CYBERSEC 2025 臺灣資安大會 | 4/15 - 4/17 臺北南港展覽二館

SECURE SOFTWARE & DEVSECOPS FORUM

Regulated Software Threat Modeling

A Practical Walk-Through

Renaud Sauvain

Software Engineering Director @West Pharmaceutical Inc.

CISSP | CSSLP | CCSP | PMP

About

- **Decades of IoT development**
- **Last 5 years in the pharma industry**
- **Challenges of sustainable security compliance**

Disclaimer

This talk shares personal experience and practical insights from working with threat modeling in regulated environments, and does not represent regulatory or legal advice in any way. Always align with your organization’s policy and compliance requirements.

CYBERSEC 2025
臺灣資安大會

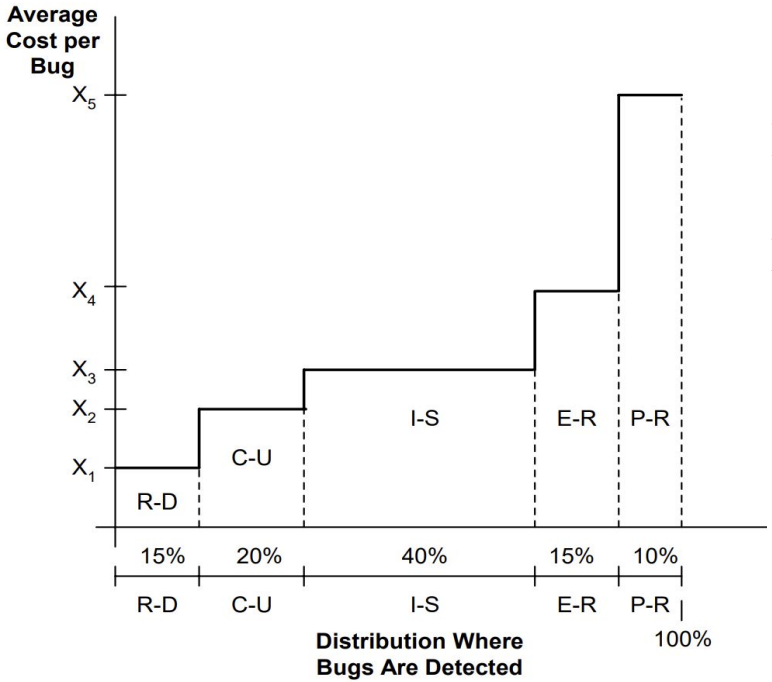
Agenda

1. **Context**
   The Stakes and Landscape
2. **SDLC Process Integration**
   The Risk Team & Activities
3. **Breaking Down the Problem**
   Discovery & Identification
4. **Actionable Risk Management**
   Assessing, Controlling & Scaling Up

① Context

The Stakes and Landscape

Objectives of Threat Modeling



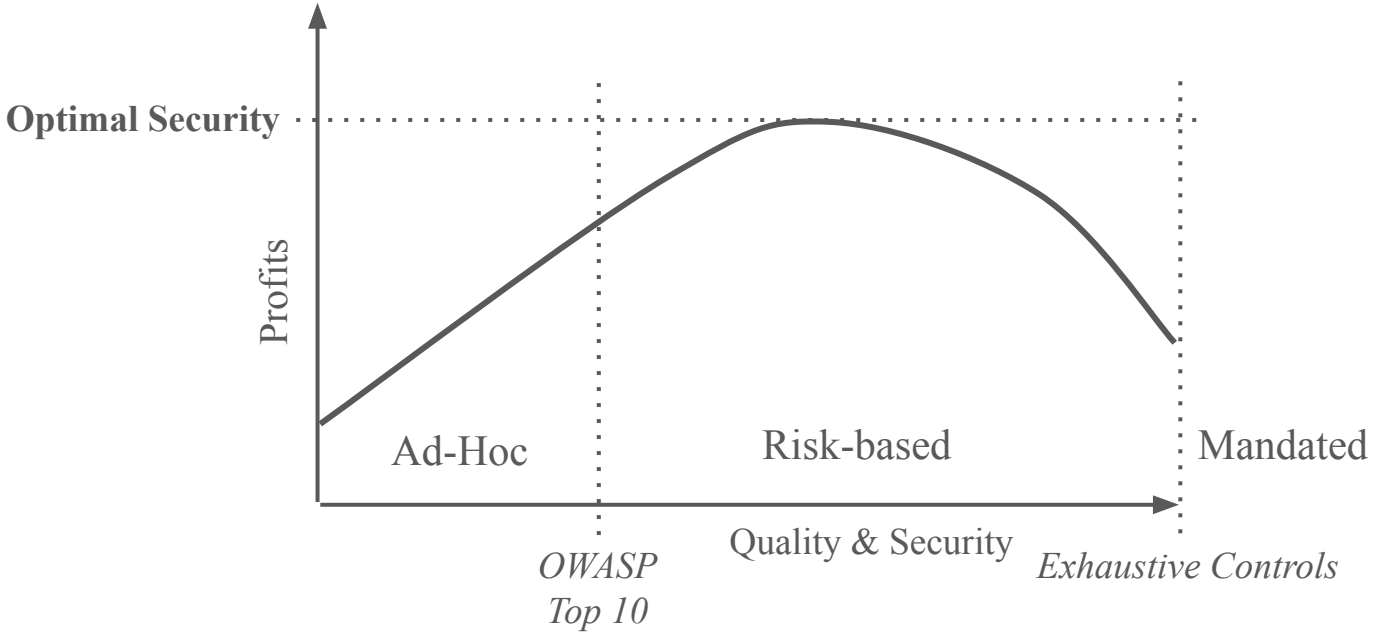
Build Secure Products

Reduce cost:

1. Limit security incidents
2. Shift security left
3. Prioritize effort

Source: NIST Economic Impacts of Inadequate Infrastructure for Software Testing

Objectives of Threat Modeling

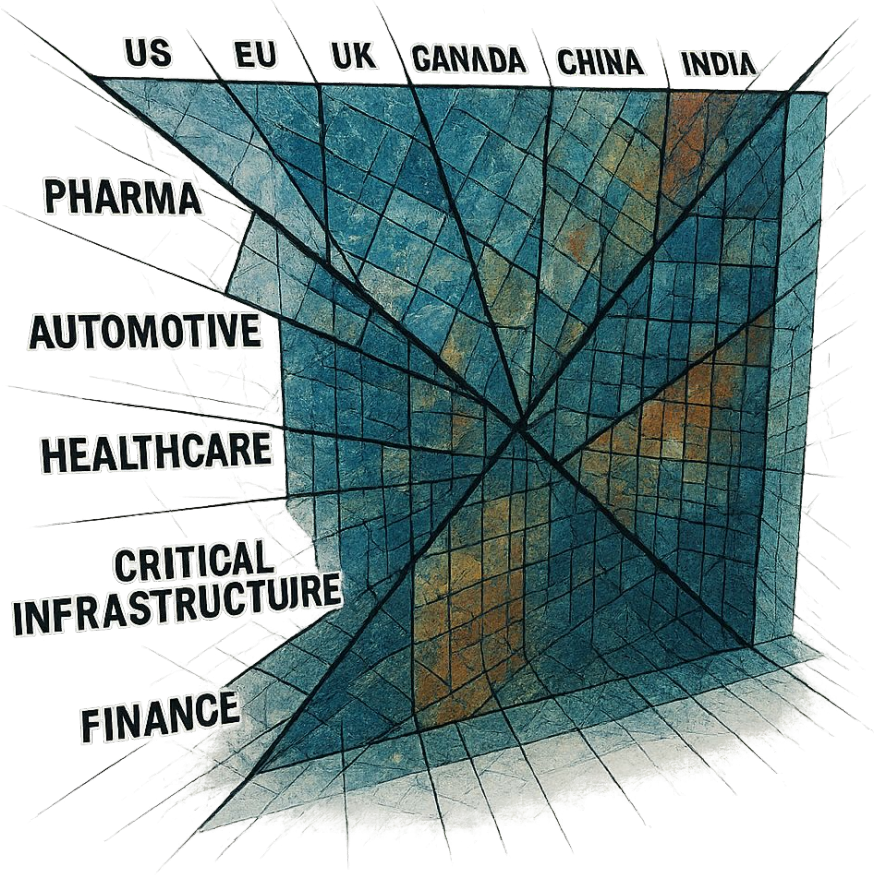


Derived from: NIST Economic Impacts of Inadequate Infrastructure for Software Testing

Objectives of Threat Modeling

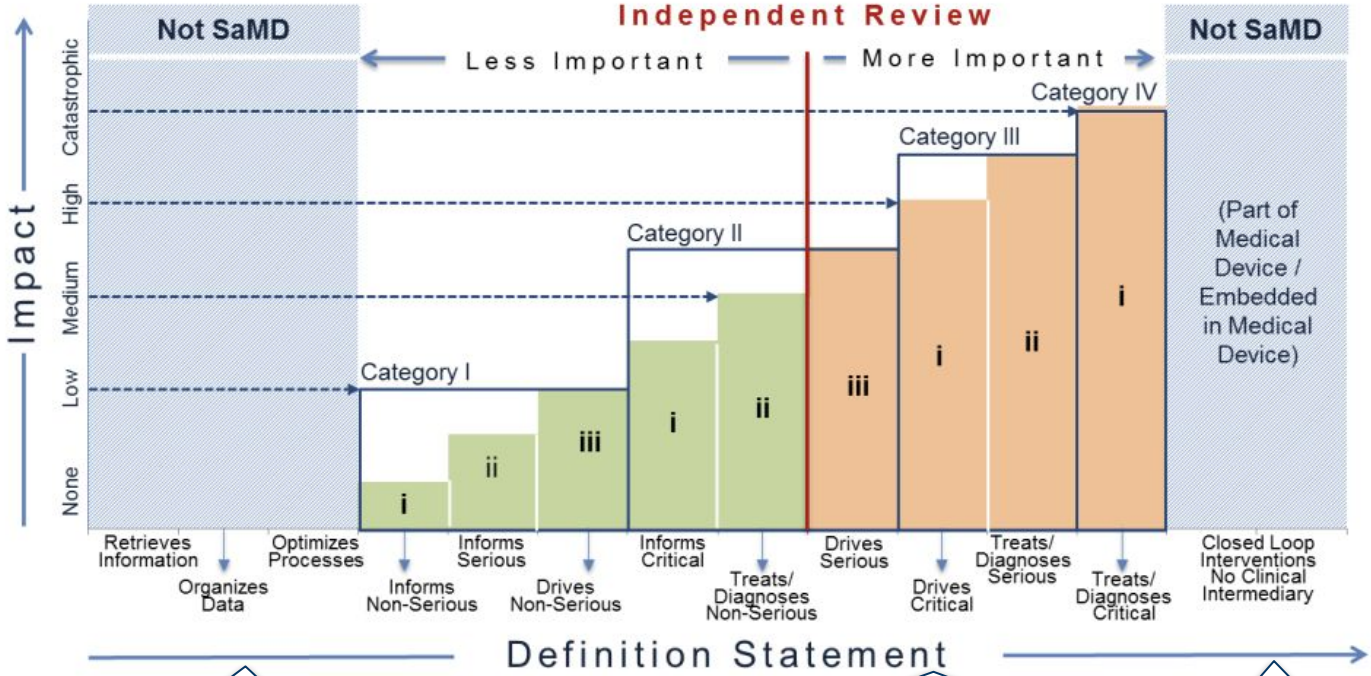
Derived from: NIST Economic Impacts of Inadequate Infrastructure for Software Testing

Fragmented Regulated Landscape



- Scattered Requirements & Terminology
- Detailed *What*, limited *How*

Fragmented Regulated Landscape: Within the same space



*Source: FDA SaMD Clinical Evaluation

Some References

	Industry	NIST	Standards	Industrial Standards	Healthcare Standards	Healthcare US
SSDLC	OWASP SAMM Microsoft SDL	SSDF SP 800-218	ISO/IEC 27034	ISO/IEC 62443-4-1	HSCC JSP	FDA SPDF
Risk Mgr.		SP 800-30 (System)	ISO/IEC 27005 (System)	ISO/IEC 62443-3-2	ISO 14971 (Safety) IEC 81001-5-2 (Security)	AAMI TIR57 FDA Cybersecurity in Medical Devices
Threat modeling	OWASP Threat Modeling Cheat Sheet CSA Cloud Threat Modeling Guide Microsoft SDL Threat Modeling Manifesto (2020)	SP 800-154 (Data centric) Cybersecurity White Paper 35				MITRE Playbook for Threat Modeling Medical Devices

② SDLC Process Integration

The Risk Team & Activities

Step 1. Assemble your risk team

Cross-functional experts

- SMEs
- Tech Lead
- Security
- IT/DevOps
- Business Analyst
- Product owner
- Quality Assurance (QA)
- ..

Step 1. Assemble your risk team

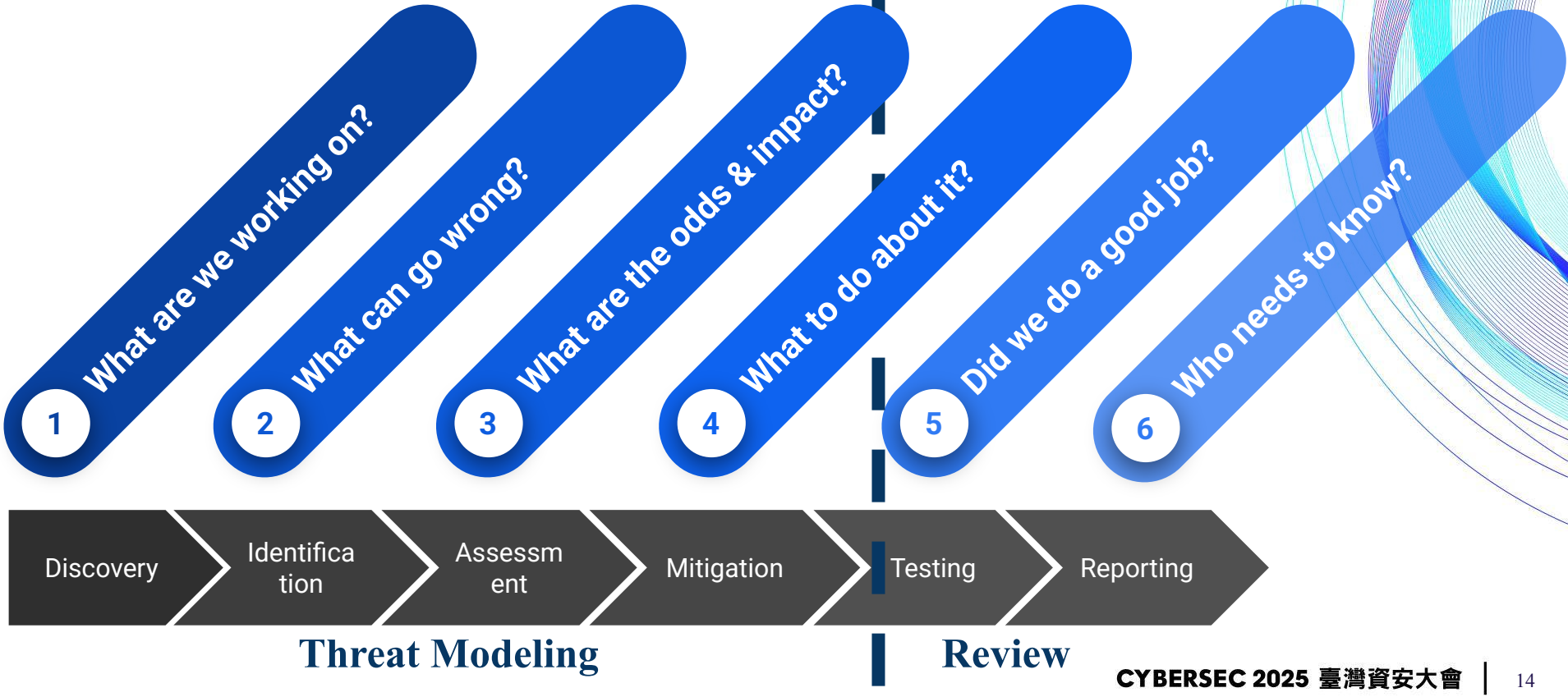
Cross-functional experts

- SMEs
- Tech Lead
- Security
- IT/DevOps
- Business Analyst
- Product owner
- Quality Assurance (QA)
- ..

Trained on

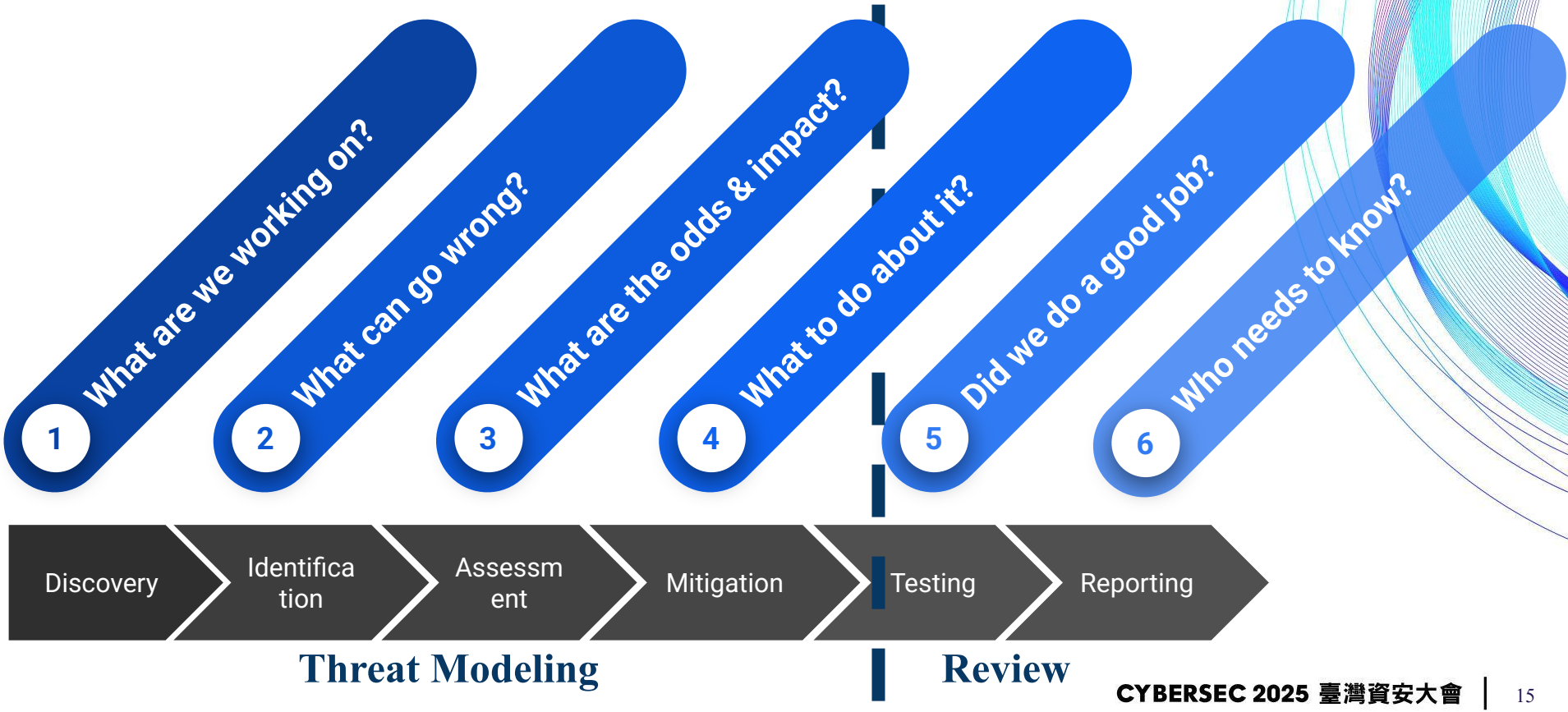
- Product requirements, architecture, ..
- Standards (eg. ISO-14971)

Step 2. Analysis: The Key Questions



Step 2. Analysis: The Key Questions

Prepare for Effective Brainstorming



Step 2. Analysis: Example

Case-study: Minimalist Web-service

- Web-Server
- Database

Failure Mode & Effect Analysis table (simplified)

Item	Failure	Effect	Severity	Occurence	Risk Priority	Control	Testing	Residual Risk
Server	💬							
DB								

Threat Modeling

Step 2. Analysis: Example

Case-study: Minimalist Web-service

- Web-Server
- Database

Failure Mode & Effect Analysis table (simplified)

Item	Failure	Effect	Severity	Occurence	Risk Priority	Control	Testing	Residual Risk
Server	XSS	Data leaked	Medium	Low	**Medium**	Input Validation		
DB								

Threat Modeling

Step 2. Analysis: Example

Case-study: Minimalist Web-service

- Web-Server
- Database

Failure Mode & Effect Analysis table (simplified)

Item	Failure	Effect	Severity	Occurence	Risk Priority	Control	Testing	Residual Risk
Server	XSS	Data leaked	Medium	Low	**Medium**	Input Validation		
DB	SQL Injection	Data corrupted	High	Low	**Medium**	Prepared Statement		

Discovery → Identification → Assessment → Mitigation → Testing → Reporting

Threat Modeling

Step 2. Analysis: Example

Case-study: Minimalist Web-service

- Web-Server
- Database

Failure Mode & Effect Analysis table (simplified)

Item	Failure	Effect	Severity	Occurence	Risk Priority	Control	Testing	Residual Risk
Server	XSS	Data leaked	Medium	Low	**Medium**	Input Validation	Pass	**Low**
DB	SQL Injection	Data corrupted	High	Low	**Medium**	Prepared Statement	Pass	**Low**

Discovery → Identification → Assessment → Mitigation → Testing → Reporting

Review

Step 3. Document

Case-study: Minimalist Web-service

- Web-Server
- Database

Failure Mode & Effect Analysis table (simplified)

Item	Failure	Effect	Severity	Occurence	Risk Priority	Control	Testing	Res Ri
Server	XSS	Data leaked	Medium	Low	**Medium**	Input Validation	Pass	
DB	SQL Injection	Data corrupted	High	Low	**Medium**	Prepared Statement	Pass	Lo

GDP

Governance

Accountability

Traceability

Review/Approval

Revision/History

Discovery → Identification → Assessment → Mitigation → Testing → Reporting

Review

Step 4. Reassessment

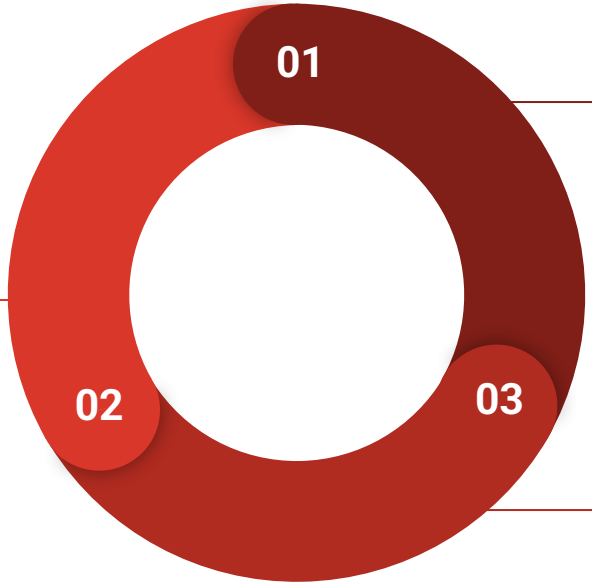
Details might not be known at first!

Refine & iterate!

A. Update the design until consensus

B. Upon changes (new version)

C. Regular interval



Requirements

To control risk

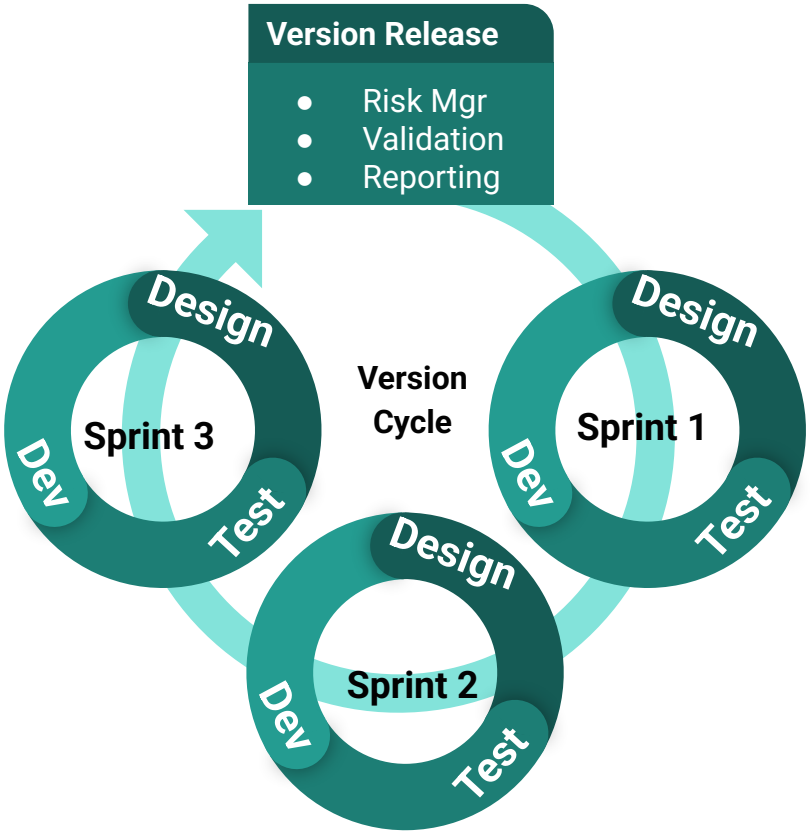
Design

Created from requirements

Risk Management

Based on design

Step 4. Continuous – Agile Risk Mgr.

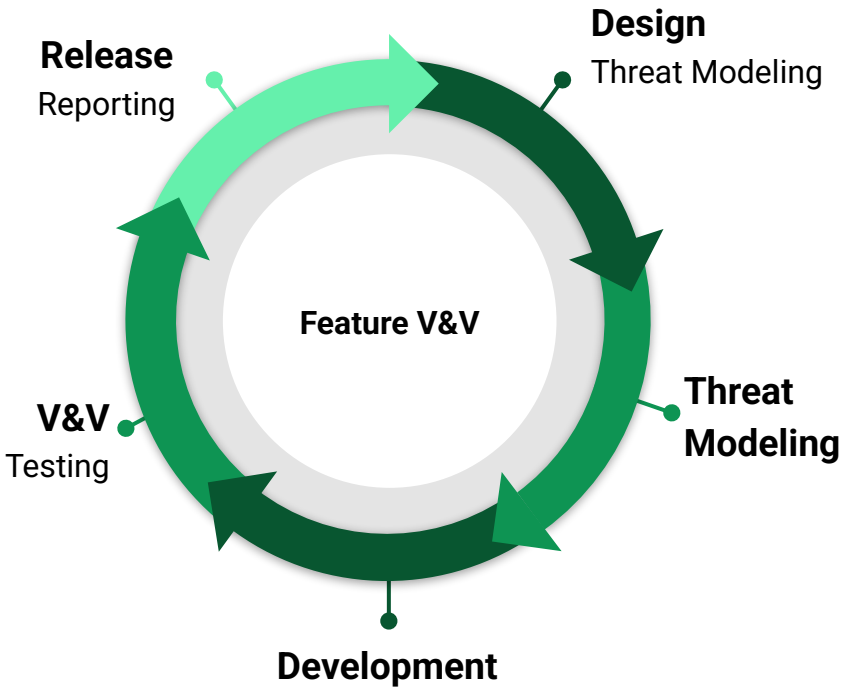


Option 1.

Agile iterations within

a Spiral of validated versions.

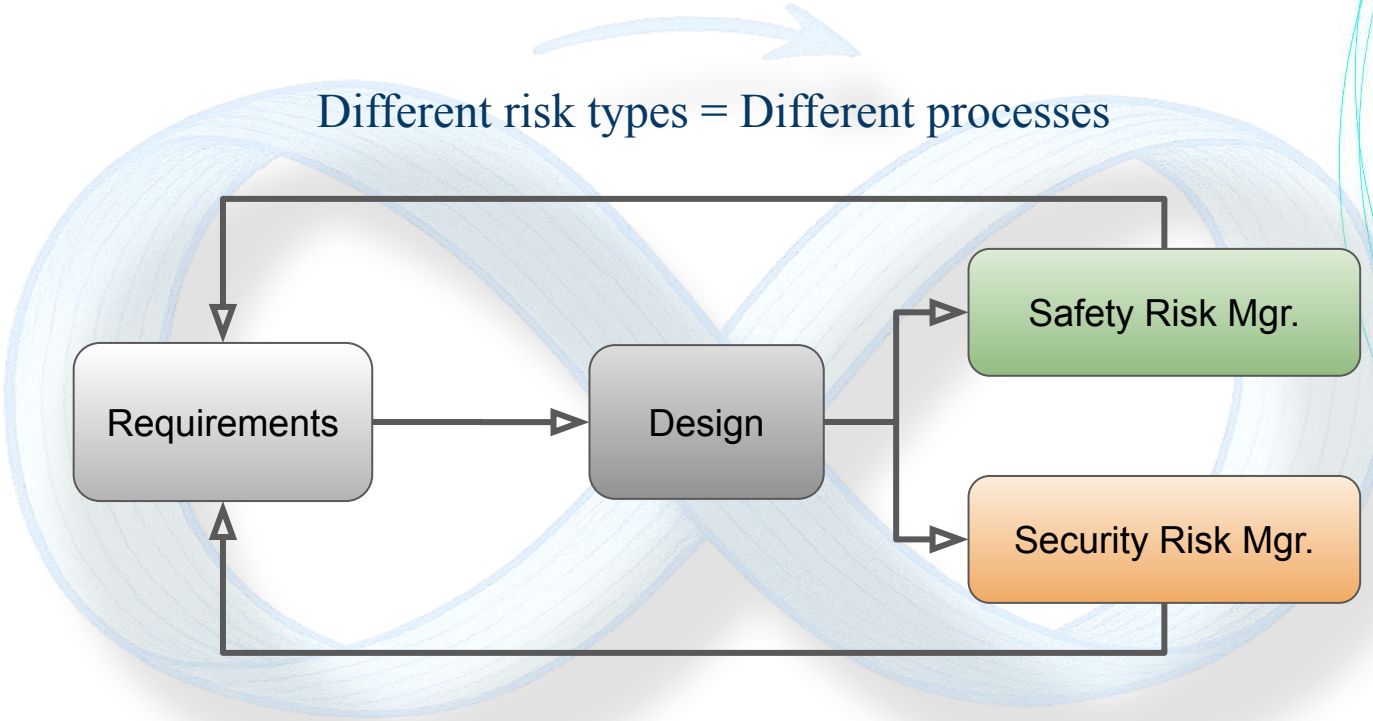
Step 4. Continuous – Agile Risk Mgr.



Option 2.

Validate features independently.

Step 4. Reassessment^2



”Safety and security risk management are distinct but connected”

– FDA Cybersecurity in Medical Devices / AAMI TIR96

Step 4. Reality Check

Here is our risk list!

RA: Ok.. is it exhaustive?

Yes our team is great!

RA: Well, prove it to an auditor!

"A device should be designed to mitigate vulnerabilities… Rationale for the methodology(ies) selected should be provided with the threat modeling documentation."

– FDA Cybersecurity in Medical Devices

Step 4. Reality Check

Here is our risk list!

RA: Ok.. is it exhaustive?

Yes our team is great!

RA: Well, prove it to an auditor!

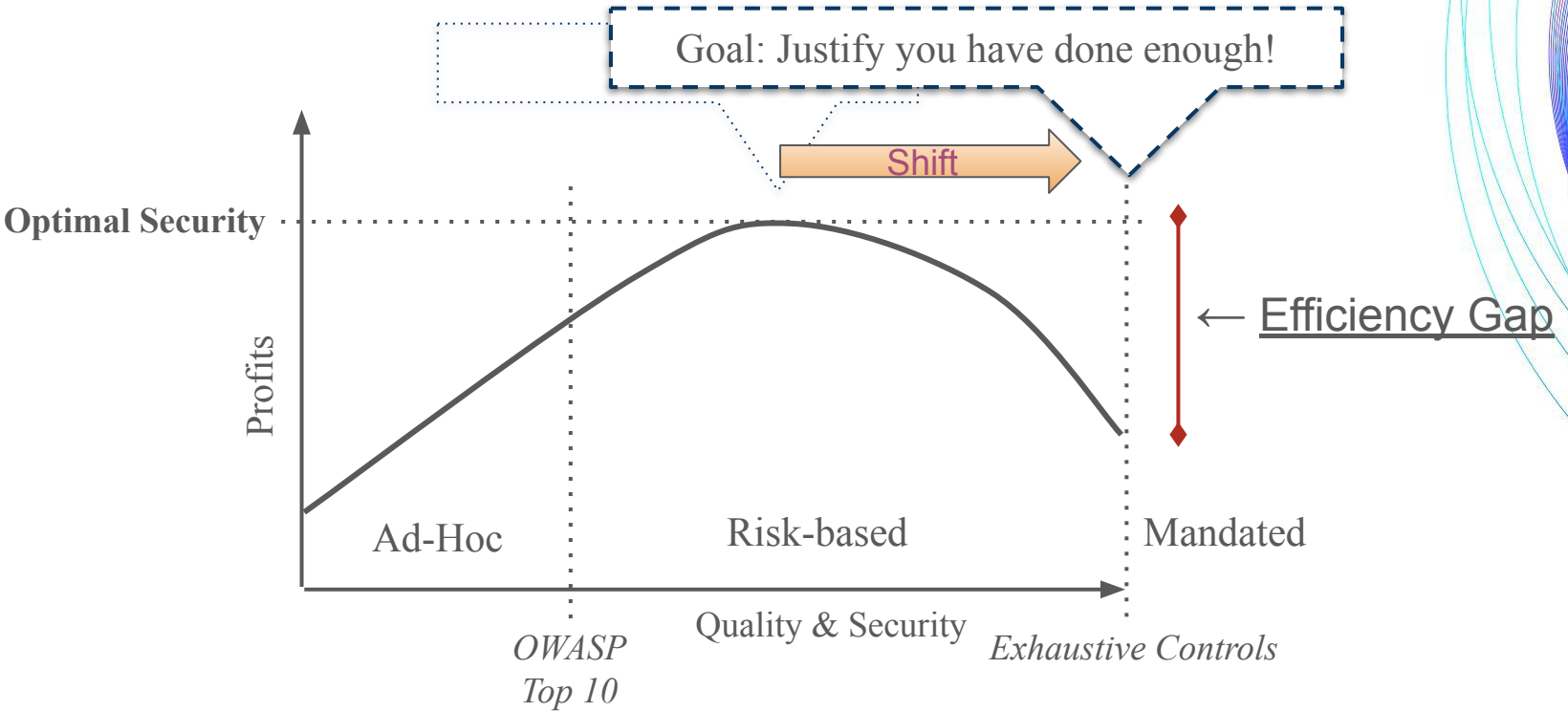
How are we supposed to do that?

"A device should be designed to mitigate vulnerabilities… Rationale for the methodology(ies) selected should be provided with the threat modeling documentation."

– FDA Cybersecurity in Medical Devices

Objectives of Threat Modeling

"Threat model supports establishing confidence that a software is fit for its intended use."
– FDA Cybersecurity in Medical Devices



Derived from: NIST Economic Impacts of Inadequate Infrastructure for Software Testing

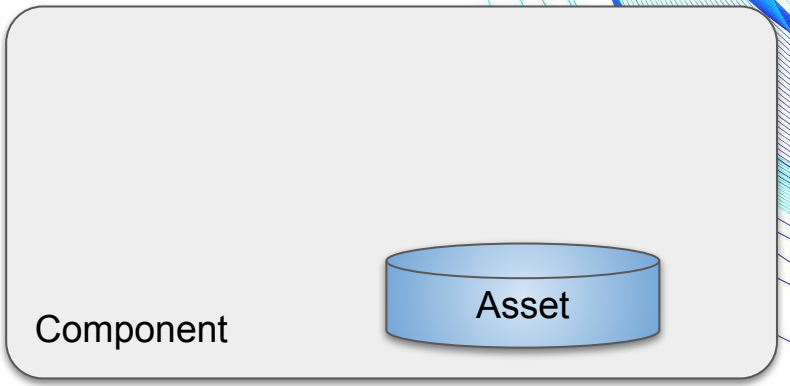
③ Breaking Down the Problem

Discovery & Identification

- OWASP Threat Modeling Cheat Sheet cheatsheetseries.owasp.org
- Microsoft Learn Create a Threat Model with DFDs learn.microsoft.com
- MITRE Playbook for Threat Modeling Medical Devices mitre.org

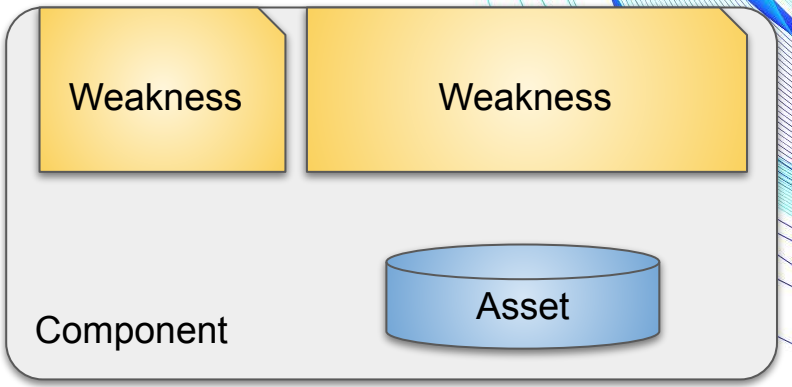
Terms

- **Asset** — Valuable data, or functionality
- **Component** — Software handling the asset



Terms

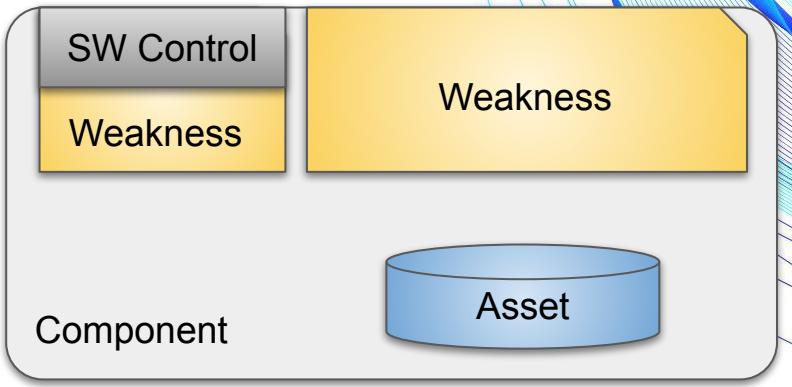
- Asset — Valuable data, or functionality
- Component — Software handling the Asset
- **Weakness** — Flaw in the handling of the Asset



*Typically found after release

Terms

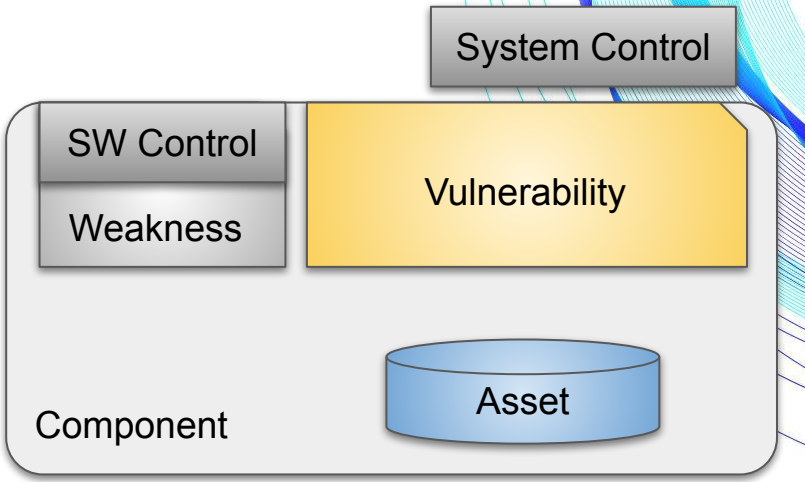
- Asset — Valuable data, or functionality
- Component — Software handling the Asset
- Weakness — Flaw in the handling of the Asset
- **Control** — Prevent Exploitability of a Weakness



*Typically found after release

Terms

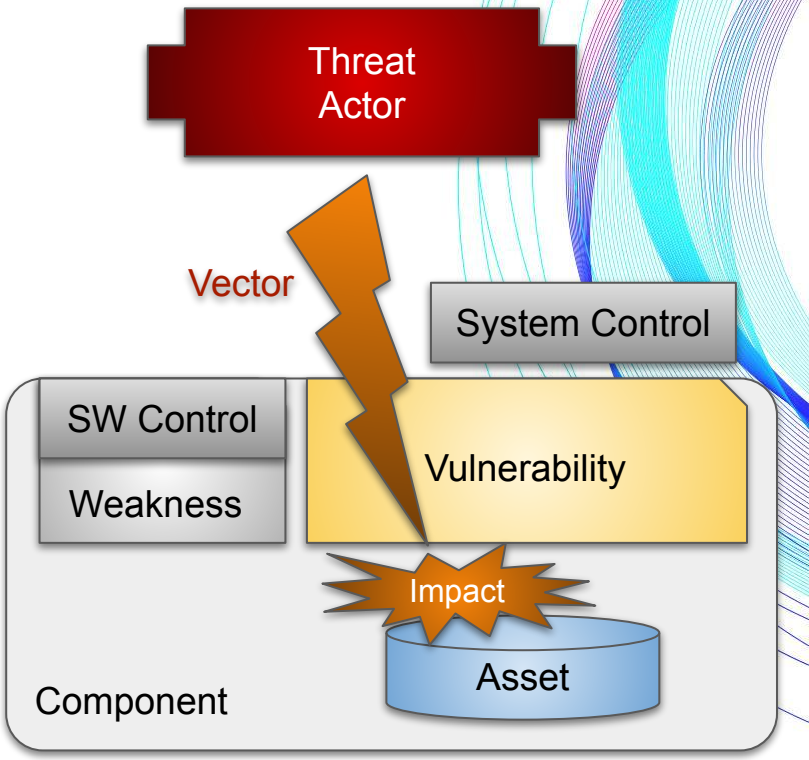
- Asset — Valuable data, or functionality
- Component — Software handling the Asset
- Weakness — Flaw in the handling of the Asset
- Control — Prevent Exploitability of a Weakness
- **Vulnerability** — Weakness that can be exploited*
- **Exploitability** — Ease of using a Vulnerability



*Typically found after release

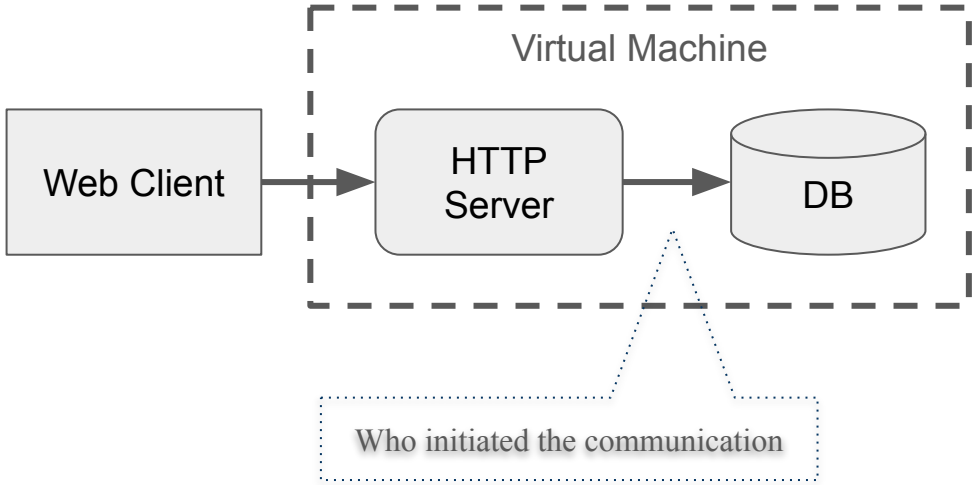
Terms

- Asset — Valuable data, or functionality
- Component — Software handling the Asset
- Weakness — Flaw in the handling of the Asset
- Control — Prevent Exploitability of a Weakness
- Vulnerability — Weakness that can be exploited*
- Exploitability — Ease of using a Vulnerability
- **Threat** — Event that could cause negative impact
- **Actor/Agent** — Entity causing the Threat
- **Vector** — The pathway to exploit a Vulnerability
- **Impact** — Severity of loss or damage done to an Asset
- **Risk** — The potential (probability & impact) of a Threat

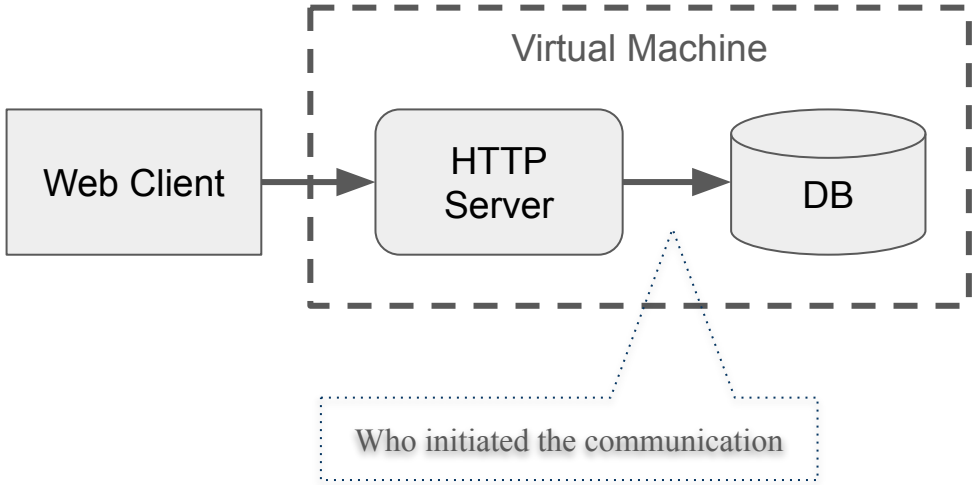


*Typically found after release

Discovery – Decomposition [Data-Flow-Diagram]

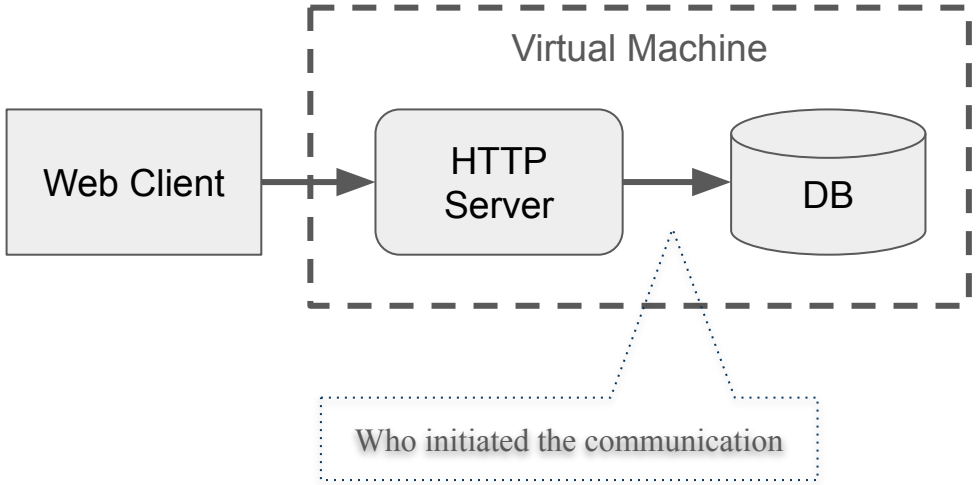


Discovery – Decomposition [Data-Flow-Diagram]



- Must be Print-safe (no color dependency)
- Don’t forget implicit behaviors (e.g. cache/temporary folder)

Discovery – Decomposition [Data-Flow-Diagram]

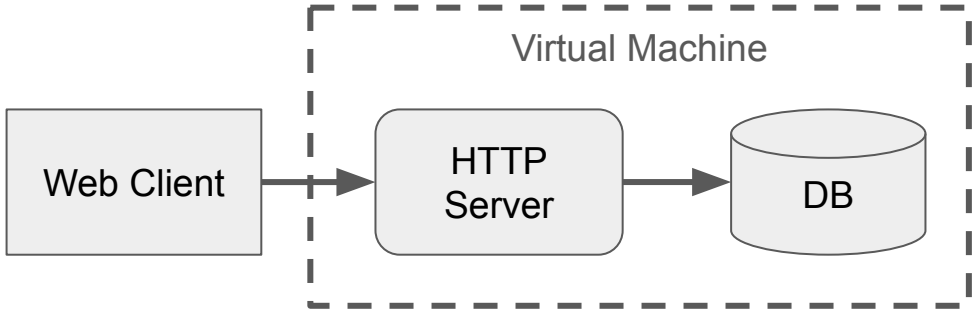


Supplements:

- Sequence
- State diagrams
- System deployment
- Backup flow

- Must be Print-safe (no color dependency)
- Don’t forget implicit behaviors (e.g. cache/temporary folder)

Discovery – Decomposition [Components list]



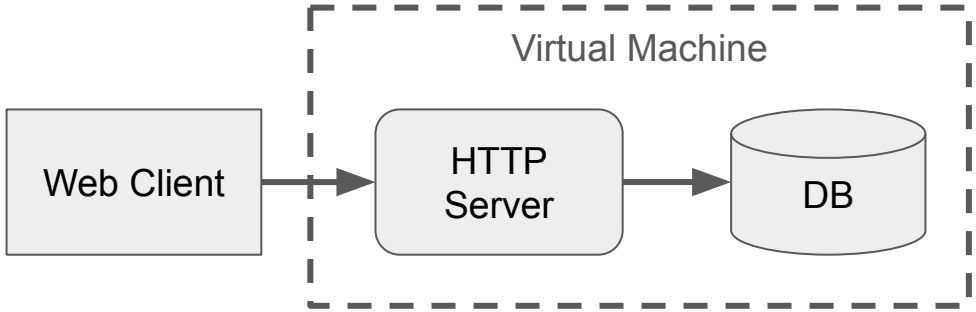
- Behavior -> Attack Surface

  Client/Server/Processor/Scheduler/UI/..
- Asset based criticality

  PHI/PII/Credentials/..
- Technology used

ID	Type	Criticality	Technology	Behavior
Server	Process	PII	Elixir	Server + Client
UserApp	External	PII	Javascript	Client
DB	DataStore	PII	MySQL	Server + FileSystem

Discovery – Decomposition [Components list]




```
Assets:
  -   id: userData
      classification: [PII]
      criticality: {C:H,I:M,A:L}
Components:
  -   id: server
      type: Process
      Technologies: Elixir
      behaviors:
            - type: Inbound
              technology: HTTP
              cross-boundary: true
              relates: userApp
              assets: [userData]
            - ..
  -   id: userApp
      ..
```

Machine-Formats:

- More complete that tables
- Independent from design (& tool)
- Better: Integration with CICD pipeline

STRIDE Analysis

	Spoofing	Tampering	Repudiation	Information disclosure	Denial of service	Elevation of privilege
DFD \ CIA	Authentication	Integrity	Integrity	Confidentiality	Availability	Authorization
Data flow		✔		✔	✔	
Data store		✔		✔	✔	
Process (Software)	✔	✔	✔	✔	✔	✔
External	✔		✔			

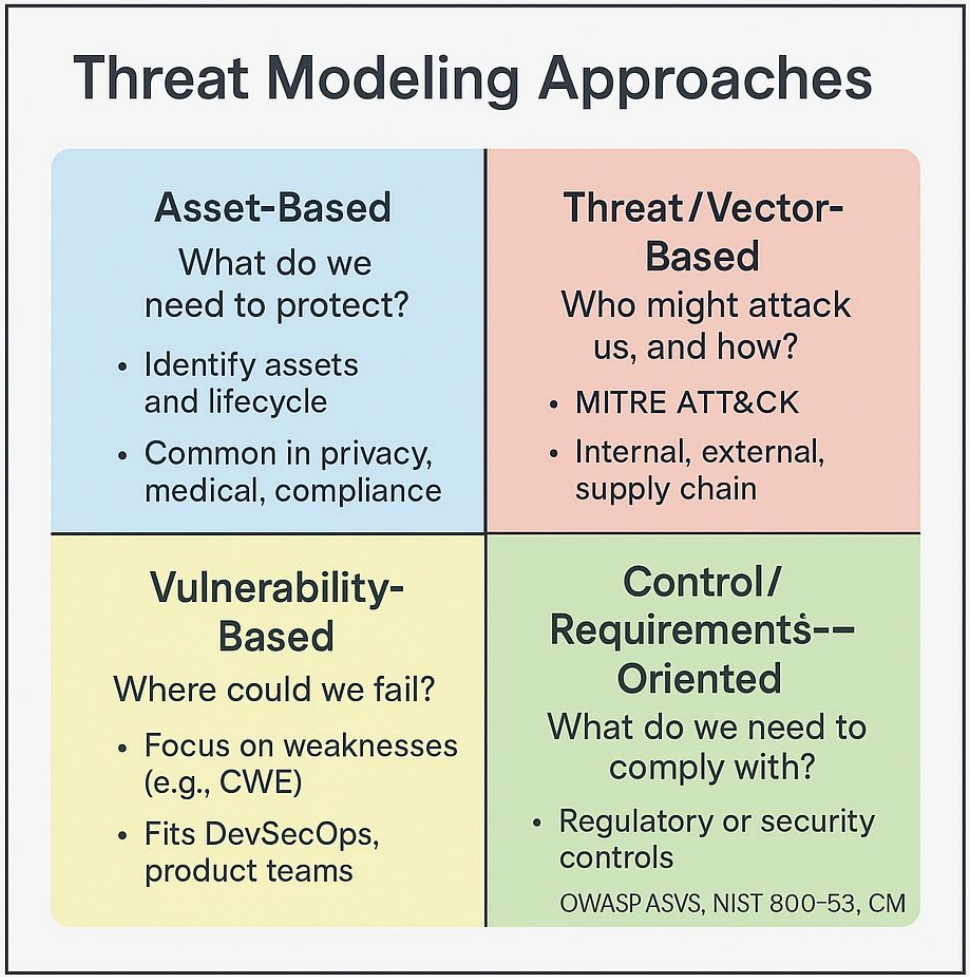
Limitations 💬

STRIDE Analysis

	Spoofing	Tampering	Repudiation	Information disclosure	Denial of service	Elevation of privilege
DFD \ CIA	Authentication	Integrity	Integrity	Confidentiality	Availability	Authorization
Data flow		✔		✔	✔	
Data store		✔		✔	✔	
Process (Software)	✔	✔	✔	✔	✔	✔
External	✔		✔			

Limitations

- Not exhaustive
- Multiple threats per type
- Software components are affected by all



Identification

Weakness (CWE)

→ Development

Vulnerability (CVE)

→ After release (System)

Vulnerability perspective for software

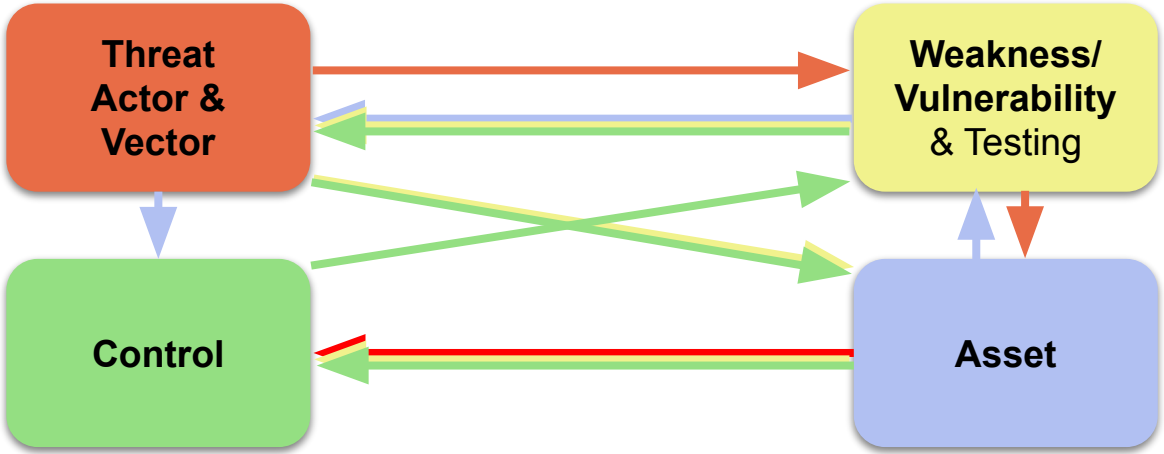
- HSCC Joint Security Plan
- FDA Cybersecurity in Medical Devices
- NIST CSF [ID.RA]

Identification – Justify coverage with Knowledge Bases

Knowledge Bases	Scope	Attacks	Weaknesses	Assets	Controls	Links to
MITRE ATT&CK	System	✔		✔	Partial	IEC 62443/NIST SP 800-53/CWE/CVE
MITRE DEFEND	System				✔	ATT&CK
MITRE CAPEC	Software/System	✔				CWE/[ATT&CK/WASC/OWASP]
MITRE CWE	Software		✔		Partial	CAPEC/CVE/[OWASP/WASC]
WASC Threat Class	Web Software	✔	✔			
OWASP	Web Software	✔	✔		Partial	
OWASP ASVS	Web Software				✔	CWE/NIST SP 800-63
CSA CCM	Web Software				✔	NIST SP 800-53 & Standards (ISO)
NIST SP 800-63	Digital Identity				✔	
NIST SP 800-53	System				✔	
IEC 62443-4-2	Software/System				✔	NIST SP 800-53

- Review availability of linkage, scoping details & machine-readable format for your needs.
- Justify your selection using component properties from the DFD (e.g technology)

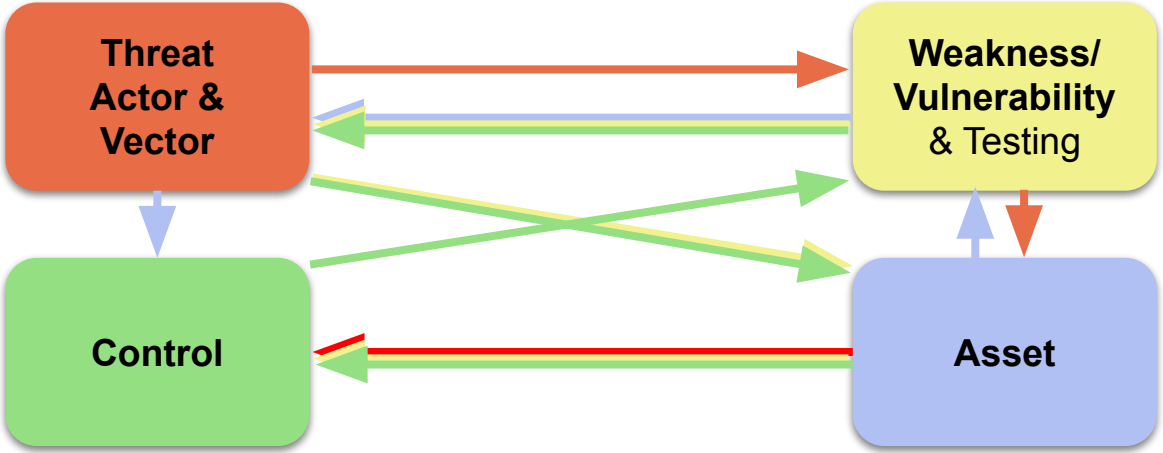
Identification – Build a threat profile



Risk ID	Description	Component ID	Asset ID	Weakness	Threats (CAPEC)	Controls (ASVS v4)
Server-79	XSS	Server	userData	CWE-79	63,85,591,592,588,209	1.4.3, 5.1.1, 5.1.2, 5.1.3, 5.1.4, 5.3.3, 5.3.4, 6.2.1
DB-564	SQL Injection	DB	userData	CWE-564	109	5.3.4

Goal: Fuel the risk assessment

Identification – Build a threat profile



Keep space for human insight!

Risk ID	Description	Component ID	Asset ID	Weakness	Threats (CAPEC)	Controls (ASVS v4)
Server-79	XSS	Server	userData	CWE-79	63,85,591,592,588,209	1.4.3, 5.1.1, 5.1.2, 5.1.3, 5.1.4, 5.3.3, 5.3.4, 6.2.1
DB-564	SQL Injection	DB	userData	CWE-564	109	5.3.4

Goal: Fuel the risk assessment

Consideration – Threat Actors

Casual	Uses known vulnerabilities
Professional	Derives vulnerabilities from common weaknesses
Persistent/State	Crafts custom vulnerabilities

Consideration – Threat Actors

Casual — Uses known vulnerabilities — You should always fix them

Professional — Derives vulnerabilities from common weaknesses

Persistent/State — Crafts custom vulnerabilities — Defense in depth

For software:

- No control over attacker
- Any weakness can eventually become a vulnerability

④ Actionable Risk Management

Assessing, Controlling & Scaling Up

Assessment – Risk = Probability × Impact

- **Quantitative** 💬
  - Numerical input from Statistical data
  - Provide a Cost perspective
  - Easy to justify

Assessment – Risk = Probability × Impact

- **Quantitative**
  - Numerical input from Statistical data
  - Provide a Cost perspective to controls RoI
  - Easy to justify

The Tornado Example

- **Probability:** Weather statistics(1/50y)
- **Impact:** Cost to rebuild(1M$)
- **Yearly Risk:** 1/50*1M$ = 20K$

Assessment – Risk = Probability × Impact

- Quantitative
  - Numerical input from Statistical data
  - Provide a Cost perspective to controls RoI
  - Easy to justify
- **Qualitative**
  - Based on fixed classes → To Justify
  - A (flexible) matrix to get a risk score → To Justify
  - Subjective determinations → To Justify

The Tornado Example

- **Probability:** Weather statistics(1/50y)
- **Impact:** Cost to rebuild(1M$)
- **Yearly Risk:** 1/50*1M$ = 20K$

Impact \ Probability	Very Low	Low	High	Very High
Very Low	Low	Low	Low	Low
Low	Low	Low	Med	Med
High	Med	Med	Med	High
Very High	Med	High	High	High

Assessment – Risk = Probability × Impact

- Quantitative
  - Numerical input from Statistical data
  - Provide a Cost perspective to controls RoI
  - Easy to justify
- Qualitative
  - Based on fixed classes → To Justify
  - A (flexible) matrix to get a risk score → To Justify
  - Subjective determinations → To Justify
- **Semi-Quantitative**

The Tornado Example

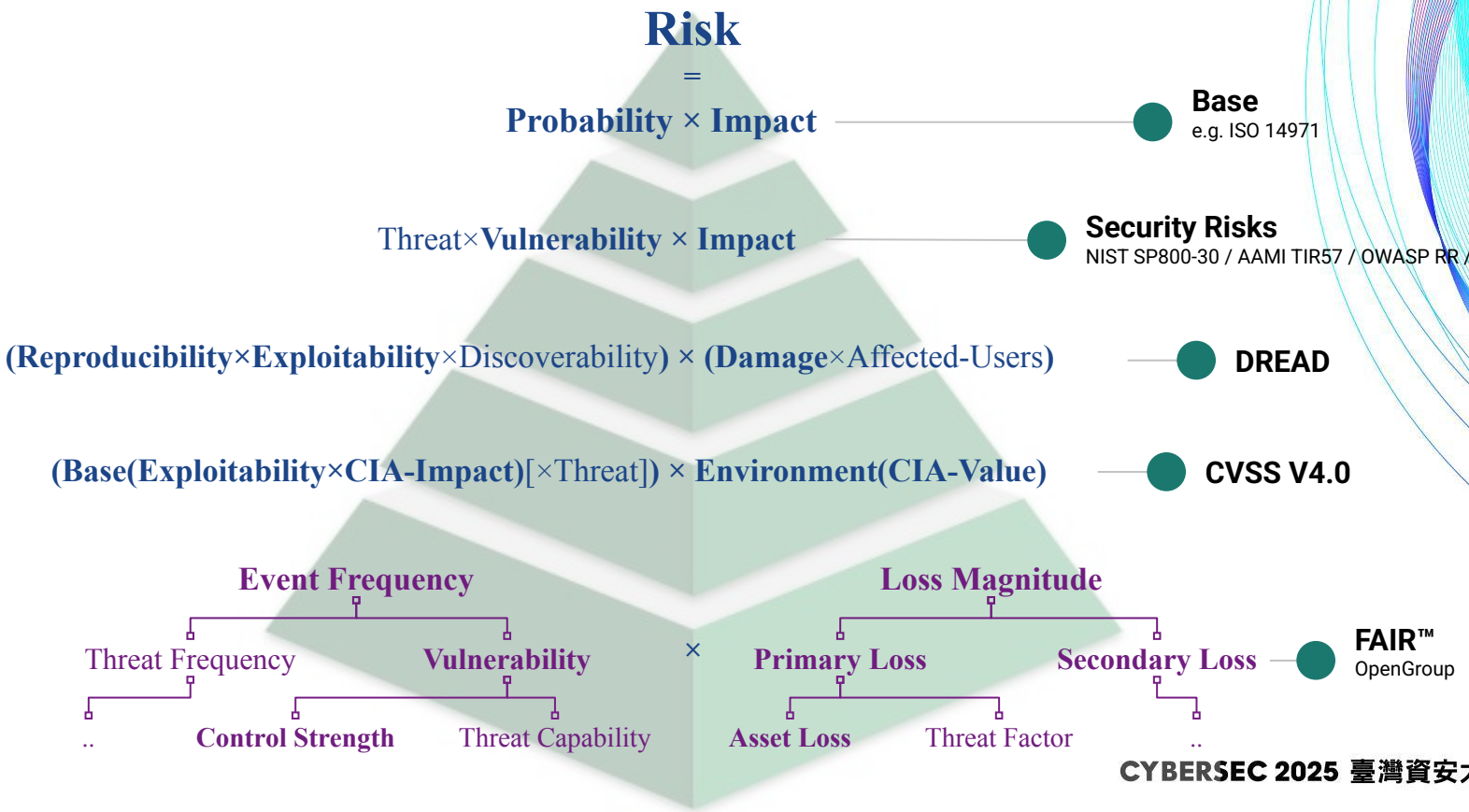
- **Probability:** Weather statistics(1/50y)
- **Impact:** Cost to rebuild(1M$)
- **Yearly Risk:** 1/50*1M$ = 20K$

Impact \ Probability	Very Low	Low	High	Very High
Very Low	Low	Low	Low	Low
Low	Low	Low	Med	Med
High	Med	Med	Med	High
Very High	Med	High	High	High

Method selection should consider:

1. The acceptance criteria
2. How control impact the residual risk

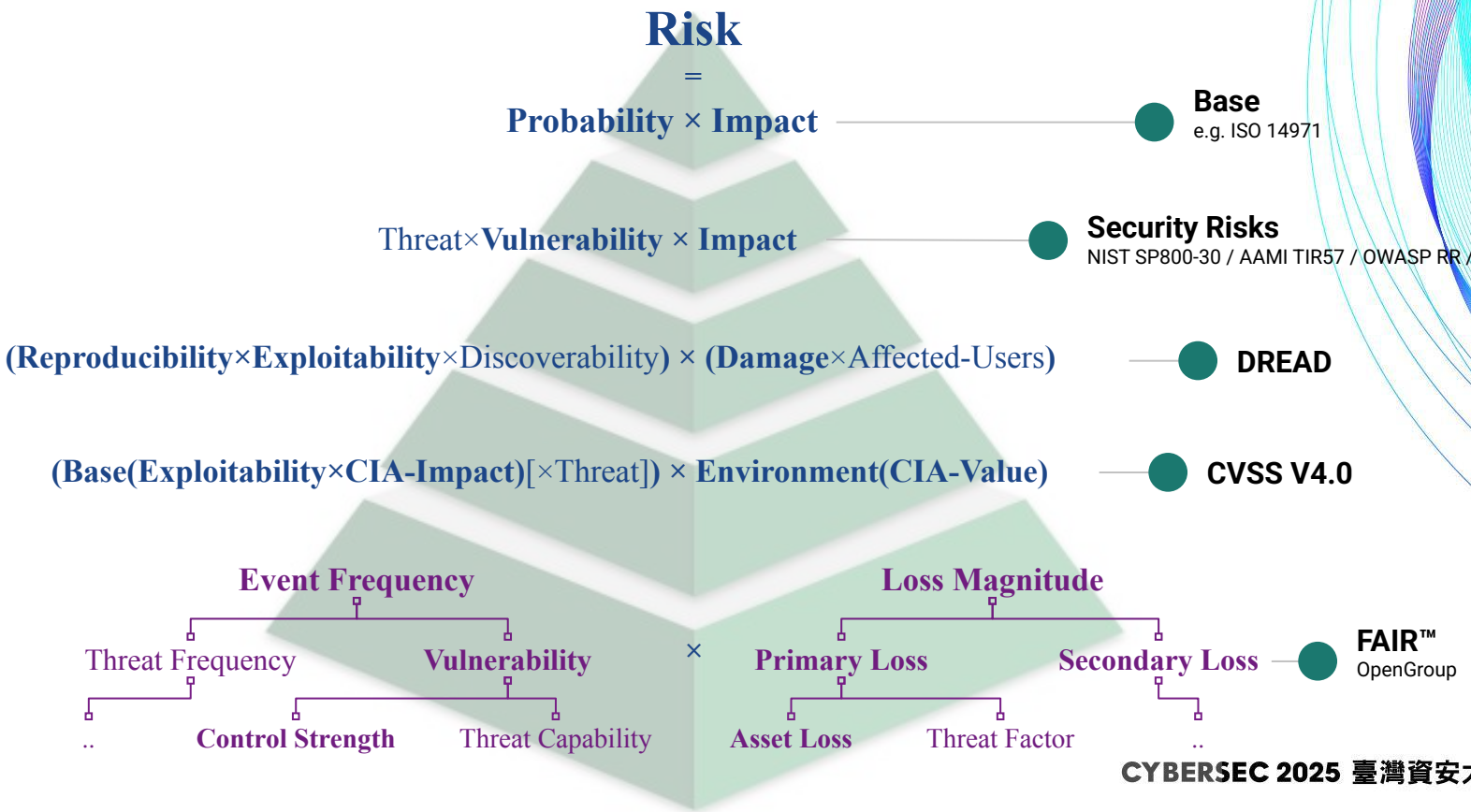
Assessment – Methods



Assessment –

Threats information might not be available.

Each input needs a justification: The more granular your model, the more work.



Assessment – CVSS v4.0

"CVSS is not a measure of risk." – NIST CSF

VS

*"It is **not possible** to quantify the **likelihood** of an incident*

*→ Focus on the **ability to exploit vulnerabilities**...*

Known vulnerabilities should be assessed as foreseeable risks

→ Focus on preventing the introduction of defects…" – FDA

Assessment – CVSS v4.0

"CVSS is not a measure of risk." – NIST CSF

VS

*"It is **not possible** to quantify the **likelihood** of an incident*

*→ Focus on the **ability to exploit vulnerabilities**...*

Known vulnerabilities should be assessed as foreseeable risks

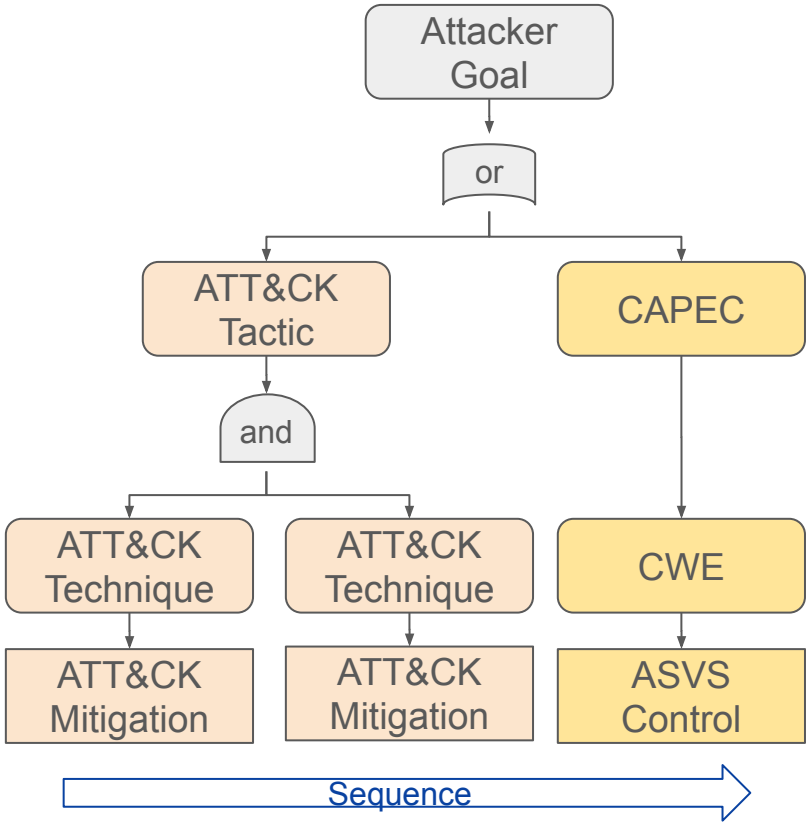
→ Focus on preventing the introduction of defects…" – FDA

- Tutorial, examples & calculators (first.org/cvss)
- Detailed discussions
  - NIST IR 7435 & 8409
  - MITRE applying-cvss-to-medical-devices
  - FDA Qualified CVSS based extension
- Compact notation. **XSS risk score 6.8**

CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:P/VC:H/VI:L/VA:N/SC:N/SI:N/SA:N/CR:H/IR:M/AR:L

	Input	Values
Exploitability	Attack Vector <Component>	**Network** / Adjacent / Local / Physical
	Attack Complexity <Weakness/Vector>	**Low** / High
	Attack Requirements <Weakness/Vector>	**None** / Present
	Privileges Required <Weakness/Vector>	None / **Low** / High
	User Interaction <Attack Tree>	None / **Passive** / Active
Impact	Impact on CIA triad <Weakness>	C: None / Low / **High** I: None / **Low** / High A: **None** / Low / High
Environment	Value of CIA triad <Asset Value>	C: **High** / Med / Low I: High / **Med** / Low A: High / Med / **Low**

Assessment – Attack Trees



- Build it using knowledge bases linkage (or be ready to justify it)
- Focus to justify assessment input & controls
- Can be used for later Pen-testing

Mitigation & Validation

1. **Create** a security requirement for each control
2. **Verify** the implementation is fulfilled
3. **Validate** the vulnerability is not exploitable
    - Build list of relevant tests
        - Justify from knowledge base

Risk ID	CVSSv4	Risk Score	Controls	Req. ID	Tests
Server-79	AV:N/AC:L/AT:N/PR:L/UI:P/VC:H/VI:L/VA:N/SC:N/SI:N/SA:N/CR:H/IR:M/AR:L	**6.8**	1.4.3, 5.1.1, 5.1.2, 5.1.3, 5.1.4, 5.3.3, 5.3.4, 6.2.1	**Sec-Service-1~8**	**SAST/DAST/Fuzz**

Mitigation & Validation

> *"Manufacturers should provide details and evidence of testing that demonstrates effective risk control measures according to the threat."*
> – FDA Cybersecurity in Medical Devices

1. **Create** a security requirement for each control
2. **Verify** the implementation is fulfilled
3. **Validate** the vulnerability is not exploitable
    - Build list of relevant tests
        - Justify from knowledge base
    - If *high* risk: Penetration-test following the attack tree

Risk ID	CVSSv4	Risk Score	Controls	Req. ID	Tests
Server-79	AV:N/AC:L/AT:N/PR:L/UI:P/VC:H/VI:L/VA:N/SC:N/SI:N/SA:N/CR:H/IR:M/AR:L	**6.8**	1.4.3, 5.1.1, 5.1.2, 5.1.3, 5.1.4, 5.3.3, 5.3.4, 6.2.1	**Sec-Service-1~8**	**SAST/DAST/Fuzz**

Some controls are out of scope of your software and must be mitigated at the system level. → Configuration baseline / User doc.

Residual Risk – Exploratory Approach

Score the confidence a weakness is not exploitable.

Residual Risk = Risk × (1 – **Confidence Score**%)

Confidence Score (%) = **control coverage** (Verification) × **test coverage** (Validation)

Coverage (%) = #Passed tests|controls / # Guidance tests|controls

XSS Example:

Controls: 6 controls implemented (out of 8 ASVS recommended)

Testing: 3 testing approaches performed (out of 3 recommended)

Risk ID	CVSSv4	Risk Score	Verification	Validation	Confidence	Residual Risk
Server-79	AV:N/AC:L/AT:N/PR:L/UI:P/VC:H /VI:L/VA:N/SC:N/SI:N/SA:N/CR:H /IR:M/AR:L	**6.8**	6/8	3/3	75%	**1.7**

Residual Risk – Exploratory Approach

Score the confidence a weakness is not exploitable.

Residual Risk = Risk × (1 – **Confidence Score**%)

Confidence Score (%) = **control coverage** (Verification) × **test coverage** (Validation)

Coverage (%) = #Passed tests|controls / # Guidance tests|controls

XSS Example:

Controls: 6 controls implemented (out of 8 ASVS recommended)

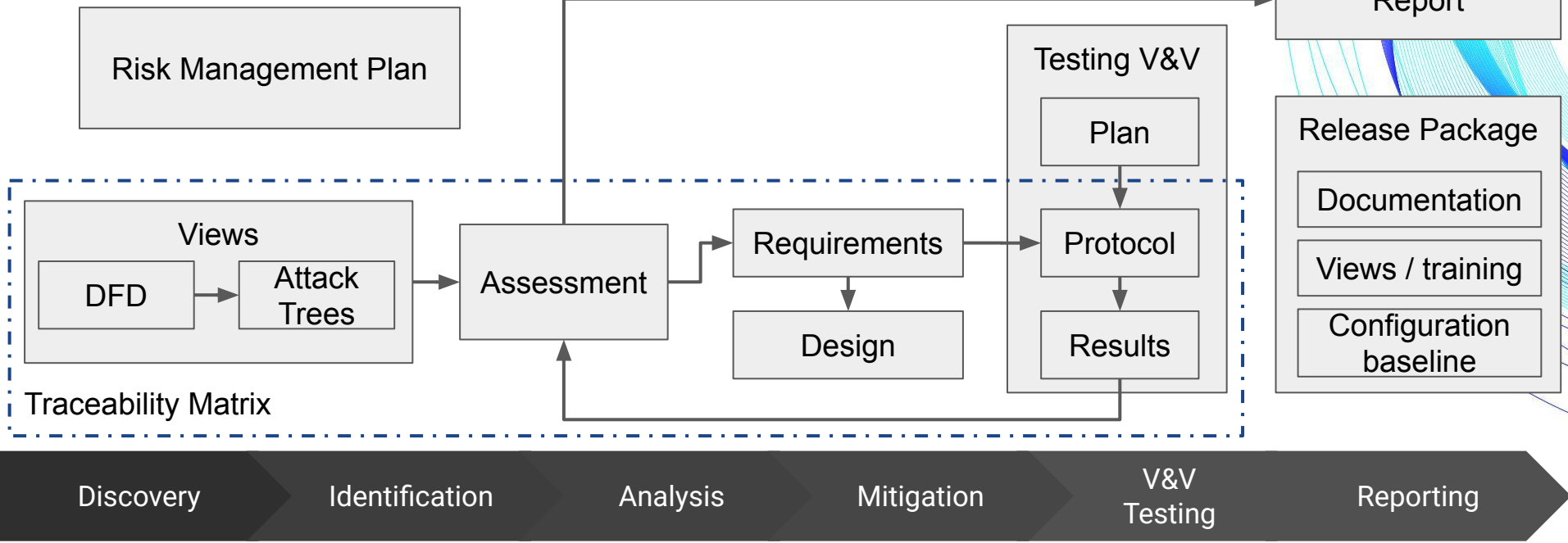
Testing: 3 testing approaches performed (out of 3 recommended)

Risk ID	CVSSv4	Risk Score	Verification	Validation	Confidence	Residual Risk
Server-79	AV:N/AC:L/AT:N/PR:L/UI:P/VC:H /VI:L/VA:N/SC:N/SI:N/SA:N/CR:H /IR:M/AR:L	**6.8**	6/8	3/3	75%	**1.7**

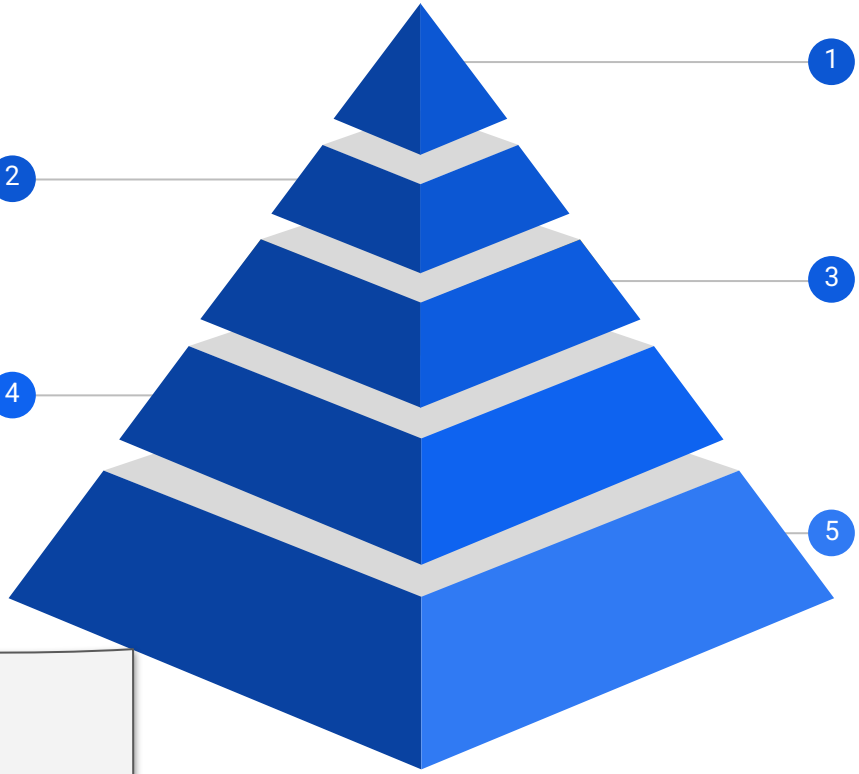
Any detection of the vulnerability would be an automatic failure.
→ Control effectiveness confidence = 0%.

Wrapping up your *Security Risk Management File*

Following your Good Documentation Practices..



Security Risk Layers



Organization Security
1 Protect the business and the people.

ISMS
Govern the information landscape. 2

System Security
3 Protect a service and its assets

SSDLC
Provide Secure Environment. 4

Software Security
5 Delivery Trustworthy Product

Threats cross roles boundaries,

Reach out to the other teams!

Automation & Sustainability

- **Scale**
  - Applications complexity keeps growing
  - Methods keeps improving
- **But maintain**
  - Defensible decisions (A to Z)
  - Demonstration of tool performance
  - Human oversight & input

"Organizations can simplify execution, employ innovative approaches for managing risk, and increase the level of automation…" – NIST

Tools impacting quality of a regulated product must be validated (Demonstrate performance)

— 21 CFR 820.70i/ISO 13485

FDA tools Registry: FDA MD Dev Tools

Automation & Sustainability

- **Scale**
  - Applications complexity keeps growing
  - Methods keeps improving
- **But maintain**
  - Defensible decisions (A to Z)
  - Demonstration of tool performance
  - Human oversight & input

Tools impacting quality of a regulated product must be validated (Demonstrate performance)

— 21 CFR 820.70i/ISO 13485

FDA tools Registry: FDA MD Dev Tools

④

"Organizations can simplify execution, employ innovative approaches for managing risk, and increase the level of automation…" – NIST

AI?

Great for supporting human in:

- Navigating sources of information
- Documentation streamlining
- Draft assessment & Check consistency

Still challenging to defend performance

Maybe soon?

Power Your Team!

- ✅Make it repeatable & efficient
- ✅DFD & CVSS – proven & practical
- ✅Use knowledge bases (e.g. MITRE)
- ✅Automate – but ensure defensibility!
- ✅No “one-size-fits-all” approach..

Q&A

Call to Action

Contribute to community knowledge bases!

Let’s Connect!

linkedin.com/in/sauvainr

Thank You

TEAM
CYBERSECURITY