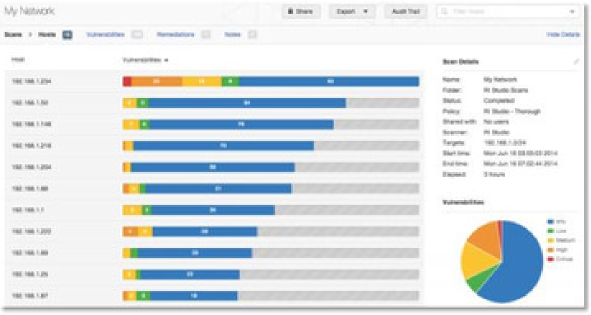
VULNERABILITY ASSESSMENTS | POWERED BY NESSUS™

DataComm

DataComm's Vulnerability Assessments powered by Nessus provides an expanded footprint to cover a wider set of testing criteria, reporting capabilities and customizable for your technology environment.

Vulnerability assessments help you reduce your organization's attack surface and ensure compliance in physical, virtual and cloud environments. Features include high-speed asset discovery, configuration auditing, target profiling, malware detection, sensitive data discovery, and more. This supports more t echnologies than competitive solutions, scanning operating systems, network devices, hypervisors, databases, web servers, and critical infrastructure for vulnerabilities, threats, and compliance violations.



Name: My Network
Folder: PI Studio Scans
Status: Completed
Policy: PI Studio - Thorough
Shared with: No users
Scanner: PI Studio
Targets: 192.168.1.0/24
Start time: [illegible]
End time: [illegible]
Elapsed: 3 hours

REPORTING AND MONITORING

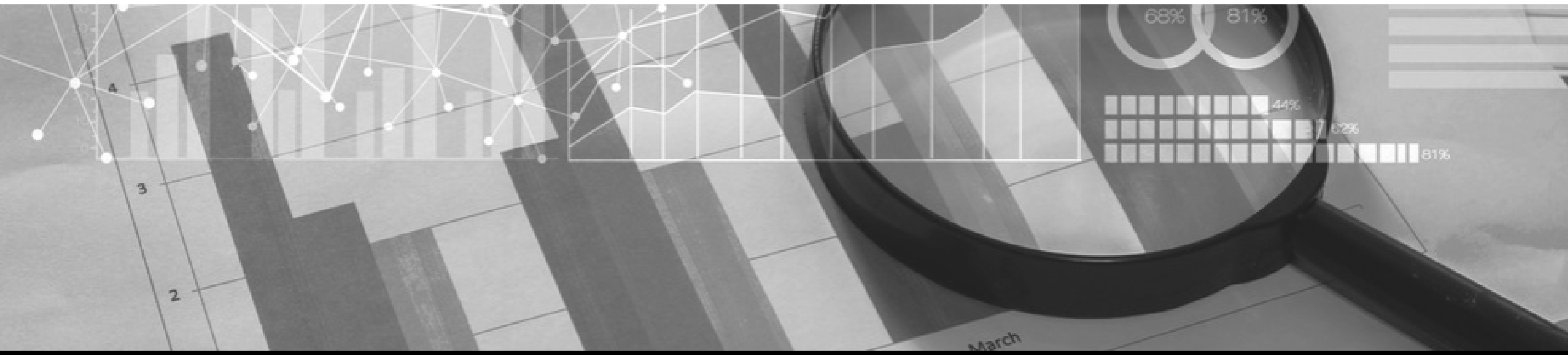
- Flexible reporting: Customize reports to sort by vulnerability or host, create an executive summary, or compare scan results to highlight changes
- Native (XML), PDF (requires Java be installed on Nessus server), HTML and CSV formats
- Targeted email notifications of scan results, remediationrecommendations and scan configuration improvements

COMPLETE VULNERABILITY COVERGARE

- Virtualization & cloud
- Malware & bot-nets
- Configuration auditing
- Web applications

SERVICE BENEFITS

- ✓ Reduce the attack surface: Prevents attacks by identifying vulnerabilities that need to be addressed
- ✓ Comprehensive: Meets the widest range of compliance and regulatory standards
- ✓ Low total cost of ownership (TCO): Complete vulnerability scanning solution for one low cost
- ✓ Constantly updated: New content continually being added by the Tenable research team
- ✓ Easily accessible: Anywhere, anytime access from an Internet browser
- ✓ Highly-accurate scanning with low false positives
- ✓ Comprehensive scanning capabilities and features
- ✓ Scalable to hundreds-of thousands of systems
- ✓ Easy deployment and maintenance
- ✓ Low cost to administer and operate



VULNERABILITY ASSESSMENTS | POWERED BY NESSUS™

DataComm

SCANNING CAPABILITIES

- Discovery: Accurate, high-speed asset discovery
- Scanning: Vulnerability scanning (including IPv4/IPv6/hybrid networks)
- Un-credentialed vulnerability discovery
- Credentialed scanning for system hardening & missing patches

COVERAGE: BROAD ASSET COVERAGE AND PROFILING

- Network devices: firewalls/routers/switches (Juniper, Check Point, Cisco, Palo Alto Networks), printers, storage
- Offline configuration auditing of network devices
- Virtualization: VMware ESX, ESXi, vSphere, Center, Microsoft, Hyper-V, Citrix Xen Server Operating systems: Windows, OS X, Linux, Solaris, FreeBSD, Cisco iOS, IBM iSeries
- Databases: Oracle, SQL Server, MySQL, DB2, Informix/DRDA, PostgreSQL, MongoDB
- Web applications: Web servers, web services, OWASP vulnerabilities
- Cloud: Scans the configuration of cloud applications like Salesforce and instances like AWS
- Compliance: Helps meet government, regulatory and corporate requirements
- Helps meet several PCI DSS requirements through configuration auditing, web application scanning Threats: Botnet/malicious, process/anti-virus auditing
- Detect viruses, malware, backdoors, hosts communicating with botnet-infected systems, known/unknown processes, web services linking to malicious content
- Compliance auditing: FFIEC, FISMA, CyberScope, GLBA, HIPAA/ HITECH, NERC, PCI, SCAP, SOX
- Configuration auditing: CERT, CIS, COBIT/ITIL, DISA STIGs, FDCC, ISO, NIST, NSA
- Control Systems Auditing: SCADA systems, embedded devices and ICS applications
- Sensitive Content Auditing: PII (e.g. credit card numbers, SSNs)

DEPLOYMENT AND MANAGEMENT

- Flexible deployment: software, hardware, virtual appliance deployed on premises or in a service provider's cloud.
- Scan options: Supports both non-credentialed, remote scans and credentialed, local scans for deeper, granular analysis of assets that are online as well as offline or remote.
- Configuration/policies: Out-of-the-box policies and configuration templates.
- Risk scores: Vulnerability ranking based on CVSS, five severity levels (critical, high, medium, low, info), customizable severity levels for recasting of risk.
- Prioritization: Correlation with exploit frameworks (Metasploit, Core Impact, Canvas, and ExploitHub) and filtering by exploitability and severity.
- Extensible: RESTful API support for integrating Nessus into your existing vulnerability management workflow.