SUPPRESSION APPROVAL · NIS2 COMPLIANCE

VulnApproval [Risk]

Accepted risk, formally signed.

Turns a vulnerability suppression into a formal risk-acceptance act, approved by the CIO and digitally signed — a NIS2 Exception Policy with a unique ID, audit-ready.

Extract. Approve. Certify.

THE PROBLEM

A suppression without a signature is a compliance gap.

In normal operations, some vulnerabilities are temporarily suppressed at the server owners' request. But the NIS2 Directive (Art. 21) requires every accepted risk to be documented and formally approved by management. A suppression without CIO approval is a compliance gap — and an audit risk.

Informal suppressions

Rules live inside the VM system, decided over email or tickets. No formal act, no management signature.

Owner hard to identify

Who requested the suppression, and why? Reconstructing the server owner is manual work and often imprecise.

NIS2 Art. 21

The directive mandates formal risk management: documentation, management approval, retained evidence.

Audit risk

In a NIS2 or ISO 27001 audit, an unapproved suppression is a finding. You need auditable evidence, not a spreadsheet.

> **Every suppression is an accepted risk that, without a formal management signature, stays exposed in an audit.**

HOW IT WORKS

From suppression to signed Exception Policy.

SAAS | NIS2 | MULTITENANT | BILINGUAL IT / EN

VulnApproval is the Cyberfero-managed SaaS that extracts suppressions from any supported VM system, enriches each record with the server owner from ServiceNow CMDB, composes a management-language package for the Global CIO and collects the digital signature — issuing a formal NIS2 Exception Policy (EP-XXX) as auditable evidence.

Audit-ready evidence

- ✓ **Unique ID** EP-YYYY-TTT-NNN per tenant and year.
- ✓ **Digital signature** by the CIO with FEA / FEQ legal value.
- ✓ **5-year retention**, immutable, with SHA-256 hash.

THE OPERATIONAL FLOW

01
VM sync
Automatic suppression pull every 24h

02
Enrichment
Owner from ServiceNow CMDB + CVE from NIST NVD

03
EP package
Scope, justifications, compensating controls

04
CIO signature
Dedicated CIO portal, sign or reject in one click

05
Archiving
Immutable audit trail, pre-expiry reminders

> **On rejection, the system automatically deletes the suppression in the VM system: the vulnerability becomes visible again within seconds, no manual work.**

CAPABILITIES

One platform, every VM system, every legal entity.

AGNOSTIC

VM System agnostic — 8 platforms

The VM connector is configurable per tenant and swappable with no impact on the approval flow, the documents or the audit trail. Switch Vulnerability Management platform by updating only the connector configuration.

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

Multitenant architecture

A single platform runs every legal entity in the group, each with isolated data, encrypted credentials and an independent approval flow.

ServiceNow CMDB integration

Automatic enrichment with the server owner name (u_server_owner field) straight from the corporate CMDB. No more manual owner lookup.

Formal NIS2 Exception Policy

Each cycle generates an EP-XXX document with unique ID, scope, compensating controls and validity — evidence ready for NIS2 and ISO 27001 audits.

Flexible digital signature

Integrated signature via API (DocuSign, Adobe Sign, Namirial…) or manual signature with upload. Both modes coexist, switchable even after go-live.

THE INTERFACE

Operator portal and CIO portal.

OPERATOR PORTAL

Esempio Manufacturing S.p.A.

HOST / CRITERION	TYPE	SERVER OWNER · CMDB	STATE
SRV-APP-01	A	M. Rossi CMDB	To approve
SRV-LNX-02	A	L. Bianchi CMDB	To approve
CVE-2024-50379	B	SRV-OT-07 · OT CMDB	Sent
CVE-2026-24061	B	SRV-LNX-08 CMDB	Approved
SRV-WEB-03	A	⚠ CMDB Gap	To approve

TENANTS · ESEMPIO GROUP

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

EP LIFECYCLE

- DRAFT — composing
- SENT — to the CIO
- APPROVED — signed
- REJECTED — auto-revoke

EP-2026-ORG-043 · NIS2 Exception Policy

Risk Acceptance — Vulnerability Suppression

EU DIRECTIVE 2022/2555 · ART. 21

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

RISK OWNER
Global CIO

SCOPE
12 suppressions · 3 hosts · 1 critical CVE

VALIDITY
01.06.2026 → 30.08.2026

Digitally signed · QES eIDAS
Microsoft Entra ID · 28.05.2026 14:32 CET

SHA-256 HASH
a3f1…9e7c

THE SUITE

REMEDIA + VulnApproval: end-to-end governance.

VulnApproval closes the remediation loop: when a vulnerability can't be fixed in time, it governs the formal risk acceptance through to leadership sign-off. One asset model, one Entra ID SSO, one audit trail.

Detection → Remediation → Suppression → CIO approval → NIS2 EP

TWO SIGNATURE MODES, COEXISTING

Mode A — API signature

AUTOMATED END-TO-END

The document is sent via API to the signing platform; the CIO signs online, the file returns via webhook.

- ✓ DocuSign · Adobe Sign · Namirial
- ✓ FEA / FEQ legal value

Mode B — Manual signature

ZERO EXTERNAL DEPENDENCIES

The system generates the PDF, the CIO signs it with their own tool and re-uploads. SHA-256 hash verified before and after.

- ✓ Aruba Sign · CNS/CRS · eIDAS
- ✓ Included in the base version

SECURITY INCLUDED IN THE FEE

TLS 1.3 + LUKS
Encryption in transit and at rest.

Tenant isolation
Cryptographically separated data.

Backup & 99.5% SLA
RPO 24h · RTO 4h · EU data center.

Entra ID SSO
Customer MFA and Conditional Access.

WHY CYBERFERO

Built to the process, not a generic GRC.

No off-the-shelf solution natively integrates multiple VM systems, management approval workflow, CMDB ownership and flexible signing into one NIS2 flow.

Total fit

Built on the customer's real process, with the real data from their CMDB and VM system — not a generic module to retrofit.

Managed service

Cyberfero runs infrastructure, updates, backups and monitoring. Zero operational burden: the customer signs, we run the rest.

Native NIS2 compliance

Formal EP, management signature, tracked ownership, immutable audit trail, periodic review: Art. 21 addressed by design.

SOLUTION	NATIVE VM CONNECTOR	CMDB OWNERSHIP	NIS2 EXCEPTION POLICY	MANAGED SERVICE
ServiceNow GRC	✗	✓	Partial	✗
Archer GRC	✗	Partial	Partial	✗
VulnApproval · Cyberfero	✓	✓	✓	✓

Indicative comparison across solution categories. "Partial" means coverage achievable only with add-on modules and customization.

NEXT STEPS

VulnApproval [Risk]

Let's bring your suppressions into compliance.

01

Demo of the interactive v3.0 prototype — operator portal and CIO portal — to the CISO and CIO.

02

Connector setup: VM system, ServiceNow CMDB, Entra ID app registration.

03

Go-live on the primary tenant; other legal entities onboarded progressively.

+39 0522 1685330

info@cyberfero.com

www.cyberfero.com

Via Statuto 3, Reggio Emilia