qualunque framework di sicurezza.

SCANNER VULNERABILITÀ

Scansioni pianificate dell'intero perimetro interno con sincronizzazione quotidiana dei database CVE, per individuare le esposizioni prima che vengano sfruttate.



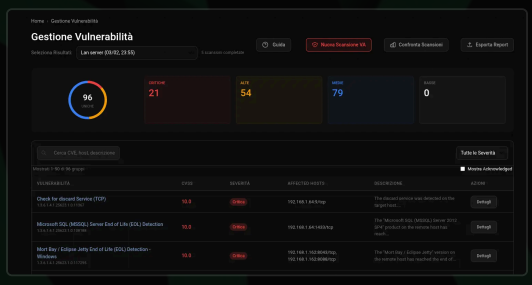


CENTRO DI COMANDO

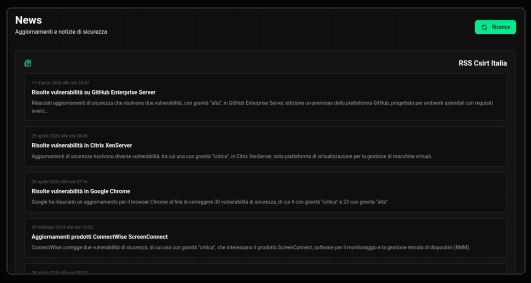
Dashboard direzionale con indicatori di conformità, distribuzione del rischio e andamento nel tempo: una lettura sintetica per le decisioni di priorità e di budget.

GESTIONE VULNERABILITÀ

Prioritizzazione basata su punteggio CVSS e contesto dell'asset, con tracciamento dello stato di remediation dalla rilevazione alla verifica di chiusura.



CAPACITÀ DI DIFESA 02

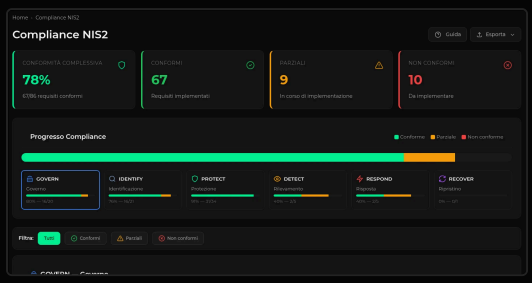


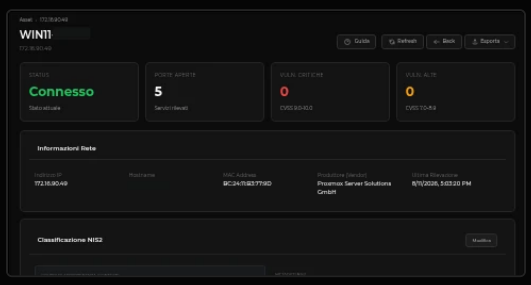
INTELLIGENCE MINACCE

Aggregazione dei bollettini del CSIRT Italia e delle principali fonti internazionali.

DASHBOARD COMPLIANCE

Stato di copertura dei requisiti tecnici NIS2, con evidenza immediata delle aree presidiate e di quelle da colmare.



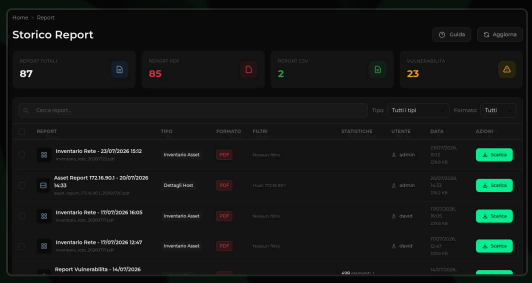


DETTAGLIO ASSET

Scheda granulare per ogni dispositivo: configurazione, software installato, vulnerabilità aperte e storico login (solo per server).

STORICO E REPORTISTICA

Archivio dei report con esportazione in PDF, Excel: la documentazione datata che dimostra la continuità del programma di sicurezza.



MATRICE DI CONFORMITÀ

ALLINEAMENTO ALLE MISURE DELL'ART. 21 · DIRETTIVA (UE) 2022/2555

REQUISITO TECNICO	RIFERIMENTO	COPERTURA MIDGARD
Gestione degli asset e inventario automatizzato	Art. 21(2)(i)	DISPONIBILE
Gestione e divulgazione delle vulnerabilità	Art. 21(2)(e)	DISPONIBILE
Analisi dei rischi sui sistemi informativi	Art. 21(2)(a)	DISPONIBILE
Valutazione dell'efficacia delle misure adottate	Art. 21(2)(f)	DISPONIBILE
Aggiornamento su nuove CVE e bollettini CSIRT	Art. 12 · Art. 29	DISPONIBILE
Evidenze e report esportabili per l'audit	Art. 21(1)	DISPONIBILE
Inventario software sugli endpoint	NIST CSF ID.AM-02	BETA v1

SISTEMA DI RACCOLTA DELLE EVIDENZE

Midgard non si limita a proteggere: produce le evidenze oggettive e datate che dimostrano la conformità tecnica agli auditor, riducendo i tempi di preparazione delle verifiche NIS2 e ISO/IEC 27001.

Nota: la matrice indica il contributo tecnico della piattaforma alle misure previste dalla normativa. Non costituisce certificazione di conformità, che dipende dall'assetto organizzativo complessivo del soggetto obbligato.

CUORE TECNOLOGICO

BASE: DEBIAN LINUX
ARCH.: X86_64 · ARM64 READY

ARCHITETTURA DI SISTEMA E DEPLOYMENT

MODULO_CORE

STACK OPERATIVO

Servizi containerizzati indipendenti: interfaccia web e API engine dimensionati per l'elaborazione continua dei dati di scansione.

MODULO_AGENTE

SENTINELLE ATTIVE

Agenti nativi Windows e Linux a impatto contenuto (CPU < 3% in condizioni operative tipiche) per il controllo di integrità e l'inventario software.

MODULO_DATI

STRATEGIA DATI

Doppio database: relazionale per la consistenza, time-series per lo storico delle scansioni. Cifratura AES-256 a riposo sul vostro storage.

REQUISITI INFRASTRUTTURALI MINIMI

PROCESSORE	4+ core	ARCHIVIAZIONE	200 GB SSD / NVMe
MEMORIA RAM	16 GB	SISTEMA OPERATIVO	Debian 12 / 13
PIATTAFORMA VM	VMware ESXi · Proxmox	CONTAINER	Proxmox LXC ready

I requisiti indicati coprono installazioni fino a circa 500 asset gestiti; per perimetri superiori il dimensionamento viene definito in fase di analisi preliminare.

ENTRA NEL REGNO

«La sicurezza non è un traguardo statico, ma una fortificazione continua del proprio perimetro digitale.»

RICHIEDI UNA DEMO

E-MAIL
info@midgardsec.it

WEB
www.midgardsec.it

DEMO
Su appuntamento