QUALYS SECURITY CONFERENCE 2019

Vulnerability Management Detection & Response (VMDR)

Chris Carlson
VP Strategy, Qualys, Inc.

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.

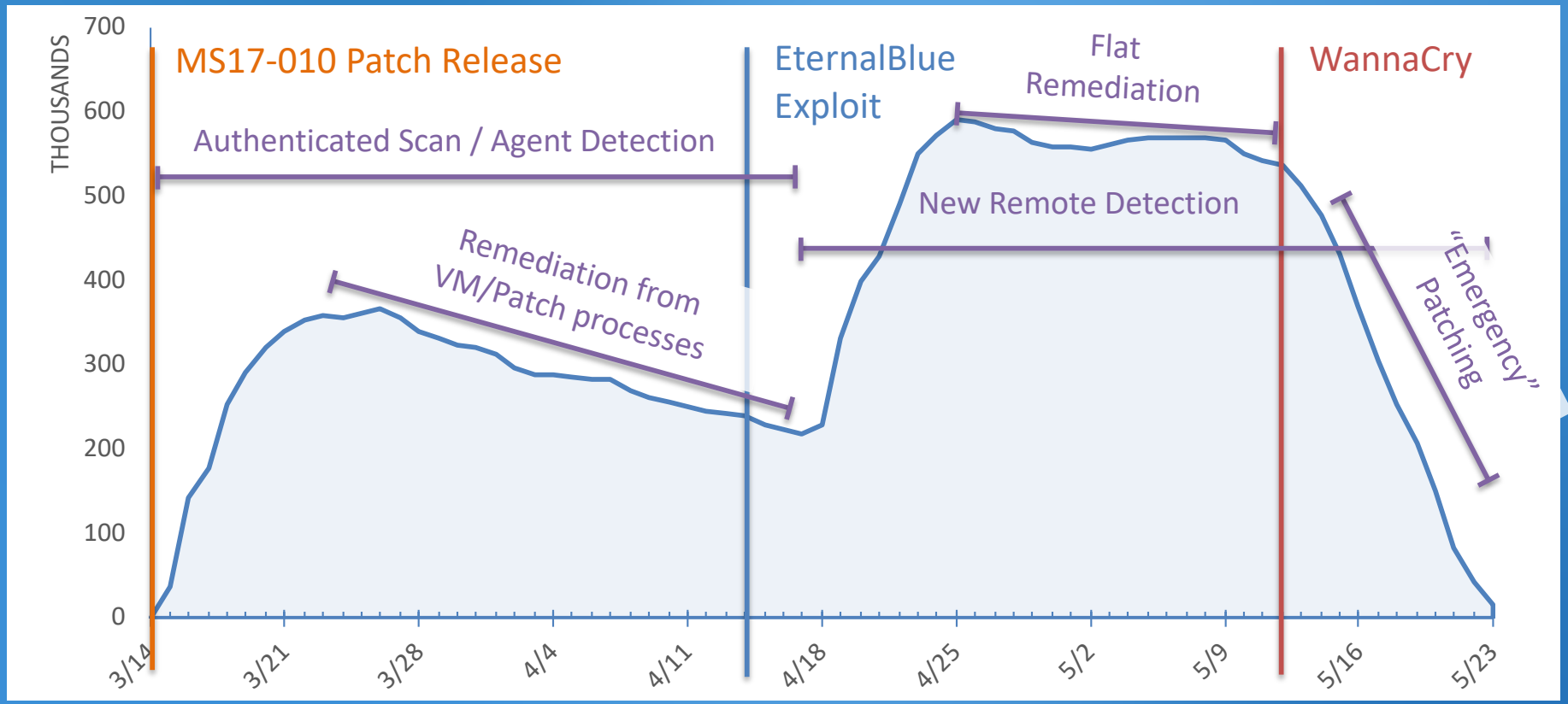
People

Process

Tools

Qualys.

WannaCry Timeline and Remediation



One solution to Discover, Assess, Prioritize and Patch critical vulnerabilities

Qualys.

Asset Discovery

Detect known and unknown assets

Workflow to add an unmanaged asset as a managed asset

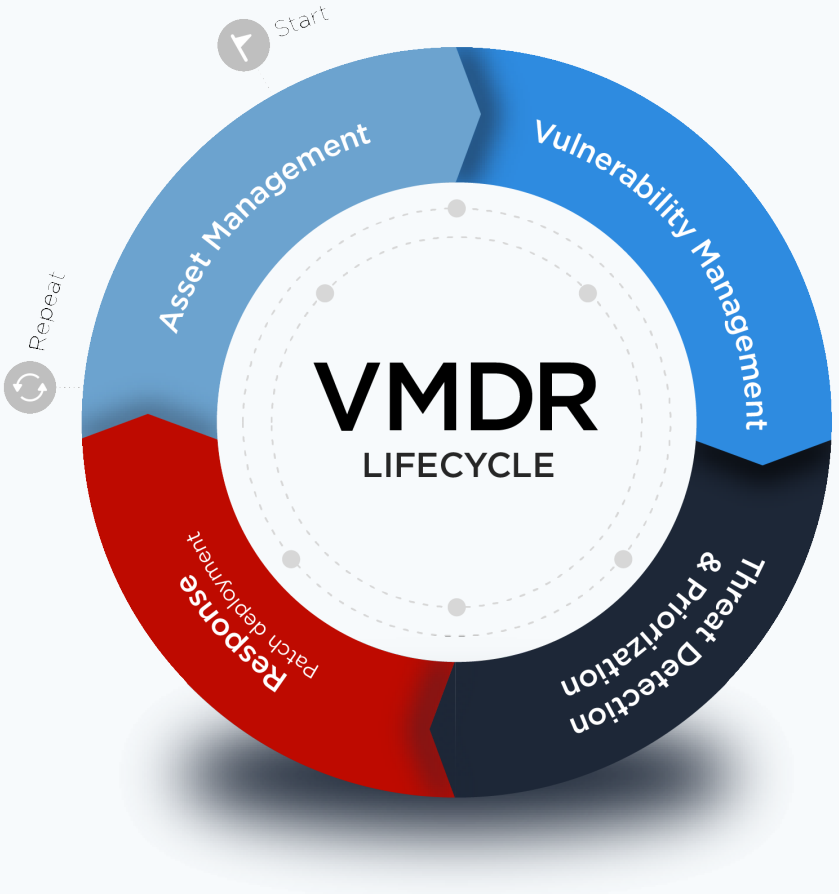
Asset Inventory

Hardware, operating system, and application inventory for all assets

Asset Normalization and Categorization

Normalize Inventory data by common attributes

Categorize by vendor, version, type



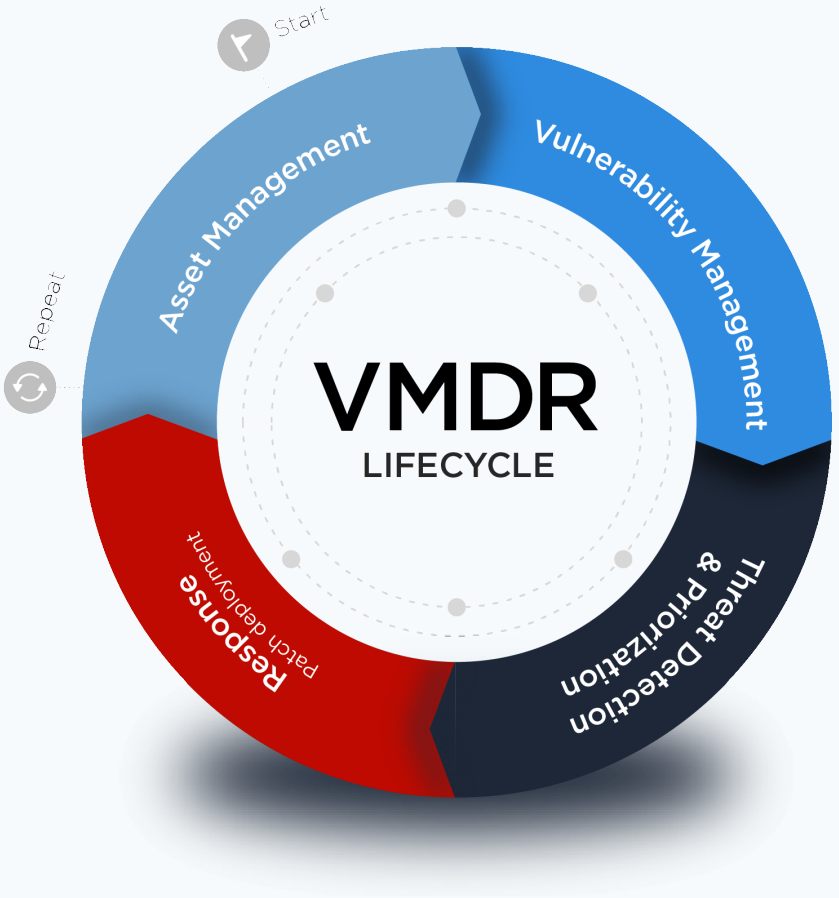
Qualys.

Vulnerability Management

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

Security Configuration Assessment

- CIS Benchmarks
- Security-related misconfigurations



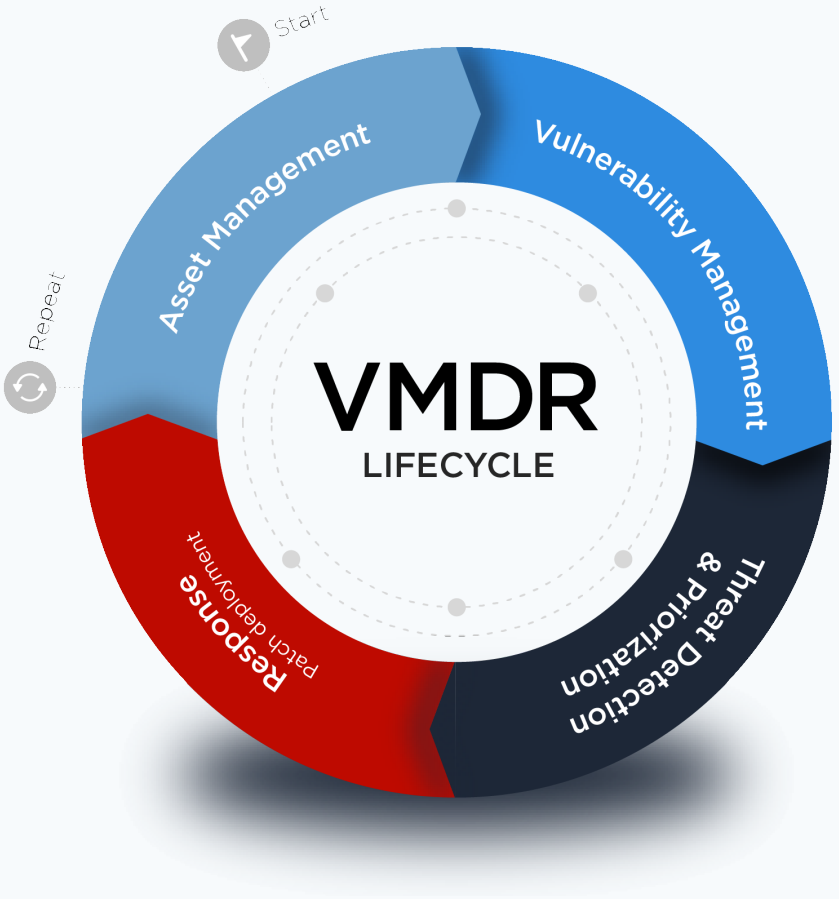
Qualys.

Prioritization

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

Machine Learning

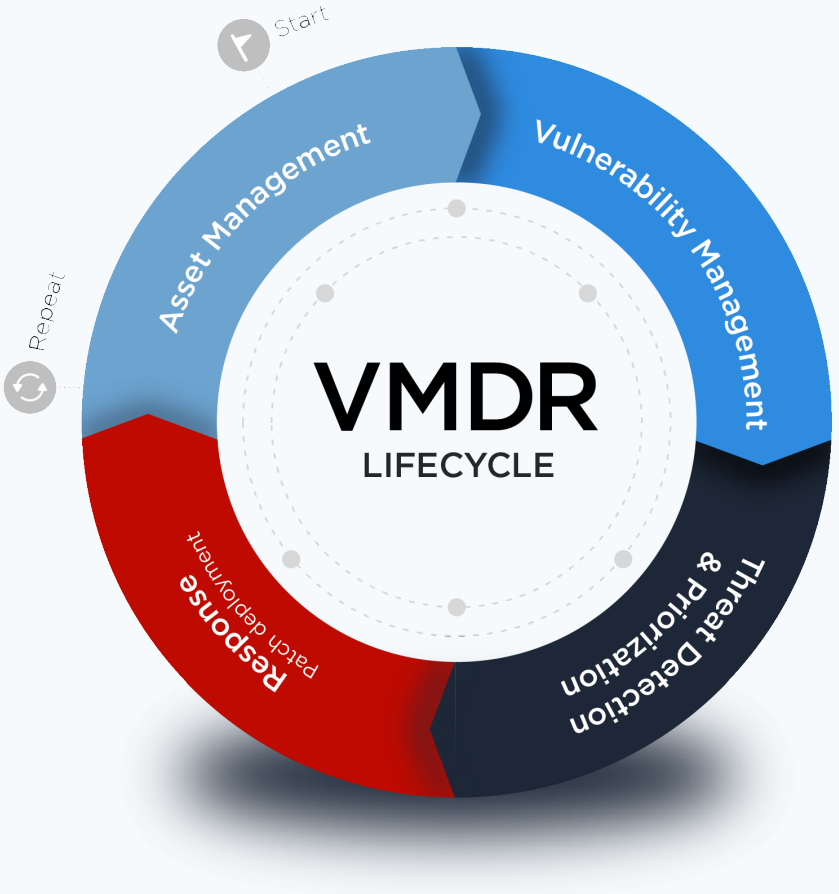
Contextual Awareness



Qualys.

Remediation

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



Qualys.

Qualys.

VMDR

ASSETS

Tags

Finance | Marketing | Human Resources | Engineering | Operations

Hosts
379

VULNERABILITIES

1343
Total Vulnerabilities

CVSS Score

High (310) | Med (320) | Low (713)

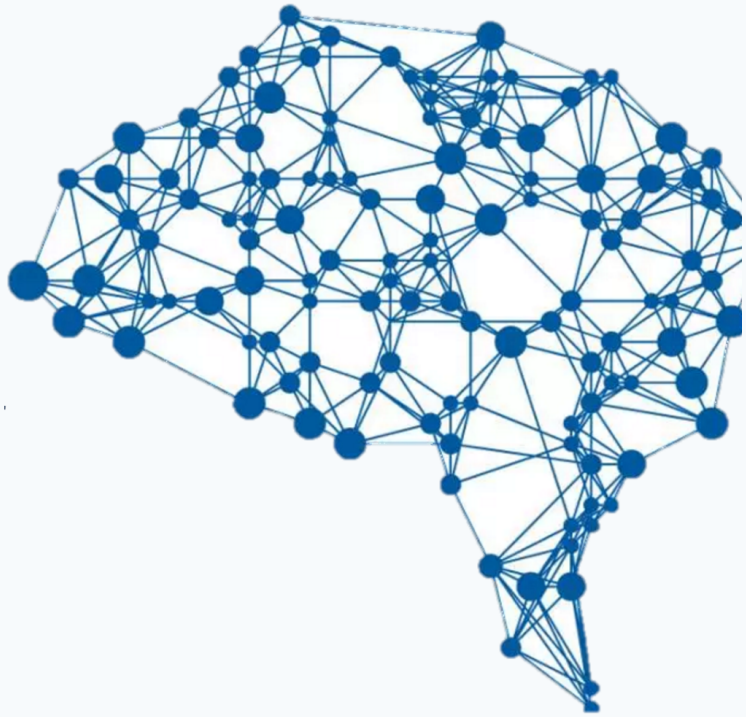
Service Level Agreement

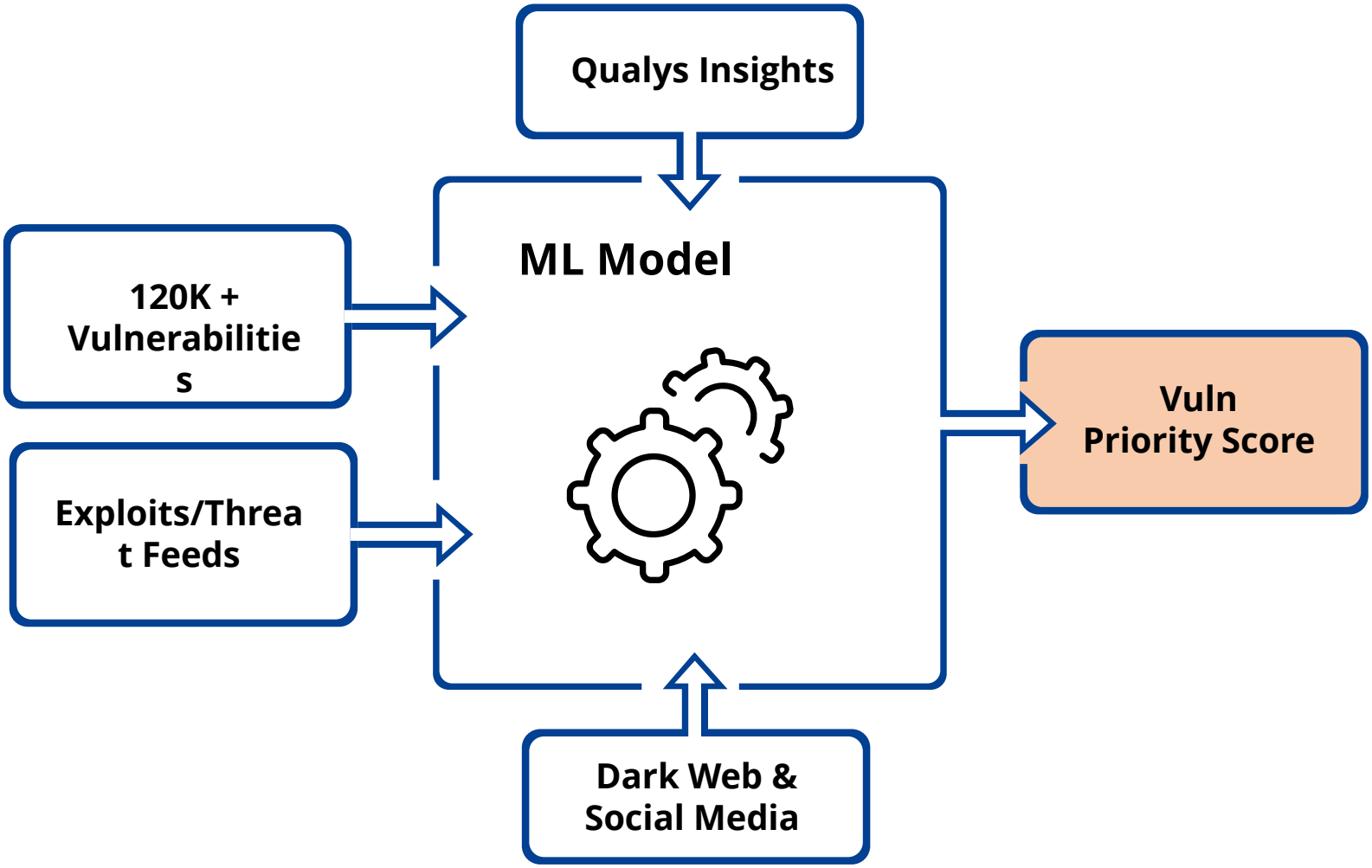
Pre-SLA (260) | 0-15+ Days (122) | 16-30 Days (108) | 31-60 Days (412) | 61-90 Days (211) | 90+ Days (230)

Qualys Threat Prioritization

Prioritization Engine – Machine Learning

Multi-Layer neural network
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

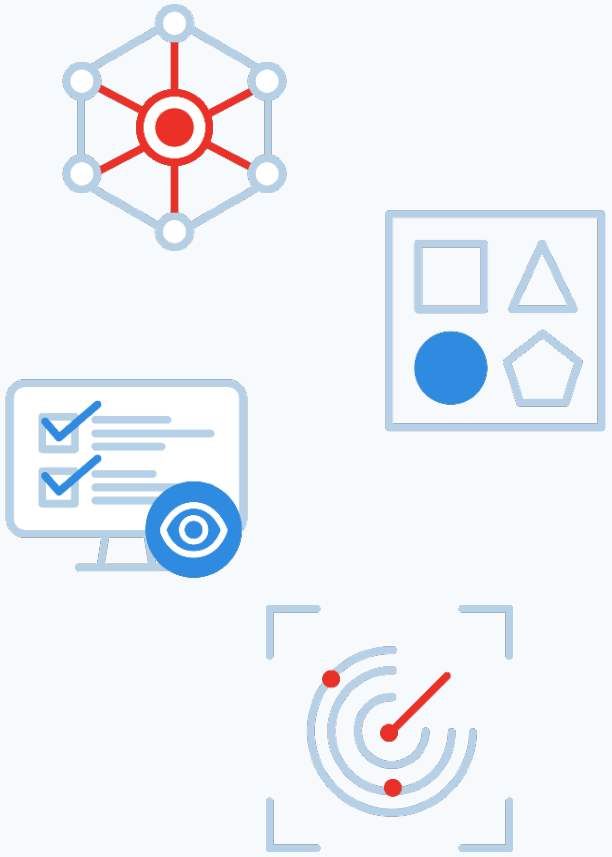


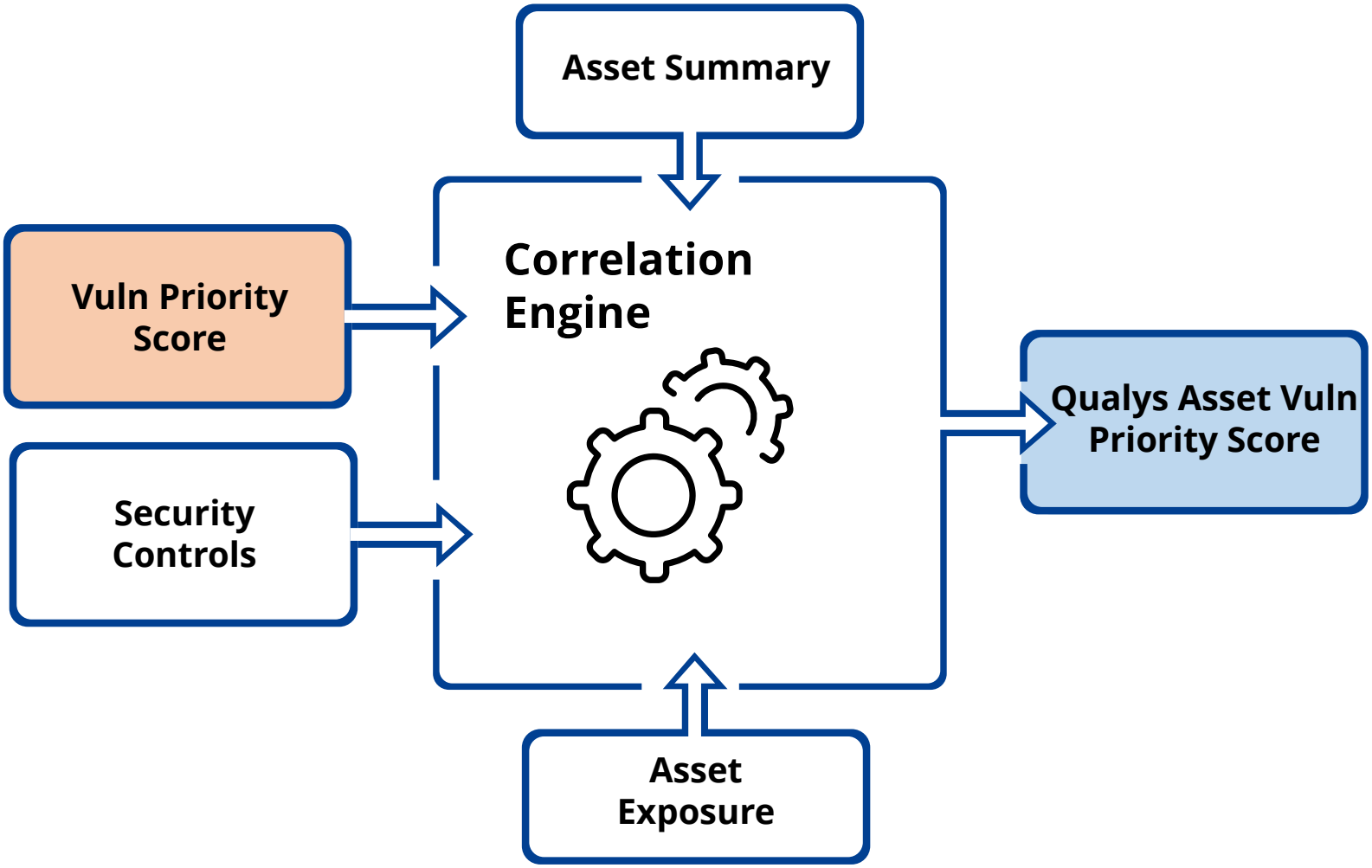

Qualys Insights
ML Model
120K + Vulnerabilities
Exploits/Threat Feeds
Vuln Priority Score
Dark Web & Social Media

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
Qualys Asset Vuln Priority Score
Security Controls
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 January 2020

Qualys.

VMDR
Concept Demo

Thank You

Chris Carlson
ccarlson@qualys.com