OPTIV | tenable

Partner Service Brief | Optiv and Tenable

How to Build A Successful Vulnerability Management (VM) Program

Executing a vulnerability management program requires input spanning all facets of your business. A lack of processes, procedures and technical expertise can lead to a growing number of vulnerabilities and increase the likelihood of a breach.

Overcoming the hurdle of remediating vulnerabilities can be a massive lift. Together, Optiv and Tenable can alleviate the challenge by applying an adversarial perspective and a methodical approach to identifying, prioritizing, verifying and remediating vulnerabilities within your unique environment.

Focus vulnerability management efforts to close your cyber exposure gap

IDENTIFICATION
Vulnerability Management programs must continually evolve along with the technology an organization uses. The vulnerability management platform must be able to identify security issues in every type of asset the organization may leverage, whether it's on-prem servers, workstations, cloud, or containers.
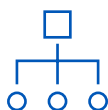
PRIORITIZATION
The number of known vulnerabilities will always increase and the longer they go unaddressed, the larger the number of issues to manage will grow. Effective prioritization needs to go beyond simple criticality scoring and incorporate multiple factors to enable organizations to respond to the right vulnerability at the right time.

REMEDIATION
Vulnerability Management solutions need to be able to engage with IT workflows that govern the actions required to ultimately remediate a discovered vulnerability. The more integration capabilities the VM platform has, the more opportunities there will be for an efficient way to engage with IT.

UNDERSTAND THE KEY CHALLENGES IN A VULNERABILITY MANAGEMENT PROGRAM

- Vulnerability Management Programs depend on
  - rapid identification
  - prioritization
  - remediation of vulnerabilities to be successful

- If one of these falls short, the entire program will degrade

- Insufficient vulnerability identification means missed vulnerabilities or false positives that can clog your process and waste resources.

- Without accurately and quickly prioritizing vulnerabilities, the system can become overwhelmed and not address the vulnerabilities that pose the biggest threat to your organization.

- The ultimate goal of vulnerability management is to address the vulnerability, and in order to do that, the VM solution needs to integrate with the organizations change management platforms successfully.

OPTIV

Leverage Optiv and Tenable

Optiv's holistic Security Services are delivered by a team of experts to solve your toughest cybersecurity challenges and minimize security weaknesses. We have partnered with Tenable to equip clients with a complete vulnerability management program to identify vulnerabilities, classify risk and prioritize remediation within your unique environment.
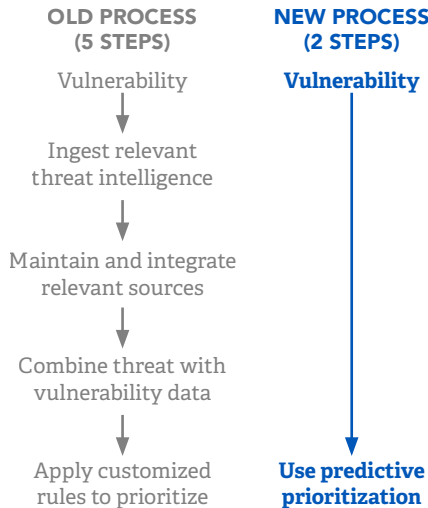
ASSESSMENT COVERAGE

Tenable's suite of vulnerability management products provide a single integrated platform for finding vulnerabilities across a vast attack surface, including IoT, cloud and containers.
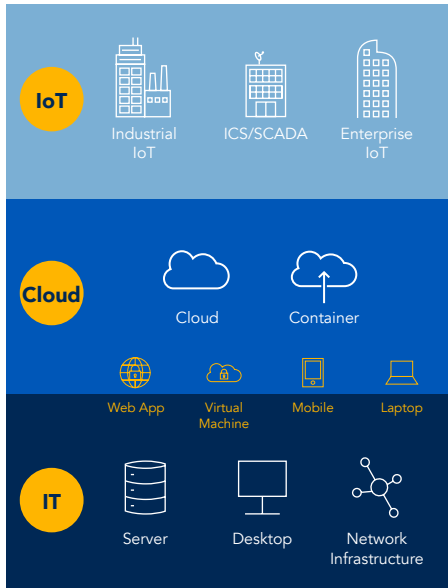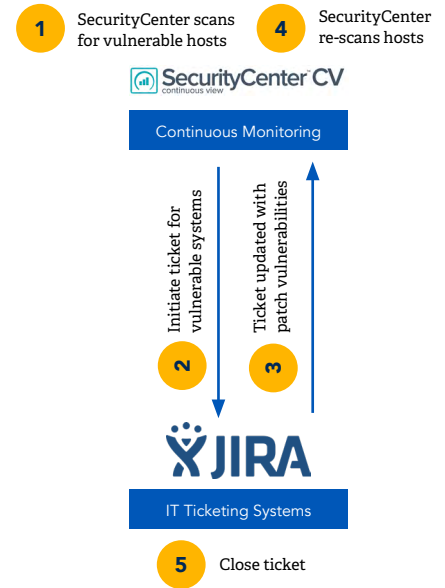
PRIORITIZATION

Tenable's predictive prioritization enables an organization to act on what matters the most, and have confidence in focusing efforts in the right direction via the Vulnerability Priority Rating.

REMEDIATION

Tenable can integrate direction with ticketing systems like ServiceNow and JIRA, and not only direct issues through those platforms, but react to workflow actions and deploy rescans to verify that the issue has been fully addressed.

IoT
- Industrial IoT
- ICS/SCADA
- Enterprise IoT

Cloud
- Cloud
- Container
- Web App
- Virtual Machine
- Mobile
- Laptop

IT
- Server
- Desktop
- Network Infrastructure

Drive Operations Efficiency with an Automated Approach

OLD PROCESS (5 STEPS)

Vulnerability
↓
Ingest relevant threat intelligence
↓
Maintain and integrate relevant sources
↓
Combine threat with vulnerability data
↓
Apply customized rules to prioritize

NEW PROCESS (2 STEPS)

Vulnerability
↓
Use predictive prioritization

1. SecurityCenter scans for vulnerable hosts
4. SecurityCenter re-scans hosts

SecurityCenter CV continuous view

Continuous Monitoring

2. Initiate ticket for vulnerable systems
3. Ticket updated with patch vulnerabilities

JIRA

IT Ticketing Systems

5. Close ticket

Secure your security.™

Optiv is a security solutions integrator – a "one-stop" trusted partner with a singular focus on cybersecurity. Our end-to-end cybersecurity capabilities span risk management and transformation, cyber digital transformation, threat management, security operations, identity and data management, and integration and innovation, helping organizations realize stronger, simpler and more costefficient cybersecurity programs that support business requirements and outcomes. At Optiv, we are modernizing cybersecurity to enable clients to innovate their consumption models, integrate infrastructure and technology to maximize value, achieve measurable outcomes, and realize complete solutions and business alignment. For more information about Optiv, please visit us at www.optiv.com.

OPTIV