iSecurity The Hub of Security Innovations

數位資安系統

CROWDSTRIKE

自組CSIRT第一步
7X24企業專屬資安應變服務

陳建棠 Matt Chen

為何需要CSIRT?

溝通協調
協同工作
資安事件
應變處置

資安事件
層出不窮

攻擊面向
廣泛多變

攻擊手法

愈趨複雜

CSIRT的由來

Carnegie Mellon University

1988

Computer Emergency Response Team

CERT Coordination Center

Computer Security Incident Response Team

Forum of Incident Response and Security Teams, FIRST

Asia Pacific Computer Emergency Response Team, APCERT

TACERT
EC-CERT
TWCSIRT
NCC-CERT
TWNCERT
TWCERT/CC

CSIRT的定位

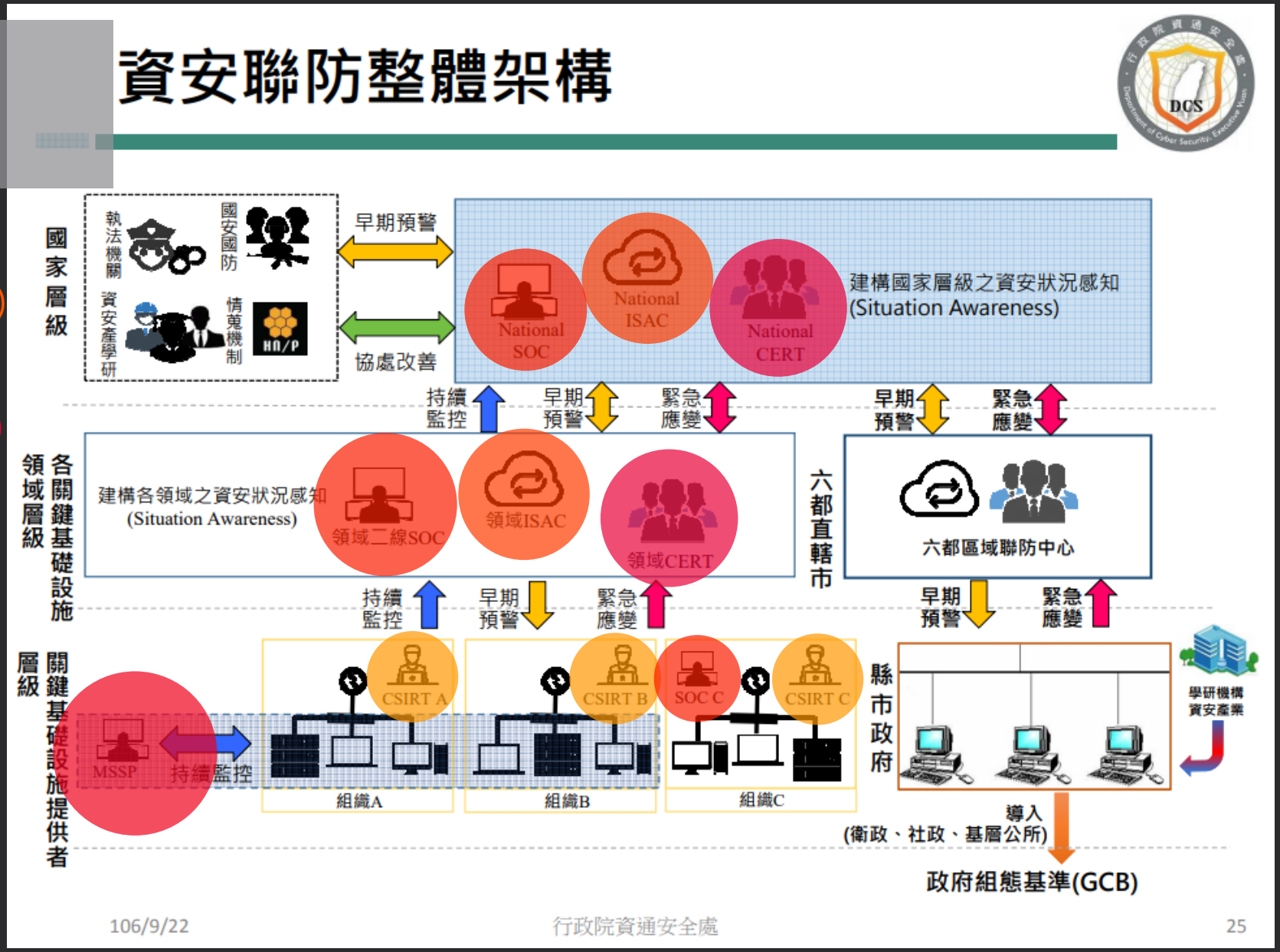
資訊分享與分析中心 (Information Sharing and Analysis Center, ISAC)

電腦緊急應變團隊 (Computer Emergency Response Team, CERT)

電腦安全事件應變小組 (Computer Security Incident Response Team, CSIRT)

資安作業中心 (Security Operation Center, SOC)

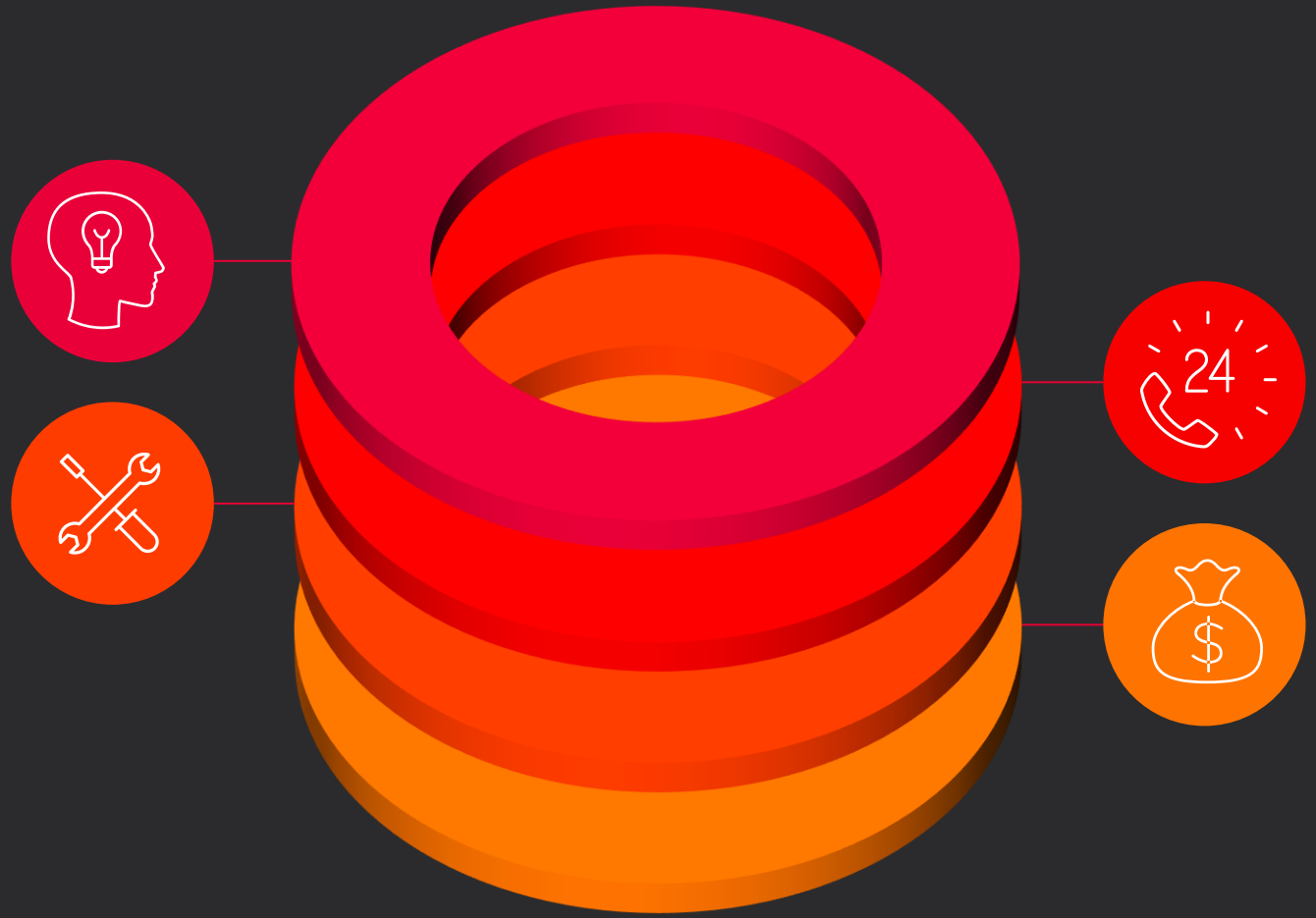
資安託管服務供應商 (Managed Security Service Provider, MSSP)



問題是...

團隊
專業資安人員
鑑識分析能力

工具
Monitoring
Detection
Prevention
Respond



維運
7x24 or 5x8
即時應變處理

成本
OPEX
CAPEX

iSecurity
The Hub of Security Innovations

踏出自組CSIRT第一步

7x24企業專屬資安應變服務

CROWDSTRIKE

FOUNDERS

GEORGE KURTZ

Co-founder & CEO

DMITRI ALPEROVITCH

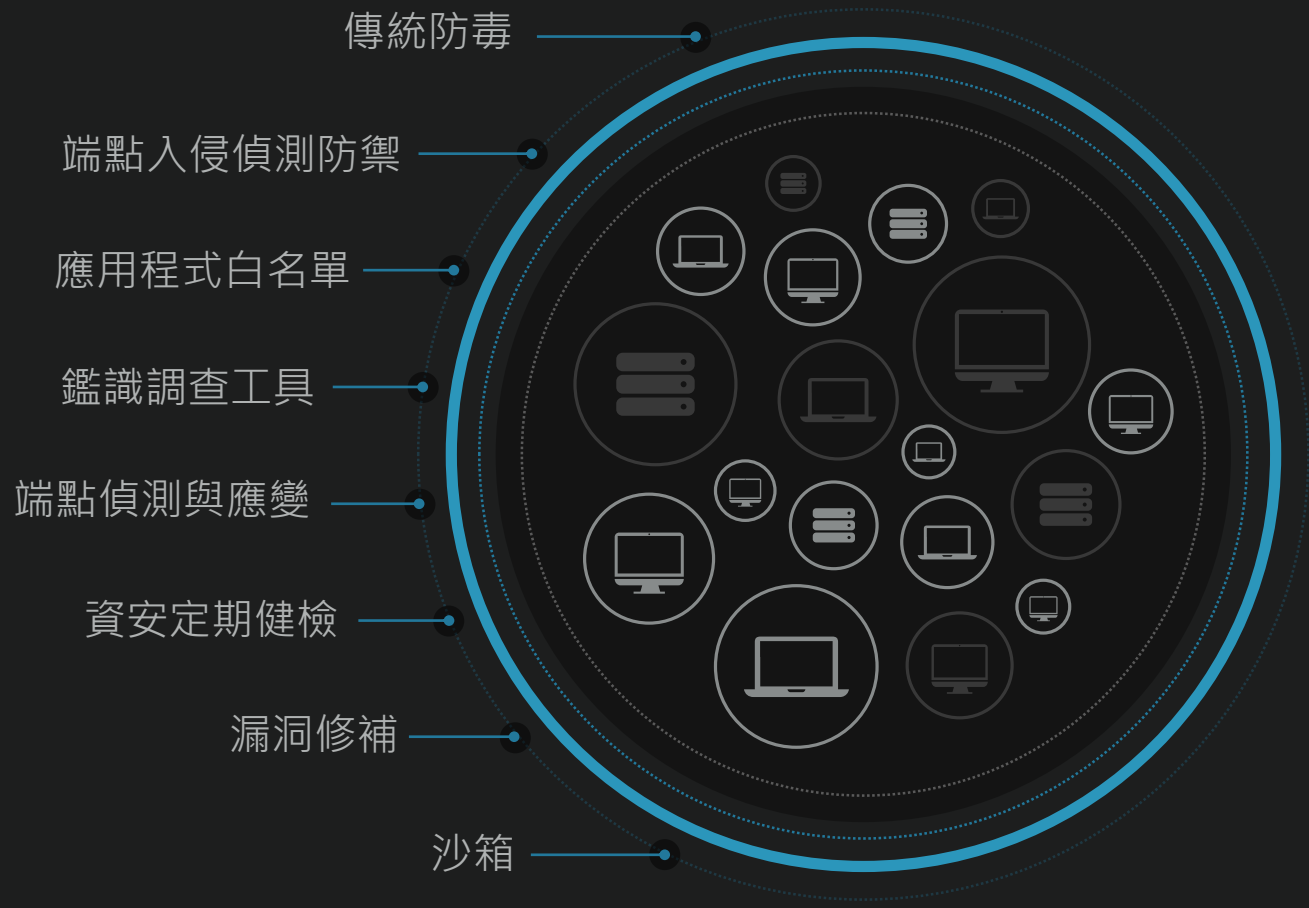
Co-founder & CTO

iSecurity
The Hub of Security Innovations

CROWDSTRIKE

問題：
越來越多的代理程式+永無止境的特徵碼

現有作法



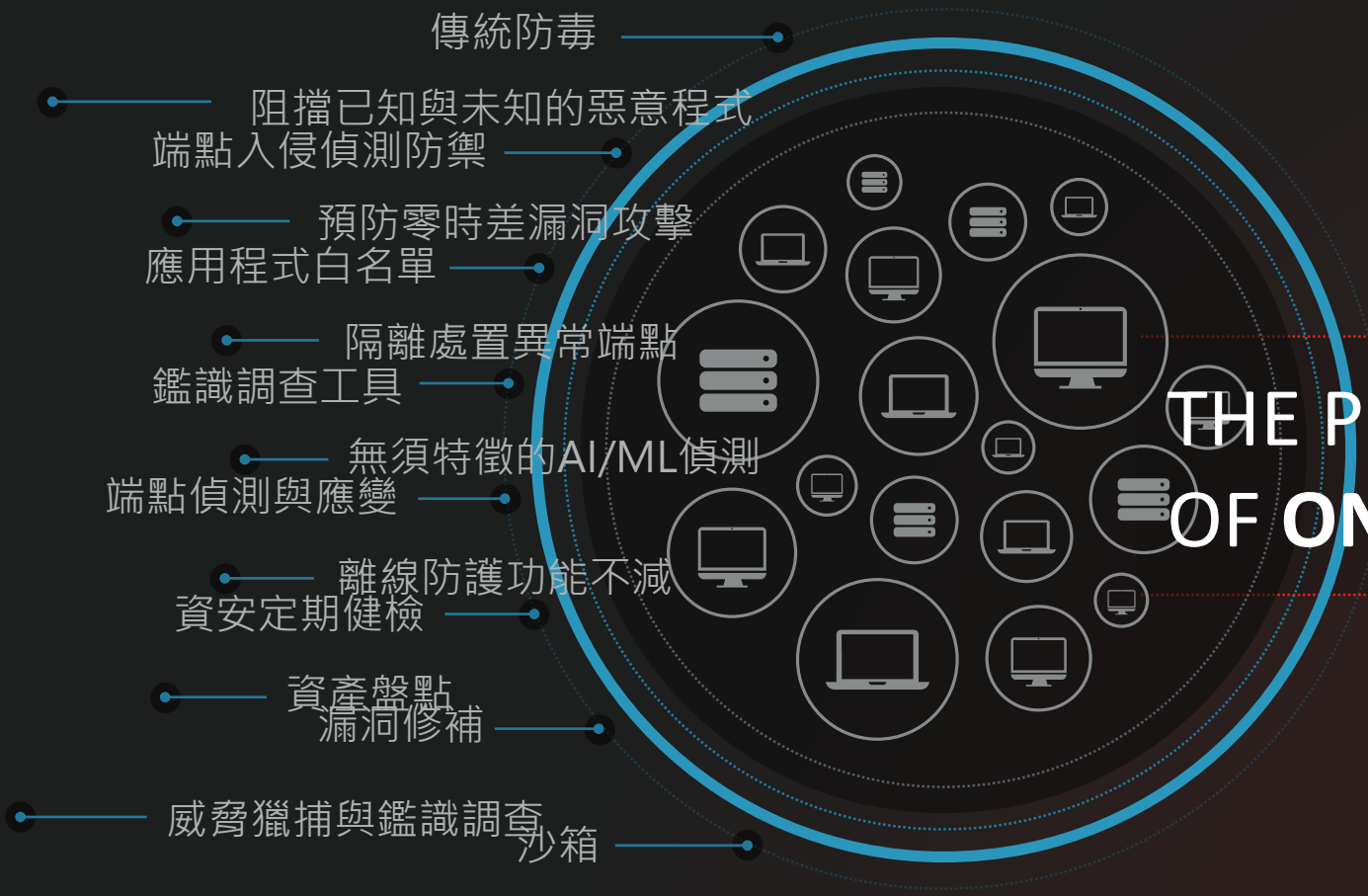
iSecurity
The Hub of Security Innovations

CROWDSTRIKE

解決方案：
CROWDSTRIKE FALCON

現有作法

單一
輕量化
代理程式



THE POWER OF **ONE**

iSecurity
The Hub of Security Innovations

為何現行做法都失敗了？

因為大家都只做一半

File Based Detection
AV Signatures
File Whitelisting
Machine Learning

Behavioral Detection
Exploit Blocking
Behavioral Analysis
Sandbox Appliance

Everything Else
IOC Detection
Forensics
SIEM Correlation

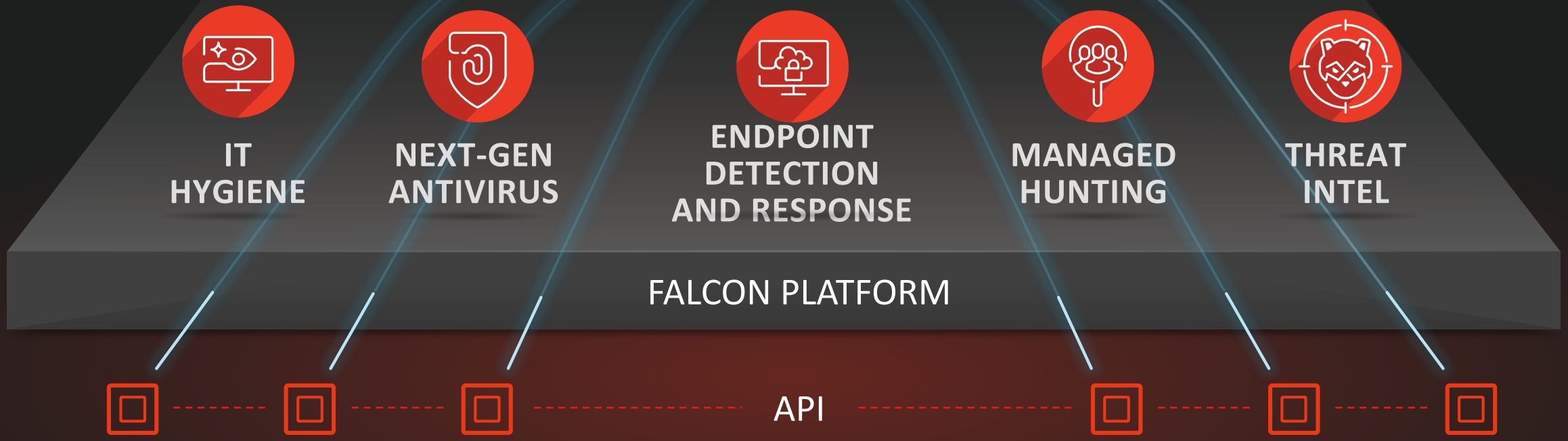
CrowdStrike Sees the Entire Kill Chain

KILL CHAIN	File Based Detection	Behavioral Detection	Everything Else	CrowdStrike Sees the Entire Kill Chain
1. RECONNAISSANCE				●
2. WEAPONIZATION	●			●
3. DELIVERY	●	●		●
4. EXPLOITATION	●	●		●
5. INSTALLATION	●	●	●	●
6. COMMAND & CONTROL			●	●
7. ACTIONS ON OBJECTIVES			●	●

CROWDSTRIKE

THE POWER OF ONE

AI POWERED PLATFORM



TECHNOLOGY PARTNER **ECOSYSTEM**

SECURITY ANALYTICS

splunk>
IBM QRadar
ArcSight An HP Company
LogRhythm
E8 SECURITY
exabeam

THREAT INTELLIGENCE PLATFORMS

THREATCONNECT
Infoblox
ANOMALI
THREATQUOTIENT

INFRASTRUCTURE

amazon web services
proofpoint
paloalto NETWORKS
BLUE COAT
ForeScout
Google Cloud Platform
zscaler
BLUVECTOR
CYPHORT
CENTRIPETAL NETWORKS

ORCHESTRATION & AUTOMATION

servicenow
DEMISTO
Phantom
swimlane
HEXADITE
SYNCURITY

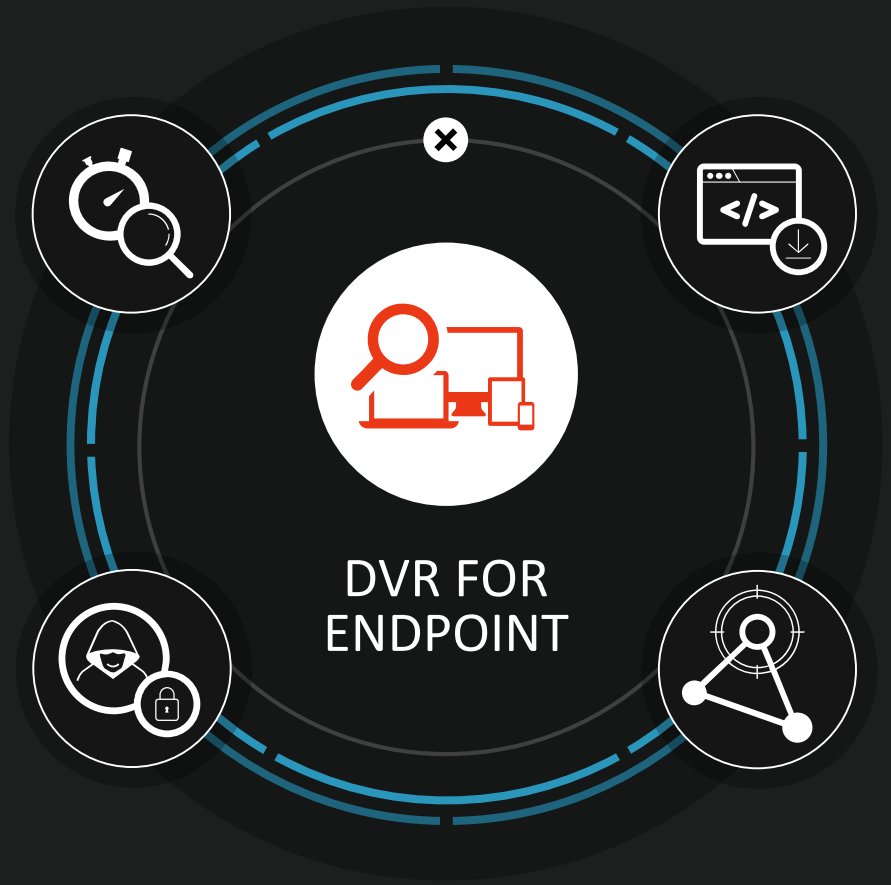
CROWDSTRIKE

SECURITY OPERATIONS

CROWDSTRIKE

ENDPOINT DETECTION AND RESPONSE – **FALCON INSIGHT**

快速查詢
即時資料
與
歷史紀錄



應變處理
與
隔離處置

BUSINESS VALUE

紀錄端點
的
一舉一動

快速查找資訊

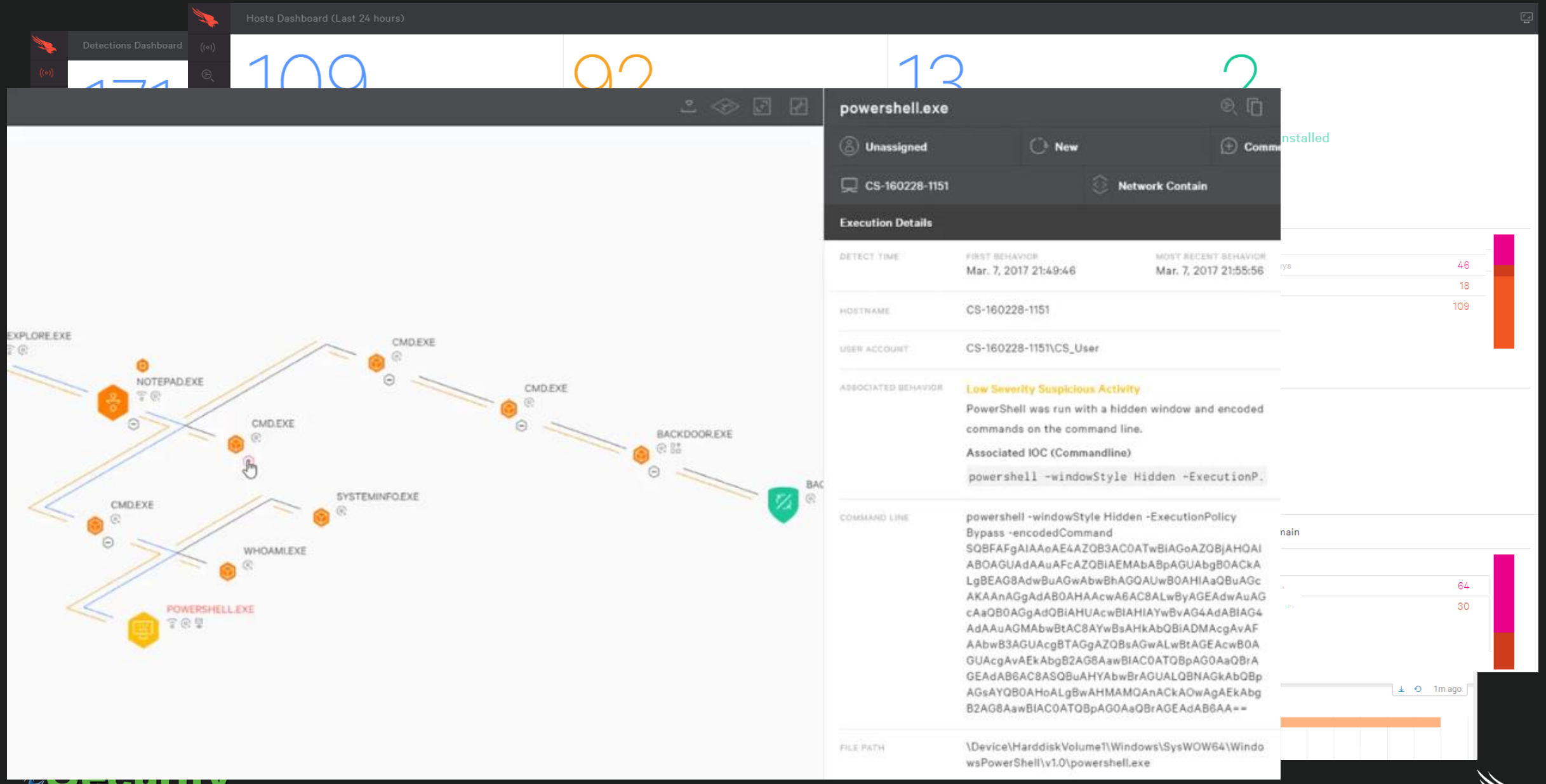
避免遺漏警報

縮短修復時間

沒有硬體、儲存成本

威脅獵捕

CROWDSTRIKE



CROWDSTRIKE

客戶POC實際案例 (期間: 一個月)

Severity	Counts
Low	1868
Medium	227
High	177
Critical	7

Host Name	事件總數	總計處理時間 (Duration)
[redacted]	37	3 小時
[redacted]	1	及時處理
[redacted]	4	3 天
[redacted]	1	及時處理
[redacted]	1	及時處理
[redacted]	3	2次，分別6分鐘和1.5天
[redacted]	6	1.5 天

iSecurity
The Hub of Security Innovations

CROWDSTRIKE

MANAGED HUNTING – **FALCON OVERWATCH**

BUSINESS VALUE

阻止可能發生的重大資安事件

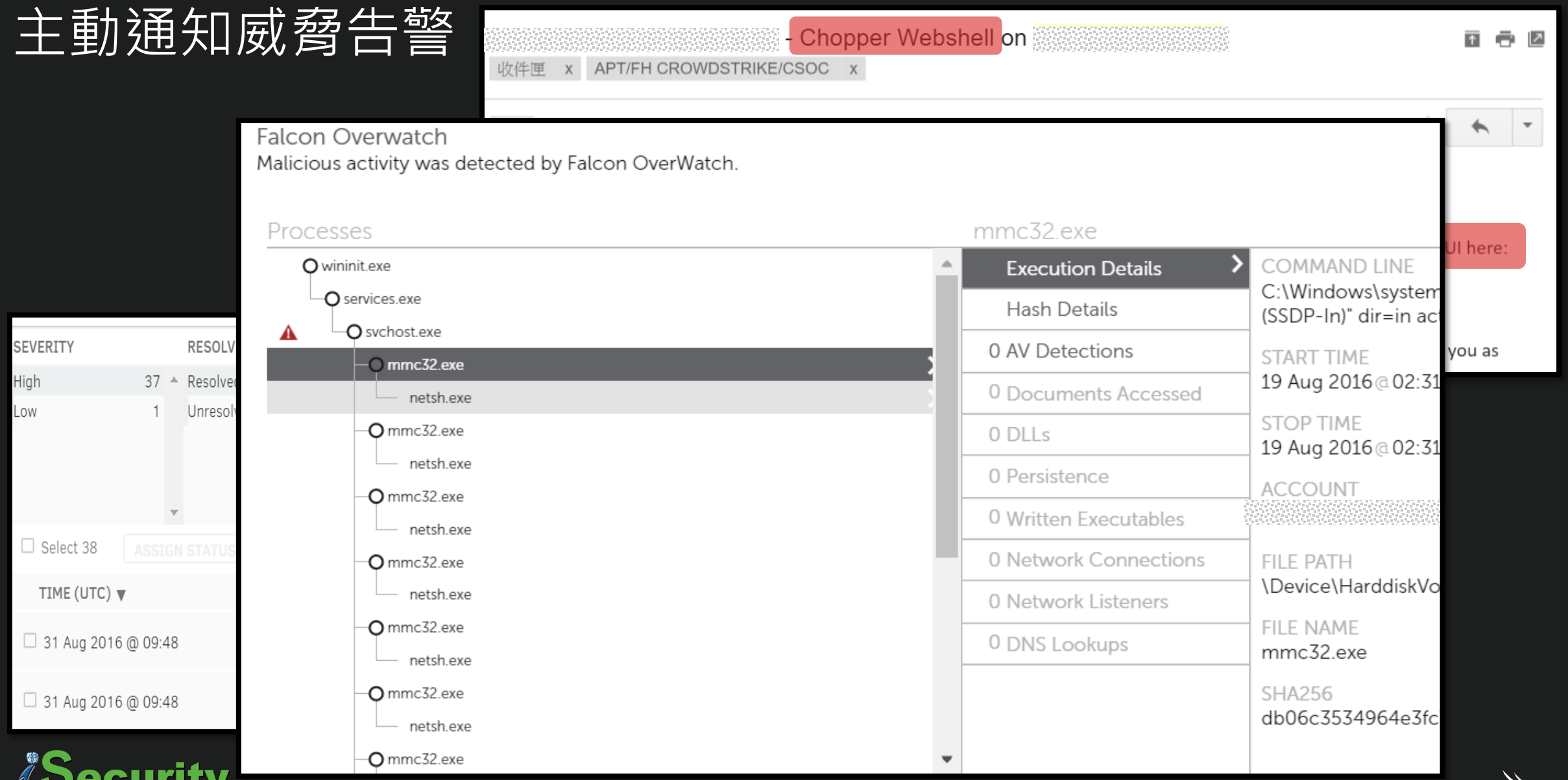
專家加持：效果加倍

社群聯防：強化抵抗力

降低誤判—關注重點

CROWDSTRIKE

主動通知威脅告警

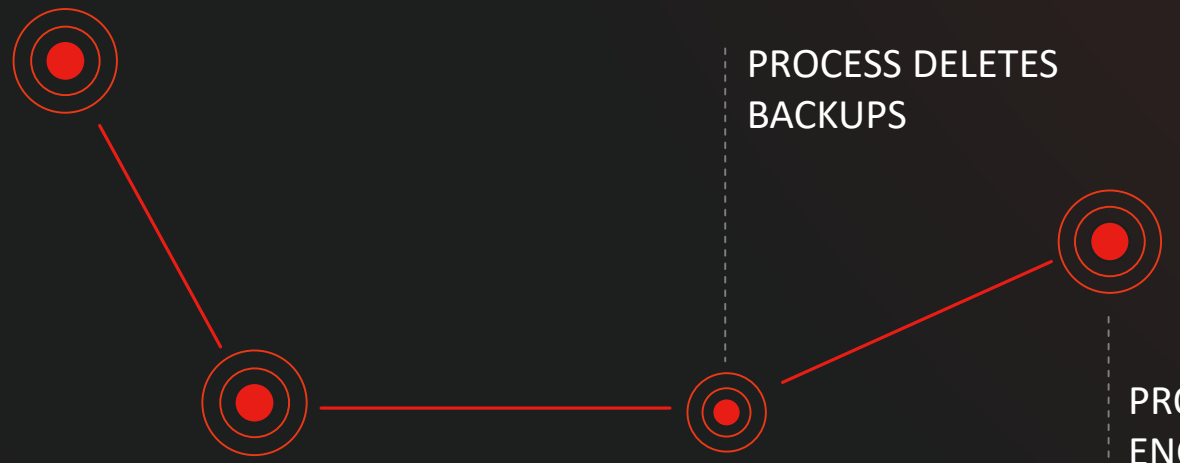


iSecurity
The Hub of Security Innovations

CROWDSTRIKE

THREATGRAPH™

事件串流處理
Event Streaming Process



IOA

Indicators
Of
Attack
攻擊指標

IOC

Indicators
of
Compromise
入侵指標

MD5 Hash
IP/Domain
Virus Signature

iSecurity
The Hub of Security Innovations

CROWDSTRIKE

ARTIFICIAL INTELLIGENCE

Powered by THREATGRAPH

FALCON PLATFORM AI

更多的原始數據
更多的AI模擬訓練
即時分析
歷史資料分析
全局視野
以資安為基礎

iSecurity
The Hub of Security Innovations

CROWDSTRIKE

THREAT INTELLIGENCE – **FALCON INTEL**

BUSINESS VALUE

專家諮詢
溝通管道

優先回應

威脅關聯

C-Level Reporting

驅動資安自動化

自有的
威脅情資分析

CROWDSTRIKE

至少有17個高度複雜的攻擊組織瞄準台灣各產業

Target Country: Taiwan × 17 Actors found ×

Origin		Target Industry		Target Country		Motivation	
China	13	Aerospace & Defense	13	United States	70	Espionage	16
India	1	Government	12	Japan	20	Criminal	2
North Korea	1	Technology	9	Germany	19		
Russian Federation	1	Financials	7	United Kingdom	19		
Unknown	1	Industrial Goods	6	India	18		
+Q		+Q	18 more	+Q	92 more	+Q	

Recent Actor Activity

COBALT SPIDER

LAST ACTIVE
November 2017

TARGET NATIONS
8 Eastern Europe, Georgia, Kazakhstan, Kuwait, Malaysi...

TARGET INDUSTRIES
1 Financials

View Profile

STARDUST CHOLLIMA

LAST ACTIVE
October 2017

TARGET NATIONS
18 Bangladesh, Belarus, Brazil, Chile, Colombia, Ecuad...

TARGET INDUSTRIES
2 Financials, Technology

View Profile

WICKED PANDA

LAST ACTIVE
September 2017

TARGET NATIONS
4 Japan, South Korea, Taiwan, United States

TARGET INDUSTRIES
5 Chemicals, Engineering, Manufacturing, Technology...

View Profile

VICEROY TIGER

LAST ACTIVE
August 2016

TARGET NATIONS
17 Afghanistan, Australia, Canada, China, India, Iran, ...

TARGET INDUSTRIES
10 Aerospace & Defense, Dissident, Financials, Gover...

View Profile

iSecurity
The Hub of Security Innovations

CROWDSTRIKE

NEXT-GEN AV – **FALCON PREVENT**

BUSINESS VALUE

預防各種類型的攻擊
阻擋已知/未知惡意程式

防止已知/未知或是Malware Free的攻擊程式

預防零時差攻擊

杜絕勒索軟體

無須更新特徵

少於1%的CPU資源

離線也能提供保護

漏洞修補

CROWDSTRIKE

We Stop Breaches

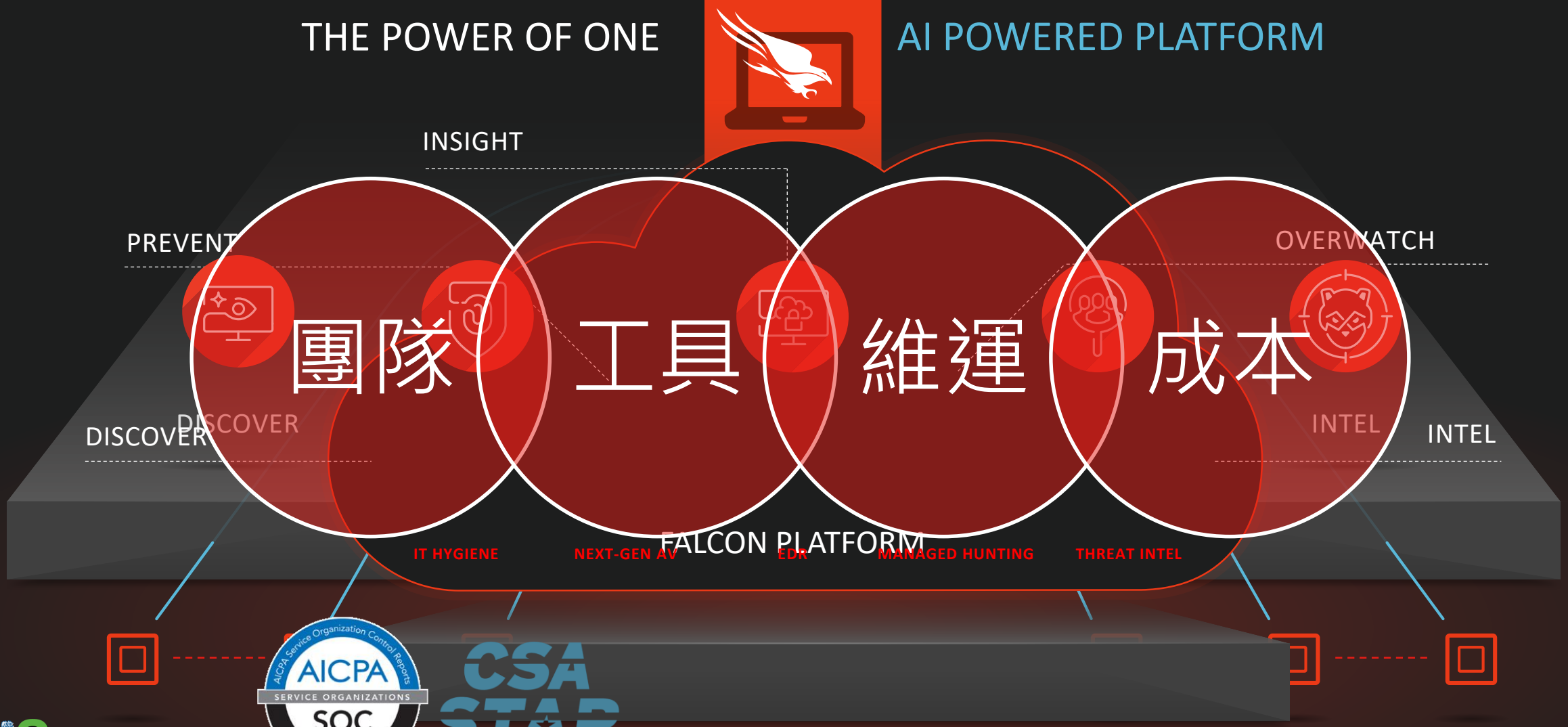
CLOUD DELIVERED
ENDPOINT PROTECTION

CROWDSTRIKE

CLOUD-DELIVERED ENDPOINT PROTECTION

THE POWER OF ONE

AI POWERED PLATFORM

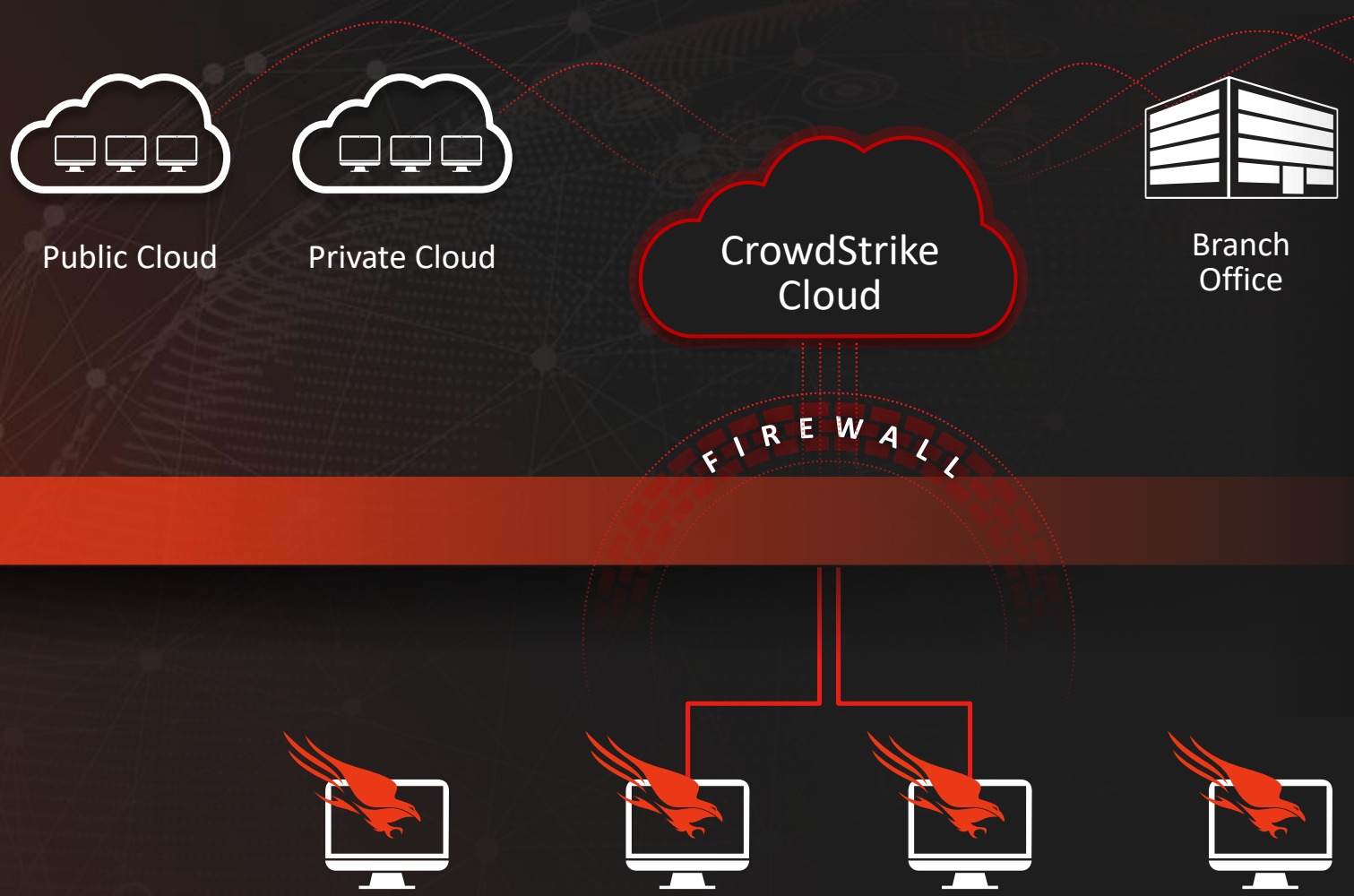


iSecurity
The Hub of Security Innovations

AICPA Service Organization Control Reports
AICPA
SERVICE ORGANIZATIONS
SOC
aicpa.org/soc
Formerly SAS 70 Reports

CSA STAR

PROTECTING EVERY ENDPOINT EVERYWHERE



BUSINESS VALUE

涵蓋企業所有端點設備

私有雲/公有雲都沒問題

Amazon, Google, Azure

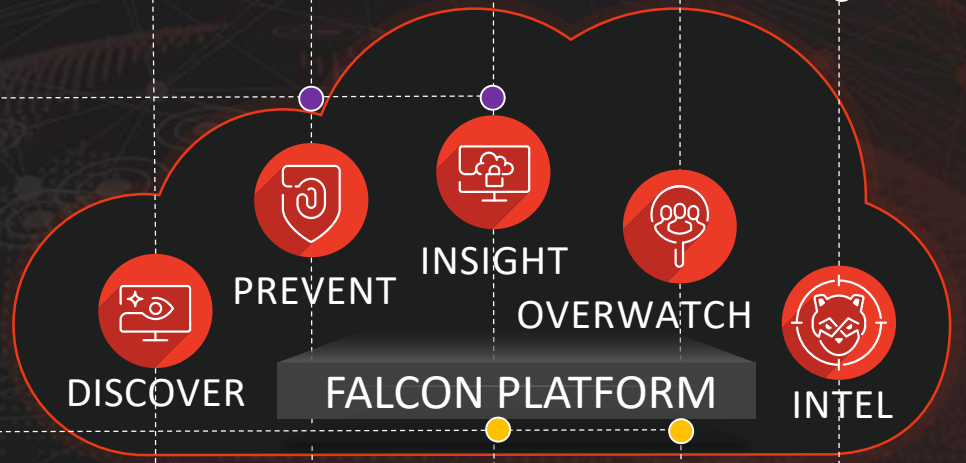
毋須佈署硬體與管理

即時更新

離線端點照樣保護

- **Identify**
  - Asset Management
  - Business Environment
  - Governance
  - Risk Assessment
  - Risk Management Strategy
- **Protect**
  - Protective Technology
  - Awareness and Training
  - Data Security
  - Information Protection Processes and Procedures
  - Maintenance
  - Access Control
- **Detect**
  - Anomalies and Events
  - Security Continuous Monitoring
  - Detection Processes
- **Respond**
  - Response Planning
  - Communications
  - Analysis
  - Mitigation
  - Improvements
- **Recover**
  - Recovery Planning
  - Improvements
  - Communications

NIST Cyber Security Framework



THE POWER OF ONE

CLOUD DELIVERED ENDPOINT PROTECTION

AI POWERED PLATFORM

CROWDSTRIKE

7X24企業專屬資安應變服務

數位資安系統