VULNERA

SOLUTION BRIEF

Vulnerability Scanning & Remediation Validation

Vulnerability identification, prioritization, and validation of remediation.

Defending corporate environments has become a complex and strategic undertaking for any security professional. With the introduction of cloud computing, infrastructure as code, and distributed workforces, organizations can no longer be clear what constitutes a “corporate boundary”. Defenders are faced with rethinking how to secure their network.

Chances are you have thousands of assets which are on and off the network at any point in time. Determining what is connected and which may introduce vulnerabilities into the network now requires a systemic and continuous approach. Organization must be able to identify real vulnerabilities, apply security measures to reduce risk, and to validate that remediation efforts have been successful.

Vulnerability Management Process

ASSESS | PRIORITIZE | RESOLVE | VALIDATE | REPORT

Solutions Overview

VULNERA provides a continuous analysis of computer systems, applications, and network infrastructures giving organizations the knowledge to identify and react to vulnerabilities in the environment. Assessment may include internal, external, and cloud systems to identify host and network-based security issues.

Continuous assessments combined with remediation validation also corroborates the effective removal of vulnerabilities once security controls have been applied. This helps organizations to better understand its assets, prioritize security risk, and reduce the likelihood of a breach.

Benefits

- Inventory accessible assets on the network (and their associated risks) to identify misconfigurations, unintended exposures, and fluctuations in the environment.
- Identify, classify, and address vulnerabilities across internal, external, and cloud systems to identify host and network-based security issues.
- Continuous data streams allow deployment of proactive security measures to remediate any known vulnerabilities.
- Re-testing verifies the application of patches and remediation efforts and documents mitigation actions.
- Satisfy compliance requirements that require organizations to have implemented technical and organizational security measures to protect data.

287

Average number of days to identify and contain a breach.

Source: Cost of a Data Breach Report 2021, IBM & Ponemon Institute

Solution Comparison

Perform non-stop security testing to identify exposed services, vulnerabilities, insecure configurations, and a number of other security weaknesses. Get unparalleled visibility into your constantly changing environment.

One-Time Assessment

7 - 14 Day Assessment

Satisfy an audit, third-party request, internal initiative, or other requirement to perform a security assessment.

- ✓ Asset Insights
- ✓ Audit-Ready Reporting
- ✓ Continuous Assessments
- ✓ VSCORE Prioritization
- ✓ Vulnerability Intelligence

Remediation Validation

60 - 90 Day Assessment

Perform an assessment and work through a remediation phase where vulnerabilities can be validated as resolved.

- ✓ Asset Insights
- ✓ Audit-Ready Reporting
- ✓ Continuous Assessments
- ✓ VSCORE Prioritization
- ✓ Vulnerability Intelligence
- ✓ Remediation Tracking
- ✓ Real-Time Dashboard

Continuous Assessments

24x7x365 Assessment

Continuously tackle vulnerability management with visibility into the assets, vulnerabilities, and remediation progress.

- ✓ Asset Insights
- ✓ Audit-Ready Reporting
- ✓ Continuous Assessments
- ✓ VSCORE Prioritization
- ✓ Vulnerability Intelligence
- ✓ Remediation Tracking
- ✓ Real-Time Dashboard
- ✓ Annual Penetration Test

Features

ASSET INSIGHTS

Gives full visibility into the devices, operating systems, ports, services, and applications that are connecting to your network and cloud environments.

AUDIT-READY REPORTING

Executive, technical, and differential reports support information security, compliance, and risk management programs.

CONTINUOUS ASSESSMENTS

Continuous analysis of computer systems, applications, and network infrastructures giving organizations the knowledge to identify and react to vulnerabilities in the environment.

VSCORE PRIORITIZATION

Visual tool automatically classifies and prioritizes threats found in the environment.

VULNERABILITY INTELLIGENCE

Real-time and historical performance metrics that provide context around threats that exist on the network.

REAL-TIME DASHBOARD

Graphical interface that visualizes the most current data of the organization's internal and external hosts, services, and vulnerabilities.

REMEDIATION TRACKING

Retesting of environment to validate the effective removal of vulnerabilities once security controls have been applied.

PENETRATION TESTING

A simulated cyber attack against the environment to identify, test, and highlight vulnerabilities within the environment.

About VULNERA

Security assessments should empower companies to achieve compliance while also improving the security of the organization. The industry is riddled with variances in quality, fragmented offerings, logistical constraints, and resource limitations. That's why VULNERA built a solution that helps organizations with the heavy-lifting so stakeholders can focus on what matters – remediating security issues.

+1 626.515.5523
www.vulnera.com | info@vulnera.com

VULNERA