Vulnerability Management

Objectives

- Review our current vulnerability management and remediation strategy
- Discuss the CTEM framework
- Propose a five-step implementation guide to CTEM

Current State

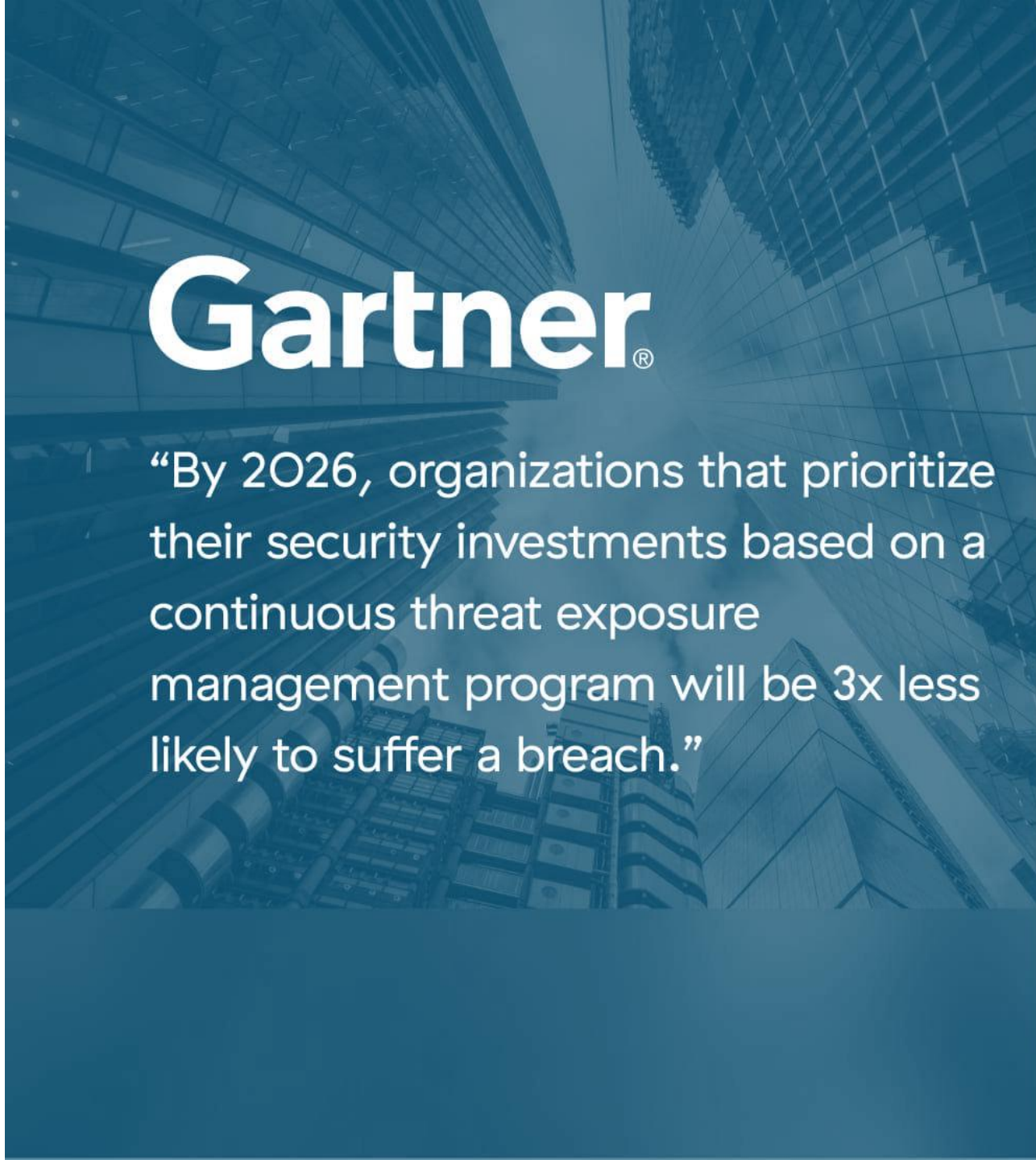
- Qualys is used to scan for vulnerabilities across our environment
- Qualys categorizes vulnerabilities based on severity (Critical, High, Medium, Low)
- Remediation efforts are driven by severity rating from the scanning tool
- We do not have a defined structure to determine what is truly critical to our business

Key Takeaway
A vulnerability identified as Critical in Qualys does not mean it is critical to our business

Introducing CTEM

Continuous Threat Exposure Management (CTEM)

- Shifts focus from vulnerability severity to business risk
- Prioritizes exposures based on asset criticality and real business impact
- Enables us to focus on what actually matters to the business



Five Step Approach to Implement CTEM

Step 1: Establish a structured asset tagging model in Qualys

Step 2: Align business criticality to assets

Step 3: Use asset tags and vulnerability data to identify high-risk assets

Step 4: Focus remediation efforts on vulnerabilities affecting high-risk assets with a direct path from external sources

Step 5: Continuously refine and improve

Detailed Approach

STEP	1 | Establish a structured asset tagging model in Qualys	2 | Align Business Criticality to Assets	3 | Identify High-Risk Assets	4 | Focus Remediation on High-Risk Assets	5 | Continuously Refine and Improve
DESCRIPTION	We have 2000 assets in Qualys We need to tag these assets by: • Asset Type (Workstation, Server, Shopfloor, Network Device) • Environment (Production, Dev) • Business Criticality (High, Medium, Low) • Business Function (MES, Aprsiso, ERP, etc) • Exposure: (Internet-facing, Internal-Only) This allows us to filter and group assets in Qualys to quickly identify high-risk systems	• Define High, Medium, Low criticality tiers on all our assets across cloud, on-prem and network based on business impact • Collaborate with Application and Infrastructure teams to assign business criticality tiers to assets	**Combine key attributes:** • Business Criticality (High / Medium / Low) • Exposure (Internet-facing, Internal-facing) • Asset Type (Server, Workstation, etc) **Example of a high-risk Asset:** • High Business Criticality • Internet-Facing • Server supporting MES application	• Prioritize critical and high vulnerabilities in Qualys on high-risk assets identified in Step 3 • Focus remediation on vulnerabilities impacting business-critical systems • Deprioritize vulnerabilities on low-impact assets	• Regularly review and update asset tagging • Validate business criticality with application and business owners • Adjust prioritization based on changes in environment, exposure and business impact

Step 1

Establish Proper Asset Tagging

Existing Asset Tagging Model

Tag Name	Total Tagged
All Machines	2000
Shopfloor_PROD_Workstation	254
Test	78
EC2	76
Oracle	27
Servers	9

Proposed Tagging Model

- Asset Type (Workstation, Server, Shopfloor, Network Device)
- Environment (Production, Dev)
- Business Criticality (High, Medium, Low)
- Business Function (MES, Network Device,ERP, etc)
- Exposure (Internet-facing, Internal-Only)

Step 2

Align Business Criticality to Assets

- Define High, Medium, Low criticality tiers on all our assets across cloud, on-prem and network based on business impact
- Collaborate with Application and Infrastructure teams to assign business criticality tiers to assets

Step 3

Identify High-Risk Assets

Combine key attributes:

- Business Criticality (High / Medium / Low)
- Exposure (Internet-facing, Internal-facing)
- Asset Type (Server, Workstation, etc)

Example of a high-risk Asset:

- High Business Criticality
- Internet-Facing
- Server supporting our ERP

Step 4

Focus Remediation on High-Risk Assets

- Prioritize critical and high vulnerabilities in Qualys on high-risk assets identified in Step 3
- Focus remediation on vulnerabilities impacting business-critical systems
- Deprioritize vulnerabilities on low-impact assets

Step 5

Continuously Refine and Improve

- Regularly review and update asset tagging
- Validate business criticality with application and business owners
- Adjust prioritization based on:
    - Changes in environment, exposure, and business impact