

Rethinking Future Cyber Security

iThome總編輯 吳其勳





Today's Cyber Threats



Cyber threats are
too fast, too big,
and too widespread for
any of us to address
them alone.

—James Comey, former FBI Director



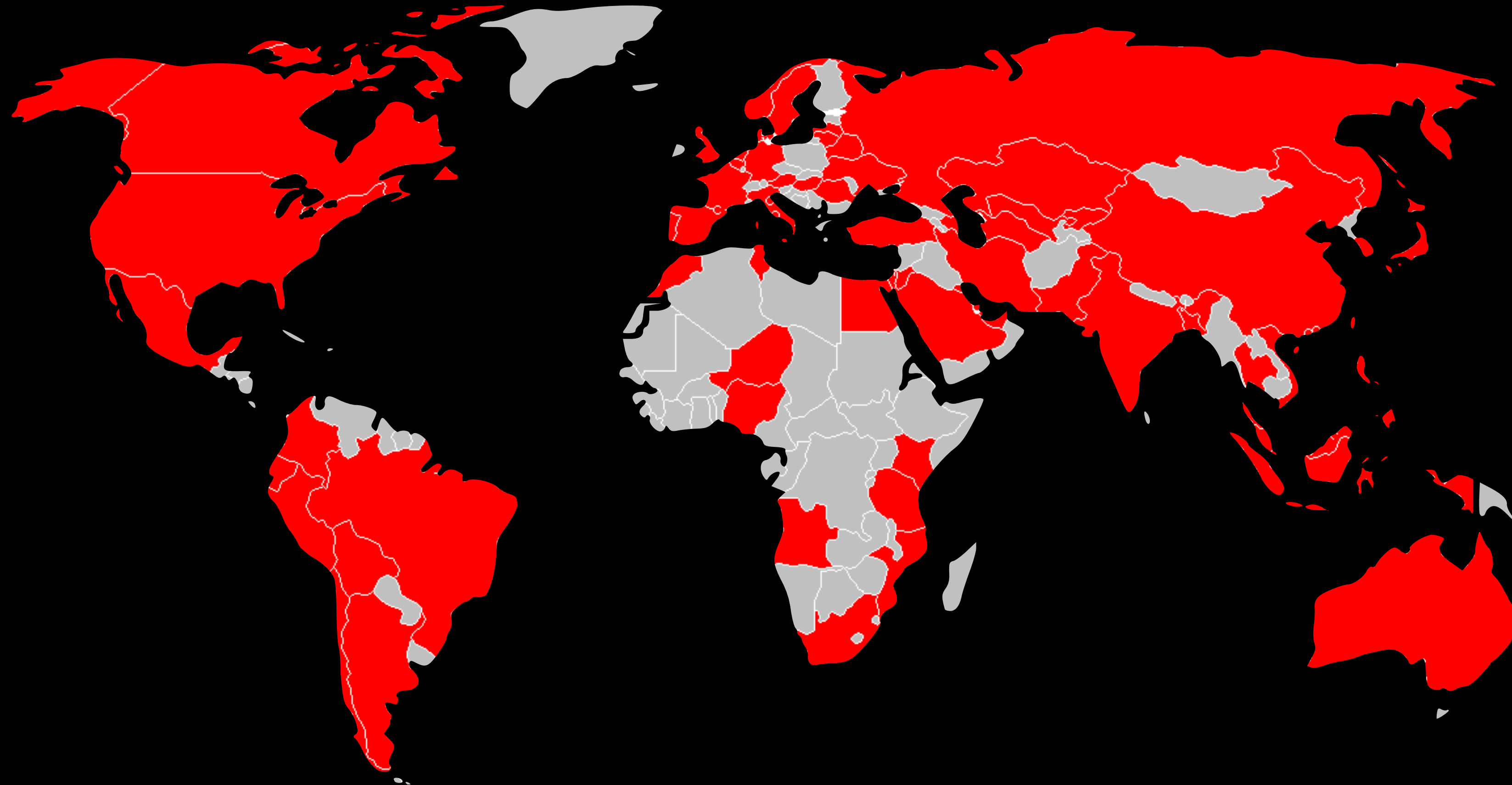
WannaCry

Ransomware Attack

Too Fast, Too Big & Too Widespread

WannaCry Ransomware Attack

12 May 2017 - 15 May 2017



4
days

300,000
computers
affected

150
countries
across the world



駭客搶銀行 SWIFT HACKED 盜轉18億

孟加拉央行

SWIFT
HACKED

盜轉10億美元
得手8100萬美元

THREAT ACTOR?

推測是

LAZARUS



國家網軍

網路黑道

恐怖組織

駭客主義

惡意員工

員工疏忽

**They are
coming for you**

遠銀SWIFT被駭事件，惡意程式特別針對遠銀系統打造，內建
2組駭客早已取得的遠銀帳密，嘗試登入所有系統

EQUIFAX[®]

DATA BREACH

1.43億美國人的個資外洩

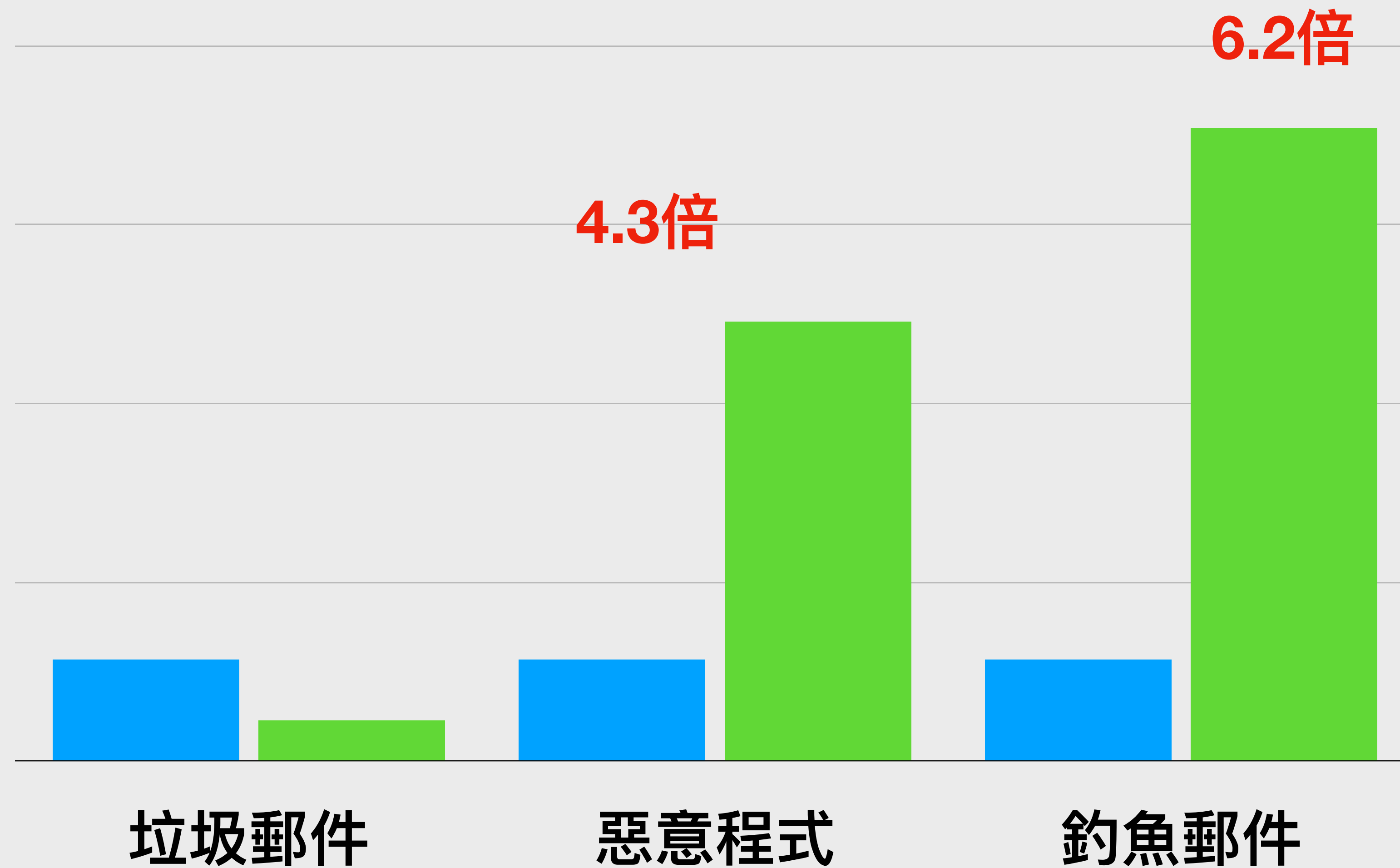
44.2%美國總人口



**網路釣魚
猖獗**

網路釣魚郵件激增

個人信箱
企業信箱



BEC 商業郵件詐騙



2017年

臺灣BEC詐騙總額

1億8736萬元

垃圾郵件

惡意程式

釣魚郵件

6.2倍

CLOUD LEAK

UBER：5千萬用戶資料、7百萬駕駛個資被竊

肇因於被駭客找到Uber的Github程式庫含有帳密資料

美國共和黨承包商放在AWS S3的1TB資料外洩

美國NSA情報平臺放在AWS S3的100GB機敏文件外洩

1.23億放在AWS S3的美國家庭資訊外洩




Start Cleaning


Go Home


Mode Settings


00:00:00



IoT安全
Security by Design

硬體安全



CIIP 關鍵基礎設施防護

A wide-angle photograph of a lush forest during autumn. Tall, slender trees with green and yellowing leaves stand against a sky with soft, white clouds. The foreground is filled with vibrant green grass. Large, bold white text is centered over the image.

平靜的週末
心存感激...

The background is a dark, futuristic digital interface. It features a glowing blue world map in the center. To the left, there's a table with data for various countries. To the right, there are several line graphs and charts with green and blue lines. The overall aesthetic is high-tech and data-driven.

Germany	Mullingen	1000000
Holland	Leiden	1000000
Portugal	Sabugal	1000000
Italy	Alm	1000000

Performance Comparison

Equipment Efficiency

Good products

Manual Correction

Disposed

威脅是複雜、動態的

ADAPTIVE DEFENSE

ACTIVE DEFENSE

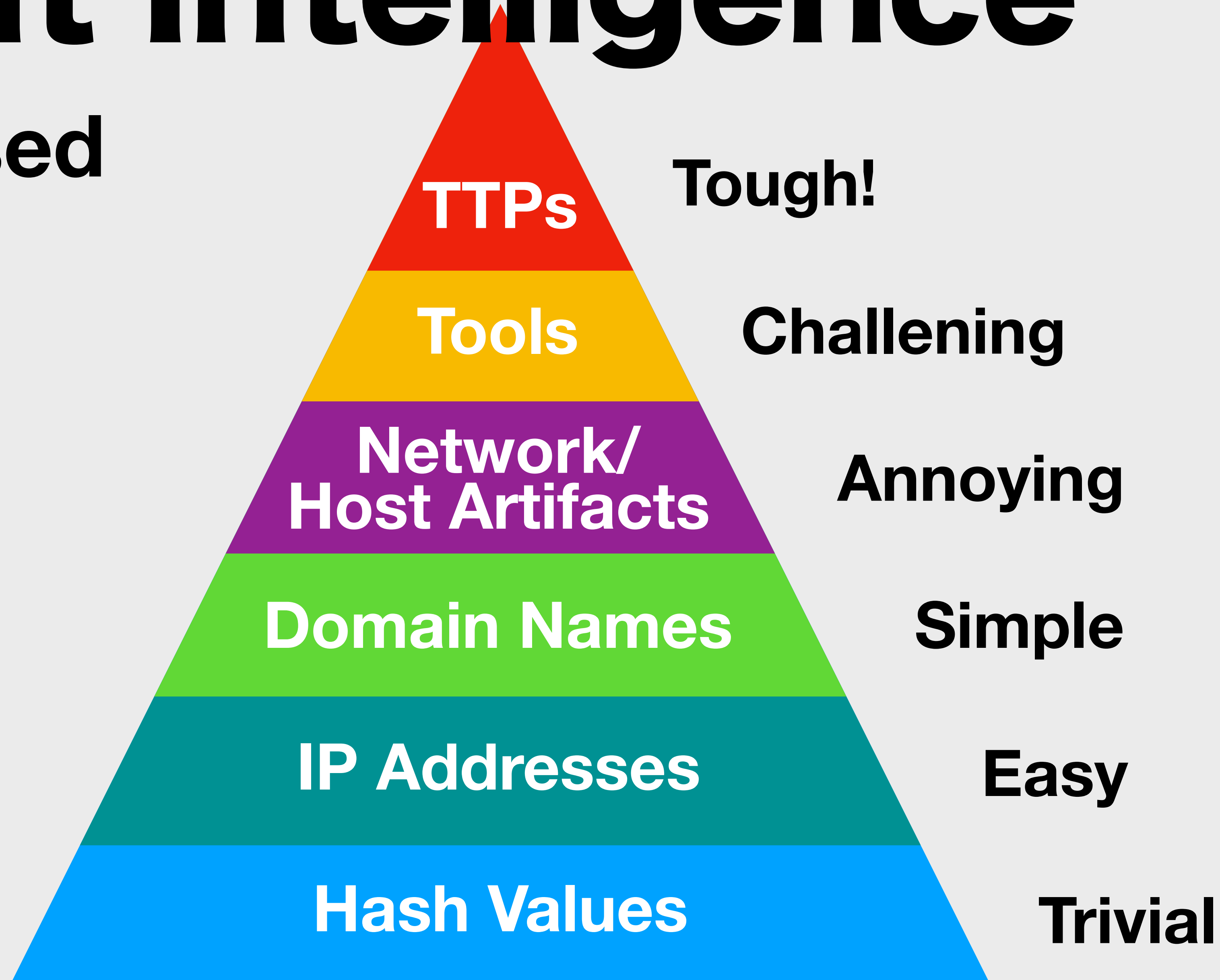
PROACTIVE DEFENSE

Threat Intelligence

**Threat-based
Defense**

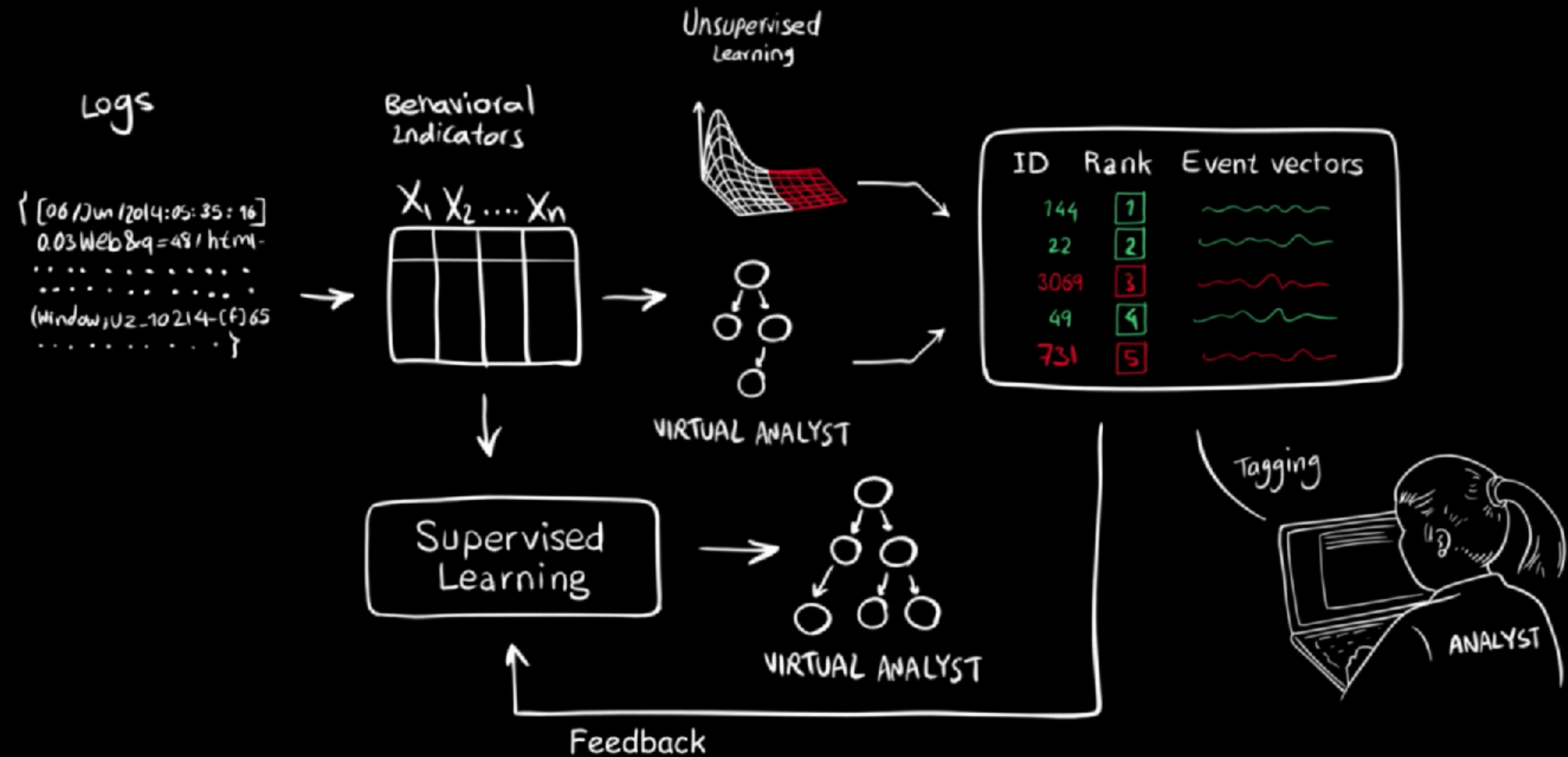
**Pyramid
of Pain**

David Bianco



AI 新資安

Day 2





RED TEAM

RED TEAM



Think like
the “Enemy”



RED TEAM

#

PENTEST

RED TEAM

CASE #1

目標：取得顧客個資

一國際知名軟體公司以取得顧客個資為目標，採取紅隊測試，最後找到公有雲服務竟有門戶大開、未設密碼的帳戶；肇因於事前測試公有雲服務發生整合問題，在不採用密碼管制權限後，問題即解決了，然而在問題解決後卻又忘了回復密碼管制。

RED TEAM

CASE #2

目標：取得公司商業機密

一公司以委託紅隊測試服務，以取得公司商業機密為目標。由於受測公司擁有強健的資安防護，經過兩個月的網路攻擊，包括系統漏洞、釣魚郵件等，皆無成效，事以至此，一般滲透測試服務就是出具報告，證明該公司防安防護極佳；然而紅隊測試轉而尋求其他方式，最後混入年度Kick-off會議，成功取得公司商業機密

DECEPTION

兵者，詭道也。

故能而示之不能，用而示之不用，
近而示之遠，遠而示之近。

-孫子兵法

WENCHESTER MYSTERY HOUSE

The image shows a large, multi-story house with a complex red-tiled roof. The house has multiple gables and a prominent white decorative cornice. The roof is covered in red tiles, and there are several small dormer windows. The house is surrounded by trees, and the sky is overcast.

蓋了38年的大怪屋
160間房間、2000扇門、10000扇窗



你不能決定敵人,但你可以決定戰場



CYBER INSURANCE
SITUATION AWARENESS
ZERO TRUST NETWORK
BUG BOUNTY



GDPR

General Data Protection Regulation

GDPR實施要點

- 2108年5月25日正式實施
- 只要公司擁有歐盟公民的個資，就適用規範
- 企業必須設置資料保護長
- 強化個人資料可攜權的權利
- 新增被遺忘權
- 個資外洩發生，必須在72小時內通報主管機關
- 個資保護系統預設納入隱私保護
- 個資當事人有權反對被自動化分析
- 要求企業落實資料保護影響評估
- 提高罰款，最高達2千萬歐元，或罰以企業年度全球營業額4%罰金



A close-up photograph of several people's hands and forearms joined together in a circle, symbolizing teamwork and collaboration. The person on the left wears multiple beaded bracelets. The person on the right wears a black leather watch. In the foreground, there is a desk with a water bottle, a jar of snacks, and a pen holder.

Collaboration

Thank You!

