Maritime Cybersecurity Briefing

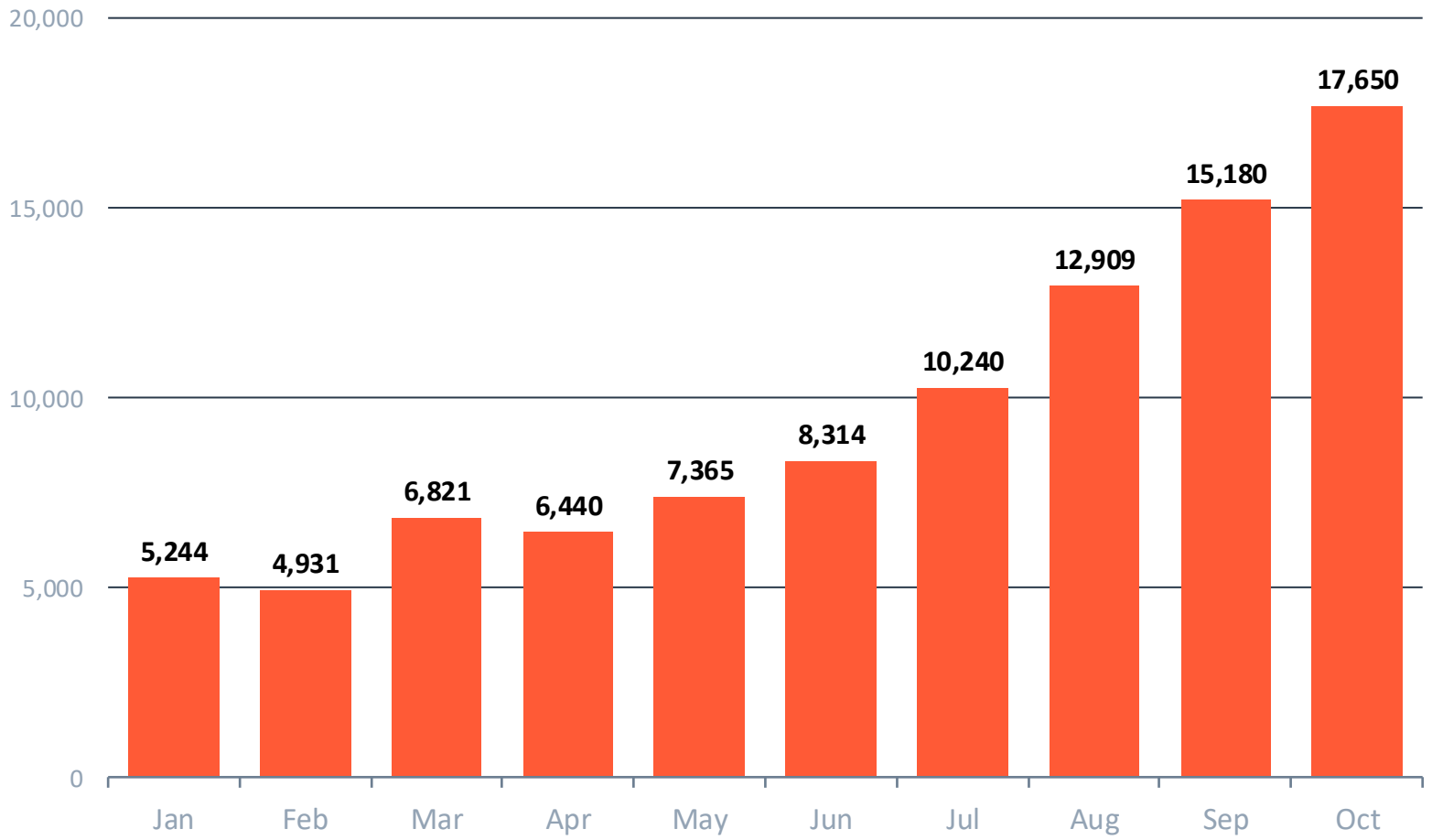
Threats • Observations • Resilience • Compliance

Tony Zhong, CISO | Port of Los Angeles

November 10, 2026

The Frontier AI Vulnerability Surge

All CVEs published per month, January to October 2026



95,000+

CVEs published from January to October 2026

3.4x

October (17,650) vs January (5,244)

9,500+

average CVEs per month, January to October

Source: cve.tools CVE Trends (cve.tools/trends), unified CVE record from CVEList V5, NVD, GHSA, CSAF and FSTEC BDU

Latest Notable Cyber Activities – Past 30 days

CRITICAL VULNERABILITIES

PATCH / VERIFY

PHP2Shell CVE-2026-109618 / 109619, CVSS 9.2, unauthenticated RCE, added to KEV.

Citrix NetScaler CVE-2026-88771 / 88772, CVSS 9.5, zero-day RCE exploited in the wild.

Legacy EBS / OCI Stack Unsupported OS and Java, SSLv2/3 and multiple critical findings. Segmentation directed.

MARITIME CAMPAIGN

38+ **Maritime Organizations listed**

18 countries | $1B+ claimed demands by n0n group

• Oct 12: Bulk listing of ports, terminals, carriers and port IT providers.

• At least 21 victims linked to CyberLogitec, indicating a probable shared service-desk / support archive entry point.

NON-INDUSTRY CYBER ACTIVITIES

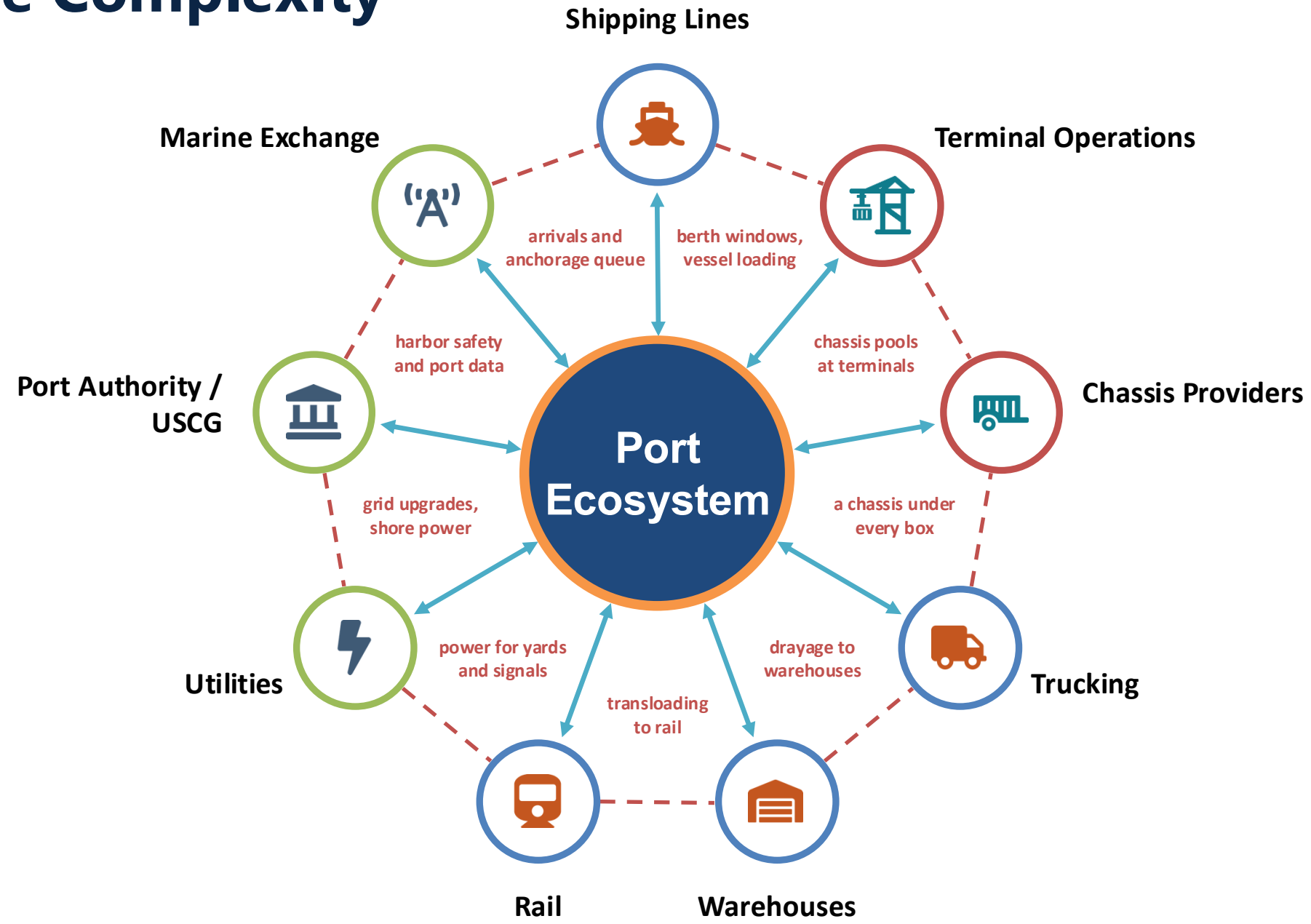
Refrigeration Incidents – Europe

• Nov 2: Belgium, the Netherlands, Ireland, Sweden, Finland, Estonia, Luxembourg and other countries

• Oct 11: Up to 700 supermarkets in France, including Intermarché, Carrefour and Coopérative U

• Disruption: Increase refrigeration temperature, spoil food

Maritime Complexity



Port of LA – Top 5 Cyber Operations Observation

1



Phishing & Social Engineering

Tricking people into giving up passwords, MFA codes or access

2



Reconnaissance

Researching and scanning to map targets, exposed systems and staff

3



Exploitation

Abusing unpatched software flaws to break into systems

4



Denial of Service (DoS / DDoS)

Flooding systems with traffic to knock services offline

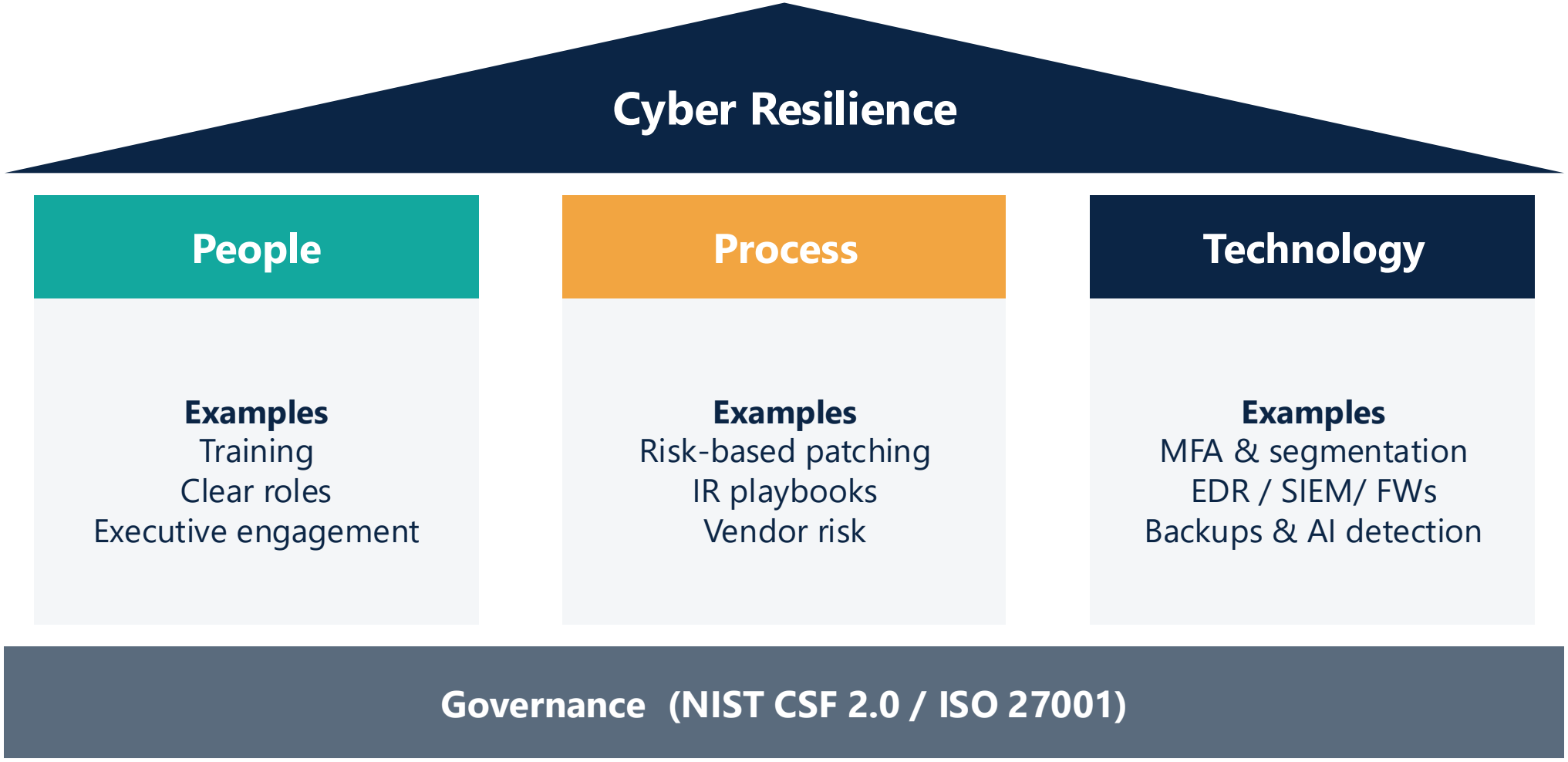
5



Malware

Ransomware, spyware and other code that steals or locks data

Building Resilience: People • Process • Technology



USCG NVIC 02-26: Maritime Cybersecurity Compliance Guidance

PUBLISHED

October 19, 2026

WHAT IT IS

Coast Guard guidance for complying with the 2025 maritime cybersecurity rule

APPLIES TO

U.S. flagged vessels, port facilities and offshore (OCS) facilities regulated under the Maritime Transportation Security Act (MTSA)

DEADLINE

Cybersecurity Plans due July 16, 2027

REQUIREMENTS

1. Designate a Cybersecurity Officer
2. Complete a cybersecurity assessment
3. Submit a Cybersecurity Plan
4. Train staff with IT or OT access
5. Control access and monitor systems
6. Report and respond to incidents
7. Run drills, exercises and audits

Source: U.S. Coast Guard, Navigation and Vessel Inspection Circular 02-26, October 2026 (dco.uscg.mil)

Thank you