APPROVAZIONE SOPPRESSIONI · CONFORMITÀ NIS2

VulnApproval [Risk]

Il rischio accettato, formalmente firmato.

Trasforma la soppressione di una vulnerabilità in un atto di accettazione del rischio approvato dal CIO e firmato digitalmente — una Exception Policy NIS2 con ID univoco, pronta per l'audit.

Estrae. **Approva.** **Certifica.**

IL PROBLEMA

Una soppressione senza firma è una lacuna di conformità.

Nel normale ciclo operativo alcune vulnerabilità vengono soppresse temporaneamente su richiesta degli owner dei server. La Direttiva NIS2 (Art. 21) impone però di documentare e far approvare formalmente dal management ogni rischio accettato. Una soppressione senza approvazione del CIO è una lacuna di conformità — e un rischio in sede di audit.

Soppressioni informali

Le regole vivono dentro il VM system, decise via email o ticket. Nessun atto formale, nessuna firma del management.

Owner difficile da individuare

Chi ha chiesto di sopprimere, e perché? Ricostruire il responsabile del server è lavoro manuale e spesso impreciso.

NIS2 Art. 21

La normativa richiede gestione formale del rischio: documentazione, approvazione del management, evidenza conservata.

Rischio di audit

In sede di audit NIS2 o ISO 27001, una soppressione non approvata è un rilievo. Serve evidenza auditabile, non un foglio Excel.

> **Ogni soppressione è un rischio accettato che, senza una firma formale del management, resta scoperto in sede di audit.**

COME FUNZIONA

Dalla soppressione alla Exception Policy firmata.

SAAS NIS2 MULTITENANT

MULTILINGUA IT / EN

VulnApproval è il sistema SaaS gestito da Cyberfero che estrae le soppressioni da qualsiasi VM system supportato, arricchisce ogni record con l'owner del server da ServiceNow CMDB, compone un pacchetto in linguaggio manageriale per il Global CIO e ne raccoglie la firma digitale — emettendo una Exception Policy NIS2 formale (EP-XXX) come evidenza auditabile.

Evidenza pronta per l'audit

- **ID univoco** EP-YYYY-TTT-NNN per tenant e anno.
- **Firma digitale** del CIO con valore legale FEA / FEQ.
- **Conservazione 5 anni** immutabile, con hash SHA-256.

IL FLUSSO OPERATIVO

01
Sync VM
Pull automatico delle soppressioni ogni 24h

02
Arricchimento
Owner da ServiceNow CMDB + CVE da NIST NVD

03
Pacchetto EP
Scope, giustificazioni, misure compensative

04
Firma CIO
Portale CIO dedicato, firma o rifiuto con un clic

05
Archiviazione
Audit trail immutabile, reminder pre-scadenza

> **In caso di rifiuto, il sistema cancella automaticamente la soppressione nel VM system: la vulnerabilità torna visibile in pochi secondi, senza intervento manuale.**

FUNZIONALITÀ

Una piattaforma, ogni VM system, ogni legal entity.

AGNOSTICO

VM System agnostico — 8 piattaforme

Il connettore VM è configurabile per tenant e sostituibile senza impatto sul flusso di approvazione, sui documenti o sull'audit trail. Cambi piattaforma di Vulnerability Management aggiornando solo la configurazione del connettore.

- CrowdStrike Falcon — LIVE
- Tenable.io — VM
- Qualys VMDR — VM
- Rapid7 InsightVM — VM
- MS Defender — MDVM
- ConnectSecure — MSP
- Wiz — CLOUD
- OpenVAS — OSS

Architettura multitenant

Un'unica piattaforma gestisce tutte le legal entity del gruppo, ciascuna con dati isolati, credenziali cifrate e flusso di approvazione indipendente.

Integrazione ServiceNow CMDB

Arricchimento automatico con il nome del server owner (campo u_server_owner) direttamente dalla CMDB aziendale. Niente più ricerca manuale del responsabile.

Exception Policy NIS2 formale

Ogni ciclo genera un documento EP-XXX con ID univoco, scope, misure compensative e validità — evidenza pronta per audit NIS2 e ISO 27001.

Firma digitale flessibile

Firma integrata via API (DocuSign, Adobe Sign, Namirial…) o firma manuale con upload. Le due modalità coesistono, selezionabili anche dopo il go-live.

L'INTERFACCIA

Portale operatore e portale CIO.

PORTALE OPERATORE

Esempio Manufacturing S.p.A.

HOST / CRITERIO	TIPO	SERVER OWNER · CMDB	STATO
SRV-APP-01	A	M. Rossi CMDB	Da approvare
SRV-LNX-02	A	L. Bianchi CMDB	Da approvare
CVE-2024-50379	B	SRV-OT-07 · OT CMDB	Inviata
CVE-2026-24061	B	SRV-LNX-08 CMDB	Approvata
SRV-WEB-03	A	⚠ CMDB Gap	Da approvare

TENANT · GRUPPO ESEMPIO

- Esempio Manufacturing S.p.A. — LIVE
- Esempio Pharma S.p.A. — CONFIG
- Esempio Medical Systems — CONFIG
- Esempio Diagnostics Inc. — CONFIG

CICLO DI VITA EP

- DRAFT — in composizione
- INVIATA — al CIO
- APPROVATA — firmata
- RIFIUTATA — auto-revoca

EP-2026-ORG-043 · NIS2 Exception Policy

Risk Acceptance — Vulnerability Suppression

DIRETTIVA UE 2022/2555 · ART. 21

ORGANIZZAZIONE
Esempio Manufacturing S.p.A. · Gruppo Esempio

RISK OWNER
Global CIO

SCOPE
12 soppressioni · 3 host · 1 CVE critica

VALIDITÀ
01.06.2026 → 30.08.2026

Firmata digitalmente · FEQ eIDAS
Microsoft Entra ID · 28.05.2026 14:32 CET

HASH SHA-256
a3f1…9e7c

LA SUITE

REMEDIA + VulnApproval: governance end-to-end.

VulnApproval chiude il cerchio della remediation: quando una vulnerabilità non è sanabile nei tempi, governa l'accettazione formale del rischio fino alla firma del vertice. Un solo modello di asset, un solo SSO Entra ID, un solo audit trail.

Detection → Remediation → Soppressione → Approvazione CIO → EP NIS2

DUE MODALITÀ DI FIRMA, COESISTENTI

Mod. A — Firma via API

END-TO-END AUTOMATIZZATA

Il documento parte via API verso la piattaforma di firma; il CIO firma online, il file rientra via webhook.

- DocuSign · Adobe Sign · Namirial
- Valore legale FEA / FEQ

Mod. B — Firma manuale

ZERO DIPENDENZE ESTERNE

Il sistema genera il PDF, il CIO lo firma col proprio strumento e lo ricarica. Hash SHA-256 verificato prima e dopo.

- Aruba Sign · CNS/CRS · eIDAS
- Incluso nella versione base

SICUREZZA INCLUSA NEL CANONE

TLS 1.3 + LUKS
Cifratura in transito e a riposo.

Isolamento tenant
Dati separati crittograficamente.

Backup & SLA 99,5%
RPO 24h · RTO 4h · DC europeo.

Entra ID SSO
MFA e Conditional Access del cliente.

PERCHÉ CYBERFERO

Aderente al processo, non un GRC generalista.

Nessuna soluzione commerciale integra nativamente VM system multipli, workflow di approvazione manageriale, ownership da CMDB e firma flessibile in un unico flusso NIS2.

Aderenza totale

Sviluppato sul processo reale del cliente, con i dati reali del suo CMDB e del suo VM system — non un modulo generico da adattare.

Servizio gestito

Cyberfero gestisce infrastruttura, aggiornamenti, backup e monitoraggio. Zero onere operativo: il cliente firma, noi facciamo girare il resto.

Conformità NIS2 nativa

EP formale, firma del management, ownership tracciata, audit trail immutabile, revisione periodica: l'Art. 21 indirizzato per costruzione.

SOLUZIONE	CONNETTORE VM NATIVO	OWNERSHIP DA CMDB	EXCEPTION POLICY NIS2	SERVIZIO GESTITO
ServiceNow GRC	✗	✓	Parz.	✗
Archer GRC	✗	Parz.	Parz.	✗
VulnApproval · Cyberfero	✓	✓	✓	✓

Confronto indicativo tra categorie di soluzioni. « Parz. » indica una copertura solo parziale, ottenibile con moduli aggiuntivi e personalizzazioni.

PROSSIMI PASSI

VulnApproval [Risk]

Mettiamo in regola le tue soppressioni.

01

Demo del prototipo interattivo v3.0 — portale operatore e portale CIO — al CISO e al CIO.

02

Setup connettori: VM system, ServiceNow CMDB, registrazione app Entra ID.

03

Go-live sul tenant principale; le altre legal entity in onboarding progressivo.

+39 0522 1685330

info@cyberfero.com

www.cyberfero.com

Via Statuto 3, Reggio Emilia