N-Sentinel Vulnerability Assessment
Endpoint Vulnerability Identification and Insights for Utilities

A managed security service for utilities that provides on-demand or scheduled vulnerability assessments of networked IP devices, identifying vulnerabilities and issues in operating systems and applications.

WHY IS VULNERABILITY ASSESSMENT ESSENTIAL?

The migration towards distribution of intelligent endpoints across a utility’s coverage area and connectivity of those endpoints via communication networks has significantly increased the points at which hackers can gain access to the network. In addition, employees using PCs and mobile devices that access the utility’s network may inadvertently introduce vulnerabilities such as downloading infected files from a thumb drive or the Internet. Finally, with the ongoing software updates that are common to almost every type of endpoint from desktops to firewalls to smart switches and transformers, each update can carry along with it new vulnerabilities. Once inside the utility’s network, operations, data and assets are potentially at risk.

Perimeter security devices such as firewalls and anti-malware remain fundamental building blocks as part of a strong defense-in-depth cybersecurity strategy. However, vulnerability assessments of endpoints should be done frequently to keep up with the dynamics of these devices and their environment. In the past, biannual vulnerability scans may have been adequate for many utilities but this is no longer the case.

Some common sources of vulnerabilities are:

- New OS or application software update introduces a vulnerability
- Unauthorized devices attempting to access the network
- Malware or viruses resident on endpoints (may have been introduced via email, thumb drive, downloaded, vendor’s laptop, vendor updates, etc.)
- Usage of unsecured protocols (like FTP and Telnet)

To protect your utility from vulnerabilities you need to know which networked devices are vulnerable and in what way, as well as how to fix the problems. With on-demand vulnerability assessments you can quickly identify vulnerabilities and take action.

Common Malware Identified by N-Sentinel Vulnerability Assessment

- Software and OS Vulnerabilities
- Configuration Issues & Policy Violations
- Default Accounts
- Malware
- Information Leakage
- Rogue Devices
- Asset Identification
- …and much more
N-SENTINEL VULNERABILITY ASSESSMENT BENEFITS

- **On-demand vulnerability assessments**
  While many utilities utilize a third party service to administer vulnerability scans a few times a year, it means that the other days of the year the utility could be compromised and issues not detected until the next scan. Vulnerability assessment scans represent a single snapshot in time. N-Sentinel Vulnerability Assessment is a managed service that enables utilities to initiate a scan – anytime, reducing risk, saving time and money.

- **Actionable insights into vulnerabilities and prioritization**
  A long list of vulnerabilities isn't useful – you need to know which are more important than others to address immediately, which systems are affected, and what actions to take. N-Sentinel Vulnerability Assessment delivers both the insights and about the vulnerability and categorizes them so action can be taken to address the highest risk ones first. We also include guidance on how to address vulnerabilities – all included as part of the service.

- **Comprehensive reports**
  Available online from our secure customer portal, users can either view the report online or download it in PDF format. The N-Sentinel Vulnerability Assessment report contains a comprehensive list of all vulnerabilities found per scanned device, along with the vulnerability’s threat level, the description of the vulnerability, recommended mitigation / solutions and useful references. Using this thorough and comprehensive report, IT/OT staff can take much faster, proactive steps to prevent potential cybersecurity issues.
- **Flexibility to scan any subnet – no limitation**

The N-Sentinel Vulnerability Assessment subscription service gives customers the freedom to scan different networks within their organization without limitations to the number of connected devices that can be scanned. That’s flexibility and high value.

- **Access to cybersecurity experts**

N-Sentinel Vulnerability Assessment customers have access to our team of cybersecurity experts who can answer questions and provide additional guidance via email and phone. We are an extension of your IT team and bring the cybersecurity expertise.

- **Easy, fast deployment and hands-off management and maintenance**

N-Sentinel Vulnerability Assessment appliances are remotely managed by N-Dimension’s team of technical team and are easily installed to scan the network of your choice. We take care of any software updates needed so you don’t have to.

- **Correlate vulnerability assessment finding with N-Sentinel Monitoring alerts**

Customers who have both N-Dimension’s N-Sentinel Vulnerability Assessment and N-Sentinel Monitoring services have the additional benefit of being able to correlate discovered vulnerability CVE’s with the intrusion Alert ID (as available) helping quickly identify if there has been an attempt to breach the utility using a specific vulnerability.

- **Flash alerts**

Flash Alerts are sent to all N-Sentinel customers periodically to inform them about cyber threats that have been reported both within and outside of the utility community and which they may encounter. Oftentimes word spreads about a threat but is scant about the details, its severity, and preventative measures utilities can take – we include all of this information with actionable steps such that customers can take proactive preventative action today. All of these, plus links to additional insights about the threat, is provided in a simple to understand email which is also available on the customer portal.
N-SENTINEL VULNERABILITY ASSESSMENT – HOW IT WORKS

The N-Sentinel Vulnerability Assessment appliance is easy to install and setup on the network to be scanned; it usually takes about 15 minutes. Once installed, customers can login to the N-Sentinel customer portal to configure to run on a daily schedule or on-demand. During this configuration setup, customers can select to exclude scanning of specific hosts. When scanning is set to run on a daily basis, the N-Sentinel appliance will run the scan at the same time each day that a customer selects. With daily vulnerability scans, IT staff can address and mitigate issues on a regular basis, thereby reducing potential risk faster.

N-SENTINEL VULNERABILITY ASSESSMENT CUSTOMER TESTIMONIAL

“It’s a huge benefit for us to be able to run a vulnerability assessment frequently. I now feel more confident in our ability to quickly identify endpoint vulnerabilities and shut them down before they become a serious issue.”

Karen St. Clair
IT Manager
Columbia Power and Water Systems

Contact us to find out what cyber threats are on your network putting your utility at risk. Don’t wait until after your system has been compromised.

E: sales@n-dimension.com
P: +1.866.837.8884

www.N-Dimension.com