AFKC
Value-Added Distributor

WHITE PAPER

VULNERABILITY MANAGEMENT

How to support an effective Vulnerability Management Program

TABLE OF CONTENTS

1. INTRODUCTION

Vulnerability management is important to an organization's overall security posture, and many organizations already have an established vulnerability management program, but most of this programs are unable to evaluate and prioritize vulnerability data effectively.

The purpose of this whitepaper is to provide knowledge about how to build an effective Vulnerability Management program in order to:

- Prioritize known vulnerabilities
- Shorten remediation times
- Increase emerging threat visibility
- Support both IT and Security Operation

2. THE KEY TO AN EFFECTIVE VULNERABILITY MANAGEMENT

2.1 When is Vulnerability Management "Effective"?

Cyberthreats are constantly evolving, Data breaches happen more frequently, Organizations need to implement a robust vulnerability management program too.

Vulnerability management is more than just running a vulnerability scanner and adjusting the resulting vulnerabilities on an annual basis. A vulnerability management program should be a robust program that includes multiple scans per year, detailed tracking and remediation, vulnerability and root-cause analysis, as well as finite reporting.

2.2 What and Where is the Gap for the adoption?

One of the difficulties of adopting a consistent program for Vulnerability Management derives from the fact that very often in Security we observe plenty of technologies which operate and think in silos, but which lack, above all, all that concerns processes and the overview of the specific issue.

In the world of Vulnerability Management there are mainly two shortcomings that may be suffered by the various market players?

- The overview of the world of vulnerabilities, often coming from completely different sectors such as, Network, Systems and Application;
- The management of the Remediation necessary to plan the activities and to keep both the IT and Security Management, the internal or external auditors, informed on the updated status of all remediation activities

2.3 Why leverage a VM Tool to be effective in the VM Program?

RHD4VM (RHD for Vulnerability Management) has been engineered fundamentally to fill these two important gaps.

RHD4VM allows to detect and manage the vulnerabilities as part of an integrated and continuous process, resulting in faster identification of the vulnerabilities and easier management of their remediation flow.

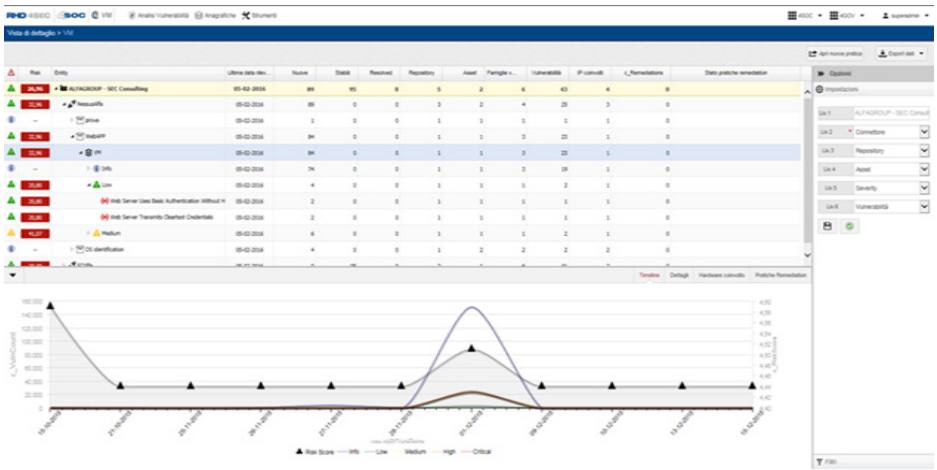
One of the main tasks of RHD 4VM is to gather information coming from completely different sources on which vulnerabilities are analysed. It is detached from the technology that scans the technological vulnerabilities (through connectors it can work with the most widespread market players like Tenable, Rapid7, Qualys, etc ..).

Specifically, RHD4VM provides 4 macro tasks:

FIG.5
The RHD 4VM Solution

- **Vulnerability Trend:** allows to see the trend of vulnerabilities in an integrated manner. Often the VM tools offer a static view of the situation, but what is important for managers is not only to have a view on the state of Vulnerabilities at a given moment, but also to monitor how vulnerabilities evolve over time, and to verify if the remediation activities undertaken have been effective (as testified by a decreasing trend).

FIG.2
Vulnerability Trend



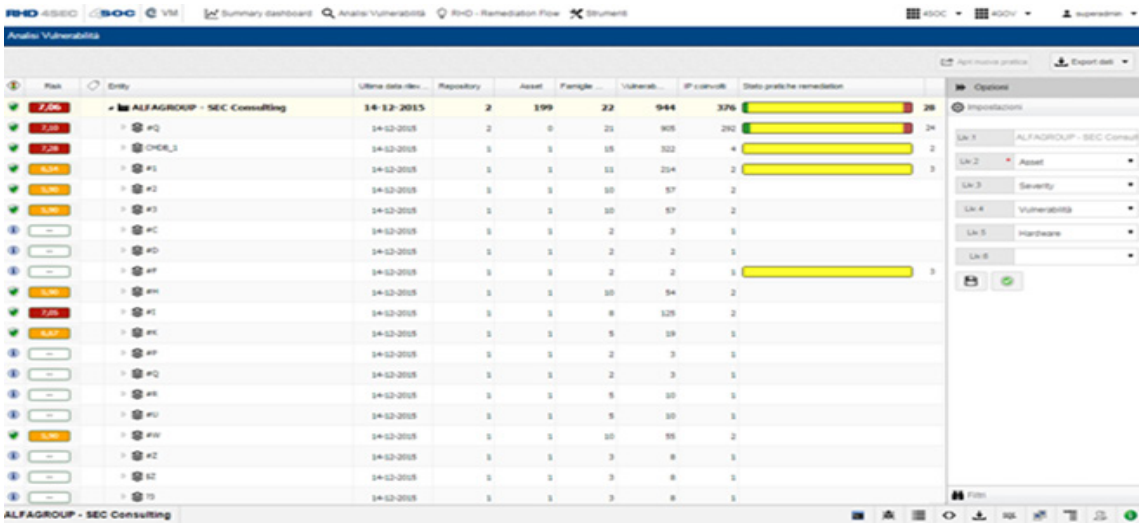
How important it is to show the trends to the auditors, so given the situation for each check that is made that this trend is improving over time and therefore actions are strategic actions fall both as volume but especially in the timing that we are declared in company.

- **Remediation Flow**: allows to easily manage the remediation flow of each detected vulnerability, thanks to RHD's process design features. Straight from the detail view of each vulnerability, RHD 4VM allows the user to open tickets which are already inclusive of all of the gathered data related to it, such as:
    - criticality of the vulnerability
    - detailed information
    - hardware involved

The case status is constantly made visible through progress bars, both available in the Vulnerability view and among the involved Asset detail, showing the evolution of the Remediation process and the status of its Tickets.

FIG.3

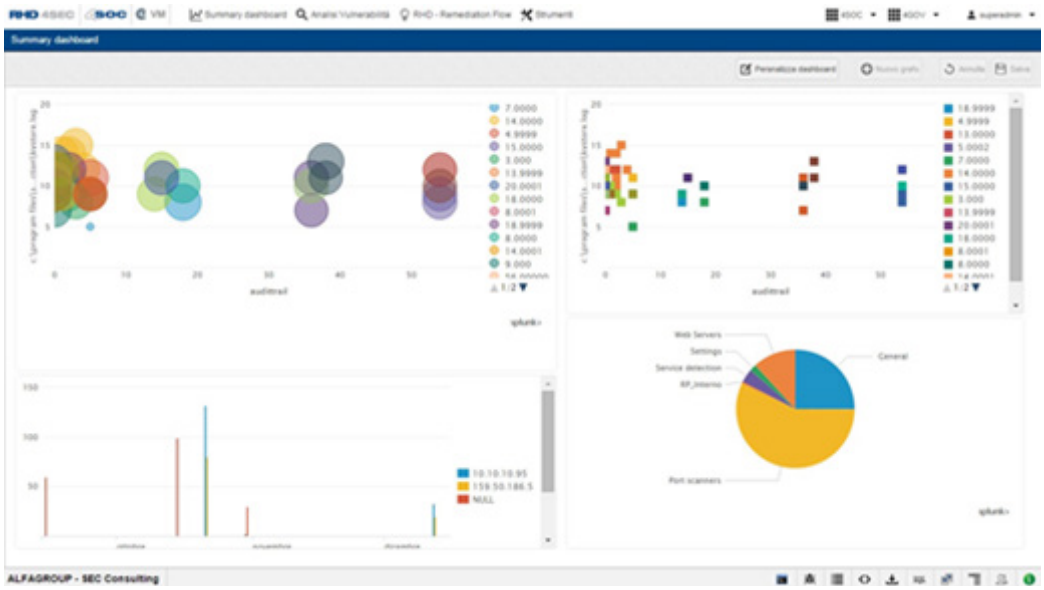
Remediation Flow



- **Risk Manager:** It is part of risk management because risk factors are associated with each vulnerability. Technological risk (often present in the international databases used by the scanners) must be correlated with the Role that a specific device / object / application has within the Organization. We can have a list of weighted risks for each Asset that define the Criticality inside the organization and prioritize the Remediation activities

- **Analytics:** collecting data and storing them, you can create reports, trend statistics and so on (FIG. 4)

FIG.4
Analytics



3. RHD 4VM: KEY FEATURES

Presentation & Reporting

- Dashboard for integrated analysis
- Real-Time Vulnerability Overview & Data Drill-Down
- Time comparison between scans with evidence of the solved/detected vulnerabilities
- Evidence of risk for both assets and services
- Dashboards and detailed views both customizable and adaptable to the specific needs of the company

Workflow

- Remediation Workflow Management with different group levels, both for services and for assets
- Automatic or Manual remediation ticket management
- Graphic Workflow creation and customisation

Administration

- Access Control
- User, Groups and Profiles management
- Registries integration with Corporate Active Directory/LDAP
- Granular profiling in relation to every single feature of the suite

Integration

- Connector Management for Tenable (Nessus, Security Center and Security Center Continuous View), Qualys and Rapid7
- Connector configuration management
- Scheduled execution of each “connector”

Asset Management

- Basic: IP and Object based
- Advanced: All the necessary information related to the specific Asset in the Organization

Companies need agile and flexible tools to reduce the risk surface, reduce the cost and complexity of vulnerability management with automated scans, actionable reports, automated remediation process based on Criticality and Prioritize the actions to reduce the security risk posture. RHD4VM is the answer.

9. WHY AFKC

Despite its recent foundation in 2016, AFKC relies on a team of professionals with many years of experience in Cyber Security and Anti-Fraud

AFKC operates through offices located in Italy and The Netherlands, ensuring a consistent presence on the National and International territory.

Adding our knowledge to Kaspersky Lab's solutions, we are able to help our Partners protect End User's Business, Information and Infrastructures from Advanced Threats, Cyber Attacks and Cybercrime. We work in cooperation with our Partners (System Integrators, Solution Providers, MSPs, VARs and Resellers) offering highly specialized services and dedicated contact persons.

Our Services

SALES ENABLEMENT

PRESALES ENABLEMENT

INTEGRATED SOLUTIONS

EDUCATION

PROFESSIONAL SERVICES

TECHNICAL SUPPORT

AFKC
Value-Added Distributor

CONTACTS

AFKC B.V.

Papendorpseweg 100
3528 BJ Utrecht, Netherlands
+31 030 799 1037
info@afkc.eu

AFKC s.r.l.

Via Fiume Giallo, 3
00144 Rome, Italy
+39 06 522 44040
info@afkc.eu

WWW.AFKC.EU