QUALYS SECURITY CONFERENCE 2020

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

CVSS Confession

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?

Vulnerability Management

Do you know the type and amount of open vulnerabilities?

Patch Management

How can you deploy patches to close high-impact vulnerabilities?

Threat Risk and Prioritization

Can you prioritize remediation based on threat intelligence?

Qualys.

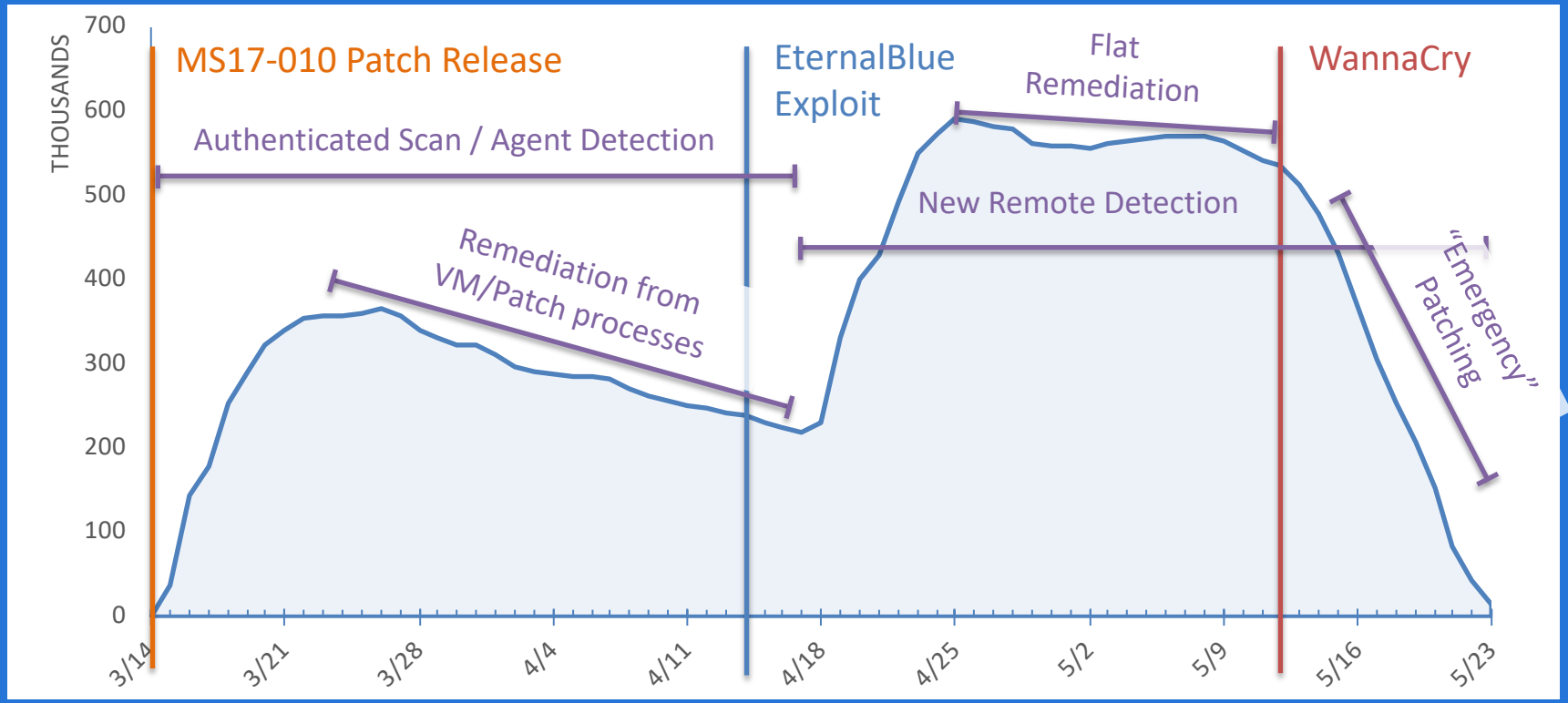
People

Process

Tools

Qualys.

WannaCry Timeline and Remediation



Qualys.

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

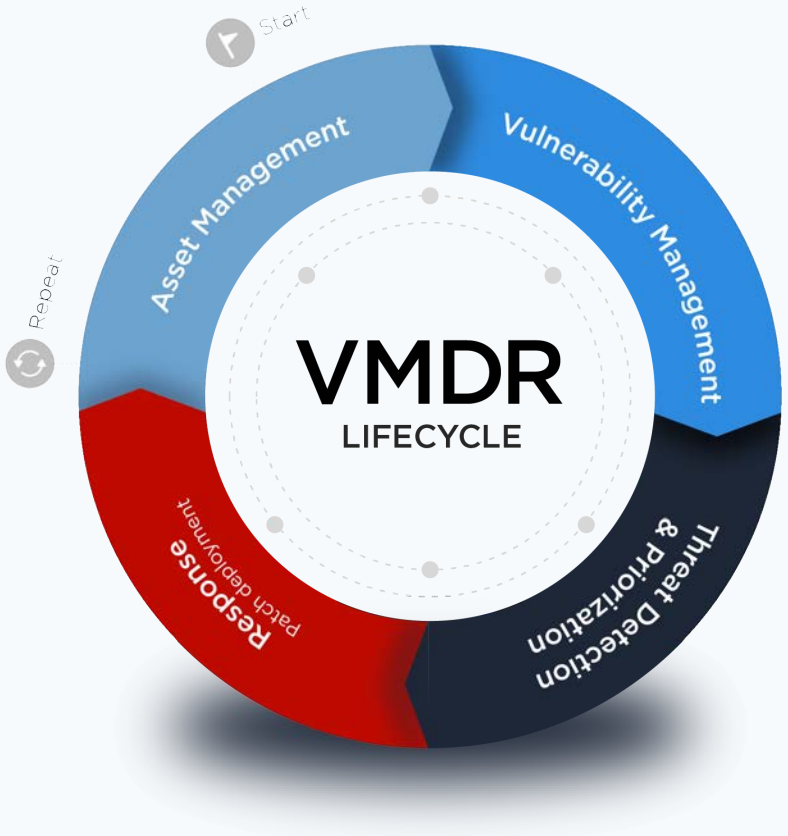
Asset Inventory

Hardware, operating system, and application inventory for all assets

Asset Normalization and Categorization

Normalize Inventory data by common attributes

Categorize by vendor, version, type



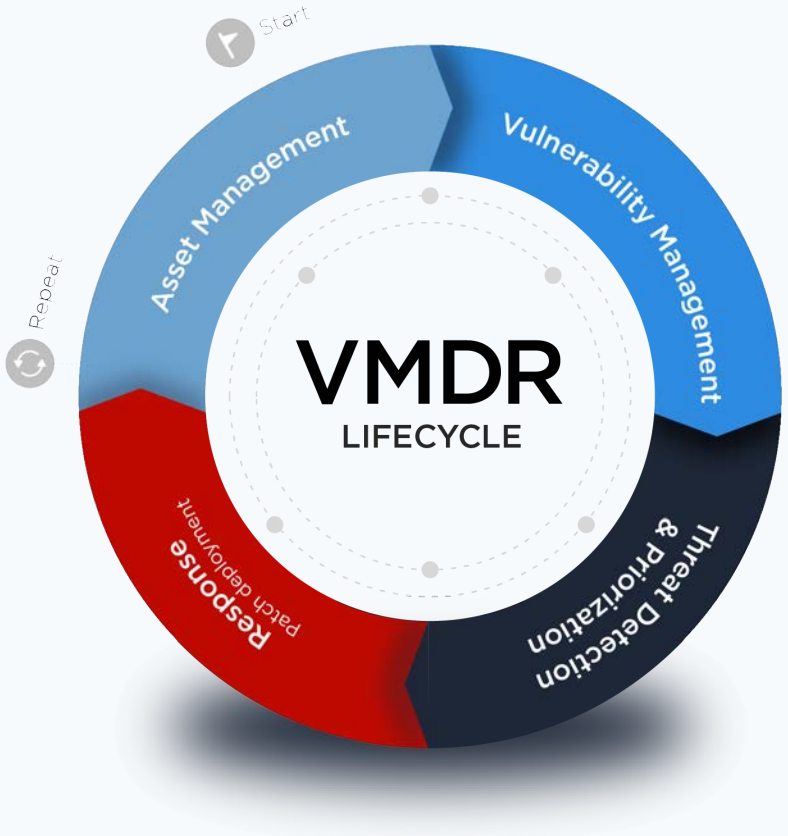
Qualys.

Vulnerability Management

- Detect vulnerabilities by QID
- CVE-to-QID mapping
- CVSSv2 and CVSSv3 base scores

Security Configuration Assessment

- CIS Benchmarks
- Security-related misconfigurations



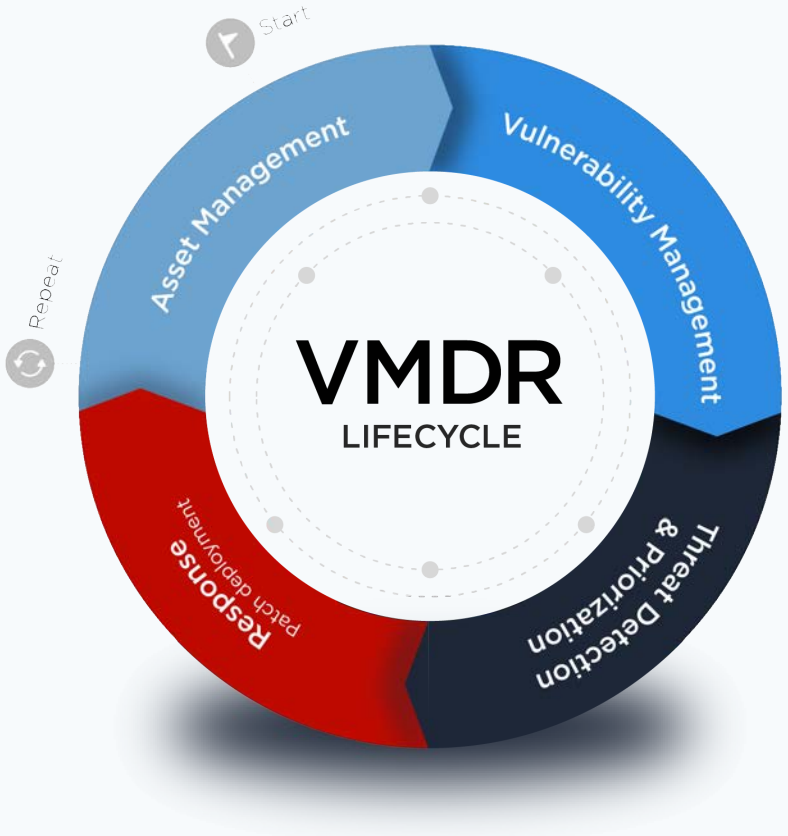
Qualys.

Prioritization

- Using real-time threat context
- Real-world exploits
- Proof of Concepts
- Exploit categorization
- Exploit severity

Machine Learning

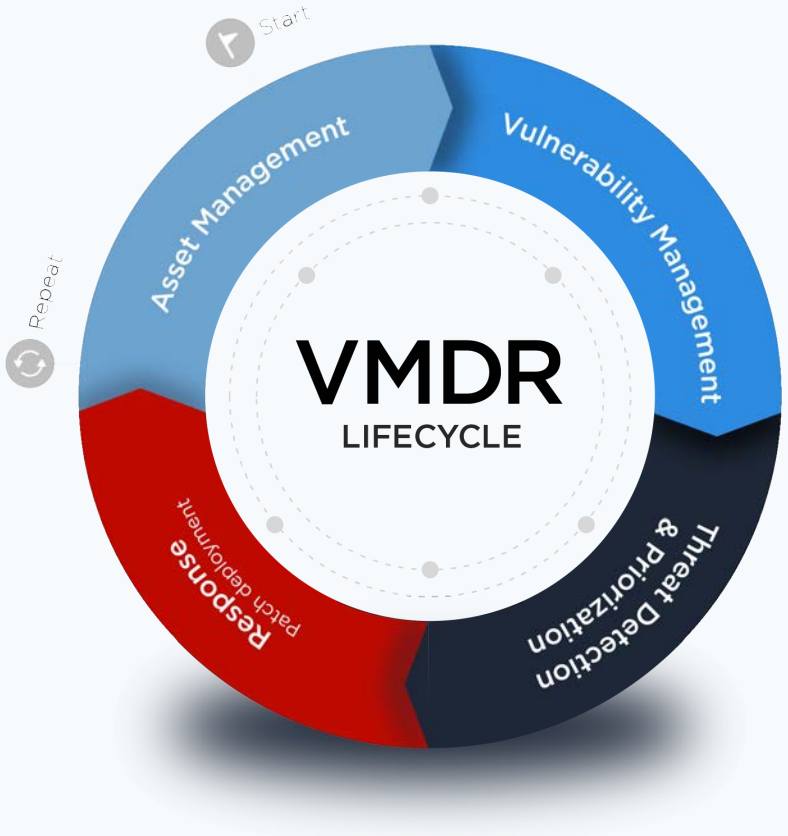
Contextual Awareness



Qualys.

Remediation

- Automatically correlate vulnerabilities to patches
- End-to-end User Interface workflows
- Fit-for-purpose visualizations and recommendations
- Orchestration for remediation



Qualys. Enterprise

← Threat Prioritization Report

Export to Dashboard | Save Report

Asset Tags (5)

Finance ✕ | Operations ✕ | Engineering ✕ | HR-HQ ✕ | HR-France ✕

Vulnerability Age

RTIs (9)

- ✓ Zero Day (10)
- ✓ High Lateral Movement (32)
- ✓ Active Attacks (12)
- ✓ Wormable (13)
- ✓ Machine Learning Probability (32)
- DOS External (25)
- ✓ High Data Loss (17)
- Vulnerable to DOS (28)
- ✓ Easily Exploitable (50)
- ✓ Exploit Kit Available (34)
- ✓ Unpatchable (23)
- ✓ Public Exploit (13)

Prioritized Assets 38
Total 379
10% of Total

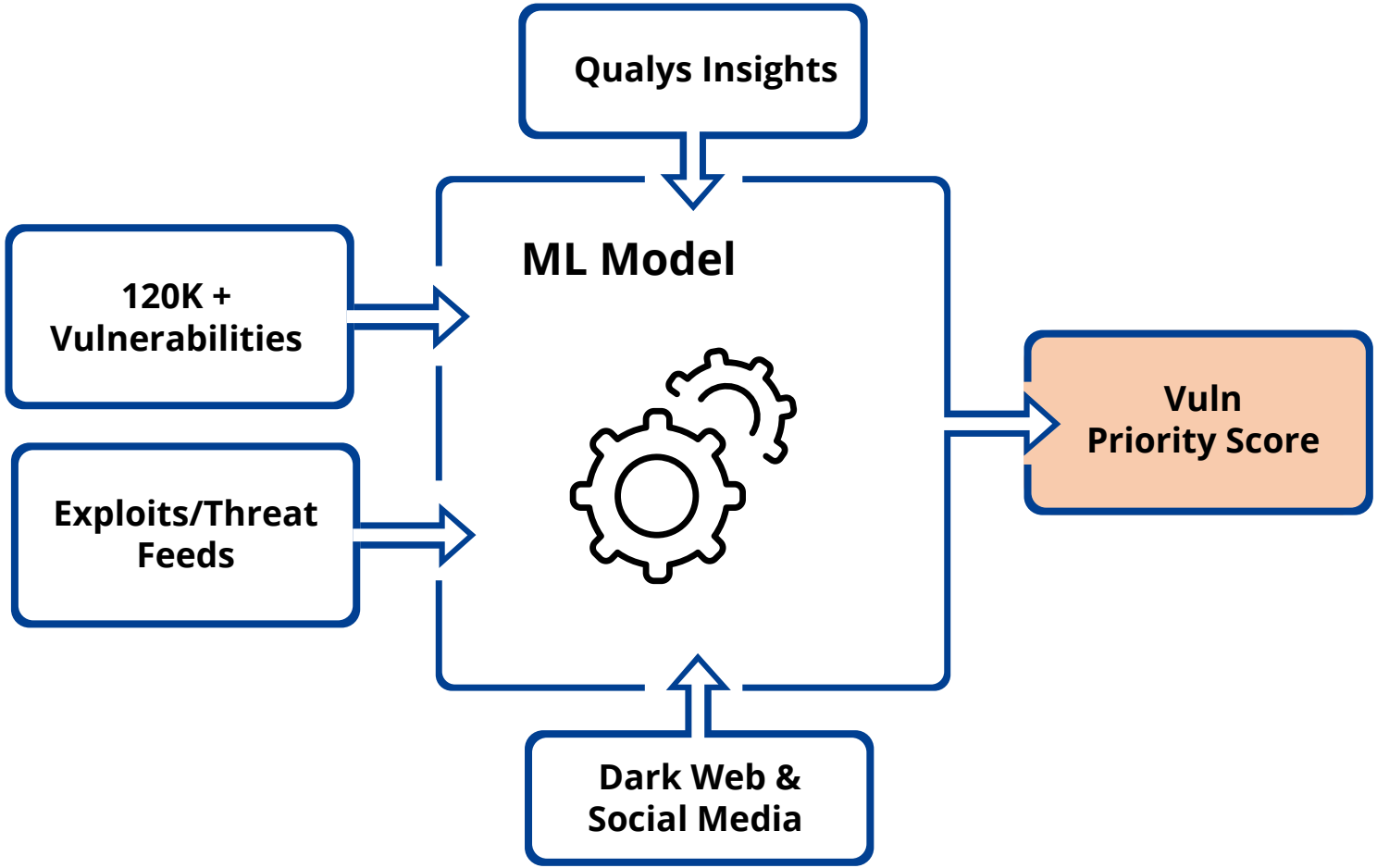
Prioritized Vulnerabilities 37
Total 1.34K
2.75% of Total

Available Patches 05
Patch Now

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

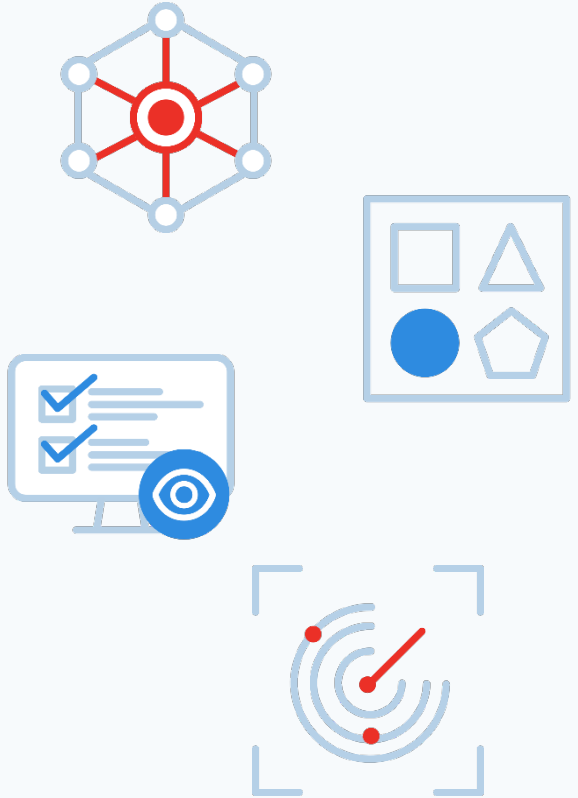
“The more time you spend on activities with low impact, the less time you have for higher impact activities”

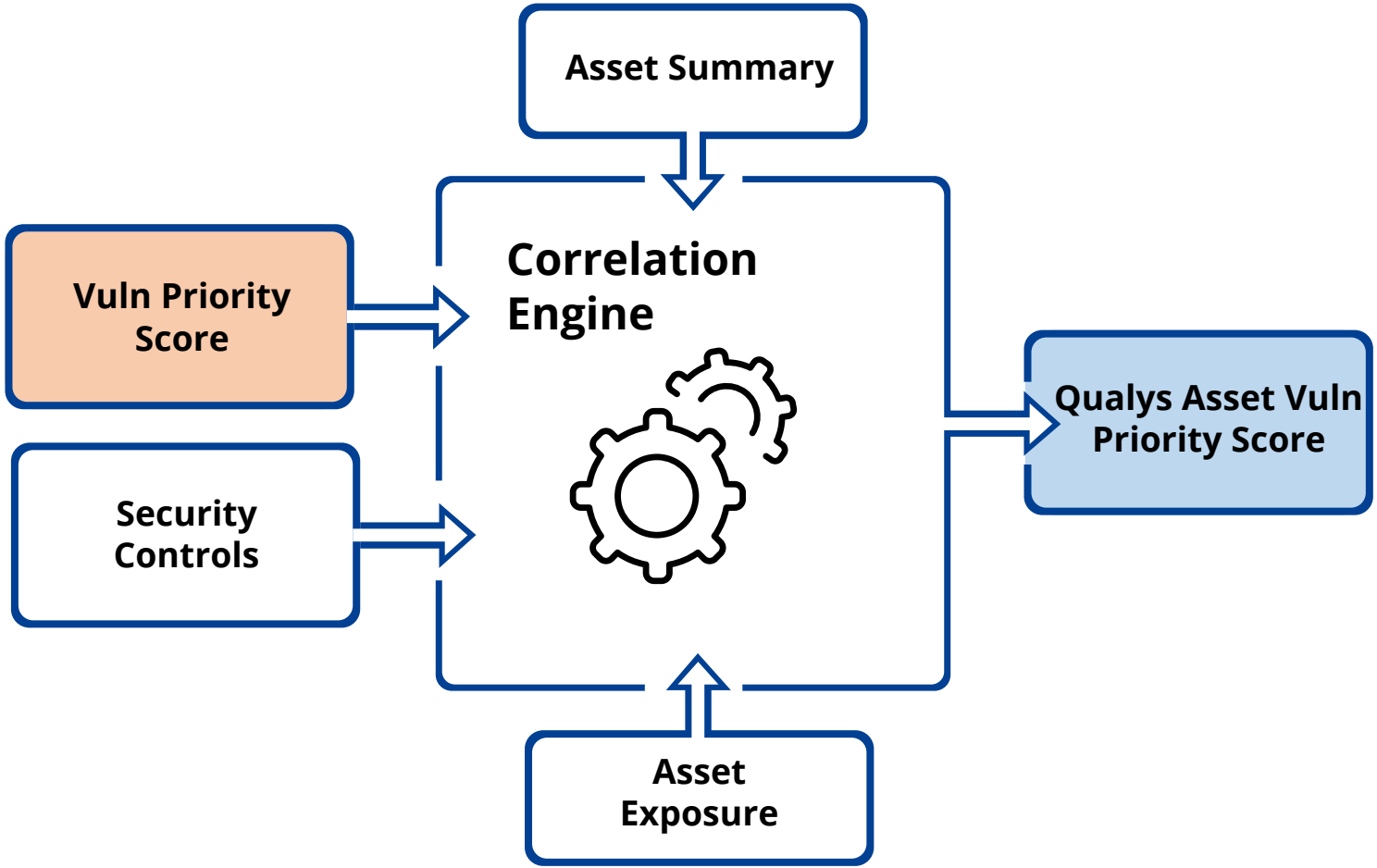

Qualys Insights
ML Model
120K +
Vulnerabilities
Exploits/Threat
Feeds
Vuln
Priority Score
Dark Web &
Social Media

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




Asset Summary
Vuln Priority Score
Correlation Engine
Security Controls
Qualys Asset Vuln Priority Score
Asset Exposure

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

VMDR
Concept Demo

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