CISCO Connect

Identity Intelligence + XDR

Rick Su
思科臺灣資安事業部
資深技術顧問
2026/07/07

AI 進化，引領無限可能
Innovate with AI. Connect with Resilience.

Agenda

1. Threat Intelligence 威脅情資
2. Identity Intelligence 身分情資
3. Cisco Identity Intelligence + XDR
4. 應用案例：使用者身分受駭調查

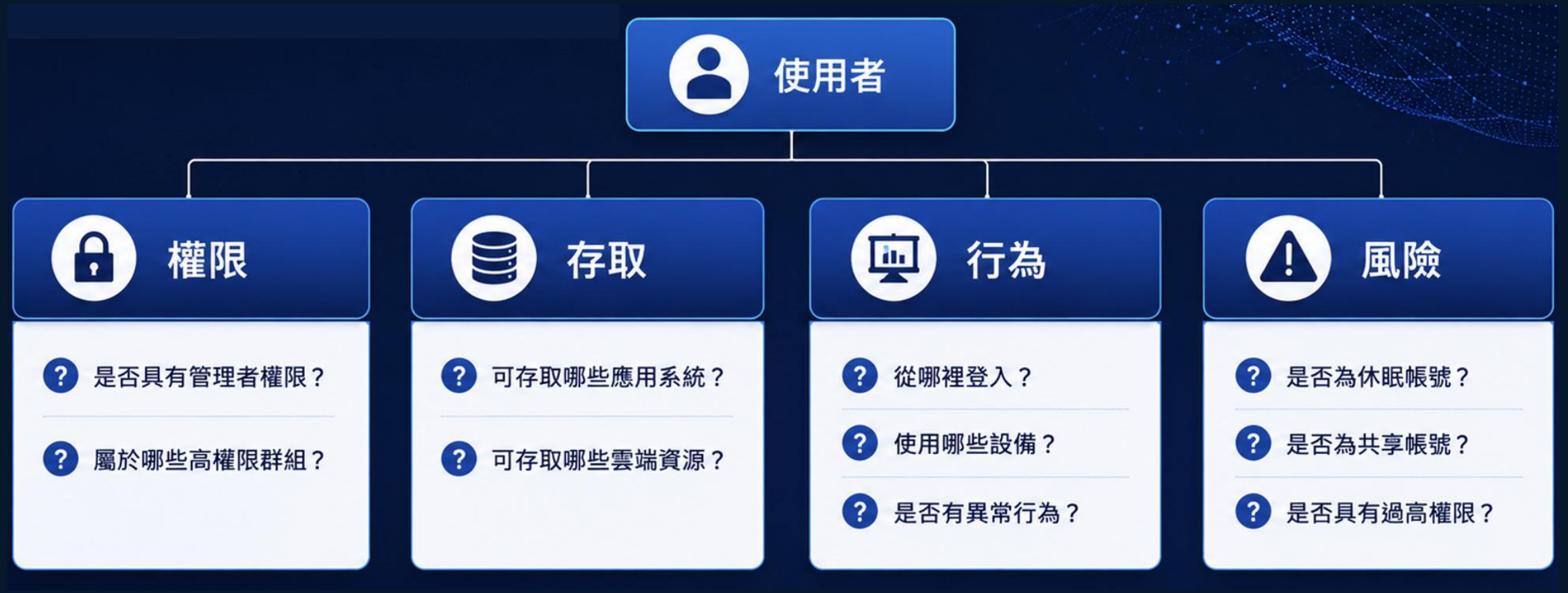
Threat Intelligence 威脅情資

策略型	戰術型	營運型
AI 威脅與風險	MITRE ATT&CK	IoC 入侵指標
量子運算風險	TTPs (戰術、技術、程序)	IP 位址
進階持續威脅	攻擊活動	網域
惡意威脅趨勢	惡意程式家族	檔案軟體雜湊值

Threat Intelligence 告訴我們：有哪些威脅正在發生？

但無法告訴我們：誰是最有可能被攻擊的人？

Identity Intelligence 身分情資



Cisco Identity Intelligence + XDR

掌握威脅來源、攻擊手法與影響範圍。

找出高風險使用者與高價值目標。

建立使用者風險輪廓與身分情資可視圖。

關聯威脅情資與身分情資，加速調查與回應。

Use Case: Compromised User Investigation

利用 Cisco Identity Intelligence + XDR 加速調查與回應

1 威脅偵測

XDR 偵測到使用者連線惡意網域

連線到惡意網域
evil-login[.]com

rick@company.com

相關情資

- 惡意網域
- 可疑 IP 位址
- 已知攻擊活動 (TTPs)

來源：Threat Intelligence

2 身分風險關聯

Cisco Identity Intelligence 自動關聯身分風險

rick@company.com

高權限帳號
Global Administrator

MFA 未啟用
增加被攻擊風險

90 天未變更密碼
增加被利用風險

異常登入國家/地區
Taiwan → Russia

來源：Identity Intelligence

3 建立身分情資

整合多維度資訊，建立使用者風險輪廓

風險評分
高風險 90 /100

4 XDR 關聯分析

將威脅情資與身分情資關聯，提升事件可信度

惡意網域連線
evil-login[.]com

+

高權限帳號
Global Administrator

+

MFA 未啟用

+

異常登入位置
Russia

事件可信度：非常高

5 快速回應

透過 XDR Playbook 自動化處置

停用使用者帳號

強制重設密碼

要求 MFA 驗證

建立 ServiceNow Ticket

通知 SOC 團隊

事件已處置

帶來的價值

快速識別真正風險
結合身分與威脅情資，找出高風險帳號

加速調查效率
減少跨系統查詢時間，快速掌握全貌

提高準確性
多維度情資關聯，降低誤報與漏報

強化自動化回應
自動化處置流程，降低營運負擔

調查時間縮短
80%+

Cisco Identity Intelligence × Cisco XDR = 更完整的情資關聯，更快的調查與更強的安全防護

Use Case: Compromised User Investigation

利用 Cisco Identity Intelligence + XDR 加速調查與回應

1 威脅偵測

XDR 偵測到使用者連線惡意網域

連線到惡意網域
evil-login[.]com

rick@company.com

相關情資
- 惡意網域
- 可疑 IP 位址
- 已知攻擊活動 (TTPs)

來源：Threat Intelligence

2 身分風險關聯

Cisco Identity Intelligence 自動關聯身分風險

rick@company.com

- 高權限帳號 Global Administrator
- MFA 未啟用 增加被攻擊風險
- 90 天未變更密碼 增加被利用風險
- 異常登入國家/地區 Taiwan → Russia

來源：Identity Intelligence

3 建立身分情資

整合多維度資訊，建立使用者風險輪廓

風險評分
高風險 90 /100

4 XDR 關聯分析

將威脅情資與身分情資關聯，提升事件可信度

- 惡意網域連線 evil-login[.]com
- \+ 高權限帳號 Global Administrator
- \+ MFA 未啟用
- \+ 異常登入位置 Russia

事件可信度：非常高

5 快速回應

透過 XDR Playbook 自動化處置

- 停用使用者帳號
- 強制重設密碼
- 要求 MFA 驗證
- 建立 ServiceNow Ticket
- 通知 SOC 團隊

事件已處置

帶來的價值

快速識別真正風險
結合身分與威脅情資，找出高風險帳號

加速調查效率
減少跨系統查詢時間，快速掌握全貌

提高準確性
多維度情資關聯，降低誤報與漏報

強化自動化回應
自動化處置流程，降低營運負擔

調查時間縮短
80%+

Cisco Identity Intelligence × Cisco XDR = 更完整的情資關聯，更快的調查與更強的安全防護

Use Case: Compromised User Investigation

利用 Cisco Identity Intelligence + XDR 加速調查與回應

1 威脅偵測

XDR 偵測到使用者連線惡意網域

連線到惡意網域
evil-login[.]com

rick@company.com

相關情資
- 惡意網域
- 可疑 IP 位址
- 已知攻擊活動 (TTPs)

來源：Threat Intelligence

2 身分風險關聯

Cisco Identity Intelligence 自動關聯身分風險

rick@company.com

高權限帳號
Global Administrator

MFA 未啟用
增加被攻擊風險

90 天未變更密碼
增加被利用風險

異常登入國家/地區
Taiwan → Russia

來源：Identity Intelligence

3 建立身分情資

整合多維度資訊，建立使用者風險輪廓

風險評分
高風險 90 /100

4 XDR 關聯分析

將威脅情資與身分情資關聯，提升事件可信度

惡意網域連線
evil-login[.]com

+

高權限帳號
Global Administrator

+

MFA 未啟用

+

異常登入位置
Russia

事件可信度：非常高

5 快速回應

透過 XDR Playbook 自動化處置

停用使用者帳號

強制重設密碼

要求 MFA 驗證

建立 ServiceNow Ticket

通知 SOC 團隊

事件已處置

帶來的價值

快速識別真正風險
結合身分與威脅情資，找出高風險帳號

加速調查效率
減少跨系統查詢時間，快速掌握全貌

提高準確性
多維度情資關聯，降低誤報與漏報

強化自動化回應
自動化處置流程，降低營運負擔

調查時間縮短
80%+

Cisco Identity Intelligence × Cisco XDR = 更完整的情資關聯，更快的調查與更強的安全防護

Use Case: Compromised User Investigation

利用 Cisco Identity Intelligence + XDR 加速調查與回應

1 威脅偵測

XDR 偵測到使用者連線惡意網域

連線到惡意網域
evil-login[.]com

rick@company.com

相關情資
- 惡意網域
- 可疑 IP 位址
- 已知攻擊活動 (TTPs)

來源：Threat Intelligence

2 身分風險關聯

Cisco Identity Intelligence 自動關聯身分風險

rick@company.com

高權限帳號
Global Administrator

MFA 未啟用
增加被攻擊風險

90 天未變更密碼
增加被利用風險

異常登入國家/地區
Taiwan → Russia

來源：Identity Intelligence

3 建立身分情資

整合多維度資訊，建立使用者風險輪廓

風險評分
高風險 90 /100

4 XDR 關聯分析

將威脅情資與身分情資關聯，提升事件可信度

惡意網域連線
evil-login[.]com

+

高權限帳號
Global Administrator

+

MFA 未啟用

+

異常登入位置
Russia

事件可信度：非常高

5 快速回應

透過 XDR Playbook 自動化處置

- 停用使用者帳號
- 強制重設密碼
- 要求 MFA 驗證
- 建立 ServiceNow Ticket
- 通知 SOC 團隊

事件已處置

帶來的價值

快速識別真正風險
結合身分與威脅情資，找出高風險帳號

加速調查效率
減少跨系統查詢時間，快速掌握全貌

提高準確性
多維度情資關聯，降低誤報與漏報

強化自動化回應
自動化處置流程，降低營運負擔

調查時間縮短
80%+

Cisco Identity Intelligence × Cisco XDR = 更完整的情資關聯，更快的調查與更強的安全防護

Use Case: Compromised User Investigation

利用 Cisco Identity Intelligence + XDR 加速調查與回應

1 威脅偵測

XDR 偵測到使用者連線惡意網域

連線到惡意網域
evil-login[.]com

rick@company.com

相關情資
- 惡意網域
- 可疑 IP 位址
- 已知攻擊活動 (TTPs)

來源：Threat Intelligence

2 身分風險關聯

Cisco Identity Intelligence 自動關聯身分風險

rick@company.com

高權限帳號
Global Administrator

MFA 未啟用
增加被攻擊風險

90 天未變更密碼
增加被利用風險

異常登入國家/地區
Taiwan → Russia

來源：Identity Intelligence

3 建立身分情資

整合多維度資訊，建立使用者風險輪廓

風險評分
高風險 90 /100

4 XDR 關聯分析

將威脅情資與身分情資關聯，提升事件可信度

惡意網域連線
evil-login[.]com

+

高權限帳號
Global Administrator

+

MFA 未啟用

+

異常登入位置
Russia

事件可信度：非常高

5 快速回應

透過 XDR Playbook 自動化處置

- 停用使用者帳號
- 強制重設密碼
- 要求 MFA 驗證
- 建立 ServiceNow Ticket
- 通知 SOC 團隊

事件已處置

帶來的價值

快速識別真正風險
結合身分與威脅情資，找出高風險帳號

加速調查效率
減少跨系統查詢時間，快速掌握全貌

提高準確性
多維度情資關聯，降低誤報與漏報

強化自動化回應
自動化處置流程，降低營運負擔

調查時間縮短
80%+

Cisco Identity Intelligence × Cisco XDR = 更完整的情資關聯，更快的調查與更強的安全防護

Use Case: Compromised User Investigation

利用 Cisco Identity Intelligence + XDR 加速調查與回應

1 威脅偵測

XDR 偵測到使用者連線惡意網域

連線到惡意網域
evil-login[.]com

rick@company.com

相關情資
- 惡意網域
- 可疑 IP 位址
- 已知攻擊活動 (TTPs)

來源：Threat Intelligence

2 身分風險關聯

Cisco Identity Intelligence 自動關聯身分風險

rick@company.com

高權限帳號
Global Administrator

MFA 未啟用
增加被攻擊風險

90 天未變更密碼
增加被利用風險

異常登入國家/地區
Taiwan → Russia

來源：Identity Intelligence

3 建立身分情資

整合多維度資訊，建立使用者風險輪廓

風險評分
高風險 90 /100

4 XDR 關聯分析

將威脅情資與身分情資關聯，提升事件可信度

惡意網域連線
evil-login[.]com

+

高權限帳號
Global Administrator

+

MFA 未啟用

+

異常登入位置
Russia

事件可信度：非常高

5 快速回應

透過 XDR Playbook 自動化處置

停用使用者帳號

強制重設密碼

要求 MFA 驗證

建立 ServiceNow Ticket

通知 SOC 團隊

事件已處置

帶來的價值

快速識別真正風險
結合身分與威脅情資，找出高風險帳號

加速調查效率
減少跨系統查詢時間，快速掌握全貌

提高準確性
多維度情資關聯，降低誤報與漏報

強化自動化回應
自動化處置流程，降低營運負擔

調查時間縮短
80%+

Cisco Identity Intelligence × Cisco XDR = 更完整的情資關聯，更快的調查與更強的安全防護

CISCO Connect

Logicalis Managed Security Service

Managed Cisco XDR

Roger Loh 羅志謙

Logicalis 亞太首席資安總監

Commercial in Confidence

CRN CHANNEL AWARDS ASIA 2025 MSSP Winner

AI 進化，引領無限可能
Innovate with AI. Connect with Resilience.

Cisco Identity Intelligence – 實際案例

Inactive Guest Users

Critical | **8** failing users (an increase since last week) | Compliance, Identity Posture Insight

Detects guest accounts that have not successfully signed in and thus are inactive.
These accounts can be overlooked during regular audits, which makes them attractive targets for bad actors that try to exploit less secure entry points. Most compliance frameworks also require inactive accounts to be assessed and removed promptly.
A user will fail this check if they have a guest account that has been inactive for more than 30 days. If needed, adjust the number of days inactive threshold in Custom Detection Settings. This could increase the accuracy and actionability of check results.

Recommended Actions

Assess the security posture of inactive guest accounts, including whether conditional access and MFA are enabled. Contact relevant stakeholders, such as the account that invited the guest user, to determine if the accounts is still needed. For accounts that are no longer required, delete them on a regular schedule, as they can be easily re-invited when necessary.

See report

Inactive Users

Moderate | **88** failing users (0.98% increase since last week) | Compliance, Identity Posture Insight

Detects enabled accounts that have not successfully signed in and thus are inactive.
These accounts pose significant security and financial risks. Dormant accounts may consume licenses unnecessarily. They also provide attackers with opportunities to exploit unused access to systems.
A user will fail this check if they have been inactive for more than 30 days. If needed, you can adjust the number of days inactive threshold in Custom Detection Settings. This could increase the accuracy and actionability of check results.

Recommended Actions

Start an access review with the user's manager to determine if the account is still required. If the account is no longer needed, deprovision it immediately to cut unnecessary risk and cost. If the account is still needed, monitor it for activity. If it remains inactive, suspend it after a grace period. Adopt the least privileged model to reduce standing entitlements and your organization's attack surface.

See report

Allow/Block Email Logins

Critical | **26** failing users (5.81% increase since last week) | Compliance, Identity Posture Insight

Identifies potentially malicious or unauthorized email domains by monitoring email addresses in authentication events or access logs. The detection combines allow/block lists with automated prevalence-based discovery over the last 30 days to flag suspicious domains.
Detection methodology:
1. Known list definition (one of the following)
- Block list enforcement: Immediately flags any domain explicitly added to the organization's block list (known malicious or prohibited domains).
- Allow list validation: Alerts when authentication occurs from domains not in the pre-approved allow list (allow list acts as a positive security model).
2. Auto-discovery mechanism: Identifies suspicious domains through prevalence analysis; domains appearing in fewer than five distinct user accounts within the evaluation window trigger alerts.
3. False-positive control: Ignore list allows security teams to suppress alerts for known-good domains.

Recommended Actions

Depending on your security posture, consider deleting users using emails with those domains and exploring why you have them in the system.

Users Sharing Authenticators

Critical | **14** failing users (no change since last week) | Compliance, Identity Posture Insight

Detects users whose phone number-based authenticators or Okta hardware security keys are registered to multiple accounts, which reduces individual accountability and can allow a single compromised or shared device to be used to access more than one identity.
Users should not share authentication credentials and should have their own dedicated authenticator so that a compromised or stolen device cannot be used to gain unauthorized access across multiple accounts within your organization.

Recommended Actions

Review the failing users to determine whether the shared authenticator represents an unintentional security gap or a known legitimate case, such as an admin account sharing with its associated day-to-day account. Link any accounts with a legitimate sharing need in Identity Intelligence so that these accounts will no longer fail the check, as linked account as treated as intentionally associated.
For all other cases, remove the shared authenticator from the additional accounts and contact the affected users. If a large number of users are failing this check, review your account onboarding process to ensure new accounts are not being provisioned with a shared or generic phone number or hardware security key.

No Strong MFA Configured

Moderate | **13** failing users (no change since last week) | Compliance, Identity Posture Insight

Detects accounts where every active multi-factor authentication method is a weak form of verification, such as SMS codes, email one-time passwords, or voice calls, leaving them more vulnerable to interception and SIM-swapping attacks than accounts protected by stronger authentication methods.
Accounts where the identity source is managed through a federated provider or Okta accounts where all weak factors are designated as recovery methods only, are excluded from this check.
The National Institute of Standards and Technology (NIST) recommends using authenticator apps or cryptographic solutions such as Duo Verified Push or Passwordless, Google Authenticator, Okta Verify, or Microsoft Authenticator, as well as hardware security keys, as strong second factors.

Recommended Actions

Encourage users to replace weak authentication methods with a stronger alternative such as an authenticator app or hardware security key, prioritizing accounts with access to critical systems and administrative privileges. Where a user has a legitimate reason to remain on a weaker method, document the exception and consider providing a physical hardware security key as a more secure fallback option.

Never Logged In

Critical | **268** failing users (1.79% increase since last week) | Compliance, Identity Posture Insight

Detects accounts that were created but never successfully used to log in.
Attackers may exploit these unused accounts to register their own MFA factors, potentially bypassing authentication controls and gaining unauthorized access.
A user will fail this check if they have not logged in 7 days after an account was created. If needed, adjust the new account grace period in Custom Detection Settings to align with your organization's procedures. This could increase the accuracy and actionability of check.

Recommended Actions

Trigger an access review with the user's manager to verify if the account is still necessary. If the account is unnecessary, suspend it immediately. If the account is needed, reset it and direct the manager to onboard the user properly.

See report

Entra ID Long Running Sessions

Moderate | **1** failing users (a decrease since last week) | Compliance, Identity Posture Insight

Detects users with long-running sessions in Entra ID, defined as more than 90 days.
Alert only on sessions that don't have any authentication record in last 30 days.
Extremely long sessions without re-authentication pose a security threat and can increase the chance of session hijacking.

Recommended Actions

Clear the end user sessions to require re-authentication.
We recommend setting "Maximum Entra ID session lifetime" to 16 hours (one working day) and "Expire session after user has been idle on Entra ID for" to 2 hours.

See report

Users With Defined Email Forward Rules

Moderate | **15** failing users (no change since last week) | Compliance, Identity Threat Insight

Detects users that have email forwarding rules defined.
Email forwarding is mostly harmless and comes from the need to deal with life changes and organizational shifts. However, this is also a known bad pattern for people knowing they are about to change jobs and is a cause of data loss.
You can add known domains to the ignore list.

Recommended Actions

Please check if the forward rule is legitimate, for example, contractors and managers, or a potential data loss issue.

See report

Non-Human Identity with Interactive Browser Access

Moderate | **19** failing users (0.75% decrease since last week) | Compliance, Identity Threat Insight, Non-Human Identities

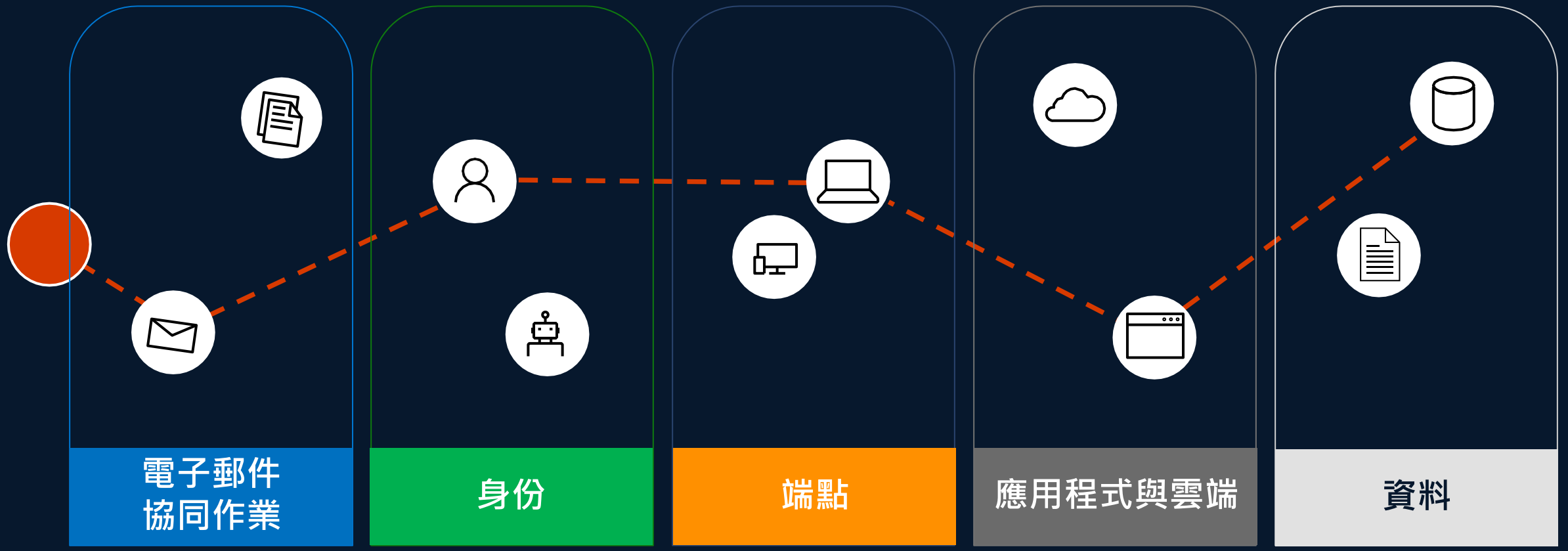
Detects non-human identities (NHIs) accessing resources using interactive browsers.
Interactive browser access by NHIs is rare and a risk factor for non-interactive accounts. This anomalous behavior should be investigated.

Recommended Actions

Please review the associated activity of the NHI(s) failing this check. Evaluate the account's behavior for signs of other security anomalies, such as interactive logins, new locations, or login failures.

See report

攻擊者是以 圖形化 思考



.....各類的工具之間，無聲息地穿透網路縫隙進行橫向移動

當前的進階威脅跨多個網域使用複雜的攻擊手法

一封精心策劃且個人化的電子郵件誘使使用者點擊.....

進而連結到可疑的網站.....

導致在使用者的本機裝置上建立異常程序（process）.....

該程序將連線到另一台機器或直接存取其資料

T1566: 魚叉式網路釣魚

T1055: 程序植入

T1189: 路過式下載破解

T1087: 帳號探索：網域帳號

T1570: 橫向工具轉移

T1048: 系統網路連線探索

廠商 A	廠商 C	廠商 E	廠商 G	廠商 D

XDR 是應對現代 AI 驅動攻擊的解答

EDR

VS.

XDR

EDR	XDR
僅限端點安全	橫跨身分、電子郵件、端點、網路、防火牆、雲端等多個領域的全方位安全與訊息關聯。
孤立的端點警報	以事件為中心的調查與回應體驗
僅能協助抵禦特定端點的攻擊，缺乏大局觀，無法有效應對進階威脅	有效防禦進階攻擊，例如勒索軟體、商業電子郵件詐騙 (BEC) 等

Cisco XDR

專為 SOC 打造的雲端原生自動化偵測與回應解決方案

端點與網路偵測 是不可或缺的核心根本

開放且具擴充性

易於使用、以設計為中心的操作者體驗

Network

Endpoint

Email

Cloud

Applications

Identity

跨域威脅遙測

攻擊可能來自任何地方，因此所有管道都必須成為威脅資料的來源

Talos Threat Intelligence

MITRE | ATT&CK Attack Framework

可執行性的情資

強大的關聯分析與頂尖的資料科學，用以探索威脅並排定優先順序

簡化地安全作業

增強人力運作以實現機器規模的安全防禦

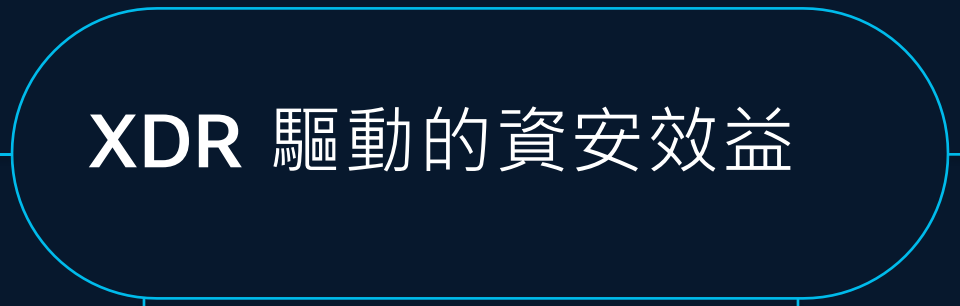
Guided Investigations

Proactive Threat Hunting

Prescriptive Response

建構於 Cisco Security Cloud 平台

將焦點轉向成效



更早偵測威脅

我們最暴露於哪些風險之中？

我們在早期偵測攻擊方面的表現如何？

依影響程度排定優先順序

我們是否優先處理對業務造成最大實質影響的攻擊？

加快調查速度

我們能多快了解攻擊的完整範圍與入侵管道？

加速回應

我們能多快充滿信心地進行回應？

安全維運（SecOps）能實現多少自動化？

我們是否有在量化指標上變得更好？

Logicalis MXDR 服務方法協助客戶逐步達成 XDR 里程碑

整合

透過整合式平台鞏固解決方案與技術

一致化

建立一個生態系統，用以彙整並豐富來自環境中所有部分的資料與遙測

協同指揮

利用 **AI** 與機器學習（**ML**）實現排定優先順序的偵測與回應

自動化

將需要最少人工干預的偵測與回應工作流程自動化

最佳化

透過主動對照基準進行執行，藉此演進並微調安全防禦

下一步

您與 Logicalis 的前行之路

Logicalis 將 Cisco XDR 與 Splunk 完美結合，並搭配經市場驗證的託管式 SOC，專為無法承受防護範圍漏洞或資安專業落差的組織量身打造

技術 (Technology)

Cisco XDR + Splunk

- **MDR (Managed Detection & Response)** 建構於 Cisco XDR 之上，防護範圍橫跨端點、網路、電子郵件、身分與雲端環境
- **Splunk 深度整合** 針對以合規為導向的資料環境，將 MDR 的可視性進一步延伸至混合雲與多雲架構
- 實現即時偵測、事件初審與分流、自動化回應，而非耗時的人工手動分析

專業知識 (Expertise)

24/7 全天候託管式 SOC

- **Cisco 認證專家團隊** 由具備 Cisco 認證的專家負責微調與維運，持續優化您的整體資安狀態
- **非傳統黑箱作業的 MSSP 模式** 每一次的警報發佈、回應動作與儀表板數據，皆完整保留在您的生態系統中
- **您保有完整的擁有權：您的環境、您的資料、您的工具 Logicalis** 的任務是讓它們更智慧地協同運作

成果效益 (Outcomes)

更快的偵測速度。更低的風險。全方位的可視性

- **提供更快速的偵測與回應** –在攻擊者觸及關鍵資料之前，即時識別出基於圖形模式的攻擊鏈
- **法規標準對齊** –包含合規性資料留存、治理報告，以及隨時應對稽核要求的數位鑑識服務
- 無論組織規模大小，皆能享有卓越的企業級 MDR 服務效益

完全透明 **Full Transparency**

24/7 全天候、全球覆蓋 **Coverage**

完整的資料擁有權 **Full Data Ownership**

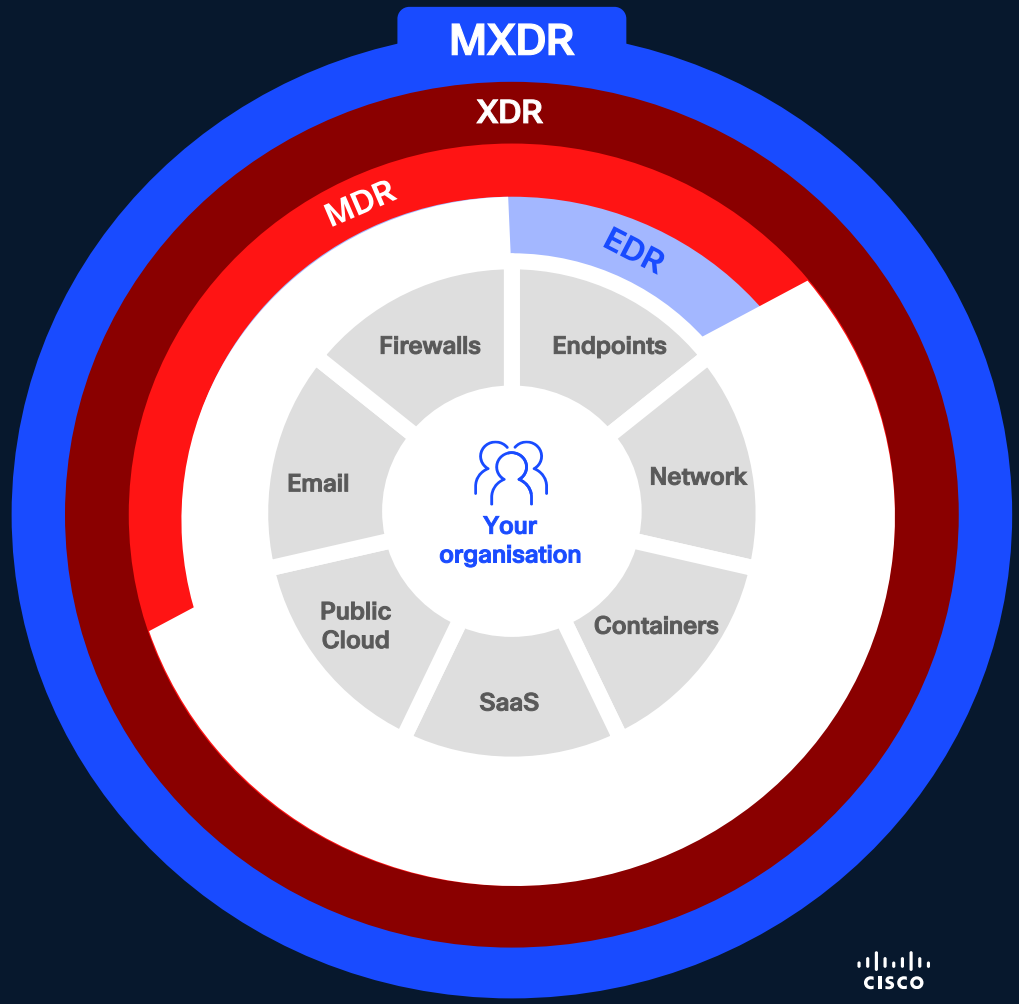
具備合規就緒能力 **Compliance-Ready**

cisco

Logicalis Cisco MXDR 服務方案

*我們的 **AI** 驅動 **MXDR** 功能透過對網路攻擊鏈的進階可視性、**AI** 驅動的自動化以及廣泛的威脅情資，全面增強安全維運（**SecOps**）*

交付項目與功能 Deliverable and Capabilities	包含
24x7x365 全天候託管、監控與回應 (Management, Monitoring, and Response)	✓
設定配置與上線引導 (Configuration and Onboarding)	✓
主動式健康檢查 (Proactive Health Checks)	✓
持續改善與微調 (Continuous Improvement and Tuning)	✓
圍堵與補救支援 (Containment and Remediation Support)	✓
XDR 整合 - 開箱即用連接器 (XDR Integration -OOTB connectors)	✓
自動化 - 開箱即用工作流程 (Automation (OOTB workflows))	✓
每月報告 (Monthly Report)	✓



https://ebooks.cisco.com/story/mxdr-managed-extended-detection-and-response__logicalis/page/1

Logicalis MSS 結合以下四大強大組件，提供全面的安全維運服務

託管式 EDR/NDR/XDR 平台

- 進階端點保護與回應
- 網路安全監控
- 雲端工作負載保護
- 電子郵件與身分安全
- 自動化回應協調策劃

基礎託管安全維運中心 (Base MSOC) 服務

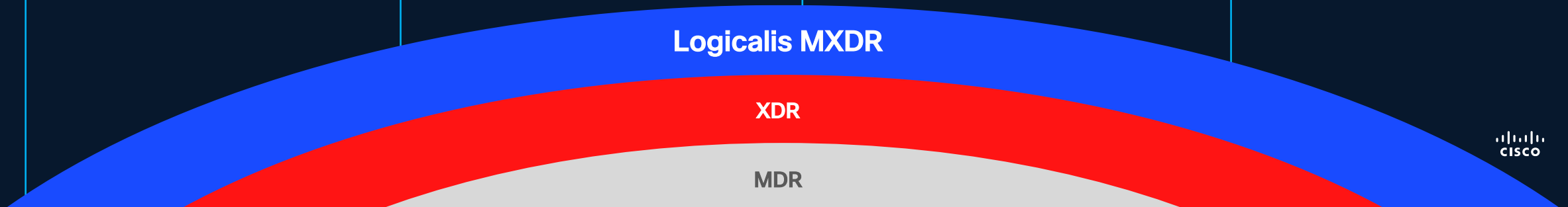
- 24x7 威脅偵測、監控與回應
- 基於 SIEM 的威脅偵測
- 漏洞管理
- 符合 NIST 800-61 R2 標準的流程
- ITSM (IT 服務管理) 整合

網路威脅情資 (CTI) 平台

- 品牌與網域冒用監控
- SEO 毒化偵測
- 外洩憑證監控
- 關鍵帳號保護
- 供應鏈風險監控
- 自動化下架服務

持續安全驗證

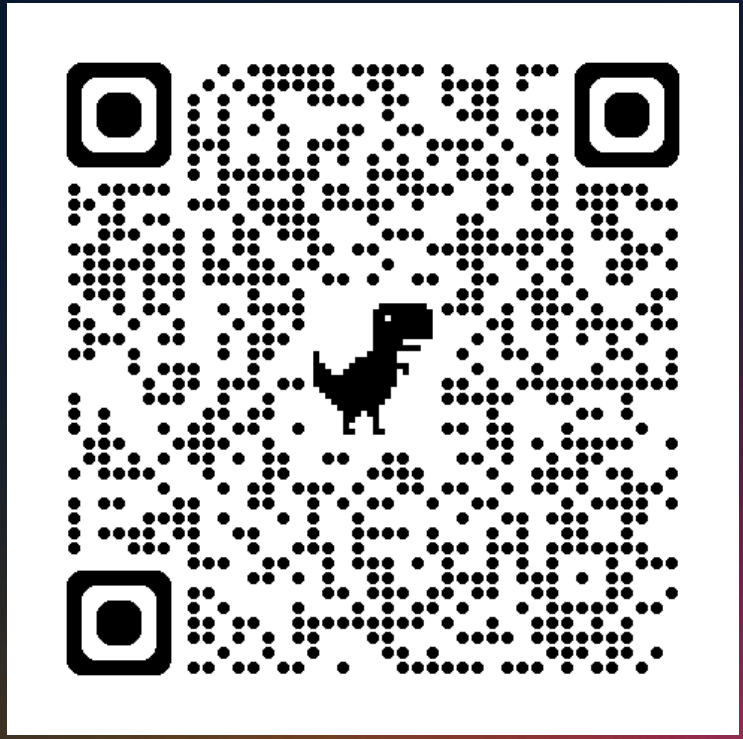
- 紫隊演練 (Purple teaming exercise)
- 攻擊模擬與偵測測試
- 控制有效性評估 (Control effectiveness assessment)
- SOC 流程改善
- 詳細洞察與建議



cisco Partner

LOGICALIS
Architects of Change

資安防護 (MXDR) 效能診斷



精準定位防禦缺口，強化企業聯防韌性

* AI 時代資安成熟度快速健檢
* 評估企業聯防能力
* 找出營運風險與改善方向
* 專家報告協助規劃後續策略

<<<< 掃描 QR Code 免費體驗

cisco

Thank you