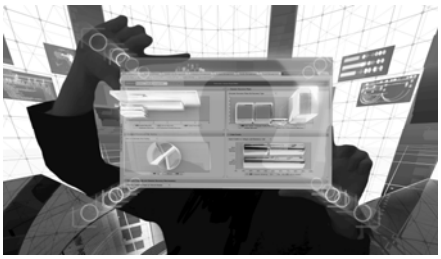
RSA VULNERABILITY RISK MANAGEMENT

Manage Entire Vulnerability Lifecycle



AT-A-GLANCE

- More secure organization with proactive management of IT security risks
- Accurate identification and prioritization of vulnerability issues
- Automation of vulnerability-management process to address issues
- Assign, measure, and report on vulnerability program KPIs

CHALLENGES

A global survey of 200 organizations shows that 40% of enterprises are overwhelmed with the security data they already collect[1]: terabytes of vulnerability scan results, configuration databases, system logs, and thousands of unknown IP addresses.

At the same time, organizations don't have an adequate understanding of this information and find it hard to answer critical questions, such as:

- How many assets do we have?
- What is the business context of each asset?
- What is the risk to my enterprise from vulnerabilities detected?

IT security analysts generally find it extremely difficult to parse these volumes of data in a consistent way. At the same time, management struggles to correlate the organization's key performance indicators (KPIs) with security information.

SOLUTION

RSA Vulnerability Risk Management (VRM) allows organizations to proactively manage IT security risks by combining asset business context, actionable threat intelligence, vulnerability assessment results, and comprehensive workflows.

For IT security analysts, VRM's analytics engine analyzes and correlates all available vulnerability and threat-intelligence data and identifies as issues the vulnerabilities impacting an organization's assets. Information is presented via an easy-to-use dashboard which provides alerts prioritized by issues, assets, and vulnerabilities along with workflow status to track issues and custom KPIs. With VRM, analysts can improve security by addressing the most important issues first as well as save time and money spent on manual tracking and report generation.

For business and IT managers, VRM's management module integrates VRM analytics with reporting, workflows, and a risk-management framework to enable data-driven security decisions and integrate KPIs into actionable plans. Workflows are automated and fully integrated with the ticketing process, enabling the IT operations team to engage with business units and other stakeholders to make informed security decisions and address vulnerabilities rapidly and consistently.

Using VRM, an organization can reduce security risk with a proactive, data-driven approach as well as meet regulatory compliance requirements.

KEY BENEFITS

Key capabilities of VRM include:

- Leveraging Big Data analytics to aggregate massive amounts of security data
- Creating and maintaining an accurate asset catalog
- Prioritizing and classifying issues based on business context, threat intelligence, and vulnerability scan results
- Tracking issues over the entire lifecycle – detection, remediation, and verification.
- Managing issues, exceptions, and remediation workflows
- Assign, measure and report on vulnerability program KPIs

[1]The Rise of Data-Driven Security – Enterprise Management Associates, Inc

KEY FUNCTIONALITY

– ***Correlate and normalize vulnerabilities and threat intelligence***

Leverage Big Data analytics to aggregate and consume massive amounts of raw data from multiple sources – vulnerability scan results, threat intelligence, and asset repositories (CMDBs, CSVs). VRM uses SCAP standards such as CVE, CPE, and CVSSv2 to store data in a standard format. In addition, an analyst can easily adjust severities according to business needs, taking advantage of VRM's capability to support CVSS v2 scores as well as user-defined scores.

– ***Track assets with business context and not just IP addresses***

VRM tracks and reports devices as unique assets. VRM catalogs IT assets and correlates with existing configuration management databases (CMDBs) to merge top-down and bottom-up attributes for the IT assets. Using VRM, the analyst can make quick prioritization decisions by using the business context of an asset along with technical information of the IT asset. VRM can be used to provide a central system of record for all IT assets in the organization.

– ***Prioritize and manage issues and stop chasing scan results***

An issue happens when vulnerability is detected on an asset. Issues are tracked through time as opposed to scan results snapshots. Issues track changes in the threat environment (e.g. an exploit is now in the wild or a server now also has customer data) or by business decisions (e.g. an exception is granted for a set of vulnerability fixes). Based on issues found, the security analyst assigns tickets and creates workflows to engage with IT operations as well as cross-functional stakeholders. As a result, dynamic decisions can be made with immediate response to change in asset criticality or vulnerability severity.

– ***Measure and report with dedicated dashboards for IT Security Analysts and CISO/Business Managers***

Measure the vulnerability-management program operational effectiveness using KPIs, trending, and filtering capabilities. The IT Security Analyst uses the Vulnerability Analytics dashboard for a consolidated view of prioritized alerts, vulnerabilities, issues, and assets. The CISO/IT Manager or Business Manager can use the Vulnerability Management dashboard for a consolidated view of KPIs across the IT organization.

– ***Use consolidated vulnerability analytics dashboard to manage vulnerabilities from multiple scanners***

Manage & prioritize vulnerabilities seamlessly across a variety of network vulnerability scanners such as Qualys, Rapid7, Nessus, McAfee and others. The vulnerability analytics engine correlates vulnerabilities reported across scanners and provides a single view for easy prioritization.