VULNERA™

SOLUTION BRIEF

CONTINUOUS ASSESSMENTS

Ongoing assessment of target environments

Continuous Assessments

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.

Vulnerability assessments are used to identify risks and vulnerabilities in computer networks, systems, hardware, applications, and other parts of the IT ecosystem. They provide your security team and organizational management with the information they need to analyze and prioritize potential security risks for remediation.

Performed on an ongoing basis, vulnerability assessments are a critical component of an overall IT risk management program. They help protect systems and data from unauthorized access and data breaches.

Having a single, biannual, monthly, or even weekly vulnerability assessment on an environment is a thing of the past given ever-evolving cyber risks.

Security is an ongoing process, and so, only multiple and comprehensive tests on the network will tell you about its security posture. A constant flow of information is needed to adequately evaluate a network and to identify threats and vulnerabilities introduced by the constantly changing status of assets connecting to it.

Using automated, continuous scans will help in reducing security problems. They not only reveal the shortcomings of a security model, but also help in improving it.

- Regular assessments define the level of risk that exists on internal, external, and cloud networks
- It establishes a business-risk curve to optimize the organization's security investments
- An inventory of all devices and services connected to the network defines the organization's attack surface and identifies vulnerabilities related to these assets
- Proactively managing vulnerabilities will reduce or eliminate the potential for exploitation and save on the resources needed to respond to incidents after they have occurred

Solution 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. Helps organizations to better understand its assets, prioritize security risk, and reduce the likelihood of a breach. Annual pentesting (Continuous Assessments option only) ensures effectiveness of controls.

Audit-ready executive, technical, and differential reports support information security, compliance, and risk management programs.

VULNERA offers One-Time Assessments, Remediation Validation, and Continuous Assessments to meet the needs of our customers.

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 with

One-Time Assessment

7 - 14 Day Engagement

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 Engagement

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 Engagement

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

How It Works

Internal, external, and/or cloud vulnerability assessments are conducted on a continuous basis to identify host, network, and cloud-based security issues within the target environment.

Assess

A list of potential target assets as well as resources to be excluded from testing is compiled for the purpose of gathering information. A list of accessible assets (hosts, hostnames, IPs, ports, and services) is identified.

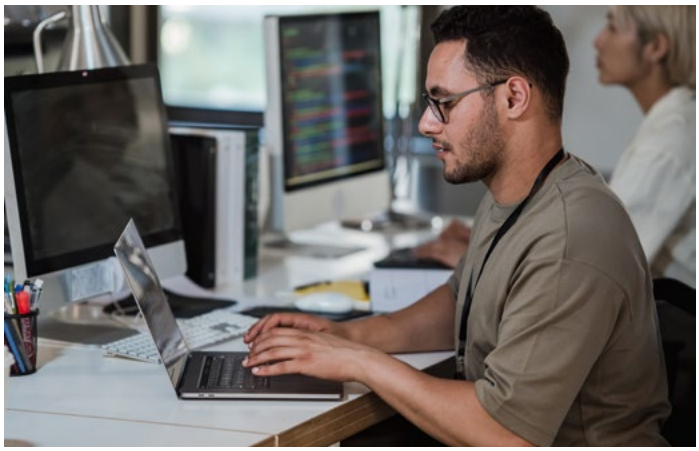
A deeper analysis of these live assets is then completed. Targeted scanning efforts using a suite of commercial, proprietary, and open source tools is used to identify host and network-based security issues present within the target environment. This phase includes matching previously identified services to known issues, as well as identifying insecure configurations. Tasks may include:

- Discovery of exploitable security issues within hosts and devices
- Identification of missing patches, recommended system upgrades and out-of-date software
- Ensure compliance with approved configuration standards
- Catalog known vulnerabilities associated with an open port or running service

Prioritize

Once vulnerabilities are identified, they are analyzed to determine the probability of a risk event occurring and the potential impact to the organization. Each vulnerability is assigned a VSCORE which incorporates a CVSS score and other traditional severity ratings combined with additional criteria, including:

- Active exploits available on the internet or in exploit packs
- Are remotely exploitable
- Often result in arbitrary code execution
- Being used in known exploit campaigns
- Has active advisories from vendors and regulating bodies



This allows teams to sort the risks by criticality – identifying those that need immediate attention from the security team. A remediation roadmap is generated for each site or entire environment.

Resolve

Once vulnerabilities have been classified and prioritized, they must be mitigated within the environment by your team. In many cases, this involves deploying a patch, upgrading, or reconfiguring a service.. Other fixes may include blocking or other administrative controls.

Validate

Just like the assessment phase, the remediation process is also continuous. To ensure security controls are effective in reducing the risk, monitoring must be in place. VULNERA continuously retests the environment is conducted and tracks new, open, and closed issues. A technical delta report is generated, highlighting resolved and persistent issues within the environment. Additionally, new vulnerabilities may be uncovered during follow-up security tests.

Reporting

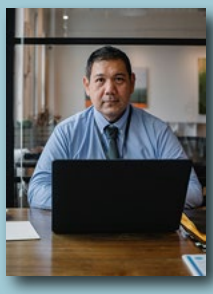
A detailed assessment report will summarize security issues, remediation strategies, and prioritized recommendations. The report includes an executive level summary which highlights key findings and an overall rating of the security posture. Technical findings are detailed with proof of concept and reproductions steps. Remediation recommendations provide immediate action items to improve the security posture of the application.

Real-time Analytics

No matter your role on the team, continuous assessments satisfy the needs of executives, technology and security teams, and operations and project management teams.

For IT & Security Teams

- Accelerates work and guides decisions based on contextualized prioritization of real-time threats
- Centralized data puts critical information at your fingertips
- Gain continuous insight into threats and remediate on an ongoing basis



For CISOs

- Real-time, end to end visibility into attack surface
- Speeds deployment of proactive security measures to remediate any known vulnerabilities
- Identify critical cyber threats including unpatched vulnerabilities

For Risk & Compliance Teams

- Enables frequent updates on the state of compliance with executives
- Centralized platform for security reporting and tracking
- Shifts focus from finger-pointing to collaboration in remediating vulnerabilities across the enterprise

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 has built vulnerability management solutions that help organizations with the heavy-lifting so stakeholders can focus on what matters – remediating security issues.

CONTACT

To learn more about how VULNERA's continuous assessments and other vulnerability management issues, please visit www.vulnera.com or call +1 626.515.5523 for a discussion with a vulnerability expert.

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

VULNERA™

SB1018 REV A 08/2022