DevOps在工業領域落地實務經驗

TJ Tai
SRE/DevOps

MOXA®

MOXA®

Tj Tai

Team Lead, SW

Tj.Tai@moxa.com

https://www.linkedin.com/in/tj-tai/

2013
Joined Moxa

10+ years
Developer Experience

10+ years
Industry Experience

Experience

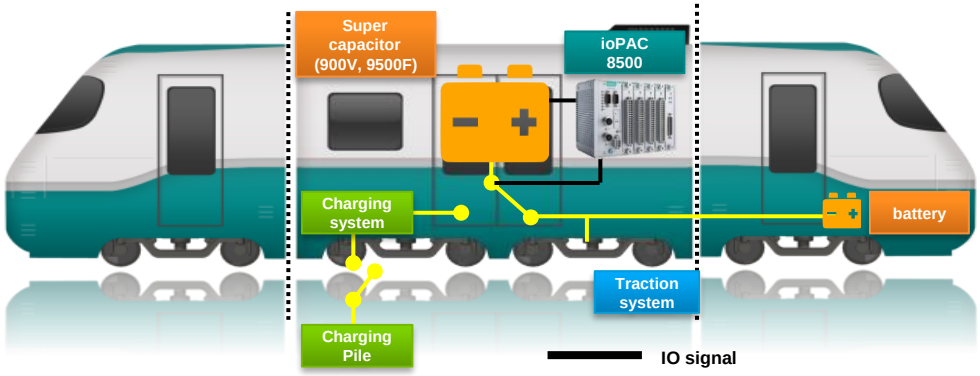
- SRE Team Lead at Moxa
- DevOps/Site Reliability Engineer at Moxa
- IIoT Product Software Developer at Moxa
- DevOps Taiwan Meetup Speaker
- AgileCommunity.tw Speaker

Education

- National Sun Yat-Sen University, Master of Department of Computer Science and Engineering

Onboard Condition Monitoring

China



- ioPAC 8500 monitor the on/off and power level of super capacitor
- Super capacitor provide the power to traction system when running.
- Super capacitor switch to charging system when arriving the station
- Battery provide the power for onboard PIS, light HVAC system

MOXA Products

- ioPAC 8500

Background & Requirements

- Small tram will limit space and wright constraint
- Need 0-50mA analog input
- Short installation period
- IEC 61131-3 programming is required
- Railway certificated

Why Moxa?

- Compact 5 slot design with light weight
- Fast customization for 0-50mA analog input
- Support IEC 61131-3 programming
- Railway EN 50155 compliance
- Anti-vibration design

Train Supervision & Information System

- **Country:**
  - Taiwan
- **Operator:**
  - Taipei Metro
- **Challenge:**
  - Combined PIS and monitoring system
  - Limited installation space
  - IP based train communication network

ioPAC 8020-C Series

Train Supervision Information System

Side Door LED Display

Train Destination Display

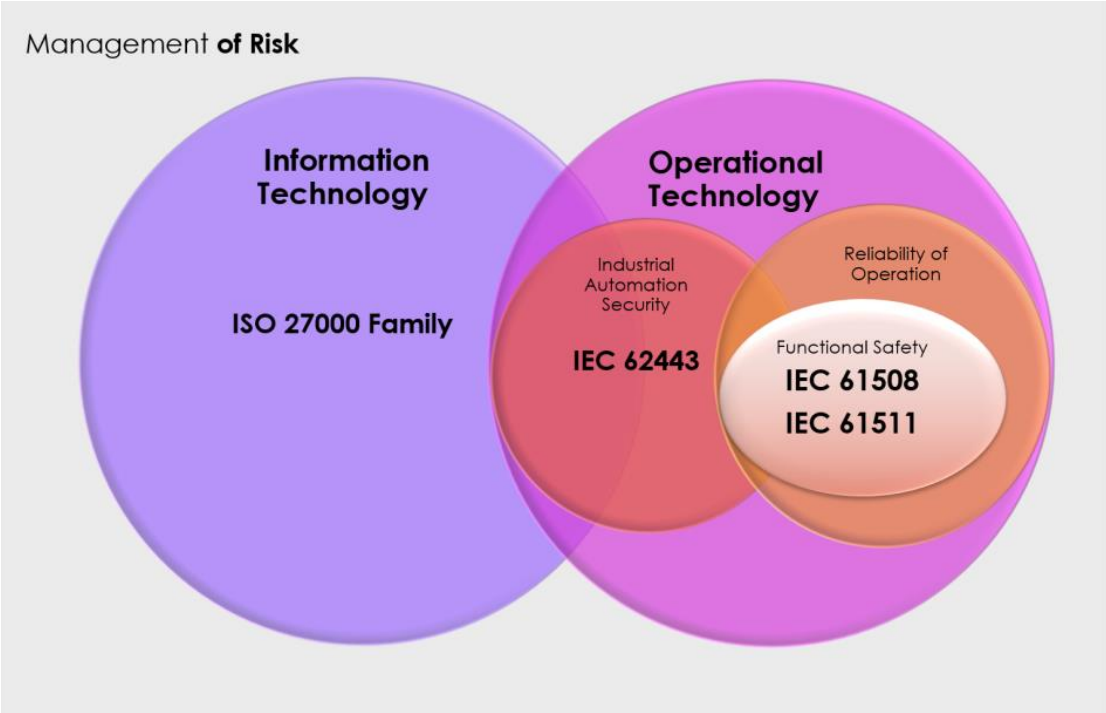
Installation – Under Passenger Seat

Compliance

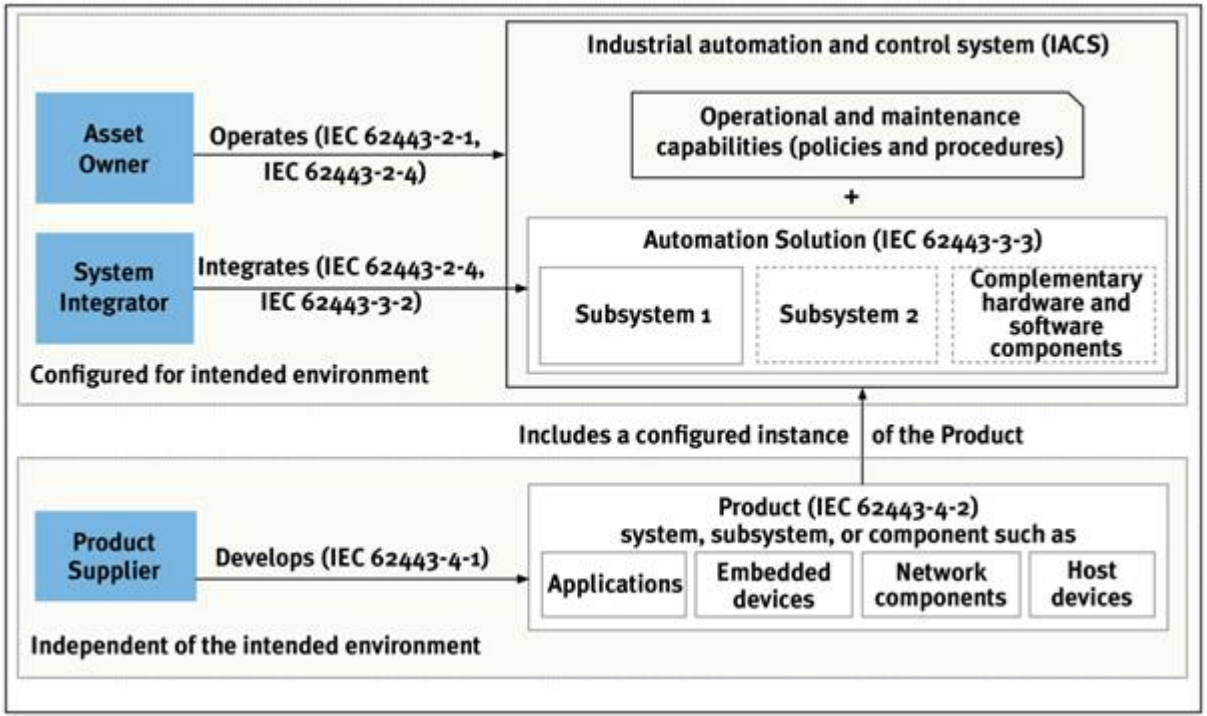
Focus

Standards	ISO 27001	NIST CSF	NIST SP800-82	IEC62443
Name	Information security management systems	NIST Cybersecurity Framework	Guide to Industrial Control Systems (ICS) Security	Security of Industrial Automation and Control Systems
Reach	International	North American	North American	International

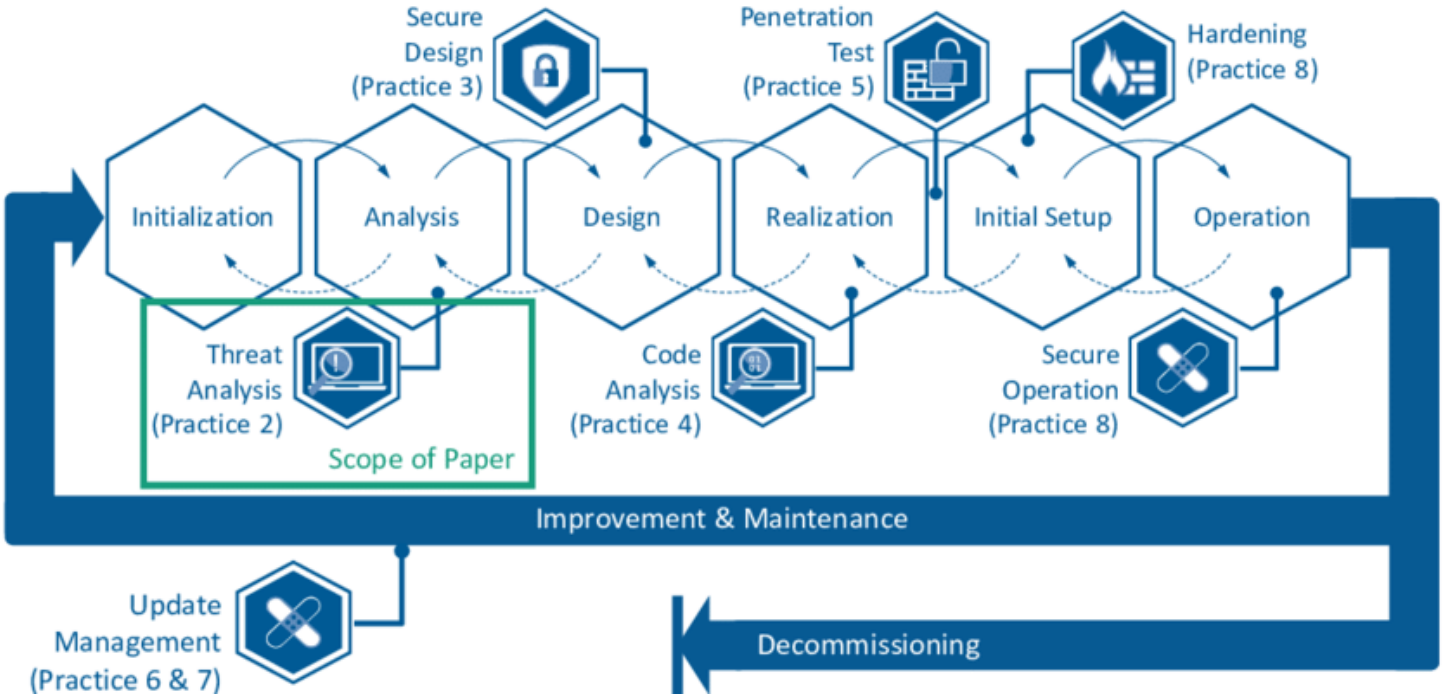
Focus

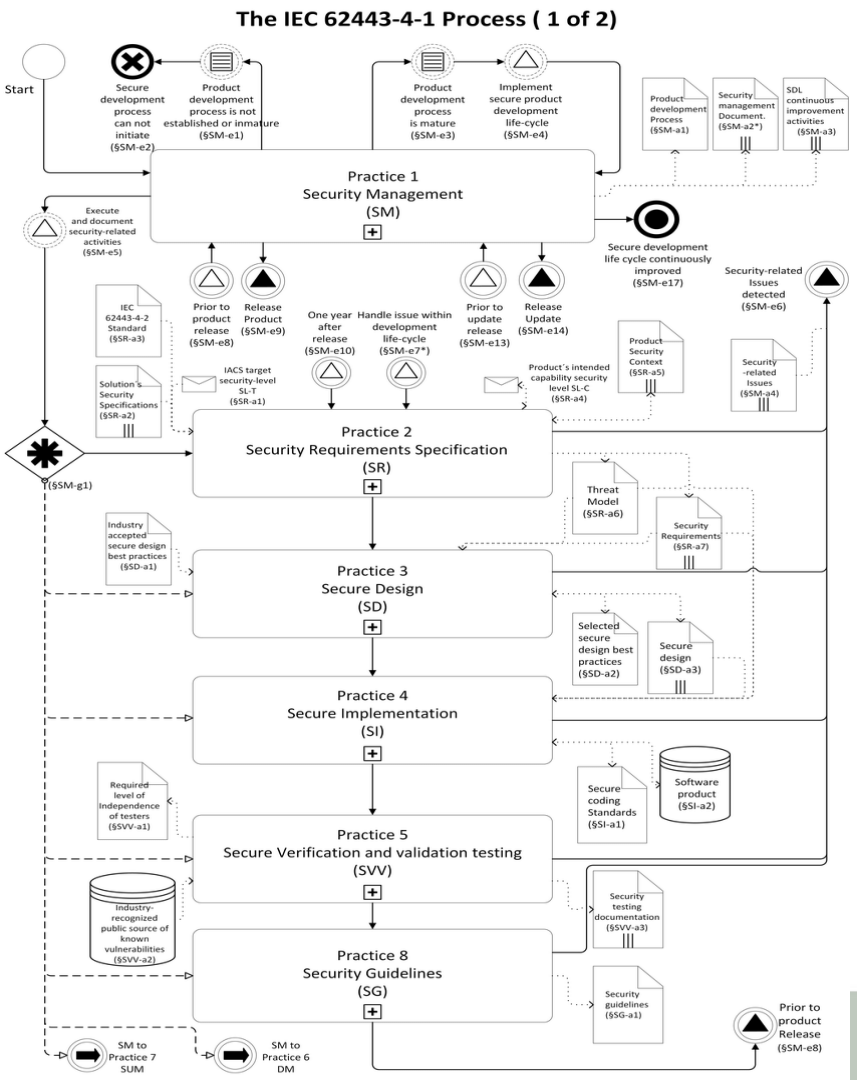

Management of Risk
Information Technology
ISO 27000 Family
Operational Technology
Industrial Automation Security
IEC 62443
Reliability of Operation
Functional Safety
IEC 61508
IEC 61511

IEC 62443-4-1



IEC 62443-4-1





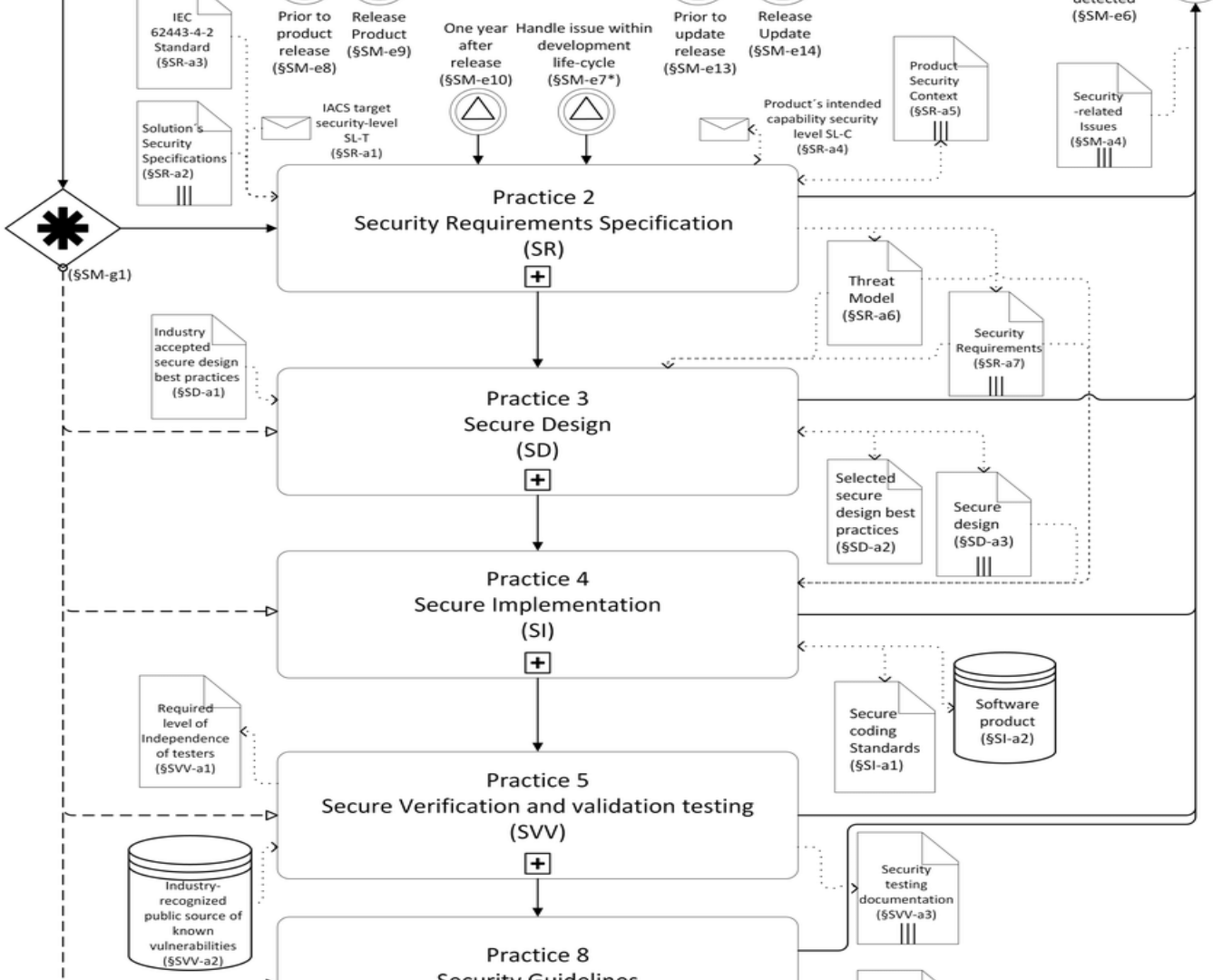
PSC

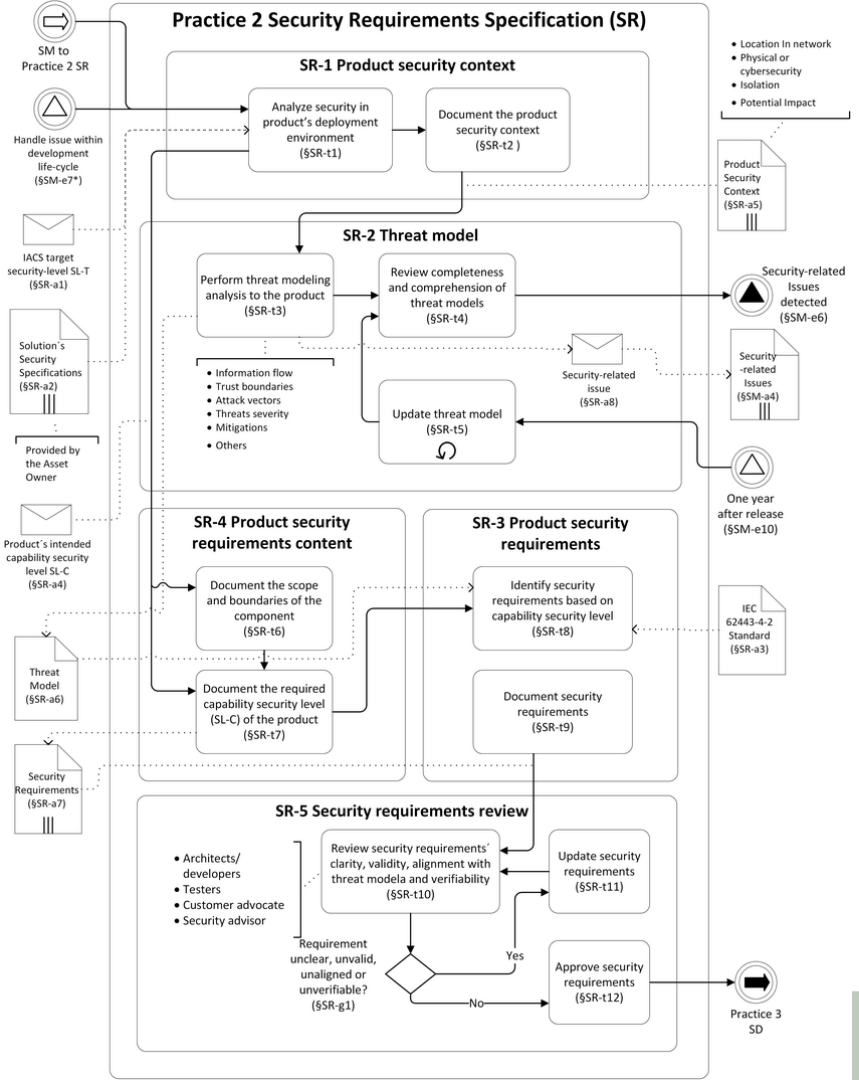
PM

PM+RD

RD

SQA


IEC 62443-4-2 Standard (§SR-a3)
Prior to product release (§SM-e8)
Release Product (§SM-e9)
One year after release (§SM-e10)
Handle issue within development life-cycle (§SM-e7*)
Prior to update release (§SM-e13)
Release Update (§SM-e14)
Product Security Context (§SR-a5)
Security -related Issues (§SM-a4)
(§SM-e6)
Solution´s Security Specifications (§SR-a2)
IACS target security-level SL-T (§SR-a1)
Product´s intended capability security level SL-C (§SR-a4)
(§SM-g1)
Practice 2
Security Requirements Specification
(SR)
Threat Model (§SR-a6)
Security Requirements (§SR-a7)
Industry accepted secure design best practices (§SD-a1)
Practice 3
Secure Design
(SD)
Selected secure design best practices (§SD-a2)
Secure design (§SD-a3)
Practice 4
Secure Implementation
(SI)
Secure coding Standards (§SI-a1)
Software product (§SI-a2)
Required level of Independence of testers (§SVV-a1)
Practice 5
Secure Verification and validation testing
(SVV)
Security testing documentation (§SVV-a3)
Industry-recognized public source of known vulnerabilities (§SVV-a2)
Practice 8


Practice 2 Security Requirements Specification (SR)
SM to Practice 2 SR
Handle issue within development life-cycle (§SM-e7*)
IACS target security-level SL-T (§SR-a1)
Solution´s Security Specifications (§SR-a2)
Provided by the Asset Owner
Product´s intended capability security level SL-C (§SR-a4)
Threat Model (§SR-a6)
Security Requirements (§SR-a7)
SR-1 Product security context
Analyze security in product's deployment environment (§SR-t1)
Document the product security context (§SR-t2)
• Location In network
• Physical or cybersecurity
• Isolation
• Potential Impact
Product Security Context (§SR-a5)
SR-2 Threat model
Perform threat modeling analysis to the product (§SR-t3)
Review completeness and comprehension of threat models (§SR-t4)
Security-related Issues detected (§SM-e6)
• Information flow
• Trust boundaries
• Attack vectors
• Threats severity
• Mitigations
• Others
Security-related issue (§SR-a8)
Security -related Issues (§SM-a4)
Update threat model (§SR-t5)
One year after release (§SM-e10)
SR-4 Product security requirements content
Document the scope and boundaries of the component (§SR-t6)
Document the required capability security level (SL-C) of the product (§SR-t7)
SR-3 Product security requirements
Identify security requirements based on capability security level (§SR-t8)
Document security requirements (§SR-t9)
IEC 62443-4-2 Standard (§SR-a3)
SR-5 Security requirements review
• Architects/ developers
• Testers
• Customer advocate
• Security advisor
Review security requirements´ clarity, validity, alignment with threat modela and verifiability (§SR-t10)
Update security requirements (§SR-t11)
Requirement unclear, unvalid, unaligned or unverifiable? (§SR-g1)
Yes
No
Approve security requirements (§SR-t12)
Practice 3 SD

IEC 62443-4-1 activity

- **Threat modeling(Threat Analysis)**
  - **Integrate with Jira**
- **Vulnerability scan(Code Analysis)**
  - **SAST**
  - **SCA**
  - **DAST**
- **Vulnerability management**

Vulnerability Scan

- **SAST**
  - **Coverity**
    - CERT Report
    - CWE Report
- **SCA**
  - **BlackDuck**
    - CVE Report
    - FOSS BOM & FOSS Statement
    - SBOM

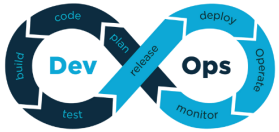
Vulnerability Scan

- **DAST**
  - **Defensics**
    - Fuzzy testing
  - **Nessus**
    - Vulnerability assessment
  - **Acuentix**
    - Web security testing

SSDLC

Secure Software Development Life Cycle

SSDLC

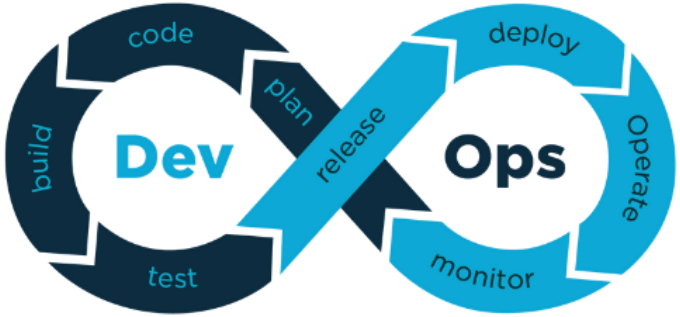


Plan	Code	CI	Test	Monitor
Issue tracking Knowledge base	Source Code Management	Auto-Scaling CI Runner(aws)	Continuous Testing	Quality Dashboard
Jira Confluence SSO	Gitlab.com SSO & ISO-27001 Control	SAST(Coverity) Build System Artifacts System (scm) SCA(BlackDuck) Valgrind	Security Testing DAST Defencis Nessus Acunetix Auto Test	Jira Dashboard Test report server

MOXA

DevOps

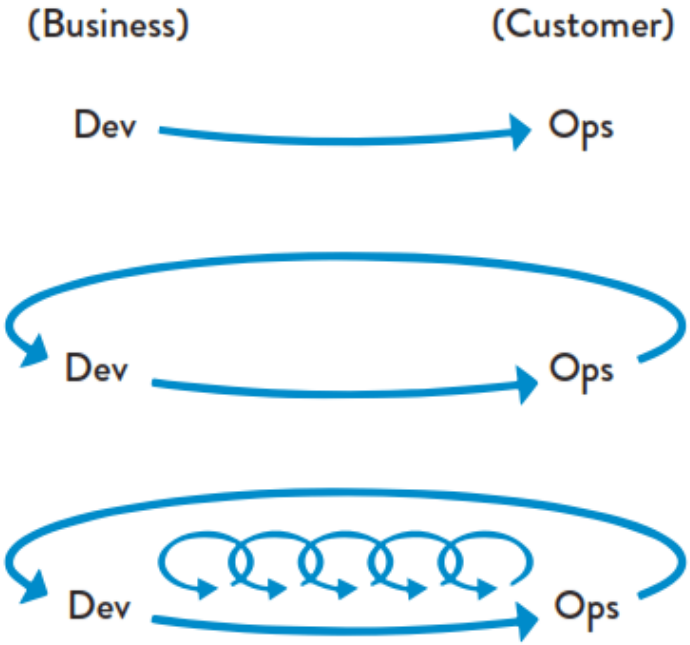
DevOps



- DevOps = Develop + Operation
- DevOps 是將開發與維運團隊所負責的工作產出進行無縫整合，以更快速更有效率的方式交付系統
- DevOps 開發維運的實務做法可促進開發團隊 (Dev) 與 IT 營運團隊 (Ops) 的合作夥伴之間更順暢、持續的溝通、協同作業、整合、可視化

DevOps

- 「Dev」與「Ops」之間的這種密切關係貫穿了開發維運生命週期SDLC的每個階段
- 這種關係推動了進一步改善、開發、測試及部署的持續客戶回饋循環
- 這些努力的結果之一可能是更快速地持續發佈必要的功能變更或新增項目
- 建立從開發到運維之間的快速流動，讓客戶的價值可以被快速交付



PSC IEC62443-4-1/4-2 產品資安

SRE Team
(DevSecOps)

IT ISMS ISO27001 企業資安

PSC IEC62443-4-1/4-2 產品資安

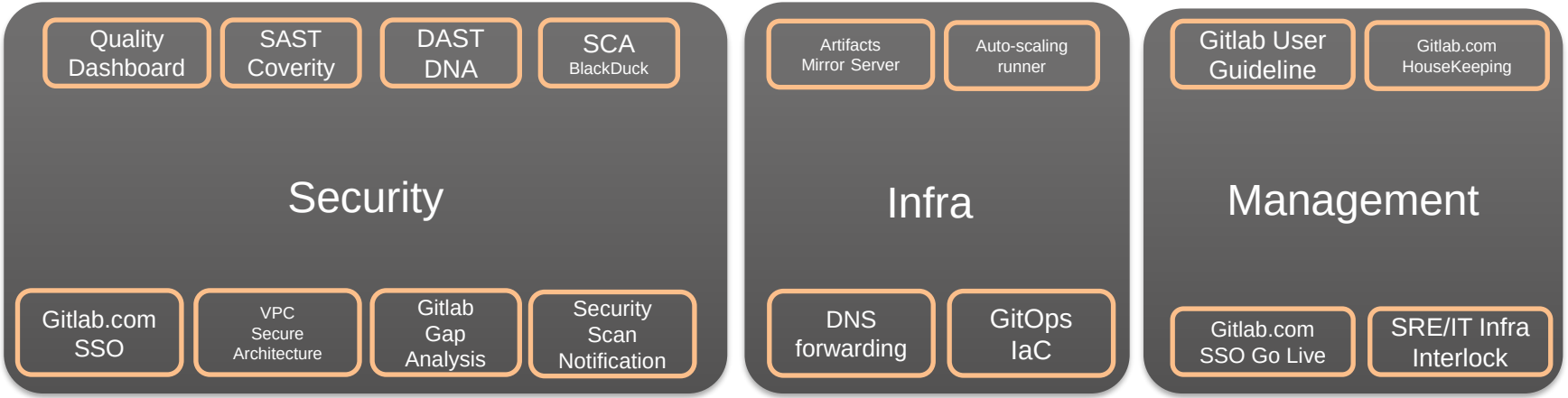
Security

Infra

Management

IT ISMS ISO27001 企業資安

PSC IEC62443-4-1/4-2 產品資安



IT ISMS ISO27001 企業資安

GOAL

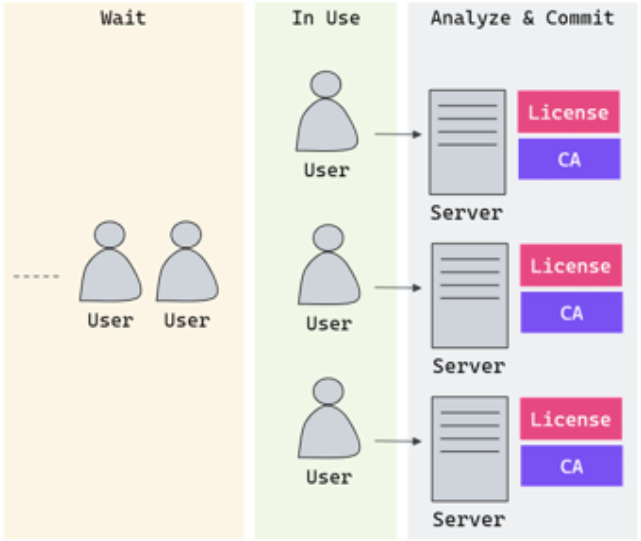
WORK WITH IT(ISO 27001) & PSC(IEC-62443) TO LET PRODUCT TEAM EASY TO ADOPT DEVSECOPS APPROACH TO MAKE SECURITY LANDING IN MOXA

DevOps Practices

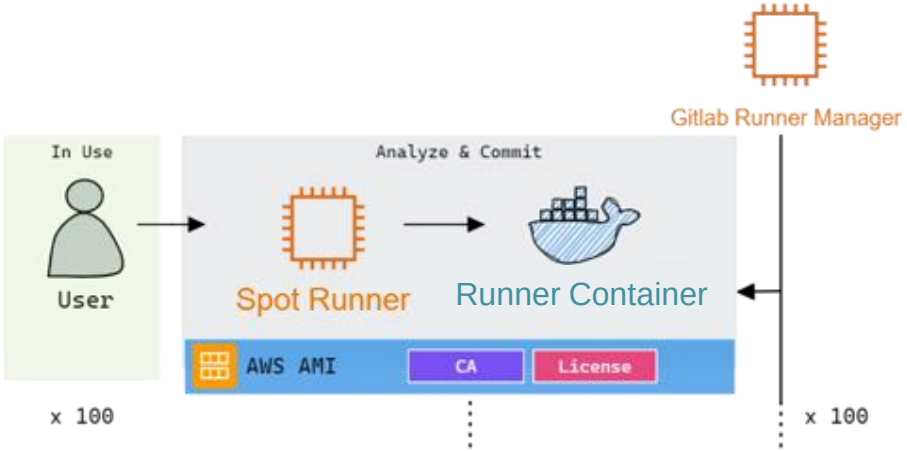
實務案例分享

免安裝 & 解決 License 限制

Before (Max 3 job)

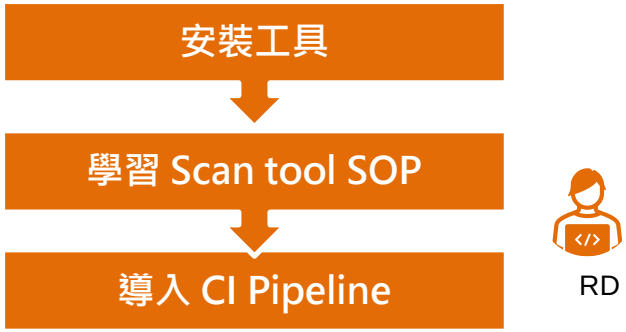


After (Max 100 job, Unlimited)

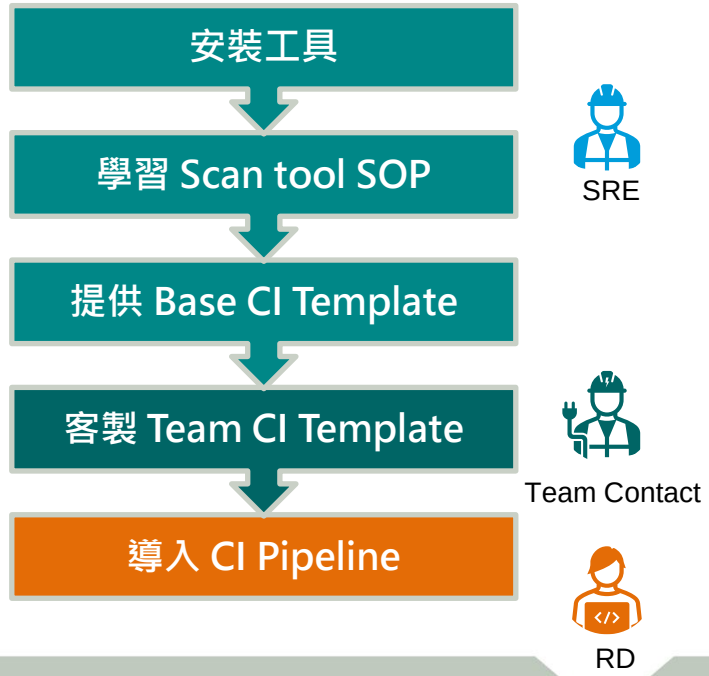


加速 CI 散佈到團隊，更合身

- **Before**

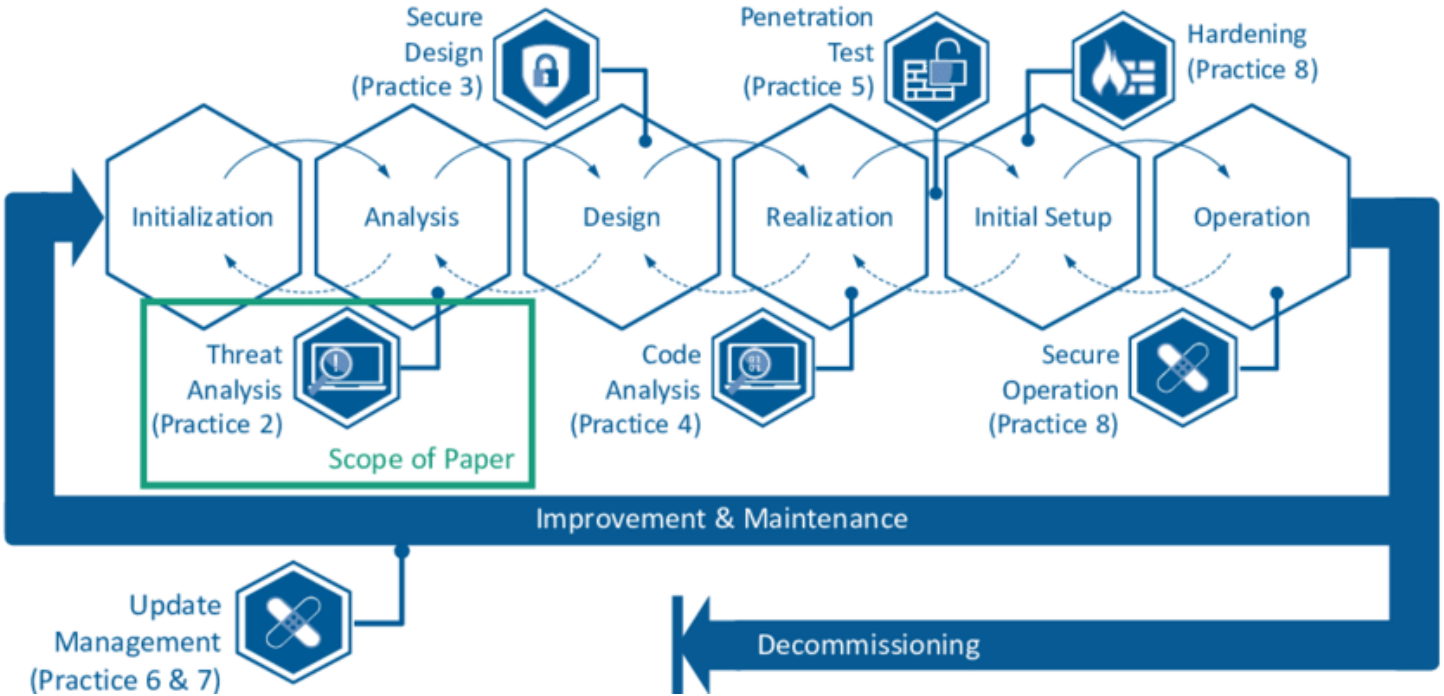


- **After**

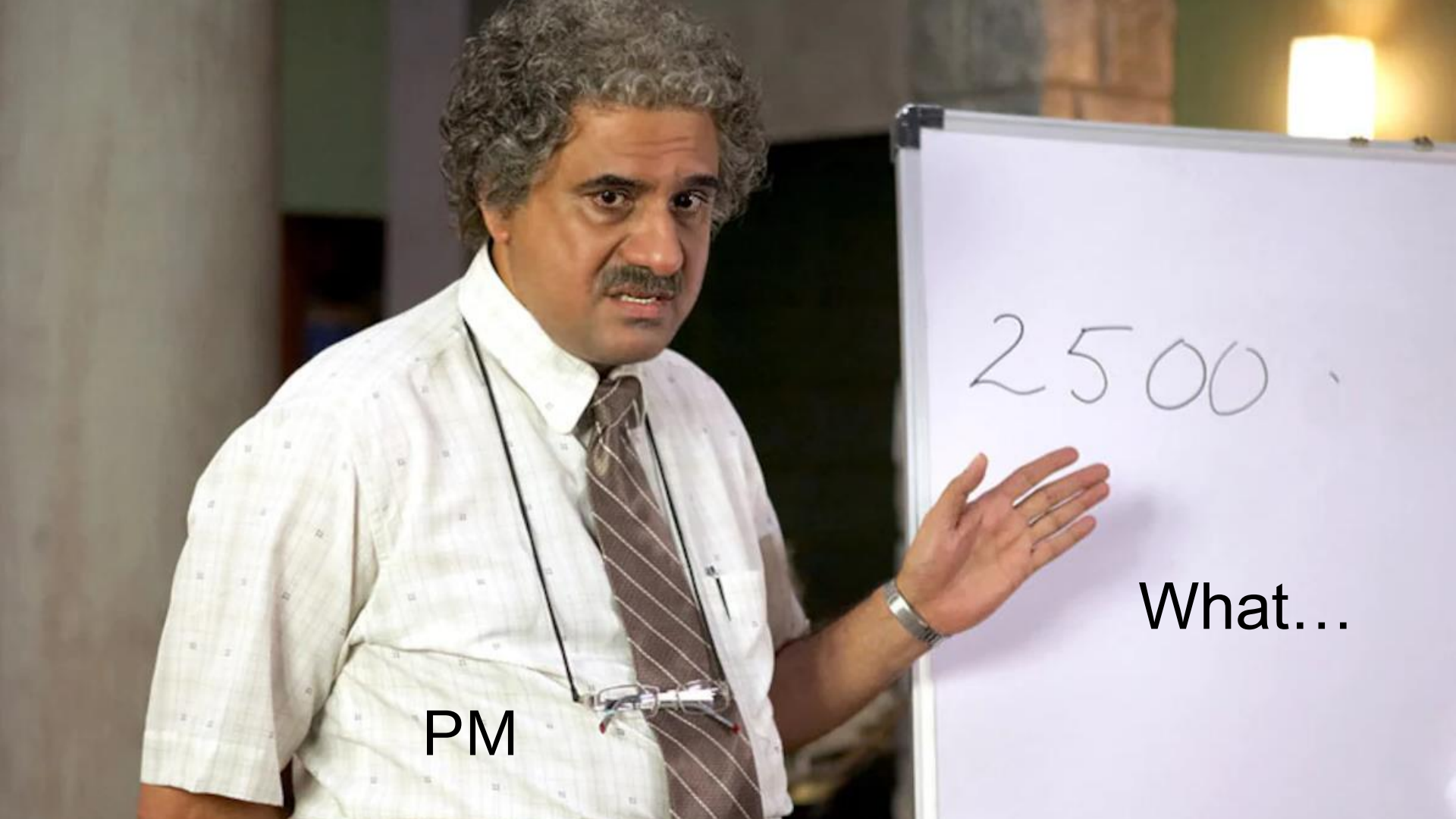



Based on a True Story
(以IO Controller專案為例)

IEC 62443-4-1




Engineer A:
DFD畫完列出來我們有596個threat要做分析
Engineer B:
我們剛剛花了1小時才完成2個threat的分析
Engineer C:
那假設我們一周花1.5天在review threat的話
我們大概要花6個月才能做完所有threat modeling分析


2500
What…
PM

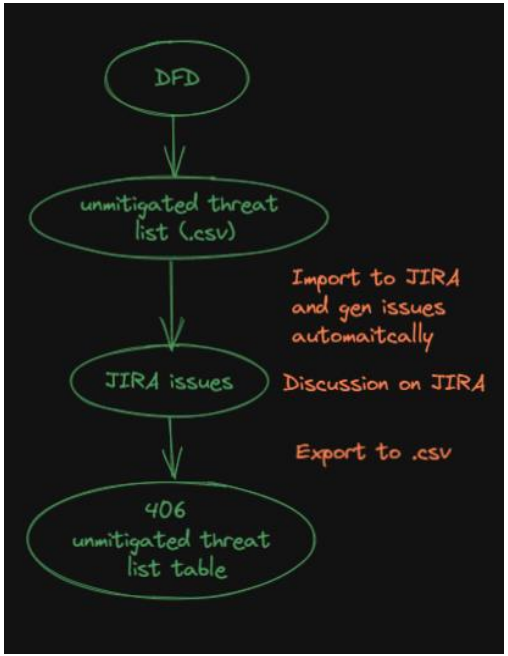
會議日期	完成項目	會議時間(hr)	每小時完成項目
9/13	3	1.5	2.00
9/14	9	2	4.50
9/20	7	1.5	4.67
9/27	15	1.5	10.00
9/29	14	1.5	9.33
10/4	21	2	10.50
10/12	11	1	11.00
10/14	13	1	13.00

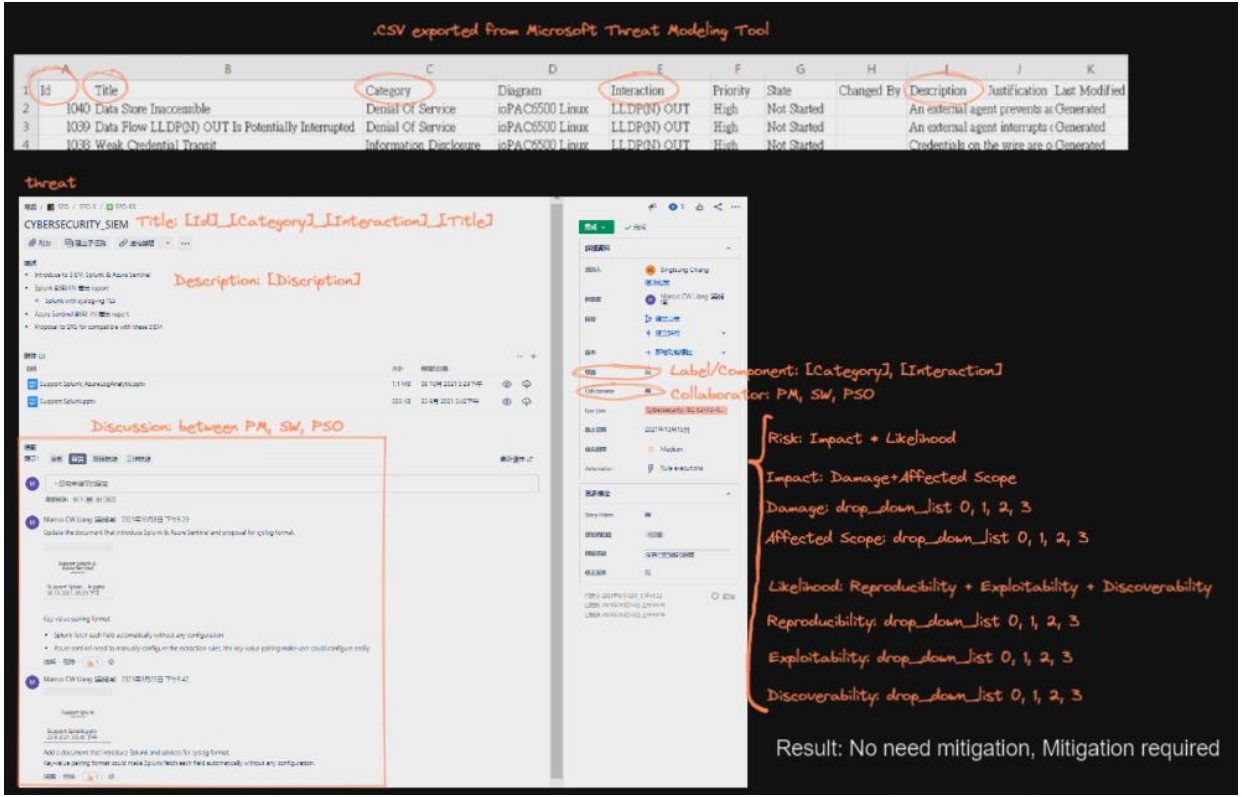
就算去掉一開始不熟悉
上手後平均1小時9條

用excel很難記錄討論過程

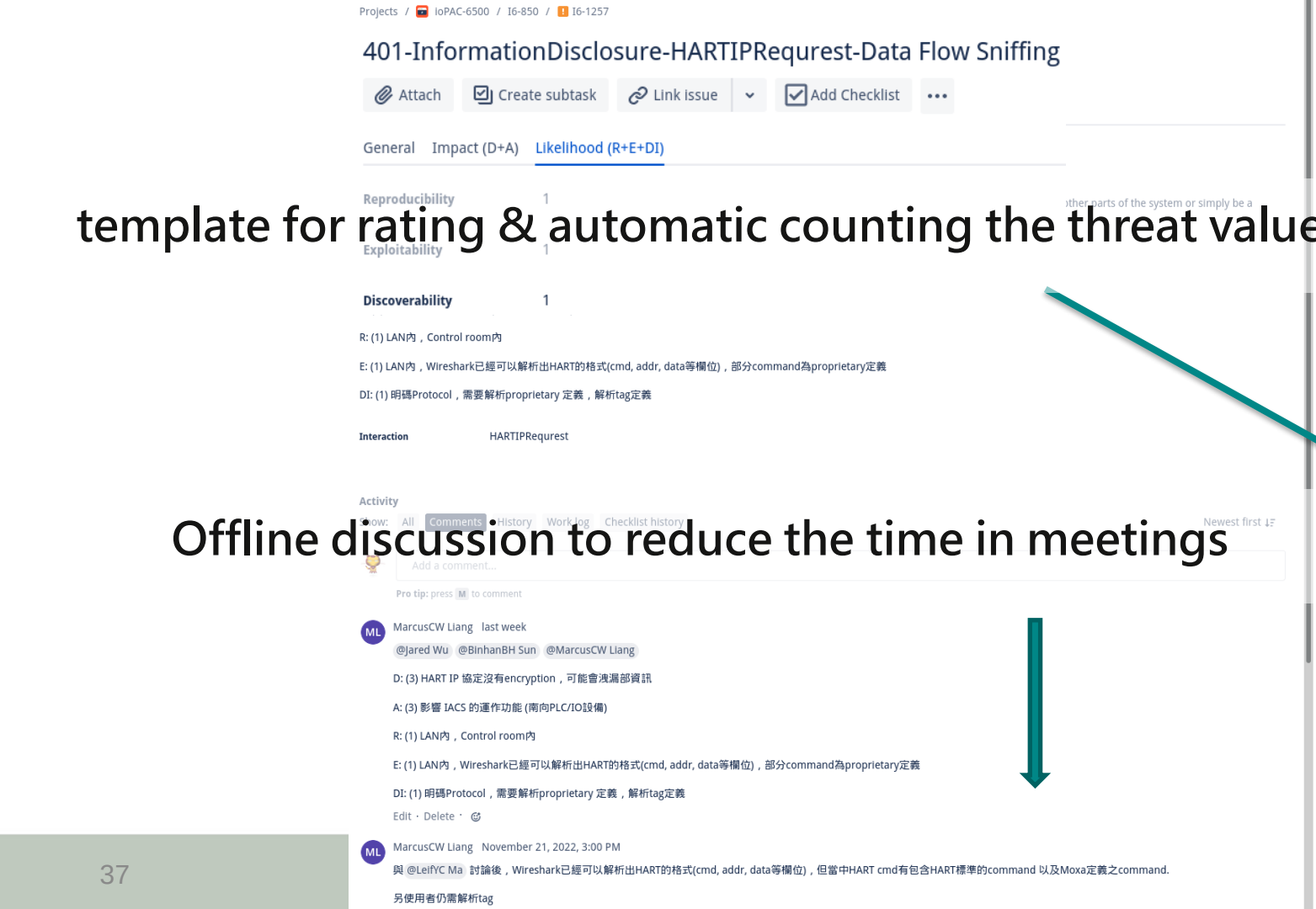

SSDLC起手式就是threat modeling
大家都想認真一條條threat review好
但這樣run下去不行啊...

Product Team 提案



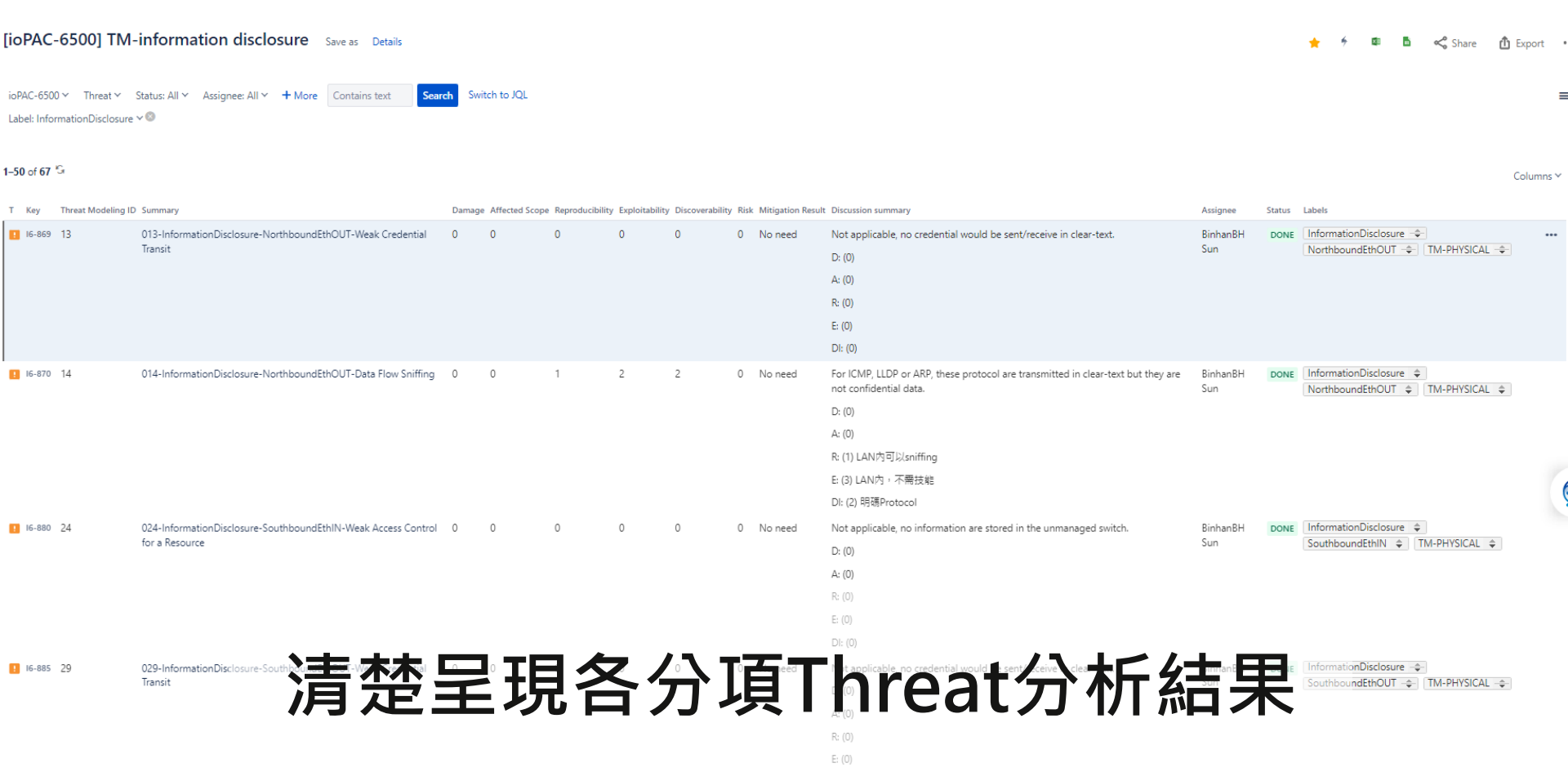



After discussed with SRE…



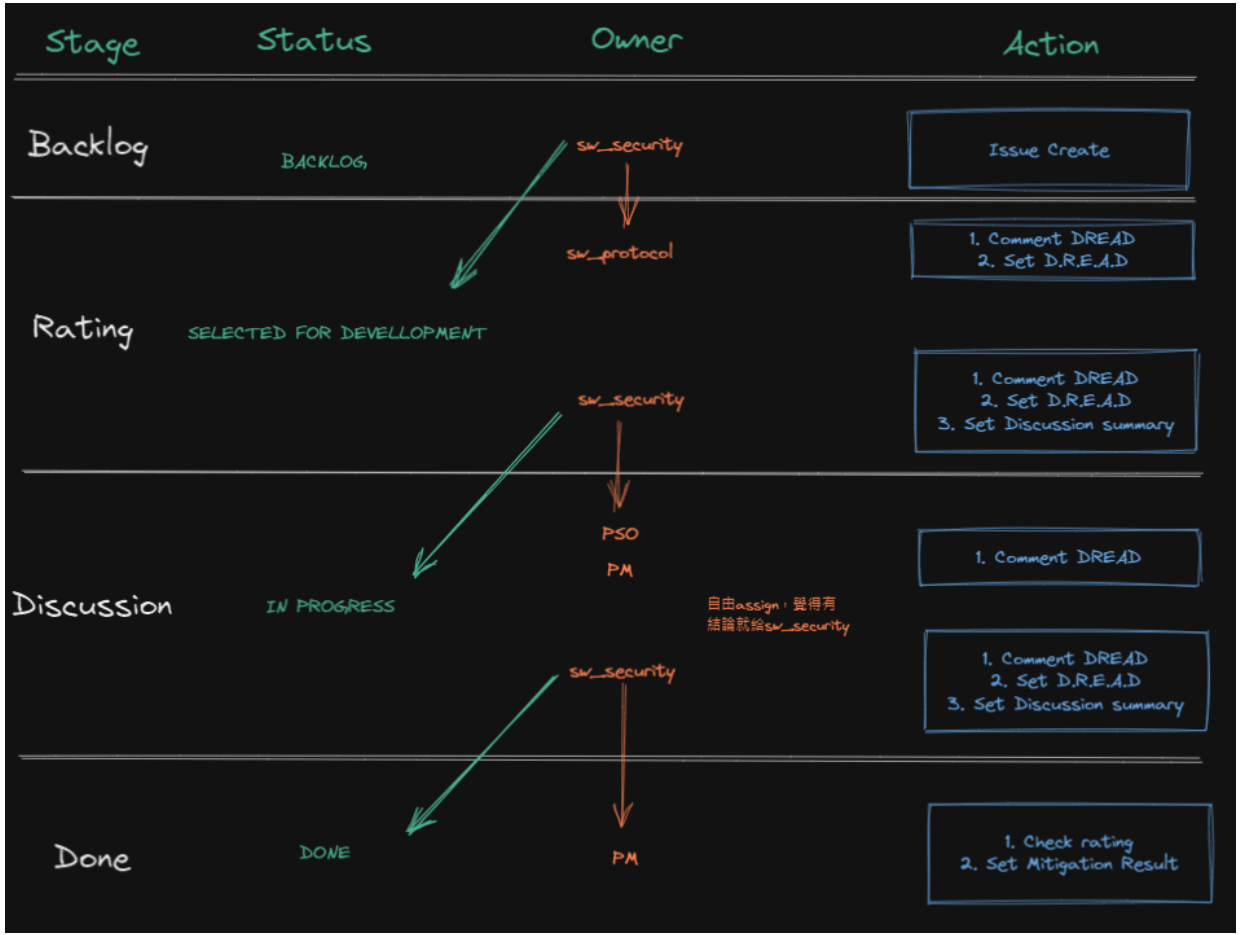
template for rating & automatic counting the threat value

Offline discussion to reduce the time in meetings



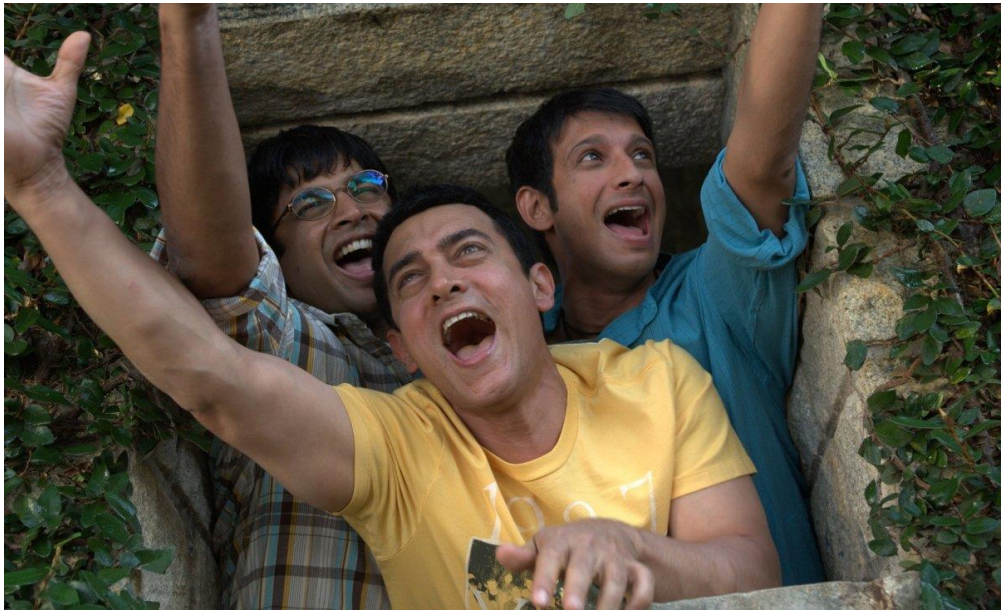
清楚呈現各分項Threat分析結果

建立出一套完整的Threat Modeling review working flow讓PM & SW & PSC三方合作順利



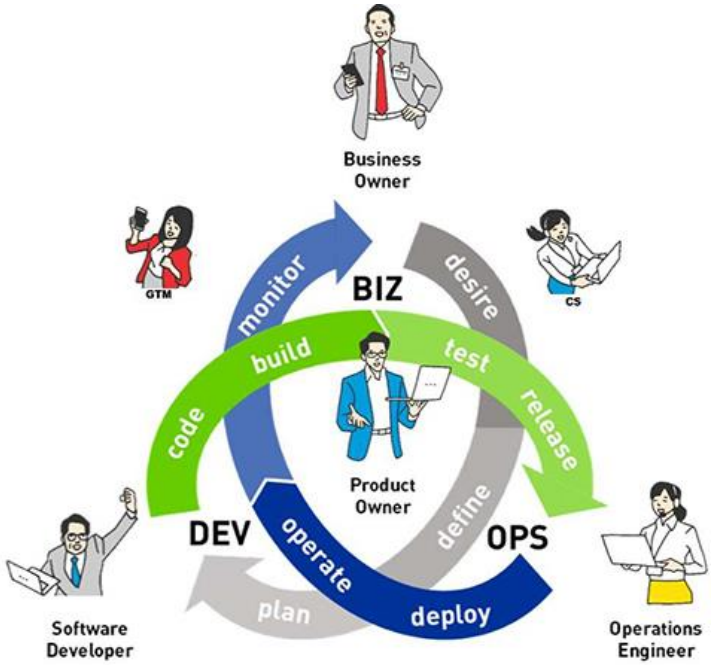
會議日期	完成項目	會議時間(hr)	每小時完成項目
9/13	3	1.5	2.00
9/14	9	2	4.50
9/20	7	1.5	4.67
9/27	15	1.5	10.00
9/29	14	1.5	9.33
10/4	21	2	10.50
10/12	11	1	11.00
10/14	13	1	13.00
10/18	18	1	18.00
10/21	17	1	17.00
10/25	28	1.5	18.67
10/27	37	1	37.00
11/1	31	1	31.00
11/3	12	1	12.00
11/8	23	1.5	15.33
11/10	29	1	29.00
11/15	32	1	32.00

2.6X



平均 1小時完成 24條threat分析
Total 時程預期可在3個月內完成

Summary

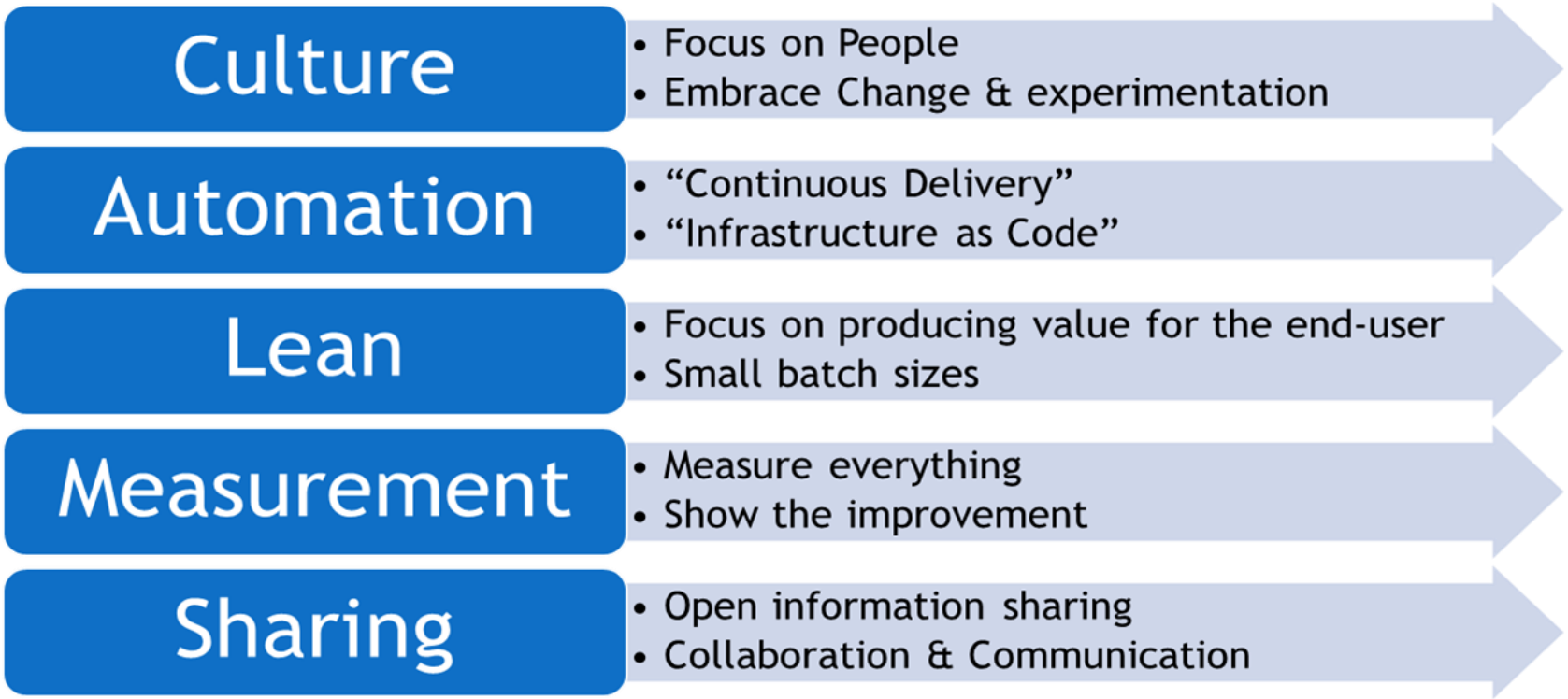


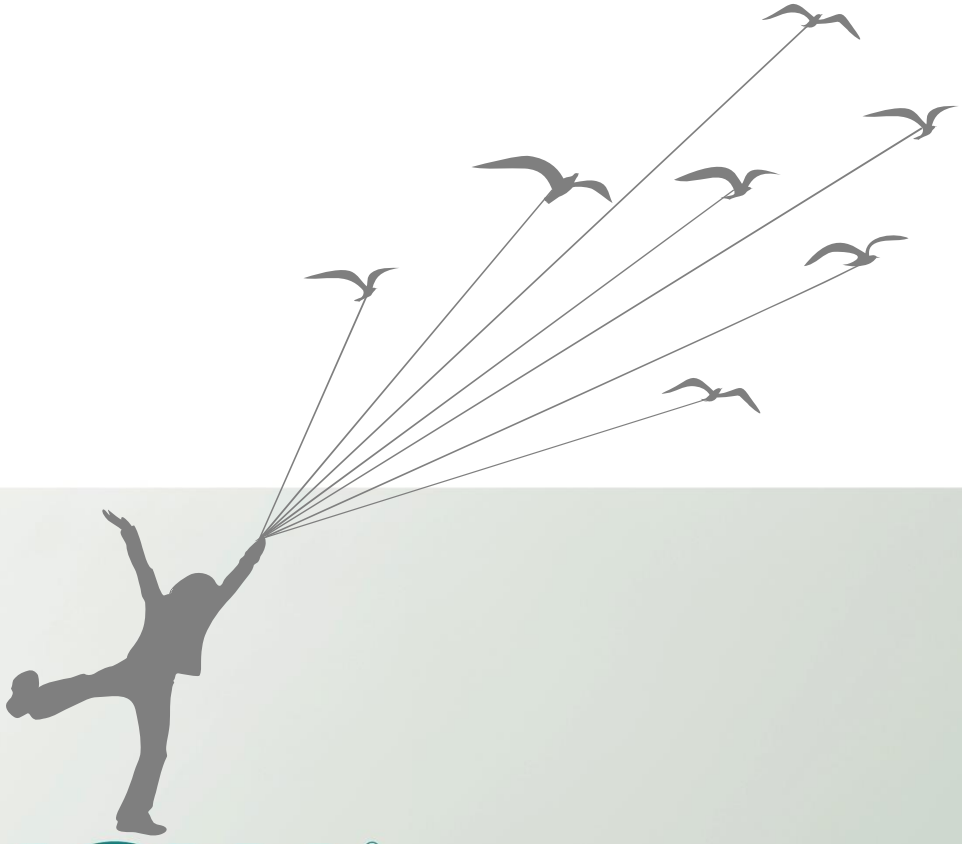
DevOps 開發維運會推動企業創新和持續的流程改善

DevOps 開發維運的實務做法鼓勵將商業價值更快、更妥善且更安全地交付給組織的終端客戶

這項價值的形式可能是更頻繁的產品發佈、功能或更新。 其中可能涉及客戶能取得產品發佈或新功能的速度，而且全部都必須達到適當程度的品質和安全性

C – Culture
A – Automation
L – Lean
M – Measurement
S – Sharing


Culture
• Focus on People
• Embrace Change & experimentation
Automation
• “Continuous Delivery”
• “Infrastructure as Code”
Lean
• Focus on producing value for the end-user
• Small batch sizes
Measurement
• Measure everything
• Show the improvement
Sharing
• Open information sharing
• Collaboration & Communication



Thank You

MOXA®

Reliable Networks ▲ Sincere Service