ALFAGROUP

RHDVM

We orchestrate. You stay secure.

Orchestrazione automatizzata. Maggior riduzione del rischio.

Per le aziende che gestiscono dati sensibili su server e applicazioni, la resilienza digitale non è più un lusso ma una necessità. **RHDVM** è una piattaforma sofisticata e efficiente per ridurre i rischi digitali gestendo l'esposizione cyber.

Le singole tecnologie possono essere efficaci nell'identificare i problemi legati alle vulnerabilità. Tuttavia, questo si traduce spesso in un numero eccessivo di avvisi e problemi che i team di sicurezza devono gestire.

La capacità di definire con accuratezza la superficie di attacco, aggregare e correlare dati da diverse fonti permette a RHDVM di fornire una **visione olistica e contestualizzata del rischio,** che supera la somma dei singoli risultati.

RHDVM SUPPORTA LE ORGANIZZAZIONI NELLA GESTIONE DELLE VULNERABILITÀ E NELLA RIDUZIONE DEI RISCHI CYBER

Combinando un potente motore di **orchestrazione e case management** con le **tecnologie di Vulnerability Assessment, Application Security e Breach Attack Simulation** leader di mercato, RHDVM integra il rilevamento, l'analisi, la prioritizzazione e la remediation delle vulnerabilità in un unico processo, continuo e ininterrotto, risultando in una gestione delle vulnerabilità più efficiente e basata sul rischio.

Alfa Group menzionata nella **SPARK Matrix™ per Exposure Management 2025**

Gartner Peer Insights

RHDVM menzionato nel report **Gartner® Market Guide per Vulnerability Assessment 2023.**

Un approccio basato sul rischio

Definisce metodi di misurazione, monitoraggio e reporting dei rischi a cui l'organizzazione è esposta

LEVA SULL'AUTOMAZIONE

Riduce le attività manuali, del TCO e della Cyber Exposure, grazie a una più rapida risposta alle vulnerabilità

GARANZIA DI UN PROCESSO CONTINUO

Aumenta l'efficacia e l'efficienza del processo di VM complessivo, grazie all'automazione del workflow basato sull'integrazione dei dati

IL VALORE DELL'ANALYTICS E DELL'INTELLIGENZA ARTIFICIALE

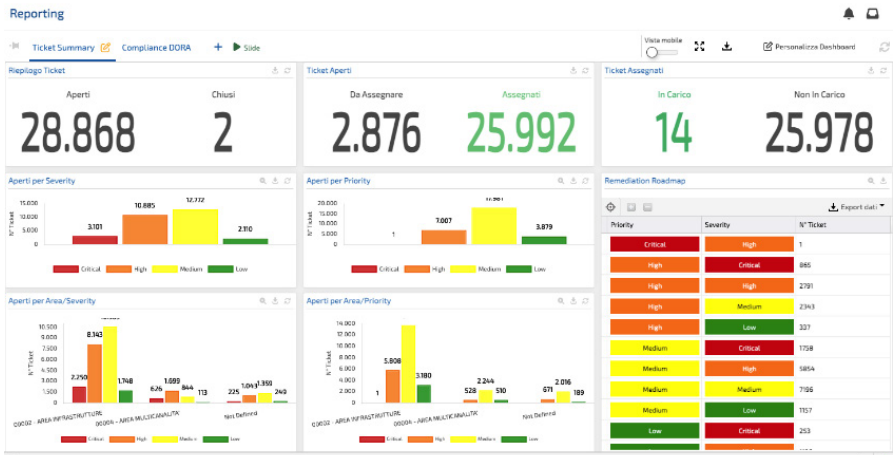
Migliora il processo decisionale sulla base del rischio con il supporto di tecnologie di Analytics e Artificial Intelligence per la prioritizzazione

*Fonte: Gartner, Guida al mercato per la valutazione delle vulnerabilità, Mitchell Schneider, Craig Lawson, Jonathan Nunez, 7 agosto 2023.

***SPARK Matrix™ (Strategic Performance Assessment and Ranking) è il framework proprietario di valutazione di QKS Group, disegnato per analizzare e classificare i vendor tecnologici.

Un unico repository per la gestione del rischio.

RHDVM offre un repository di vulnerabilità unificato per gestire tutto in un unico ambiente. Ora è possibile raccogliere e aggregare dati strutturati e non strutturati provenienti da varie fonti in un'**unica interfaccia**.
Condividi le **informazioni da un'unica fonte** con le parti interessate e coordina gli sforzi di correzione senza perdere tempo.



Connessione nativa a diverse fonti

- VA, DAST, SAST, SCA,
- attività manuali (RED Teaming e PT)
- tecnologie leader di mercato (connettori off-the-shelf)
- strumenti non standard (connettori personalizzati)

Archiviazione e gestione avanzata dei dati

- raccolta e archiviazione di dati da varie fonti in un unico ambiente
- database strutturati e NoSQL integrati per Big Data

Analisi, enrichment e correlazione dei dati

- miglioramento continuo dei KRI attraverso Business Analytics
- enrichment, aggregazione e correlazione dei risultati di VA con dati non relativi alle vulnerabilità
- gestione data-driven del workflow

PRIORITIZZAZIONE DELLE VULNERABILITÀ

Sfrutta le informazioni sulle minacce e il contesto aziendale per l'attività di remediation

Gestione semplice ed efficiente

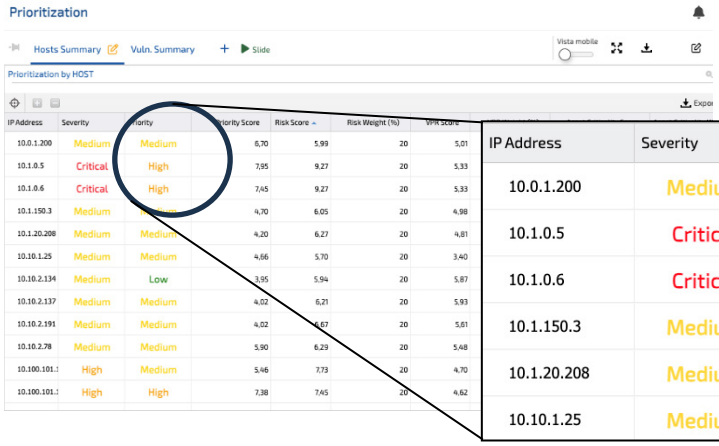
- arricchimento con dati di Threat Intelligence
- riclassificazione della severity basata sulla probabilità di sfruttamento
- indici di criticità degli asset e indicatori di priorità delle remediation

Prioritizzazione e remediation basati sul contesto

- raccolta di dati sugli asset critici
- adeguamento del flusso di remediation in base alla rivalutazione delle priorità
- KRI sulla security posture e action list

Exposure Intelligence

- benchmark con i peer del settore e confronto dell'efficacia KPI
- connettori off-the-shelf per più sorgenti di Threat Intelligence
- avvisi di corrispondenza tra modello di minaccia emergente e vulnerabilità



IP Address	Severity	Priority	Priority Score	Risk Score	Risk Weight (%)
10.0.1.200	Medium	Medium	6,70	5,99	20
10.1.0.5	Critical	High	7,95	9,27	20
10.1.0.6	Critical	High	7,45	9,27	20
10.1.150.3	Medium	Medium	4,70	6,05	20
10.1.20.208	Medium	Medium	4,20	6,27	20
10.10.1.25	Medium	Medium	4,66	5,70	20

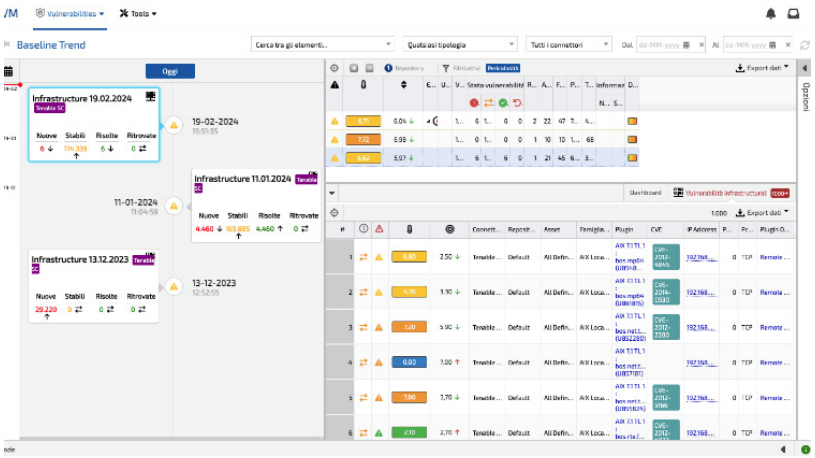
ASSET CRITICALITY

Individua, gestisci e prioritizza gli asset più critici per la tua organizzazione

RHDVM consente di sincronizzare e integrare le informazioni sulla gestione degli asset nel processo di Exposure Management

VANTAGGI

- definizione di quali vulnerabilità devono essere corrette per prime e identificazione degli stakeholder per ogni fase della remediation
- implementazione di KRI che collegano vulnerabilità e informazioni di business
- rilevazione host non funzionanti e asset sconosciuti
- gestione efficace dei requisiti normativi (ISO27001, NIST, ecc.)



Connessione nativa agli strumenti di asset management

- tecnologie leader di mercato (connettori off-the -shelf) e strumenti non standard (connettori personalizzati)

Registro di Asset Management migliorato

- impostazione di indicatori per la security posture di singoli/gruppi di asset
- individuare eventuali gap tra l'infrastruttura nota e quella reale
- tracciare l'evoluzione degli asset all'interno dell'organizzazione

Prioritizzazione delle attività di Remediation e Workflow management

- definizione delle priorità di remediation in base alla criticità degli asset
- coinvolgimento degli stakeholder appropriati per ogni fase di remediation
- remediation e mitigazione dei sistemi non funzionanti

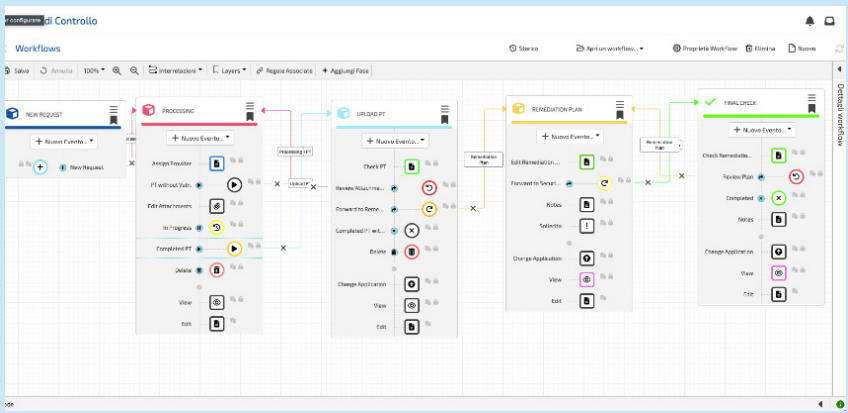
EXPOSURE WORKFLOW GOVERNANCE

Ottieni il pieno controllo del processo di gestione del rischio

RHDVM offre ai team di sicurezza la possibilità di pianificare e definire tutte le fasi del processo in linea con le esigenze dell'organizzazione.

VANTAGGI

- consente agli stakeholders di gestire tutte le vulnerabilità nel loro ambito
- monitora in tempo reale le attività di remediation e l'avanzamento per scopi di auditing e analisi performance
- definisce piani di remediation che includono vincoli, policy ed eccezioni.



Governance end-to-end della CTEM

- processo CTEM (Continuous Threat Exposure Management) in 5 fasi: scoping, discovery, prioritizzazione, validazione, mobilitazione
- pianificazione, progettazione e monitoraggio della strategia di remediation
- sistema di autorizzazione avanzato per la cooperazione tra team

Configurazione di Workflow personalizzabili

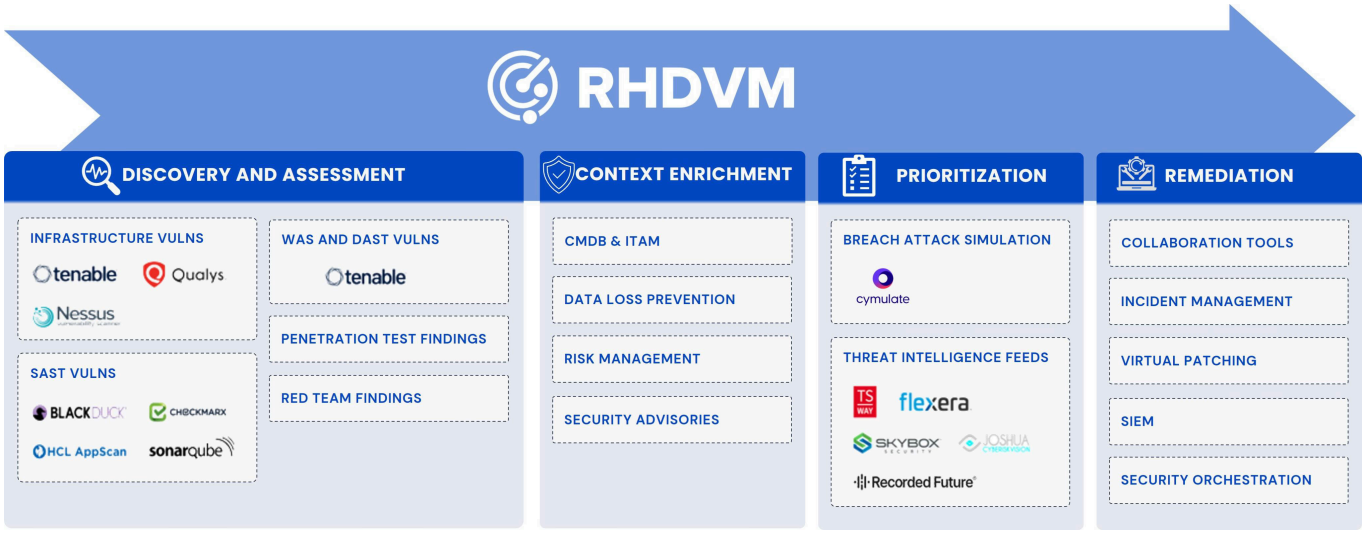
- personalizzazione attraverso low-code workflow editor
- moduli di input completamente personalizzabili
- configurazione di vincoli, criteri ed eccezioni
- configurazione di autorizzazioni, approvazioni, escalation e notifiche
- distribuzione di processi singoli o multipli per risultato

Come funziona RHDVM

RHDVM si integra nativamente con i principali strumenti di valutazione delle vulnerabilità, report di penetration test e red teaming e dati di threat intelligence.

La tecnologia utilizza connettori standard e personalizzati per raccogliere e fornire dati ad altre tecnologie, arricchendo, correlando e prioritizzando le attività di remediation per gli asset critici. Il suo motore di workflow e gestione del rischio offre processi preimpostati e un editor low-code per personalizzarli, garantendo piena **governance della security posture** del rischio.

Da un unico pannello è possibile osservare la posture di rischio in tempo reale. **RHDVM** può scambiare dati con sistemi esterni come software di IT Ticketing, SIEM/SOAR e CMDB per massimizzare l'integrazione.



Benefici di RHDVM

- Piattaforma di gestione condivisa delle vulnerabilità
- Visione olistica: centralizzazione dei dati di rischio
- Orchestrazione dati end-to-end: correlazione e aggregazione delle informazioni per generare insight utili a indirizzare la prioritizzazione, adottando un approccio risk-based
- Aumento dell'efficienza operativa

Scopri di più

www.alfagroup.ai **info@alfagroup.ai** **@AlfaGroupIT**

Alfa Group S.p.A. è una PMI Innovativa italiana in rapida crescita e il partner strategico per potenziare la resilienza della sicurezza digitale, promuovendo attivamente una cultura in cui i rischi di frode cyber e digitale sono considerati in ogni azione strategica. Grazie a soluzioni all'avanguardia come N.O.V.A. (Next-Gen Operations for Vulnerability & Antifraud) e alla tecnologia proprietaria RHD, l'azienda sfrutta l'Intelligenza Artificiale avanzata per rilevare e prevenire le frodi. Il suo approccio integrato (persone, dati, processi e tecnologia) garantisce un impatto misurabile: sul mercato da quasi 30 anni, Alfa Group protegge oltre 120 istituti finanziari, monitora circa 23 milioni di utenti con le sue soluzioni di Fraud Management e mette in sicurezza più di 450.000 asset IT attraverso i suoi servizi di Cyber Exposure Management.
Per maggiori informazioni visita **www.alfagroup.ai**