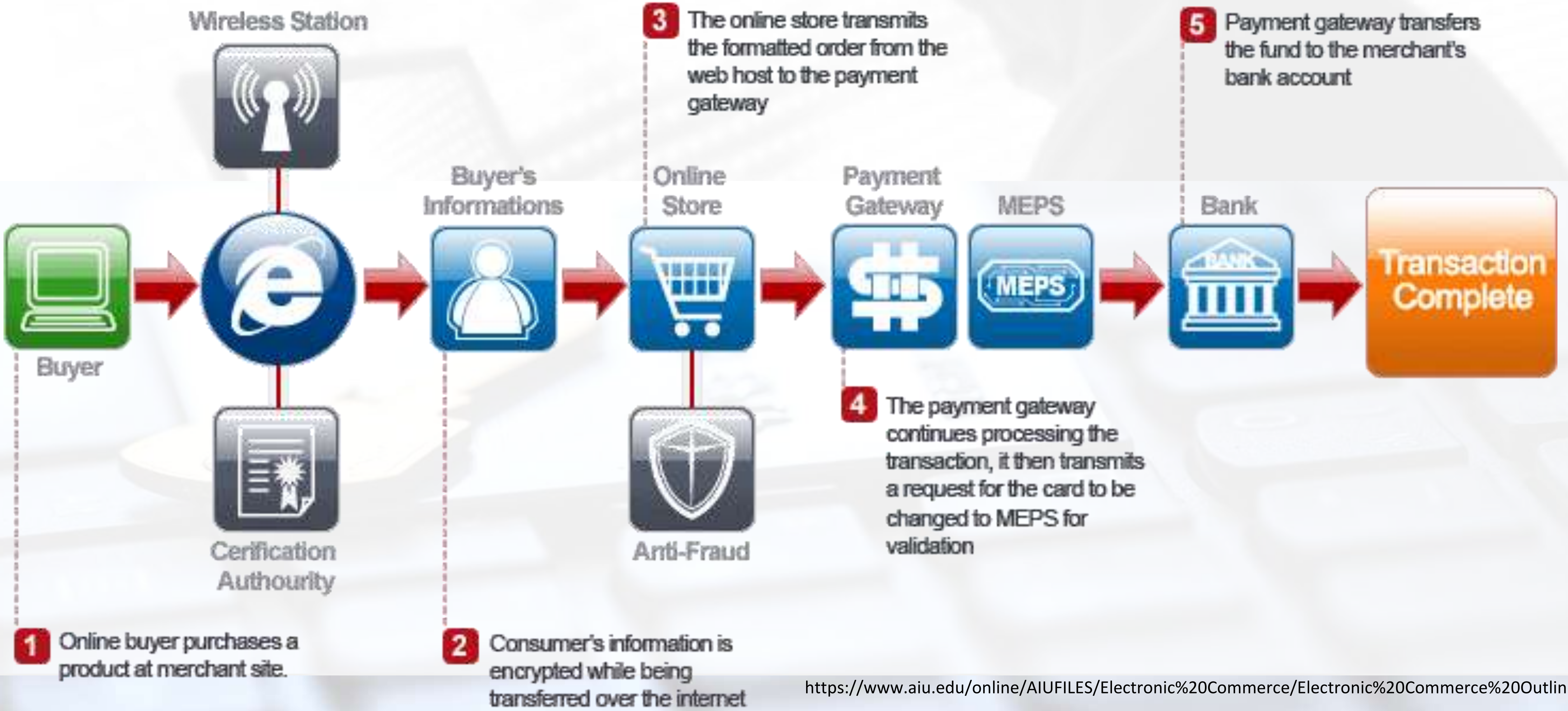
工業技術研究院
Industrial Technology
Research Institute

電子商務 － 主動安全防禦

卓傳育 博士

資料中心系統軟體組
資訊與通訊研究所

E-commerce Security



1 Online buyer purchases a product at merchant site.

2 Consumer's information is encrypted while being transferred over the internet

3 The online store transmits the formatted order from the web host to the payment gateway

4 The payment gateway continues processing the transaction, it then transmits a request for the card to be changed to MEPS for validation

5 Payment gateway transfers the fund to the merchant's bank account

https://www.aiu.edu/online/AIUFILES/Electronic%20Commerce/Electronic%20Commerce%20Outline.html

Six Dimensions of E-commerce Security

1. **Integrity**: prevention against unauthorized data modification
2. **Nonrepudiation**: prevention against any one party from reneging on an agreement after the fact
3. **Authenticity**: authentication of data source
4. **Confidentiality**: protection against unauthorized data disclosure
5. **Privacy**: provision of data control and disclosure
6. **Availability**: prevention against data delays or removal

https://www.techgenyz.com/2017/04/05/e-commerce-major-threats-e-commerce-security/

http://www.uky.edu/~dsianita/390/390wk4.html

E-commerce Threats

1. Client computer threats
   - Trojan horse
   - Active contents
   - Viruses
3. Communication channel threats
   - Sniffer program
   - Backdoor
   - Spoofing
   - Denial-of-service
4. Server threats
   - Privilege setting
   - Server Side Include (SSI), Common Gateway Interface (CGI)
   - File transfer
   - Spamming

Countermeasure / Defense Mechanisms

- 1. Client computer protection
  - Privacy -- Cookie blockers; Anonymizer
  - Digital certificate
  - Browser protection
  - Antivirus software
  - Computer forensics expert
- 2. Communication channel protection
  - Encryption
    - * Public-key encryption vs Private-key encryption
    - * Encryption standard: Data Encryption Standard (DES), Advanced Encryption Standard (AES)
  - Protocol
    - * Secure Sockets Layer (SSL)
    - * Secure HyperText Transfer Protocol (HTTPS)
  - Digital signature

    Bind the message originator with the exact contents of the message
- 3. Server protection
  - Access control and authentication
    - * Digital signature from user
    - * Username and password
    - * Access control list
  - Firewalls

    International Computer Security Association's classification:
    - * Packet filter firewall
    - * Application level proxy server
    - * Stateful packet inspection

電子商務安全規範

101 年度電子商務交易安全及資安服務平台推動計畫

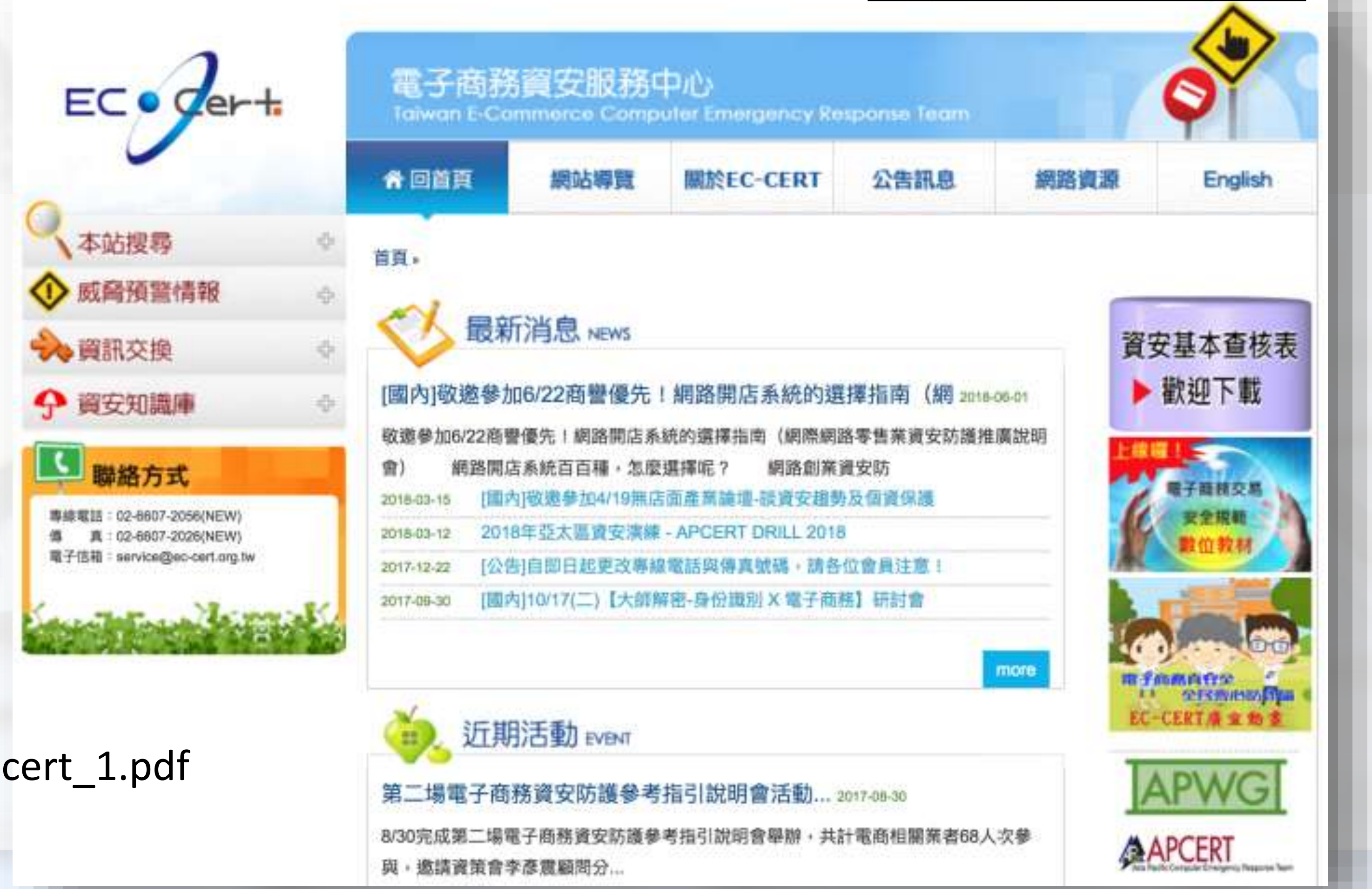
電子商務交易安全規範
(網路平台、供應商、物流商)修正版

財團法人資訊工業策進會編製

中華民國 101 年 11 月

http://www.cnra.org.tw/edm/ec-cert_1.pdf

http://ec-cert.org.tw/



聯絡方式

專線電話：02-6607-2056(NEW)
傳　　真：02-6607-2026(NEW)
電子信箱：service@ec-cert.org.tw

最新消息 NEWS

[國內]敬邀參加6/22商譽優先！網路開店系統的選擇指南（網 2018-06-01

敬邀參加6/22商譽優先！網路開店系統的選擇指南（網際網路零售業資安防護推廣說明會）　網路開店系統百百種，怎麼選擇呢？　網路創業資安防

2018-03-15	[國內]敬邀參加4/19無店面產業論壇-談資安趨勢及個資保護
2018-03-12	2018年亞太區資安演練 - APCERT DRILL 2018
2017-12-22	[公告]自即日起更改專線電話與傳真號碼，請各位會員注意！
2017-08-30	[國內]10/17(二)【大師解密-身份識別 X 電子商務】研討會

近期活動 EVENT

第二場電子商務資安防護參考指引說明會活動... 2017-08-30

8/30完成第二場電子商務資安防護參考指引說明會舉辦，共計電商相關業者68人次參與，邀請資策會李彥震顧問分...

How to Minimize Security Threats

1. Perform a risk assessment → a list of information assets and their value to the firm

2. Develop a security policy → a written statement on:

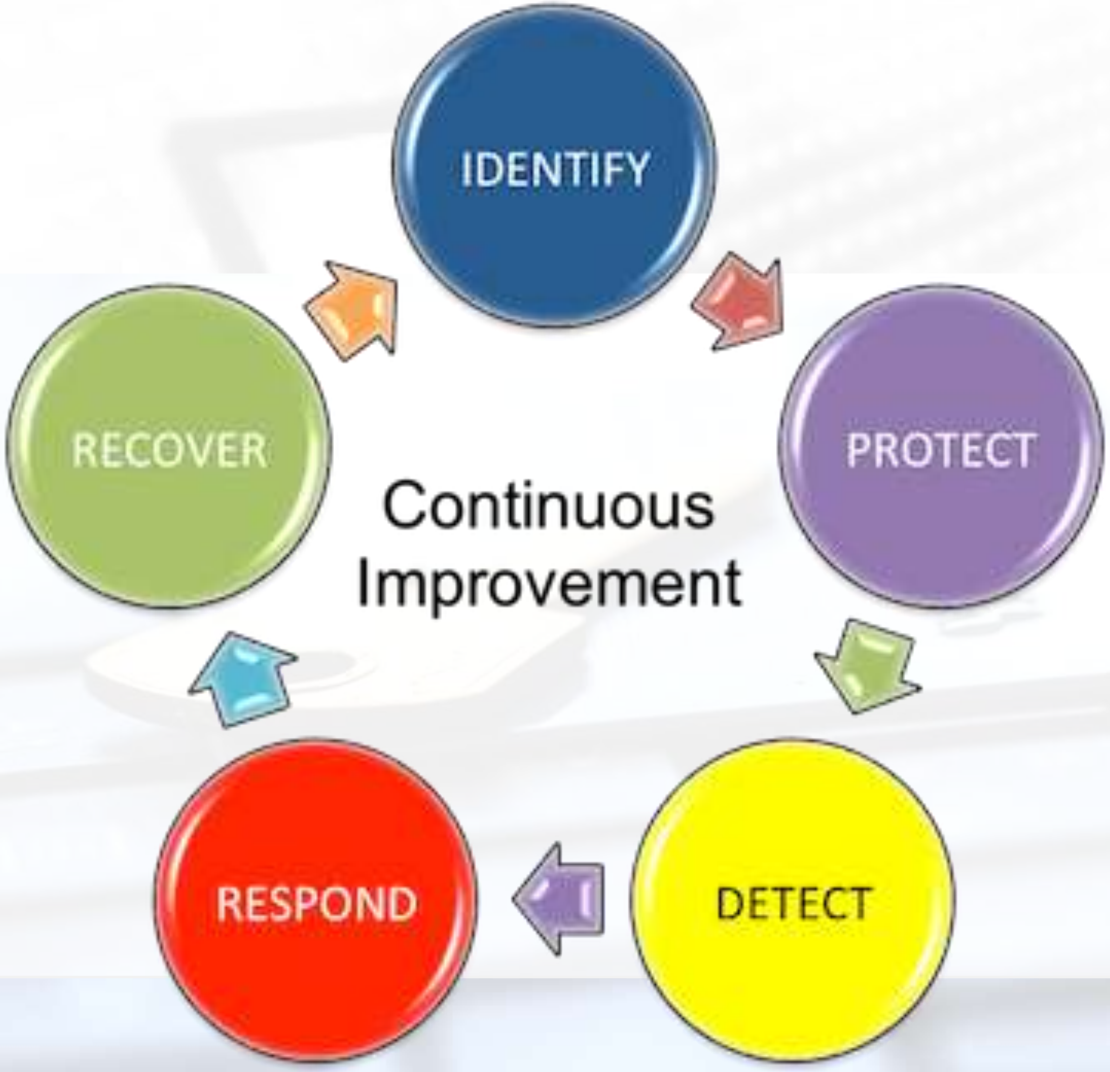
   * what assets to protect from whom?
   * why these assets are being protected?
   * who is responsible for what protection?
   * which behaviors are acceptable and unacceptable?

3. Develop an implementation plan → a set of action steps to achieve security goals

4. Create a security organization → a unit to administer the security policy

5. Perform a security audit → a routine review of access logs and evaluation of security procedures

NIST Cyber Security Framework



<u>Risk Assetment</u>

1. Integrity
2. Nonrepudiation
3. Authenticity
4. Confidentiality
5. Privacy
6. Availability

- ISO 27001
- ISO 27002

Trends Shaping E-Commerce

Looking Ahead
to the Future of
E-Commerce
Security
https://www.verifi.com/in-the-news/looking-ahead-future-e-commerce-security/

- **Automated return process.** This solves one of the lingering problems with e-commerce – buying products sight unseen. An automated return process can limit chargebacks and friendly fraud along with enhancing customer satisfaction. Update your return/refund policy to respond best to the way customers are shopping and buying.
- **M-commerce adoption.** The m-commerce sales numbers are only increasing, which highlights the need for merchants to shift focus to a seamless and secure mobile app experience. Brand loyalty depends on a successful customer experience.
- **Personalization.** Virtual assistants, instant messaging marketing, and customized page display. Customers want the brick-and-mortar personalization experience extended to their m-commerce and e-commerce shopping.
- **Customer insecurity.** Today's customers know the risks of e-commerce, the threat of fraud and data breaches. Customers must have confidence in merchant payments security. Remind customers that password requirements and security measures are for their benefit.
- More and more customers are "preview shopping" online before visiting a brick-and-mortar store. The omnichannel experience gives merchants the chance to capture customers both in-store and online. However, it all comes down to providing customers a truly personalized, dynamic, secure, and customer-friendly shopping experience.

https://www.verifi.com/in-the-news/looking-ahead-future-e-commerce-security/

E-Commerce Security of the Future

- **Verified by Visa in 2018**. In April 2018, Visa is making changes to its Verified by Visa program to phase out static passwords and problems with its enrollment process. These changes are being made to address threats to customer security.
- **Mastercard Identity Check**. Often referred to as selfie pay – Mastercard allows customers to verify their identity with a photo of their face or a digital fingerprint. Purchase speed and authentication happens immediately, giving merchants and customers what they want.
- **Real-time security**. The customer transaction happens instantly, requiring merchants to provide real-time verification and authentication. This depends on completing back-end fraud and authentication checks while the customer is browsing and adding items to their cart.
- **General Data Protection Regulation (GDPR)**. In May 2018, GDPR replaces the EU Data Protection Act. This legislation places new demands on merchant responsibility for data security.
- **Multilayered intelligence**. Multilayered intelligence extends to merchant-customer knowledge and using the right security solution at the right time. The guessing is eliminated with a multilayered approach.

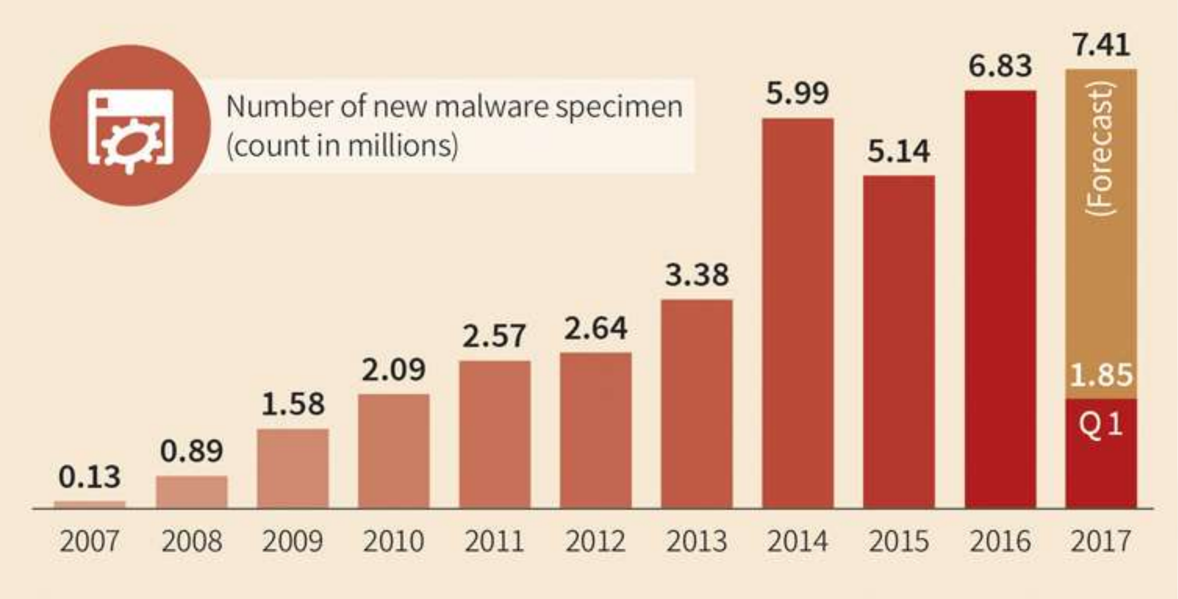
https://www.verifi.com/in-the-news/looking-ahead-future-e-commerce-security/

Do Not Stand Still

- If there is one thing we know for sure, it is this: change is coming and it’s coming fast. Merchants must be ready to evolve and anticipate customer demands and fraudster threats. The proactive approach is a must. This means acting today to be ready for tomorrow.
- Know that the tools, technologies, and expertise are available to you. It’s time to take the first move and be ready to seize the opportunities of e-commerce in 2018.

主動安全防禦

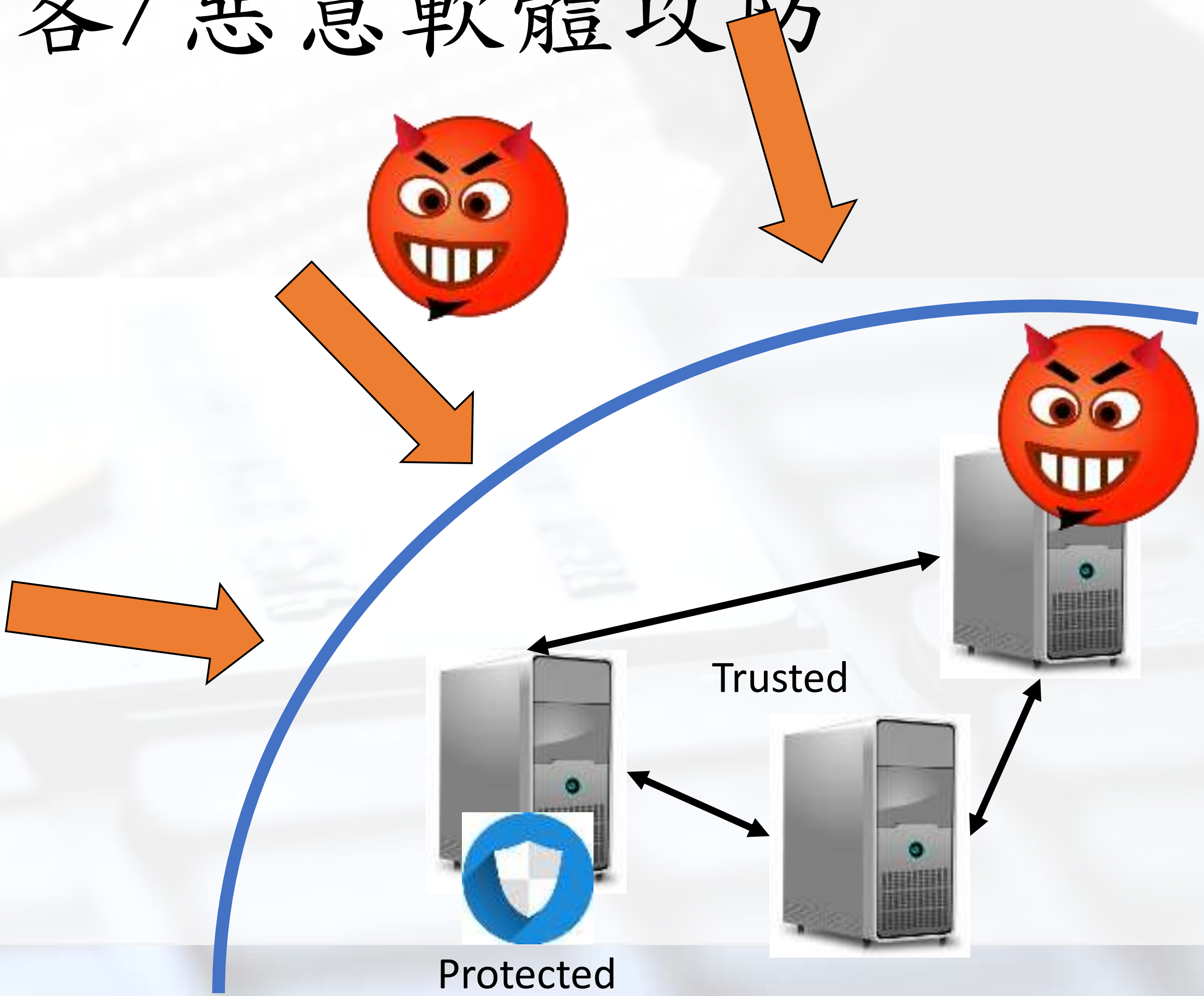
越來越多的惡意程式，防毒軟體難以對抗



資料來源: Malware Trend 2017, G-Data Security blog, https://blog.gdatasoftware.com/2017/04/29666-malware-trends-2017

- 需要更嚴格的端點保護
  - 將惡意攻擊全部擋住是幾乎不可能的

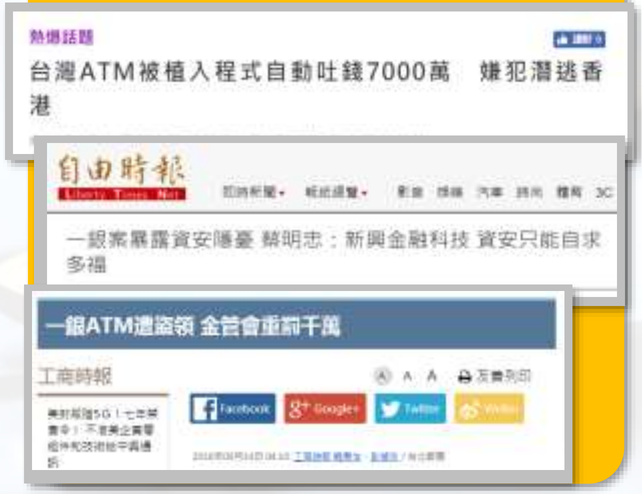
無孔不入的駭客/惡意軟體攻防



台灣二度淪陷 駭客搶銀行

第一銀行

第一銀行在105年7月10日凌晨，於臺北及臺中市合計22家分行41台ATM提款機遭清空，車手在不需要提款卡、帳號密碼、在沒有接觸到提款機的情況下，提款機自動開啟吐鈔口，並將提款機內存放現金全部吐出，累積遭盜走現金新臺幣8千萬餘元。



熱爆話題

台灣ATM被植入程式自動吐錢7000萬 嫌犯潛逃香港

自由時報 Liberty Times Net

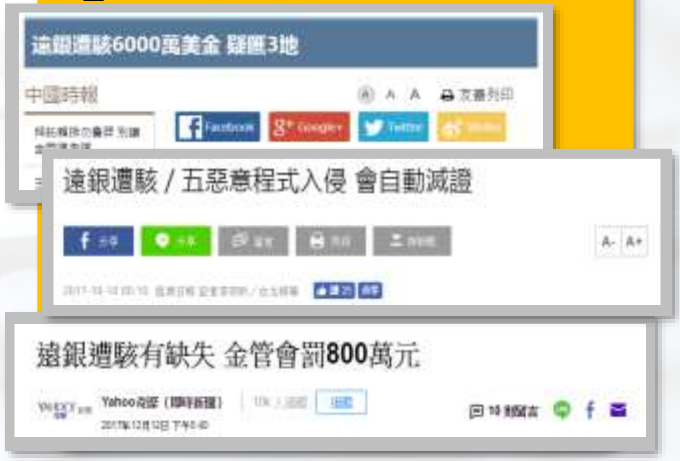
一銀案暴露資安隱憂 蔡明志：新興金融科技 資安只能自求多福

一銀ATM遭盜領 金管會重罰千萬

工商時報

遠東商銀

遠東商銀於106年10月3日上午發現電腦遭到惡意程式攻擊，駭客假冒遠銀名義透過SWIFT(環球銀行金融電信協會)組織系統發出7個電文，使遠銀境外分行之外幣帳戶依據電文內容，執行付款至斯里蘭卡、柬埔寨及美國等地銀行帳戶，遭駭金額計有美金6,010萬4,000元，折合新臺幣約18億餘元



遠銀遭駭6000萬美金 疑匯3地

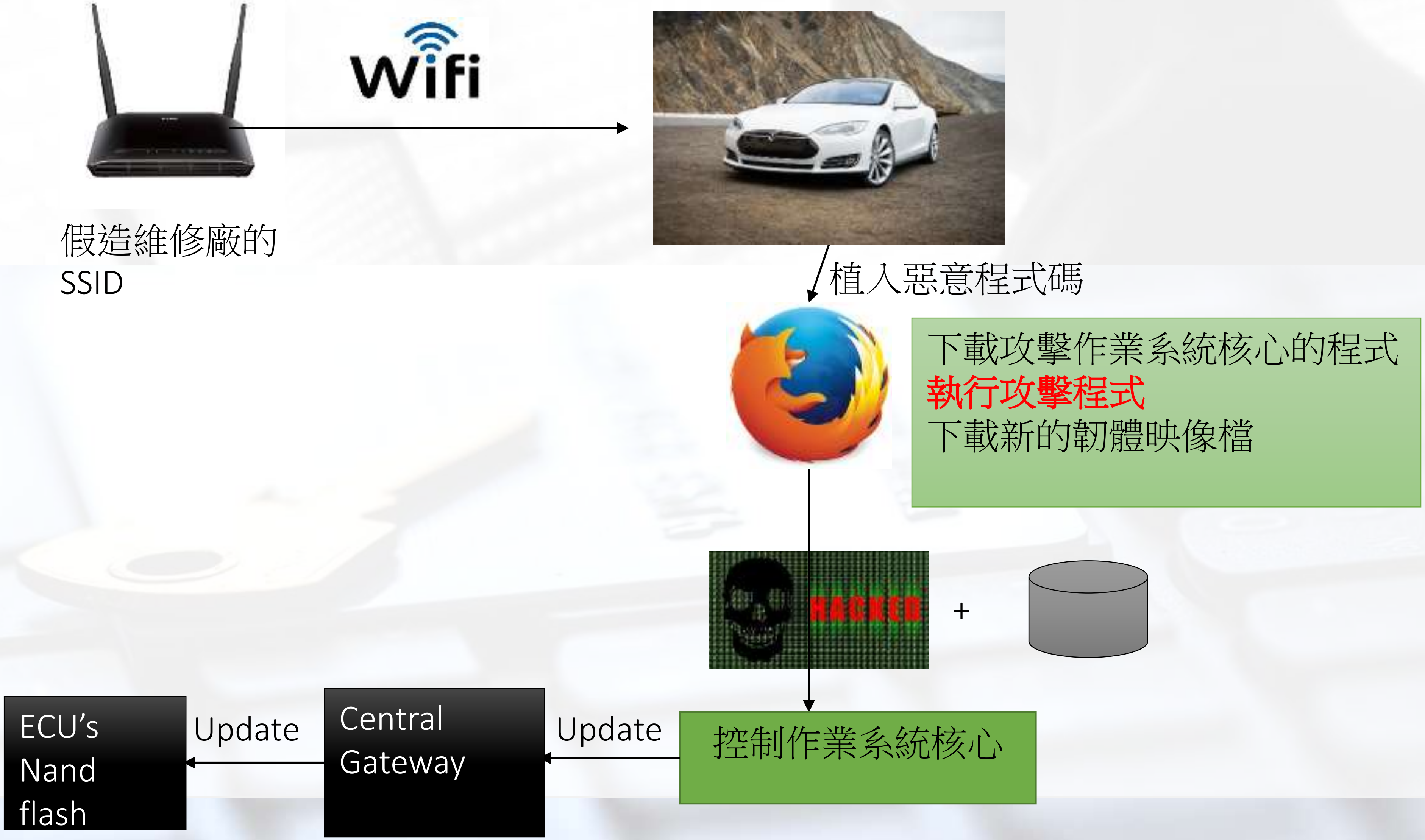
中國時報

遠銀遭駭／五惡意程式入侵 會自動滅證

遠銀遭駭有缺失 金管會罰800萬元

Yahoo奇摩（即時新聞）

車載資安 – Keen Lab 入侵 Tesla



假造維修廠的
SSID

植入惡意程式碼

下載攻擊作業系統核心的程式
執行攻擊程式
下載新的韌體映像檔

+

控制作業系統核心

Update

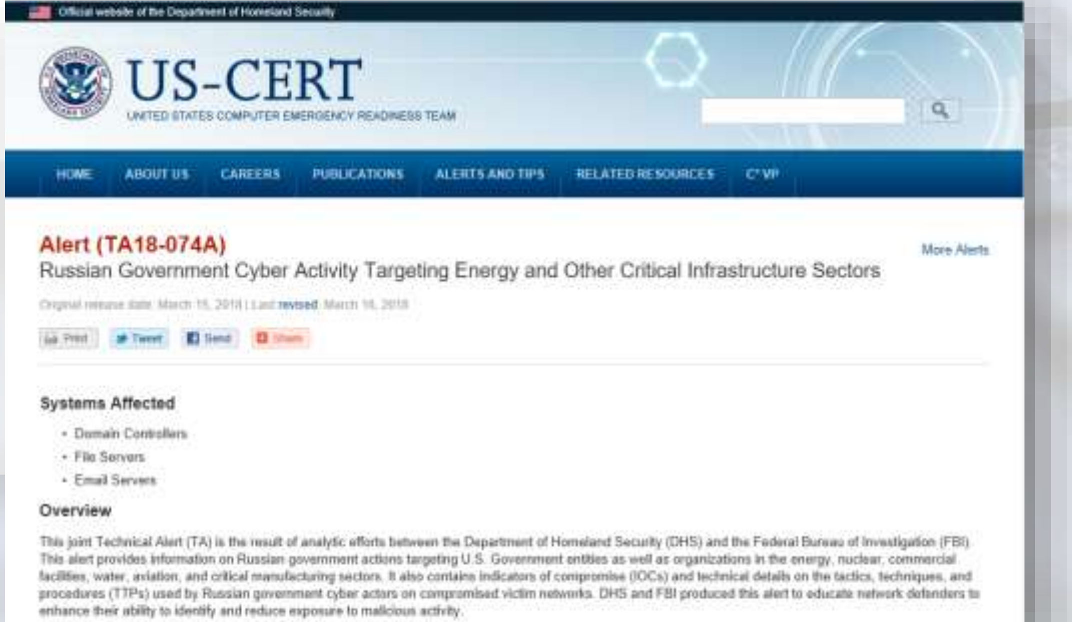
Central
Gateway

Update

ECU's
Nand
flash

Russia hacked the US electric grid

- The Russian hackers used **decades-old** tactics to gain access
  - Stage 1: Reconnaissance
    - 感染外部網站，鎖定目標攻擊
    - 低資安管理承包商
  - Stage 2: Weaponization
    - Email社交攻擊
    - 水坑攻擊
  - Stage 3: Delivery
  - Stage 4: Exploitation
  - Stage 5: Installation
    - **Establishing Local Accounts: symantec_help.jsp**
    - **enu.cmd**
      - netsh firewall set opmode disable
      - netsh advfirewall set allprofiles state off
      - …



Alert (TA18-074A)

Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors

Original release date: March 15, 2018 | Last revised: March 16, 2018

Systems Affected

- Domain Controllers
- File Servers
- Email Servers

Overview

This joint Technical Alert (TA) is the result of analytic efforts between the Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI). This alert provides information on Russian government actions targeting U.S. Government entities as well as organizations in the energy, nuclear, commercial facilities, water, aviation, and critical manufacturing sectors. It also contains indicators of compromise (IOCs) and technical details on the tactics, techniques, and procedures (TTPs) used by Russian government cyber actors on compromised victim networks. DHS and FBI produced this alert to educate network defenders to enhance their ability to identify and reduce exposure to malicious activity.

“We think that by far the most effective mitigation work that we’ve seen on the Android platform over the last three years has been the investment in attack surface reduction. The deployment and tightening of selinux policies and the addition of seccomp sandboxing both result in an attacker needing to find more vulnerabilities in a smaller attack surface.”

Mark Brand - Google Project Zero

Jeff Vander Stoep and Sami Tolvanen

Android Kernel Security

Linux Security Summit Aug 2018

android

Access controls are "hard" mitigations which can be applied without knowledge of exploitation techniques.

BAKER HUGHES a GE company

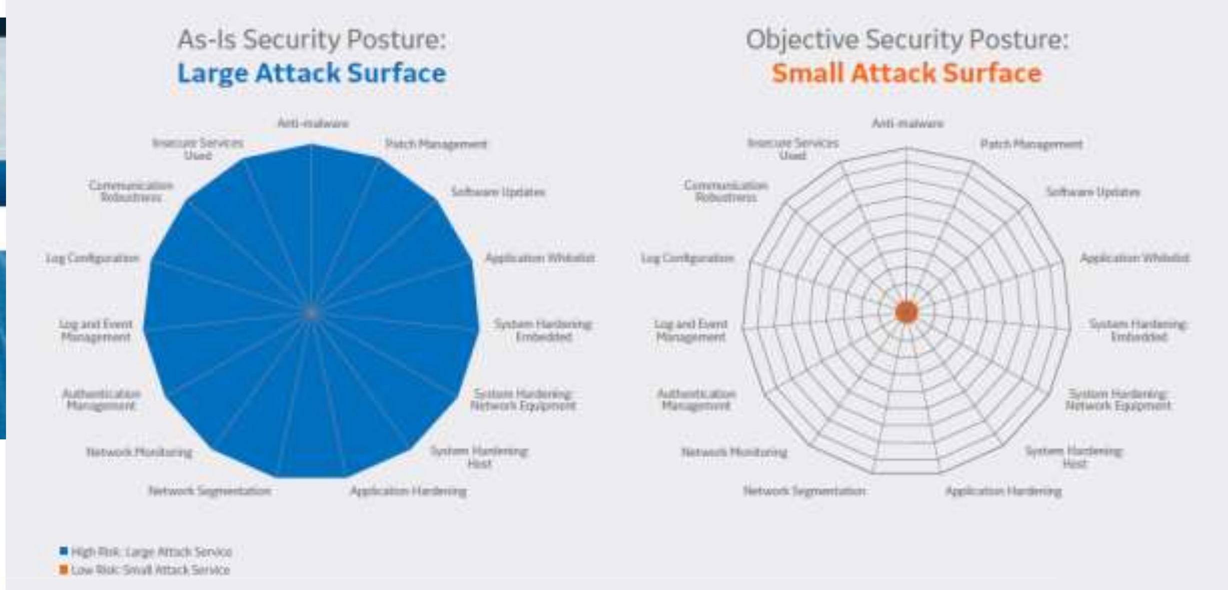
Seven Strategies for Defending Industrial controls

Official website of the Department of Homeland Security

ICS-CERT

INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

The National Cybersecurity and Communications Integration Center (NCCIC) is the Nation's flagship cyber defense, incident response, and operational integration center. Our mission is to reduce the Nation's risk of systemic cybersecurity and communications challenges.



As-Is Security Posture: **Large Attack Surface**

Objective Security Posture: **Small Attack Surface**

7

NUMBER OF STRATEGIES

recommend by ICS-CERT to mitigate top cyber threats.

243

AVERAGE NUMBER OF DAYS

before detection that a system is compromised.

10/12

THE NUMBER OF SOFTWARE PATCHES TESTED MONTHLY

in the BHGE Validation Lab that require modifications to ensure no negative effect on operations.

26%

OF INCIDENTS

investigated by ICS-CERT were spear phishing, making it the leading threat for 2016.

74%

OF EXPLOITS

are targeted at applications, with more than 40% of those being Microsoft & Adobe.

98%

NUMBER OF INCIDENTS

ICS-CERT responded to in FY2014 and FY2015 that would have been prevented using the Seven Strategies.

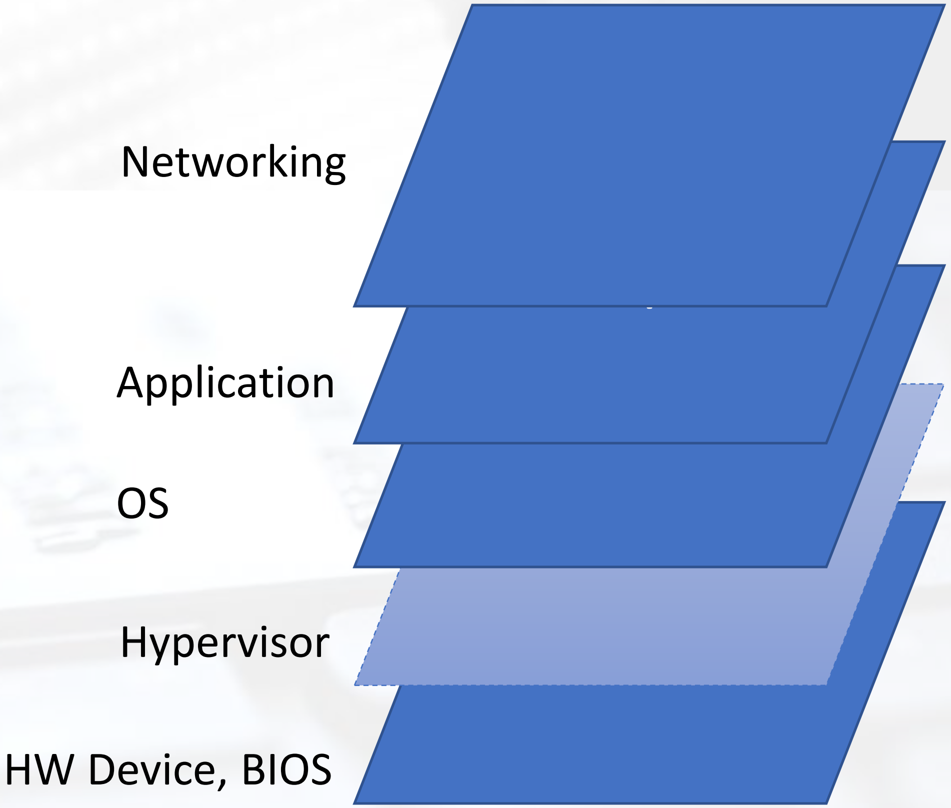
SecurityST addresses ALL 7 STRATEGIES

Percentages represent the number of ICS-CERT reported incidents in 2014 and 2015 that would have been prevented using that specific strategy.

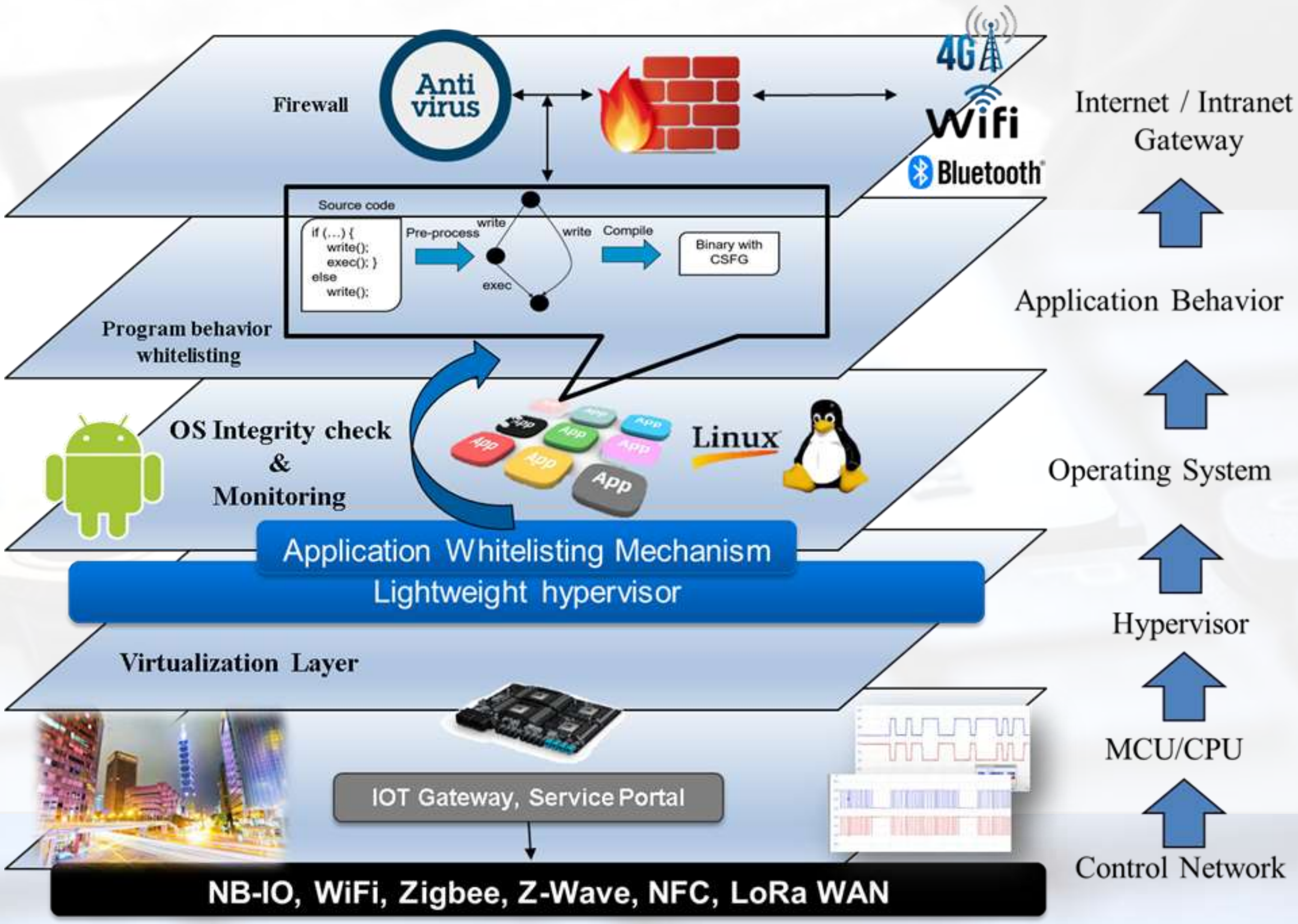
38%	APPLICATION WHITELISTING
29%	PROPER CONFIGURATION/ PATCH MANAGEMENT
17%	REDUCE YOUR ATTACK SURFACE
9%	BUILD A DEFENDABLE ENVIRONMENT
4%	MANAGE AUTHENTICATION
2%	MONITOR AND RESPOND
1%	SECURE REMOTE ACCESS

基於白名單概念的安全系統設計架構

- 網路白名單
- 程式行為白名單
- 作業系統
  - 使用者帳戶白名單
  - 存取資源權限控管白名單
  - 應用程式執行白名單
- 虛擬化管理層
  - 作業系統核心攻擊
- 硬體,CPU, BIOS
  - CPU flaw, Cache incoherence



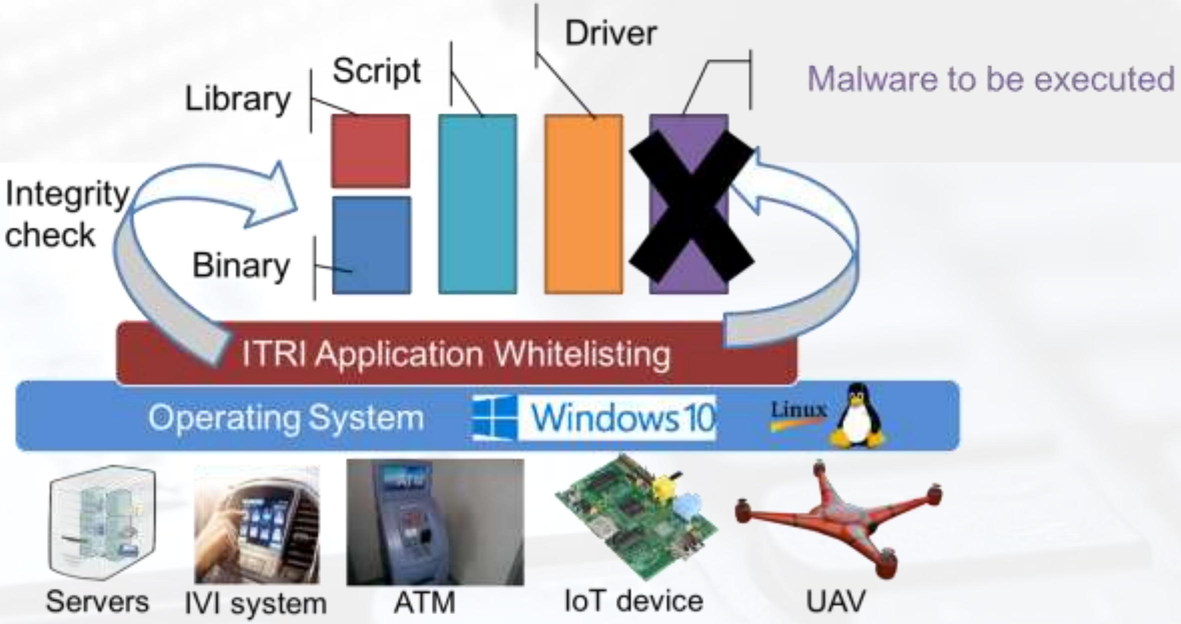
多層次應用程式白名單防護架構



安全執行平台

- 針對 Windows / Linux 提供白名單保護，程式將執行時，攔截並檢查程式完整性

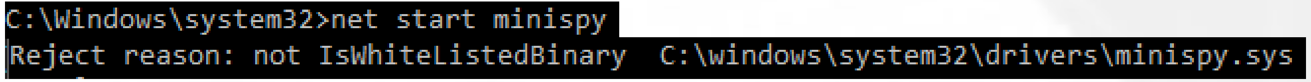
- 檢查類型
  - Executable
  - DLL / shared object
  - Script
  - Kernel driver



- 二階段驗證更新、安裝
  - 應用程式安裝、更新與白名單資料庫更新去耦合化
  - 自動更新時，紀錄寫入的 Executables

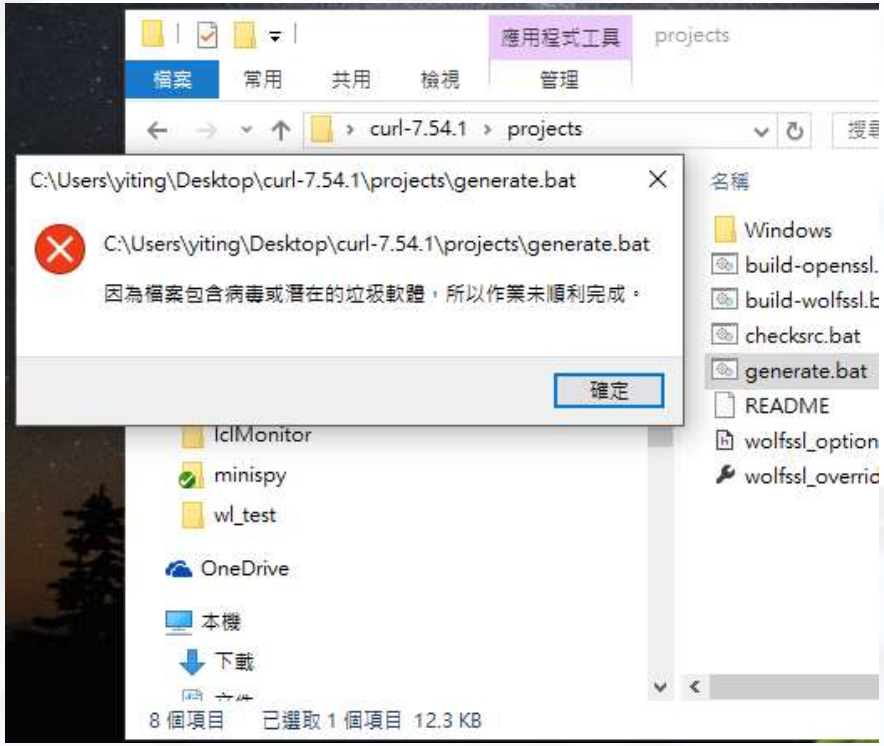
阻擋執行!

Execute Driver



```
C:\Windows\system32>net start minispy
Reject reason: not IsWhiteListedBinary  C:\windows\system32\drivers\minispy.sys
```

Execute script

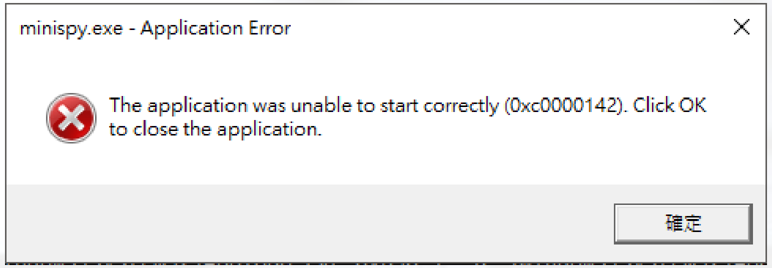


C:\Users\yiting\Desktop\curl-7.54.1\projects\generate.bat

C:\Users\yiting\Desktop\curl-7.54.1\projects\generate.bat

因為檔案包含病毒或潛在的垃圾軟體，所以作業未順利完成。

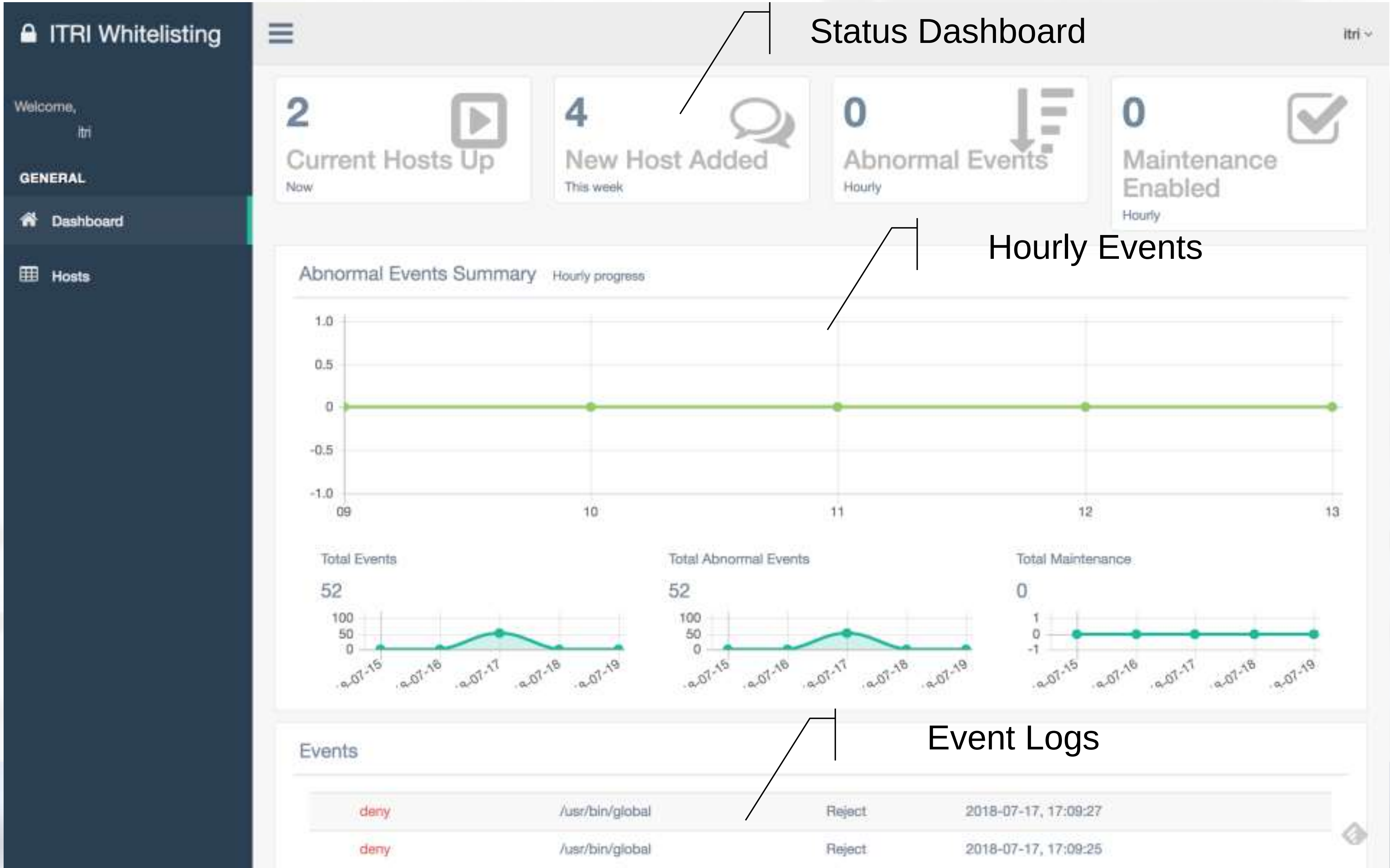
Execute EXE



minispy.exe - Application Error

The application was unable to start correctly (0xc0000142). Click OK to close the application.

遠端控制介面 – Dashboard



ITRI Whitelisting

Welcome,
itri

GENERAL

Dashboard

Hosts

itri

2
Current Hosts Up
Now

4
New Host Added
This week

0
Abnormal Events
Hourly

0
Maintenance Enabled
Hourly

Abnormal Events Summary Hourly progress

Total Events
52

Total Abnormal Events
52

Total Maintenance
0

Events

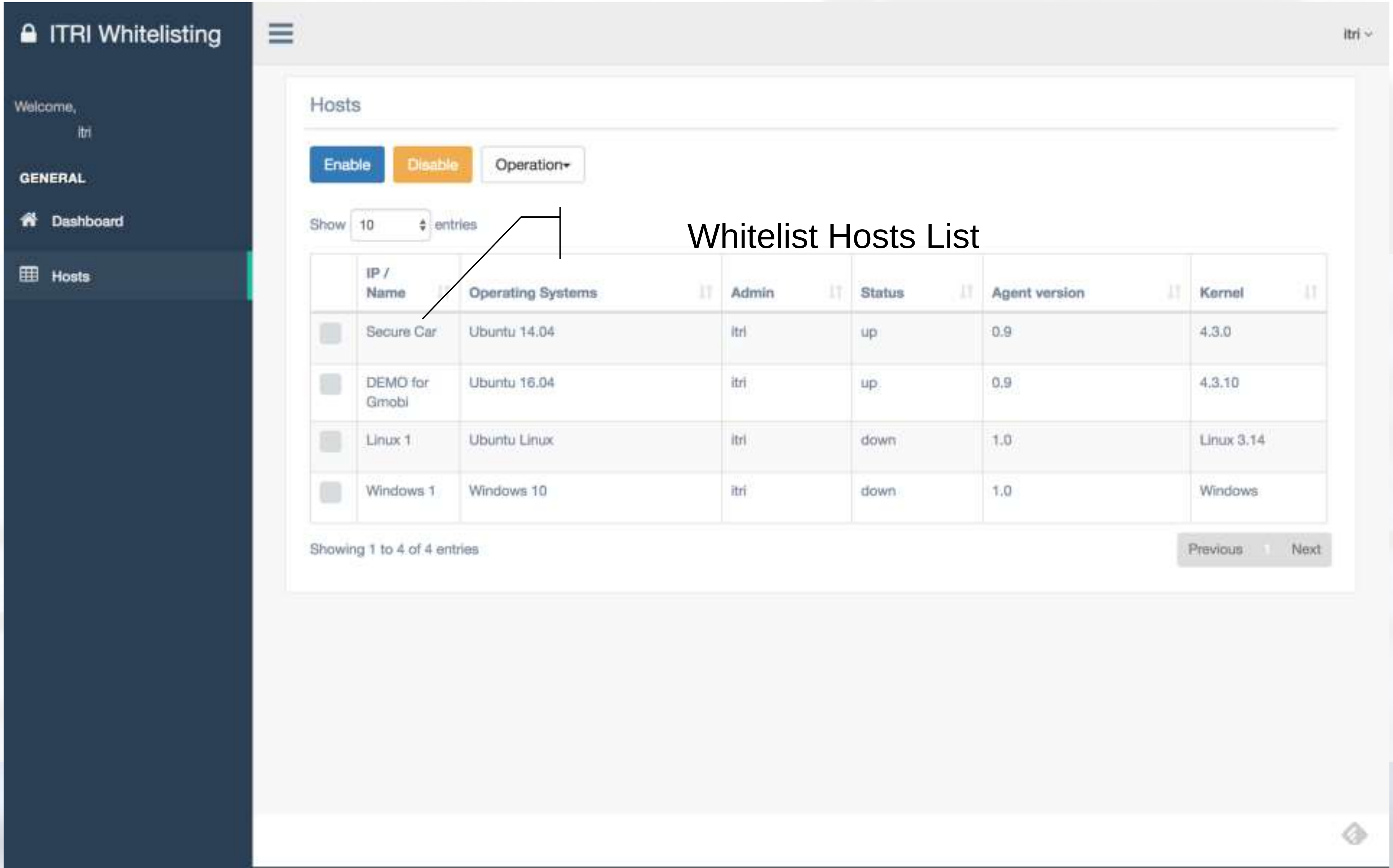
deny	/usr/bin/global	Reject	2018-07-17, 17:09:27
deny	/usr/bin/global	Reject	2018-07-17, 17:09:25

Status Dashboard

Hourly Events

Event Logs

遠端控制介面 – Host 操作 (1/3)



Hosts

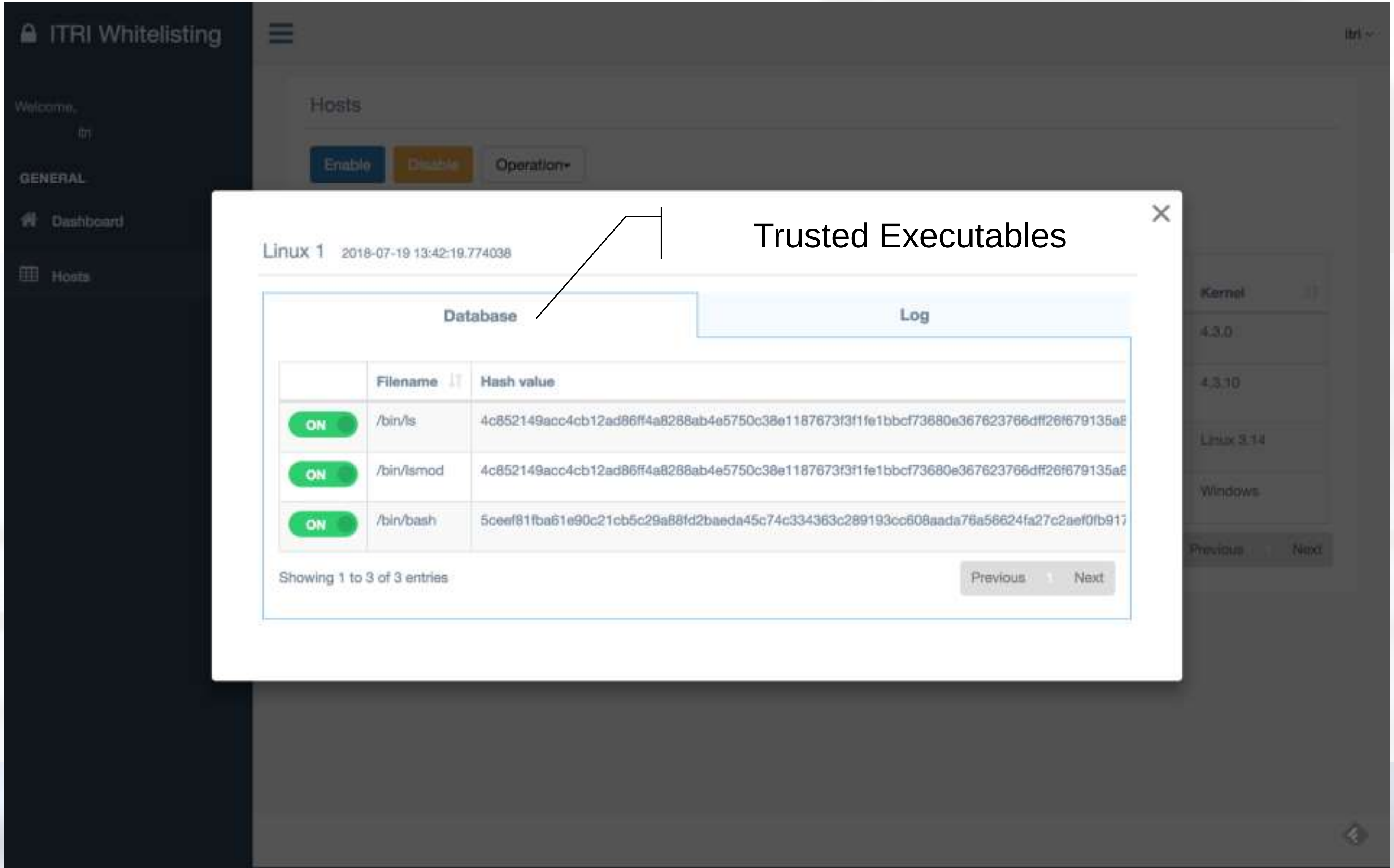
Show 10 entries

Whitelist Hosts List

	IP / Name	Operating Systems	Admin	Status	Agent version	Kernel
□	Secure Car	Ubuntu 14.04	itri	up	0.9	4.3.0
□	DEMO for Gmobi	Ubuntu 16.04	itri	up	0.9	4.3.10
□	Linux 1	Ubuntu Linux	itri	down	1.0	Linux 3.14
□	Windows 1	Windows 10	itri	down	1.0	Windows

Showing 1 to 4 of 4 entries

遠端控制介面 – Host 操作 (2/3)



Trusted Executables

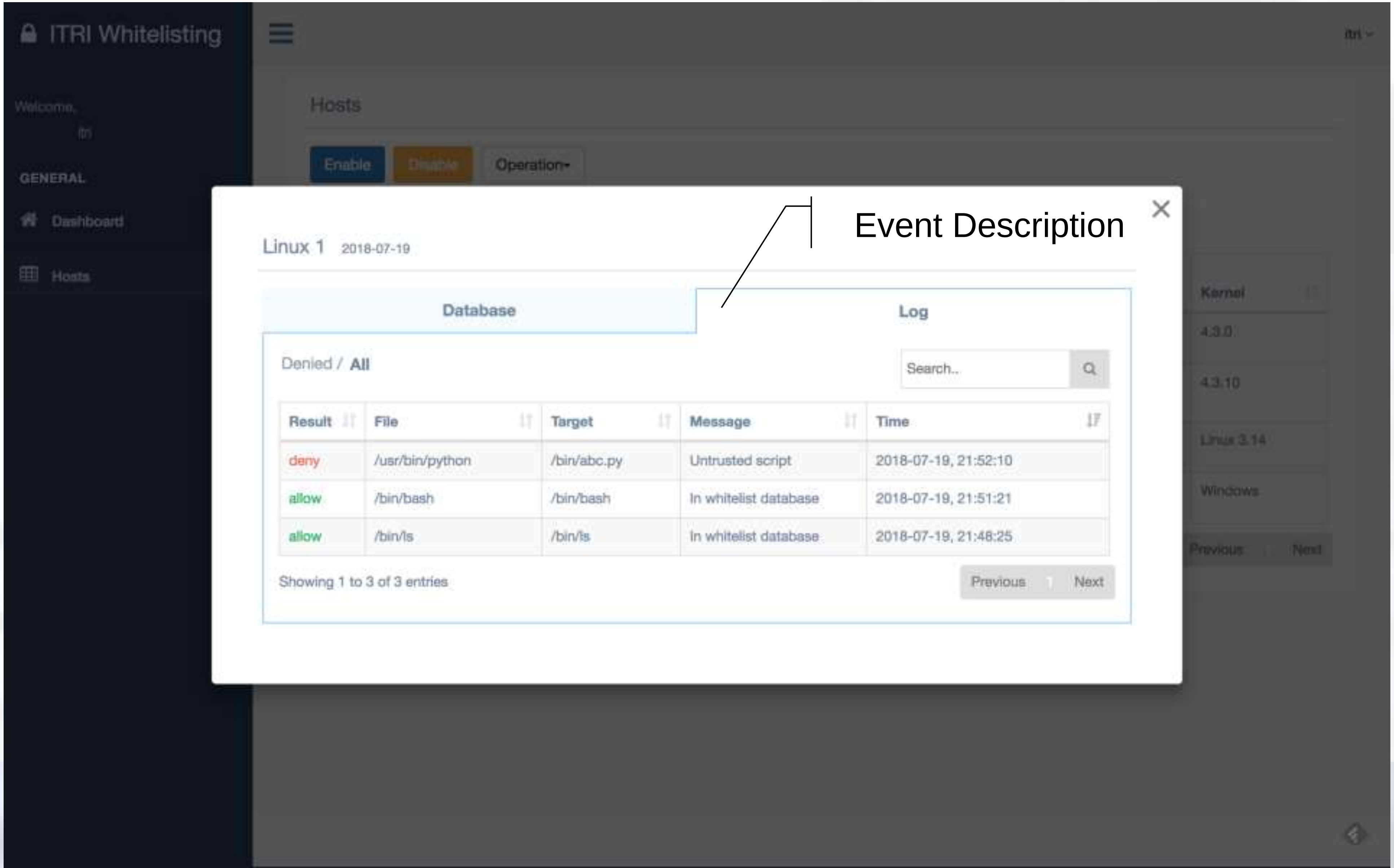
Linux 1 2018-07-19 13:42:19.774038

	Filename	Hash value
ON	/bin/ls	4c852149acc4cb12ad86ff4a8288ab4e5750c38e1187673f3f1fe1bbcf73680e367623766dff26f679135a
ON	/bin/lsmod	4c852149acc4cb12ad86ff4a8288ab4e5750c38e1187673f3f1fe1bbcf73680e367623766dff26f679135a
ON	/bin/bash	5ceef81fba61e90c21cb5c29a88fd2baeda45c74c334363c289193cc608aada76a56624fa27c2aef0fb91

Showing 1 to 3 of 3 entries

Previous 1 Next

遠端控制介面 – Host 操作 (3/3)



Event Description

Linux 1 2018-07-19

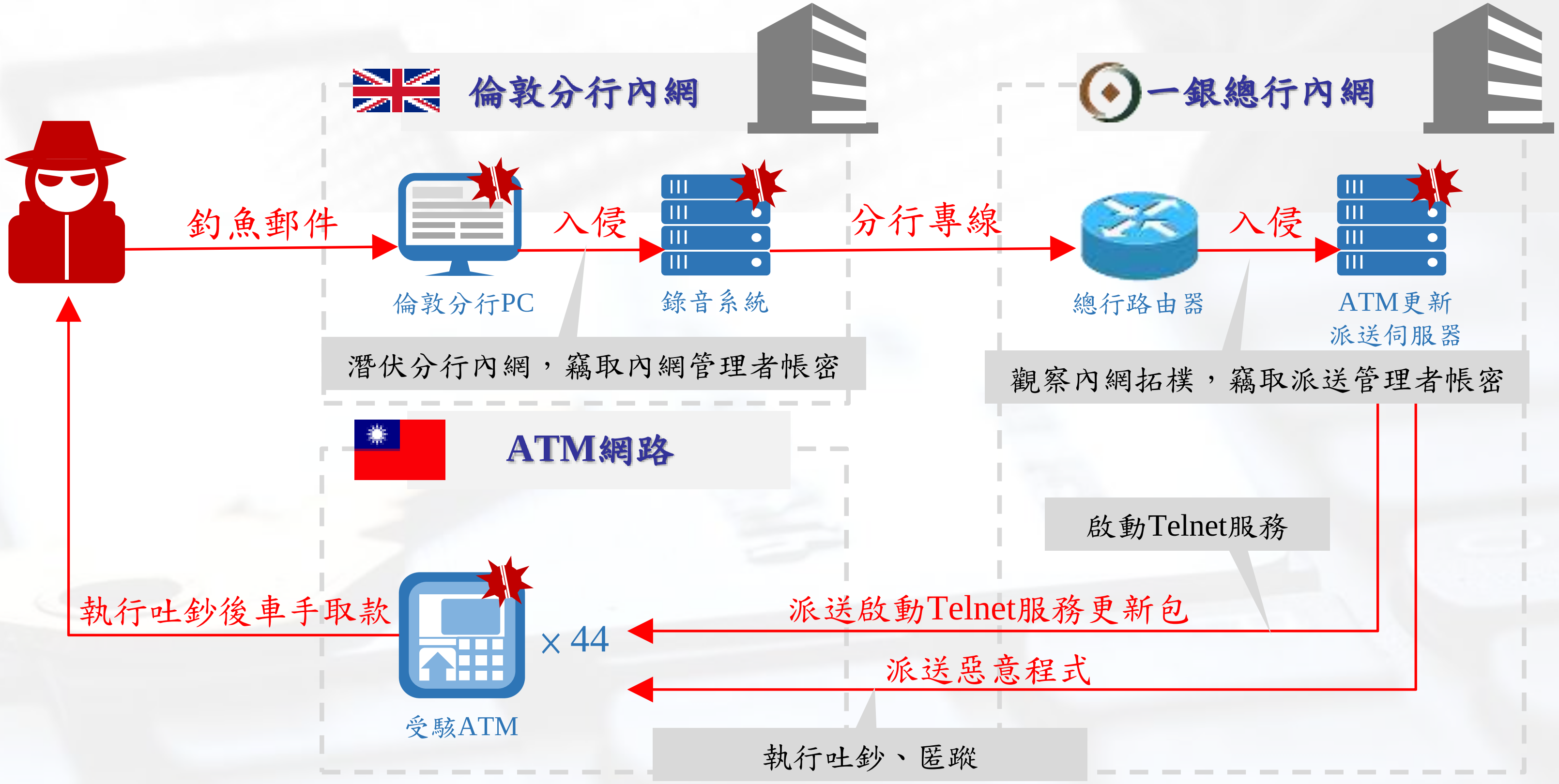
Denied / **All**

Result	File	Target	Message	Time
deny	/usr/bin/python	/bin/abc.py	Untrusted script	2018-07-19, 21:52:10
allow	/bin/bash	/bin/bash	In whitelist database	2018-07-19, 21:51:21
allow	/bin/ls	/bin/ls	In whitelist database	2018-07-19, 21:48:25

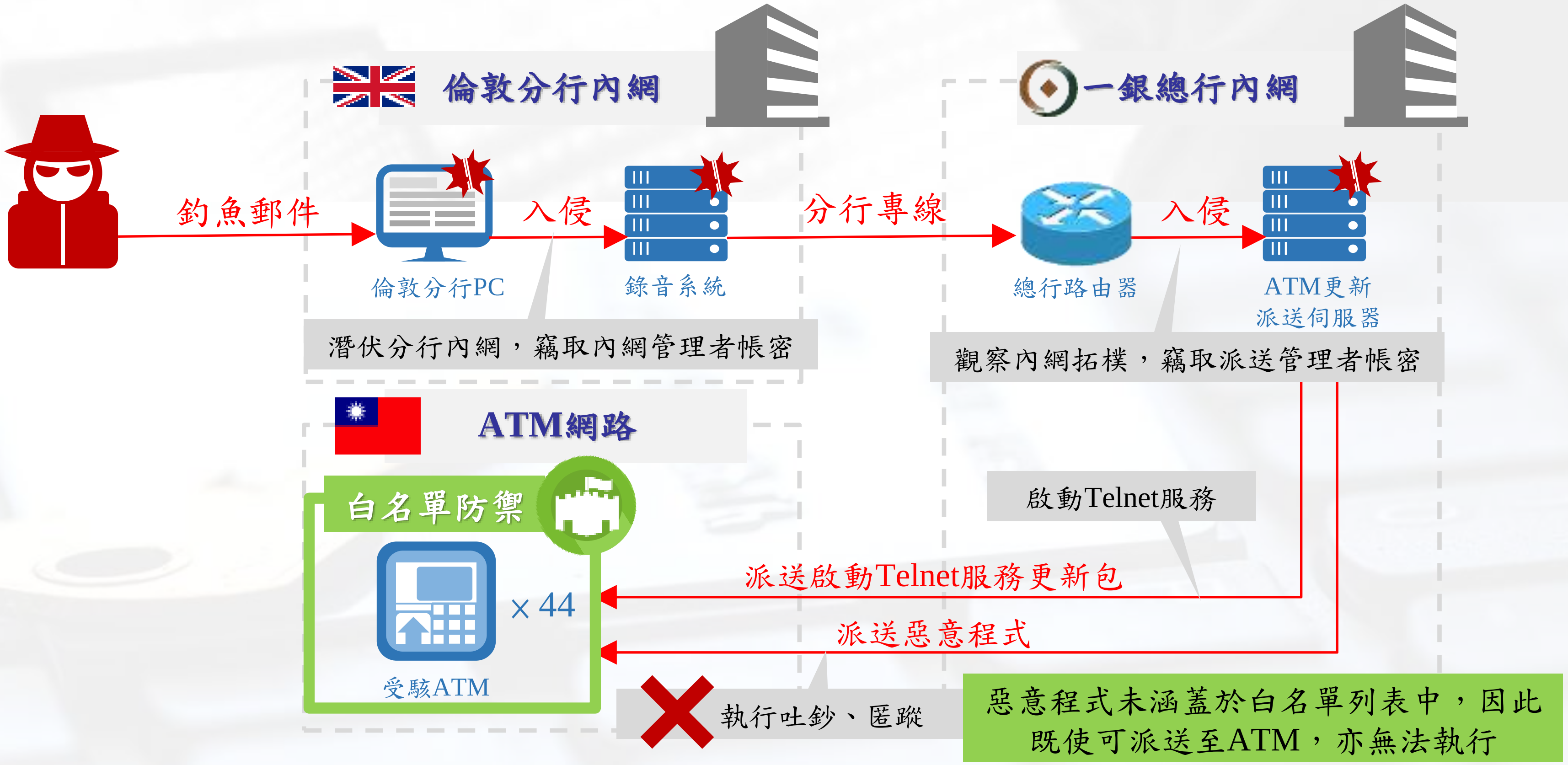
Showing 1 to 3 of 3 entries

Previous 1 Next

第一銀行ATM盜領事件流程



一銀事件 ＋ 應用程式白名單



倫敦分行內網

一銀總行內網

釣魚郵件

入侵

分行專線

入侵

倫敦分行PC

錄音系統

總行路由器

ATM更新
派送伺服器

潛伏分行內網，竊取內網管理者帳密

觀察內網拓樸，竊取派送管理者帳密

ATM網路

白名單防禦

×44

受駭ATM

啟動Telnet服務

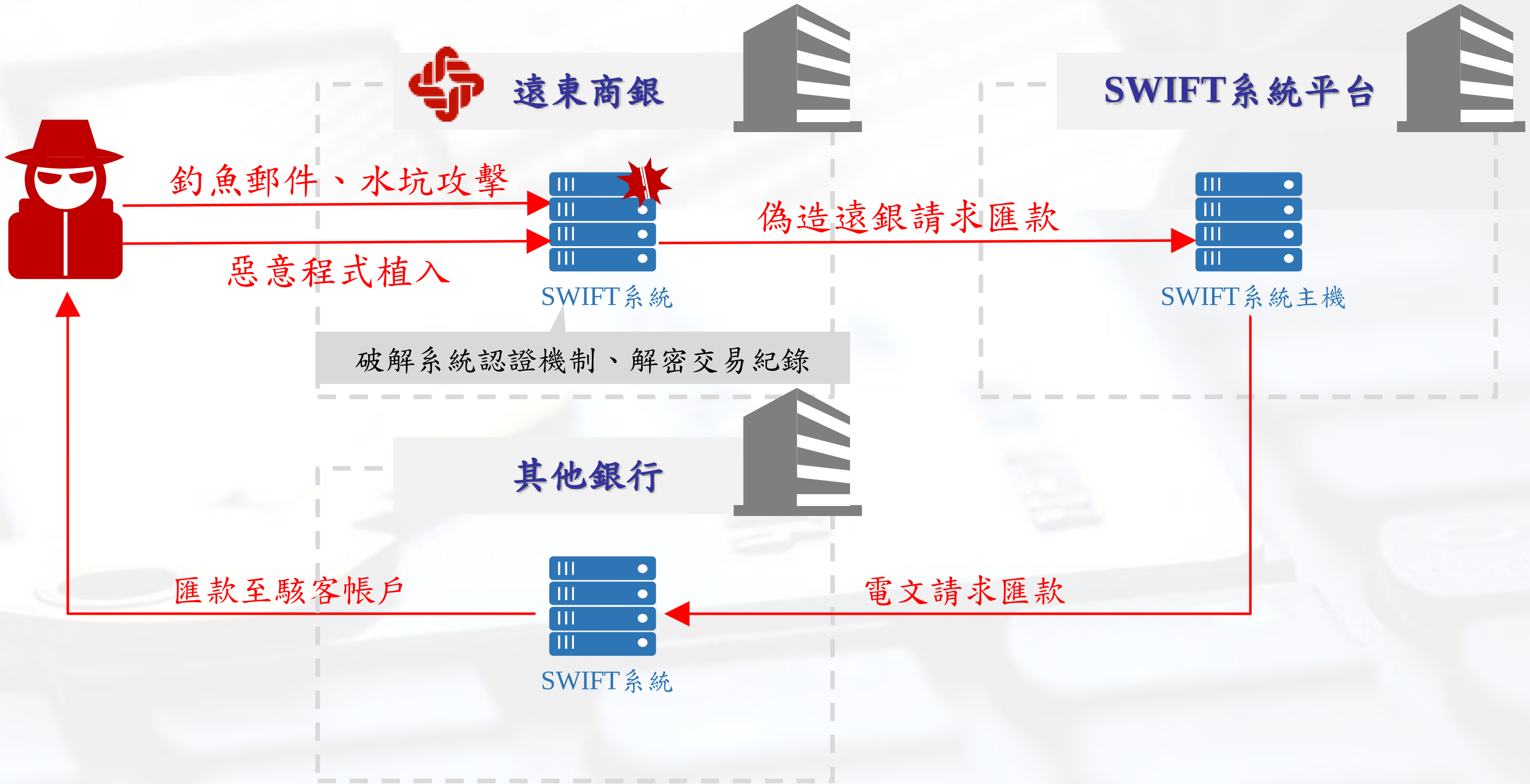
派送啟動Telnet服務更新包

派送惡意程式

執行吐鈔、匿蹤

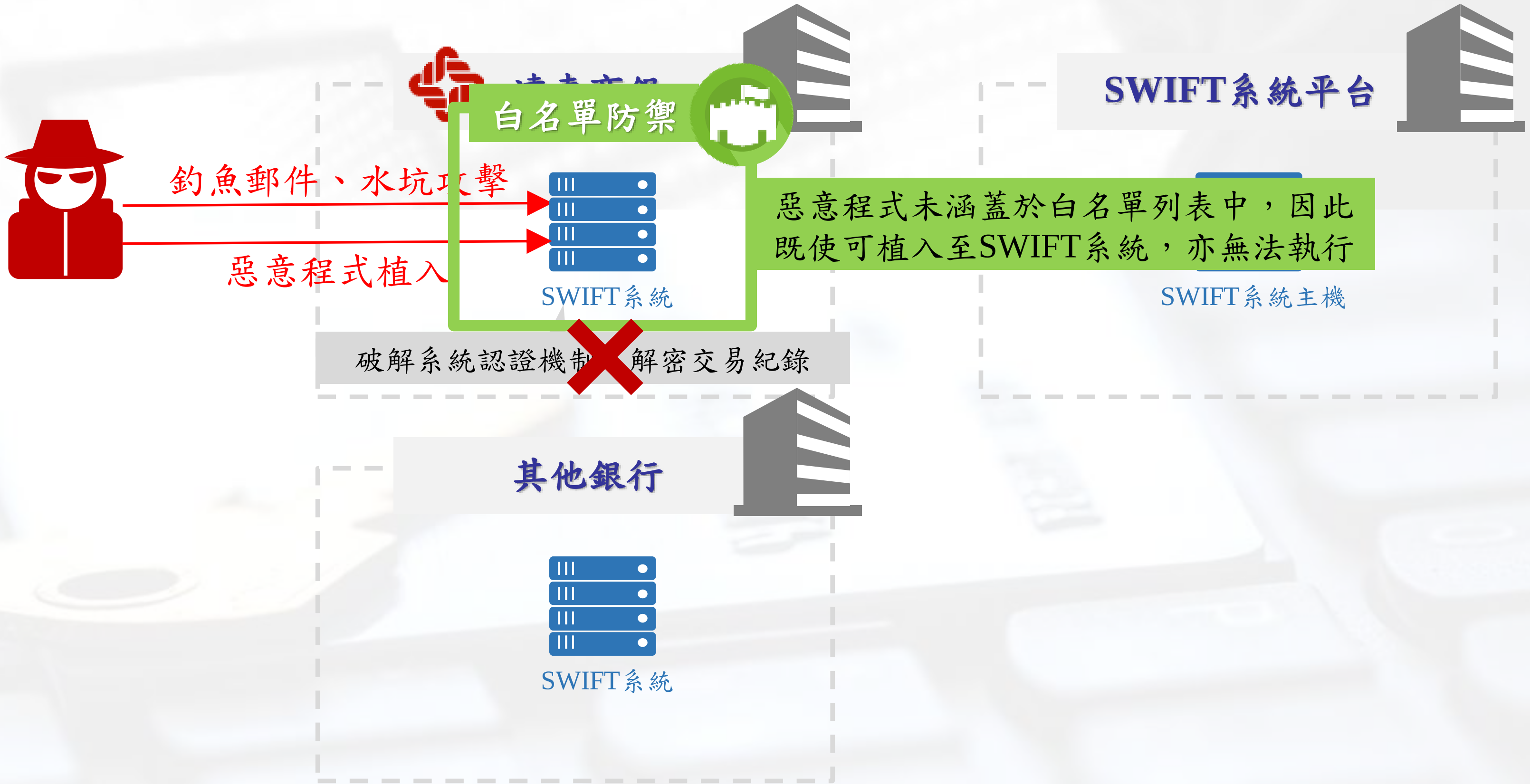
惡意程式未涵蓋於白名單列表中，因此
既使可派送至ATM，亦無法執行

遠東商銀受駭事件流程



遠東商銀
SWIFT系統平台
釣魚郵件、水坑攻擊
惡意程式植入
SWIFT系統
偽造遠銀請求匯款
SWIFT系統主機
破解系統認證機制、解密交易紀錄
其他銀行
匯款至駭客帳戶
電文請求匯款
SWIFT系統

遠東事件 + 應用程式白名單



遠東商銀

白名單防禦

釣魚郵件、水坑攻擊

惡意程式植入

SWIFT系統

惡意程式未涵蓋於白名單列表中，因此既使可植入至SWIFT系統，亦無法執行

破解系統認證機制

解密交易紀錄

SWIFT系統平台

SWIFT系統主機

其他銀行

SWIFT系統

面對未知資安威脅，我們需要更安全的系統

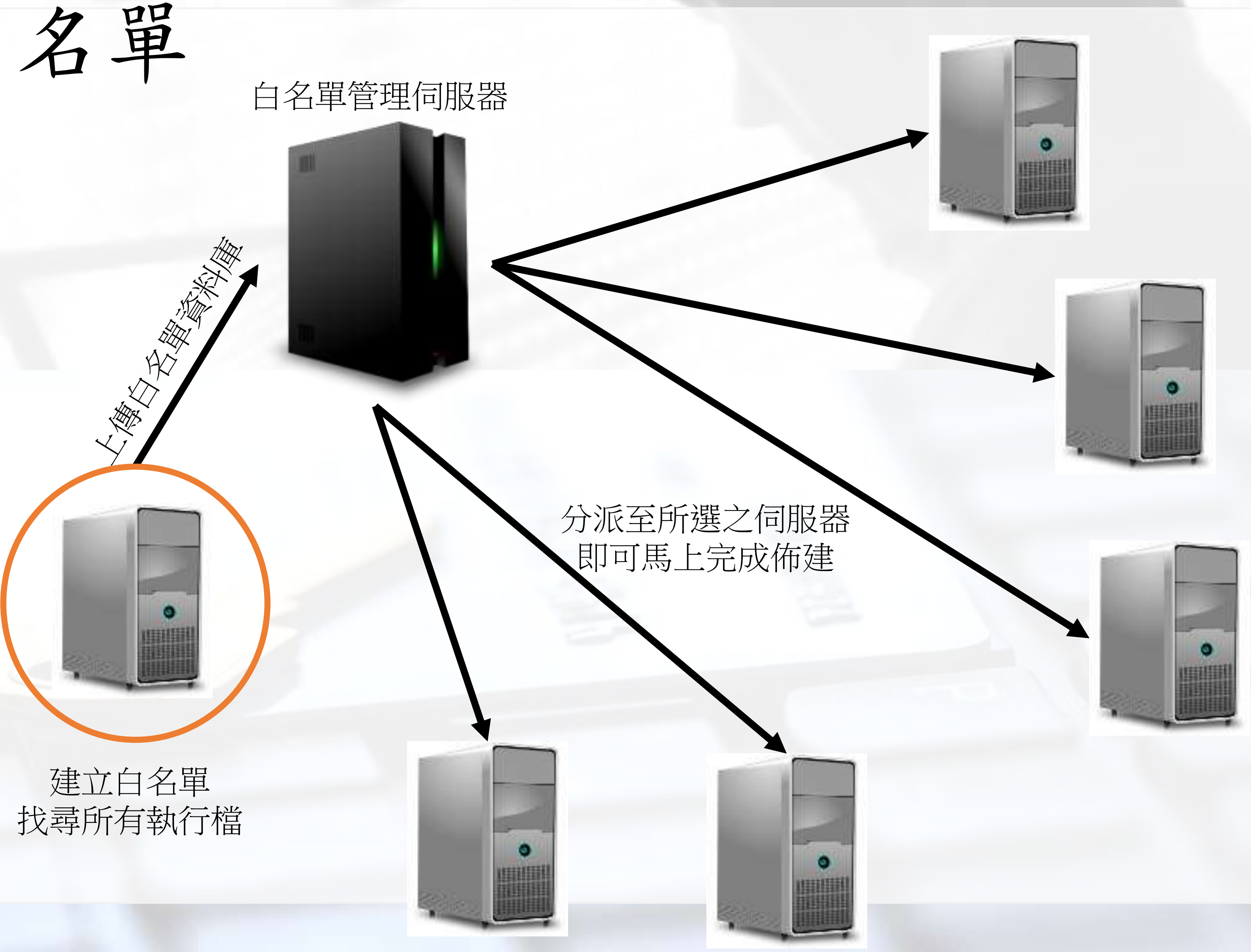
工業技術研究院
Industrial Technology
Research Institute

Application Whitelisting by ITRI

- 工研院應用程式白名單技術
- 針對封閉環境、固定功能系統提供高度保護
- 檢查待執行的程式、函式庫、Script 與驅動程式完整性
- 二階段安裝與更新，嚴格管理白名單資料庫

- 支援 Windows 與 Linux 作業系統

建置白名單



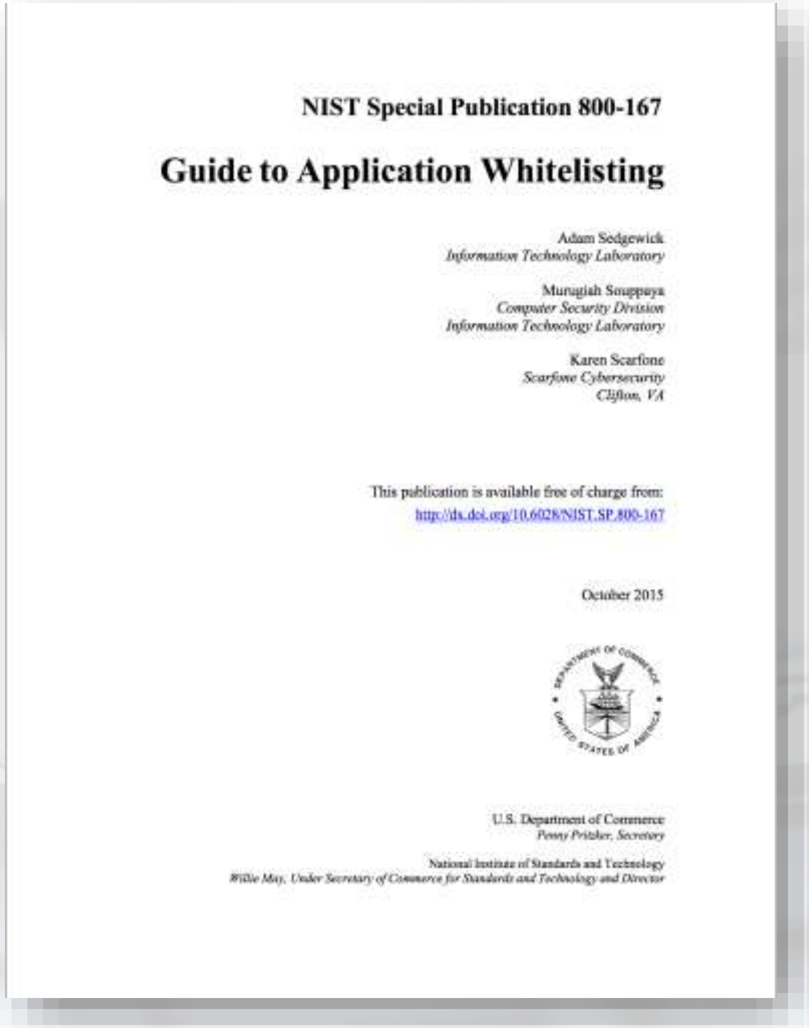
白名單管理伺服器

上傳白名單資料庫

分派至所選之伺服器
即可馬上完成佈建

建立白名單
找尋所有執行檔

Application Whitelisting is a must for national security



NIST Special Publication 800-167

Guide to Application Whitelisting

Adam Sedgewick
Information Technology Laboratory

Murugiah Souppaya
Computer Security Division
Information Technology Laboratory

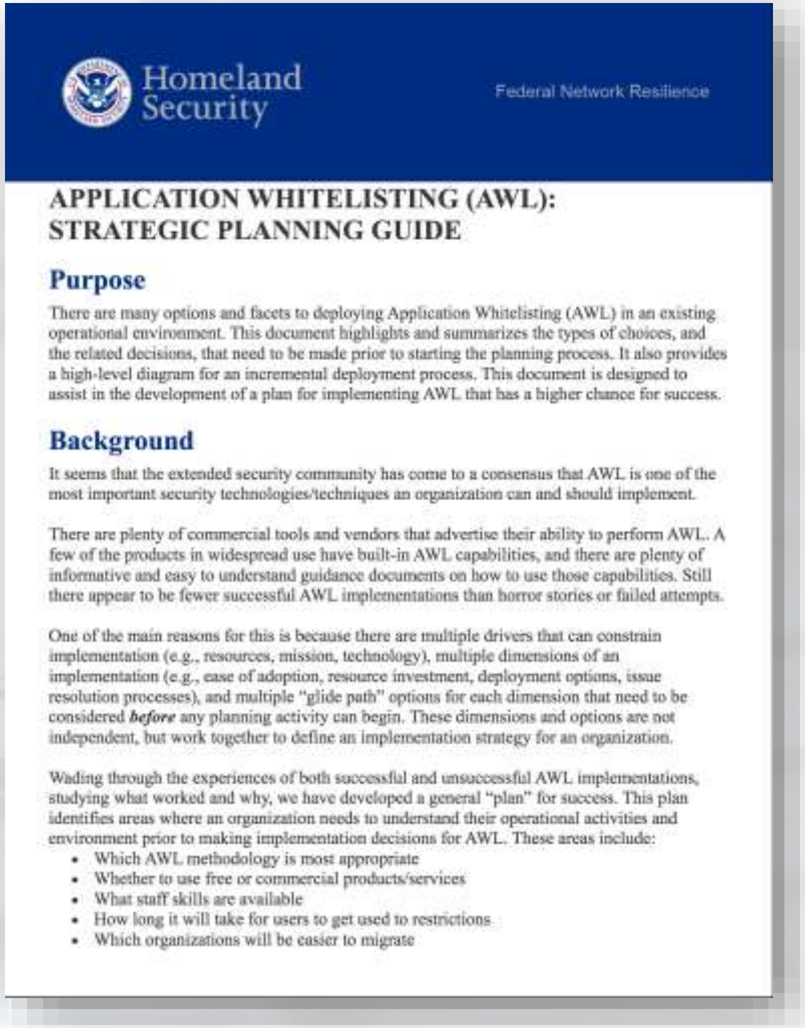
Karen Scarfone
Scarfone Cybersecurity
Clifton, VA

This publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.SP.800-167

October 2015

U.S. Department of Commerce
Penny Pritzker, Secretary

National Institute of Standards and Technology
Willie May, Under Secretary of Commerce for Standards and Technology and Director



Homeland Security

Federal Network Resilience

APPLICATION WHITELISTING (AWL):
STRATEGIC PLANNING GUIDE

Purpose

There are many options and facets to deploying Application Whitelisting (AWL) in an existing operational environment. This document highlights and summarizes the types of choices, and the related decisions, that need to be made prior to starting the planning process. It also provides a high-level diagram for an incremental deployment process. This document is designed to assist in the development of a plan for implementing AWL that has a higher chance for success.

Background

It seems that the extended security community has come to a consensus that AWL is one of the most important security technologies/techniques an organization can and should implement.

There are plenty of commercial tools and vendors that advertise their ability to perform AWL. A few of the products in widespread use have built-in AWL capabilities, and there are plenty of informative and easy to understand guidance documents on how to use those capabilities. Still there appear to be fewer successful AWL implementations than horror stories or failed attempts.

One of the main reasons for this is because there are multiple drivers that can constrain implementation (e.g., resources, mission, technology), multiple dimensions of an implementation (e.g., ease of adoption, resource investment, deployment options, issue resolution processes), and multiple "glide path" options for each dimension that need to be considered ***before*** any planning activity can begin. These dimensions and options are not independent, but work together to define an implementation strategy for an organization.

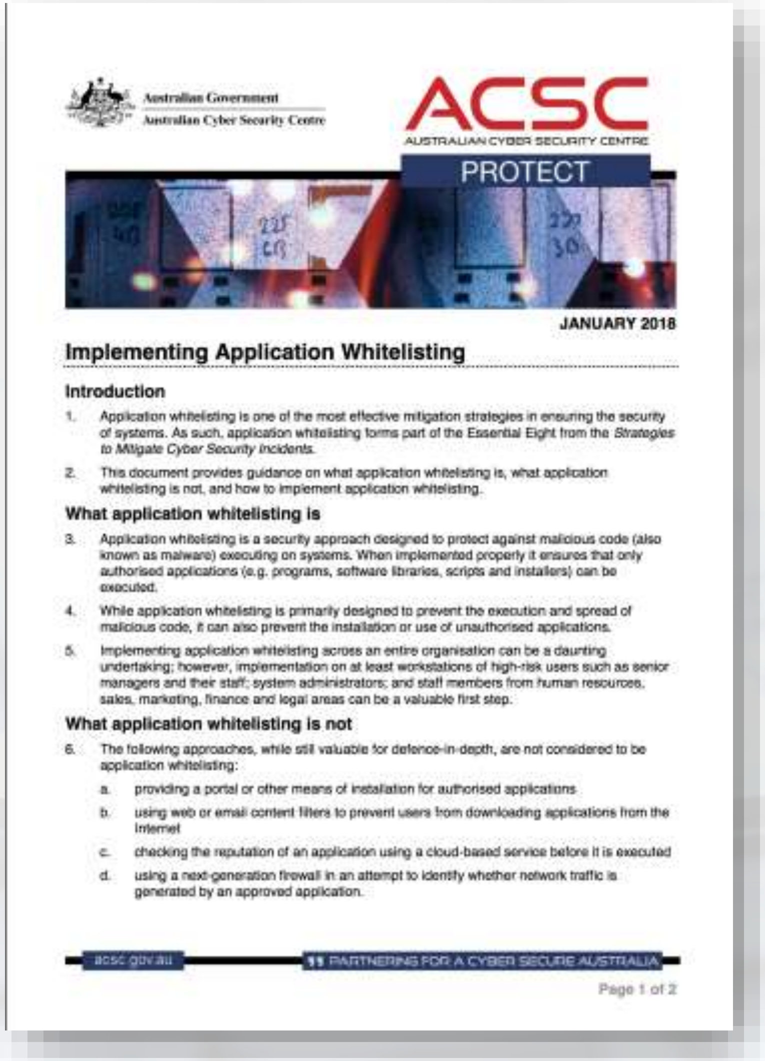
Wading through the experiences of both successful and unsuccessful AWL implementations, studying what worked and why, we have developed a general "plan" for success. This plan identifies areas where an organization needs to understand their operational activities and environment prior to making implementation decisions for AWL. These areas include:

- Which AWL methodology is most appropriate
- Whether to use free or commercial products/services
- What staff skills are available
- How long it will take for users to get used to restrictions
- Which organizations will be easier to migrate

https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-167.pdf

https://www.us-cert.gov/sites/default/files/cdm_files/FNR_NIS_OTH_AWL_Strategic_Planning_Guide.pdf

Application Whitelisting as a global cyber security defense strategy



Australian Government
Australian Cyber Security Centre

ACSC
AUSTRALIAN CYBER SECURITY CENTRE

PROTECT

JANUARY 2018

Implementing Application Whitelisting

Introduction

1. Application whitelisting is one of the most effective mitigation strategies in ensuring the security of systems. As such, application whitelisting forms part of the Essential Eight from the *Strategies to Mitigate Cyber Security Incidents*.
2. This document provides guidance on what application whitelisting is, what application whitelisting is not, and how to implement application whitelisting.

What application whitelisting is

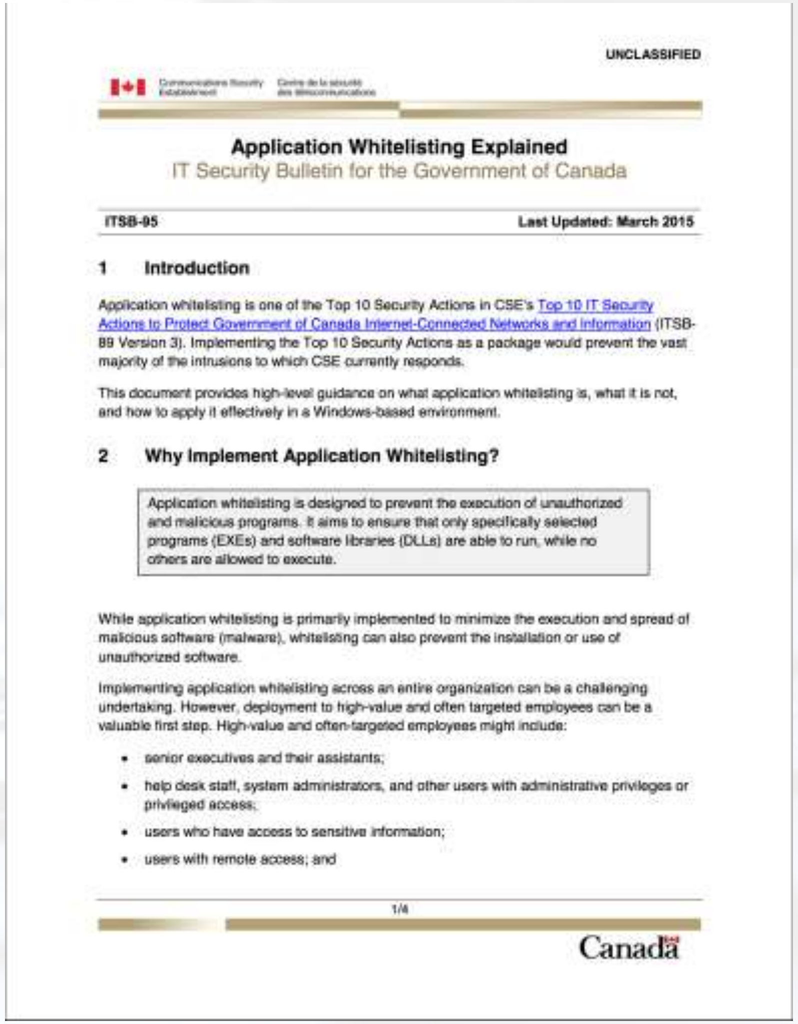
3. Application whitelisting is a security approach designed to protect against malicious code (also known as malware) executing on systems. When implemented properly it ensures that only authorised applications (e.g. programs, software libraries, scripts and installers) can be executed.
4. While application whitelisting is primarily designed to prevent the execution and spread of malicious code, it can also prevent the installation or use of unauthorised applications.
5. Implementing application whitelisting across an entire organisation can be a daunting undertaking; however, implementation on at least workstations of high-risk users such as senior managers and their staff; system administrators; and staff members from human resources, sales, marketing, finance and legal areas can be a valuable first step.

What application whitelisting is not

6. The following approaches, while still valuable for defence-in-depth, are not considered to be application whitelisting:
   a. providing a portal or other means of installation for authorised applications
   b. using web or email content filters to prevent users from downloading applications from the Internet
   c. checking the reputation of an application using a cloud-based service before it is executed
   d. using a next-generation firewall in an attempt to identify whether network traffic is generated by an approved application.

acsc.gov.au   PARTNERING FOR A CYBER SECURE AUSTRALIA

Page 1 of 2



UNCLASSIFIED

Communications Security Establishment   Centre de la sécurité des télécommunications

Application Whitelisting Explained

IT Security Bulletin for the Government of Canada

ITSB-95   Last Updated: March 2015

1 Introduction

Application whitelisting is one of the Top 10 Security Actions in CSE's Top 10 IT Security Actions to Protect Government of Canada Internet-Connected Networks and Information (ITSB-89 Version 3). Implementing the Top 10 Security Actions as a package would prevent the vast majority of the intrusions to which CSE currently responds.

This document provides high-level guidance on what application whitelisting is, what it is not, and how to apply it effectively in a Windows-based environment.

2 Why Implement Application Whitelisting?

Application whitelisting is designed to prevent the execution of unauthorized and malicious programs. It aims to ensure that only specifically selected programs (EXEs) and software libraries (DLLs) are able to run, while no others are allowed to execute.

While application whitelisting is primarily implemented to minimize the execution and spread of malicious software (malware), whitelisting can also prevent the installation or use of unauthorized software.

Implementing application whitelisting across an entire organization can be a challenging undertaking. However, deployment to high-value and often targeted employees can be a valuable first step. High-value and often-targeted employees might include:

- senior executives and their assistants;
- help desk staff, system administrators, and other users with administrative privileges or privileged access;
- users who have access to sensitive information;
- users with remote access; and

1/4

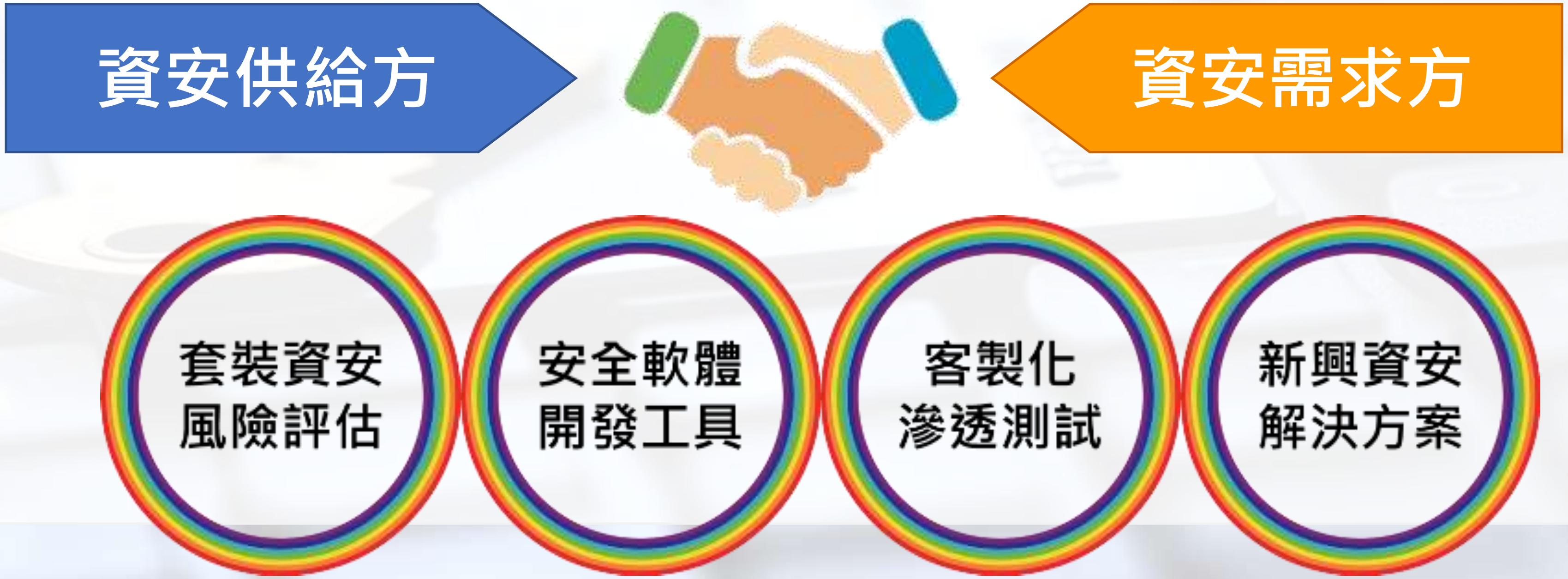
Canada

https://acsc.gov.au/publications/protect/Application_Whitelisting.pdf
https://www.cse-cst.gc.ca/en/system/files/pdf_documents/itsb-95-eng.pdf

資安強化百寶箱 —「資安整合服務平台」

經濟部工業局107年 新興資安產業生態系推動計畫

- 打造資安強化示範場域，創造需求帶動資安產業發展
- 提供安全軟體開發工具服務，厚植產業安全開發能量
- 鼓勵發展自主新興資安解決方案，聚焦主動安全強化



資安供給方

資安需求方

套裝資安風險評估

安全軟體開發工具

客製化滲透測試

新興資安解決方案

套裝資安風險評估

—了解資安環境，評估資安風險，擬定資安強化策略

套裝資安
風險評估

資安供給方

資安需求方

輔導40家廠商落實資安健檢
→10萬→1萬
→14萬→4萬

依我國公司法設立，並由中央主管機關核准登記之本國公司

安全軟體開發工具

— 強化產業安全產品開發流程
— 鼓勵發展資安強化開發工具

安全軟體
開發工具

資安供給方

資安需求方

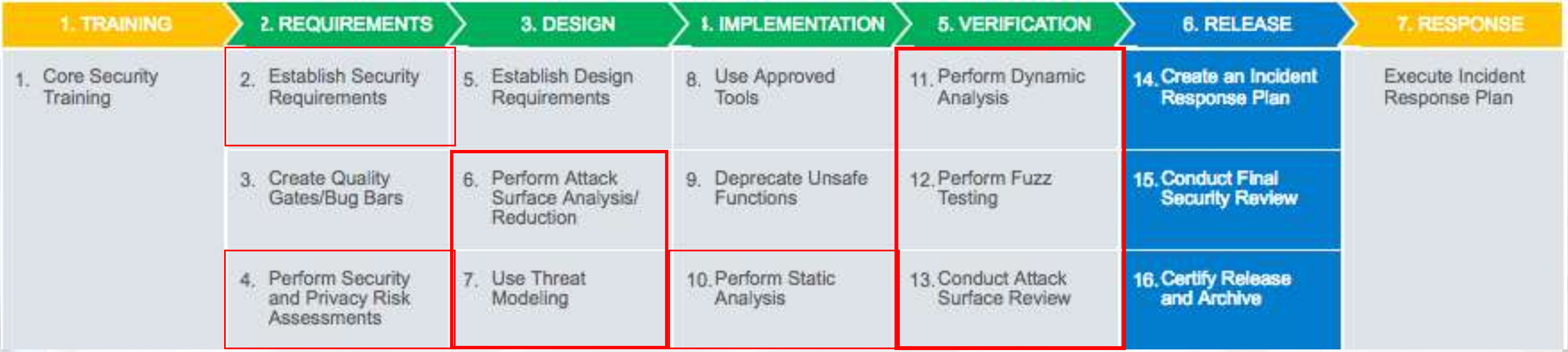
按需採購上架安全軟體開發工具
→最高100萬授權採購

源碼掃瞄工具、弱點掃瞄工具、滲透測試工具、弱點追蹤工具...

按需申請使用上架安全軟體開發工具
→限額免費
→平台優惠價格

安全軟體開發流程

- https://www.microsoft.com/en-us/SDL/process/release.aspx



1. TRAINING	2. REQUIREMENTS	3. DESIGN	4. IMPLEMENTATION	5. VERIFICATION	6. RELEASE	7. RESPONSE
1. Core Security Training	2. Establish Security Requirements	5. Establish Design Requirements	8. Use Approved Tools	11. Perform Dynamic Analysis	14. Create an Incident Response Plan	Execute Incident Response Plan
	3. Create Quality Gates/Bug Bars	6. Perform Attack Surface Analysis/ Reduction	9. Deprecate Unsafe Functions	12. Perform Fuzz Testing	15. Conduct Final Security Review	
	4. Perform Security and Privacy Risk Assessments	7. Use Threat Modeling	10. Perform Static Analysis	13. Conduct Attack Surface Review	16. Certify Release and Archive	

客制化專業滲透測試

— 鼓勵強化核心服務系統或產品滲透測試

客製化
滲透測試

資安供給方

資安需求方

按場域或產品需求執行專業滲透測試服務
→最高40%，上限100萬服務折扣

應用場域或產品開發 ，按需申請專業滲透測服務
→自籌60%

新興資安解決方案

— 鼓勵**發展或導入**新興資安解決方案

新興資安
解決方案

資安供給方

資安需求方

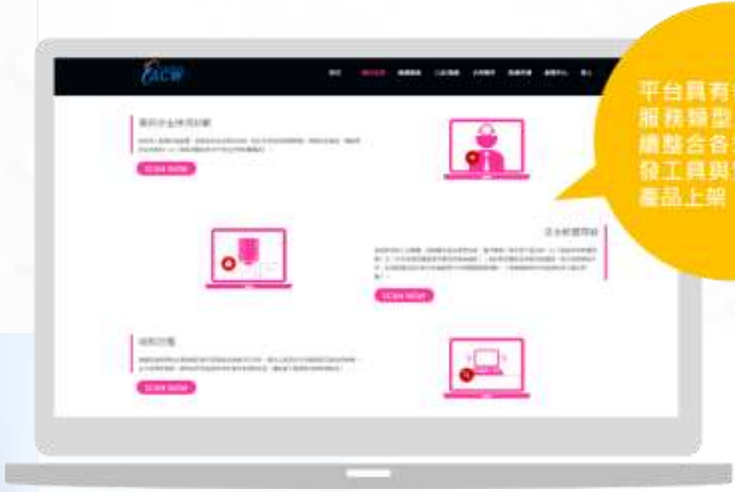
上架整合平台提供服務
→最高40%，上限100萬
服務折扣

使用整合服務平台新興資安產品服務
→限額免費
→折扣優惠
→40%整合導入折扣

已上架安全軟體開發工具

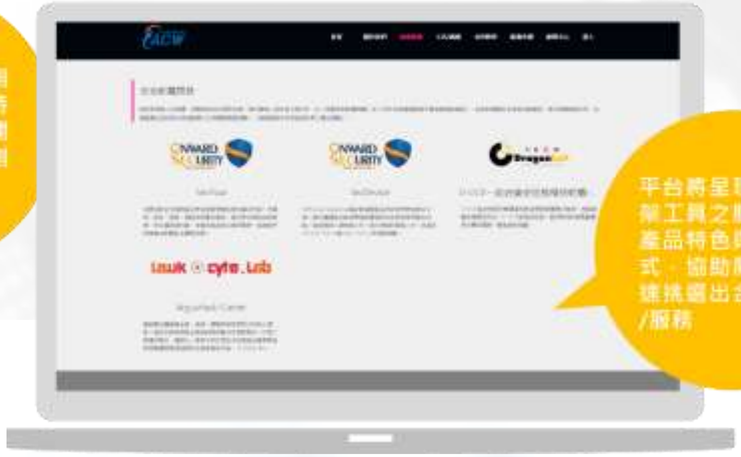
- 滲透測試:	
- ITRI_PT	雲服務，或預約人工施測
- OnwardSecurity SecDevice	按次預約使用授權，人工施測
- OnwardSecurity SecFlow	雲服務
- ArgusHack-Carrier	按次預約使用授權，人工施測
- OpenVAS	雲服務，或預約人工施測
- Nmap	雲服務，或預約人工施測
- Metasploit	人工施測
- W3af	雲服務，或預約人工施測
- Burpsuite	雲服務，或預約人工施測
- ZAP	雲服務，或預約人工施測
- Arachni	雲服務，或預約人工施測
- Nikto	雲服務，或預約人工施測
- 源碼分析:	
- SonarQube	雲服務，或預約人工施測
- 端點防護:	
- AIR Cloud Platform (Xensor)	雲服務，或預約人工施測
- GCB檢測:	
- D-GCB	雲服務，或預約人工施測

平台檢測服務類型



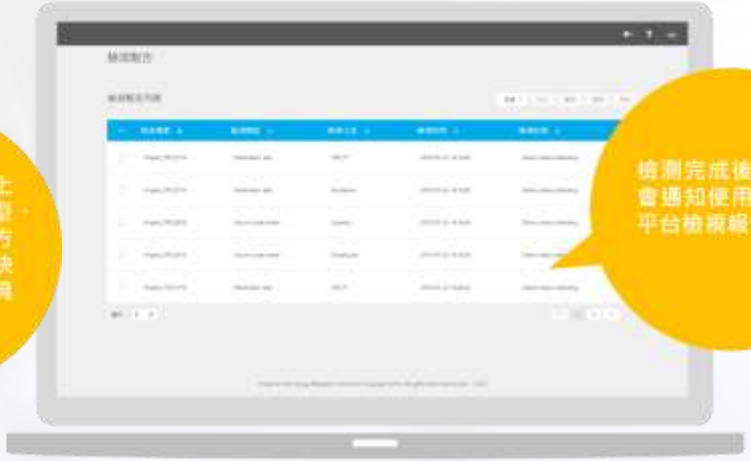
平台具有多種檢測服務類型，並將持續整合各式安全開發工具與資安新創產品上架

平台整合上架工具介紹



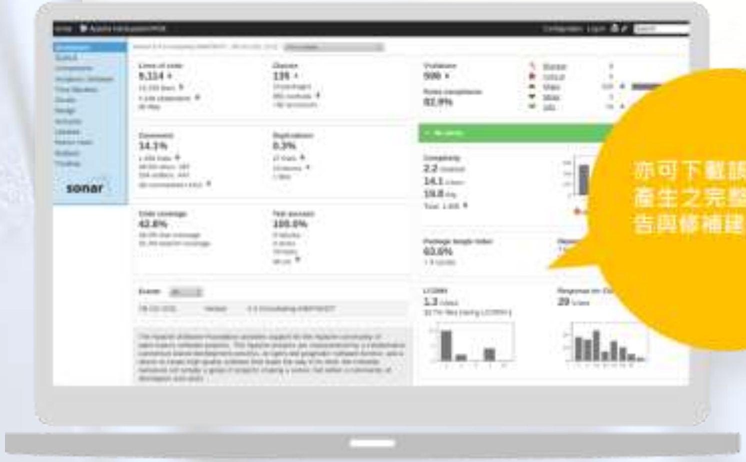
平台將呈現各式上架工具之服務類型、產品特色與操作方式，協助需求方快速挑選出合適工具/服務

源碼檢測-報告檢視(1/2)



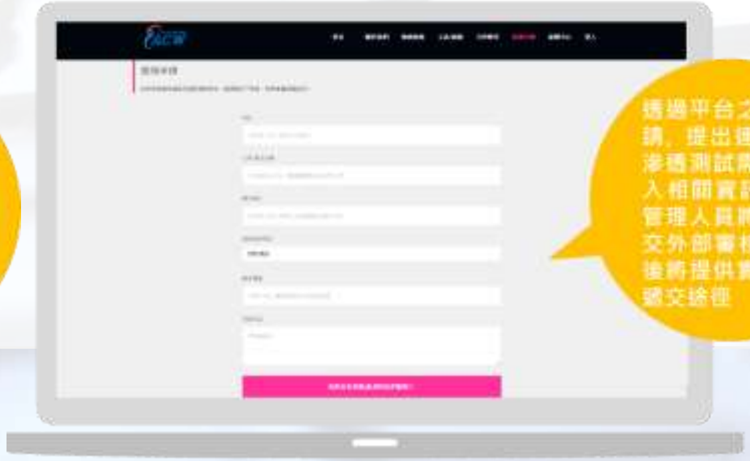
檢測完成後系統將會通知使用者進入平台檢視報告摘要

源碼檢測-報告檢視(2/2)



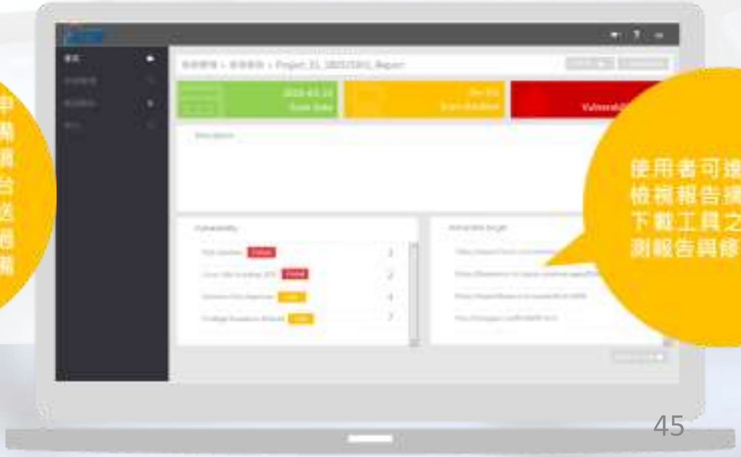
亦可下載該工具所產生之完整檢測報告與修補建議

滲透測試-服務申請



透過平台之服務申請，提出連網設備滲透測試需求並填入相關資訊，平台管理人員將盡速送交外部審核，通過後將提供實體設備遞交途徑

滲透測試-報告檢視



使用者可進入平台檢視報告摘要亦可下載工具之完整檢測報告與修補建議

資安風險的認知與主動管理作為

- 性命攸關 → 安全第一
- 自駕車上路
  - 2020 – 2030 – 2047
- 安全容錯 + 安全責任
  - 供應鏈管理
    - 永續經營/友善社會/環保共生
    - 資安確保

自主資安強化

安全設備導入

供應鏈安全管理

電子商務－主動安全防禦

- 自主資安強化管理 -> 供應鏈資安規範管理
- 固定功能服務主機或設備 -> 固定功能的軟體環境
- ISO 2700X -> 安全軟體開發流程(Secure SDLC)

- 應用程式白名單 -> 杜絕「未知」的惡意程式
  - 固定功能、無人、機互動程式安裝管理的連網設備
  - 公務作業主機
- 資安強化百寶箱 —「資安整合服務平台」

主動安全強化的三支箭

自主資安強化

安全設備導入

供應鏈安全管理

- 防火牆/防毒軟體/端點防護..
- 應用程式白名單
- 滲透測試 / 紅隊演練

- 供應鏈自我安全檢驗證明
- 主動軟體執行環境固化防護
- 供應鏈安全軟體開發稽核