Reputation, Regulation and Risk: Navigating the Cybersecurity Tides

Murali Ayyappan

Principal – New Business, Qualys

The R-Rated Realities of Cyber (SEA Edition)

THE RAGING THREAT LANDSCAPE: *GLOBAL STORMS & LOCAL CURRENTS IN SEA*

REPUTATION: HARD TO EARN, EASY TO LOSE

REGULATION: NAVIGATING ASEAN'S EVOLVING COMPLIANCE MAP

RISK: FROM SILOED STRUGGLES TO UNIFIED REGIONAL STRENGTH

The Only Constant is... More Threats

31%

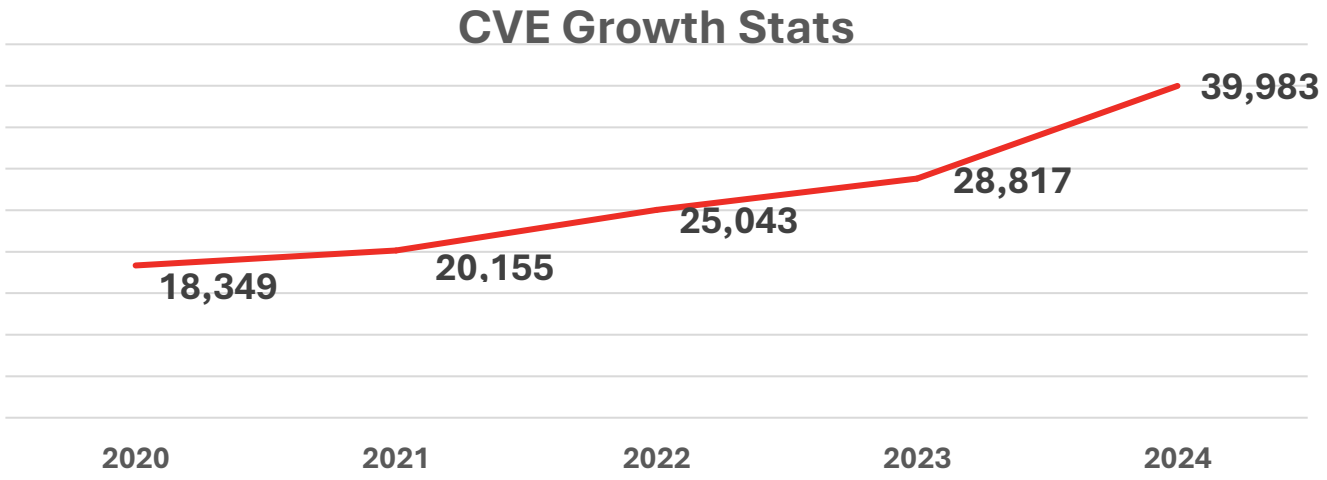
YOY Rate of CVE Growth

6.89

Average CVSS Score

133

Average CVEs per day



Average adversary breakout: **48 minutes**

Fastest: **51 SECONDS**

79% of detections are MALWARE-FREE.

Asia-based cybercrime syndicates expanding worldwide from SEA.

Attack Vectors: They're Getting Creative (and AI-Powered!)

Vishing attacks up 442%
Use of deepfakes surged 1500%.

Help desk social engineering rising.

GenAI is a "force multiplier" for adversaries – better social engineering, faster development.

SEA Context: Ransomware, RATs, infostealers still huge in SEA, often via email. QR code scams emerging.

TOP INITIAL ACCESS steps : Credential Abuse & Vuln Exploitation

Intrusion as a Service

52%

Vulns related to Initial Access

50%

Ads from Access Brokers up YOY

Current State of Vulnerability Management

NCSC Guidelines

5 Days	14 Days
External	Internal

57.7% Remediated Vulnerabilities

30.6 Days
Mean Time to Remediate

19.5 Days	11.1 Days
Time to Weaponize	Exploitation Opportunity

Attackers have an 11-day advantage

48K
Patches from Microsoft, 10K from third parties

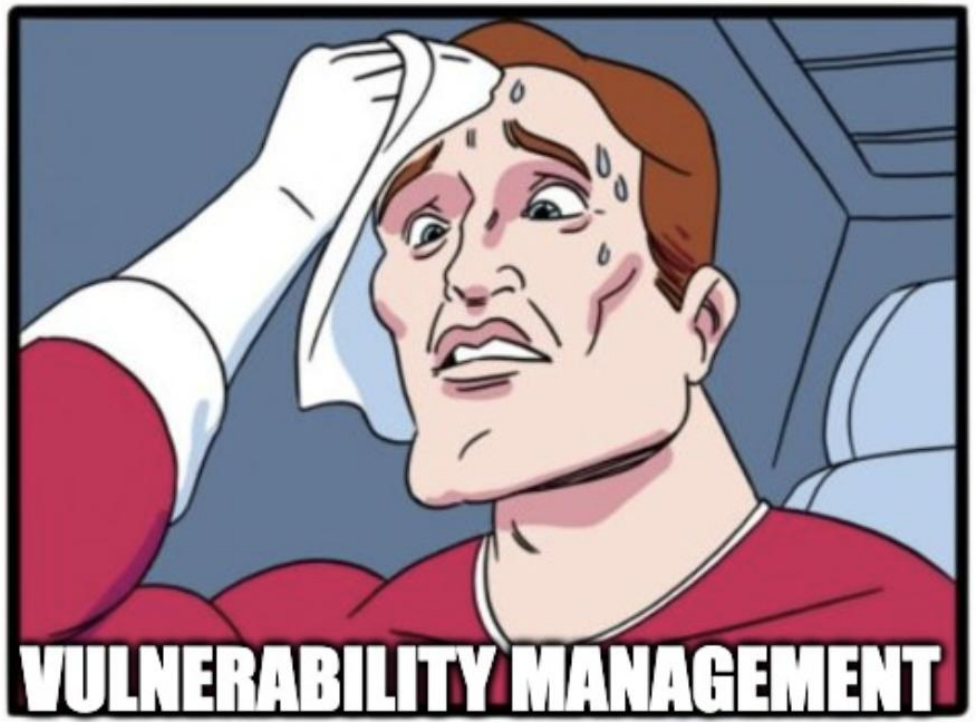
Internet-Facing Assets

33%
Risky vuln patches not prioritized for Patch Tuesday

40%
Vulns due to 3rd party software not patched

Qualys.

Current state of Vulnerability Management



The High Cost of a Tarnished Reputation

The scale of SEA-based cybercrime syndicates (fraud, trafficking) creates significant regional reputational risk.

Darknet markets facilitate this

DBIR: Third-party breaches (doubled to 30%) amplify this.

Regulation: The Ever-Expanding Maze

Expect more focus on supply chain security.

Risk of being cut off from international systems if anti-cybercrime measures are deemed insufficient.

The Numerous Sources of Cyber Risk

...and New Stakeholders to Communicate With

Risk Sources

- Data Center
- Installed Software
- AI
- Cloud Resources
- IT Assets
- Workloads
- IoT
- Identities
- SaaS Apps
- Modules & Packages

Risk Factors

- Vulnerabilities
- Unauthorized software
- Infra/DB Misconfigurations
- Open-source vulnerabilities
- Access risks
- Missing required software
- Unauthorized File Changes
- Cloud Misconfigurations
- Sensitive data leakage risks
- Endpoint Malicious activities
- Technology debt risks
- Web application risks

Apps & Environments

Cloud Misconfiguration Fixes

Application, Open-source vulnerabilities

Dev Teams

SOC, Pen-test team

CISO

Risk Stakeholders

- CIO
- CEO
- IT/Ops Teams
- DevOps Teams
- Vulnerability Management
- Audit / GRC

APPLICATIONS

OPERATING SYSTEMS

CLOUD / CONTAINERS / VMs

IT / WORKSTATIONS / SERVERS

IOT

EXTERNAL DEVICES

Challenge of Risk Prioritization

Managing Attack Surface for Business

Knowing Assets

- Hybrid Environment, Dynamic assets
- Lacks context from Business

Lack of Business context and Noise

resulting in More work post VM, Risk assessment & Remediation

Unable to view unified ‘Toxic Insights’ from siloed findings

31%

Assets **unknown but** known your attackers!, from where the attacks start

45%

Of critical assets are missing business criticality, context

78%

Vulns High/Critical by CVSS **Only 18% with evidence of attacks**

50%

Vuln Risk due to Tech Debt of EOL/EOS Software

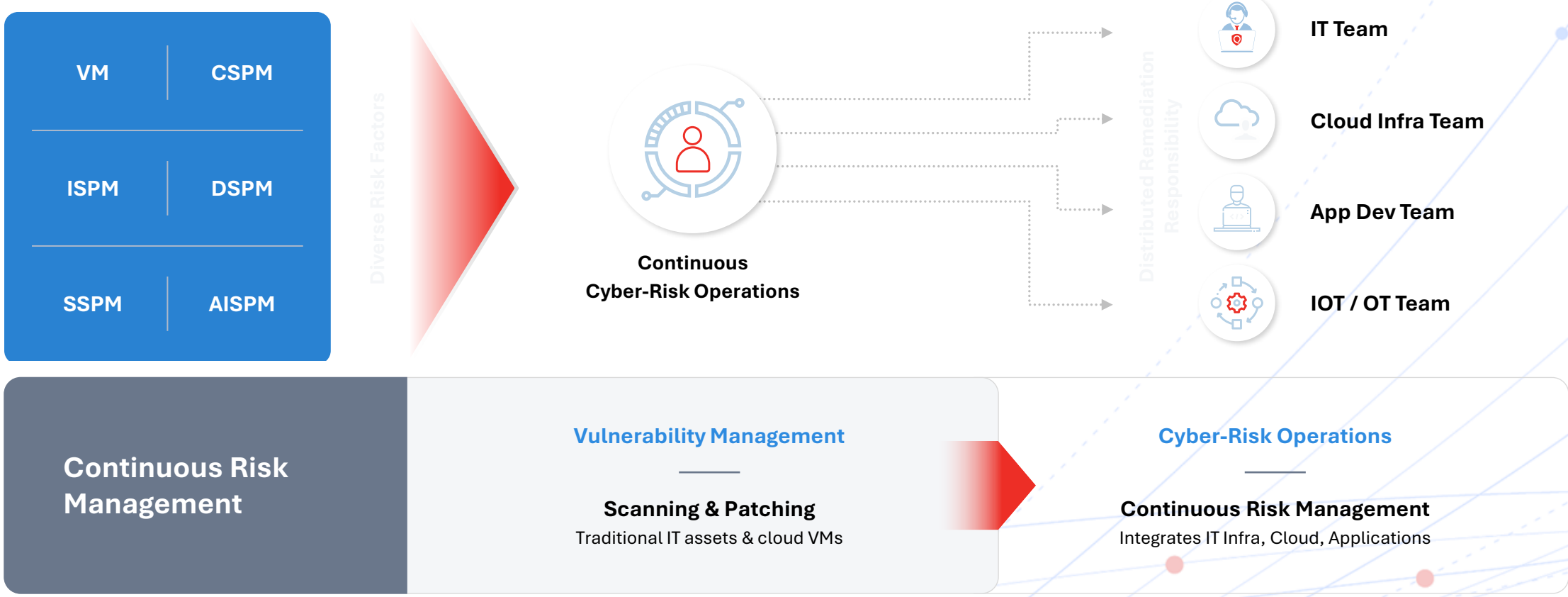
33%

Software are not required, increasing attack surface, cost and efforts on VM, Patch

Qualys.

Charting the course forward - The Rise of the Risk Operations Center (ROC)

Centralized Risk Orchestration



Continuous Risk Management

Vulnerability Management

Scanning & Patching
Traditional IT assets & cloud VMs

Cyber-Risk Operations

Continuous Risk Management
Integrates IT Infra, Cloud, Applications

Qualys.

Foundations of a Risk Operations Center (ROC)

Security Posture Data

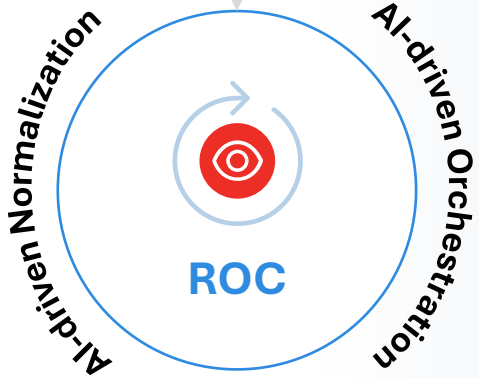
Centrally aggregated security posture data (vulnerabilities & misconfigurations) from asset-specific tools

Threat Intelligence

Vulnerability and threat intelligence to accelerate decision-making and prioritization at scale

Business Context

Contextualization with asset criticality and business impact metrics along with attribution of asset and risk ownership to enable automated workflows



Continuous Threat Exposure Management (CTEM)
CISO

Cyber Risk Quantification (CRQ)
CFO

Automated Compliance
Chief Compliance Officer

Qualys.

One Platform for Centralized Risk Orchestration

Quantify with Business Context

Add business context to quantify cyber risk in monetary terms by evaluating loss attributes and value at risk (VAR).

Enrich with Threat Intelligence

Enrich risk data with Qualys-curated feeds from 25+ threat intelligence sources.

Prioritize with TruRisk™ Score

Prioritize risks by factoring in severity, exploitability, asset criticality & business impact.

Risk Factors Aggregation

Consolidate risk findings across different asset types—including VMs, OT/IOT, cloud, code, user identities & more.

Risk Response Orchestration

Orchestrate precise risk response using AI-driven workflows for "patchless" remediation, automated tickets & real-time alerts.

Unified Asset Inventory

Visualize your attack surface with a unified asset inventory, integrating data from Qualys and third-party sources.

Compliance & Executive Reporting

Ensure compliance readiness with tailored executive reporting and detailed audit trails.

Qualys.

Thank You

Qualys.