VULNERA™

RESOURCE GUIDE

VULNERABILITY MANAGEMENT

Getting Started with Vulnerability Management

Among the responsibilities of CISOs and security teams is responsibly ensuring that technology risks are managed appropriately. These risks can be identified and remediated by detecting vulnerabilties, assessing their potential impact, and deploying corrective measures to eliminate – or at least reduce – the risk.

> *Vulnerability Management is the continuous process of identifying, classifying, prioritizing, remediating, and mitigating software vulnerabilities.*

According to the U.S. National Vulnerability Database, thousands of new vulnerabilities are discovered each year. To have an effective vulnerability management program, a process and technologies must be designed to detect, assess, and mitigate these vulnerabilities.

This resource guide was developed to help locate resources to help you gain a working knowledge of the vulnerability management process as well as identify best practices for incorporating them into your own program.

Cybersecurity and Infrastructure Security Agency (CISA)

- Vulnerability Management
- Cyber Essentials Starter Kit
- Cyber Resilience Review (CRR)
- Related Resources

Federal Financial Institutions Examination Council (FFIEC)

- Information Security Booklet

Gartner (requires subscription)

- Vulnerability Assessment Technology and Vulnerability Management Practices
- Protect Your Business Assets with a Roadmap for Maturing Information Security Program

Health Insurance Portability and Accountability Act (HIPAA)

- Guidance on Risk Analysis
- Cyber Security Guidance Material

International Organization for Standardization (ISO)

- ISO/IEC TR 20004:2015 Information technology -- Security techniques -- Refining software vulnerability analysis under ISO/IEC 15408 and ISO/IEC 18045 (fee)

National Institute of Standards and Technology (NIST)

- National Vulnerability Database
- NCP Repository
- 800-53 Controls (NIST Risk Management Framework – RMF)
- SCAP Validated Tools
- NIST Cybersecurity Framework (CSF)
- NISTIR 7946 CVSS Implementation Guidance
- SP 800-40 v.4.0 Creating a Patch and Vulnerability Management Program
- Technical Guide to Information Security Testing and Assessment

- Prioritizing Cybersecurity Risk for Enterprise Risk Management

The Office of the National Coordinator for Health Information Technology (ONC)

- Health IT Privacy and Security Resources for Providers

Payment Card Industry (PCI) Security Standards Council

- Navigating PCI DSS – Understanding the Intent of the Requirements v.2.0 See sections 5 and 6, Maintain a Vulnerability Management Program
- Software Security Framework At-a-Glance
- Transitioning from PA-DSS to the PCI Software Security Framework
- PCI Quick Reference Guide

Ponemon Institute

- Costs and Consequences of Gaps in Vulnerability Response

SANS

SANS Vulnerability Management Maturity Model

Additional Resources

- National Cyber Awareness System
- Common Vulnerability Scoring System (CVSS)
- Common Vulnerabilities and Exposures (CVE)

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.

Our Solutions include:
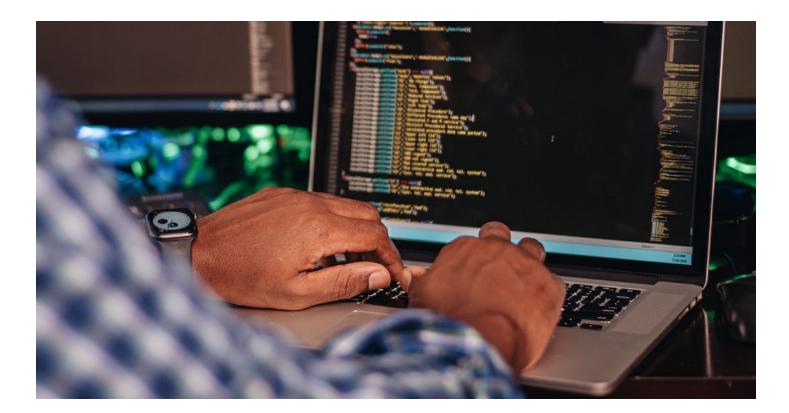
One-Time Assessments
7-14 Day Engagement
Used to satisfy an audit, third-party request, internal initiative,
or other requirement to perform a security audit.

Remediation Validation
60-90 Day Engagement
Conduct an assessment and work through remediation
so you can validate vulnerabilities are resolved.

Continuous Assessment
24x7x365 Engagement
Continuously tackle vulnerability management with visibility
into assets, vulnerabilities, and remediation progress.

VULNERA™

www.vulnera.com | **+1 626.515.5523**