Vulnerability Assessment

Don't Make It Easy

The more complicated your network is, the more vulnerabilities you have. Identifying these issues can be a daunting task for any IT department, especially when it comes to sorting through scan results to begin remediation.

With our Vulnerability Assessment, one of our cybersecurity experts will perform a comprehensive scan of your networks to determine internal and external vulnerabilities. We'll also provide expert review to help you identify which vulnerabilities are the most critical, which are easy to remediate, and whether or not any are false positives. After your engagement, you will have acccess to our Vulnerability Management platform to assist with remediation.

Our Approach

Depending on the complexity of your network and the level of testing you are looking for, we have three Vulnerability Assessment offerings to meet your needs. If you're looking for more manual testing of your networks, check out our Enhanced and Comprehensive Network Vulnerability Assessments or maybe even a Penetration Test.

New vulnerabilities are discovered regularly, so it's best practice to perform vulnerability scans at least once per month. With our Vulnerability Management software, you can perform unlimited vulnerability scans on your own, and then sort, search, and filter your results to prioritize vulnerabilities based on what's most important for your organization to address. Through our platform, you can assign vulnerabilities to your team and track remediation progress, then understand which have been fixed, which haven't, and why. It is also a great resource to show security progress and improvement over time.

Vulnerability Assessment Offerings:

Vulnerability Assessment (VA)
Includes a network scan of all devices with manual false-positive testing of a sample of the scanned results. We will outline all identified vulnerabilities and offer best practice recommendations to secure your organization's network.

Enhanced Vulnerability Assessment (EVA)
Involves advanced manual testing of external and internal networks as well as training on our Vulnerability Management platform for successive report delivery.

Comprehensive Network Vulnerability Assessment (CNVA)
Includes onsite testing to assess vulnerabilities within ALL aspects of your company. This can include organizational practices and procedures, employee policy awareness, wireless networks, physical security, and even data disposal practices.

Frequently Asked Questions

Does this replace the need for a penetration test?
No. Vulnerability scanning is not capable of identifying whether certain vulnerabilities are actually exploitable.

Is penetration testing included in this service?
No, it is not. We have separate services for Internal Penetration Testing and External Penetration Testing.

Is the scanner a hardware appliance?
No, the scanner is an agent-less software scanner.

Do you conduct authenticated or unauthenticated scans?
The scanner can perform either, so we give you the option along with our recommendation. We recommend that the first couple of scans are unauthenticated.

How does your scanner connect to my network?
The scanner must be installed on a workstation or in a virtual environment.

Will this hurt my network?
This is extremely unlikely as we do not attempt any denial of service attacks.

I already have a vulnerability scanner. Would your product integrate with mine?
If you have a Nessus, Nexpose, or Qualys scanner, we can integrate the results into our web application, which allows users to interact with the data to manage vulnerabilities and create reports.

If a vulnerability is marked as a false positive or acceptable, will it ever show up again in my scanning results?
No, the vulnerability will not show up again in your results.

Does your scanner detect rogue devices?
Yes, this is done using the network discovery tool.