



Lauren Holloway

CISSP, CISA, CISM
Director, Data Security Standards
PCI Security Standards Council



John Bloomfield

CISSP, CISA, CISM, CDPSE, PCIP
Manager, Data Security Standards
PCI Security Standards Council

2025
EUROPE
COMMUNITY
MEETING

Vulnerability Management for PCI DSS

A Risk-Based Approach

PCI DSS Vulnerability Scans

External vulnerability scans (ASV scans)

Internet-facing IPs

PCI-Approved Scan Vendor (ASV)

Pass/fail – all vulnerabilities above CVSS 3.9 are fixed

Internal vulnerability scans

Internal systems

Qualified internal staff or an external resource

Vulnerabilities resolved or addressed according to entity's assigned risk

Is penetration testing a vulnerability scan?

No, it is not

Attempts to exploit vulnerabilities

Complements but does not replace scans

External ASV Scans

Requirement 11.3.2

- Internet-facing IP addresses – more risk!
- Using a PCI-listed Approved Scan Vendor
- Passing scan required at least once every three months
- Passing = all medium and high vulnerabilities are resolved

Vulnerability Scans & Approved Scanning Vendors

A Resource Guide from PCI Security Standards Council

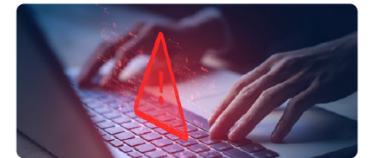
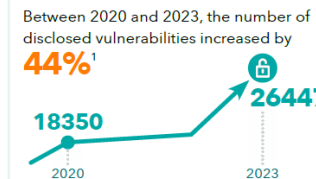
What is a Vulnerability Scan?

A process for identifying security weaknesses and flaws in systems and software. New vulnerabilities, security holes, and bugs are being discovered daily. Test your systems regularly to identify weaknesses and address them as soon as possible.

Why are vulnerability scans important?

In 2023, **25%** of high-risk vulnerabilities were exploited on the day of disclosure.¹

Another **50%** of these high-risk vulnerabilities were exploited within 19 days.¹



One of the main ways attackers access an organization is by **exploiting vulnerabilities**²

Sources:

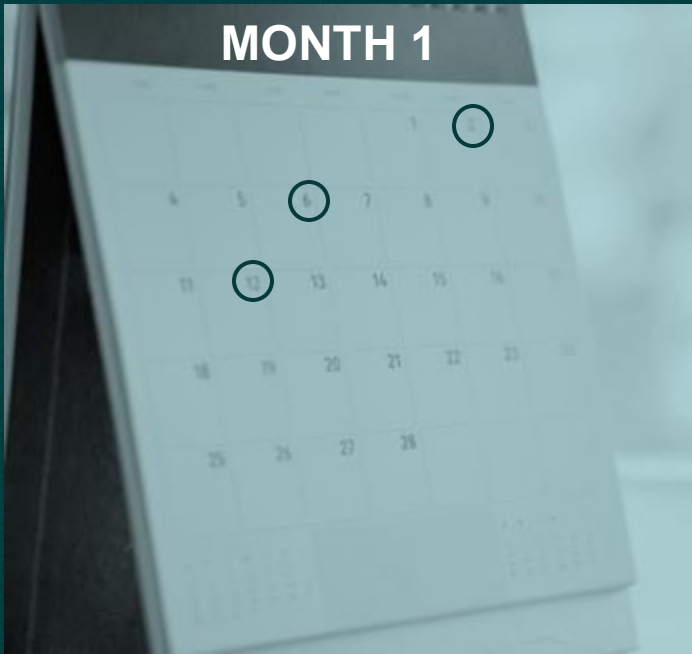
1: [Qualys 2023 Threat Landscape Year in Review: If Everything Is Critical, Nothing Is](#)

2: [2023 Verizon Data Breach Investigation Report](#)

Regular vulnerability scans help an organization identify and address vulnerabilities promptly, which reduces the likelihood of an attacker exploiting a vulnerability and potentially compromising the organization and all its payment account data.

What is an Approved Scanning Vendor (ASV)?





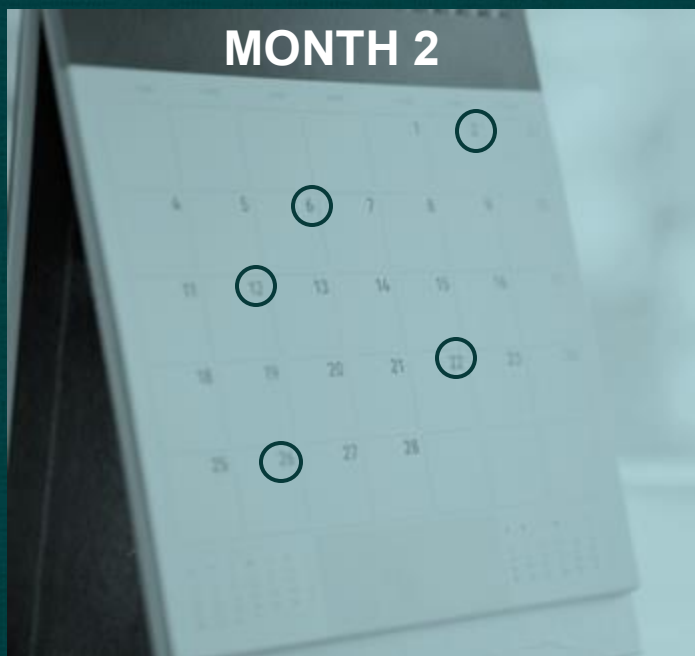
Strongly Encouraged – Scan More Frequently!

- More opportunities to find and correct vulnerabilities within the 3-month period
- Finding vulnerabilities earlier reduces the risk of an attacker exploiting them
- Multiple scans means not forgetting to perform a scan that period

SCAN

REMEDiate

RESCAN



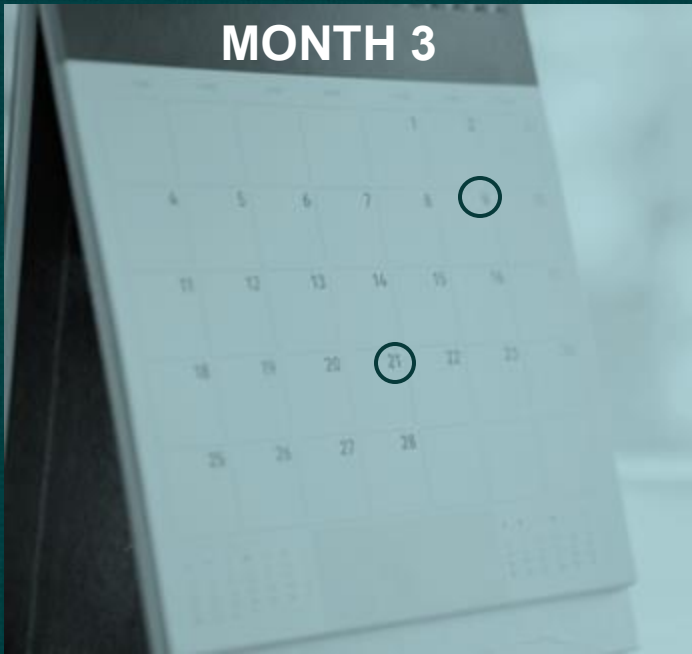
Strongly Encouraged – Scan More Frequently!

- More opportunities to find and correct vulnerabilities within the 3-month period
- Finding vulnerabilities earlier reduces the risk of an attacker exploiting them
- Multiple scans means not forgetting to perform a scan that period

SCAN

REMEDiate

RESCAN



Strongly Encouraged – Scan More Frequently!

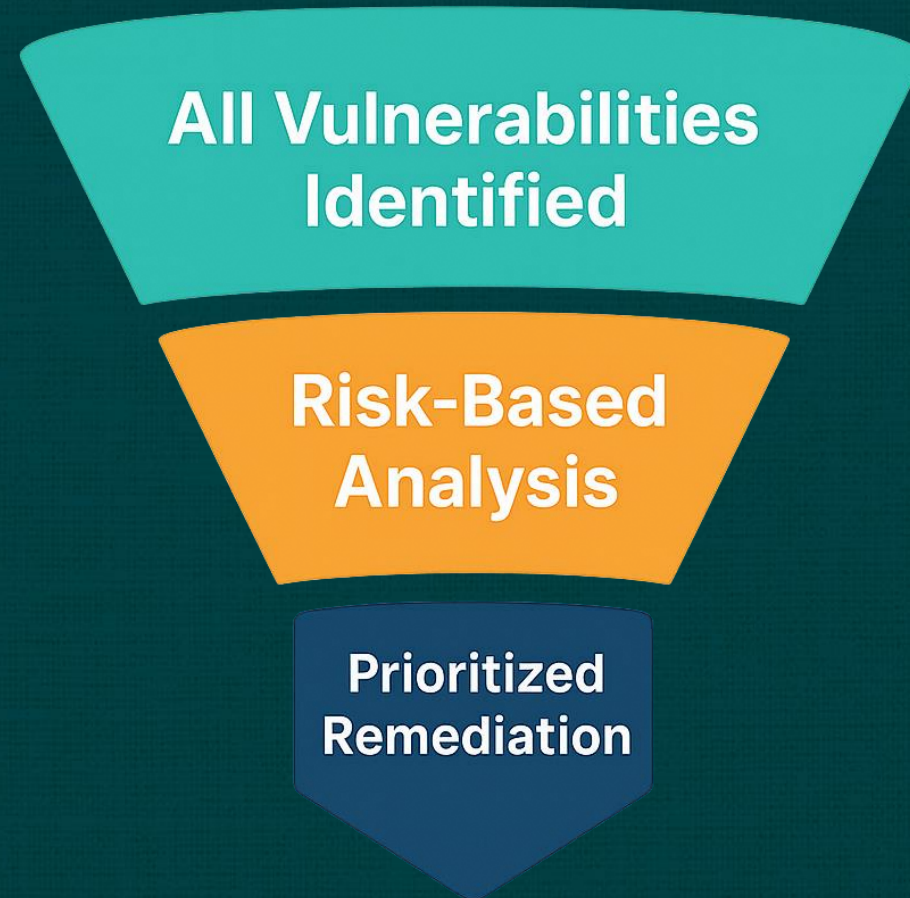
- More opportunities to find and correct vulnerabilities within the 3-month period
- Finding vulnerabilities earlier reduces the risk of an attacker exploiting them
- Multiple scans means not forgetting to perform a scan that period

SCAN

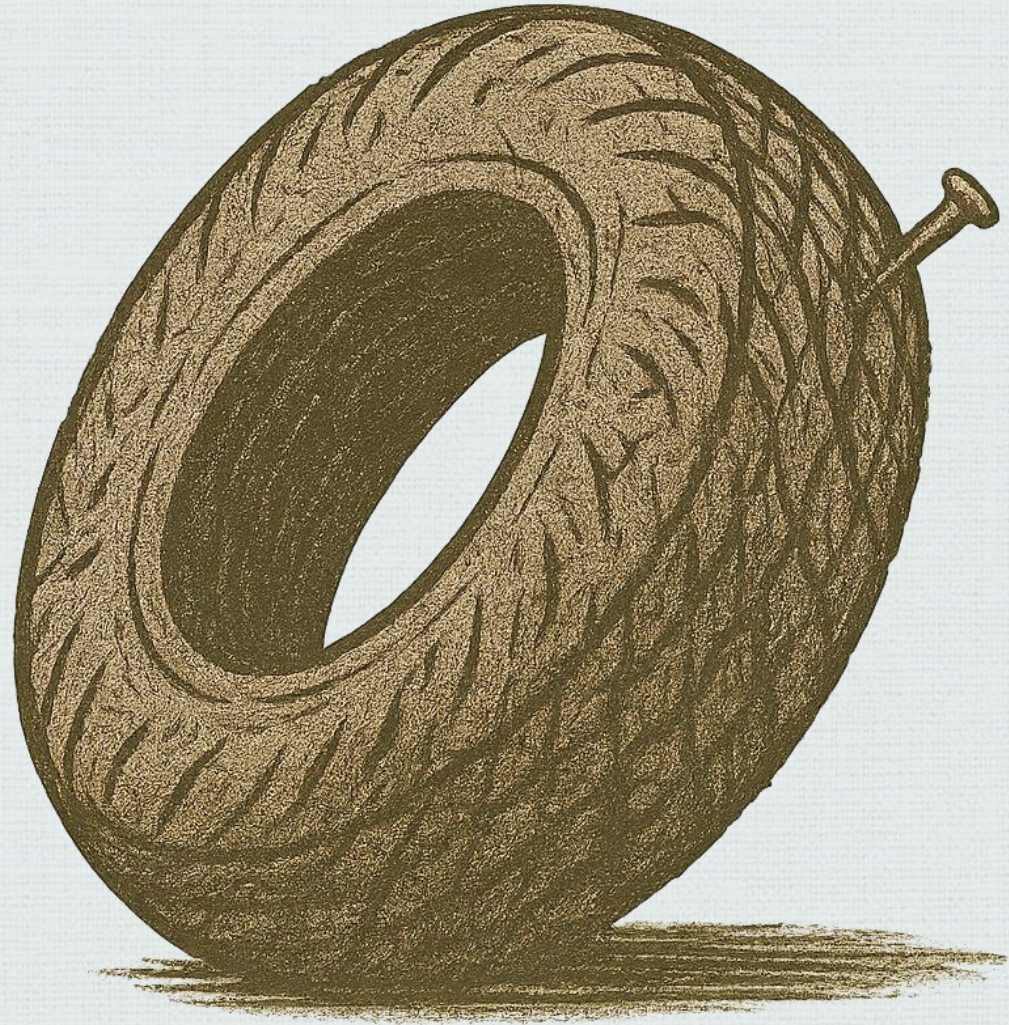
REMEDiate

RESCAN

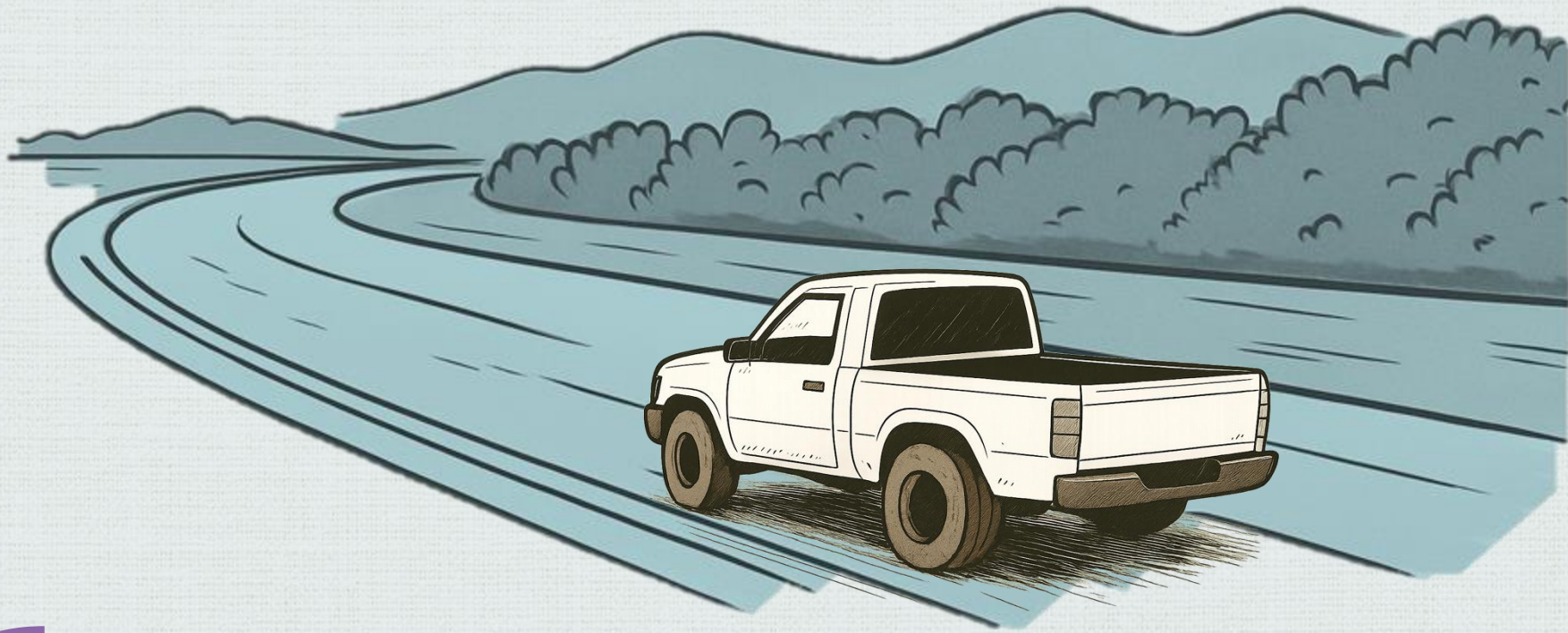
Internal Vulnerability Processes



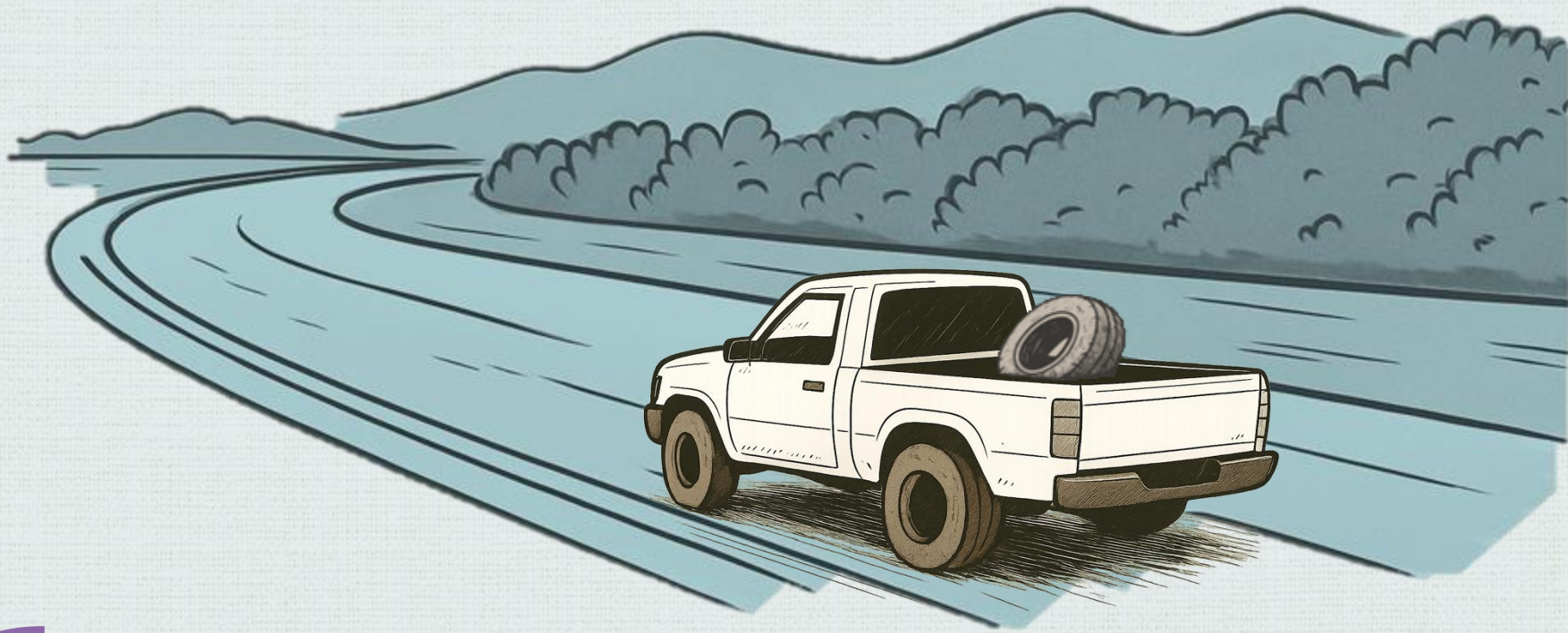
Tyres



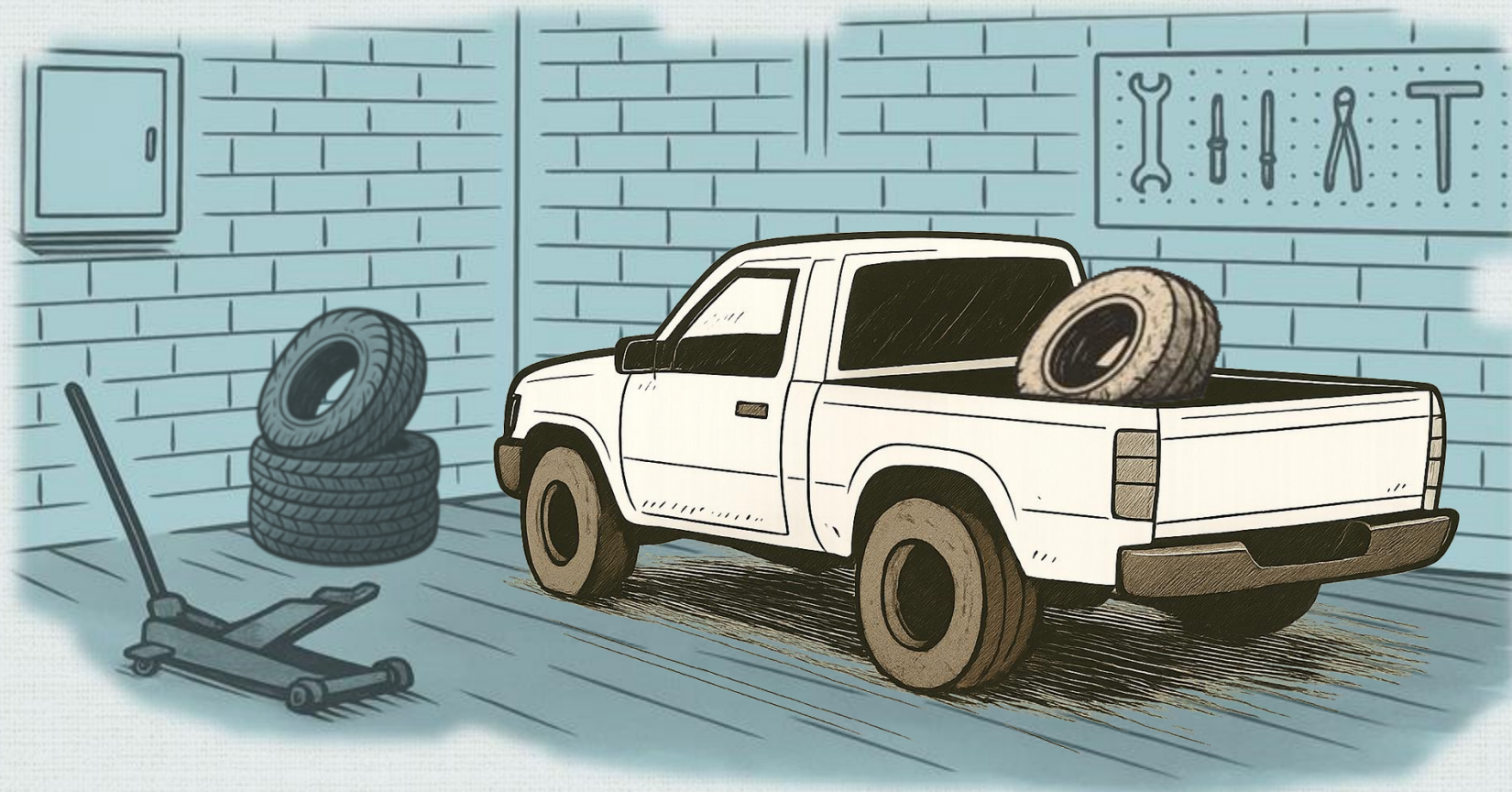
The worn damaged tyre...



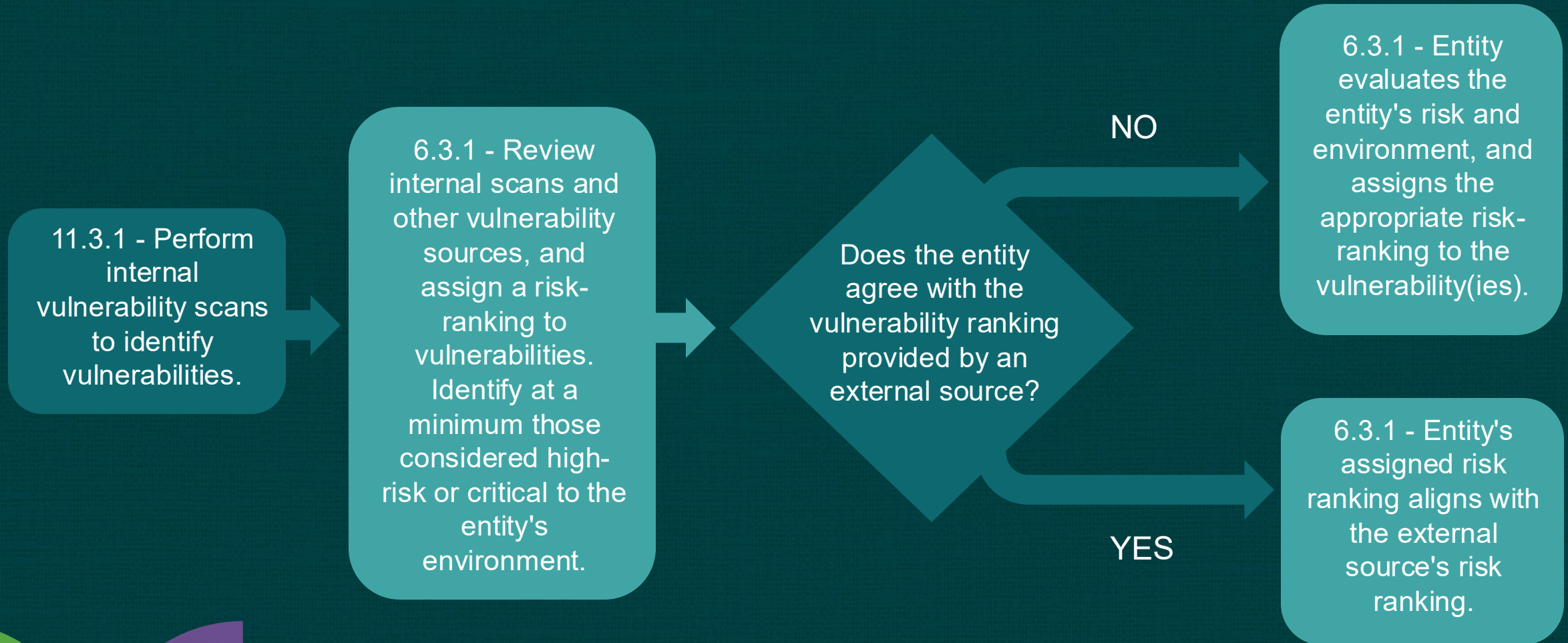
...the damaged
spare...



...in the garage.



Identify and Risk-Rank Vulnerabilities



Resolve or Address Vulnerabilities

CRITICAL AND HIGH RISKS

11.3.1 - Resolve critical and high-risk vulnerabilities according to the risk rankings the entity assigned in Requirement 6.3.1.

CRITICAL

6.3.3 - Install patches/updates for all critical vulnerabilities within one month of release.

ALL OTHER RISKS

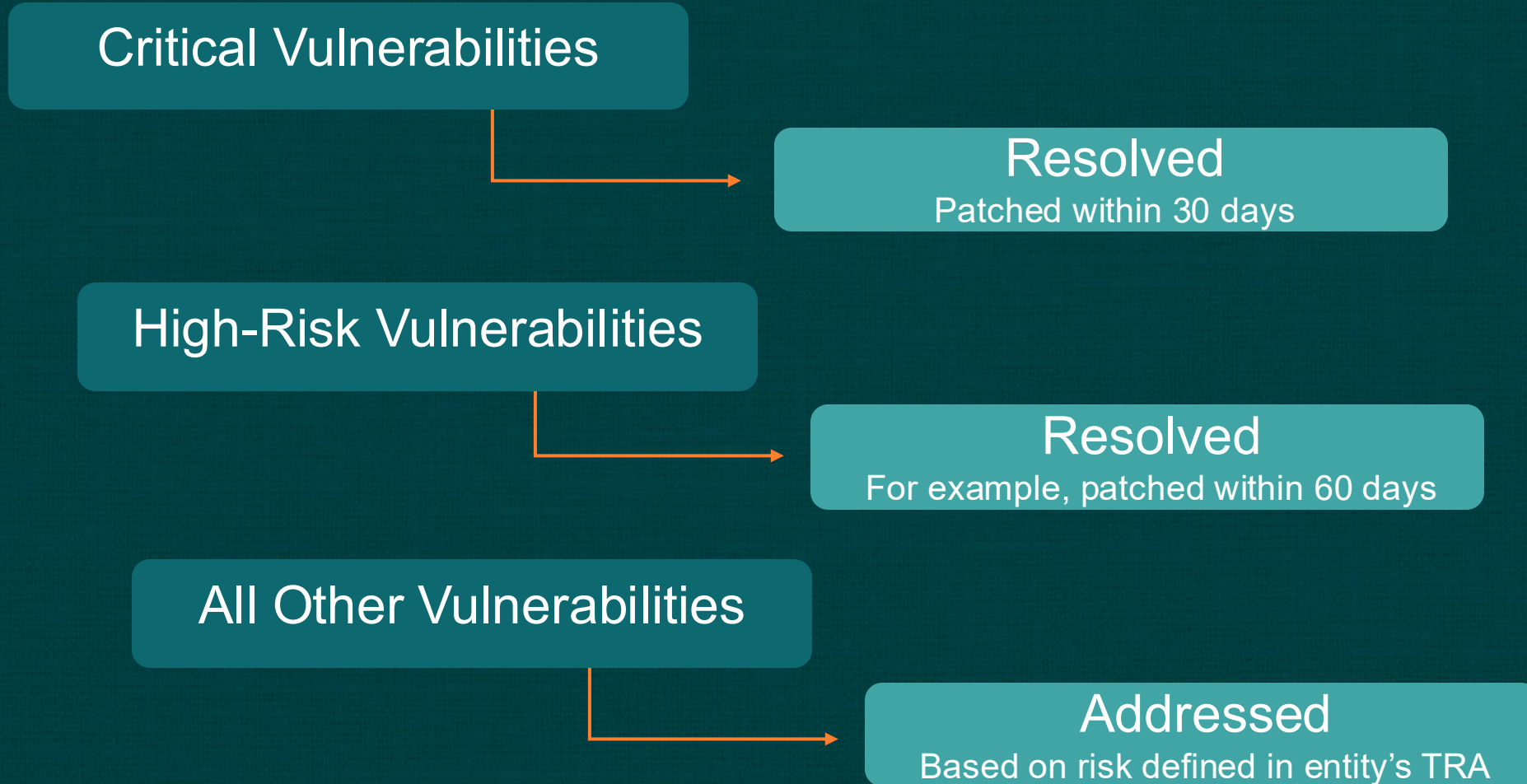
11.3.1.1 - Address all other vulnerabilities (not critical or high-risk) based on the entity's risk defined in a TRA.

HIGH-RISK

6.3.3 - Install all other applicable patches/updates within the time frame determined by the entity, based on the level of risk identified in Requirement 6.3.1.

"All other" includes patches/updates for high-risk vulnerabilities and any lower risk vulnerabilities.

Critical, High, and All Other Vulnerabilities



Difference Between Resolve and Address

Resolve

Fix or solve the vulnerability

Examples:

- Install a security patch
- Change a configuration
- Add a compensating control
- Disable a service
- Decommission a system
- Transfer the risk

Address

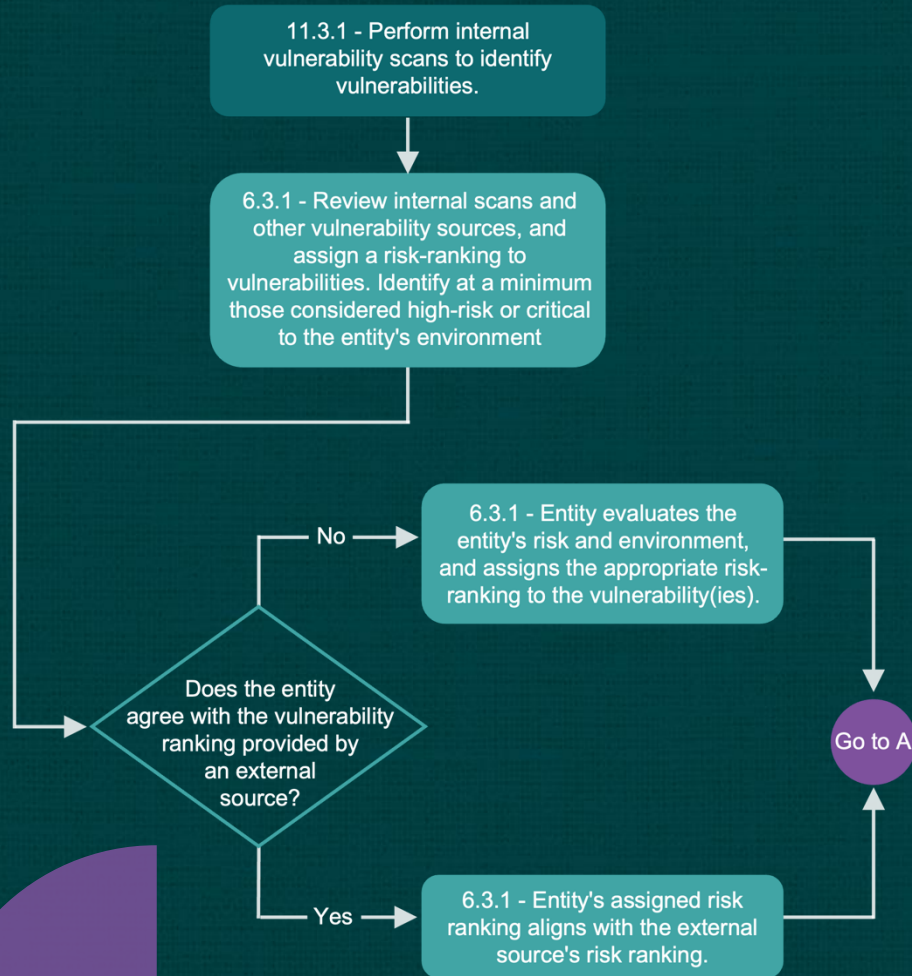
Determine whether to *resolve the vulnerability* or mitigate the risk by *addressing it in another way*.

Examples:

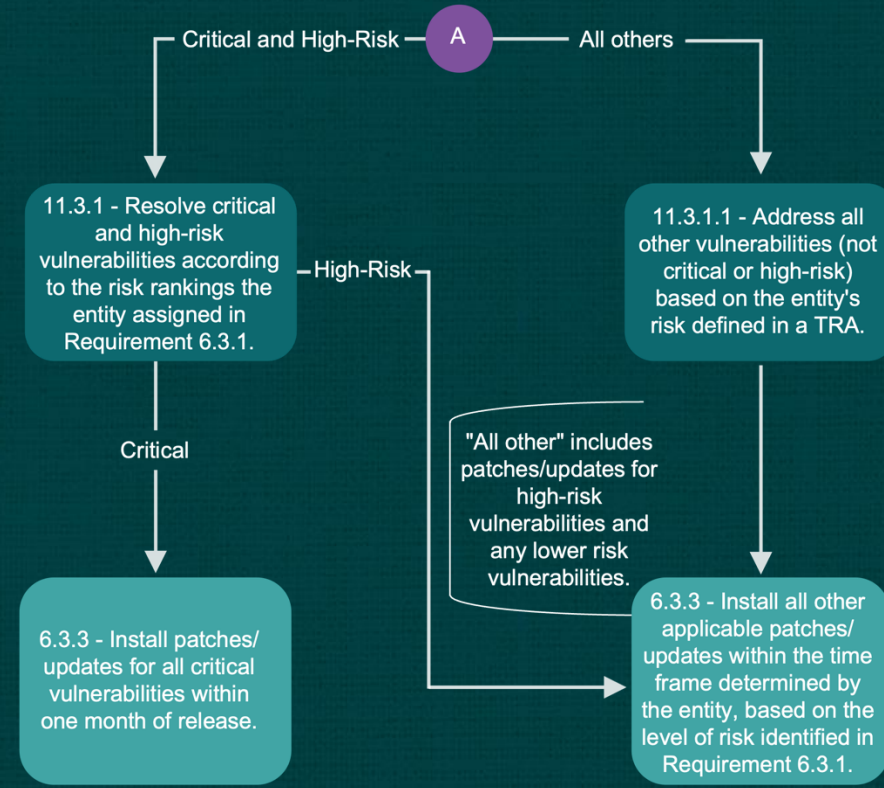
- Resolve it
- Accept a low-risk vulnerability after evaluating risk (TRA)

PCI DSS Vulnerability Management Processes

Identify and Risk-Rank Vulnerabilities



Resolve or Address Vulnerabilities



Resolve - the entity solves or fixes the vulnerability.

Address - the entity determines whether to resolve the vulnerability or to mitigate the risk by addressing the vulnerability in another way (e.g., with a compensating control or by disabling a vulnerable service).

Understanding Internal Vulnerabilities

Severity \neq Risk without context

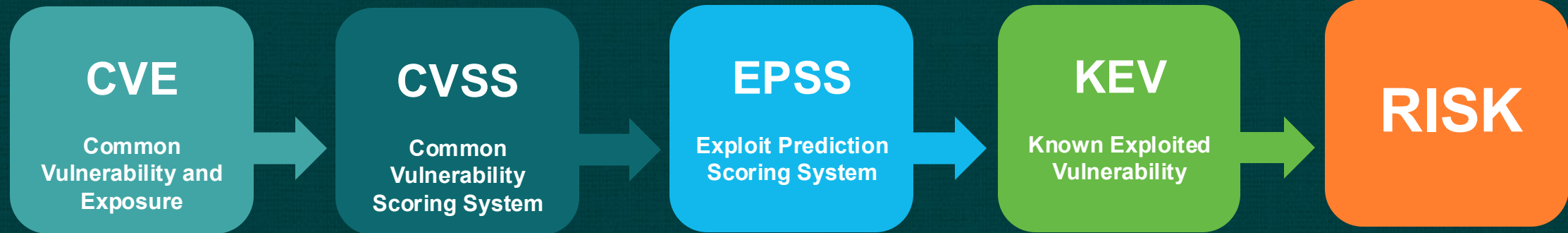
- A vulnerability does not always mean real-world risk
- Focus on data-driven signals
- Use context layers to prioritize effectively



Understanding Internal Vulnerabilities

Severity \neq Risk without context

- A vulnerability does not always mean real-world risk
- Focus on data-driven signals
- Use context layers to prioritize effectively



Building Context to Target the Risks

Threat Intelligence and Multiple Sources

- Scanning alone is not the full picture
- KEV + EPSS for near-real-time risk scoring
- Combine internal scan data with external intel
- Feed into a centralized risk-ranking process
- Context turns raw CVEs into actionable priorities



Building Context to Target the Risks

Threat Intelligence and Multiple Sources

- Scanning alone is not the full picture
- KEV + EPSS for near-real-time risk scoring
- Combine internal scan data with external intel
- Feed into a centralized risk-ranking process
- Context turns raw CVEs into actionable priorities



TRA for All Other Vulnerabilities

Targeted Risk Analysis (TRA) - Your Risk Translator

INPUTS

Ranked vulnerabilities,
affected assets, asset criticality

ANALYSIS

Vulnerability risk by
asset

OUTPUTS

Vulnerability risk rank
per asset, how to
address, frequency

- Document in accordance with TRA Requirement 12.3.1
- Show assessor TRA and supporting documentation/evidence
- Annually - re-evaluate risk and re-assess prior decisions



Authenticated Internal Scans – New in v4.x

Requirement 11.3.1.2

- Required after March 2025
- All internal scans, except for systems that are unable to accept credentials

What is an Authenticated Scan?

Unauthenticated Scans

No authentication
(no username/password)

See only what an external attacker
with no credentials sees

Limited view hides many
vulnerabilities

Authenticated Scans

Authenticate with
privileges

See configs, software,
permissions, etc.

Full, privileged view reveals
many vulnerabilities

PCI DSS Vulnerability Management: Key Takeaways

External ASV scans
Requirement 11.3.2

Pass/Fail

Resolve all vulnerabilities with CVSS scores of 4.0 through 10.0

Performed by a PCI-listed ASV

At Least One Passing Scan Every 3 Months

PCI DSS Vulnerability Management: Key Takeaways

Internal Scans
Requirement 11.3.1

Identify & Risk Rank
Requirement 6.3.1

Resolve with Patching
Requirement 6.3.3

Or Address per a TRA
Requirement 11.3.1

The background is a dark teal color. It features several large, overlapping geometric shapes: a purple arc in the top left, a green arc in the top center, a large orange arc on the right side, a teal arc in the bottom left, and a purple arc in the bottom right. The word "Conclusion" is written in white, bold, sans-serif font in the center-left area.

Conclusion



2025 EUROPE COMMUNITY MEETING