CYBER RANGE

企業級資安實戰攻防術
思科數位靶場實戰服務

Cisco Cyber Range

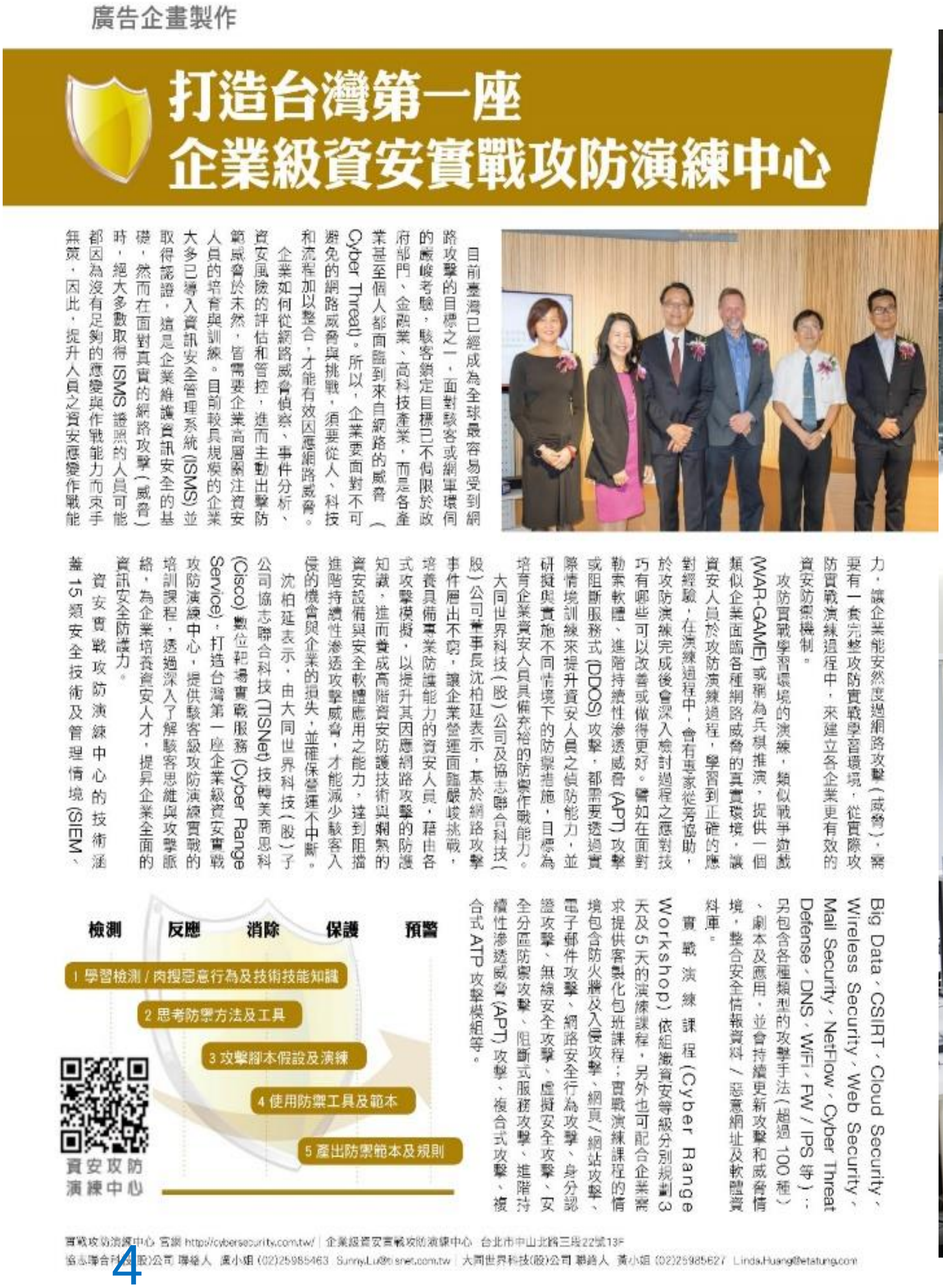
TISNet 協志聯合科技　大同大學

大綱

- 資安實戰攻防演練：數位靶場服務
- 資安威脅與人才培育
- 資訊安全維運基本要求
- Cyber Range Service
- 思科網路學會資安課程
- 合作模式與總結
- Q&A

資安實戰攻防演練：數位靶場服務

建構台灣第一座企業級的「資安實戰攻防演練中心」
- Cisco Cyber Range 技術移轉



廣告企畫製作

打造台灣第一座 企業級資安實戰攻防演練中心

目前臺灣已經成為全球最容易受到網路攻擊的目標之一，面對駭客或網軍環伺的嚴峻考驗，駭客鎖定目標已不侷限於政府部門、金融業、高科技產業，而是各產業甚至個人都面臨到來自網路的威脅（Cyber Threat）。所以，企業要面對不可避免的網路威脅與挑戰，須要從人、科技和流程加以整合，才能有效因應網路威脅。

企業如何從網路威脅偵察、事件分析、資安風險的評估和管控，進而主動出擊防範威脅於未然，皆需要企業高層關注資安人員的培育與訓練。目前較具規模的企業大多已導入資訊安全管理系統(ISMS)並取得認證，這是企業維護資訊安全的基礎，然而在面對真實的網路攻擊（威脅）時，絕大多數取得ISMS證照的人員可能都因為沒有足夠的應變與作戰能力而束手無策，因此，提升人員之資安應變作戰能力，讓企業能安然度過網路攻擊（威脅），需要有一套完整攻防實戰學習環境，從實際攻防實戰演練過程中，來建立各企業更有效的資安防禦機制。

攻防實戰學習環境的演練，類似戰爭遊戲(WAR-GAME)或稱為兵棋推演，提供一個類似企業面臨各種網路威脅的真實環境，讓資安人員於攻防演練過程，學習到正確的應對經驗，在演練過程中，會有專家從旁協助，於攻防演練完成後會深入檢討過程之應對技巧有哪些可以改善或做得更好。譬如在面對勒索軟體、進階持續性滲透威脅(APT)攻擊或阻斷服務式(DDOS)攻擊，都需要透過實際情境訓練來提升資安人員之偵防能力，並研擬與實施不同情境下的防禦措施，目標為培育企業資安人員具備充裕的防禦作戰能力。

大同世界科技（股）公司及協志聯合科技（股）公司董事長沈柏延表示，基於網路攻擊事件層出不窮，讓企業營運面臨嚴峻挑戰，培養具備專業防護能力的資安人員，藉由各式攻擊模擬，以提升其因應網路攻擊的防護知識，進而養成高階資安防護技術與嫻熟的資安設備與安全軟體應用之能力，達到阻擋進階持續性滲透攻擊威脅，才能減少駭客入侵的機會與企業的損失，並確保營運不中斷。

沈柏延表示，由大同世界科技（股）子公司協志聯合科技(TISNet)技轉美商思科(Cisco)數位靶場實戰服務(Cyber Range Service)，打造台灣第一座企業級資安實戰攻防演練中心，提供駭客級攻防演練實戰的培訓課程，透過深入了解駭客思維與攻擊脈絡，為企業培養資安人才，提昇企業全面的資訊安全防護力。

資安實戰攻防演練中心的技術涵蓋15類安全技術及管理情境(SIEM、Big Data、CSIRT、Cloud Security、Wireless Security、Web Security、Mail Security、NetFlow、Cyber Threat Defense、DNS、WiFi、FW / IPS 等)；另包含各種類型的攻擊手法（超過100種）、劇本及應用，並會持續更新攻擊和威脅情境，整合安全情報資料／惡意網址及軟體資料庫。

實戰演練課程(Cyber Range Workshop)依組織資安等級分別規劃3天及5天的演練課程，另外也可配合企業需求提供客製化包班課程；實戰演練課程的情境包含防火牆及入侵攻擊、網頁/網站攻擊、電子郵件攻擊、網路安全行為攻擊、身分認證攻擊、無線安全攻擊、虛擬安全攻擊、安全分區防禦攻擊、阻斷式服務攻擊、進階持續性滲透威脅(APT)攻擊、複合式攻擊、複合式ATP攻擊模組等。

檢測　反應　消除　保護　預警

1 學習檢測 / 肉搜惡意行為及技術技能知識

2 思考防禦方法及工具

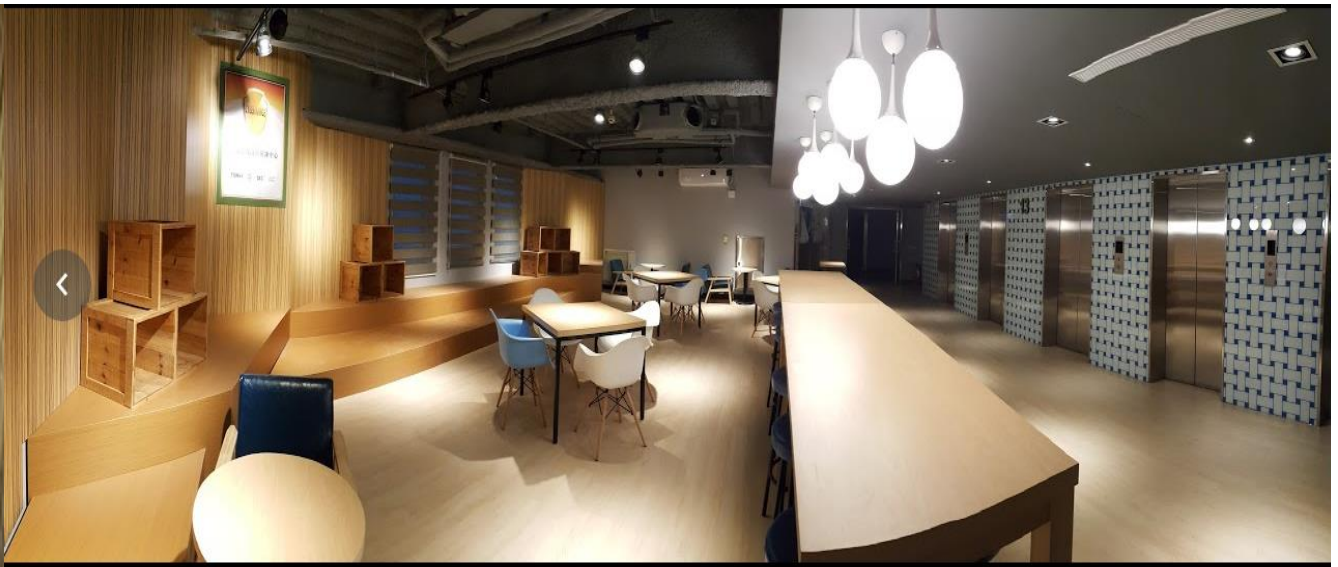
3 攻擊腳本假設及演練

4 使用防禦工具及範本

5 產出防禦範本及規則

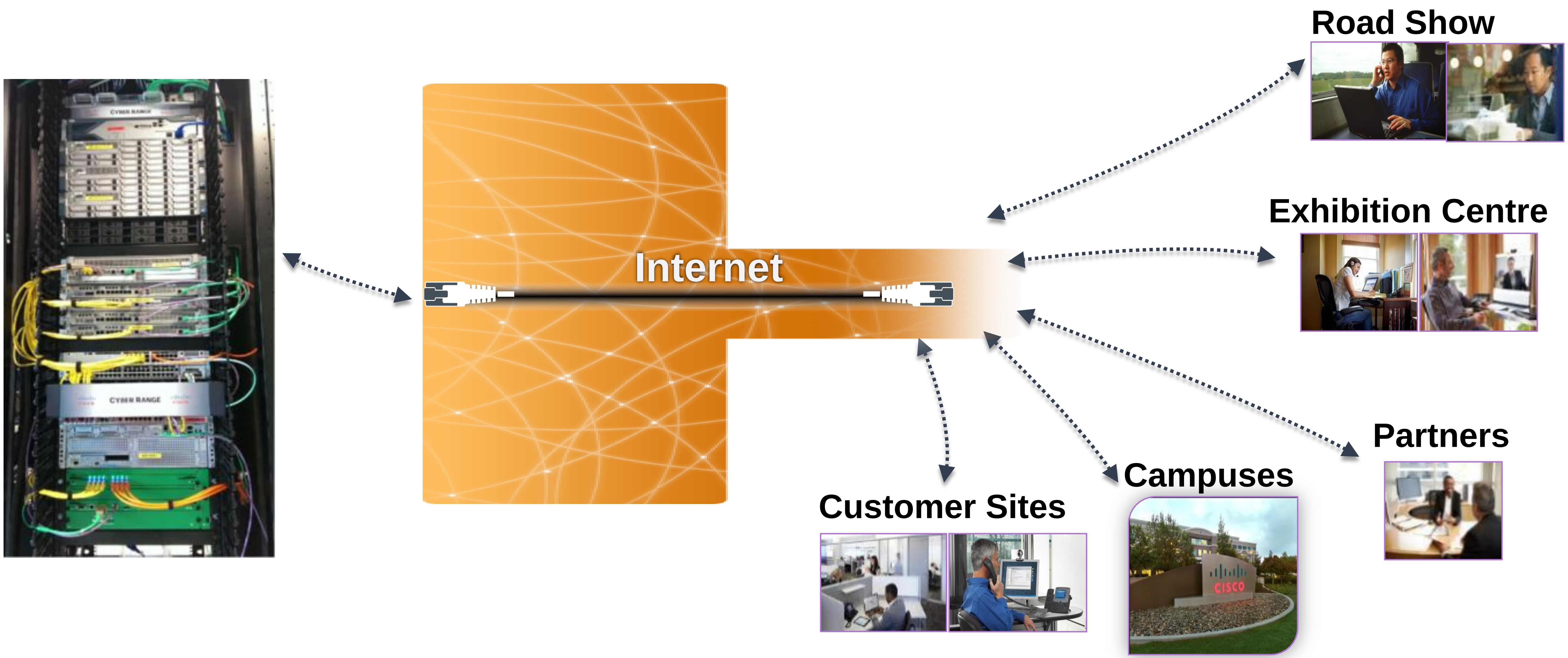
資安攻防演練中心

實戰攻防演練中心 官網 https://cybersecurity.com.tw/ | 企業級資安實戰攻防演練中心 台北市中山北路三段22號13F
協志聯合科技(股)公司 聯絡人 盧小姐 (02)25985463 Sunny.Lu@tisnet.com.tw | 大同世界科技(股)公司 聯絡人 黃小姐 (02)25985627 Linda.Huang@etatung.com



TISNet 協志聯合科技　　大同大學

Cyber Range Remote Capabilities



Internet

Road Show

Exhibition Centre

Partners

Campuses

Customer Sites

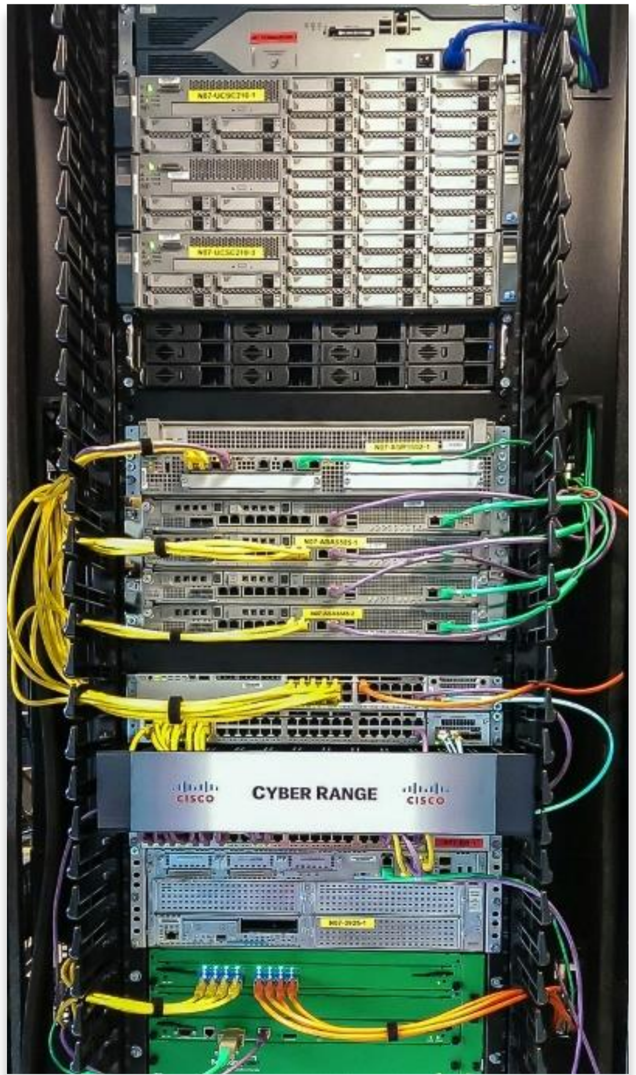
TISNet 協志聯合科技 大同大學

Cyber Range Service Delivery Platform

Cyber Range Is A Platform to Experience the Intelligent Cyber Security for the Real World

Customer Outcomes

- A Platform for Service Delivery and Learning
- Deeper understanding of leading security methodologies, operations, and procedures
- Empower customers with the architecture and capability to combat modern cyber threats



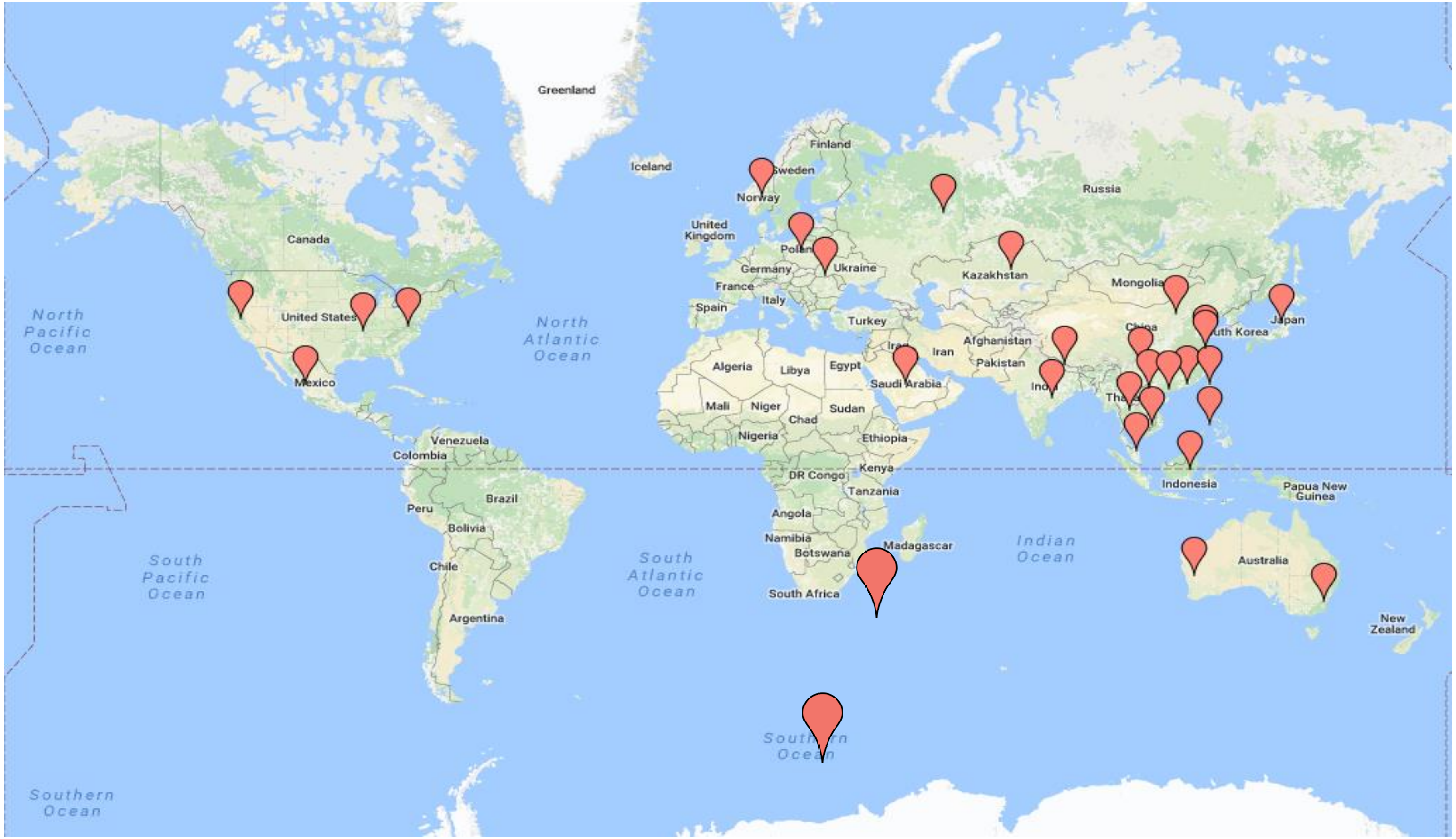
The Solution at a Glance

- Over 100 Attack Cases for 12 Technology Solutions
- 100+ applications simultaneously merged with 200-500 different Malware types
- Virtual environment accessible from any place in the world

PEOPLE PROCESS DATA THINGS

TISNet 協志聯合科技 大同大學

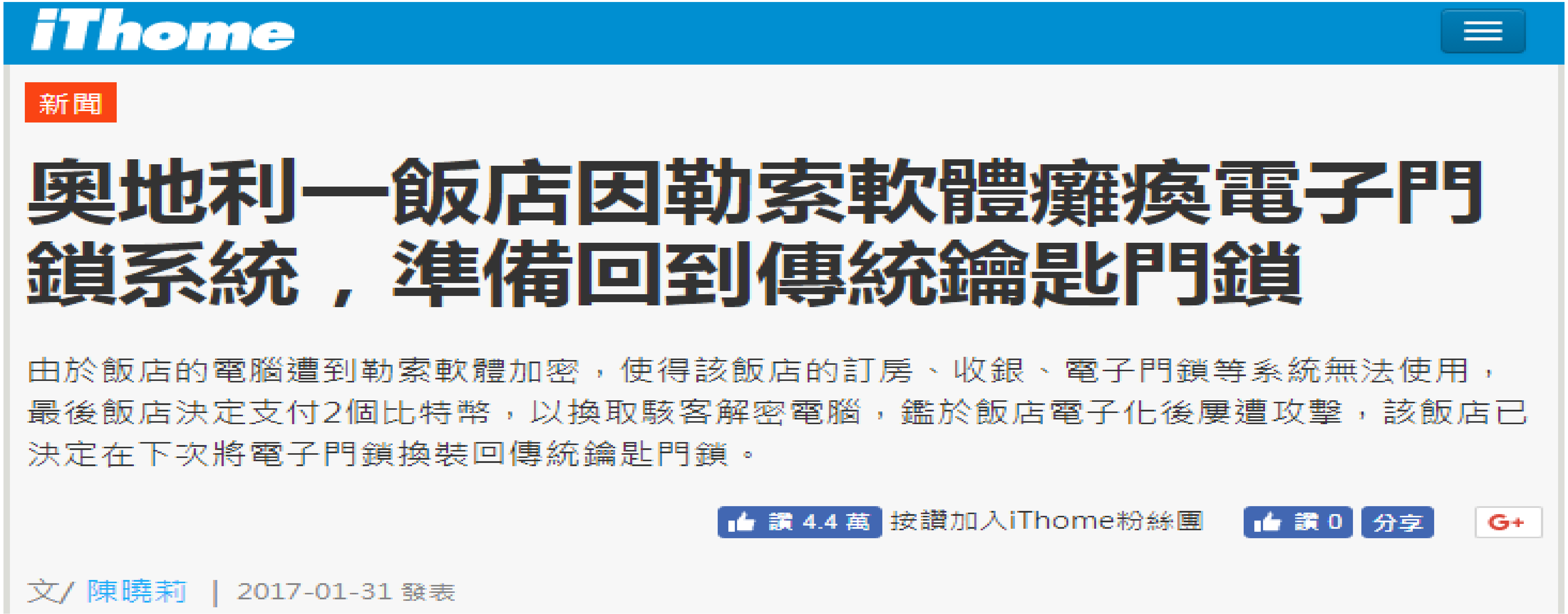
Cisco攻防演練足跡 Over 100 Cyber Range Workshops around world



TISNet 協志聯合科技 大同大學

資安威脅與人才培育

門鎖管理系統被駭，製不了卡無法營業



新聞

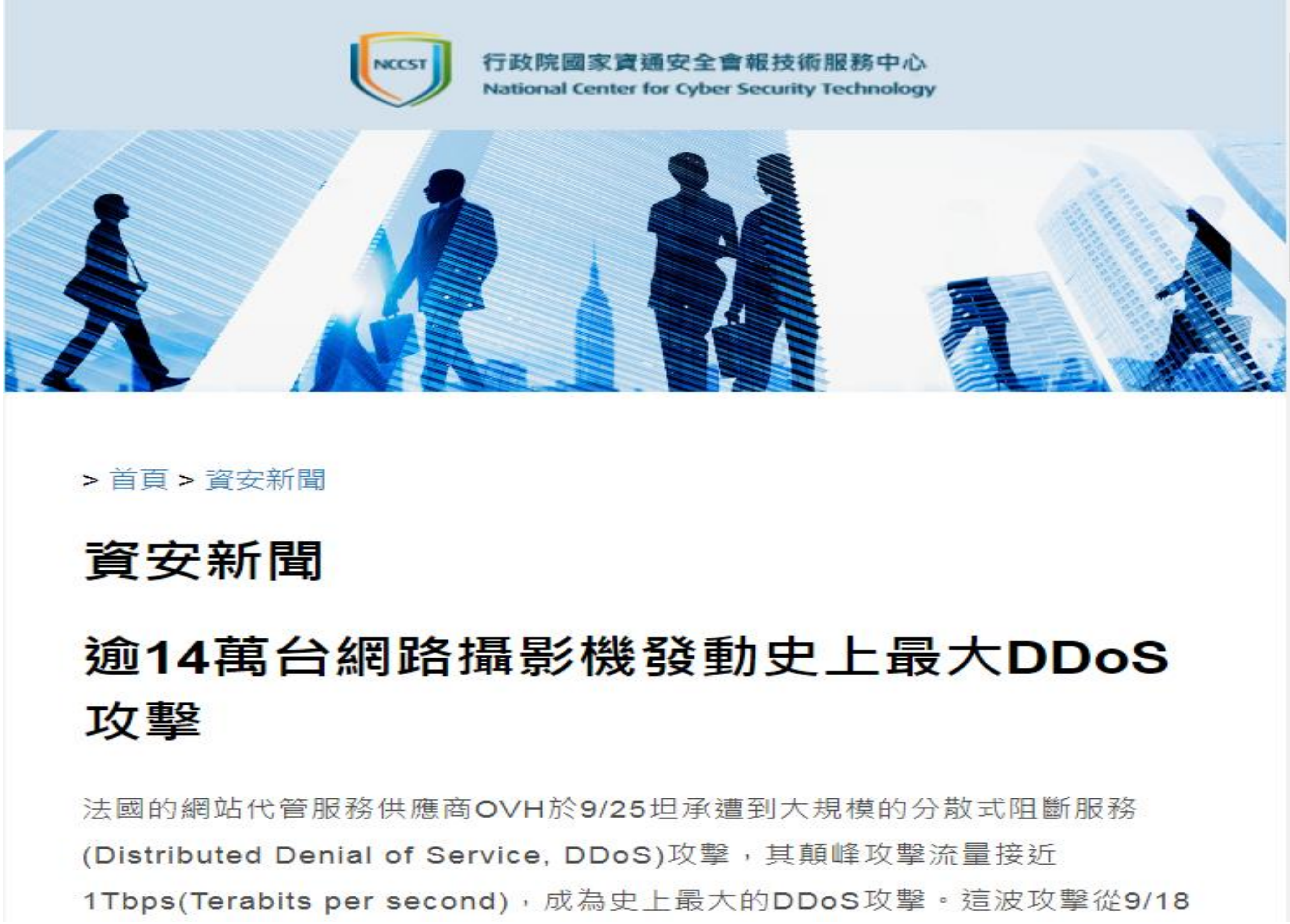
奧地利一飯店因勒索軟體癱瘓電子門鎖系統，準備回到傳統鑰匙門鎖

由於飯店的電腦遭到勒索軟體加密，使得該飯店的訂房、收銀、電子門鎖等系統無法使用，最後飯店決定支付2個比特幣，以換取駭客解密電腦，鑑於飯店電子化後屢遭攻擊，該飯店已決定在下次將電子門鎖換裝回傳統鑰匙門鎖。

文/ 陳曉莉 | 2017-01-31 發表

資料來源：iThome

網路攝影機成為新一代攻擊的馬前卒



行政院國家資通安全會報技術服務中心
National Center for Cyber Security Technology

> 首頁 > 資安新聞

資安新聞

逾14萬台網路攝影機發動史上最大DDoS攻擊

法國的網站代管服務供應商OVH於9/25坦承遭到大規模的分散式阻斷服務(Distributed Denial of Service, DDoS)攻擊，其巔峰攻擊流量接近1Tbps(Terabits per second)，成為史上最大的DDoS攻擊。這波攻擊從9/18

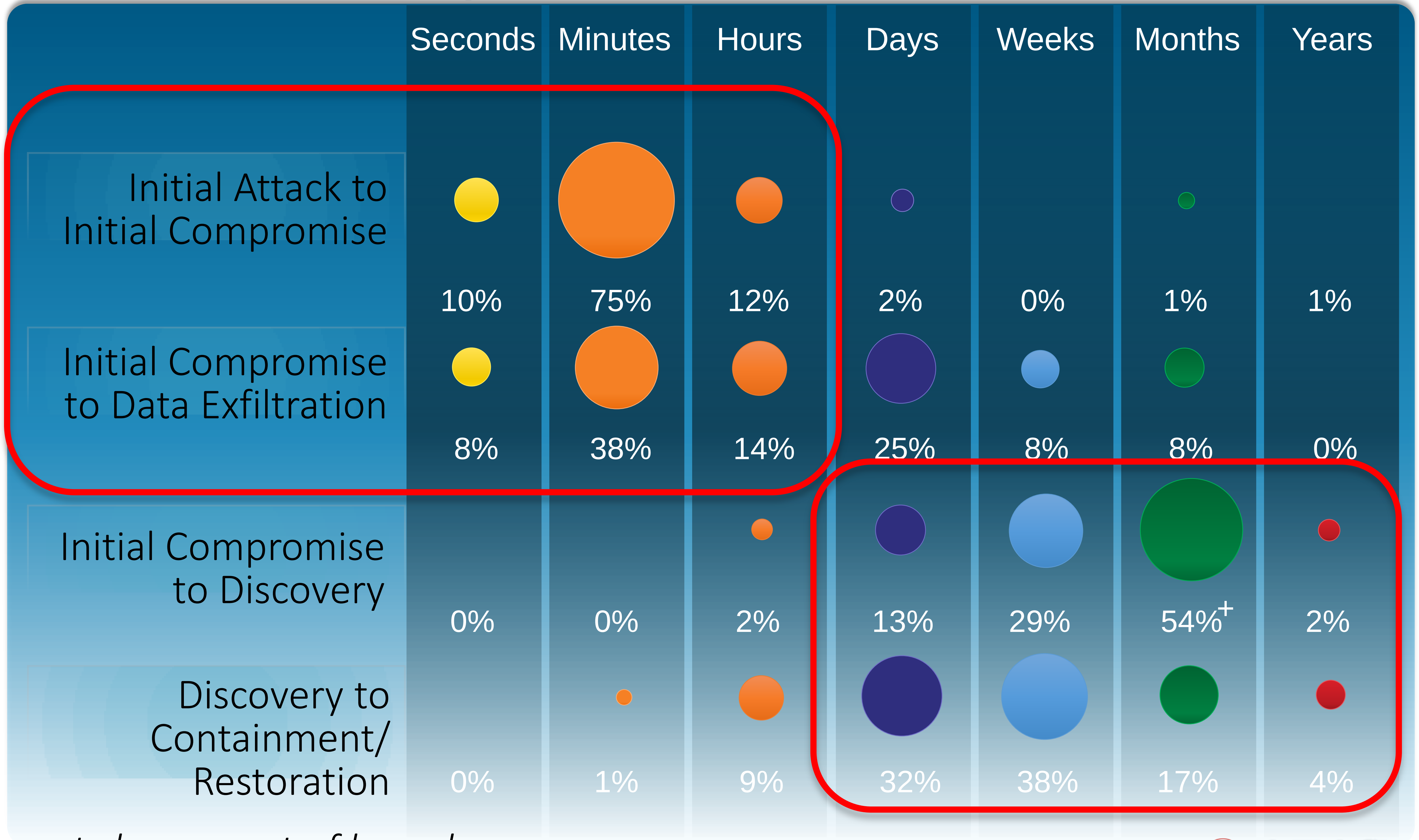
資料來源：
行政院資通安全會報

Breaches Happen In Hours ….

But Go Undetected For Weeks/Months

In 60% of breaches, data is stolen in hours.

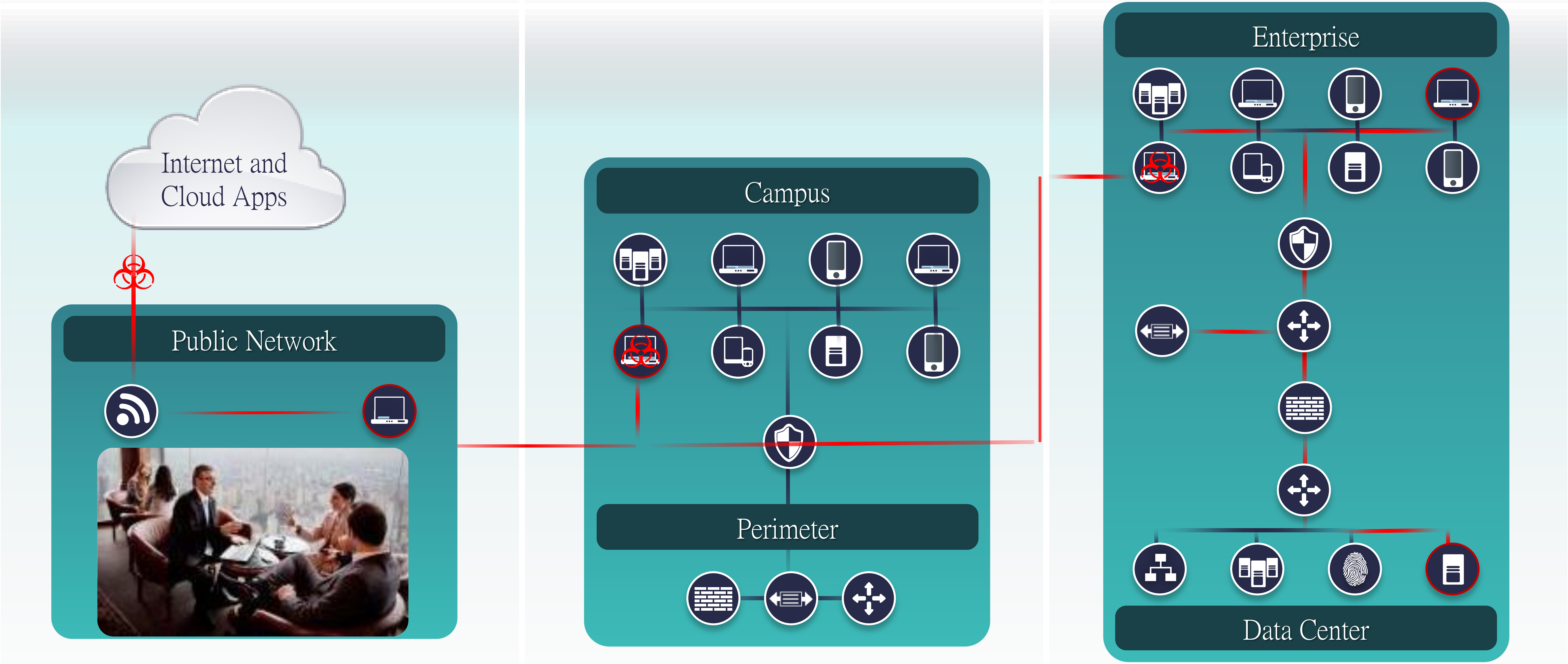
85% of breaches are not discovered for weeks.



	Seconds	Minutes	Hours	Days	Weeks	Months	Years
Initial Attack to Initial Compromise	10%	75%	12%	2%	0%	1%	1%
Initial Compromise to Data Exfiltration	8%	38%	14%	25%	8%	8%	0%
Initial Compromise to Discovery	0%	0%	2%	13%	29%	54%$^{+}$	2%
Discovery to Containment/ Restoration	0%	1%	9%	32%	38%	17%	4%

Timespan of events by percent of breaches

Anatomy of a Modern Threat

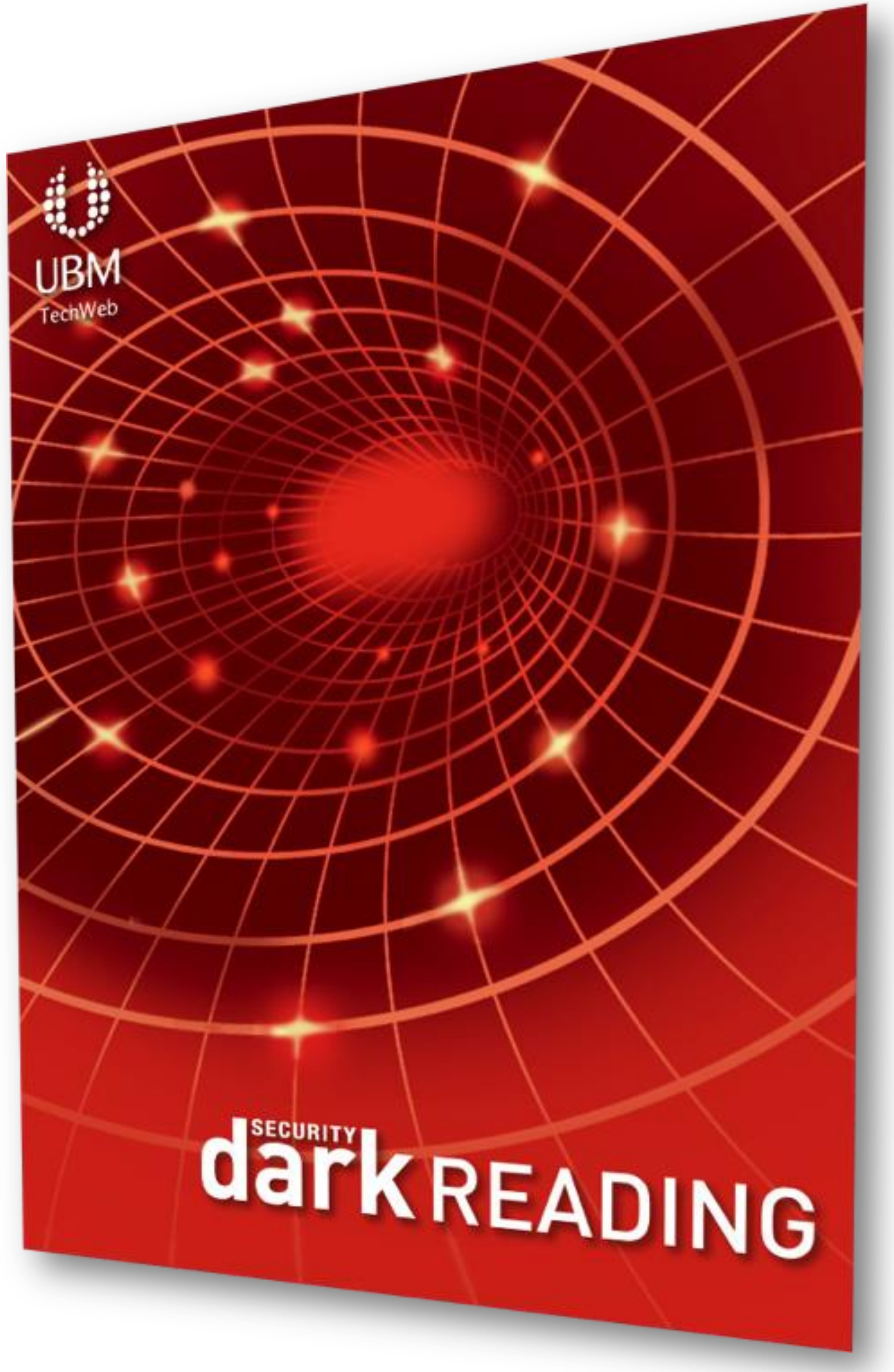


Infection entry point occurs outside of the enterprise

Advanced online threat bypasses perimeter defense

Threat spreads and attempts to exfiltrate valuable data

> “There's now a growing sense of fatalism: It's no longer if or when you get hacked, but the assumption that you've already been hacked, with a focus on minimizing the damage.”

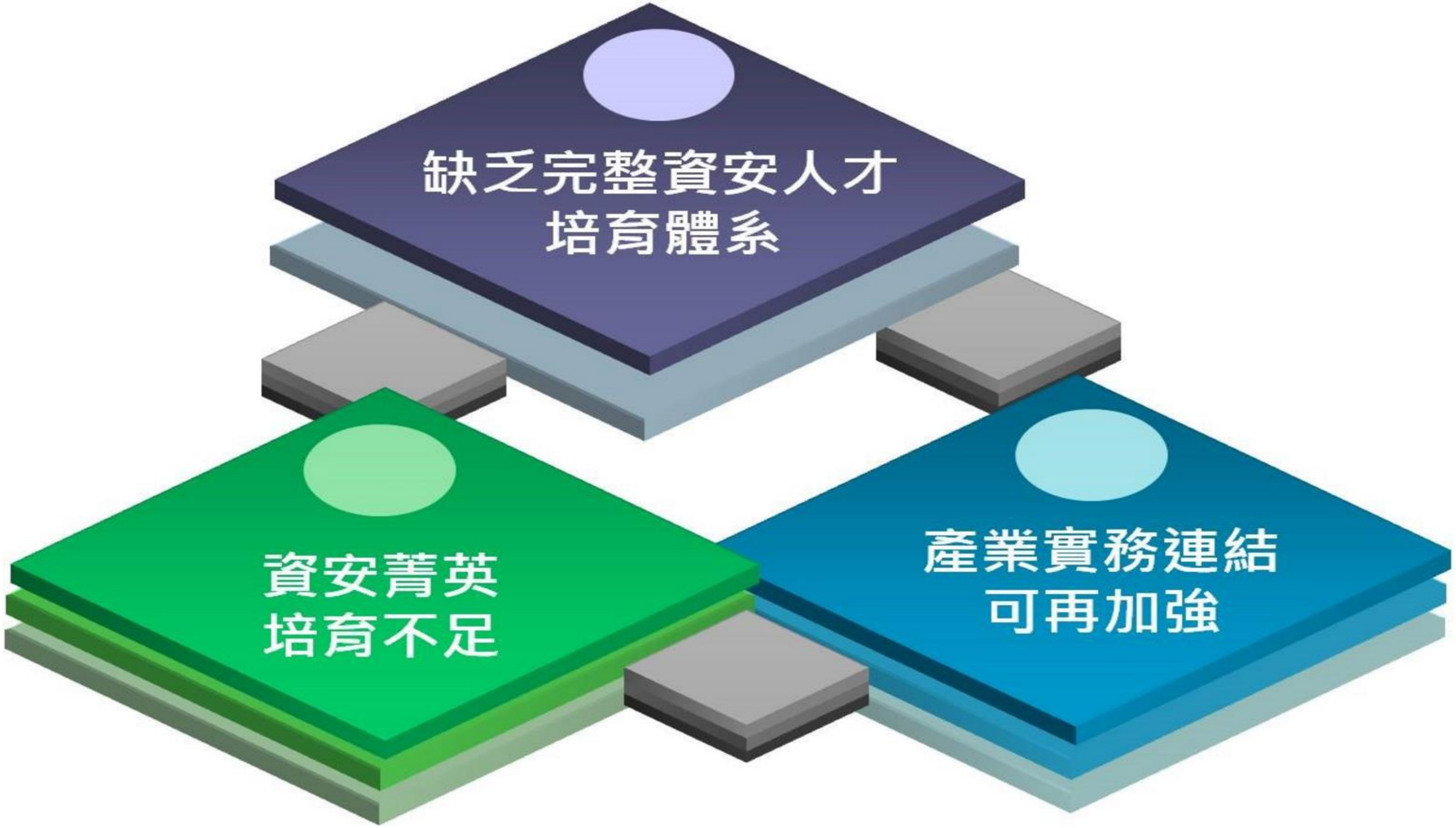


Source: *Security’s New Reality: Assume the Worst; Dark Reading*

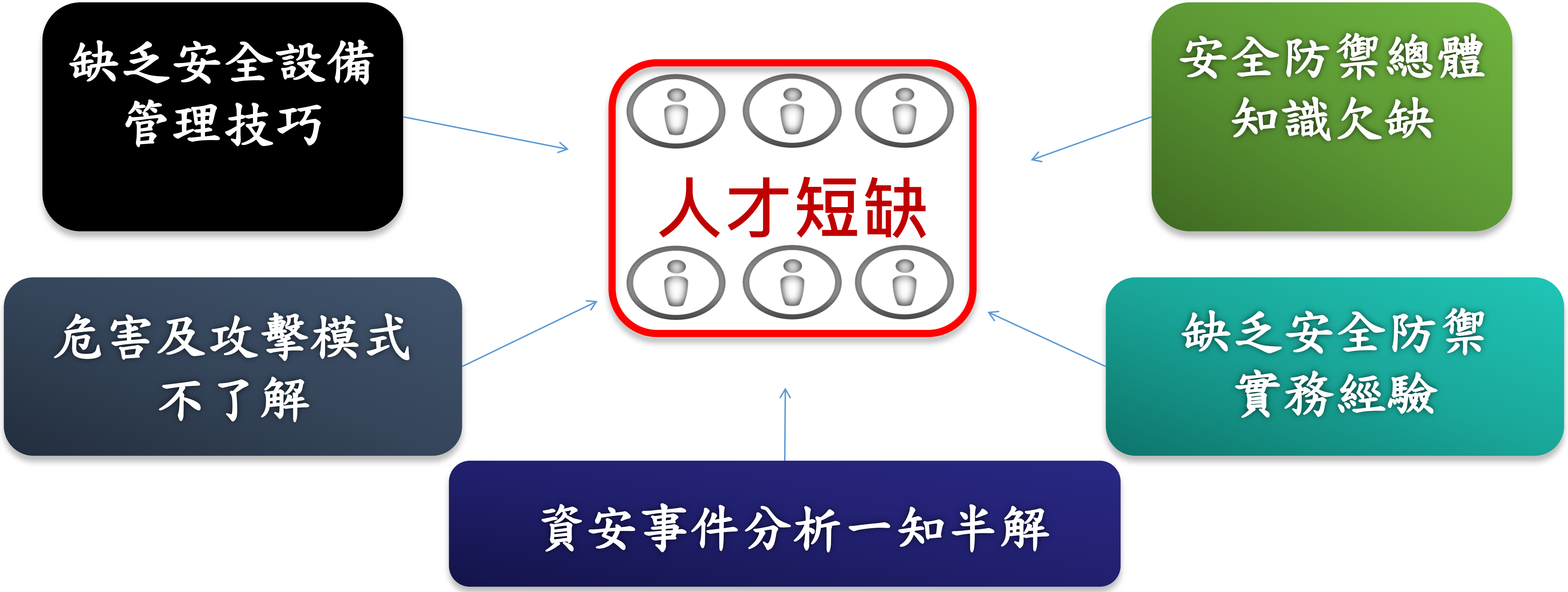
我們的資安捍衛戰士在哪裡?

人才培育的挑戰

如何培育量足質精的資安人才，以確保國家安全及社會穩定?



台灣產業資安防禦困境



人才短缺

缺乏安全設備管理技巧

安全防禦總體知識欠缺

危害及攻擊模式不了解

缺乏安全防禦實務經驗

資安事件分析一知半解

資訊安全維運基本要求

Cyber Security Operations Basics

VISIBILITY

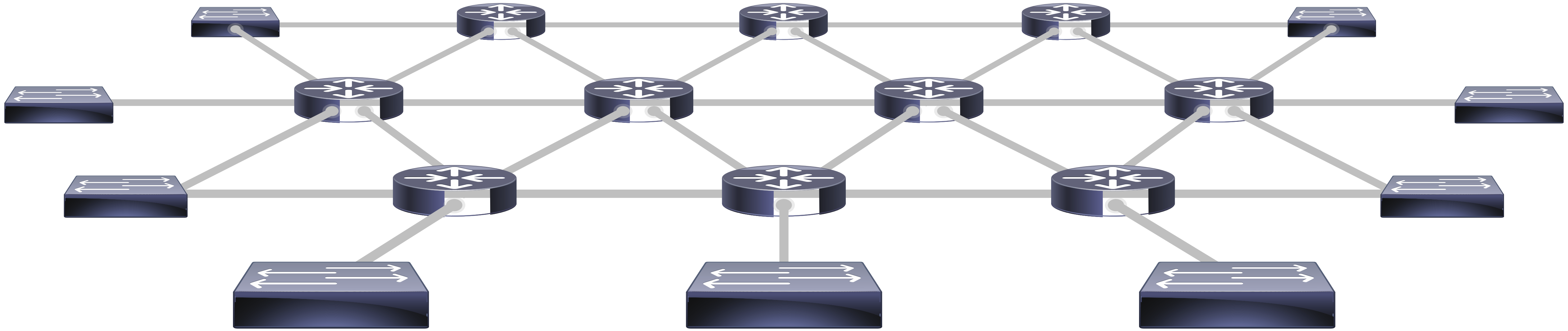
Deep Insight to Detect Advanced Threats

INTELLIGENCE

Contextual Awareness to Pinpoint Attacks

CONTROL

Ubiquitous Defense to Manage Threats



Visibility

Identity

User, device, access, location, time

AVC

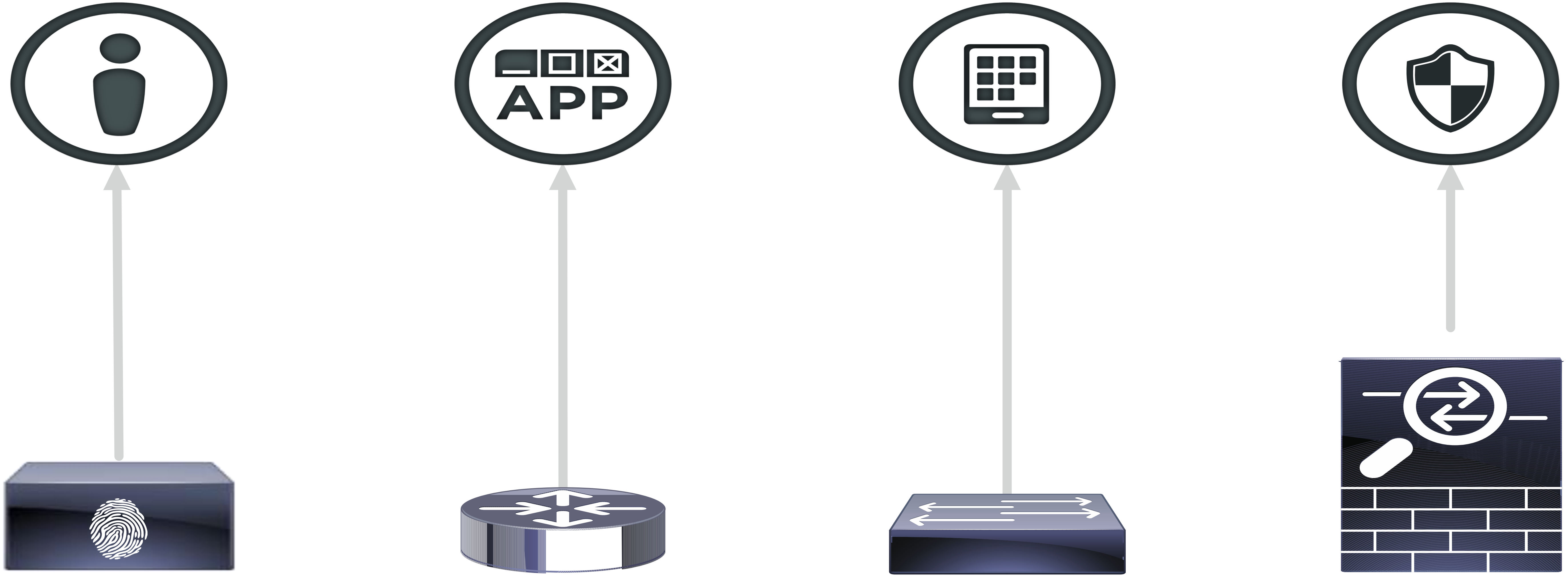
Application recognition and identification

NetFlow

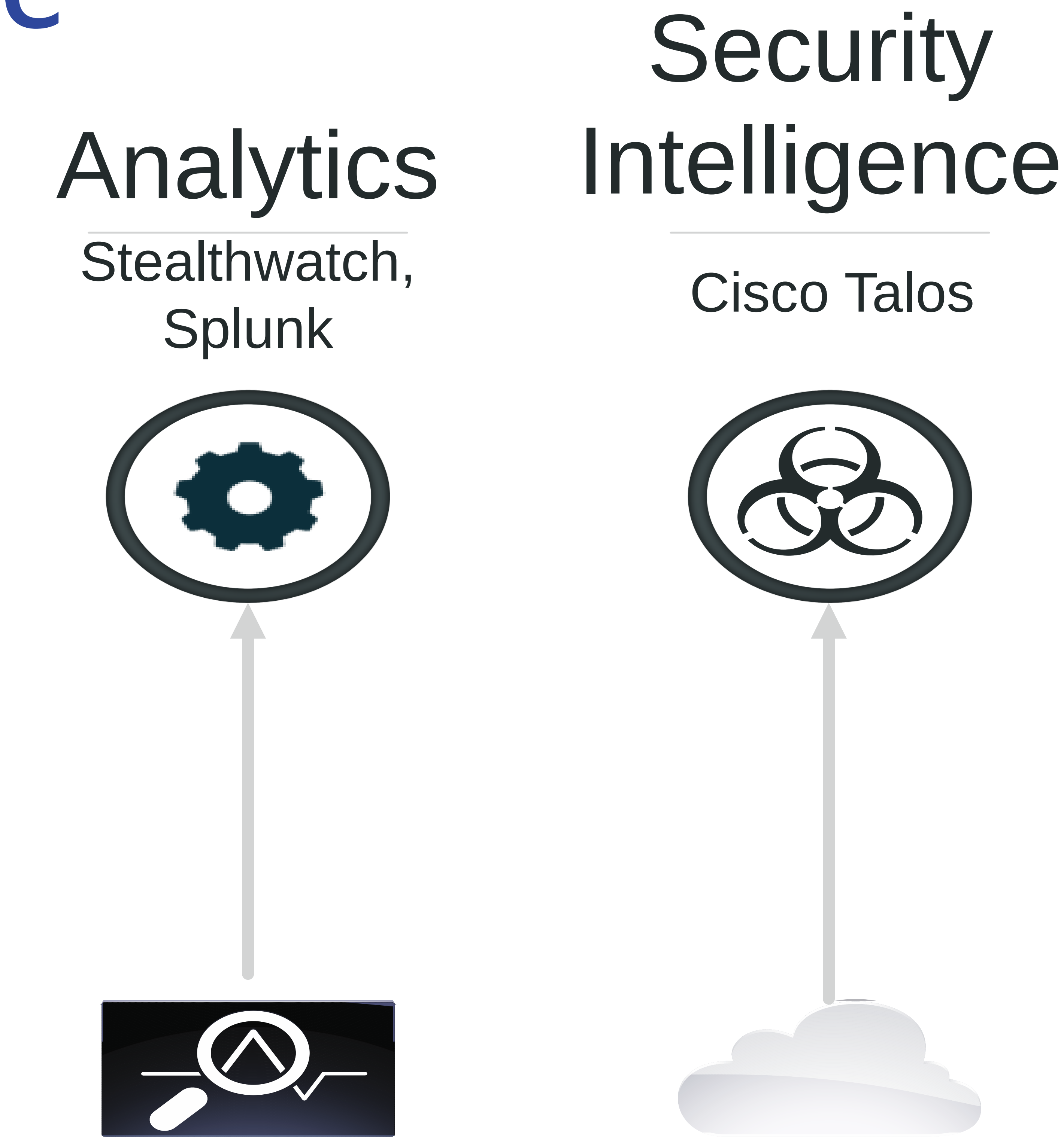
Network-wide traffic patterns

Security

Firewall, intrusion, web & email security



Intelligence



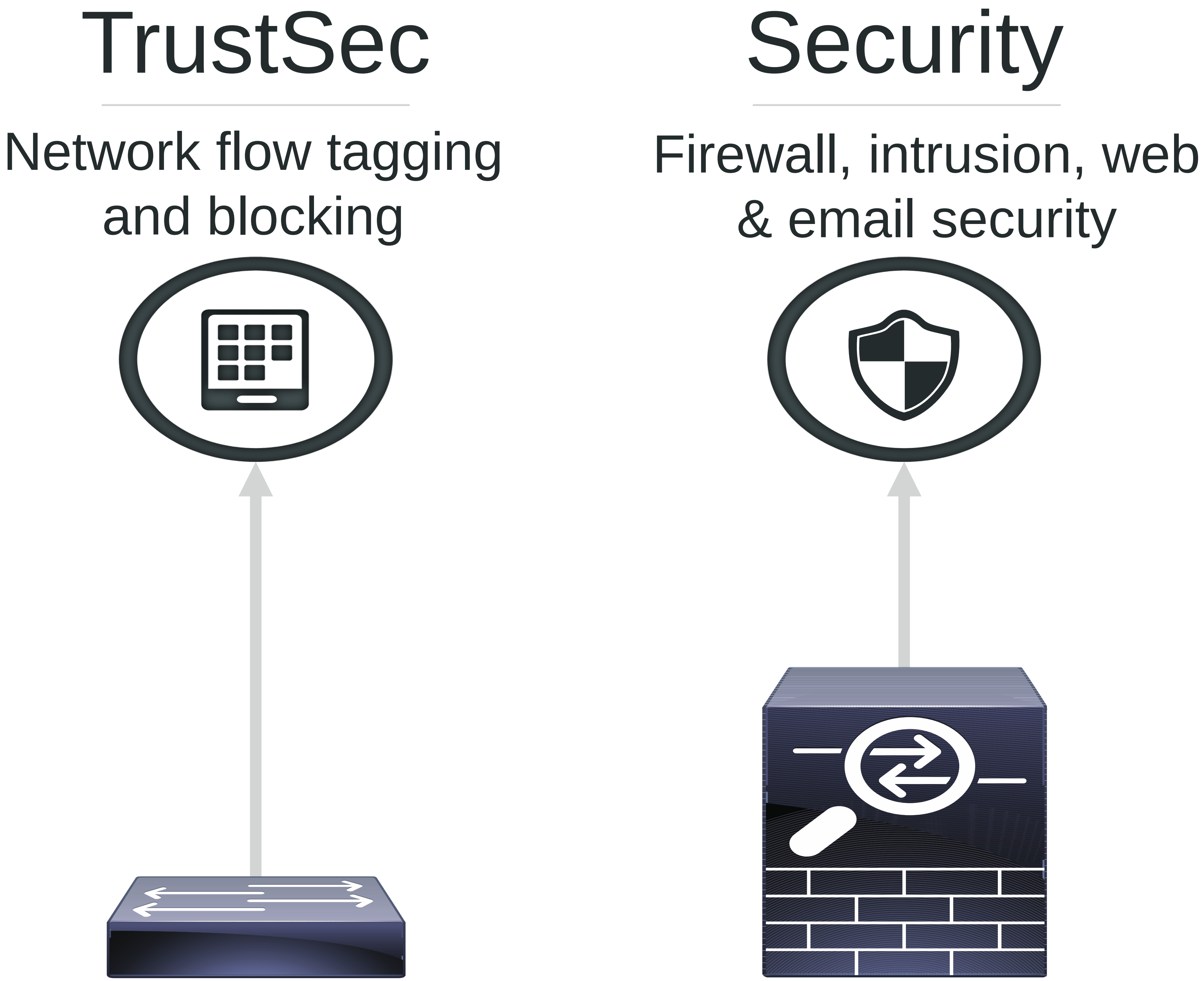
Analytics

Stealthwatch, Splunk

Security Intelligence

Cisco Talos

Control



TrustSec

Network flow tagging and blocking

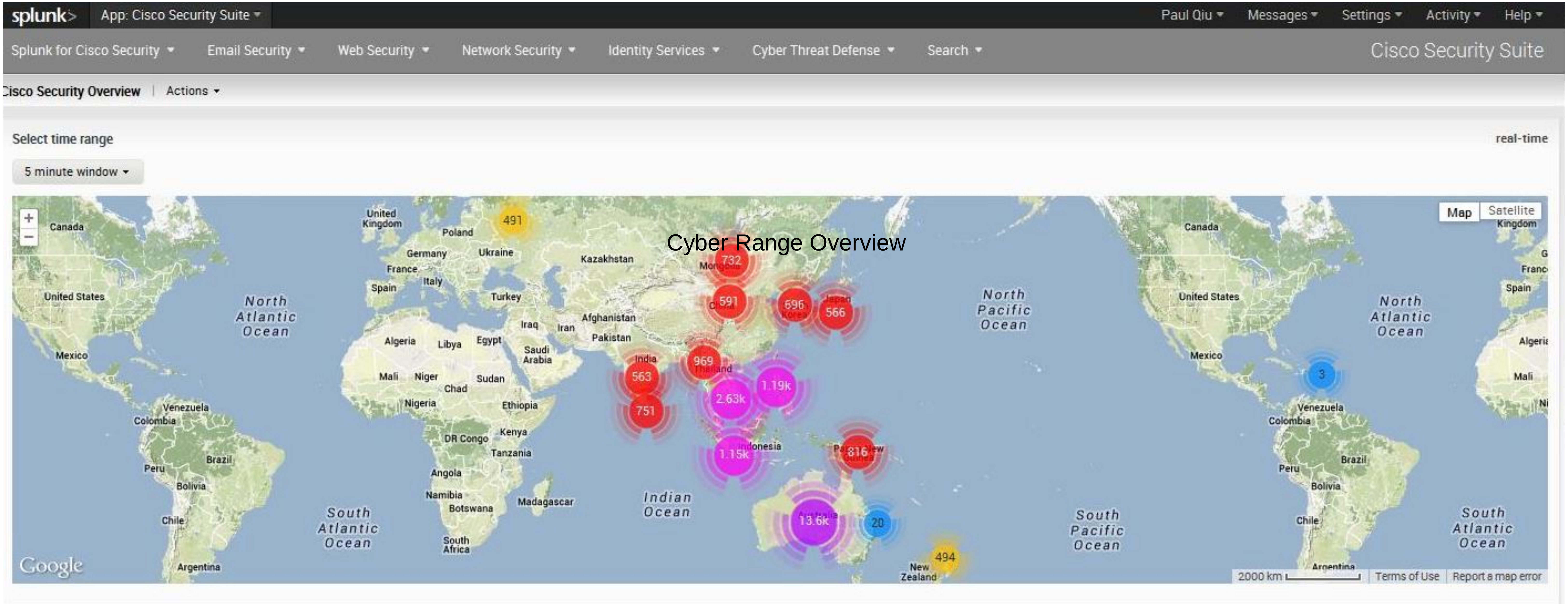
Security

Firewall, intrusion, web & email security

Cyber Range Service

Cyber Range Security Dashboard

A platform to experience the intelligent Cyber Security for the real world

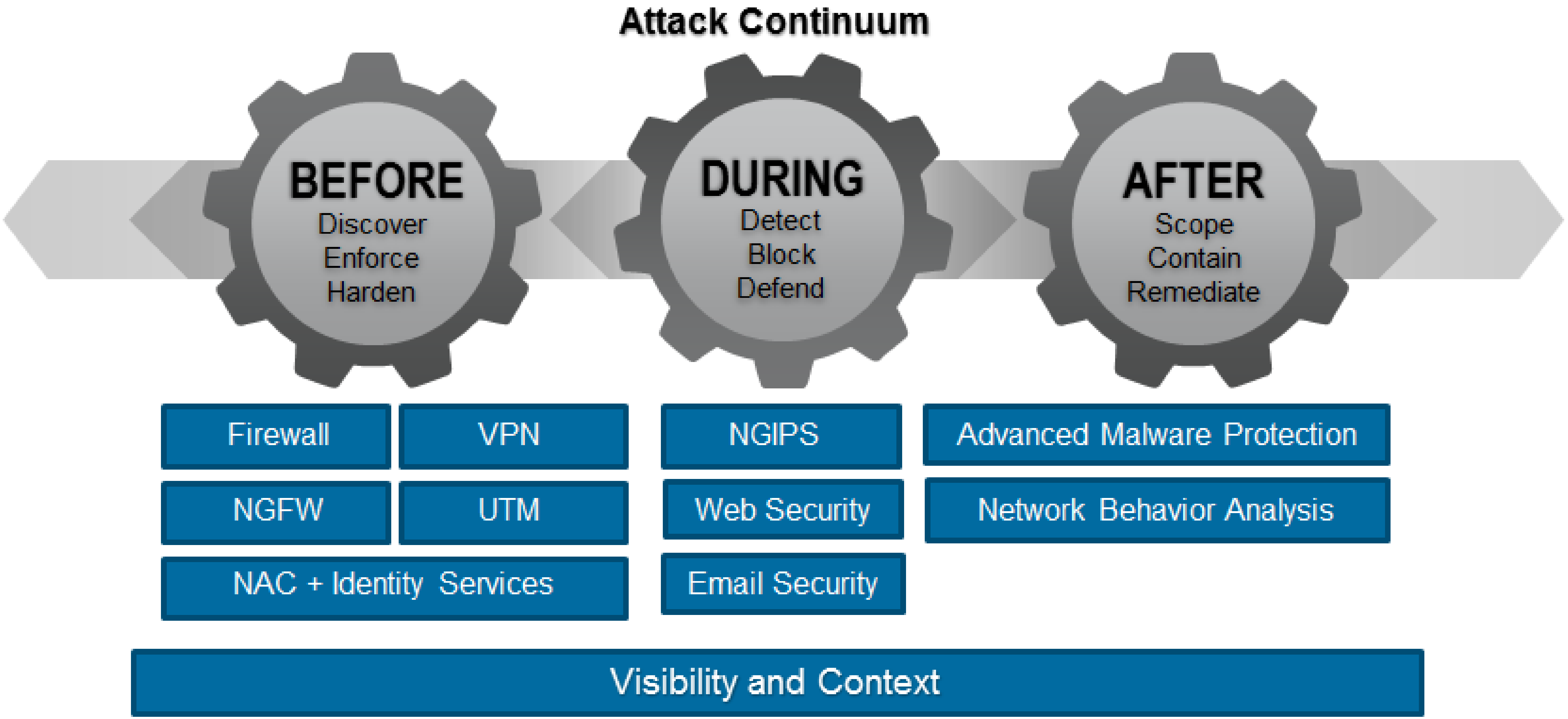


Select time range: 5 minute window

real-time

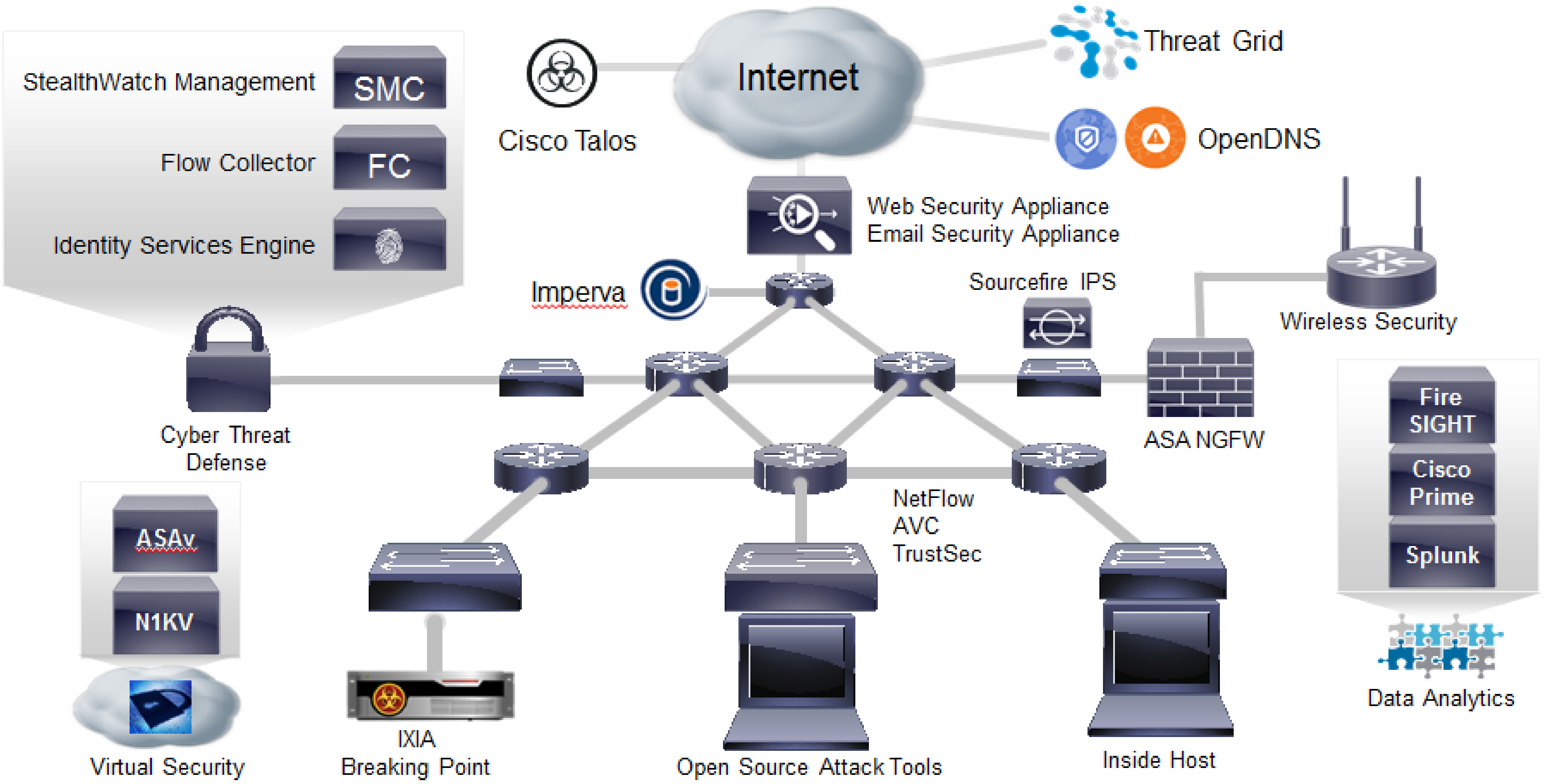
Cyber Range Overview

Covering The Entire Attack Continuum



TISNet 協志聯合科技 大同大學

Cyber Range Network Components Overview



TISNet 協志聯合科技 大同大學

Cisco Cyber Range Service Features

Infrastructure	Attacks	Visibility and Control
• Wired, wireless, and remote access • Network and routing • Client simulator • Server simulator • Application simulator • Traffic generation	• Day 0 Attack/New threats • DDoS • Network reconnaissance • Application attacks • Data Loss • Computer malware • Mobile device malware • Wireless Attacks • Evasion techniques • Botnet simulation • Open source attack tools • Virtual Network Attacks	• Global Threat Intelligence(Cloud) • Firewall & IDS/IPS • Signature based Detection • Behaviour based Detection • Data Loss Prevention • Web & email Security • Application Visibility & Control • Wireless Security • Identity & access management • Security and event management • Event correlation • Packet Capture and Analysis • Virtual Network Security • TrustSec-SGT • Software Defined Network

Cyber Warfare Teams

Red Team

AGENDA: Infiltrate networks to steal data and/or cause damage for publicity or gain.

Skill Set: High

LOCATION: Everywhere

Blue Team

AGENDA: Monitor and defend attacks against “Cyber Range Networks” and their clients.

Skill Set: High

LOCATION: Security Operations Centre

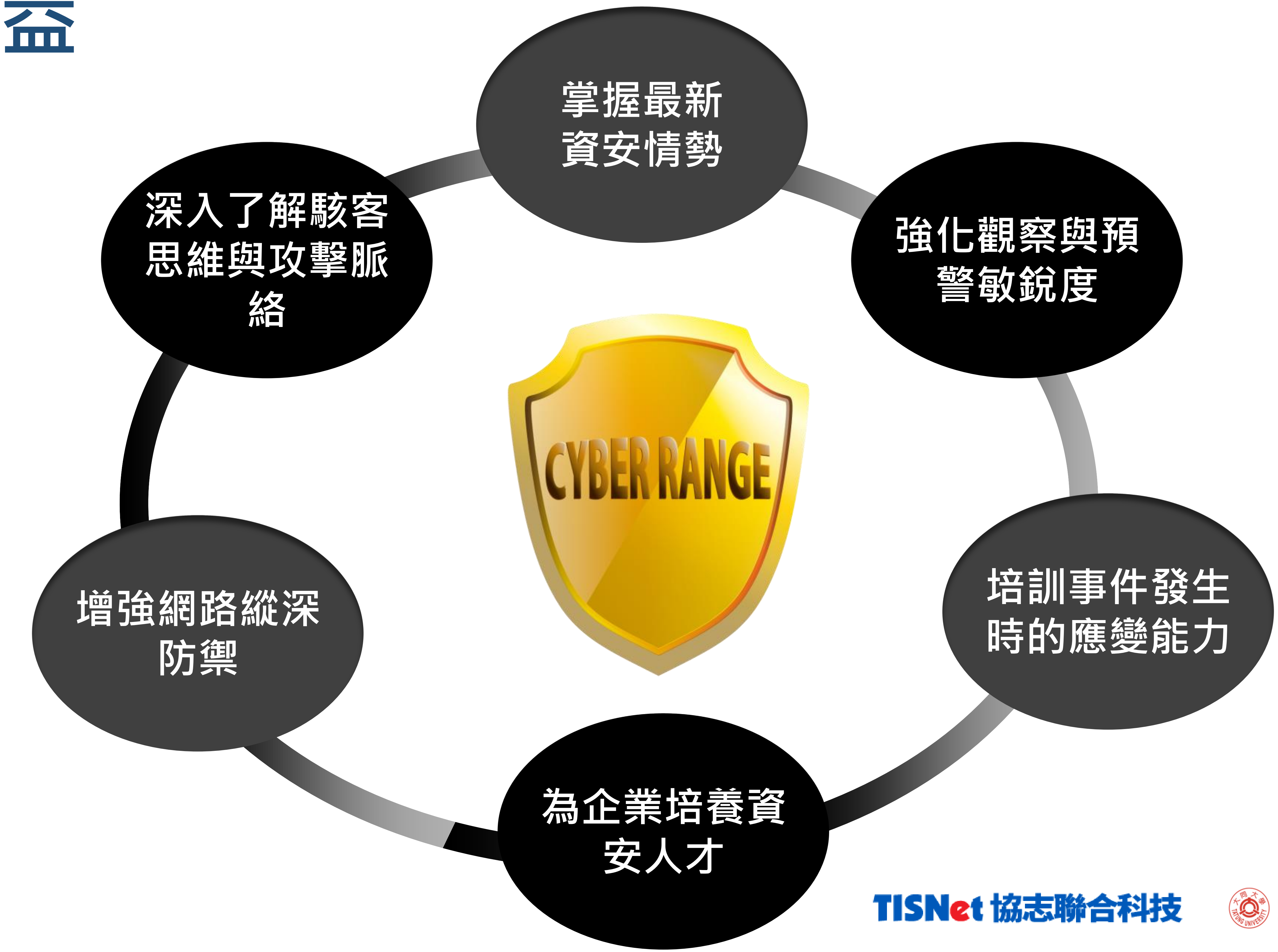
Green Team

AGENDA: Enhance knowledge of attack and defence strategies. Hopes to one day join the red or blue teams.

Skill Set: Varied

LOCATION: This room

演練效益



掌握最新資安情勢

強化觀察與預警敏銳度

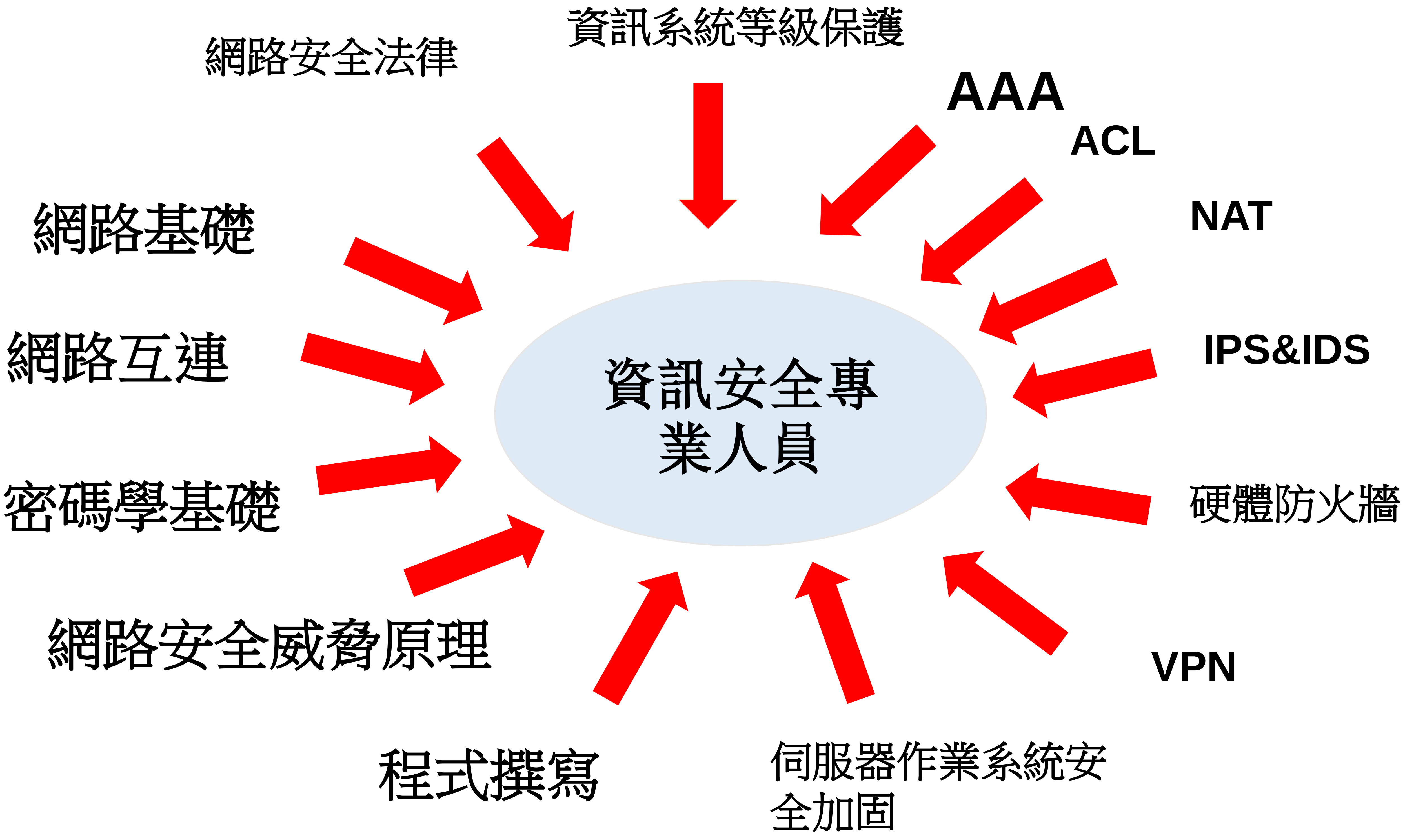
培訓事件發生時的應變能力

為企業培養資安人才

增強網路縱深防禦

深入了解駭客思維與攻擊脈絡

思科網路學會資安課程



資訊安全專業人員

網路安全法律

資訊系統等級保護

AAA

ACL

NAT

IPS&IDS

硬體防火牆

VPN

伺服器作業系統安全加固

程式撰寫

網路安全威脅原理

密碼學基礎

網路互連

網路基礎

思科網路學會資安課程與內容對應關係

思科網院資安相關課程	資安相關課程	安全知識點
ITE第12章	資訊安全導論/資訊安全基礎	Windows系統安全、家用無線局域網安全
網路安全簡介	資訊安全導論/資訊安全基礎	安全需求、安全攻擊、資訊保護、網路保護
CCNA1	電腦網路	OSI参考模型、TCP参考模型、TCP/IP協議、IP位址、乙太網
CCNA2、CCNA3	網路互聯/路由與交換/實用組網	靜態路由、預設路由、RIP、OSPF、VLAN、VLAN之間的通信、ACL、NAT
CCNA4	互連網路	VPN、ACL、LAN安全、SNMP、SPAN、障礙排除
網路安全基礎	資訊安全基礎	網路安全威脅、漏洞和攻擊、密碼學基礎、數位簽字、存取控制、高可用性、伺服器加固等
CCNA-SECURITY	電腦網路安全/防火牆技術/VPN技術	密碼學基礎、物理安全、ACL、AAA、IPS、IDS、802.1X、接入安全、硬體防火牆、各種VPN技術、網路安全測試技術
CCNA Cybersecurity Operations	網路安全與資訊對抗/資訊安全技術	網路安全中心、WINDOWS系統及安全加固、LINUX系統及安全加固、安全攻擊工具及攻擊、IP服務&企業服務及攻擊、終端安全保護、網路安全監控
python	Python程式設計	Python程式設計

CCNA Cyber Ops

Career-Ready
Step into your technology career

Now Ready on www.netacad.com!

Course Overview

CCNA Cyber Ops introduces the core security concepts and skills needed to monitor, detect, analyze and respond to sources of threats and vulnerabilities in computer networks. It emphasizes the practical application of the skills needed to respond to security events to maintain and ensure security operational readiness of secure networked systems.

Benefits

Students wants to begin a career in the rapidly growing area of cybersecurity operations at the associate level, with alignment to the Cisco CCNA Cybersecurity Operations certification.

Learning Components

- 13 chapters, quizzes, and chapter exams
- Virtual Machine Hands-on labs
- Certification practice exam, practice final, final exam and skills-based assessment

Features

Target Audience: Graduating students of technical colleges, community colleges

Prerequisites: None

Languages: English

Course Delivery: Instructor-led

Estimated Time to Complete: 70 hours

合作模式與總結

與學校之合作模式

- 短期培訓課程
- 長期租用
  - 連同設施與講師

總結

- 亞歷克．羅斯『未來產業』：未來第四大發光發熱產業是網路安全
- 台灣依據網路智慧新台灣政策白皮書，政府思考逐步擴大資安科研人才培育
- 資安專業人才培育不易且資安威脅不斷演進，資安人員也必須隨時充實專業知識以因應新的威脅情勢