CROWDSTRIKE

資安的零信任觀念如何應用在現實環境中

張閔壽
技術經理
敦陽科技股份有限公司 Stark Technology Inc

Stark Technology Inc.
敦陽科技股份有限公司

1. 什麼是零信任
2. 零信任 與 NIST 800-207
3. 零信任 7 大原則
4. 建立零信任策略的 5 個步驟
5. 資安的零信任觀念如何應用在現實環境中
6. 導入零信任的 7 個提問

什麼是零信任

2010 年由 John Kindervag 提出

Zero Trust is a powerful concept, but the recent hype surrounding it has led to numerous interpretations. Agreeing to a term set that defines the concept will greatly improve the ease with which we can then implement this Zero Trust strategy. This is why we'd like to introduce the Zero Trust dictionary, an authoritative lexicon with definitions and terminology defined by John Kindervag, the Creator of Zero Trust.

THE ZERO TRUST DICTIONARY

An authoritative lexicon on Zero Trust terminology

Zero Trust is everywhere. Everyone is talking about it and writing about it. That's why we have summarized the most essential information about authentic Zero Trust in one authoritative lexicon. If you're looking for structured information about this security strategy, this is a must-read.

In this edition we cover the following topics:

- **The key concepts** of Zero Trust
- **Design principles** of a Zero Trust network
- **5 steps** to **implementing** Zero Trust
- **Zero Trust terms** explained
- The Zero Trust **Maturity model**

DOWNLOAD

https://on2it.net/john-kindervag/#zt-dictionary

什麼是零信任？

- 零信任是一種策略，有助於防止組織的資料洩漏。
- 零信任原則「絕不信任，始終驗證」，是一種能引起高層共鳴的策略，可以使用現成的技術達成戰略部署。
- 零信任策略與技術脫鉤，因此技術雖然會隨著時間變化，但是零信任策略依然相同。

ZERO TRUST

Zero Trust is a strategic initiative that helps prevent successful data breaches by eliminating digital trust from your organization. Rooted in the principle of "never trust, always verify," Zero Trust is designed as a strategy that will resonate with the highest levels of any organization, yet can be tactically deployed using off-the-shelf technology. Zero Trust strategy is decoupled from technology, so while technologies will improve and change over time, the strategy remains the same.

百花齊放的零信任

網路：

雲：

身份訪問管理：

網路安全：

CDN：

防毒：

伺服器虛擬化：

YouTube

ZERO TRUST WEBINAR

How Microsoft does Zero Trust

Microsoft 365

觀看次數：8153次 • 7 個月前

字幕

Webinar - The What, Why and How of Implementing a Zero...

Symantec

觀看次數：943次 • 9 個月前

Zscaler Zero Trust Webinar

BytesTechnology

觀看次數：759次 • 2 年前

Webinar: Zero Trust Services in Kubernetes

CNCF [Cloud Native Computi...

觀看次數：5673次 • 10 個月前

4K

Webinar - How Enterprises Can Effectively Operate Zero...

Symantec

觀看次數：619次 • 8 個月前

How Zero Trust improves security and the user...

Cisco Nederland

觀看次數：1.3萬次 • 1 年前

How to Create a Comprehensive Zero Trust...

Cisco

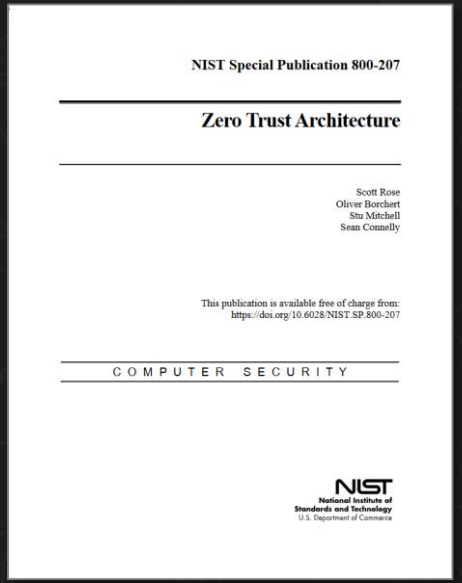
觀看次數：485次 • 6 個月前

Webinar Zero-Trust and Strong Customer...

Keyless

觀看次數：2次 • 1 天前

零信任 與 NIST SP 800-207



NIST Special Publication 800-207

Zero Trust Architecture

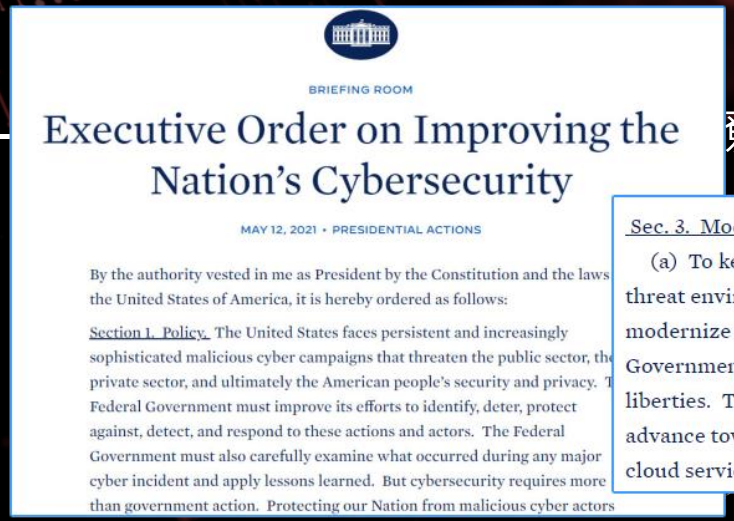
Scott Rose
Oliver Borchert
Stu Mitchell
Sean Connelly

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-207

COMPUTER SECURITY

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

- 2020年8月，NIST 公布 SP 800-207 標準文件
- 2021年5月12日，美國總統拜登下達行政命令，推動美國聯邦政府網路安全現代化，要求導入零信任架構的網路安全策略。
- 這份行政命令中，規定當地政府機構要在 60 天內，制定實施 ZTA（Zero Trust Architecture）的計畫，並參考 NIST 標準文件指引的導入建議。
- 由 NIST 公布的 SP 800- 瞭解 ZTA 的重要參考依據。



BRIEFING ROOM

Executive Order on Improving the Nation's Cybersecurity

MAY 12, 2021 • PRESIDENTIAL ACTIONS

By the authority vested in me as President by the Constitution and the laws the United States of America, it is hereby ordered as follows:

Section 1. Policy. The United States faces persistent and increasingly sophisticated malicious cyber campaigns that threaten the public sector, th private sector, and ultimately the American people's security and privacy. T Federal Government must improve its efforts to identify, deter, protect against, detect, and respond to these actions and actors. The Federal Government must also carefully examine what occurred during any major cyber incident and apply lessons learned. But cybersecurity requires more than government action. Protecting our Nation from malicious cyber actors

Sec. 3. Modernizing Federal Government Cybersecurity.

(a) To keep pace with today's dynamic and increasingly threat environment, the Federal Government must take de modernize its approach to cybersecurity, including by incr Government's visibility into threats, while protecting priva liberties. The Federal Government must adopt security be advance toward Zero Trust Architecture; accelerate move cloud services, including Software as a Service (SaaS), Infr

零信任 7 大原則

零信任 7 大原則

一. 所有的資料來源與運算服務都要被當作是資源。

二. 不管哪個位置的裝置通訊，都需確保安全。

三. 對於企業資源的存取，必須針對每次連線為基礎作許可審核。

四. 資源的存取應該要基於用戶端識別、應用服務、資安觀察狀態，以及包含的行為或環境，動態決定。

零信任 7 大原則

五. 企業必須監控與衡量所有相關資訊資產的正確性與安全狀態。

六. 在允許存取之前，所有的資源的身分鑑別與授權機制，都要依監控結果動態決定，並且嚴格落實。

七. 企業應該要盡可能收集有關資訊資產、網路架構、骨幹，以及通訊的現況，並用這些資訊來增進安全狀態。

建立零信任策略的 5 個步驟

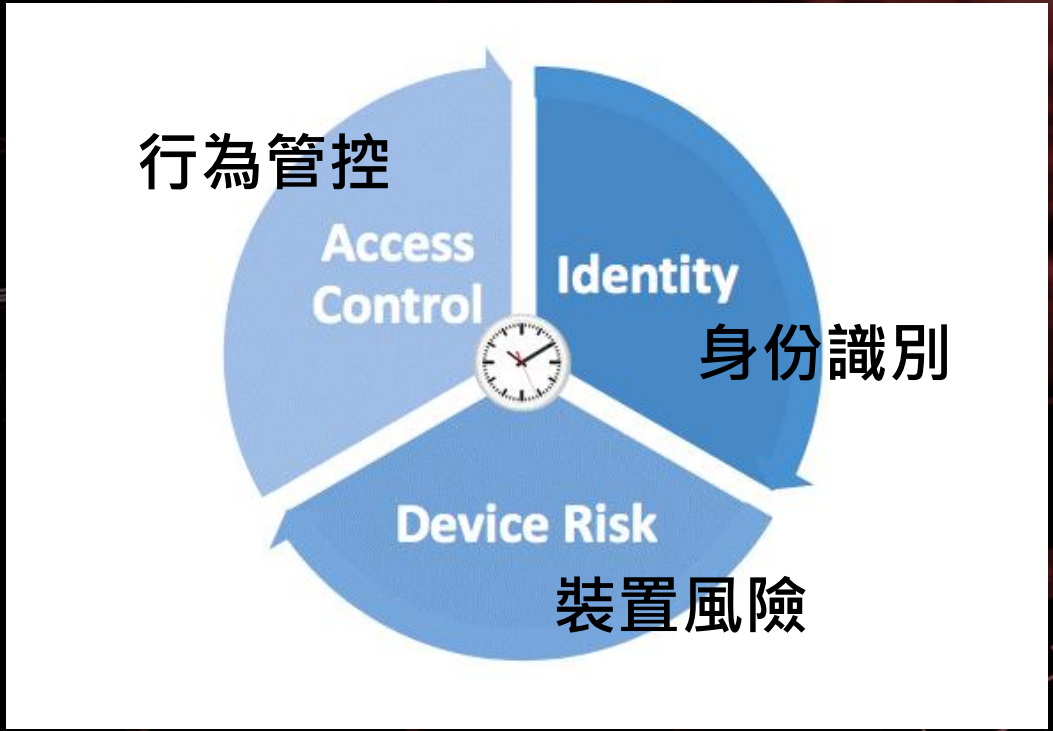
建立零信任策略的 5 個步驟

- 步驟 1. 存取任何網路資源都需要即時驗證
- 步驟 2. 定義設備信任
- 步驟 3. 以使用者為中心，定義個人化安全基準
- 步驟 4. 收集使用案例
- 步驟 5. 逐漸擴大規模

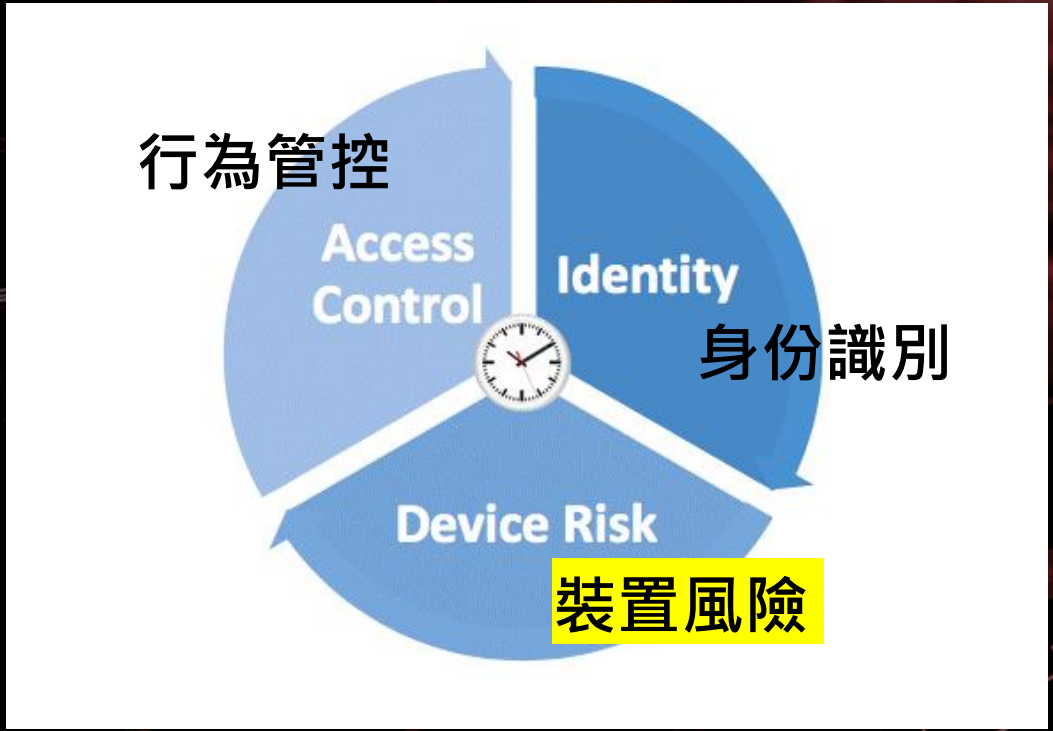
資安的零信任觀念如何應用在現實環境中

CROWDSTRIKE

建立零信任策略的三個面向



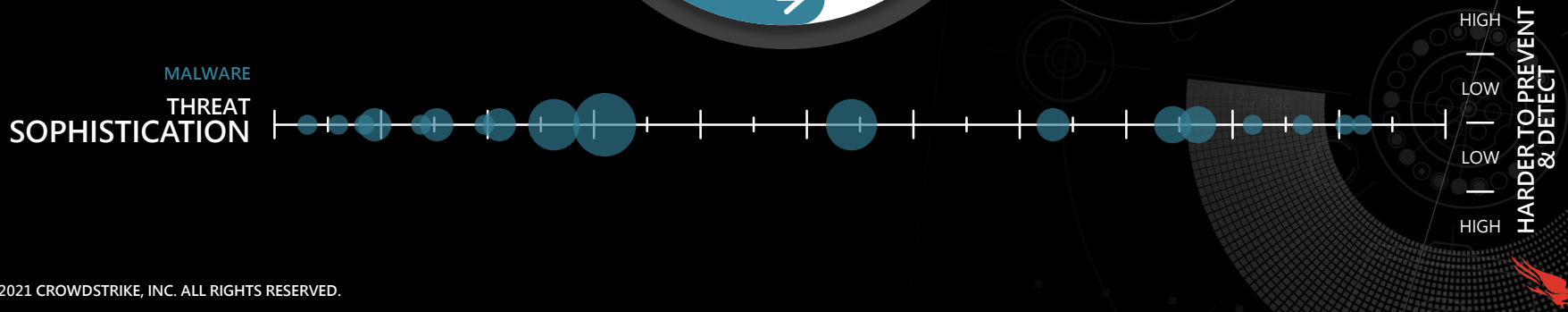
建立零信任策略的三個面向



現時防禦措施討論

惡意檔案攻擊

32%



CROWDSTRIKE

現時防禦措施討論

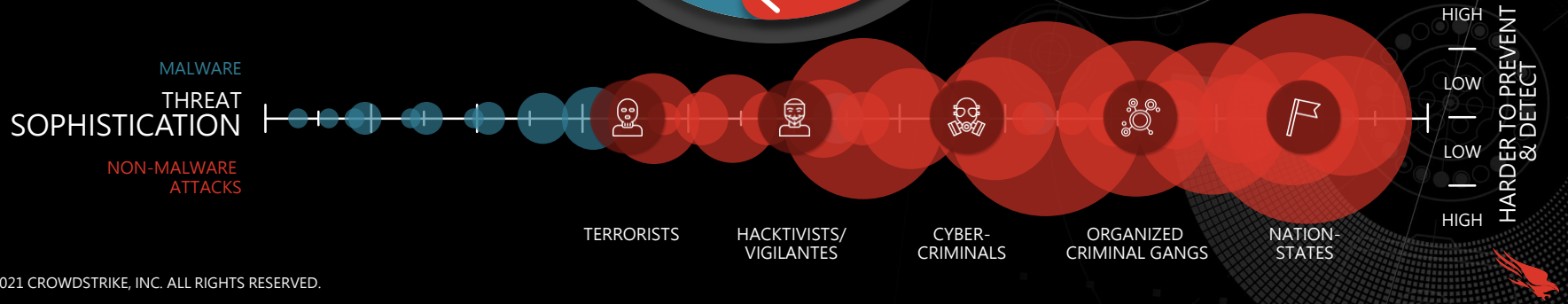
惡意檔案攻擊

32%

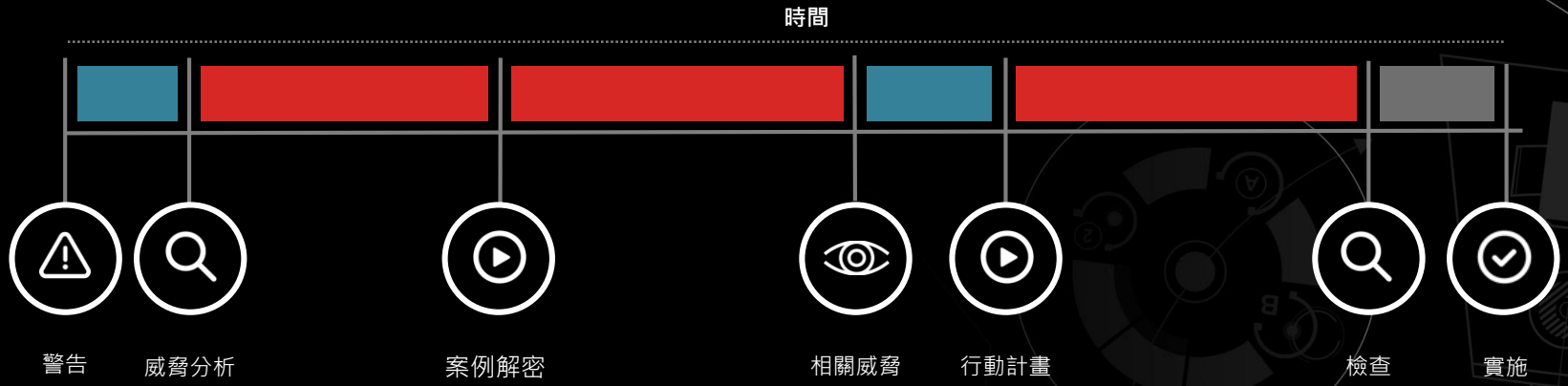
YOU NEED COMPLETE
BREACH
PREVENTION

非惡意檔案攻擊
(無檔案式攻擊)

68%



面對進階攻擊的回應時間過長



面臨的挑戰

需要 高階技能	耗時 的分析	太多 分析工具	容易出錯 需要人力校正

新聞

報導：鴻海墨西哥廠在11月底遭勒索軟體攻擊

Bleeping Computer宣稱得到資安產業以及對鴻海墨國工廠發動攻擊者的說詞，來證實這起攻擊事件

文/ 陳曉莉 | 2020-12-08 發表

圖片來源: Nadkachna, CC BY 3.0 , via Wikimedia Commons

資安新聞網站Bleeping Computer本周報導，全球最大的電子製造業者鴻海（Foxconn）位於墨西哥華雷斯城（Ciudad Juárez）的Foxconn CTBG工廠，在今年11月29日遭到DoppelPaymer勒索軟體攻擊，駭客在加密系統檔案之前先下載了檔案，並在12月7日於其資料外洩網站公布了部份的資料。此外，DoppelPaymer也是先前外傳攻擊仁寶的兇手。

Foxconn CTBG是在2005年就建立了，佔地68.2萬平方呎，剛好座落在美墨邊境，靠近美國德州與新墨西哥州，專門組裝電子設備以供應美洲市場。不過，現在Foxconn CTBG的官網已呈現HTTP 404的錯誤狀態。

Bleeping Computer報導，該報一直在追蹤鴻海被駭的傳言，一直到本周看到駭客釋出了部份無關緊要的鴻海商業文件，此外，來自資安產業的消息來源亦與該報分享了駭客於鴻海伺服器上留下的勒索信件，要求鴻海支付贖金以換得解密金鑰及所下載的備份資料，所提出的價碼為1804.0955個比特幣，價值超過3,400萬美元。

此外，Bleeping Computer甚至直接與駭客取得了聯繫，駭客宣稱該攻擊竊取了

專題報導

千億營收電商的SRE之旅

摩根大通2022科技新戰略

紅帽邊緣運算新戰略

疑似攻擊程式樣本曝光，官方也終

以否認，並認為疑似是駭客入侵

是有可能因駭客攻

讚加入iThome粉絲團 讚 298 分享

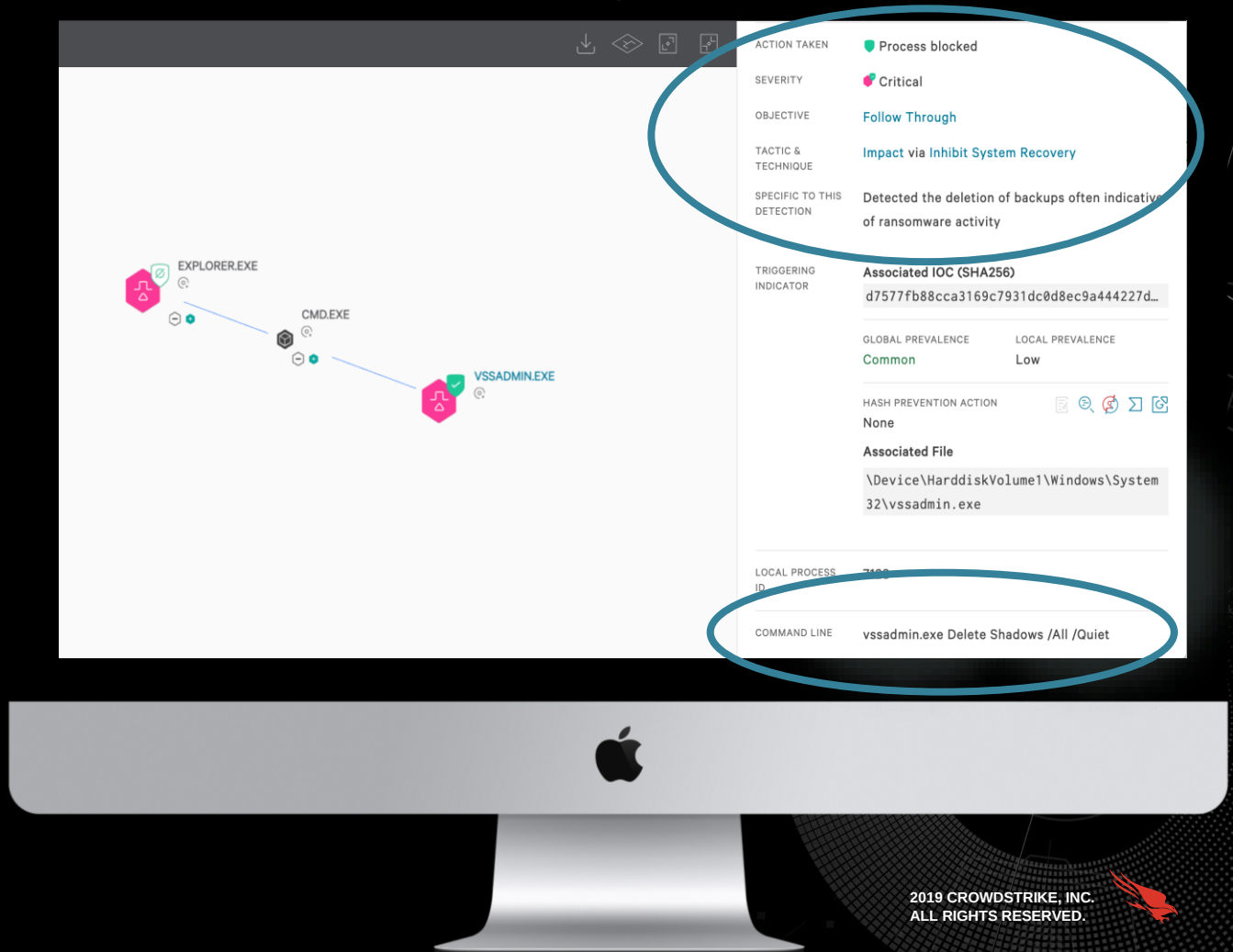
尚未有加油站系統無法使用狀態發生。

單一 AGENT 的解決方案

CROWDSTRIKE

NGAV

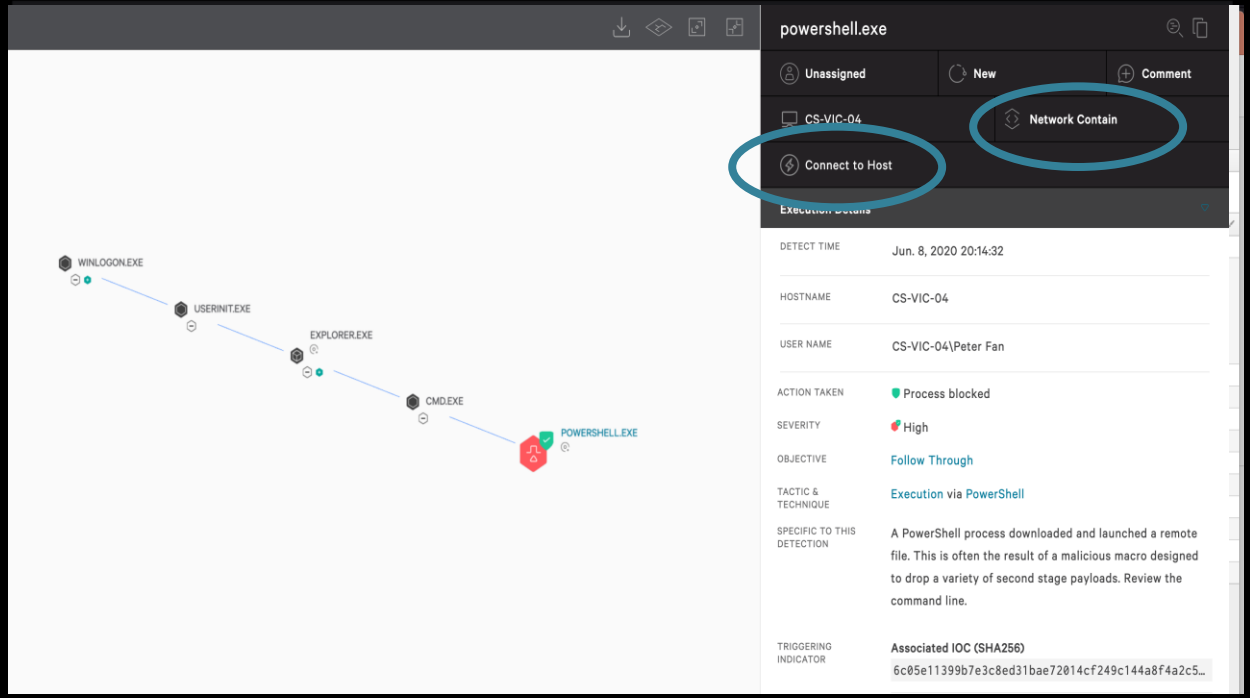
- 阻擋所有型態的攻擊
- 防範已知/未知惡意軟體
- 防範 ZERO-DAY 攻擊
- 排除勒索軟體
- 不須病毒碼更新
- 使用者幾乎無感—低於1%的CPU使用率
- 安裝無須重開機
- 離線保護能力相同



CROWDSTRIKE

EDR

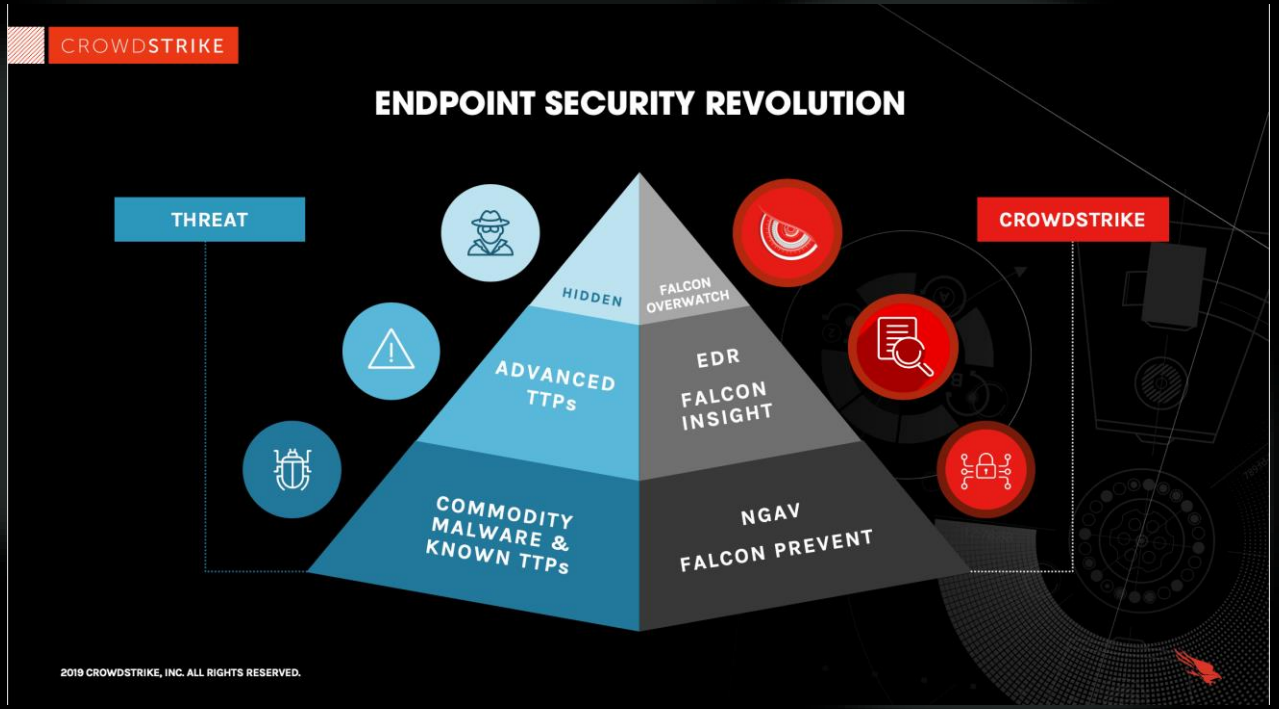
- 端點的錄影機:
  行為全都錄
- 即時與歷史搜尋
- 反應與隔離
- 威脅獵補



CROWDSTRIKE

OVERWATCH

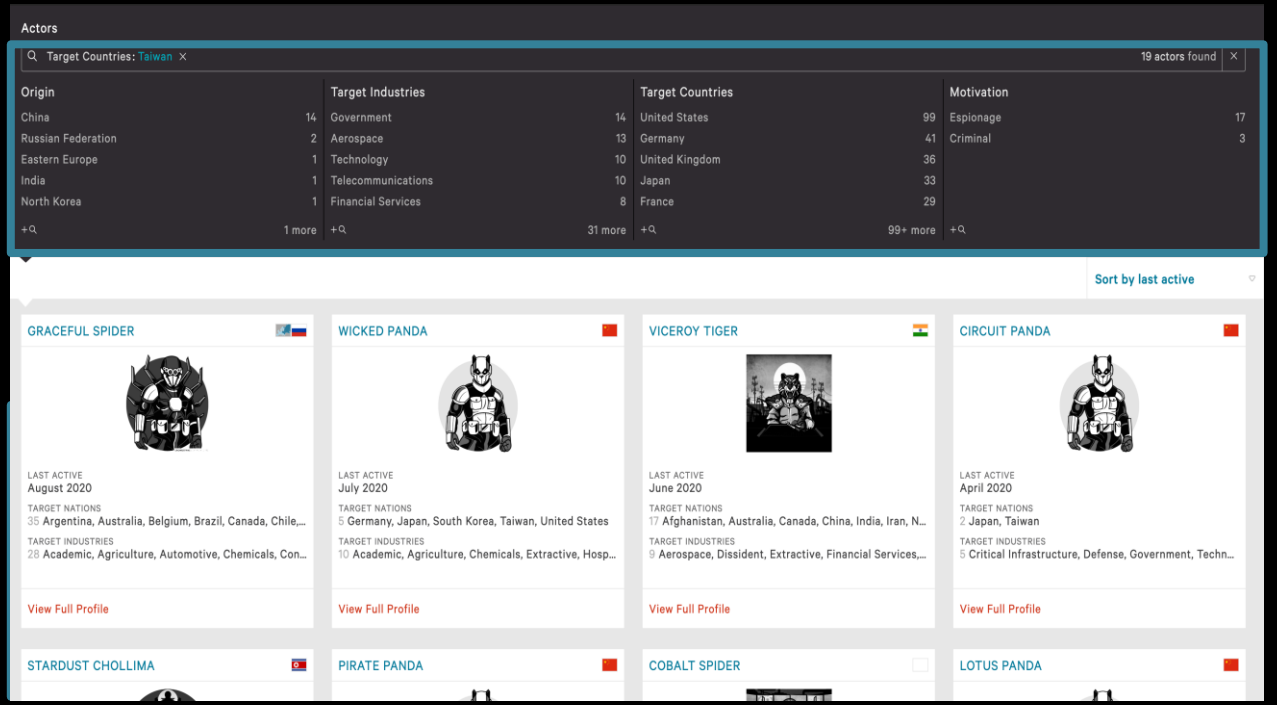
- 提供 7x24x365 入侵示警服務
- 人類專家
- 深入威脅分析
- 專業人士提供指導



CROWDSTRIKE

INTELLIGENCE & SANDBOX

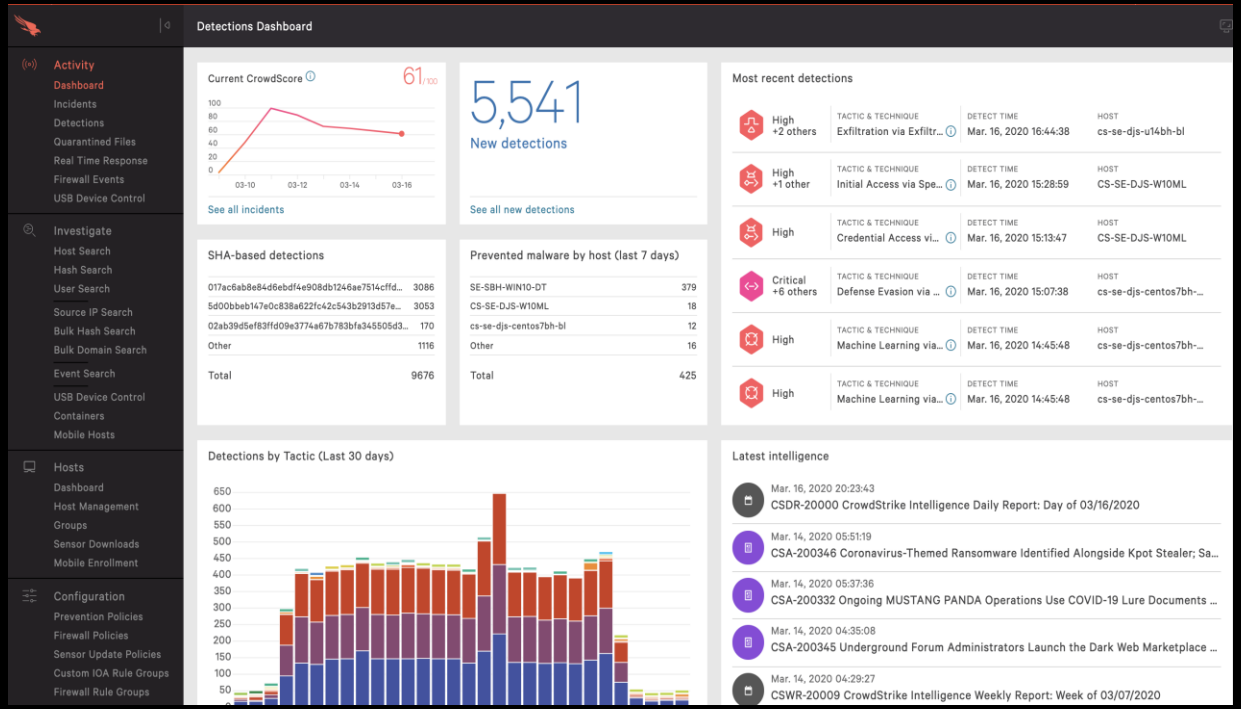
- 駭客、惡意資訊
- IOC指標
- 威脅報告
- 惡意軟體沙箱
- 惡意軟體樣本
- 客製化情報



CROWDSTRIKE

FALCON PLATFORM

- 超輕量 AGENT
- 單一 AGENT / 管理界面
- WINDOWS , LINUX, MAC, IOS, ANDROID
- 線上擴充商店
- 提供 API 整合



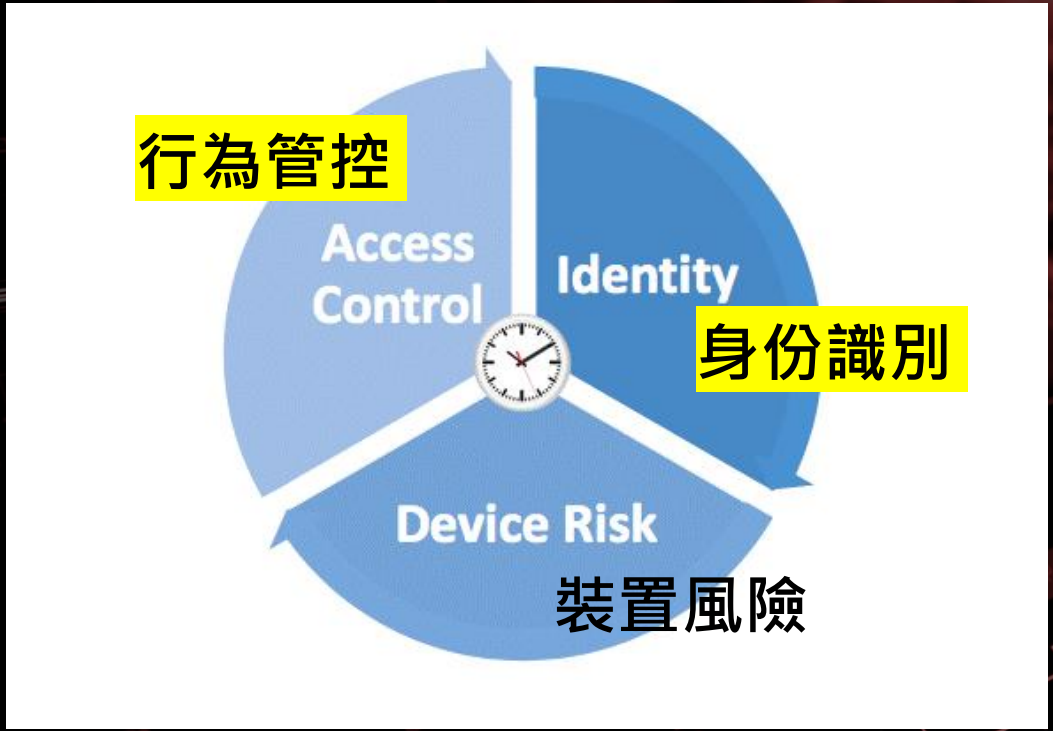
威脅情資，了解您的對手

每一次的攻擊，背後都是一個人類對手

FALCON 威脅情資揭露了他們的動機與技巧，讓您先一步領先敵手

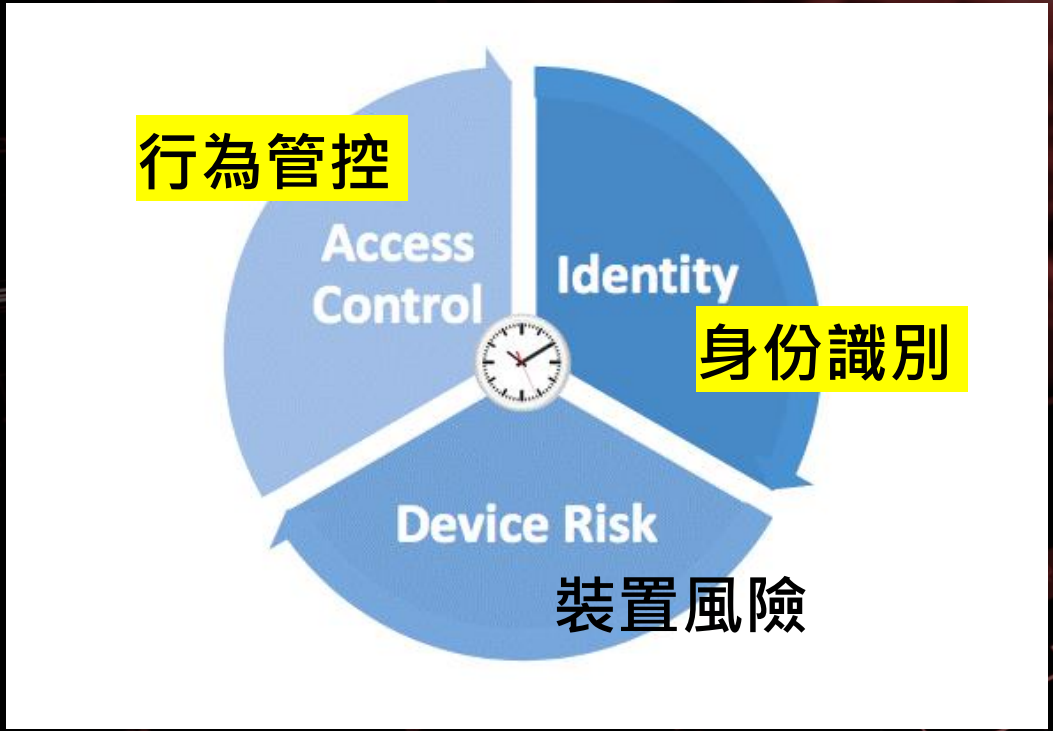
CROWDSTRIKE

建立零信任策略的三個面向



CROWDSTRIKE

建立零信任策略的三個面向



零信任 = 資安數位轉型？

Identities 身份識別	Endpoints 端點安全	Network 網路保護	Analytics 行為分析	Automation 自動化	Applications 關鍵應用

CROWDSTRIKE

身份保護刻不容緩

趕快關注這 80% 的問題

80%

IDENTITIES

80% of data breaches have a connection to compromised privileged credentials

80% 的資料洩漏事件與憑證有關

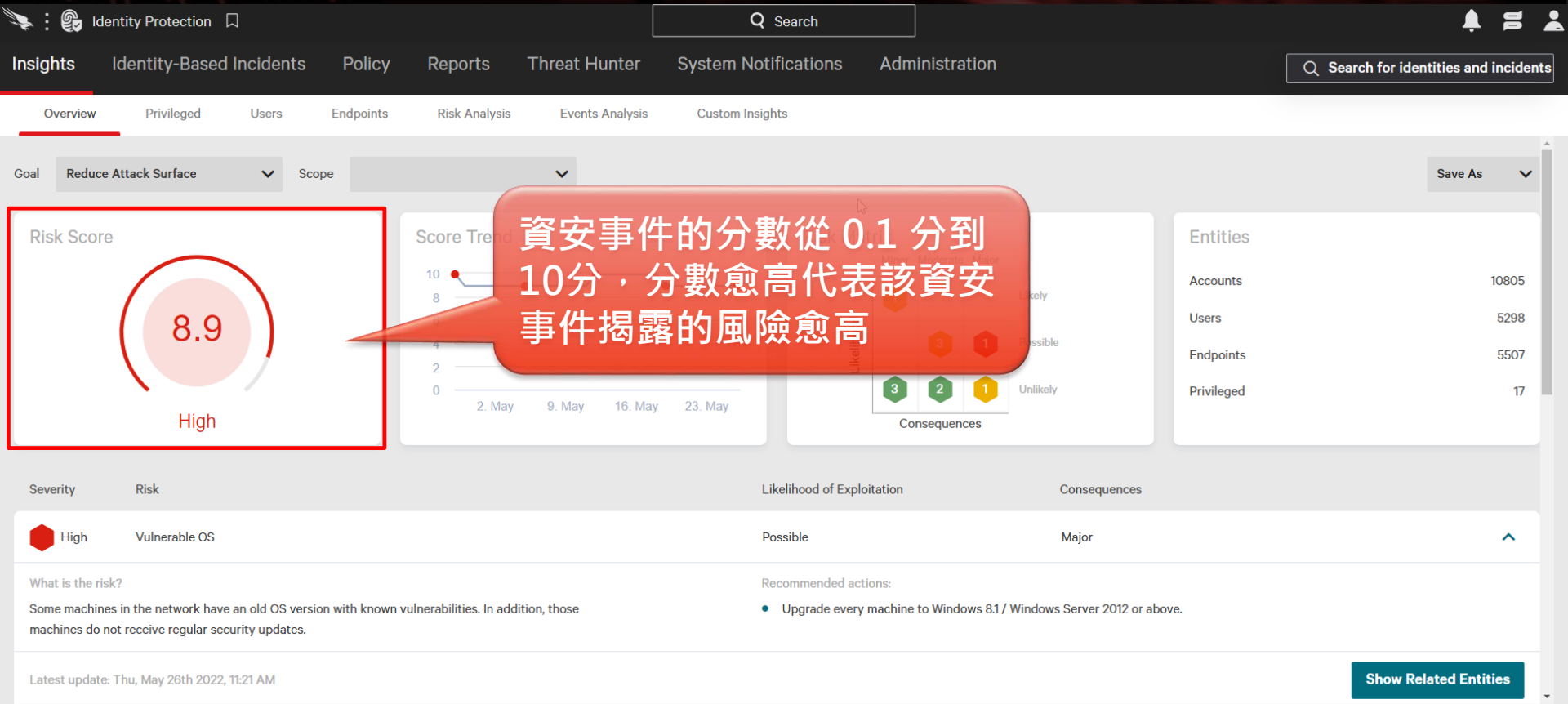
- FORRESTER RESEARCH

80% of breaches within hacking involve brute force or the use of lost or stolen credentials.

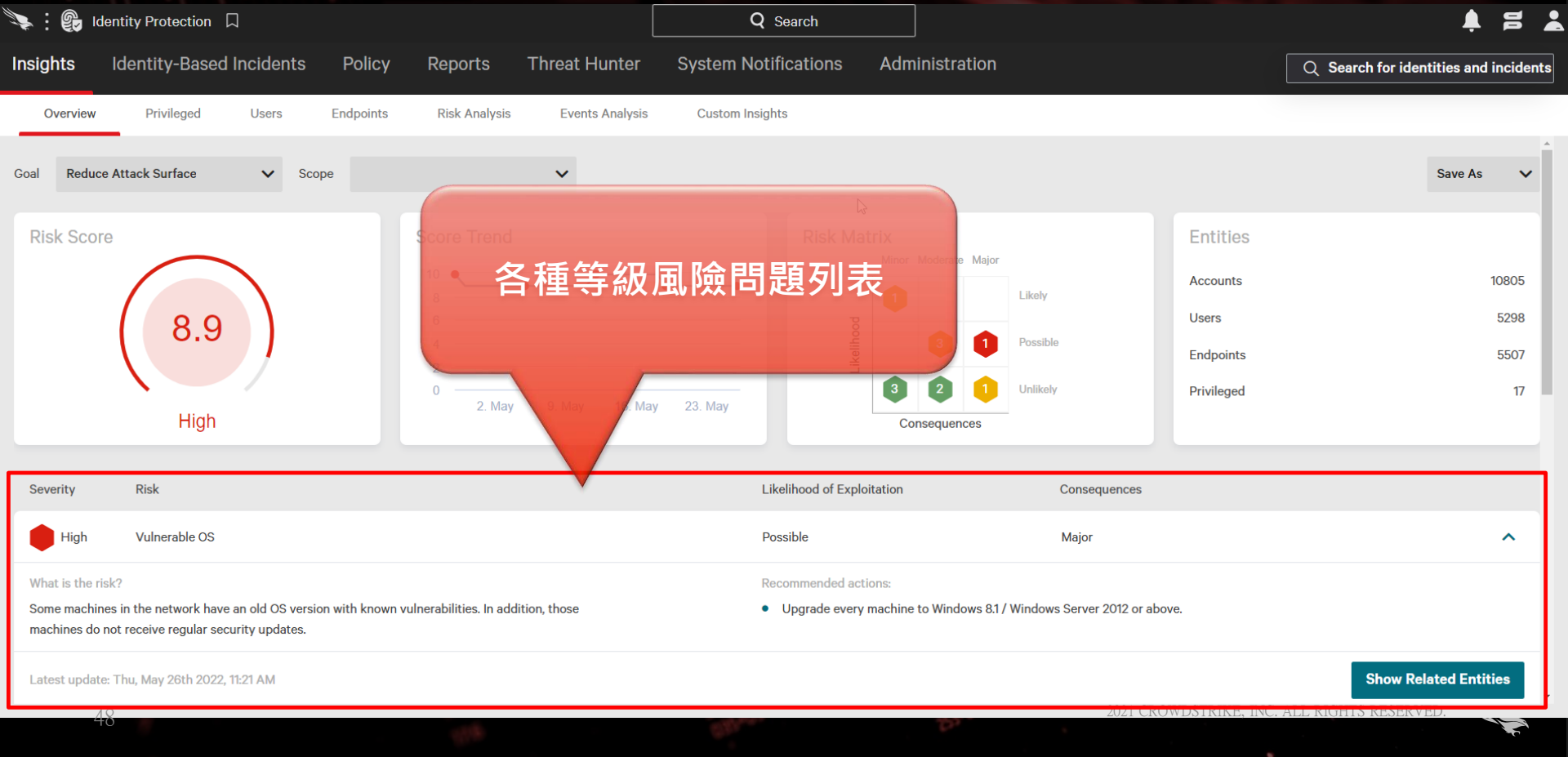
80%的駭客攻擊涉及暴力破解或外瀉的密碼

- VERIZON DBIR 2020

Endpoints
Network
Analytics
Automation
Applications



資安事件的分數從 0.1 分到 10分，分數愈高代表該資安事件揭露的風險愈高



各種等級風險問題列表

Severity	Risk	Likelihood of Exploitation	Consequences
High	Vulnerable OS	Possible	Major
Medium	Compromised Password	Likely	Minor
Medium	SMB Signing Disabled	Possible	Moderate
Medium	LDAPS Channel Binding is not Required	Possible	Moderate
Medium	LDAP Signing is not Required	Possible	Moderate
Medium	NTLMv2 Compatibility	Unlikely	Major
Low	Stealthy Privileges	Unlikely	Moderate
Low	Attack Path to a Privileged Account	Unlikely	Moderate

Severity	Risk	Likelihood of Exploitation	Consequences
High	Vulnerable OS	Possible	Major

What is the risk?

Some machines in the network have an old OS version with known vulnerabilities. In addition, those machines do not receive regular security updates.

Recommended actions:

- Upgrade every machine to Windows 8.1 / Windows Server 2012 or above.

Latest update: Thu, May 26th 2022, 4:21 PM

Show Related Entities

Severity	Risk	Likelihood of Exploitation	Consequences
Medium	Compromised Password	Likely	Minor

What is the risk?

Some accounts have passwords that are known to be compromised. Compromised passwords are usually collected from known password breaches or contain commonly used phrases, and are easy to guess.

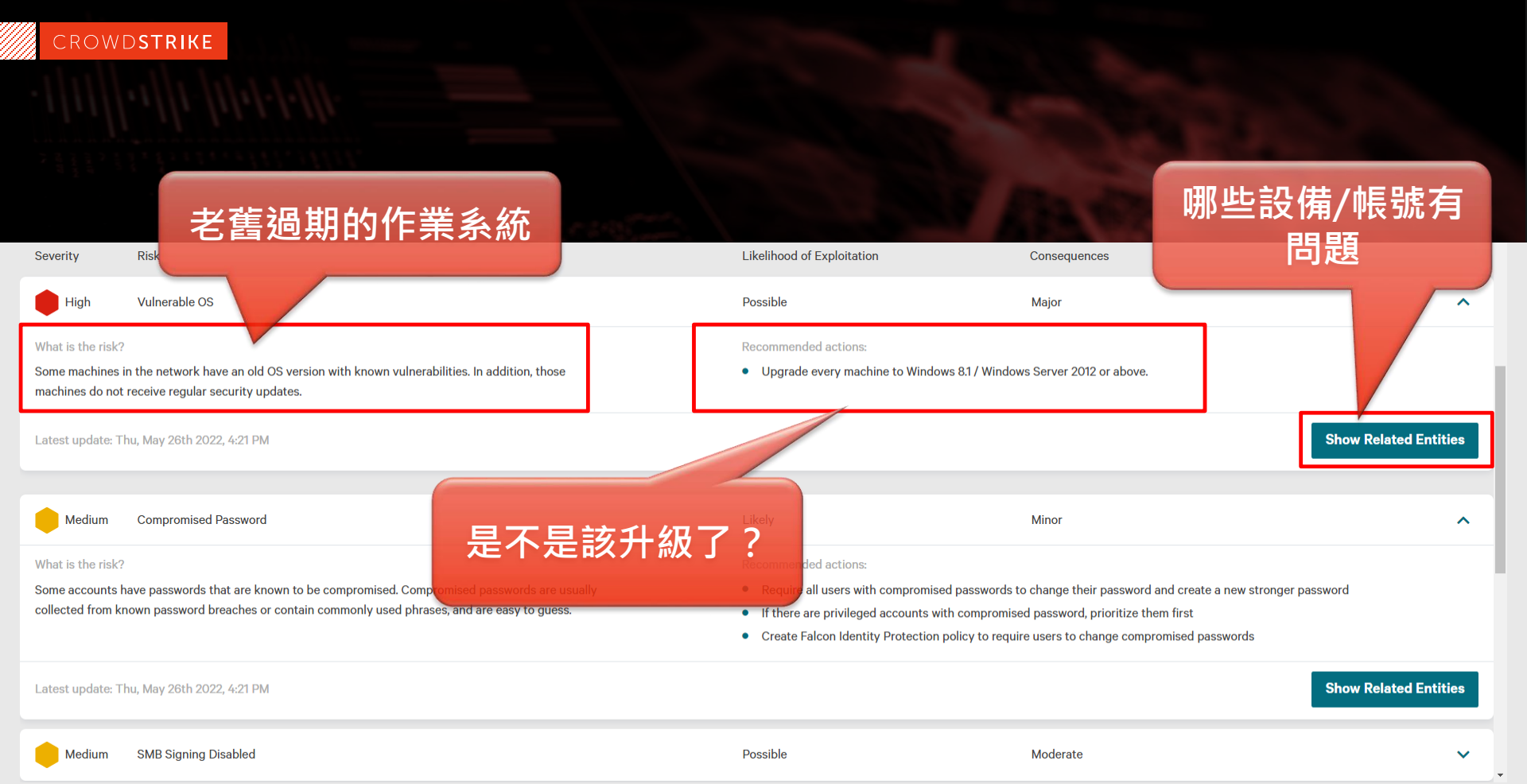
Recommended actions:

- Require all users with compromised passwords to change their password and create a new stronger password
- If there are privileged accounts with compromised password, prioritize them first
- Create Falcon Identity Protection policy to require users to change compromised passwords

Latest update: Thu, May 26th 2022, 4:21 PM

Show Related Entities

Severity	Risk	Likelihood of Exploitation	Consequences
Medium	SMB Signing Disabled	Possible	Moderate



Severity	Risk	Likelihood of Exploitation	Consequences
High	Vulnerable OS	Possible	Major

What is the risk?

Some machines in the network have an old OS version with known vulnerabilities. In addition, those machines do not receive regular security updates.

Recommended actions:

- Upgrade every machine to Windows 8.1 / Windows Server 2012 or above.

Latest update: Thu, May 26th 2022, 4:21 PM

Show Related Entities

Medium	Compromised Password	Likely	Minor

What is the risk?

Some accounts have passwords that are known to be compromised. Compromised passwords are usually collected from known password breaches or contain commonly used phrases, and are easy to guess.

Recommended actions:

- Require all users with compromised passwords to change their password and create a new stronger password
- If there are privileged accounts with compromised password, prioritize them first
- Create Falcon Identity Protection policy to require users to change compromised passwords

Latest update: Thu, May 26th 2022, 4:21 PM

Show Related Entities

Medium	SMB Signing Disabled	Possible	Moderate

Severity	Risk
High	Vulnerable OS

What is the risk?

Some machines in the network have an old OS version with known vulnerabilities. Those machines do not receive regular security updates.

Latest update: Thu, May 26th 2022, 4:21 PM

Severity	Risk
Medium	Compromised Password

What is the risk?

Some accounts have passwords that are known to be compromised. Compromised passwords are usually collected from known password breaches or contain commonly used phrases, and are easy to guess.

Latest update: Thu, May 26th 2022, 4:21 PM

Medium	SMB Signing Disabled	Possible	Moderate

有問題的
設備/帳號

Related Entities

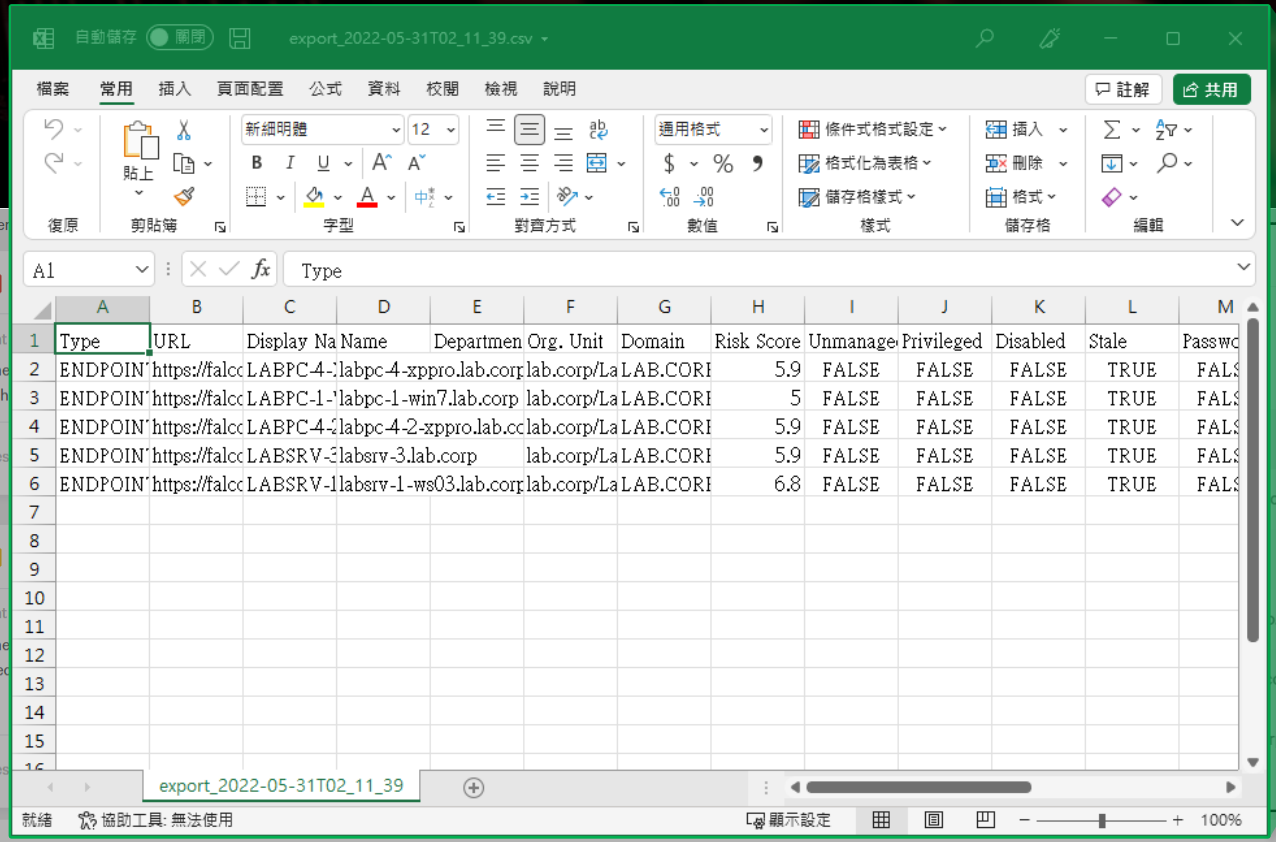
Vulnerable OS

CSV | Save As Custom Insights

Type	Primary	Secondary	Attributes	Score
	LABSRV-1-WS03	labsrv-1-ws03.lab.corp		6.8
	LABSRV-3	labsrv-3.lab.corp		5.9
	LABPC-4-2-XPPRO	labpc-4-2-xppro.lab.corp		5.9
	LABPC-4-XPPRO	labpc-4-xppro.lab.corp		5.9
	LABPC-1-WIN7	labpc-1-win7.lab.corp		5

CROWDSTRIKE

趕緊輸出報表



export_2022-05-31T02_11_39.csv

	A	B	C	D	E	F	G	H	I	J	K	L	M
1	Type	URL	Display Na	Name	Departmen	Org. Unit	Domain	Risk Score	Unmanage	Privileged	Disabled	Stale	Passwo
2	ENDPOIN	https://falcc	LABPC-4-2	labpc-4-xppro.lab.corp		lab.corp/La	LAB.CORI	5.9	FALSE	FALSE	FALSE	TRUE	FALS
3	ENDPOIN	https://falcc	LABPC-1-'	labpc-1-win7.lab.corp		lab.corp/La	LAB.CORI	5	FALSE	FALSE	FALSE	TRUE	FALS
4	ENDPOIN	https://falcc	LABPC-4-2	labpc-4-2-xppro.lab.cc		lab.corp/La	LAB.CORI	5.9	FALSE	FALSE	FALSE	TRUE	FALS
5	ENDPOIN	https://falcc	LABSRV-3	labsrv-3.lab.corp		lab.corp/La	LAB.CORI	5.9	FALSE	FALSE	FALSE	TRUE	FALS
6	ENDPOIN	https://falcc	LABSRV-1	labsrv-1-ws03.lab.corp		lab.corp/La	LAB.CORI	6.8	FALSE	FALSE	FALSE	TRUE	FALS

老舊作業系統實體隔離一樣是弱點

2018-03-19 10:03

司法院遭駭！隔離外網還是被入侵　謝昀澤：未更新系統是漏洞

▲日前司法院電腦遭駭客入侵，也讓外界擔心其卷宗是否會外流。（圖／視覺中國CFP）

記者林昱均／台北報導

日前司法院遭爆料其29間地方法院約243台電腦在3月7日遭到駭客攻擊，遭到攻擊的電腦皆為作業系統為Windows XP及Windows 2003之電腦，但司法院強調已封鎖殺除病毒，對民眾並無影響。KPMG安侯建業數位科技安全負責人謝昀澤表示，部分政府機關、醫療機構及其他關鍵基礎設施業者，在預算不足的情況下，**經常出現以「實體隔離」作為防護手段並延遲更新過時作業系統**，這些具連網能力又未更新的電腦或系統，**正是駭客搜尋的弱點入口**。

司法院表示，3月7日晚上約8點時，發現有駭客攻擊台北地方法院公文主機，當晚並即關機，並使用防火牆等資安作業阻斷連線。不料，隔日上午司法院也發現台南地方法院電腦教室Win XP作業系統的電腦，在去年底便遭駭客從巴基斯坦IP入侵成功，並被植入「零時差電腦病毒，導致司法院及所屬各機關之單一登入系統的帳號密碼，遭駭客入侵竊取，目前司法院已全面在主機布建APT防衛系統。

對此謝昀澤指出，近年來國內、外常常會用「實體隔離」作為主要防護手段的關鍵基礎設施產業遭到駭客入侵的事件，也就是讓電腦僅限於內網，不連接到外部網路。他認為，雖然「實體隔離」仍然是相當有效的資安防護措施，但是因為資訊技術的改變，現在幾乎所有的設備都具備連網能力，所以大幅提高了「實體隔離」的管控困難度，另部分組織常以「實體隔離」為由，將必須進行的資訊系統、作業系統更新的延遲合理化，帶來更大的資安隱憂。

不僅如此，謝昀澤也表示，根據KPMG 2017全球網際犯罪調查報告資訊顯示，有高達80%的受訪對象雖然已投資新興科技如雲端科技、行動技術、社群媒體等，但報告中也顯示，**高達81%受訪對象針對新科技的資安只投入不到10%**，因為一般組織常將資安預算視為無法創造價值的花費，編列年度預算時，而資安運算常被優先檢討減列或緩列的項目。謝昀澤認為，這種只看新科技應用價值，而忽略導入伴隨資安風險的情況，將讓組織處於越來越高的資安風險中。

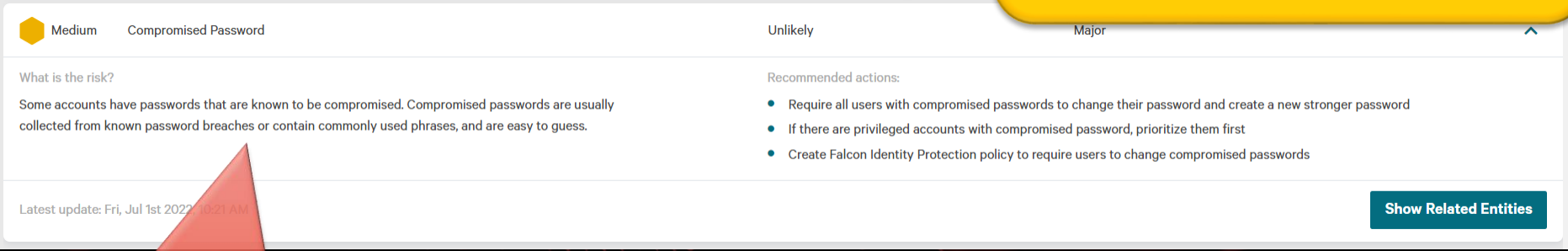
原文網址：https://finance.ettoday.net/news/1133196

CROWDSTRIKE

外洩的密碼

解決方案

- 要求所有密碼洩露的用戶更改密碼並創建一個新的更強的密碼
- 如果有密碼洩露的特權帳戶，請優先處理
- 創建 Falcon 身份保護 Policy 以要求用戶更改已洩露的密碼



密碼已洩露

某些帳戶的密碼已經被洩露。洩露的密碼通常是從已知的密碼洩露資料庫中收集，或包含常用字庫，並且很容易被猜到

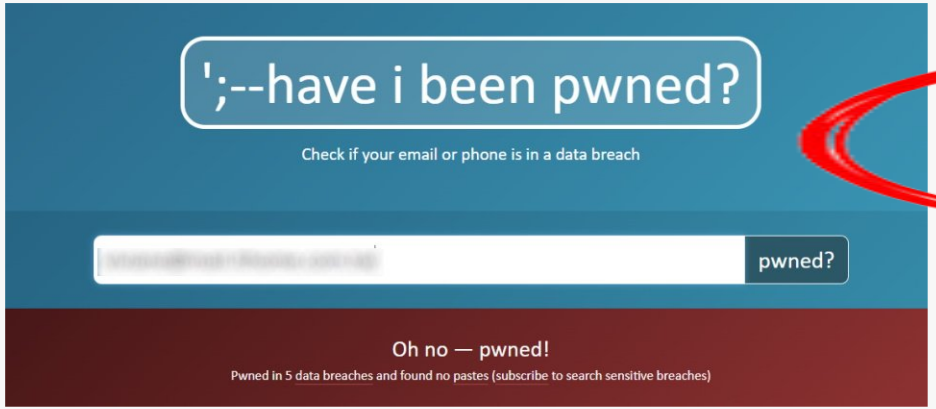
外洩密碼被用了56億次

新聞

繼美國之後，英國也加入提供外洩密碼予Have I Been Pwned的行列

英國國家犯罪調查局（NCA）近期提供Have I Been Pwned（HIBP）平臺逾5.8億筆的外洩密碼資料，當中近2.3億筆屬於新密碼，也讓HIBP的外洩密碼資料庫規模增加38%

文/ 陳曉莉 | 2021-12-21 發表



由澳洲安全專家Troy Hunt在2013年所建立的Have I Been Pwned（HIBP）外洩密碼查詢平臺，在今年5月開源之際，宣布美國聯邦調查局（FBI）將把所查獲的

由澳洲安全專家Troy Hunt在2013年所建立的Have I Been Pwned（HIBP）外洩密碼查詢平臺，在今年5月開源之際，宣布美國聯邦調查局（FBI）將把所查獲的外洩資料匯入HIBP專案，本周Hunt指出，英國的國家犯罪調查局（National Crime Agency，NCA）也已將大量的外洩密碼貢獻給HIBP。

HIBP原本就蒐集了6.13億筆的外洩密碼，此次NCA則提供了逾5.8億筆的外洩密碼，當中近2.3億筆屬於新密碼，也讓HIBP的外洩密碼資料庫規模超越8.4億筆，增加了38%。HIBP也計算出這8.4億筆的外洩密碼總計被使用了近56億次，顯示有不少使用者在不同的服務中採用同樣的密碼。

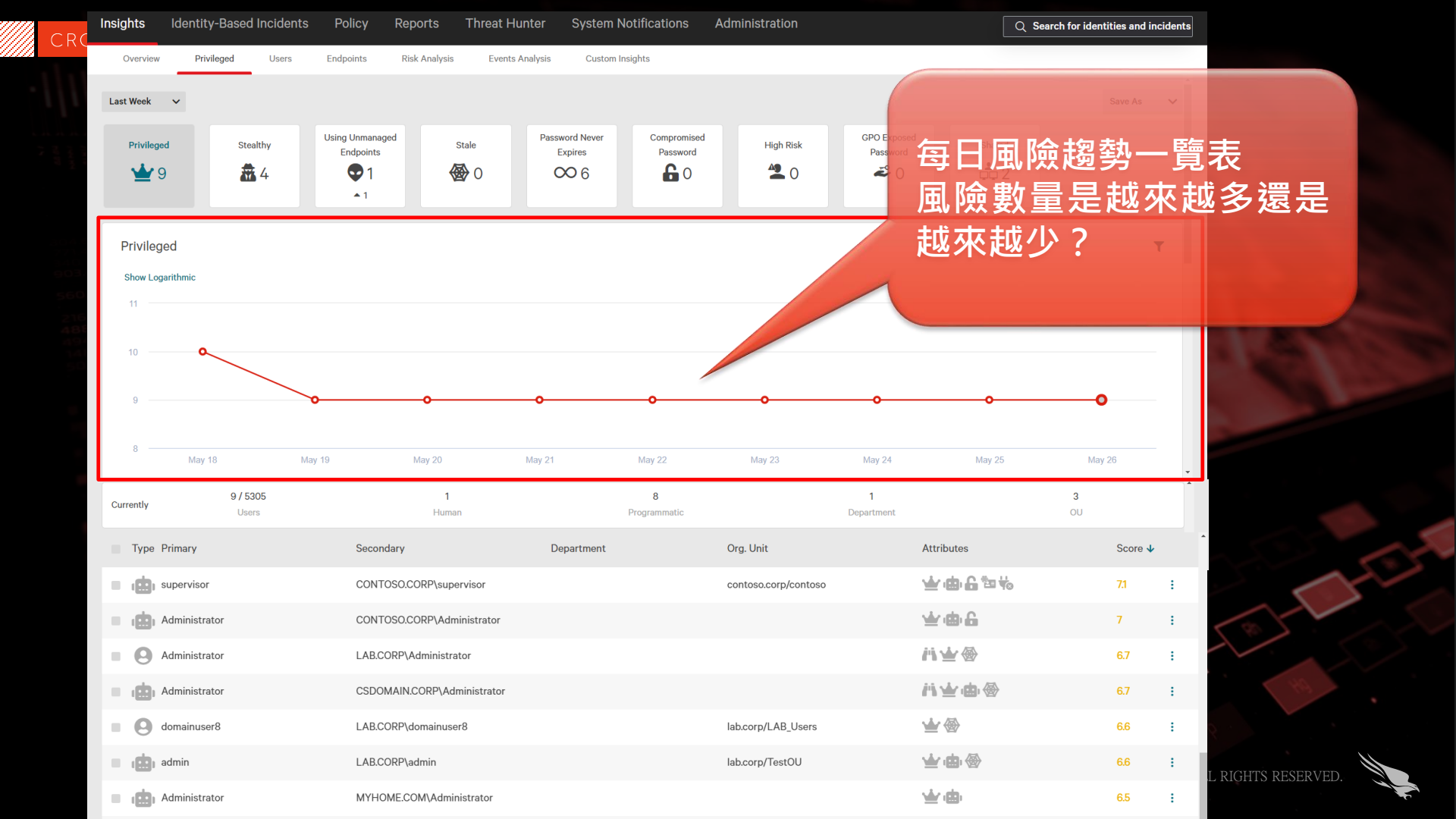
NCA表示，這些外洩資料都是該組織於過去幾年所取得，特別是與那些平臺被駭或用戶資料遭竊的企業合作，協助企業保護用戶的帳號安全。

NCA也透露，最近該組織還在一個曝露的雲端儲存服務中，看到大量的外洩憑證，包含電子郵件帳號與密碼，同時涉及多個已知或未知的資料外洩事件。

HIBP服務可讓使用者以電子郵件查詢自己所使用的服務與密碼是否曾外洩過，同時也能讓各業者了解自家服務的安全狀況。研究人員或業者可透過Pwned

原文網址：https://www.ithome.com.tw/news/148479

CROWDSTRIKE



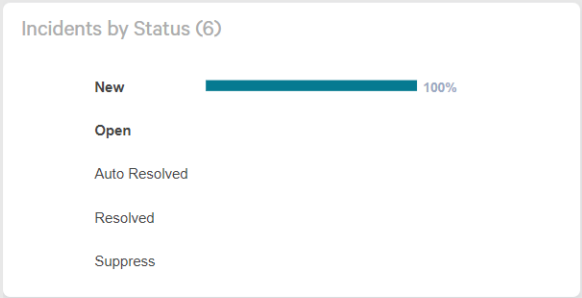
CROWDSTRIKE

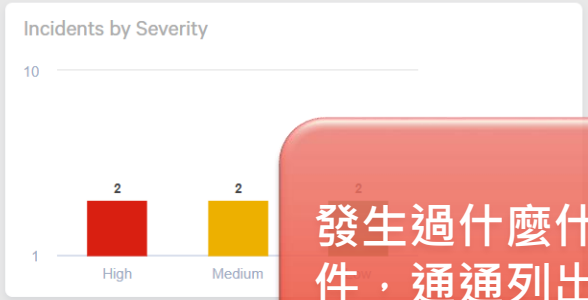
Insights | Identity-Based Incidents | Policy | Reports | Threat Hunter | System Notifications | Administration

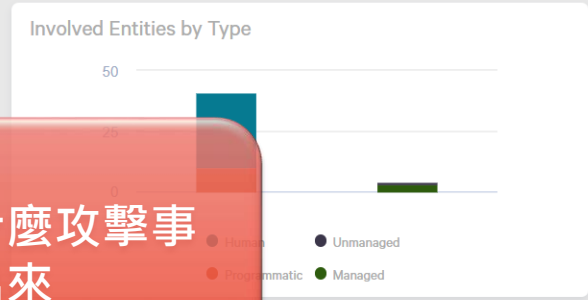
Search for identities and incidents

Identity-Based Incidents | Exceptions

Show Informational Incidents | All Time







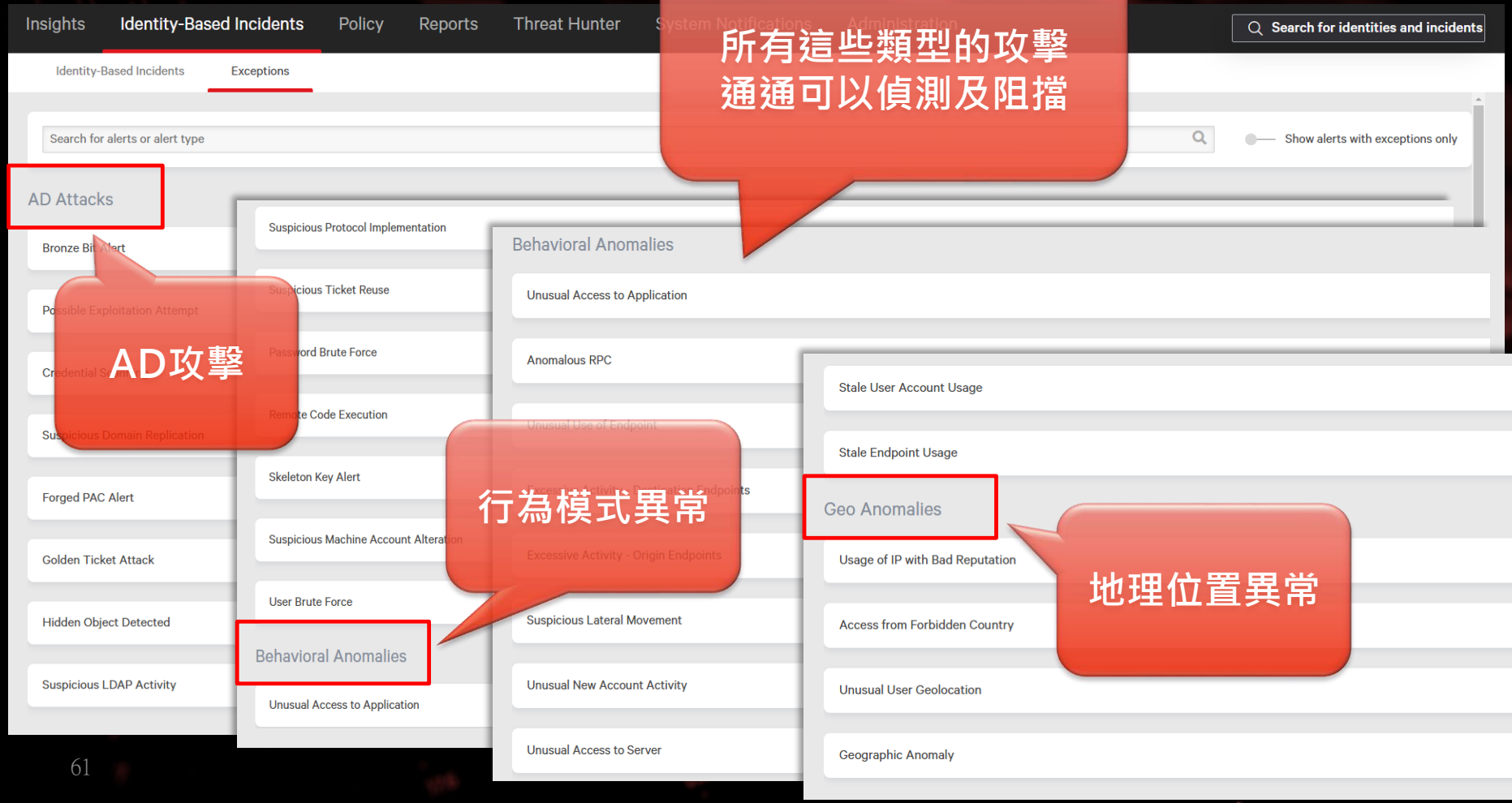
發生過什麼什麼攻擊事件，通通列出來

Add Filter

6 Incidents

Incident Type	Entities Involved	Last Update Time	Severity	ID	Status
Possible Compromised Endpoint	PC01 黎家霖	May 30th 2022 4:54 PM	High	INC-4311	New
Potential Risky Activity	張俊杰 192.168.1.47	May 19th 2022 6:14 PM	Low	INC-83	New
Suspicious Domain Activity	許孟霖 and 12 more	May 17th 2022 8:14 PM	Medium	INC-36	New
Suspicious Domain Activity	Administrator and 34 more	May 17th 2022 5:00 PM	Low	INC-29	New
	湯欣慧	May 6th 2022			

CROWDSTRIKE



解決方案

- 查看攻擊路徑並檢查可以刪除哪些路徑
- 確保特權帳戶僅登錄受保護的主機
- 刪除不需要的本地管理員權限

Medium Attack Path to a Privileged Account

What is the risk?

This non-privileged account has an attack path to a privileged account, which can be traversed to compromise the privileged account's credentials.

Recommended actions:

- Review the attack path and examine which connections can be removed.
- Ensure privileged accounts only log into protected endpoints.
- Remove unwanted local admin privileges.

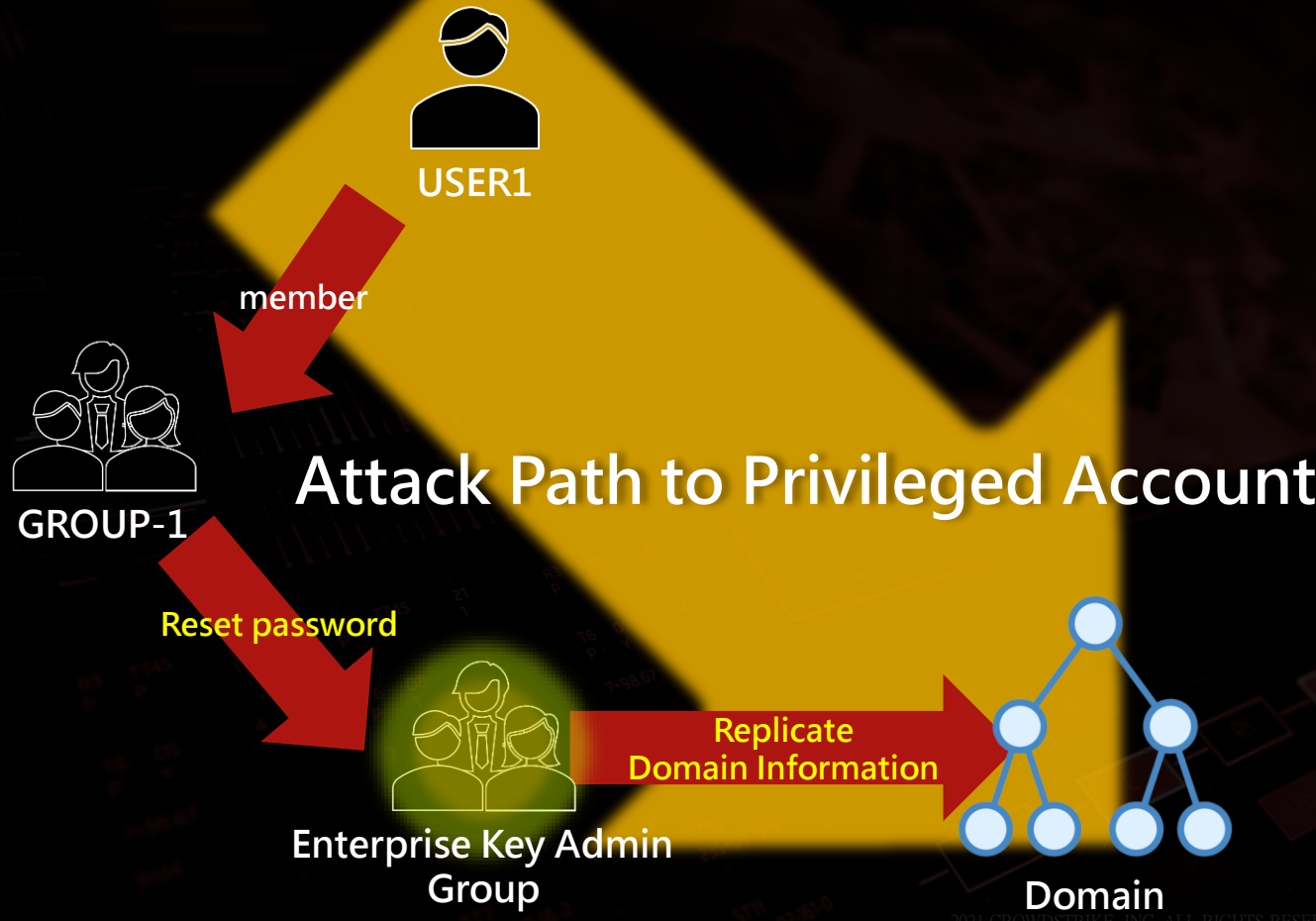
Additional Details:

MIS-TEST has one or more attack paths available to the privileged account Enterprise Key Admins. For example:

1. MIS-TEST is a (direct/indirect) member of GROUP-1
2. GROUP-1 permitted to reset Enterprise Key Admins's password.
3. Enterprise Key Admins permitted to replicate domain information, including hashes.

特權帳戶的攻擊路徑

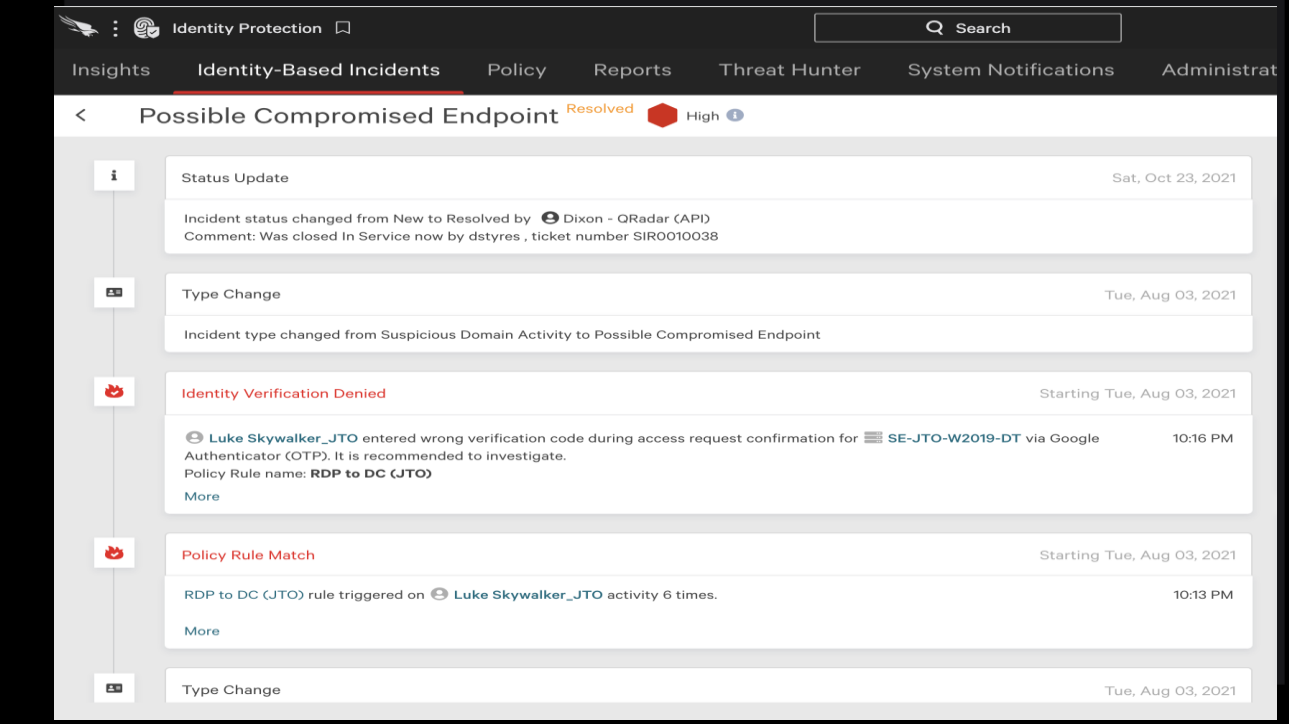
一些非特權帳戶具有特權帳戶的攻擊路徑，可以經由這些路徑以攻擊特權帳戶或網域



CROWDSTRIKE

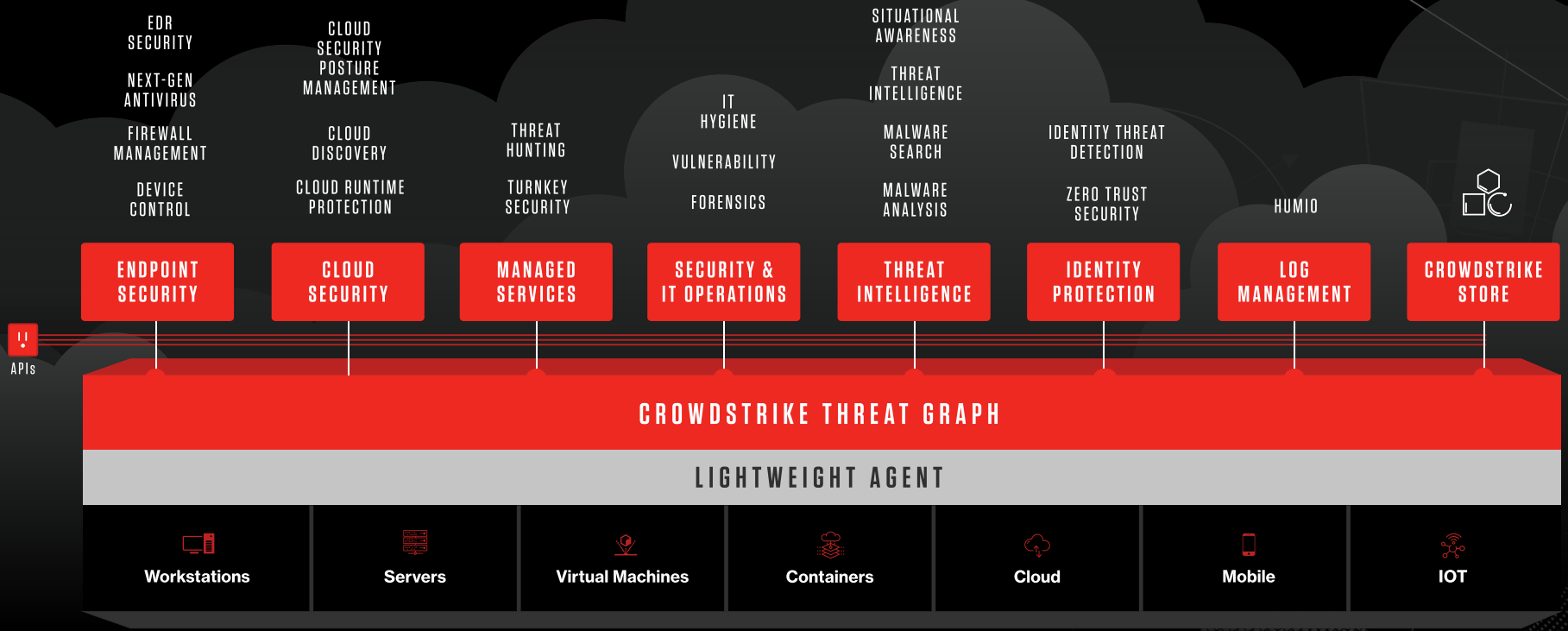
IDENTITY PROTECTION

- 在攻擊前發現威脅
- 擴大威脅防護覆蓋面
- 即時檢查 RDP 控制、GOLDEN TICKET，與各種攻擊手段
- 自動化的帳號行為監控



CROWDSTRIKE

CrowdStrike Falcon Platform



導入零信任的 7 個提問

要問廠商的 7 個問題

問題 1. 是否符合 NIST 800-207 標準？

問題 2. 如何保護免受……的威脅？

問題 3. 是否可以設定基於風險的策略？

問題 4. 可以即時處理哪些數據，需創建日誌文件？

問題 5. 只是零信任網路存取嗎？

要問廠商的 7 個問題

問題 6. 能否延伸以支持現有的設備與投資？

問題 7. 如何防範未受控管或是老舊的系統？

CROWDSTRIKE

WE STOP BREACHES

Stark Technology Inc.
敦陽科技股份有限公司