Vulnerability Management Detection & Response (VMDR)

Prateek Bhajanka
VP, Product Management | VMDR
Qualys, Inc.
“A **Vulnerability** is only as bad as the **Threat exploiting it** and the **Impact** on the organization”
Challenges with Vulnerability Management

Overwhelming number of vulnerabilities
No Vulnerability to Patch correlation
CVSS and CVE being too skewed
Vulnerability Assessment as a feature
Penetration testing being used Interchangeably with VM
No Single platform
2.1. CVSS Measures Severity, not Risk

The CVSS Specification Document has been updated to emphasize and clarify the fact that CVSS is designed to measure the severity of a vulnerability and should not be used alone to assess risk.

Concerns have been raised that the CVSS Base Score is being used in situations where a comprehensive assessment of risk is more appropriate. The CVSS v3.1 Specification Document now clearly states that the CVSS Base Score represents only the intrinsic characteristics of a vulnerability which are constant over time and across user environments. The CVSS Base Score should be supplemented with a contextual analysis of the environment, and with attributes that may change over time by leveraging CVSS Temporal and Environmental Metrics. More appropriately, a comprehensive risk assessment system should be employed that considers more factors than simply the CVSS Base Score. Such systems typically also consider factors outside the scope of CVSS such as exposure and threat.
Vulnerability Management Lifecycle

- **Asset Inventory**: Do you know what all your assets are and where they are?
- **Patch Management**: How can you deploy patches to close high-impact vulnerabilities?
- **Vulnerability Management**: Do you know the type and amount of open vulnerabilities?
- **Threat Risk and Prioritization**: Can you prioritize remediation based on threat intelligence?
People
Process
Tools

Discover & Scale
Report & Research
Prioritize Threats
Remediate Patch
WannaCry Timeline and Remediation

- **MS17-010 Patch Release**
- **Authenticated Scan / Agent Detection**
- **Remediation from VM/Patch processes**
- **EternalBlue Exploit**
- **New Remote Detection**
- **Flat Remediation**
- **“Emergency” Patching**

THOUSANDS

Introducing Qualys.

VMDR

Vulnerability Management, Detection and Response

One solution to Discover, Assess, Prioritize and Patch critical vulnerabilities
Asset Discovery
Detect known and unknown assets
Workflow to add an unmanaged asset as a managed asset

Asset Inventory
Hardware, operating system, and application inventory for all assets

Asset Normalization and Categorization
Normalize Inventory data by common attributes
Categorize by vendor, version, type
Vulnerability Management
Detect vulnerabilities by QID
CVE-to-QID mapping
CVSSv2 and CVSSv3 base scores

Security Configuration Assessment
CIS Benchmarks
Security-related misconfigurations
Prioritization
- Using real-time threat context
- Real-world exploits
- Proof of Concepts
- Exploit categorization
- Exploit severity

Machine Learning

Contextual Awareness
Remediation

Automatically correlate vulnerabilities to patches
End-to-end User Interface workflows
Fit-for-purpose visualizations and recommendations
Orchestration for remediation
Prioritization Engine – Machine Learning

Python and Tensor Flow
Dataset of 120,000+ Vulnerabilities
  132 Vulnerability Features
Live Exploits / POCs
Historical Threat Patterns
Historical Vulnerable Software/Vendor
Dark Web and Social Media References
Qualys Security Researchers
Learns New Patterns and Intelligence Daily
“The more time you spend on activities with low impact, the less time you have for higher impact activities”
Contextual Awareness

Your Network is Unique to You

External Facing Assets
Network Reachability / Cloud Security Groups
Zero-Trust Networking / BeyondCorp
Business / Customer Applications
Data Sensitivity and Data Access Governance
Asset System Configuration
Security Control Validation
VMDR comes with much more

- Unlimited Cloud Agents
- Unlimited Container Sensors
- Unlimited Passive Sensors
- Certificate Inventory
- Cloud Inventory
- Container Inventory
- Mobile Device Inventory
- Asset Categorization
- Asset Normalization
- Configuration Assessment
- CIS Benchmarks
- Continuous Monitoring
- Patch Detection and CVE Correlation

Available February 2020
Industry terms or Acronyms

RBVM - Risk based approach to VM
TCVM - Threat Centric Vulnerability Prioritization or Management
VPT - Vulnerability Prioritization Technologies
TVM - Threat and Vulnerability Management
Security Posture
ASM - Attack Surface Management
Penetration Testing
Thank You

Prateek Bhajanka
pbhajanka@qualys.com