FORTINET

Secure OT Summit 2022

護航 OT/IT 融合 創新數位發展

從營運策略思考資訊安全

王蜀英 Kernel Wang

Siemens 智慧基礎建設 維護處 協理

從運營策略思考資訊安全

王蜀英 維護處 協理
西門子股份有限公司
智慧基礎建設

SIEMENS

綱要

1. 前言
2. One breaching system case
3. Experienced cases of CyberSecurity
4. 省思
5. 對策

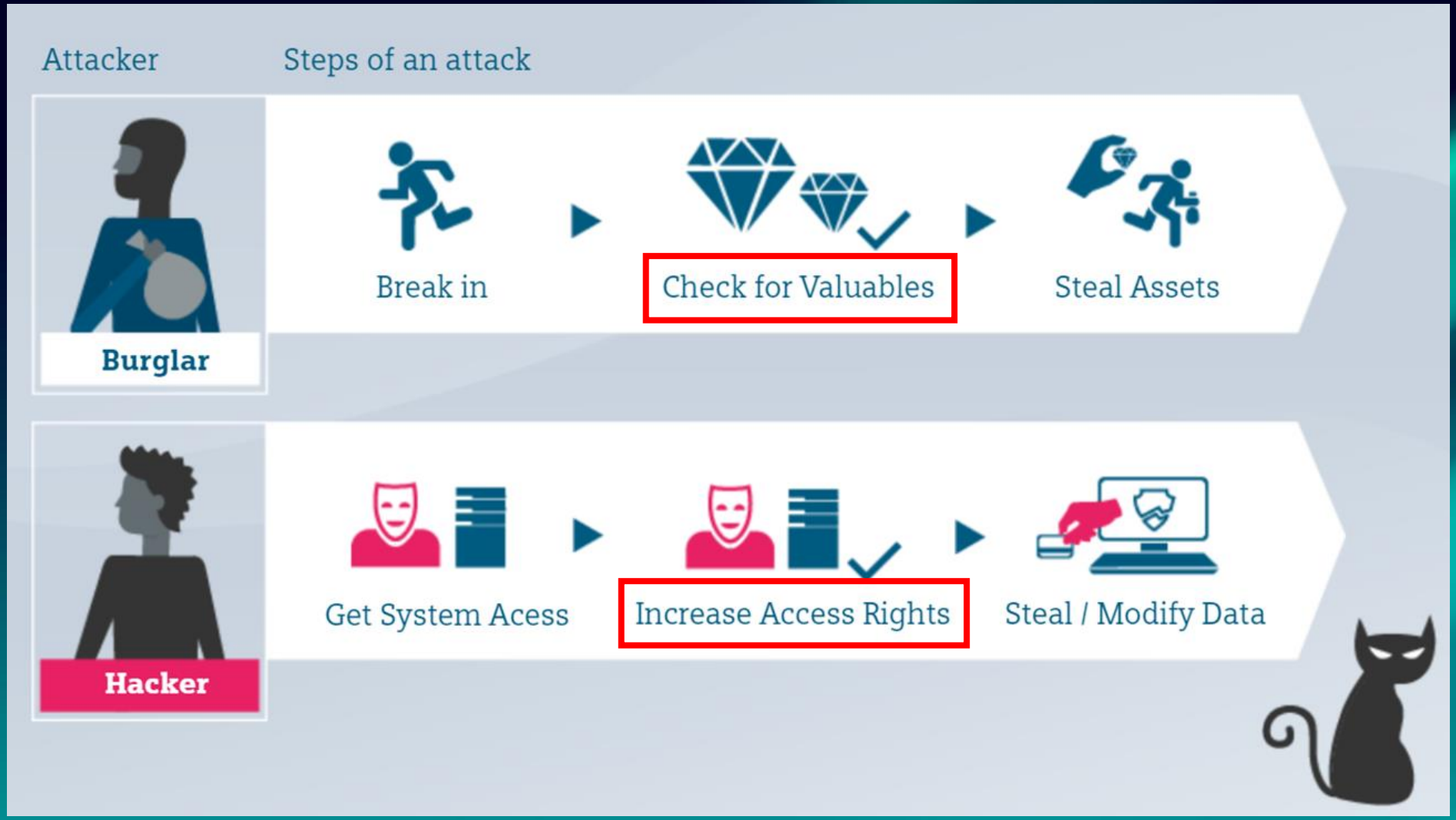
SIEMENS

前言

- 安全，以管理為基礎；管理，以人為基礎。
- Security vs. Cybersecurity

SIEMENS

Approach to breaching a system



SIEMENS

One breaching system case

SIEMENS

Experienced cases of CyberSecurity

1. Y2K - 千禧年危機
2. 2015 Ukraine Power Hack
3. 2017 WannaCry Attack

SIEMENS

Y2K - 千禧年危機

- 是指由於電腦程式設計的一些問題，使得電腦在處理2000年1月1日以後的日期和時間時，可能會出現不正確的操作，從而可能導致一些敏感的工業部門（比如電力，能源）和銀行，政府等部門在2000年1月1日零點工作停頓甚至是發生災難性的結果。 摘錄自維基百科

SIEMENS

2015 Ukraine Power Hack

- BlackEnergy 的最新完整版本(BE3)出現在 2014 年，於2015 年 12 月 23 日，烏克蘭電網遭到黑客攻擊，導致烏克蘭約 23 萬用戶斷電1-6 小時，即為BE3所致。
- 分散式阻斷服務攻擊（distributed denial-of-service attack，简称DDoS)，是一種網路攻擊手法，其目的在於使目標電腦的網路或系統資源耗盡，使服務暫時中斷或停止，導致其正常使用者無法存取。 當駭客使用網路上兩個或以上被攻陷的電腦作為「殭屍」向特定的目標發動「阻斷服務」式攻擊時，稱為分散式阻斷服務攻擊亦稱洪水攻擊。據2014年統計，被確認為大規模DDoS的攻擊已達平均每小時28次。摘錄自維基百科

SIEMENS

2015 Ukraine Power Hack

Step 1

Spearphising and **infection** of an office laptop with the **„BlackEnergy" malware.**

Step 2

Network scans in the **IT network** from the infected laptop. They found a **connection** to an **OT supervision platform.**

SIEMENS

2017 WannaCry Attack

- WannaCry是一種利用NSA的「永恆之藍」漏洞利用程式透過網際網路對全球執行Microsoft Windows作業系統的電腦進行攻擊的加密型勒索軟體兼蠕蟲病毒。該病毒利用AES-128和RSA演算法惡意加密使用者檔案以勒索比特幣。
- 永恆之藍（英語：EternalBlue）是美國國家安全局(NSA)開發的漏洞利用程式，於2017年4月14日被黑客組織影子掮客洩漏。

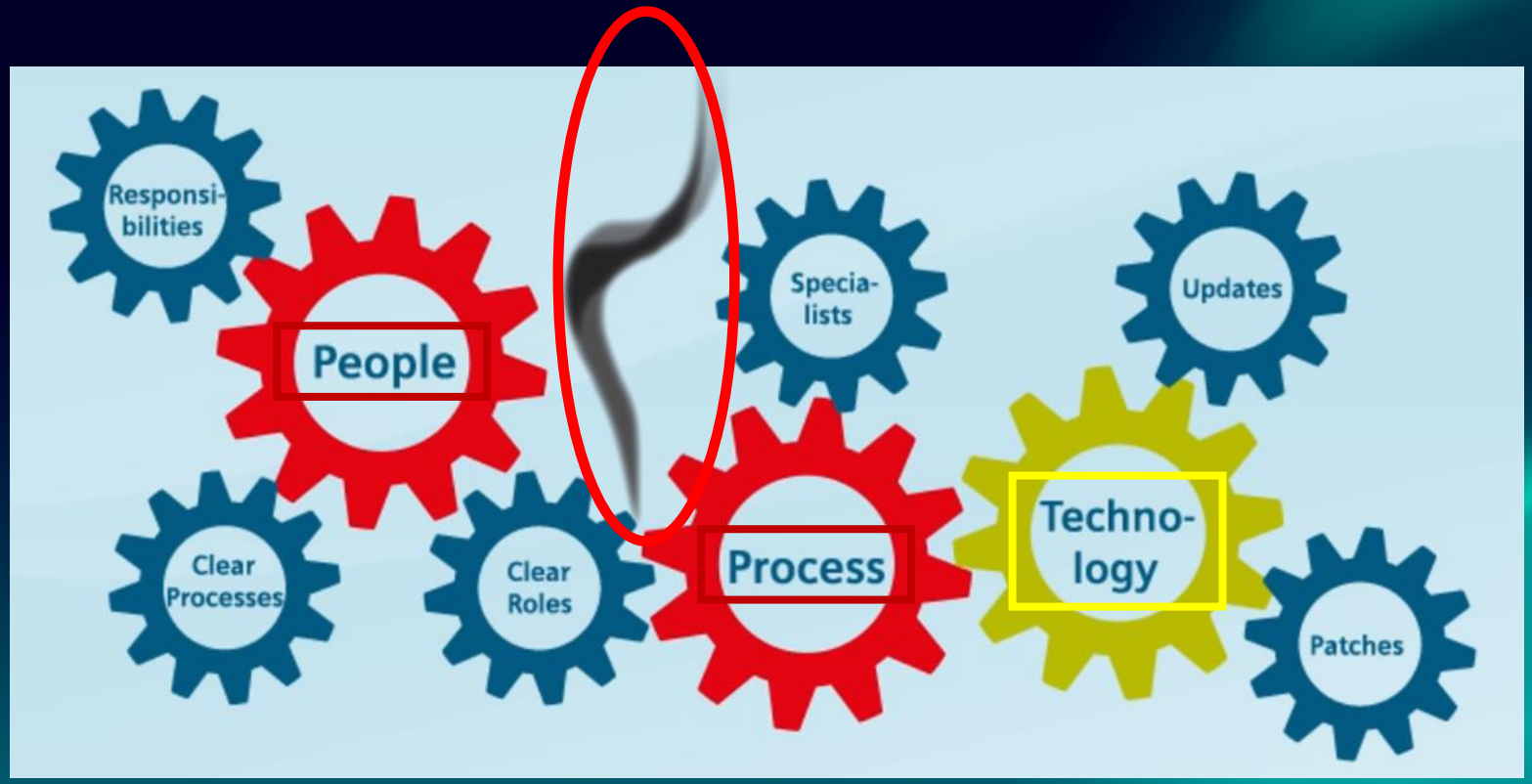
摘錄自維基百科

SIEMENS

2017 WannaCry Attack

SIEMENS

省思

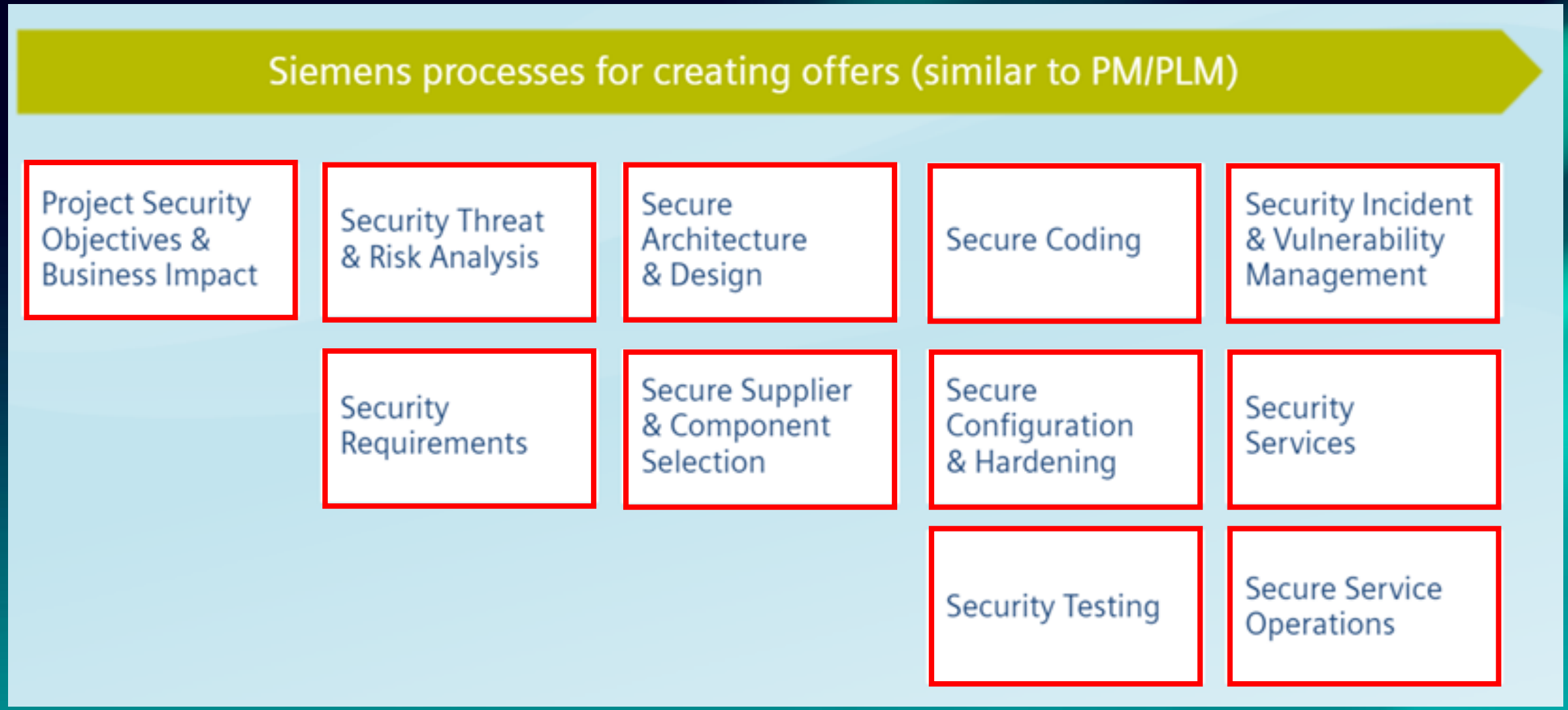


Security needs to be addressed at the beginning of product development.

The Security Threat & Risk Analysis (TRA) is the basis of systematic security risk management and is performed along the lifecycle. The aim is to ensure "security by design" and to hand over products and solutions that are securely configured and hardened.

SIEMENS

對策


Siemens processes for creating offers (similar to PM/PLM)
Project Security Objectives & Business Impact
Security Threat & Risk Analysis
Secure Architecture & Design
Secure Coding
Security Incident & Vulnerability Management
Security Requirements
Secure Supplier & Component Selection
Secure Configuration & Hardening
Security Services
Security Testing
Secure Service Operations

SIEMENS

選擇解決方案的條件

- Availability (or Reliability)
- Scalability
- Total Cost Ownership (or compatibility)

SIEMENS

結語

- 從產品(軟/硬體)設計開始，就必須導入Cybersecurity。
- 必須定期檢討Cybersecurity的管理流程與人員遵循的整合程度。
- 必須要認知Cybersecurity常態化的事實。

SIEMENS

感謝聆聽!

Secure OT Summit 2022

護航 OT/IT 融合 創新數位發展