RHDVM

GOVERNANCE END-TO-END DEL CICLO DI VITA DELLE VULNERABILITA'

Oggi le organizzazioni si affidano sempre più a soluzioni e applicazioni software per migliorare la propria efficienza operativa: questo comporta una superficie di attacco molto più ampia che include un numero sempre crescente di vulnerabilità. Gli scanner di vulnerabilità sono molto efficaci nel rilevare le vulnerabilità, ma per i team di sicurezza questo risulta in innumerevoli alerts da controllare e problemi da risolvere.

Ma non tutte le vulnerabilità hanno lo stesso livello di criticità: le organizzazioni complesse devono ottimizzare effort e risorse spesso limitati, per concentrarsi su quelle che costituiscono una minaccia reale per il business.

RHD VM SUPPORTA LE ORGANIZZAZIONI NELLA GESTIONE DELLE VULNERABILITÀ E NELLA RIDUZIONE DEI RISCHI CYBER.

Combinando un potente motore di orchestrazione e case management con tecnologie di Vulnerability Assessment leader di mercato, RHD VM 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.

IL NOSTRO VALORE

- **UTILIZZARE UN APPROCCIO BASATO SUL RISCHIO**
  Definire metodi di misurazione, monitoraggio e reporting dei rischi a cui l'organizzazione è esposta
- **FARE LEVA SULL'AUTOMAZIONE**
  Riduzione delle attività manuali, del TCO e della Cyber Exposure, grazie a una più rapida risposta alle vulnerabilitità
- **GARANTIRE UN PROCESSO CONTINUO**
  Aumentare l'efficacia e l'efficienza del processo VM complessivo, grazie all'automazione del workflow basato sull'integrazione dei dati
- **TRARRE VALORE DA ANALYTICS E INTELLIGENZA ARTIFICIALE**
  Migliorare il processo decisionale sulla base del rischio con il supporto di tecnologie di Analytics e Artificial intelligence per la prioritizzazione

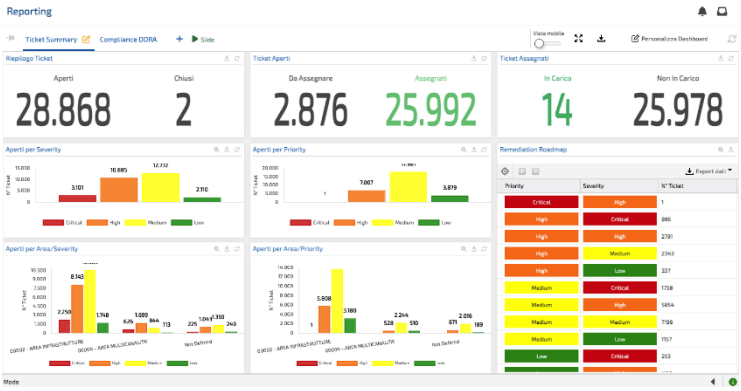
* Fonte: Gartner, Guida al mercato per la valutazione delle vulnerabilità, Mitchell Schneider, Craig Lawson, Jonathan Nunez, 7 agosto 2023.

KEY CAPABILITIES

REPOSITORY UNIFICATO DELLE VULNERABILITÀ
Gestisci tutte le vulnerabilità in un unico ambiente

RHD VM consente la raccolta e l'aggregazione di dati strutturati e non strutturati provenienti da fonti diverse in un repository unificato che permette di:

- analizzare, correlare e aggregare qualsiasi tipo di vulnerabilità in un'unica interfaccia grafica;
- condividere le informazioni con i giusti stakeholder e
- pianificare la remediation;
- definire KRI specifici per determinare la Security Posture aziendale



Connessione nativa a diverse fonti:
VA, DAST, SAST, SCA, attività manuali (RED Teaming e PT), tecnologie leader di mercato (utilizzando connettori off-the-shelf), strumenti non standard (utilizzando connettori personalizzati).

Archiviazione e gestione avanzata dei dati:

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

Analisi, Enrichment e Correlazione dei dati:

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

PRIORITIZZAZIONE DELLE VULNERABILITÀ
Sfrutta le informazioni sulle minacce e il contesto aziendale per definire le attività di remediation

RHD VM fornisce una gestione semplice ed efficiente della prioritizzazione delle vulnerabilità e delle attività di remediation attraverso:

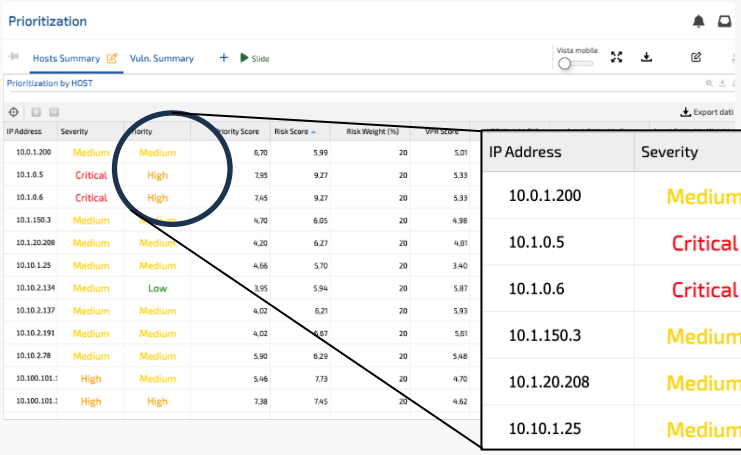
- arricchimento delle informazioni sulle vulnerabilità con dati di Threat Intelligence;
- riclassificazione della severity delle vulnerabilità basata sulla loro probabilità di essere sfruttate;
- indici di criticità degli asset e indicatori di priorità delle remediation.

Prioritizzazione e remediation basati sul contesto:

- raccolta di dati sugli asset critici;
- adeguamento del flusso di remediation in base alla rivalutazione delle priorità;
- KRI che mostrano la security posture e le azioni da intraprendere per prime.

Vulnerability Intelligence:

- connettori off-the-shelf per più sorgenti di Threat Intelligence;
- connettori Tenable Lumin per Vulnerability Intelligence forniscono un benchmark con i peer del settore e un confronto dell'efficacia dei KPI;
- avvisi di corrispondenza tra un modello di minaccia emergente e una vulnerabilità nota.



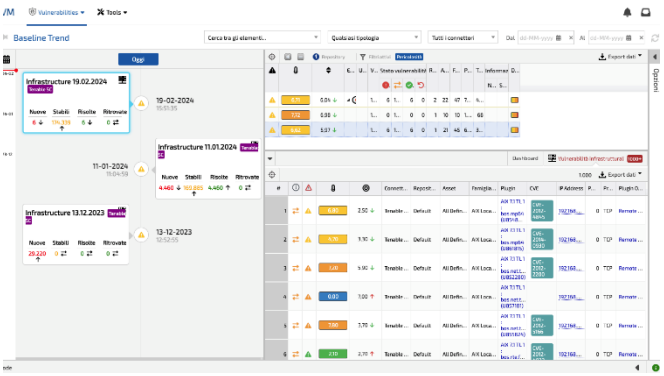
IP Address	Severity	Priority	Priority Score	Risk Score	Risk Weight (%)
10.0.1.200	Medium	Medium	6,70	5,99	20
10.1.0.5	Critical	High	7,95	9,27	20
10.1.0.6	Critical	High	7,45	9,27	20
10.1.150.3	Medium	Medium	4,70	6,05	20
10.1.20.208	Medium	Medium	4,20	6,27	20
10.10.1.25	Medium	Medium	4,66	5,70	20

KEY CAPABILITIES

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

RHD VM consente di sincronizzare e integrare le informazioni sulla gestione degli asset nel processo di Vulnerability Management, al fine di:

- determinare quali vulnerabilità devono essere corrette per prime;
- sapere quali stakeholder devono agire in ogni fase del processo di remediation;
- implementare KRI che correlino le vulnerabilità e le informazioni di business;
- rilevare host non funzionanti e/o asset sconosciuti;
- affrontare efficacemente più requisiti di conformità (ISO27001, NIST, ecc.).



Connessione nativa agli strumenti di asset management:

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

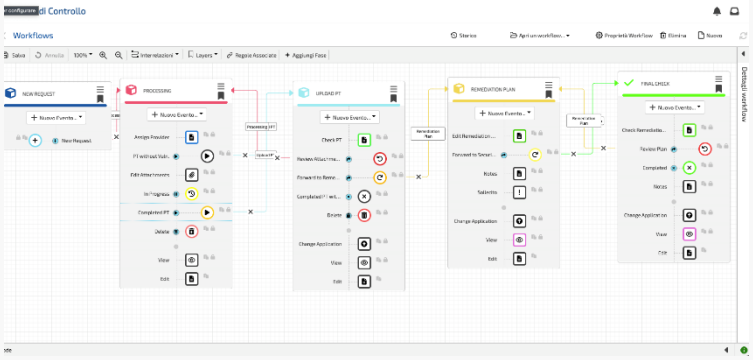
Prioritizzazione delle attività di Remediation e Workflow Management:

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

VULNERABILITY WORKFLOW GOVERNANCE
Ottieni il pieno controllo del processo di gestione delle vulnerabilità

RHD VM offre ai team di sicurezza la possibilità di pianificare e definire tutte le fasi del processo in linea con le esigenze dell'organizzazione. Questo permette di:

- consentire agli stakeholders di gestire tutte le vulnerabilità nel loro ambito;
- monitorare in tempo reale le attività di remediation e il loro avanzamento per scopi di auditing e valutazione delle prestazioni;
- definire piani di remediation che tengano conto di vincoli, policy ed eccezioni.



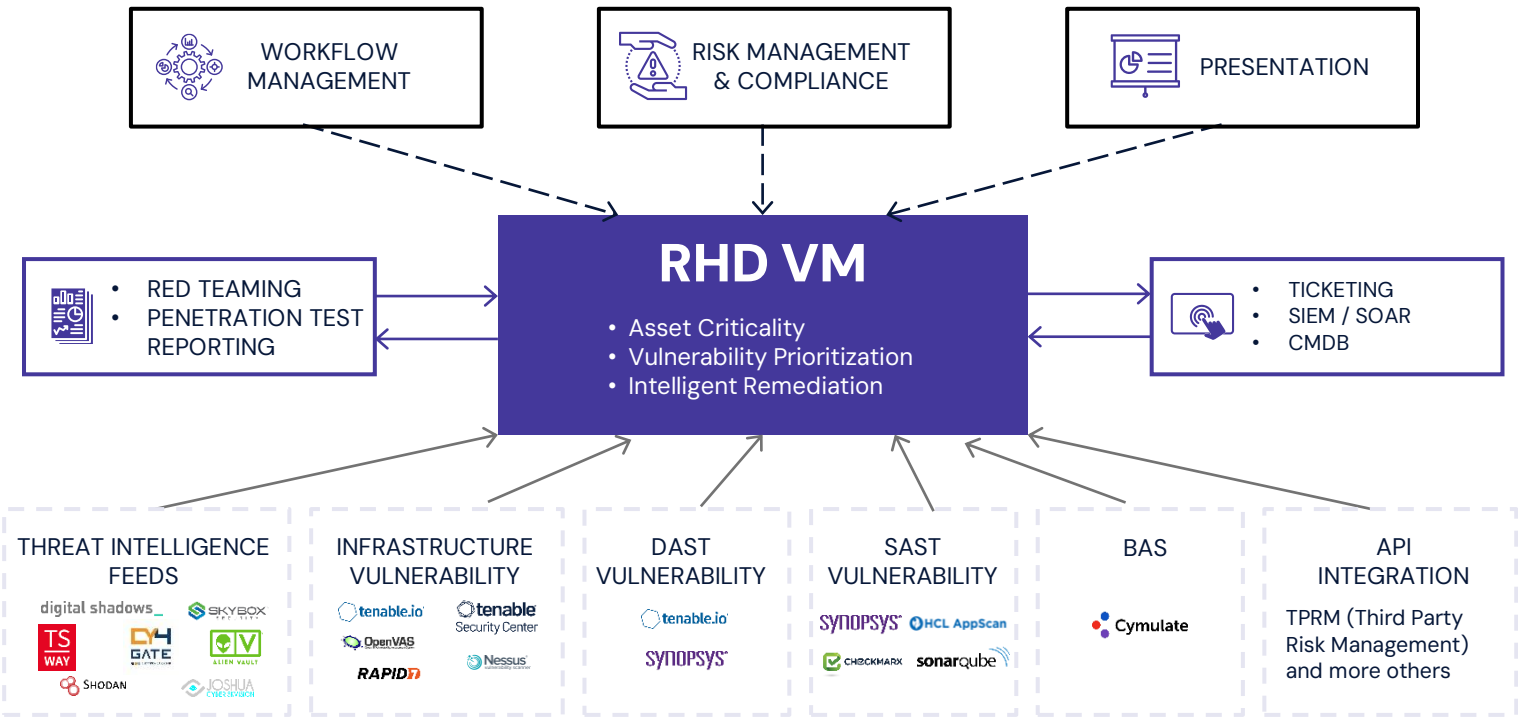
Governance end-to-end della gestione continua dell'esposizione alle minacce:

- 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;
- monitoraggio in tempo reale delle attività di remediation per scopi di auditing e valutazione delle prestazioni.

Creazione e Configurazione di Workflow Personalizzabili:

- «low-code» workflow editor per una completa personalizzazione;
- 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 ogni tipo di risultato.

HOW RHD VM WORKS



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

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. RHD VM può scambiare dati con sistemi esterni come software di IT Ticketing, SIEM/SOAR e CMDB per massimizzare l'integrazione.

RHD VM è la soluzione ideale per organizzazioni complesse e grandi imprese che:

- cercano uno strumento collaborativo per la gestione delle vulnerabilità;
- hanno uno o più Vulnerability Scanners e Prioritization Technologies implementati con successo e hanno bisogno di centralizzare e orchestrare i loro dati;
- hanno bisogno di arricchire e correlare i dati sulle risorse e sulle vulnerabilità provenienti da diverse fonti interne ed esterne;
- hanno difficoltà a stabilire le priorità delle attività di remediation in base alle metriche di rischio aziendale;
- vogliono semplificare il processo di remediation delle vulnerabilità e ridurre le attività manuali e l'intervento umano.

www.alfagroup.it
info@alfagroup.it
@AlfaGroupIT