ALFAGROUP

RHDVM

GET FULL, EXTENSIVE GOVERNANCE OF THE ENTIRE VULNERABILITY LIFECYCLE

THE GOVERNANCE CHALLENGE IN VULNERABILITY MANAGEMENT

Today's organizations rely more and more on software solutions and applications to improve their operational efficiency; these technologies are prone to vulnerabilities that can be exploited by cyberattackers. While many of them already have in place the tools for detecting and addressing these vulnerabilities, the underlying Vulnerability Management process is often overlooked, resulting in a disavantage in vulnerability response:

- **57% of organizations don't know which vulnerabilities pose the greatest risk to their business**
- **73% of organizations do not claim to have complete visibility into the vulnerability management lifecycle**
- **60% of data breach victims say they were breached due to a known unpatched vulnerability**
- **52% of organizations say they are at a disadvantage in responding to vulnerabilities due to the use of manual processes**

Data Source: Ponemon Institute

Manual processes hinder the timely patching of vulnerabilities: **in 2021, the estimated average time for a patch is 102 days.**

The automation and end-to-end governance of Vulnerability Management processes can help significantly reduce the time and effort required to respond to vulnerabilities.

THE PRIORITIZATION CHALLENGE IN VULNERABILITY MANAGEMENT

Vulnerability priotization has been identified by security professionals as one of the top challenges when it comes to Cyber Security. Vulnerability scanners do a great job at detecting vulnerabilities, and this leaves security teams with thousands and thousands of alerts to check and issues to address. Luckily, not all of them share the same level of criticality, but this makes determining which vulnerabilities need more attention and in which order a key step of Vulnerability Management. Organizations rely on different criteria for prioritization, for example:

- **38% of organizations relies on Common Vulnerability Scoring System (CVSS) as a vulnerability security score**
- **37% of organizations takes into account which vulnerabilities are most likely to be used by attackers**
- **25% of organizations takes into account which exposed assets are most important/ critical for the business**

On average, each scan detects 779.935 unique vulnerabilities.

Organizations can't possibily verify and patch each and every one of them and, without a clear prioritization process, teams struggle to agree upon which vulnerability might pose a greater risk for the business, delaying remediation and wasting precious time. Risk-Based Vulnerability management **and business contextualization of vulnerabilities** help determine their actual risk level and decide which ones need to be addressed first.

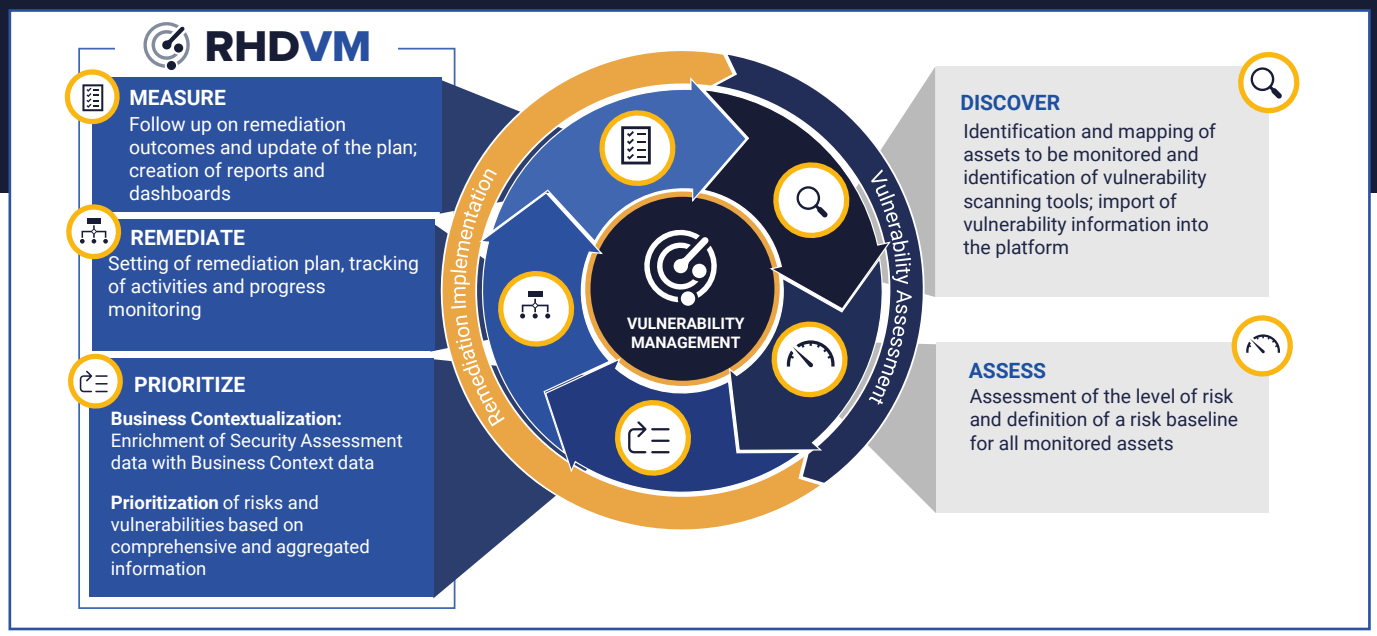
RISKS AND LIMITATIONS IN CURRENT SOLUTIONS

- Remediation process management is often not available or extremely limited
- The business context "weight", of the single asset within the organization is often not taken into consideration by the levels of aggregation available in most platforms
- CISOs need an integrated overview that also includes external security assessments
- Most Vulnerability Management solutions are not designed from a process perspective
- Processing and analyzing Vulnerability data takes as much time as remediation efforts
- Manage Cyber exposure and avoid a breach from exploited unpatched system.
- Lack of Historical data showing which platforms take more time to patch than others, and why.
- Lack of remediation metrics to track and key performance indicators (KPIs)

THE **ALFA GROUP** SOLUTION: RHDVM

RHD VM is the solution developed by Alfa Group to specifically address these Vulnerability Management challenges.

Combining industry-leading Vulnerability Management technologies with the Alfa Group Digital Business Process Management, Case Management and Orchestration platform, RHD VM allows the entire lifecycle of vulnerability management to be part of an integrated and continuous security process, resulting in better risk management and efficient remediation flow.



KEY CAPABILITIES

INTEGRATED VULNERABILITY MANAGEMENT

REMEDIATION FLOW

RHD VM allows agile management of the remediation flow for each detected vulnerability, thanks to its process design visual configuration features:

- Creation of the remediation workflow
- Enrichment of Asset information
- Setting of remediation plan
- Implementation and monitoring of remediation plan
- Follow-up and closing

RISK MANAGER

RHD VM allows the prioritization of risks and remediation actions by combining the action of Vulnerability Management technologies already present in the organization with the integrated Asset Manager.

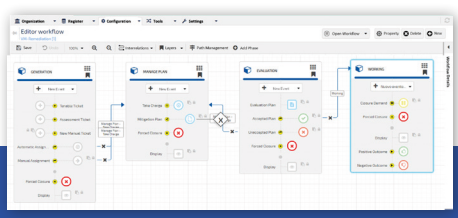
The Vulnerability View includes:

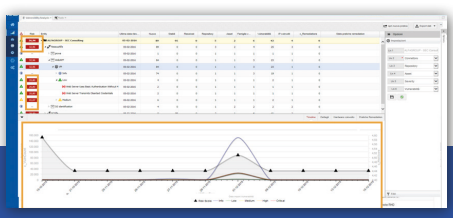
- Risk index
- Severity index
- Assets involved
- Vulnerability details
- Timeline

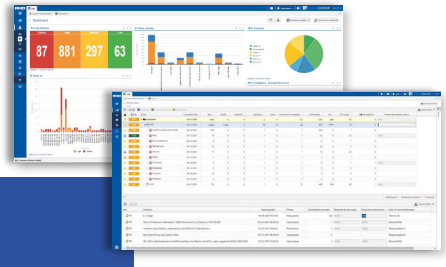
VA TREND & ANALYTICS

RHD VM's Data Visualization provides a comprehensive and immediate view on the vulnerabilities acquired by the RHD Connector. It allows the analysis of asset, vulnerability, risk and remediation details, at various levels of depth.

Dashboards and detailed views are both adaptable to the specific needs of the company through customizable widgets.







TECHNOLOGY INTEGRATION

RHD VM's push / pull technology (the so called "Connectors") allows RHD VM to gather from and provide data to other softwares and solutions, to enrich and orchestrate all Vulnerability information from a single interface.

RHD VM comes with built-in connectors with the major Cyber Risk Management technologies on the market, including (but not limited to): Tenable (and Nessus), Digital Shadows, Q6 Cyber, Qualys.

Want to know more about RHD VM? Scan here!

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