

# Risk-Based Cyber Posture in MedTech

1<sup>st</sup> July 2025  
4pm SGT

**Speaker:** Paul Bok, Head of  
Cybersecurity, APAC, TÜV Rheinland

Webinar

APACMed  
The voice of MedTech

TÜVRheinland®  
Precisely Right.



# Administrative Details



This webinar will be **recorded**, and materials will be available after the session.

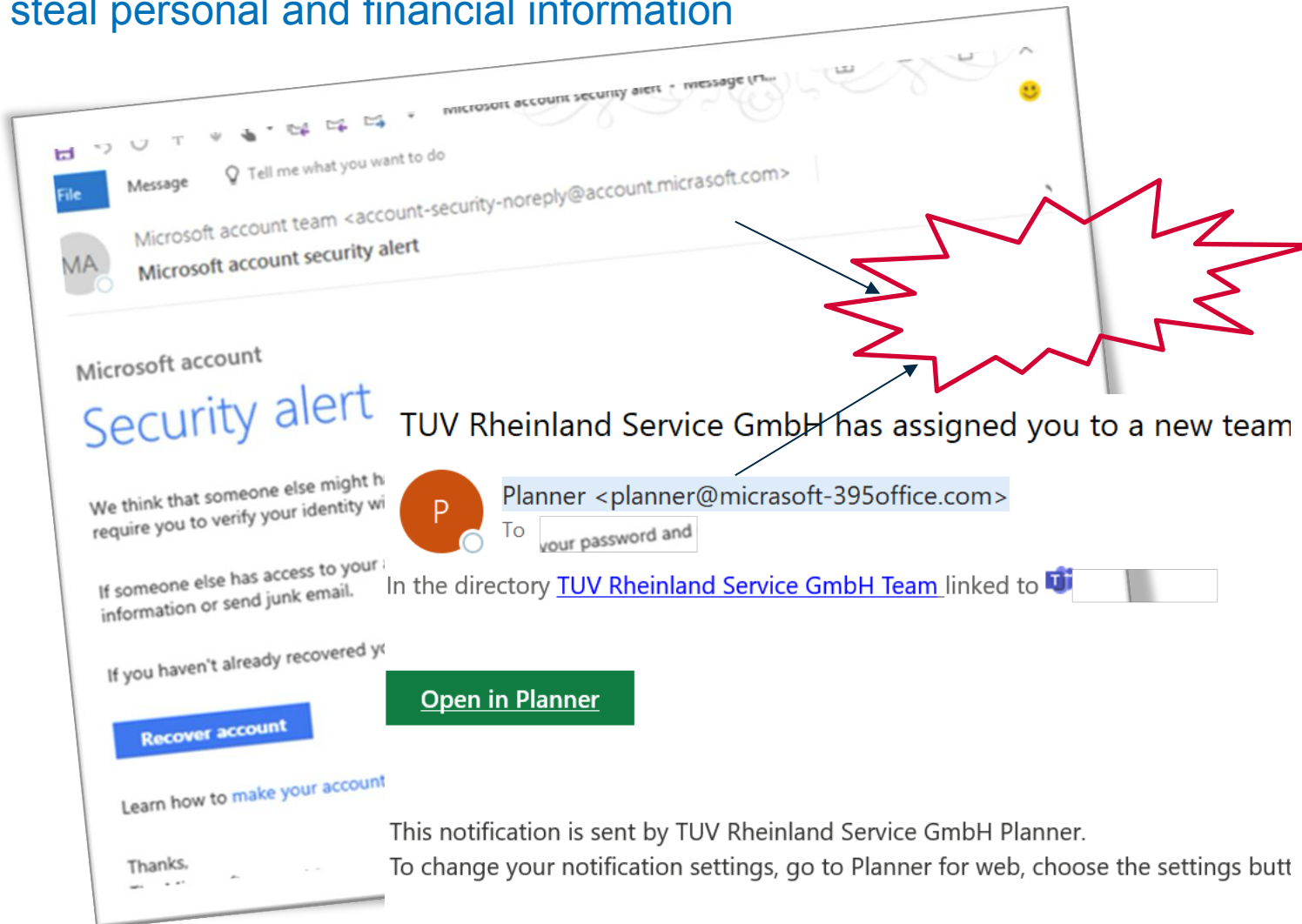


There will be **10 minutes Q&A** session after the presentation. If you have any questions for the presenter, kindly share them via the **Q&A function in Zoom**.

# Introduction

# Social Engineering

The tactic of manipulating, influencing, or deceiving a victim to gain control over a computer system, or to steal personal and financial information



*“The biggest threat to the security of a company is not a computer virus, an unpatched hole in a key program or a badly installed firewall. In fact, the biggest threat could be **you**”*

# Potential Cyber-Security Threat – Medical Device

The U.S. Food and Drug Administration is warning patients using certain Medtronic MiniMed insulin pumps that the devices pose a **potential cybersecurity risk**.



wireless radio frequency (RF) with other devices such as a blood glucose meters, glucose sensor transmitters, and CareLink™ USB devices.

Security researchers have identified potential cybersecurity vulnerabilities related to these insulin pumps. An unauthorized person with special technical skills and equipment could potentially connect wirelessly to a nearby insulin pump to **change settings and control insulin delivery**.

**Impact:** This could lead to **hypoglycemia** (if additional insulin is delivered) or **hyperglycemia** and **diabetic ketoacidosis** (if not enough insulin is delivered).

Insulin Pump	Software Versions
MiniMed™ 508 pump	All
MiniMed™ Paradigm™ 511 pump	All
MiniMed™ Paradigm™ 512/712 pumps	All
MiniMed™ Paradigm™ 712E pump	All
MiniMed™ Paradigm™ 515/715 pumps	All
MiniMed™ Paradigm™ 522/722 pumps	All
MiniMed™ Paradigm™ 522K/722K pumps	All
MiniMed™ Paradigm™ 523/723 pumps	Software Versions 2.4A or lower
MiniMed™ Paradigm™ 523K/723K pumps	Software Versions 2.4A or lower
MiniMed™ Paradigm™ Veo™ 554/754 pumps	Software Versions 2.6A or lower
MiniMed™ Paradigm™ Veo™ 554CM/754CM pumps	Software Versions 2.7A or lower

# Complex Ecosystem of Medical Device Supply Chain

Healthcare industry which includes medical device supply chain is increasingly interconnected and integrated with various suppliers, software developers and equipment manufacturers which are potential targets for malicious threat actors.

*Medical device supply chain reflects the complexity of this diverse ecosystem*

*Critical to build a risk aware culture and management system across the medical device supply chain*



# Compromised Medical Devices Poses Serious Risks to Safety, Privacy & Ops

Compromised medical devices can lead to misdiagnosis and improper treatment, medical devices compromised with backdoors enable attackers to siphon sensitive information and malware infected medical devices can cause hospital information systems to malfunction



## Patient Health

- System used for diagnosis, monitoring and treatment
- Medical devices
- Medical equipment
- Hospital Information System



## Data Privacy

- Patient PII records such as medical records and insurance information
- Employee PII
- Research and drug trial data
- Payroll
- Intellectual Property



## Hospital Operations

- Staff scheduling databases
- Hospital-paging systems
- Building controls
- Pneumatic tube support systems
- Inventory systems
- Administration



# Compromised Medical Devices Poses Serious Risks to Safety, Privacy & Ops

- Medical devices will often contain complex electronics (often electromechanical) with supporting software or firmware. The latter is often used to control specific features of a device and will often be loaded directly onto a chipset. There are a large number of potential risks to medical devices, but more common examples include:
  - **Flawed or defective software and firmware.** Writing software code that is free of security issues is very difficult. In many instances software developers have not been trained to write secure software and are unaware of the risks. In many cases the software has not undergone a test to check for security issues.
  - **Incorrectly configured network services.** This could include the use of unencrypted connections to the internet resulting in patient data being transmitted in plain/clear text. Attackers could take advantage of open network services and use them as an entry point on a device.
  - **Security and privacy issues** such as the use of poor passwords or excessive permissions where a basic user can access administration features. It is not uncommon to see passwords written down and taped or stuck to the device. Passwords may also be “hard coded” in a device, making their retrieval by hackers simple.
  - **Poor data protection.** This may occur due to the absence or poor use of data encryption. If used properly encryption is a powerful mechanism to protect data at rest and in transit (i.e. as it is being sent across a network). Most failures in data protection stem from incorrect use of encryption keys and poor technical implementations.
  - **Improper disposal or loss of the device** with on-board memory still containing patient data. The secure destruction of the device needs to be factored into the cost of ownership and the disposal process documented and audited. People lose smartphones every day, but if such a device has patient sensitive data on it the medical device manufacturer could be subject to a regulatory investigation.
  - **Malware and spyware targeting medical devices.** Hackers and cyber criminals look for the easiest return on their investment of time and money for each attack. Medical devices may not yet be subject to more general cyber-attacks, unless by mistake, but targeted attacks for specific nefarious purposes must never be discounted.





# FDA & IEC 81001-5-1 Overview

# FDA Guidance – 524(b)

## Key Elements

- 524(b)(1): **Plans to Manage Vulnerabilities**
  - To submit a plan to monitor, identify, and address post-market cybersecurity vulnerabilities and exploits.
  - This includes having procedures for coordinated vulnerability disclosure.
- 524(b)(2): **Cybersecurity Processes and Updates**
  - Mandates that manufacturers design, develop, and maintain processes and procedures to provide reasonable assurance that the device and related systems are cybersecure.
  - Requires to make post-market updates and patches available to address vulnerabilities
- 524(b)(3): **Software Bill of Materials(SBOM)**
  - Manufacturers of cyber devices to provide a SBOM, including
    - ✓ Commercial
    - ✓ Open-source
    - ✓ Off-the-shelf software components



# FDA Guidance - Requirement

## Cyber Security

- Static and dynamic code analysis including testing for credentials that are "hardcoded", default, easily guessed, and easily compromised
- Vulnerability scanning
- Robustness testing
- Penetration testing
- Third party test reports
- Evidence of security effectiveness of third-party OTS software in the system (Also related to OTTS deficiency).

### IEC 81001-5-1 Requirement:

- **Risk Management:** Continuous Risk Assessment
- **Secure Development:** Secure Coding Practices & Design Principal
- **Testing & Assessment:** Regular Security Audits, Vulnerability Scanning, & Penetration Testing.
- **Incident Response Protocols:** Procedures for Detecting, Responding to, & Recovering
- **Maintenance:** Security Updates, Patches and Continuous Monitoring

### FDA Requirement

**Abuse or misuse cases, malformed and unexpected inputs**

**Robustness Testing**

**Fuzz testing**

**Attack surface analysis**

**Vulnerability chaining**

**Closed box testing of known vulnerability scanning**

**Software composition analysis of binary executable files**

**Static and dynamic code analysis, including testing for credentials that are “hardcoded,” default, easily guessed, and easily compromised**

## IEC 81001-5-1:2021

International standard that defines the cybersecurity components of a product lifecycle for “health software”

- “Software intended to be used specifically for managing, maintaining, or improving health of individual persons, or the delivery of care, or which has been developed for the purpose of being incorporated into a medical device”
- Software in a Medical Device (SiMD);
- Software as part of hardware specifically intended for health-related use;
- Software as a medical device (SaMD); and
- Software-only products for other health-related uses

## IEC 81001-5-1:2021 Framework

- IEC 81001-5-1 is not meant to be a complete standalone standard for developing a medical device cybersecurity program
  - 42 other standards cross-referenced for additional guidance
  - Including NIST SP800-30 Rev 1 (Risk Management)
- Based on IEC 62443 and IEC 62304
  - IEC 62443-4-1: Secure product development lifecycle requirements
    - Modified to account for factors unique to medical devices
  - IEC 62304 Medical device software — Software life cycle processes
- IEC 81001-5-1 only provides high-level requirements
  - References other standards for specific implementation details

# IEC 81001-5-1 Annexes

- Much of the ‘meat’ of 81001-5-1 is provided in the annexes
  - Annex A (informative) Rationale
  - Annex B (informative) Guidance on implementation of SECURITY LIFE CYCLE ACTIVITIES
  - **Annex C (informative) Threat modelling**
  - Annex D (informative) Relation to practices in IEC 62443-4-1:2018
  - Annex E (informative) Documents specified in IEC 62443-4-1
  - **Annex F (normative) Transitional health software**
  - Annex G (normative) Object identifiers

# IEC 81001-5-1 Sample Cross-References

## IEC 81001-5-1

IEC 62443-4-1

IEC 62304

### 4. General Requirements

- ISO 13485 - Quality Management
- Common Vulnerability Scoring System (CVSS)
- ISO 14971 Risk Mgt.
- ISO/TR 24971 Risk Mgt.

### 5. Software Development

- ISO 24765 Software Engineering
- IEC TR 60601-4-5 Security Specifications
- IEC 80001-2-2 Risk Management
- IEC 62304 Software Development

### 6. Software Maintenance

- IEC TR 60601-4-5 Security Specifications

### 7. Risk Management

- Common Vulnerability Scoring System (CVSS)
- MITRE scoring rubric for medical devices
- ISO 14971 Risk Mgt.
- ISO/IEC Guide 51

### 8. Configuration Management

- IEC 62304:2006\*

### 9. Problem Resolution

- ISO/IEC 29147 Vulnerability disclosure
- ISO 13485 - Quality Management
- ISO 14971 Risk Mgt.
- IEC 63069 Process Measurement

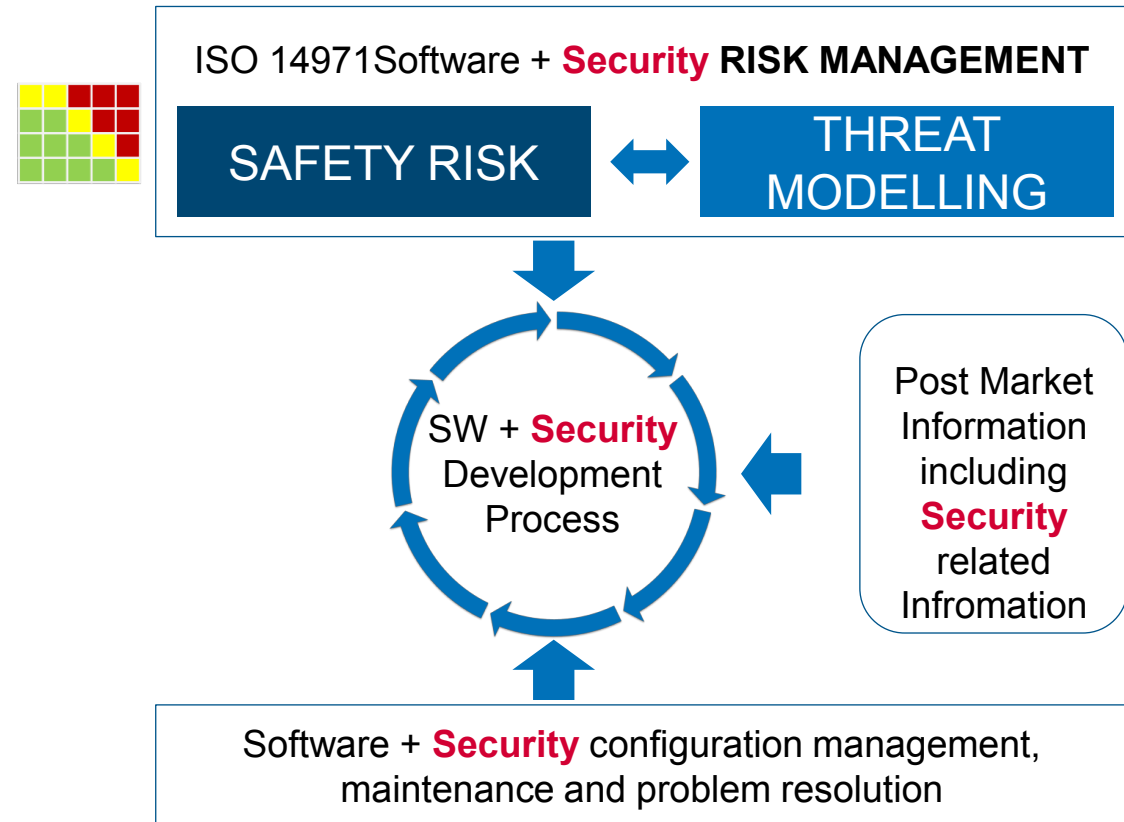
Product Lifecycle



# Security Life-Cycle

IEC 62304 Software Life Cycle & IEC 81001-5-1:2021 Security Product Life Cycle

- Documented security activities within Technical File to be present
- Security activity DOES NOT depend on safety classification of the medical device
- 3rd party software/hardware to be considered (**SBOM**)
- Development Environment Security & Secure Coding Standards

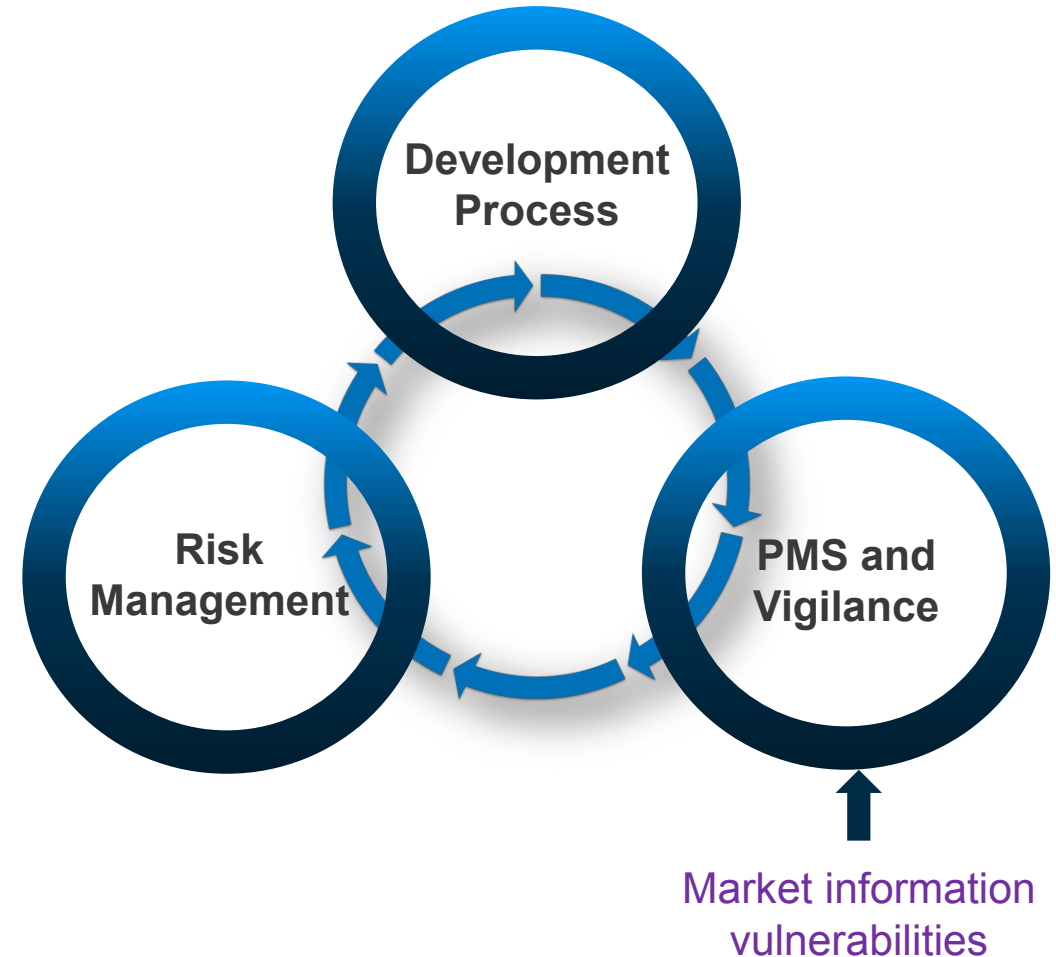


## Software problem resolution PROCESS (Section 9)

- Requirements for handling of reported/identified vulnerabilities and security issues
  - 9.2 Receiving notifications about VULNERABILITIES
  - 9.3 Reviewing VULNERABILITIES
  - 9.4 Analysing VULNERABILITIES
  - 9.5 Addressing SECURITY-related issues
- Emphasis is on post-market support, but the requirements also apply to the development process

# Post-Market Activities

- Vulnerability monitoring
  - NIST: National vulnerability database:  
<https://nvd.nist.gov/>
  - Common Vulnerability Database:  
<https://cve.org/index.html>
- Relevant Documents kept up-to-date, reviewed periodically and ensures state-of-the-art compliance
- Reporting adverse events



# What to do with LEGACY Software?

1. Re-develop the software implementing security activities, measures are considered
2. TRANSITIONAL HEALTH SOFTWARE\* conformance

## Security consideration:

- Security requirements analyzed (e.g threat modeling)
- Be tested for vulnerabilities (e.g penetration testing)
- Residual Security RISKS assessed and evaluated

## Security measures can include for example:

- Mandate compensating controls (e.g defence in depth)
- Update operation guidelines
- Etc.

*\*TRANSITIONAL HEALTH SOFTWARE: HEALTH SOFTWARE, which was released prior to publication of IEC 81001-5-1 and which does not meet all requirements specified in IEC 81001-5-1*

IEC 81001-5-1:2021 Annex F



# Threat Identification & Mitigation

# KEV

## Known Exploited Vulnerabilities

A	B	C	D	E	F	G	H	I	J	K
cveID	vendorProject	product	vulnerabilityName	dateAdded	shortDescription	requiredAction	dueDate	knownRansomware	notes	cwes
CVE-2023-0386	Linux	Kernel	Linux Kernel Improper Owner	6/17/2025	Linux Kernel contains	Apply mitigation	7/8/2025	Unknown	This vulner	CWE-282
CVE-2023-33538	TP-Link	Multiple Routers	TP-Link Multiple Routers Com	6/16/2025	TP-Link TL-WR940N	Apply mitigation	7/7/2025	Unknown	https://ww	CWE-77
CVE-2025-43200	Apple	Multiple Products	Apple Multiple Products Unsp	6/16/2025	Apple iOS, iPadOS, i	Apply mitigation	7/7/2025	Unknown	https://support.apple	
CVE-2025-33053	Microsoft	Windows	Microsoft Windows External	6/10/2025	Microsoft Windows c	Apply mitigation	7/1/2025	Unknown	https://msr	CWE-73

- <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>
- Subset of CVE(Common Vulnerabilities and Exposures)
- Maintained by CISA

### ❖ Characteristics

- Dynamic Updates
- Curated List
- Detailed information
- Global Relevance

### ❖ Limitations

- Retrospective Nature
- Potential Lag
- Not all Exploits Included
- Lack of Context

FREE CYBER SERVICES | SECURE BY DESIGN | SECURE OUR WORLD | SHIELDS UP | REPORT A CYBER ISSUE

**America's Cyber Defense Agency**  
NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

Search

Topics | Spotlight | Resources & Tools | News & Events | Careers | About

Home / Known Exploited Vulnerabilities Catalog

SHARE: Facebook | X | LinkedIn | Email

### Filters

What are you looking for?

Date Added (optional)

Sort by (optional)

Items per page (optional)

APPLY

## Known Exploited Vulnerabilities Catalog

For the benefit of the cybersecurity community and network defenders—and to help every organization better manage vulnerabilities and keep pace with threat activity—CISA maintains the authoritative source of vulnerabilities that have been exploited in the wild. Organizations should use the KEV catalog as an input to their vulnerability management prioritization framework.

[HOW TO USE THE KEV CATALOG](#)

The KEV catalog is also available in these formats:

- [CSV](#)
- [JSON](#)
- [JSON Schema \(updated 06-25-2024\)](#)
- [Print View](#)

# SBOM

## Mapping baseline components with SPDX and CycloneDX

- **Syft + Gype, CyconeDX CLI**
- **Black Duck, Synk, FOSSA**



Attribute	ISO/IEC 5962:2021	SPDX 3.0	CycloneDX v1.6 (ECMA-424)
SBOM Author Name	(6.8) Creator:	Core. <a href="#">CreationInfo.createdBy</a>	metadata.authors
SBOM Timestamp	(6.9) Created:	Core. <a href="#">CreationInfo.created</a>	metadata.timestamp
SBOM Type	(6.10) CreatorComment:	Software. <a href="#">Sbom.s bomType</a>	metadata.lifecycles
SBOM Primary Component	(11.1) Relationship: DESCRIBES	Software. <a href="#">Sbom.rootElement</a>	metadata.component
Component Name	(7.1) PackageName:	Software. <a href="#">Package.name</a>	components[].name
Component Version String	(7.3) PackageVersion:	Software. <a href="#">Package.packageVersion</a>	components[].version
Component Supplier Name	(7.5) PackageSupplier:	Software. <a href="#">Package.suppliedBy</a>	metadata.supplier components[].supplier



# SBOM

## CLI Example

### ➤ Syft + Grype, CyconeDX CLI

```
syft -o json debian:10 | jq '.artifacts[0].packages[0].vulnerabilities'
```

✓ Pulled image  
✓ Fetched image  
✓ Read image  
✓ Cataloged image [91 packages]

```
{
  "name": "grep",
  "version": "3.3-1",
  "type": "deb",
  "sources": [
    {
      "found-by": "dpkg-cataloger",
      "locations": [
        "/var/lib/dpkg/status"
      ]
    }
  ],
  "metadata": {
    "package": "grep",
    "source": "",
    "version": "3.3-1"
  }
}
```

```
pbok@DESKTOP-KPHV9RG:/mnt/c/Shared/test$ grype sbom:./test_sbom.json
✓ Scanned for vulnerabilities [0 vulnerability matches]
└─ by severity: 0 critical, 0 high, 0 medium, 0 low, 0 negligible
└─ by status: 0 fixed, 0 not-fixed, 0 ignored
No vulnerabilities found
```

```
pbok@DESKTOP-KPHV9RG:~$ grype sbom:./cyclonedx.json
✓ Scanned for vulnerabilities [70 vulnerability matches]
└─ by severity: 0 critical, 3 high, 15 medium, 5 low, 47 negligible
└─ by status: 0 fixed, 70 not-fixed, 0 ignored (1 dropped)
```

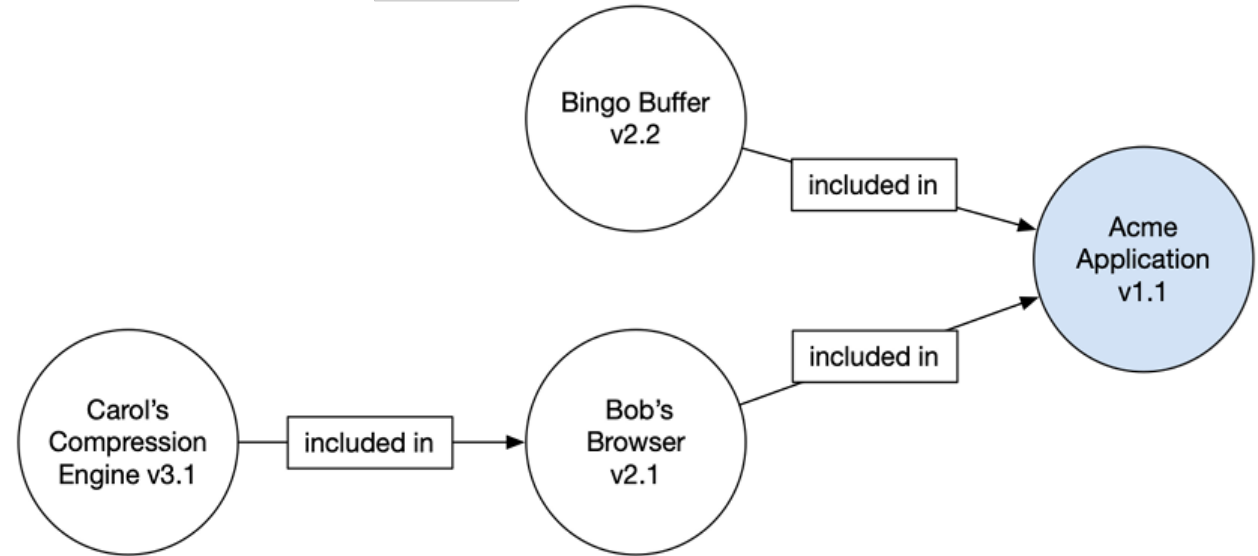
NAME	INSTALLED	FIXED-IN	TYPE	VULNERABILITY	SEVERITY
apt	2.6.1		deb	CVE-2011-3374	Negligible
bsdutils	1:2.38.1-5+deb12u3		deb	CVE-2022-0563	Negligible
coreutils	9.1-1	(won't fix)	deb	CVE-2016-2781	Low
coreutils	9.1-1		deb	CVE-2017-18018	Negligible
gcc-12-base	12.2.0-14		deb	CVE-2022-27943	Negligible
gcc-12-base	12.2.0-14		deb	CVE-2023-4039	Negligible
gpgv	2.2.40-1.1		deb	CVE-2022-3219	Negligible
libapt-pkg6.0	2.6.1		deb	CVE-2011-3374	Negligible
libblkid1	2.38.1-5+deb12u3		deb	CVE-2022-0563	Negligible
libc-bin	2.36-9+deb12u9	(won't fix)	deb	CVE-2025-0395	High
libc-bin	2.36-9+deb12u9		deb	CVE-2010-4756	Negligible
libc-bin	2.36-9+deb12u9		deb	CVE-2018-20796	Negligible
libc-bin	2.36-9+deb12u9		deb	CVE-2019-1010022	Negligible
libc-bin	2.36-9+deb12u9		deb	CVE-2019-1010023	Negligible
libc-bin	2.36-9+deb12u9		deb	CVE-2019-1010024	Negligible
libc-bin	2.36-9+deb12u9		deb	CVE-2019-1010025	Negligible
libc-bin	2.36-9+deb12u9		deb	CVE-2019-9192	Negligible
libc6	2.36-9+deb12u9	(won't fix)	deb	CVE-2025-0395	High
libc6	2.36-9+deb12u9		deb	CVE-2010-4756	Negligible
libc6	2.36-9+deb12u9		deb	CVE-2018-20796	Negligible
libc6	2.36-9+deb12u9		deb	CVE-2019-1010022	Negligible
libc6	2.36-9+deb12u9		deb	CVE-2019-1010023	Negligible
libc6	2.36-9+deb12u9		deb	CVE-2019-1010024	Negligible
libc6	2.36-9+deb12u9		deb	CVE-2019-1010025	Negligible

# SBOM – Additional information

## Target: Each Software Component

- The FDA states may be provided separately from the SBOM:
  - The software level of support from the component manufacturer(e.g., actively maintained, no longer maintained, etc.)
  - **The end-of-support date.**
- The FDA recommends manufacturers provide:
  - Safety and security **risk assessment** of each known vulnerability (including device and system impacts);
  - Details of applicable **safety and security risk controls to address the vulnerability.**
- **Automation**

Conceptual SBOM graph



Conceptual SBOM table

Component Name	Supplier	Version	Author	Hash	UID	Relationship
Application	Acme	1.1	Acme	0x123	234	Primary
--- Browser	Bob	2.1	Bob	0x223	334	Included in
--- Compression Engine	Carol	3.1	Acme	0x323	434	Included in
--- Buffer	Bingo	2.2	Acme	0x423	534	Included in

# CVSS

## Common Vulnerability Scoring System

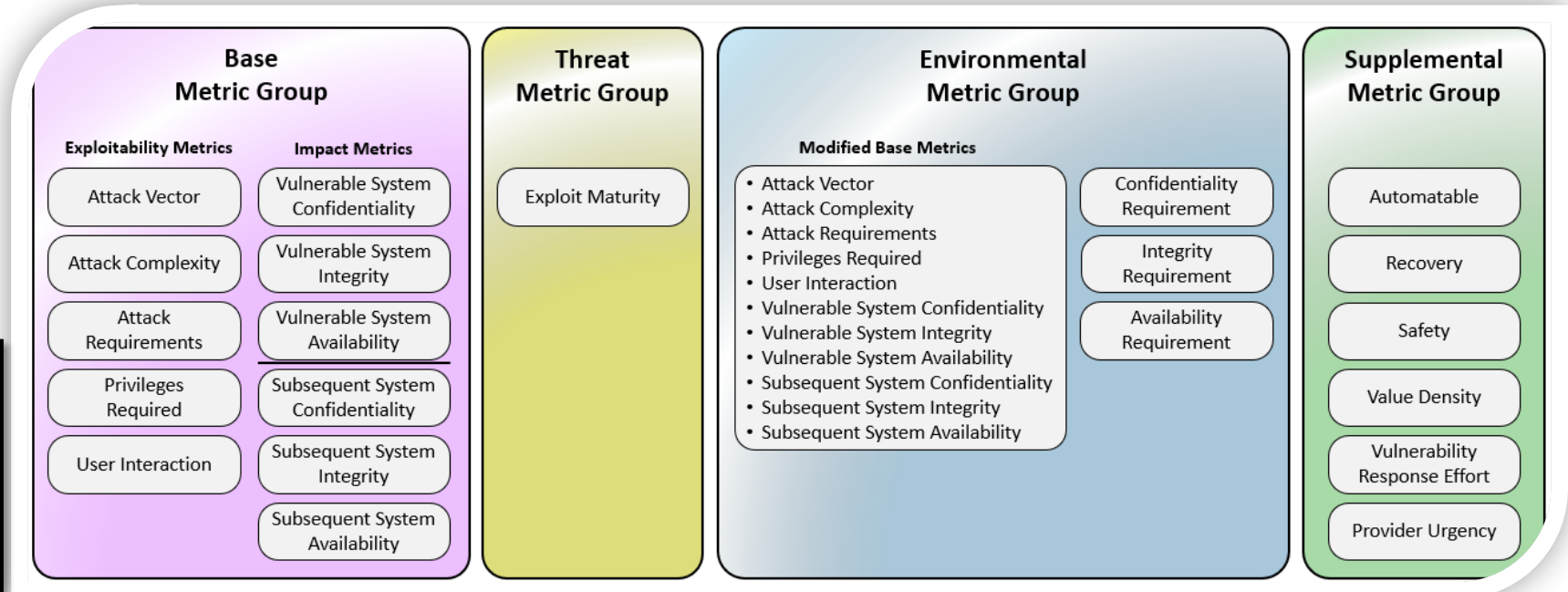
### Exploitability Metrics for V 3.1

- Attack Vector (AV)
- Attack Complexity(AC)
- Privileges Required(PR)
- User Interaction(UI)
- Scope (S)
- CIA

**Common Vulnerability Scoring System Version 3.1 Calculator**

기초 지표 기초 점수

공격 벡터 (AV)	범위 (S)
<input type="radio"/> 네트워크 (N) <input type="radio"/> 인접 네트워크 (A) <input type="radio"/> 로컬 (L)	<input type="radio"/> 변화 없음 (U) <input type="radio"/> 변화함 (C)
공격 복잡성 (AC)	기밀성 영향 (C)
<input type="radio"/> 낮음 (L) <input type="radio"/> 높음 (H)	<input type="radio"/> 없음 (N) <input type="radio"/> 낮음 (L) <input type="radio"/> 높음 (H)
요구 권한 (PR)	무결성 영향 (I)
<input type="radio"/> 없음 (N) <input type="radio"/> 낮음 (L) <input type="radio"/> 높음 (H)	<input type="radio"/> 없음 (N) <input type="radio"/> 낮음 (L) <input type="radio"/> 높음 (H)
사용자 참여 (UI)	가용성 영향 (A)
<input type="radio"/> 없음 (N) <input type="radio"/> 필요함 (R)	<input type="radio"/> 없음 (N) <input type="radio"/> 낮음 (L) <input type="radio"/> 높음 (H)



# CVSS

## Common Vulnerability Scoring System

### Rating Scale

- None
- Low: 0.1 ~ 3.9
- Medium: 4.0 ~ 6.9
- High: 7.0 ~ 8.9
- Critical: 9.0 ~ 10.0

Rating	CVSS Score
None	0.0
Low	0.1 - 3.9
Medium	4.0 - 6.9
High	7.0 - 8.9
Critical	9.0 - 10.0

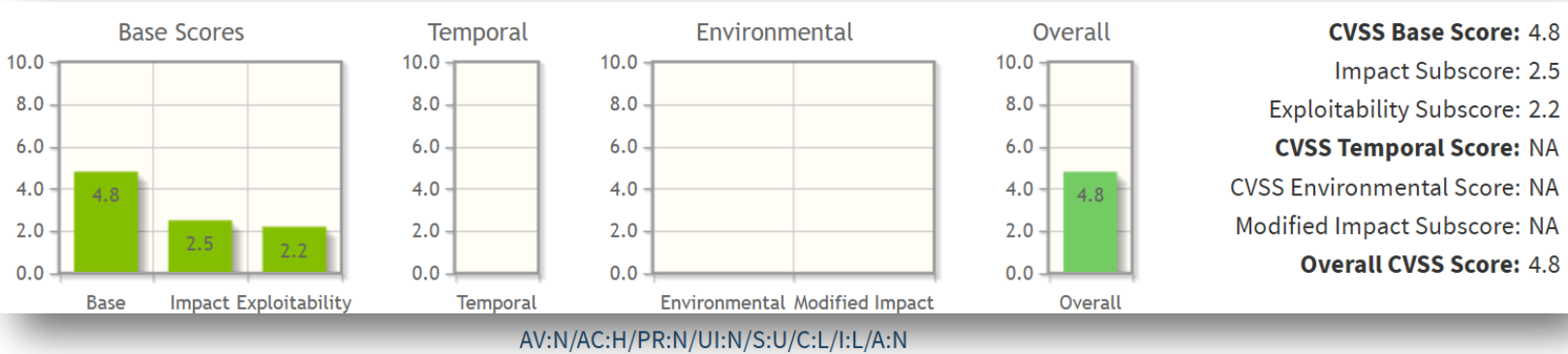
Metric	Metric Value	Numerical Value
Attack Vector / Modified Attack Vector	Network	0.85
	Adjacent	0.62
	Local	0.55
	Physical	0.2
Attack Complexity / Modified Attack Complexity	Low	0.77
	High	0.44
Privileges Required / Modified Privileges Required	None	0.85
	Low	0.62 (or 0.68 if Scope / Modified Scope is Changed)
	High	0.27 (or 0.5 if Scope / Modified Scope is Changed)
User Interaction / Modified User Interaction	None	0.85
	Required	0.62
Confidentiality / Integrity / Availability / Modified Confidentiality / Modified Integrity / Modified Availability	High	0.56
	Low	0.22
	None	0

# CVSS

## Common Vulnerability Scoring System

### Example: CVE-2023-4039

- Rating Scale
- CVE vs KEV



### Base Score Metrics

#### Exploitability Metrics

##### Attack Vector (AV)\*

**Network (AV:N)** Adjacent Network (AV:A) Local (AV:L) Physical (AV:P)

##### Attack Complexity (AC)\*

Low (AC:L) **High (AC:H)**

##### Privileges Required (PR)\*

**None (PR:N)** Low (PR:L) High (PR:H)

##### User Interaction (UI)\*

**None (UI:N)** Required (UI:R)

##### Scope (S)\*

**Unchanged (S:U)** Changed (S:C)

#### Impact Metrics

##### Confidentiality Impact (C)\*

None (C:N) **Low (C:L)** High (C:H)

##### Integrity Impact (I)\*

None (I:N) **Low (I:L)** High (I:H)

##### Availability Impact (A)\*

**None (A:N)** Low (A:L) High (A:H)

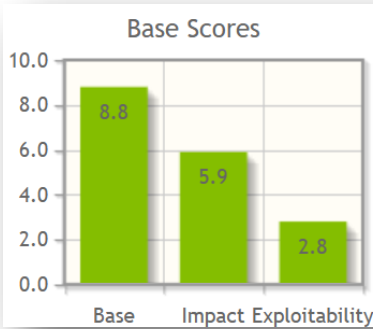
# CVSS

## Common Vulnerability Scoring System

### Example: CVE-2025-33053

- Rating Scale
- CVE vs KEV
- WebDAV—the Web Distributed Authoring and Versioning protocol
- Remote Code Execution

### Recommendations:



**This CVE is in CISA's Known Exploited Vulnerabilities Catalog**

Reference CISA's BOD 22-01 and Known Exploited Vulnerabilities Catalog for further guidance and requirements.

Vulnerability Name	Date Added	Due Date	Required Action
Microsoft Windows External Control of File Name or Path Vulnerability	06/10/2025	07/01/2025	Apply mitigations per vendor instructions, follow applicable BOD 22-01 guidance for cloud services, or discontinue use of the product if mitigations are unavailable.

CVSS Base Score: 8.8  
Impact Subscore: 5.9  
Exploitability Subscore: 2.8  
CVSS Temporal Score: NA  
CVSS Environmental Score: NA  
Modified Impact Subscore: NA  
Overall CVSS Score: 8.8

### Base Score Metrics

#### Exploitability Metrics

##### Attack Vector (AV)\*

**Network (AV:N)** Adjacent Network (AV:A) Local (AV:L) Physical (AV:P)

##### Attack Complexity (AC)\*

**Low (AC:L)** High (AC:H)

##### Privileges Required (PR)\*

**None (PR:N)** Low (PR:L) High (PR:H)

##### User Interaction (UI)\*

None (UI:N) **Required (UI:R)**

##### Scope (S)\*

**Unchanged (S:U)** Changed (S:C)

#### Impact Metrics

##### Confidentiality Impact (C)\*

None (C:N) Low (C:L) **High (C:H)**

##### Integrity Impact (I)\*

None (I:N) Low (I:L) **High (I:H)**

##### Availability Impact (A)\*

None (A:N) Low (A:L) **High (A:H)**



# CVSS

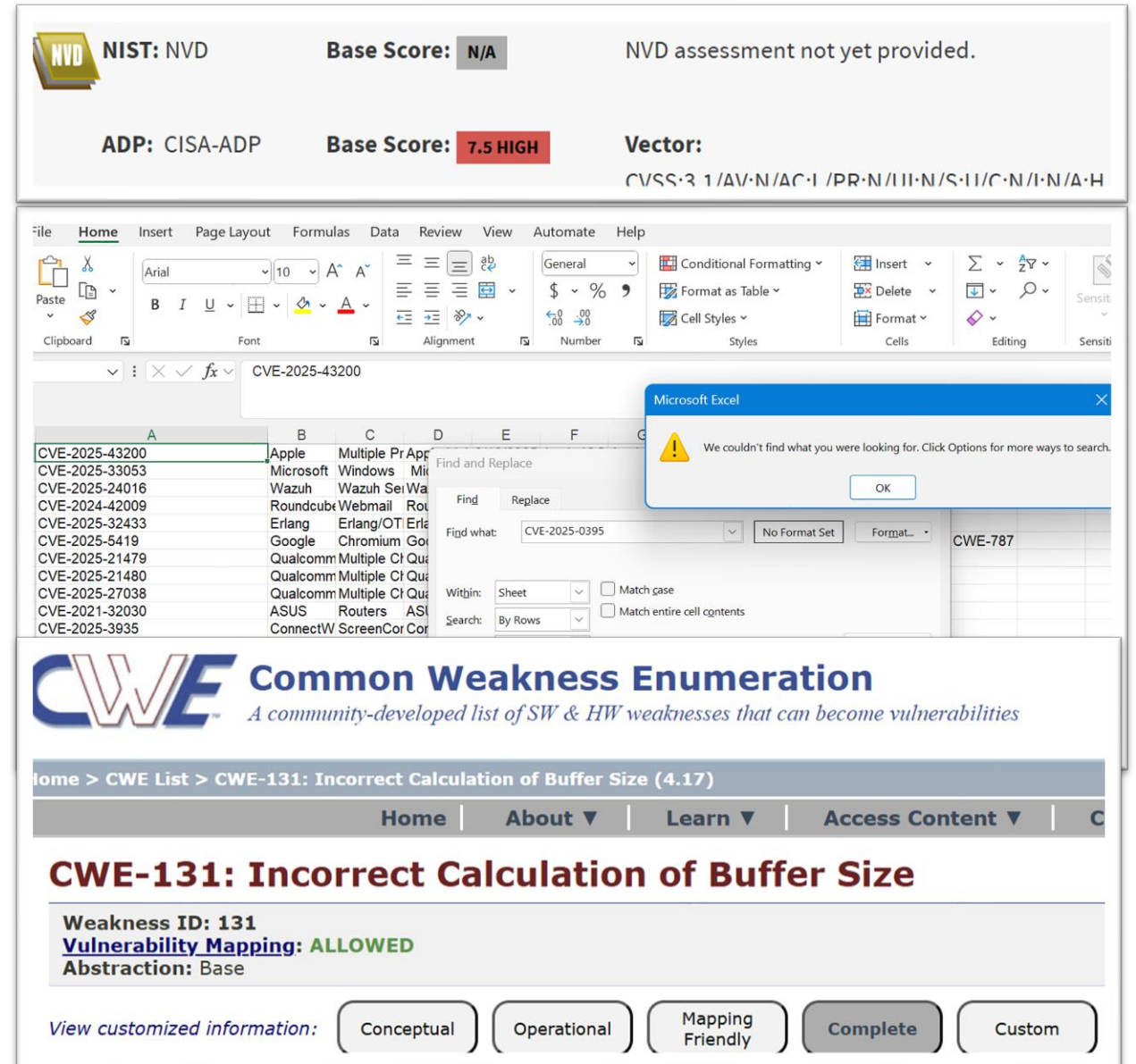
## Common Vulnerability Scoring System

### Example: CVE-2025-0395

- Rating Scale
- Buffer Overflow vulnerability in glibc version 2.13 to 2.40 fails (CWE-131)
- CVE? Or KEV? Why?

### Mitigation:

1. Patch your system accordingly
2. Impact Analysis
3. General Mitigation Strategies:
  - ✓ Least Privilege
  - ✓ Secure Baseline Configurations
  - ✓ Rigorous Testing: assert() or handle input from untrusted sources
  - ✓ Malicious Code Protections



The image shows two screenshots. The top screenshot is from the NIST National Vulnerability Database (NVD) for CVE-2025-0395. It displays a Base Score of 7.5 (HIGH) and a Vector string: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:II/C:N/I:N/A:H. The bottom screenshot is from the Common Weakness Enumeration (CWE) website, specifically the page for CWE-131: Incorrect Calculation of Buffer Size (4.17). It shows the weakness ID, a vulnerability mapping of 'ALLOWED', and an abstraction of 'Base'. Navigation buttons for 'Conceptual', 'Operational', 'Mapping Friendly', 'Complete', and 'Custom' are visible at the bottom.

**NIST: NVD** Base Score: **N/A** NVD assessment not yet provided.

**ADP: CISA-ADP** Base Score: **7.5 HIGH** Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:II/C:N/I:N/A:H

Microsoft Excel error message: We couldn't find what you were looking for. Click Options for more ways to search.

**CWE Common Weakness Enumeration**  
A community-developed list of SW & HW weaknesses that can become vulnerabilities

Home > CWE List > CWE-131: Incorrect Calculation of Buffer Size (4.17)

Home | About | Learn | Access Content

**CWE-131: Incorrect Calculation of Buffer Size**

Weakness ID: 131  
Vulnerability Mapping: **ALLOWED**  
Abstraction: Base

View customized information: Conceptual Operational Mapping Friendly **Complete** Custom



# Safety vs Security

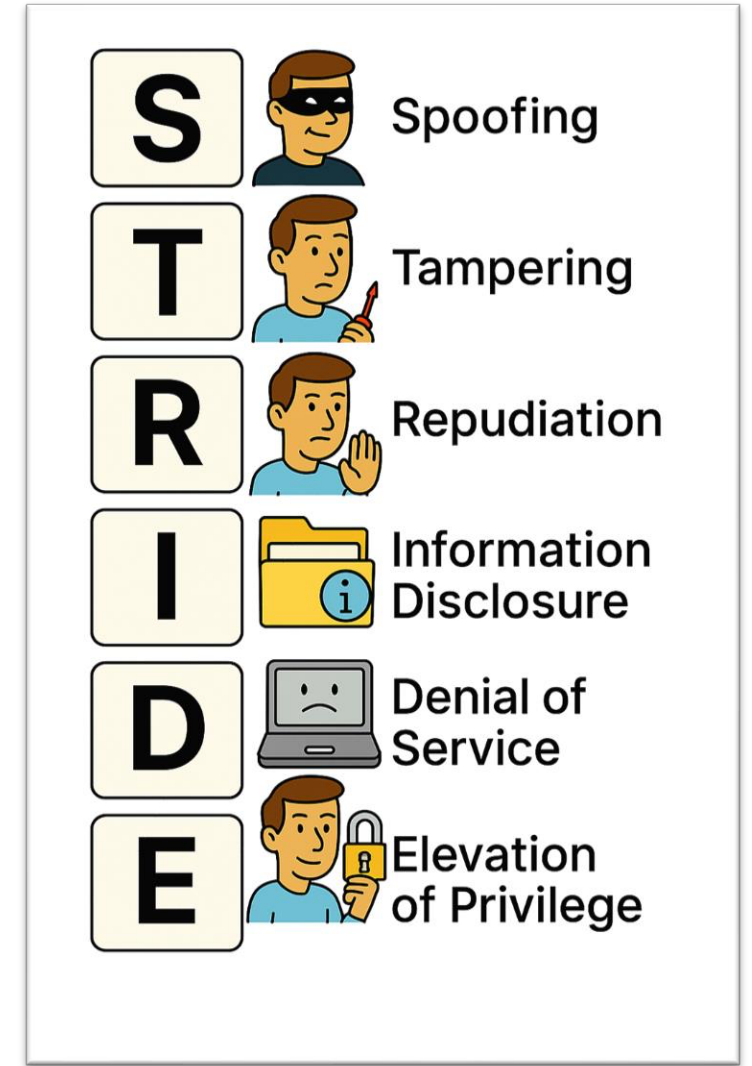
Safety risk management	Security risk management (Threat management)
Risk identification process Identify Safety Issues	Threat Modeling Identify software vulnerabilities
Risk Level Assignment (Severity x Occurrence Probability)	Vulnerability scoring: E.g: Common Vulnerability Scoring System (CVSS)
Risk mitigation E.g: Risk control measures	Threat mitigation E.g. Defense in depth, security control measures, coding
Residual Safety Risk evaluation E.g: Safety testing (IEC 60601-1)	Residual Vulnerability Risk evaluation E.g: Vulnerability testing, Penetration testing

# Threat Modeling

## STRIDE

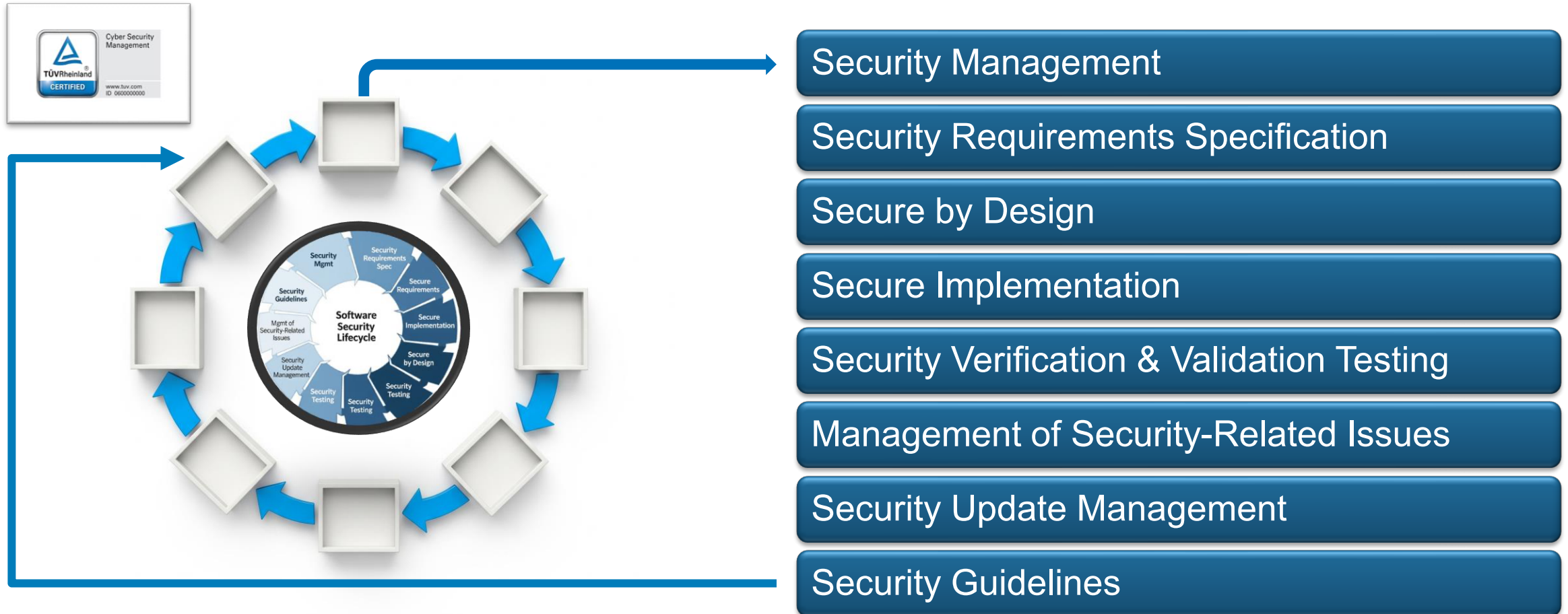
1. Spoofing
2. Tempering
3. Repudiation
4. Information Disclosure
5. Denial of Service
6. Elevation of Privilege

Violation ?



# Secure Development Lifecycle (SDL)

8 practices



# Secure Product Development: Security and Privacy by Design

Secure Guidelines Development helps organization to adopt processes that standardize security best practices across a range of products and/or applications

## Key Client Issues Addressed

- Lack of a standard approach to securing products and applications causes cybersecurity issues.
  - Without security requirements, architecture reviews and testing being integrated into the entire lifecycle of products and application development, there will be vulnerabilities and security weaknesses that need to be rectified after the products and applications are being shipped out to the market.
  - The triage and response needed to deal with these security issues would require additional costs, time and effort which can be prevented in the first place. As a result, developers spend too much time fixing code they wrote in the past and not enough focusing on the future.
- Unavailability of standard secure product development approach, developers tend to repeat the same security mistakes over and over again which further complicates debugging and security testing.
- Without a standard approach for secure product development, it is difficult for organizations to provide assurance to customers that the products and applications have been developed with security best practices in mind and can be systematically verified.

**A standardized secure development builds smarter code, safer products, and lasting trust**

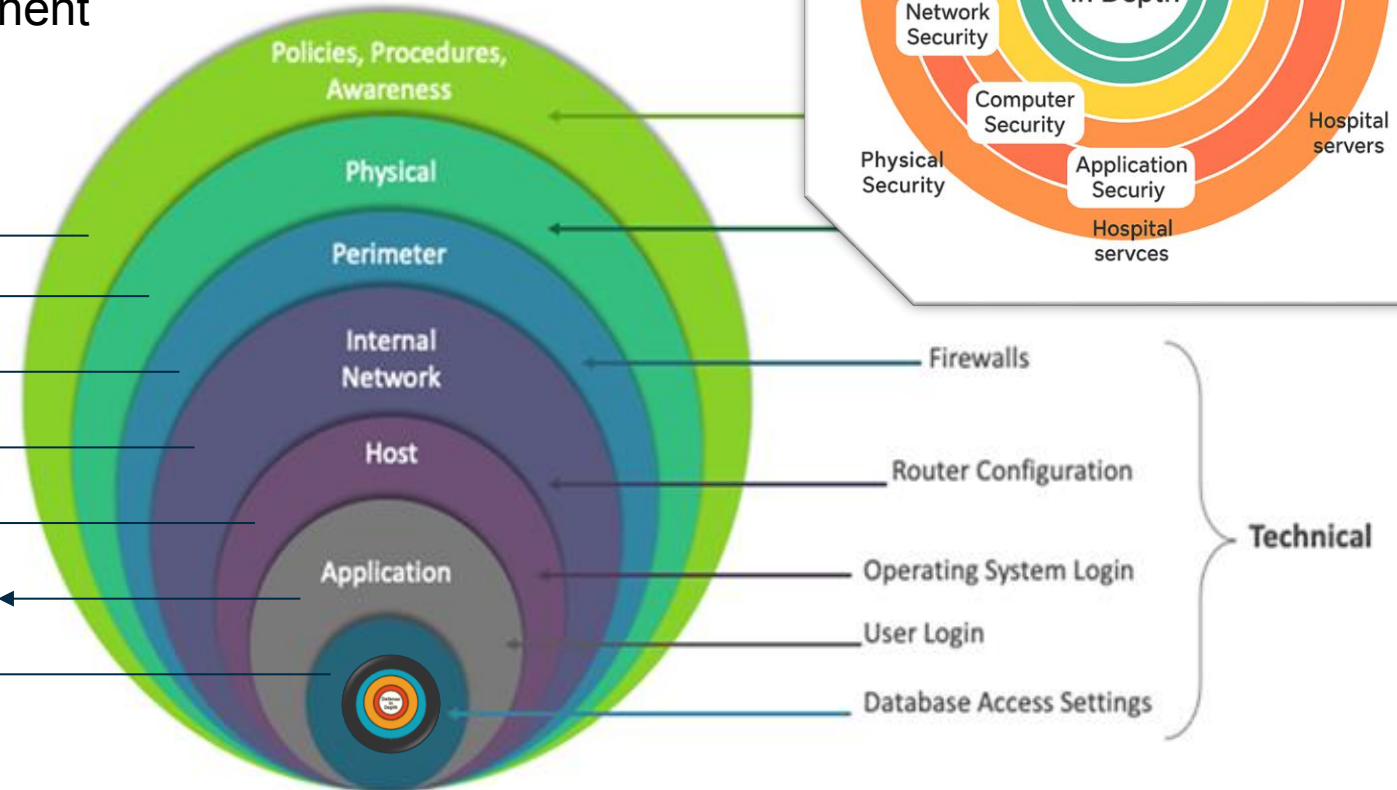
# Threat Mitigation

Secure by Design -> Defense-in-Depth

Building Security into each System Component

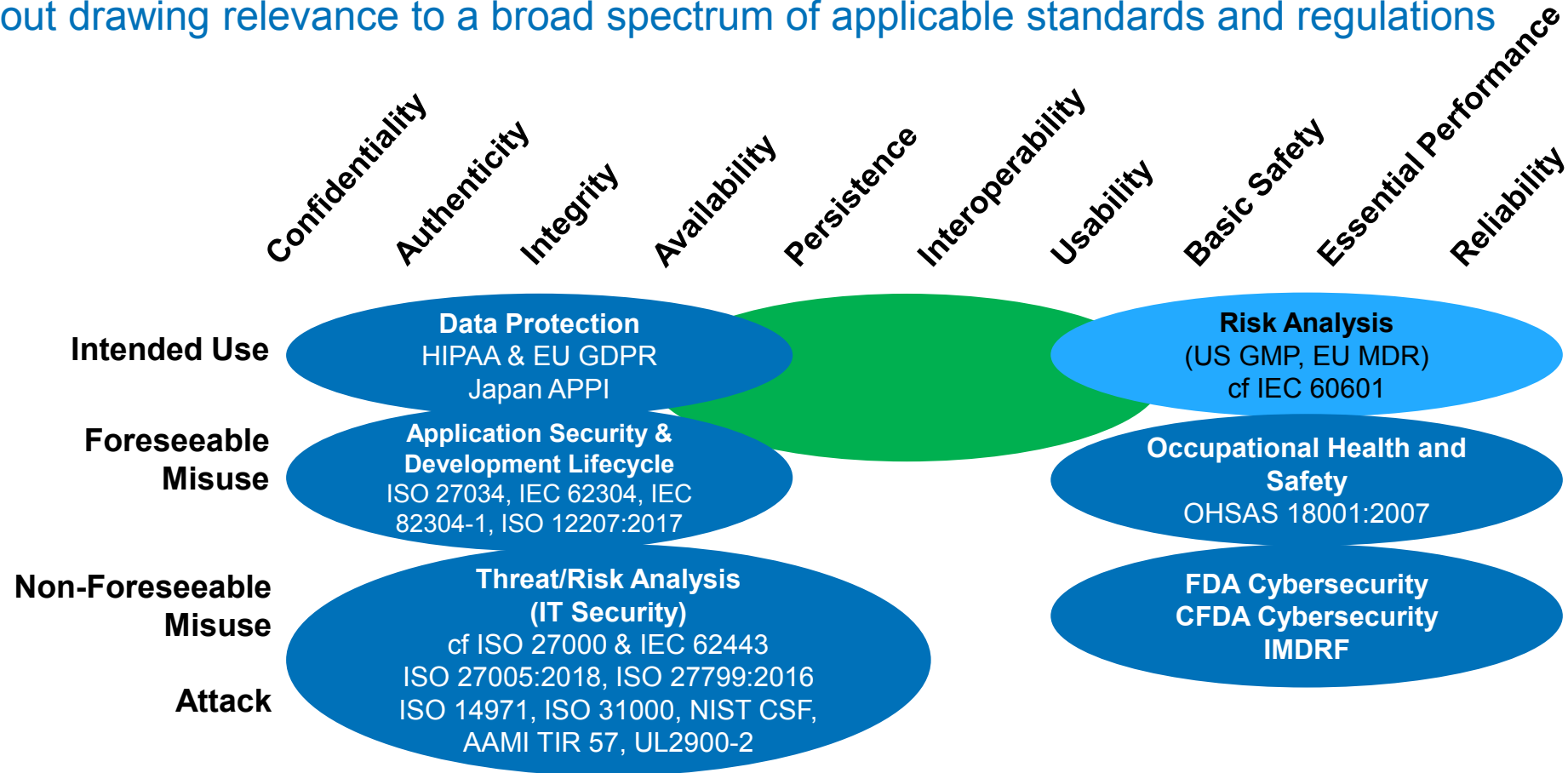
## ➤ 3Ps

- Perimeter Security
- Remote and 3<sup>rd</sup> Party Access
- Network Architecture
- Host OS & Removable Devices
- Applications
- Communications to Field Devices
- Local Field Controllers



# Testing and Assessment : Mapping Standards and Regulations

Emerging Standards and Regulations have specific areas of focus – but maintain cybersecurity hygiene is about drawing relevance to a broad spectrum of applicable standards and regulations





Q&A





<https://tinyurl.com/rate-event>

# Thank you!

If you have any questions or feedback, kindly  
contact [sfong@apacmed.org](mailto:sfong@apacmed.org) or  
[devya@apacmed.org](mailto:devya@apacmed.org)

