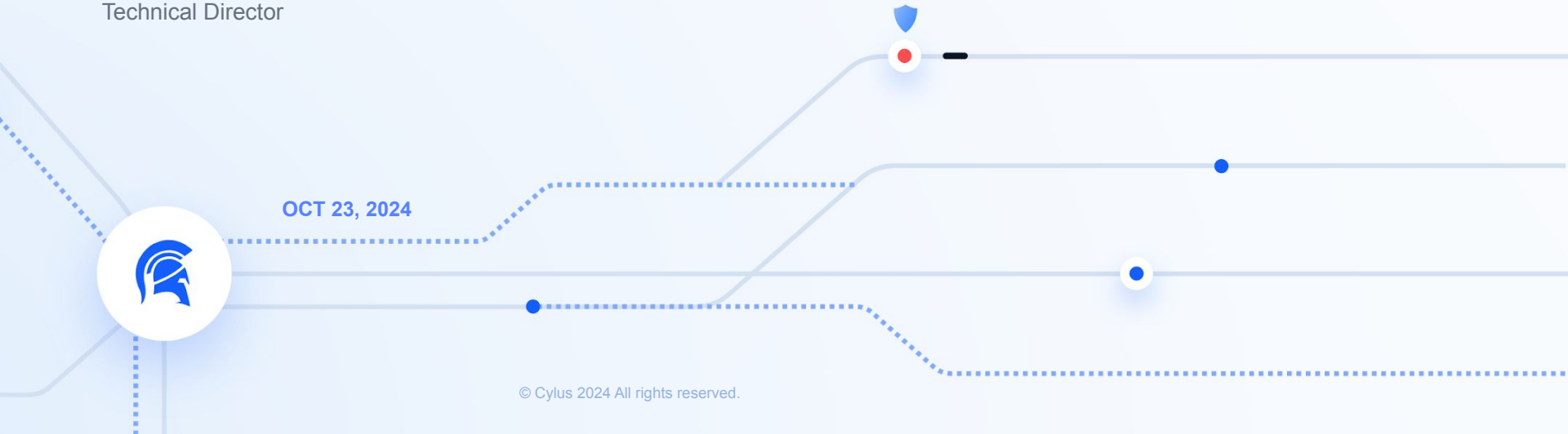
CYLUS

Vulnerability Management in the Rail Environment

Yoni Korlander
Technical Director



OCT 23, 2024

About Me

Yoni Korlander
Technical Director

- Over 15 years of experience in cybersecurity, telecom and critical infrastructure. Specializing in product and technical leadership roles
- Technical Director at Cylus
- Oversaw cybersecurity solution implementations in both transit and freight rail companies in North America

My Challenge:

Being the first talk after lunch.

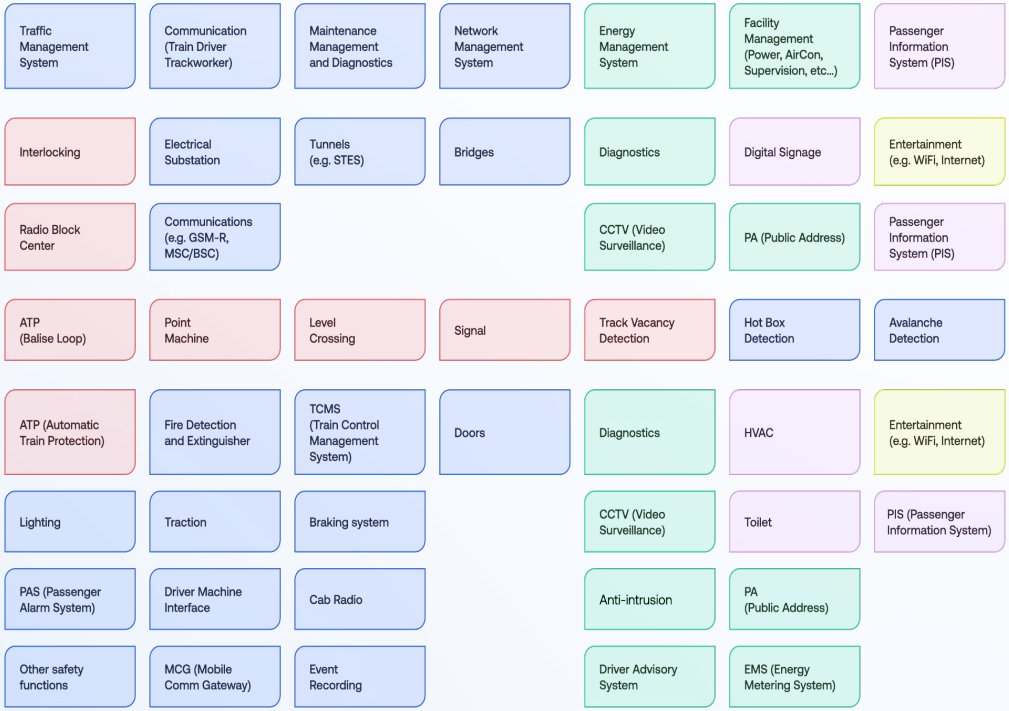
CYLUS

Securing Rail is Hard.

CYLUS

You Probably Know This Already

- Multi-vendor networks
- Tens of thousands of assets
- Various maturity levels
- 30-year lifecycle



Designed systems often become obsolete before they are deployed.

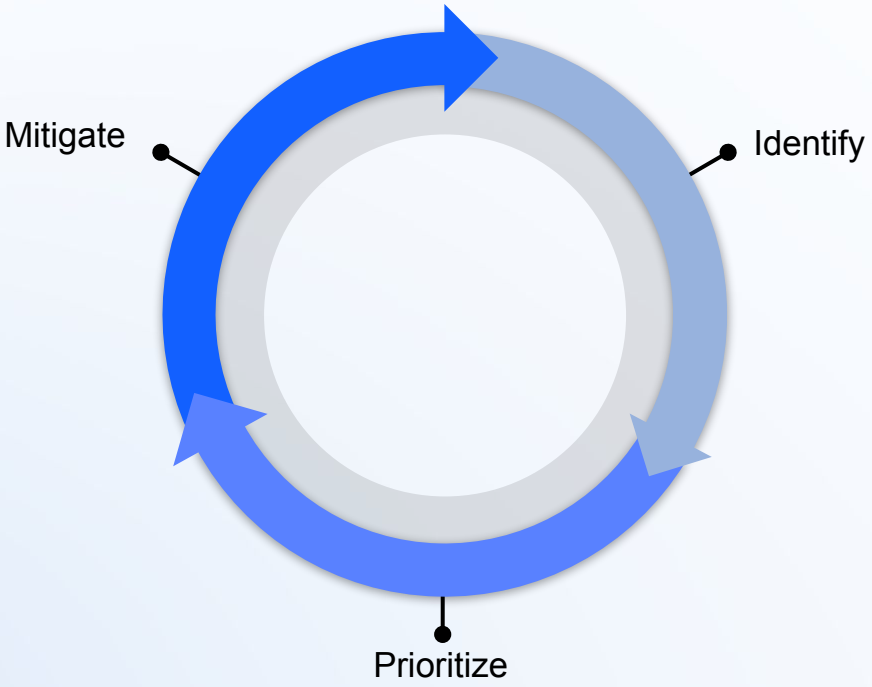
CYLUS

You Can Still Manage Vulnerabilities Effectively

- Focus on what's worth your time and risk
- Don't chase patching everything
- Create a plan for both install base and new builds

CYLUS

The Vulnerability Management Pillars



CYLUS

Pillar I: Identification

CYLUS

Pillar I: Identification

The goal: Understand what vulnerabilities you have in your environment

The Process:

- Identify the assets in your environment
- Identify the software used in your assets
- Identify how vulnerabilities apply to software used in your assets

CYLUS

Asset and Software Identification

- Automatic passive network discovery
- Integration with 3rd party asset information (even if it’s spreadsheets)
- Active querying for information enrichment **(*)**
- Integration with SBOM information (if such exists)
- Extract known vulnerabilities for software information

(*) Good luck with safety approvals

CYLUS

Pillar II: Prioritization

CYLUS

2024 CVE Received and Processed

CVEs Received and Processed

Time Period	New CVEs Received by NVD	New CVEs Analyzed by NVD
Today	0	0
This Week	227	227
This Month	2219	1667
Last Month	2534	2590
This Year	31378	13044

CYLUS

Vulnerabilities Calculation: The Naive Approach

of Assets X # of Vulnerabilities per Asset =

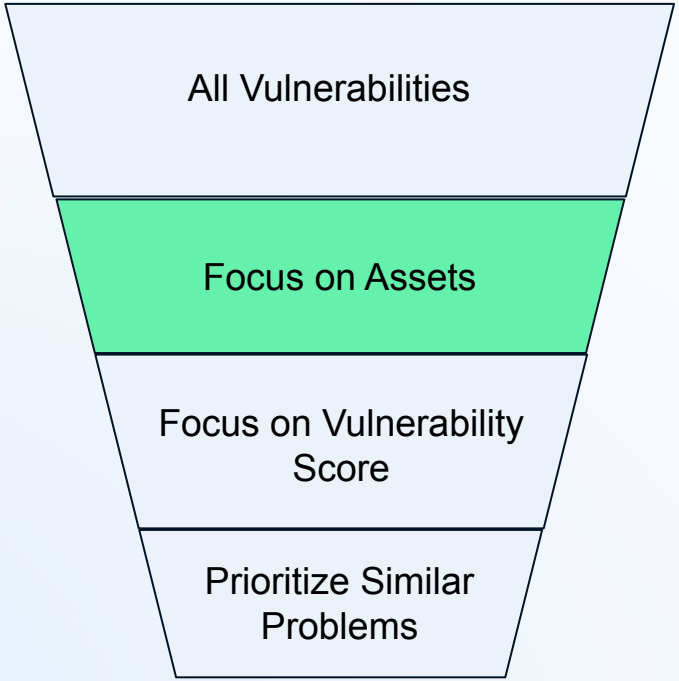
CYLUS

How Do We Reduce the Noise?

- Prioritize your assets
- Prioritize your vulnerabilities
- Prioritize solving similar problems

CYLUS

The Prioritization Funnel



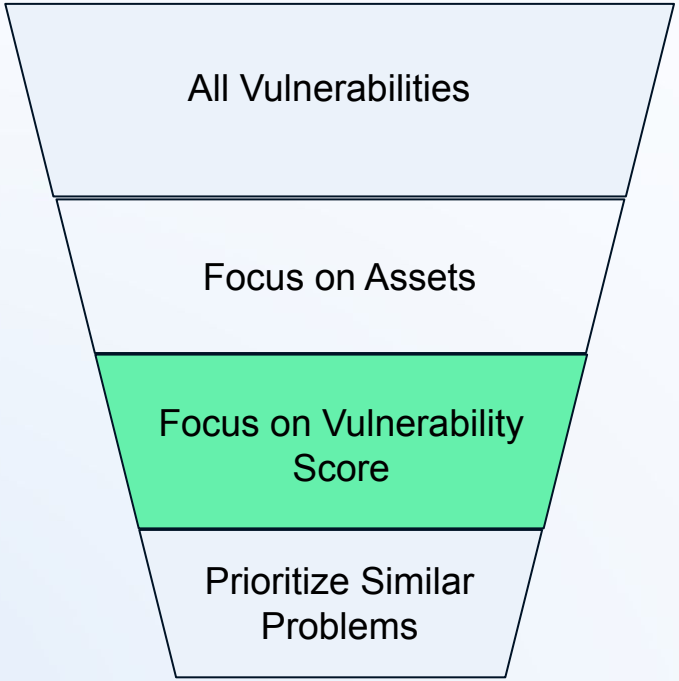
CYLUS

Prioritize Your Assets

- Not all assets are the same. Focus your efforts where it matters most.
- Key Strategies:
  - Crown Jewels First: Assets critical to safety, operations, or compliance
  - External-facing Systems: Systems exposed to external parties or networks, especially those connected to third-party organizations.
  - Wireless Interfaces: Assets with wireless connections, as these can be more vulnerable (e.g., train control systems).

CYLUS

The Prioritization Funnel



CYLUS

Prioritize Your Vulnerabilities

Sample Sources:

1. CISA ICS-CERT
2. Vendor security advisories

Examples:

1. Asset information - context, SIL, Wireless connections
2. Network information - closed/internet facing/wireless connections

Examples:

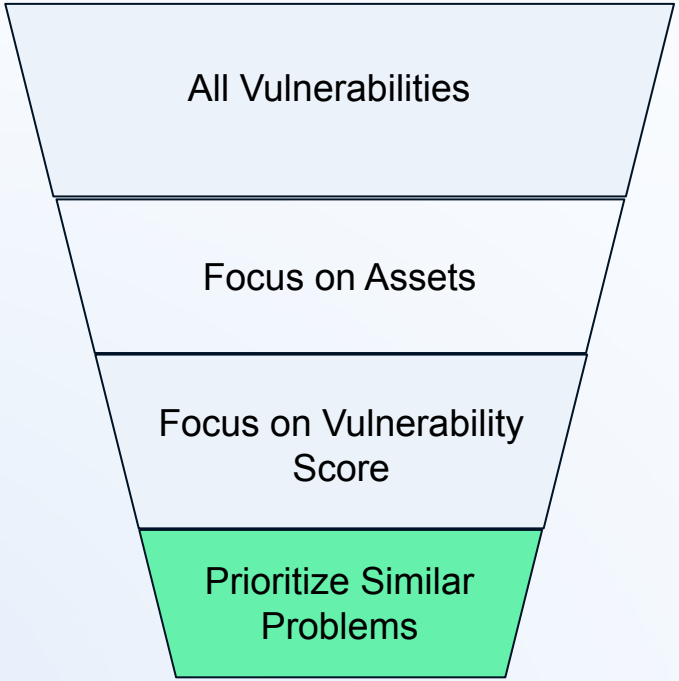
1. KEV
2. Vendor-specific advisories

Reachability

Exploitability

CYLUS

The Prioritization Funnel



CYLUS

Prioritize Solving Similar Problems

- Rail networks have a repetitive nature:
  - Same fleet trains use the same software and hardware configuration
  - Signaling stations and bungalows built similar to each other
- Cluster your vulnerable assets by geographical location, type, vendor, software version, and focus solving them together.

Pillar III: Mitigation

CYLUS

Pillar III: Mitigation

Based on your priorities, collect approved patches and start planning your patching program.

The sad truth: You won't be able to patch it all.

CYLUS

Alternative Mitigations (AKA Compensating Controls)

- Configuration and isolation of vulnerable assets
- Continuous monitoring and detection of assets for exploit signatures
- Incident Response planning
- Prioritize for decommissioning

CYLUS

Make it Easier for Future Self: The Checklist for New Build

- Require hardening by design
- Require vulnerability notification and management
- Ask for SBOM, make sure the vendor maintains it

These activities are not set and forget.

CYLUS

Key Takeaways

- Vulnerability Management in rail is hard…
- It’s key to define a strategy for both install base and new build
- Effective prioritization is a must
- Patching is not the only way to reduce the risk of vulnerabilities

CYLUS

Questions?

CYLUS

CYLUS

Thank you!

Feel free to reach out:

yoni@cylus.com