ZUSO Generation
The best defense is offense.

臺灣證券交易所
115年證券商資通安全會議
攻擊者眼中的資安團隊隱形差距

2026.03.20

如梭世代股份有限公司
sales@zuso.ai

ZUSO Generation

The best defense is offense.

Leo Ho

zo@zuso.ai

演講

2014 HITCON 台灣駭客年會 Speaker

2015 SITCON 學生計算機年會 Speaker

2017 OWASP Taiwan Speaker

2018 OWASP 台灣資安高峰會

專長

資安檢測

資安事件調查

駭客攻擊手法

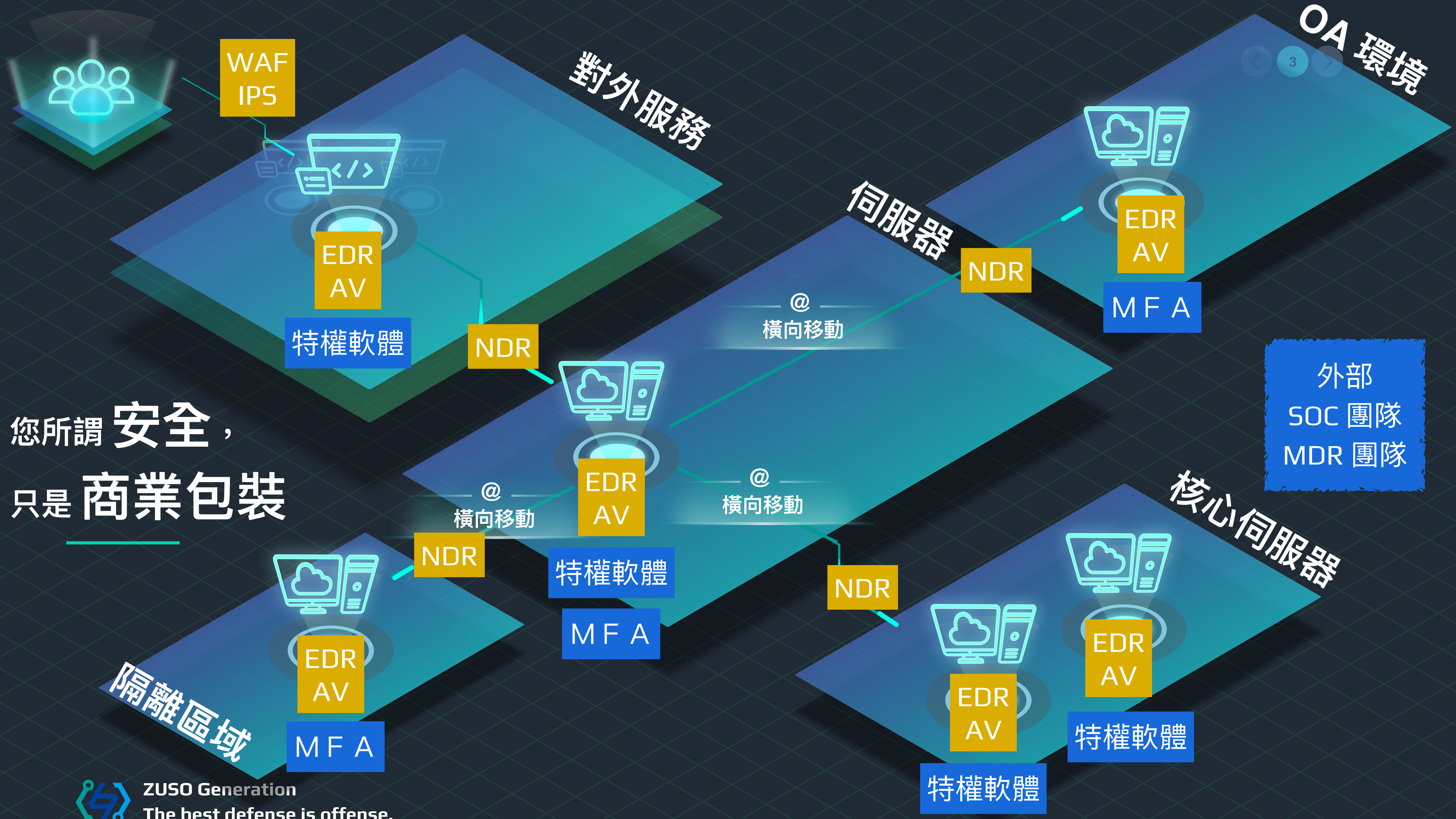
證照

Offensive Security Certified Professional

Certificated Ethical Hacker

Computer Hacking Forensic Investigator

ISO 27001 / ISO 20000 / BS 10012



OA 環境

EDR
AV

M F A

NDR

伺服器

對外服務

WAF
IPS

EDR
AV

特權軟體

NDR

@
橫向移動

EDR
AV

特權軟體

M F A

@
橫向移動

@
橫向移動

NDR

隔離區域

EDR
AV

M F A

NDR

核心伺服器

EDR
AV

特權軟體

EDR
AV

特權軟體

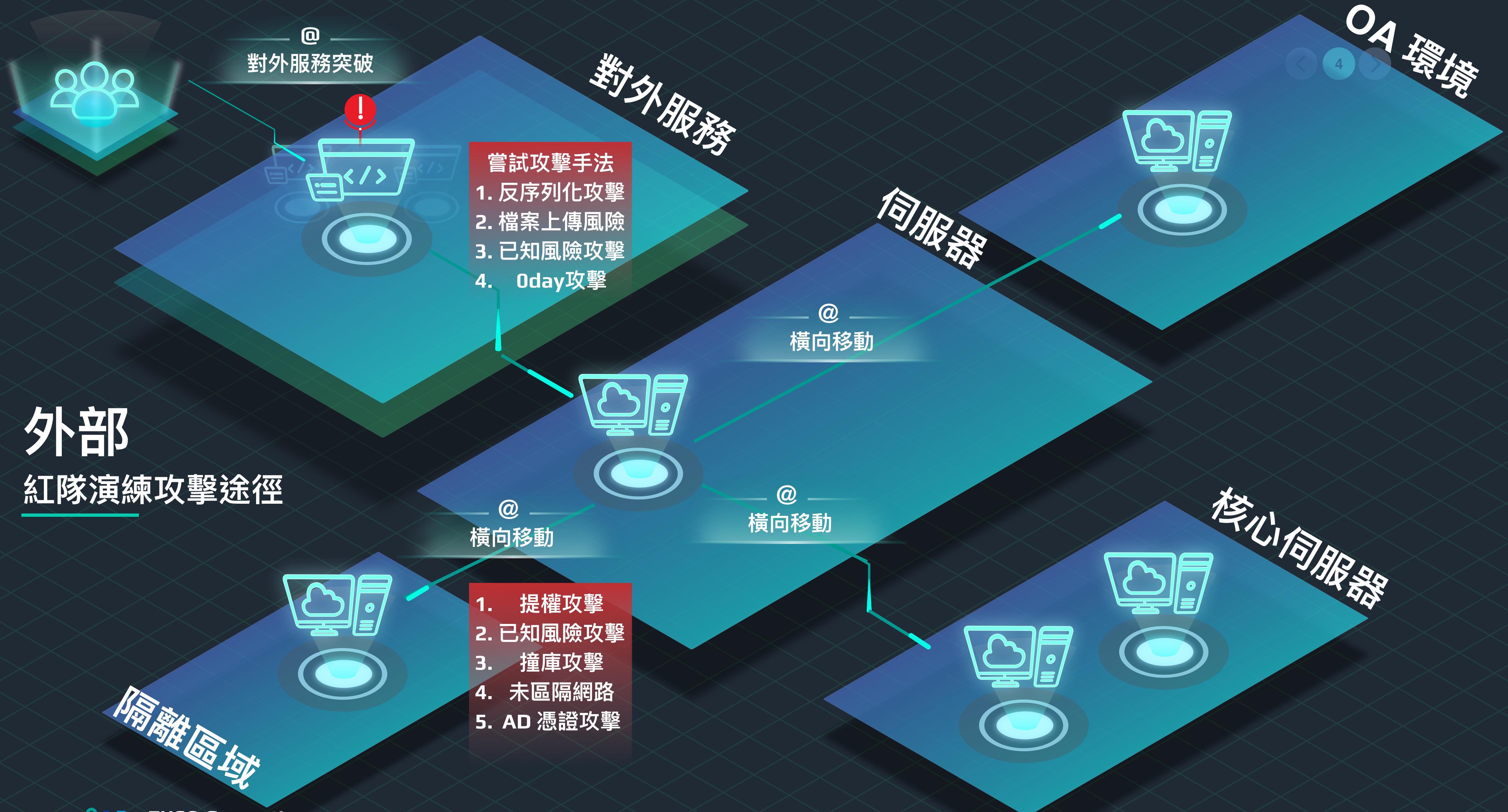
外部
SOC 團隊
MDR 團隊

您所謂 **安全**，

只是 **商業包裝**

外部

紅隊演練攻擊途徑



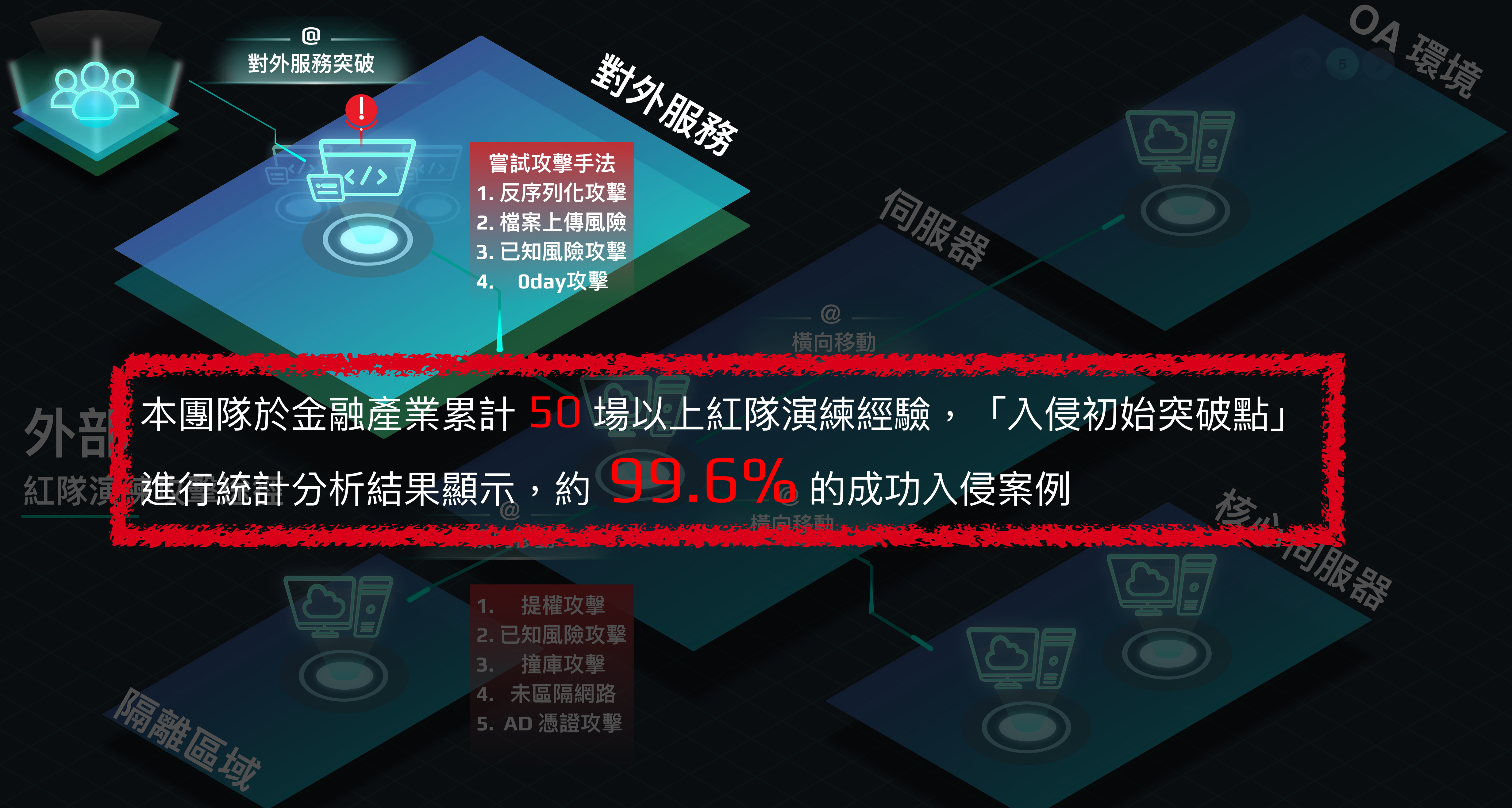
嘗試攻擊手法

1. 反序列化攻擊
2. 檔案上傳風險
3. 已知風險攻擊
4. 0day攻擊

1. 提權攻擊
2. 已知風險攻擊
3. 撞庫攻擊
4. 未區隔網路
5. AD 憑證攻擊

ZUSO Generation
The best defense is offense.

本團隊於金融產業累計 50 場以上紅隊演練經驗，「入侵初始突破點」進行統計分析結果顯示，約 99.6% 的成功入侵案例



@
對外服務突破

對外服務

嘗試攻擊手法
1. 反序列化攻擊
2. 檔案上傳風險
3. 已知風險攻擊
4. 0day攻擊

伺服器

OA 環境

@
橫向移動

外部

紅隊演

@

橫向移動

核心伺服器

1. 提權攻擊
2. 已知風險攻擊
3. 撞庫攻擊
4. 未區隔網路
5. AD 憑證攻擊

隔離區域

ZUSO Generation
The best defense is offense.

WAF
IPS
對外服務
EDR
AV
特權軟體
NDR
伺服器
NDR
EDR
AV
MFA
OA 環境
@
橫向移動
外部
SOC 團隊
MDR 團隊
您所謂安全，只是商業包裝
@
橫向移動
EDR
AV
橫向移動
核心伺服器
MFA
EDR
EDR
AV
隔離區域
MFA
特權軟體
特權軟體

工具堆疊 ≠ 對抗思維

「操作安全」讓你忙
「理解安全」讓你看見攻擊路徑

攻擊者看的不是設備清單，而是「縫」

ZUSO Generation
The best defense is offense.

認知差異

攻擊者

KPI

時間 × 隱蔽 ×
路徑最短

防禦者

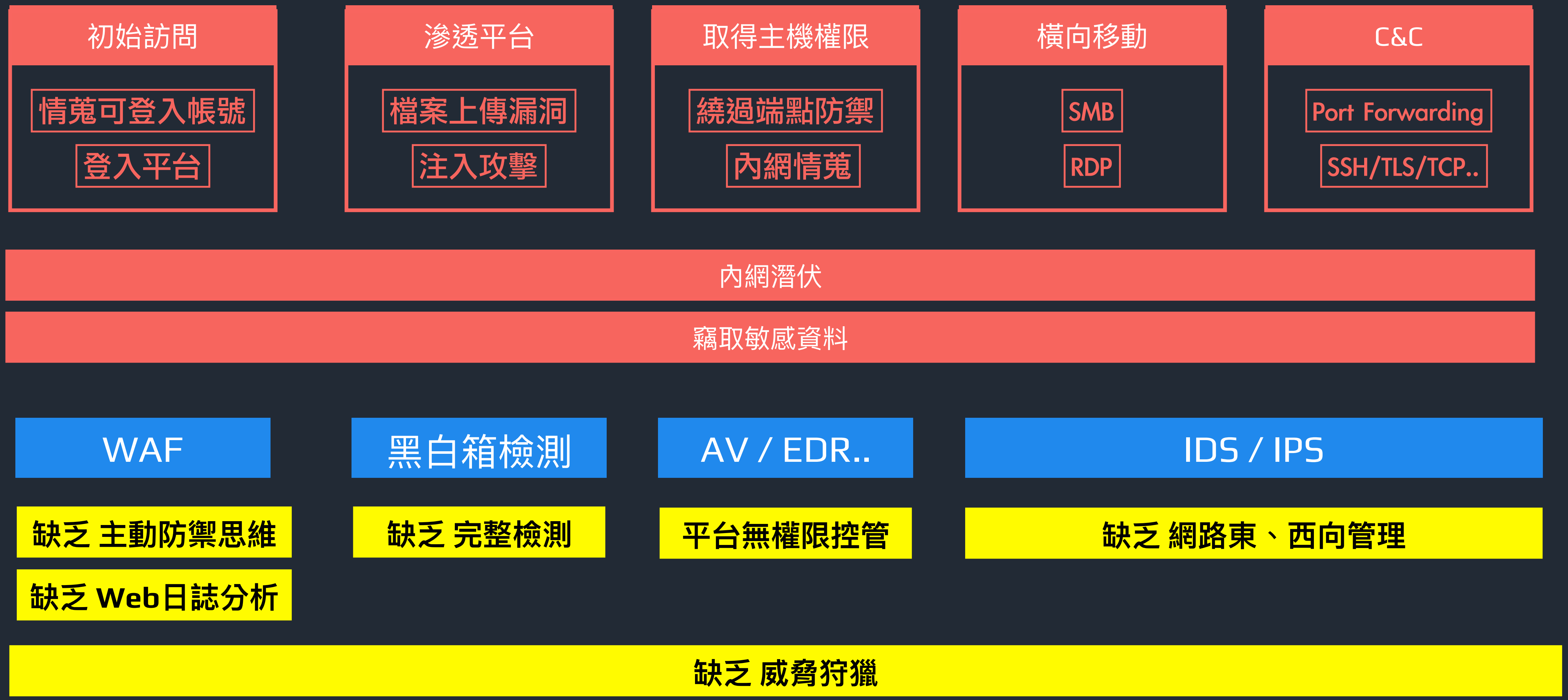
KPI

合規 × 稽核 ×
設備覆蓋率

最少動作
最大收益

可交付
可稽核

紅隊都是從縫尋找途徑



初始訪問

情蒐可登入帳號

登入平台

滲透平台

檔案上傳漏洞

注入攻擊

取得主機權限

繞過端點防禦

內網情蒐

橫向移動

SMB

RDP

C&C

Port Forwarding

SSH/TLS/TCP..

內網潛伏

竊取敏感資料

WAF

缺乏 主動防禦思維

缺乏 Web日誌分析

黑白箱檢測

缺乏 完整檢測

AV / EDR..

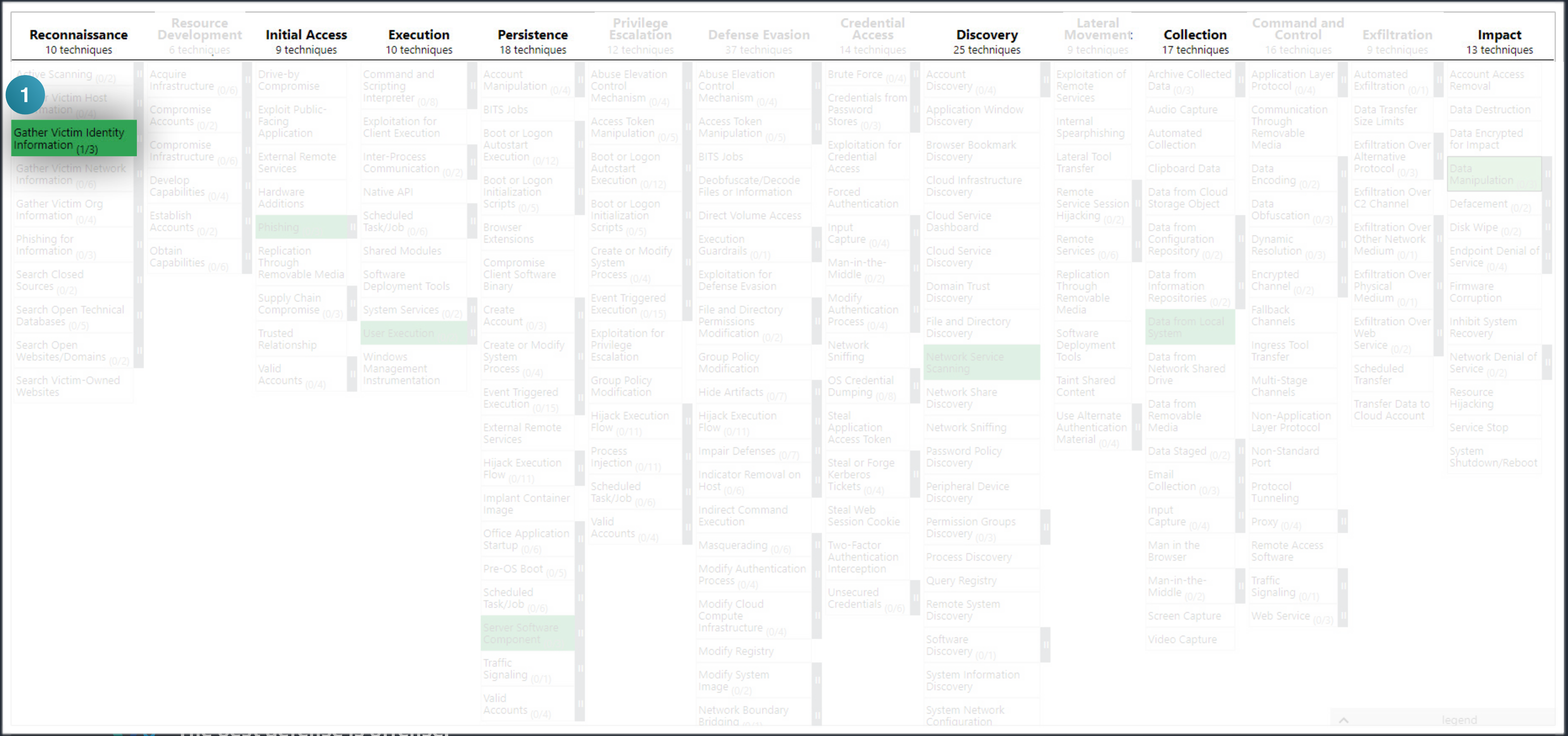
平台無權限控管

IDS / IPS

缺乏 網路東、西向管理

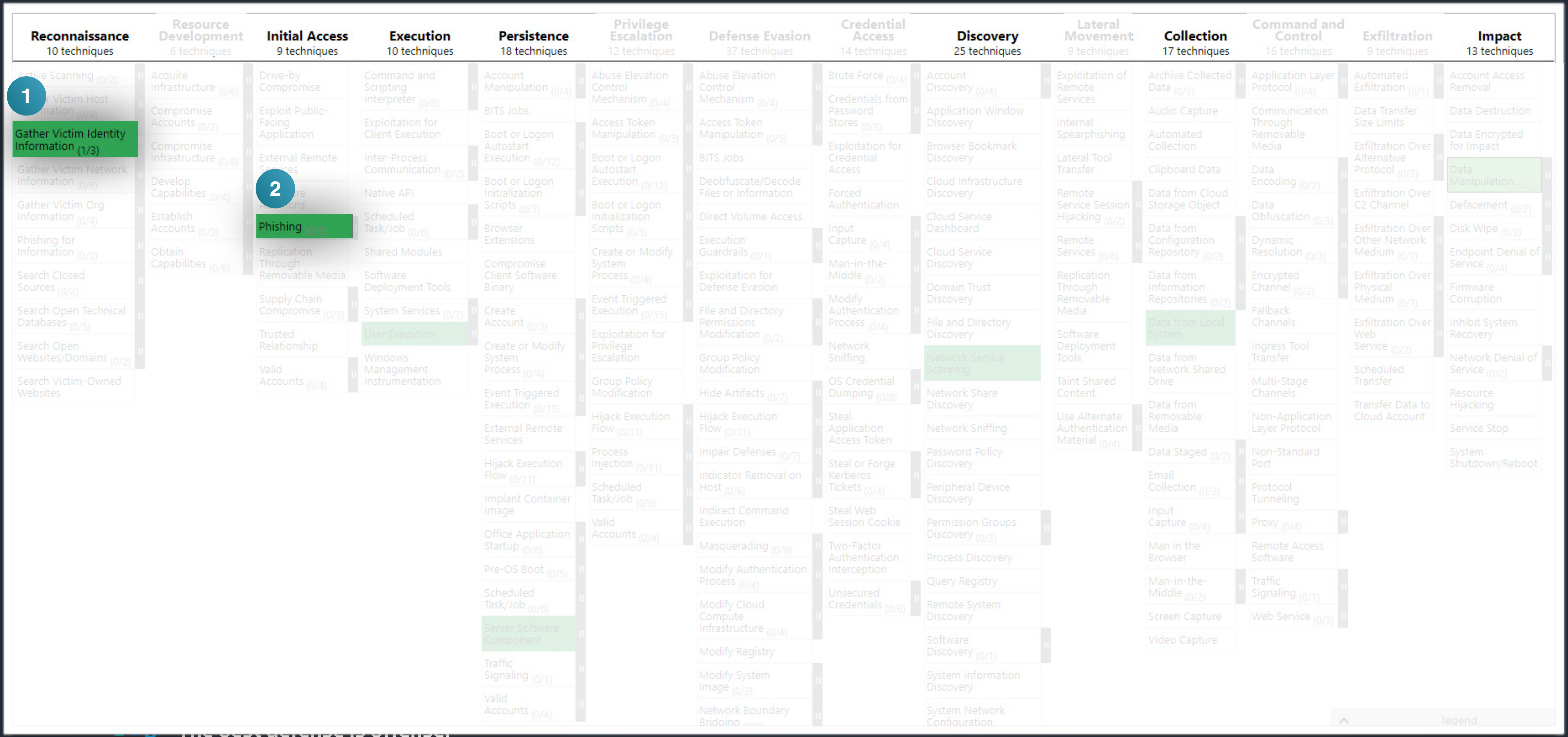
缺乏 威脅狩獵

金融資安事件 - MITRE ATT&CK



Reconnaissance 10 techniques	Resource Development 6 techniques	Initial Access 9 techniques	Execution 10 techniques	Persistence 18 techniques	Privilege Escalation 12 techniques	Defense Evasion 37 techniques	Credential Access 14 techniques	Discovery 25 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 16 techniques	Exfiltration 9 techniques	Impact 13 techniques
Active Scanning (0/2)	Acquire Infrastructure (0/6)	Drive-by Compromise	Command and Scripting Interpreter (0/8)	Account Manipulation (0/4)	Abuse Elevation Control Mechanism (0/4)	Abuse Elevation Control Mechanism (0/4)	Brute Force (0/4)	Account Discovery (0/4)	Exploitation of Remote Services	Archive Collected Data (0/3)	Application Layer Protocol (0/4)	Automated Exfiltration (0/1)	Account Access Removal
Gather Victim Host Information (0/4)	Compromise Accounts (0/2)	Exploit Public-Facing Application	Exploitation for Client Execution	BITS Jobs	Access Token Manipulation (0/5)	Access Token Manipulation (0/5)	Credentials from Password Stores (0/3)	Application Window Discovery	Internal Spearphishing	Audio Capture	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Gather Victim Identity Information (1/3)	Compromise Infrastructure (0/6)	External Remote Services	Inter-Process Communication (0/2)	Boot or Logon Autostart Execution (0/12)	Boot or Logon Autostart Execution (0/12)	BITS Jobs	Exploitation for Credential Access	Browser Bookmark Discovery	Lateral Tool Transfer	Automated Collection	Data Encoding (0/2)	Exfiltration Over Alternative Protocol (0/3)	Data Encrypted for Impact
Gather Victim Network Information (0/6)	Develop Capabilities (0/4)	Hardware Additions	Native API	Boot or Logon Initialization Scripts (0/5)	Boot or Logon Initialization Scripts (0/5)	Deobfuscate/Decode Files or Information	Forced Authentication	Cloud Infrastructure Discovery	Remote Service Session Hijacking (0/2)	Clipboard Data	Data Obfuscation (0/3)	Exfiltration Over C2 Channel	Data Manipulation (0/3)
Gather Victim Org Information (0/4)	Establish Accounts (0/2)	Phishing	Scheduled Task/Job (0/6)	Browser Extensions	Create or Modify System Process (0/4)	Direct Volume Access	Input Capture (0/4)	Cloud Service Dashboard	Remote Services (0/6)	Data from Cloud Storage Object	Dynamic Resolution (0/3)	Exfiltration Over Other Network Medium (0/1)	Defacement (0/2)
Phishing for Information (0/3)	Obtain Capabilities (0/6)	Replication Through Removable Media	Shared Modules	Compromise Client Software Binary	Event Triggered Execution (0/15)	Execution Guardrails (0/1)	Man-in-the-Middle (0/2)	Cloud Service Discovery	Replication Through Removable Media	Data from Configuration Repository (0/2)	Encrypted Channel (0/2)	Exfiltration Over Physical Medium (0/1)	Disk Wipe (0/2)
Search Closed Sources (0/2)		Supply Chain Compromise (0/3)	Software Deployment Tools	Create Account (0/3)	Exploitation for Privilege Escalation	Exploitation for Defense Evasion	Modify Authentication Process (0/4)	Domain Trust Discovery	Software Deployment Tools	Data from Information Repositories (0/2)	Fallback Channels	Exfiltration Over Web Service (0/2)	Endpoint Denial of Service (0/4)
Search Open Technical Databases (0/5)		Trusted Relationship	System Services (0/2)	Create or Modify System Process (0/4)	Group Policy Modification	File and Directory Permissions Modification (0/2)	Network Sniffing	File and Directory Discovery	Taint Shared Content	Data from Local System	Ingress Tool Transfer	Scheduled Transfer	Firmware Corruption
Search Open Websites/Domains (0/2)		Valid Accounts (0/4)	User Execution	Event Triggered Execution (0/15)	Hijack Execution Flow (0/11)	Group Policy Modification	OS Credential Dumping (0/8)	Network Service Scanning	Use Alternate Authentication Material (0/4)	Data from Network Shared Drive	Multi-Stage Channels	Transfer Data to Cloud Account	Inhibit System Recovery
Search Victim-Owned Websites			Windows Management Instrumentation	External Remote Services	Process Injection (0/11)	Hide Artifacts (0/7)	Steal Application Access Token	Network Share Discovery		Data from Removable Media	Non-Application Layer Protocol		Network Denial of Service (0/2)
				Hijack Execution Flow (0/11)	Scheduled Task/Job (0/6)	Hijack Execution Flow (0/11)	Steal or Forge Kerberos Tickets (0/4)	Network Sniffing		Data Staged (0/2)	Non-Standard Port		Resource Hijacking
				Implant Container Image	Valid Accounts (0/4)	Impair Defenses (0/7)	Steal Web Session Cookie	Password Policy Discovery		Email Collection (0/3)	Protocol Tunneling		Service Stop
				Office Application Startup (0/6)		Indicator Removal on Host (0/6)	Two-Factor Authentication Interception	Peripheral Device Discovery		Input Capture (0/4)	Proxy (0/4)		System Shutdown/Reboot
				Pre-OS Boot (0/5)		Indirect Command Execution	Unsecured Credentials (0/6)	Permission Groups Discovery (0/3)		Man in the Browser	Remote Access Software		
				Scheduled Task/Job (0/6)		Masquerading (0/6)		Process Discovery		Man-in-the-Middle (0/2)	Traffic Signaling (0/1)		
				Server Software Component		Modify Authentication Process (0/4)		Query Registry		Screen Capture	Web Service (0/3)		
				Traffic Signaling (0/1)		Modify Cloud Compute Infrastructure (0/4)		Remote System Discovery		Video Capture			
				Valid Accounts (0/4)		Modify Registry		Software Discovery (0/1)					
						Modify System Image (0/2)		System Information Discovery					
						Network Boundary Bridging		System Network Configuration					

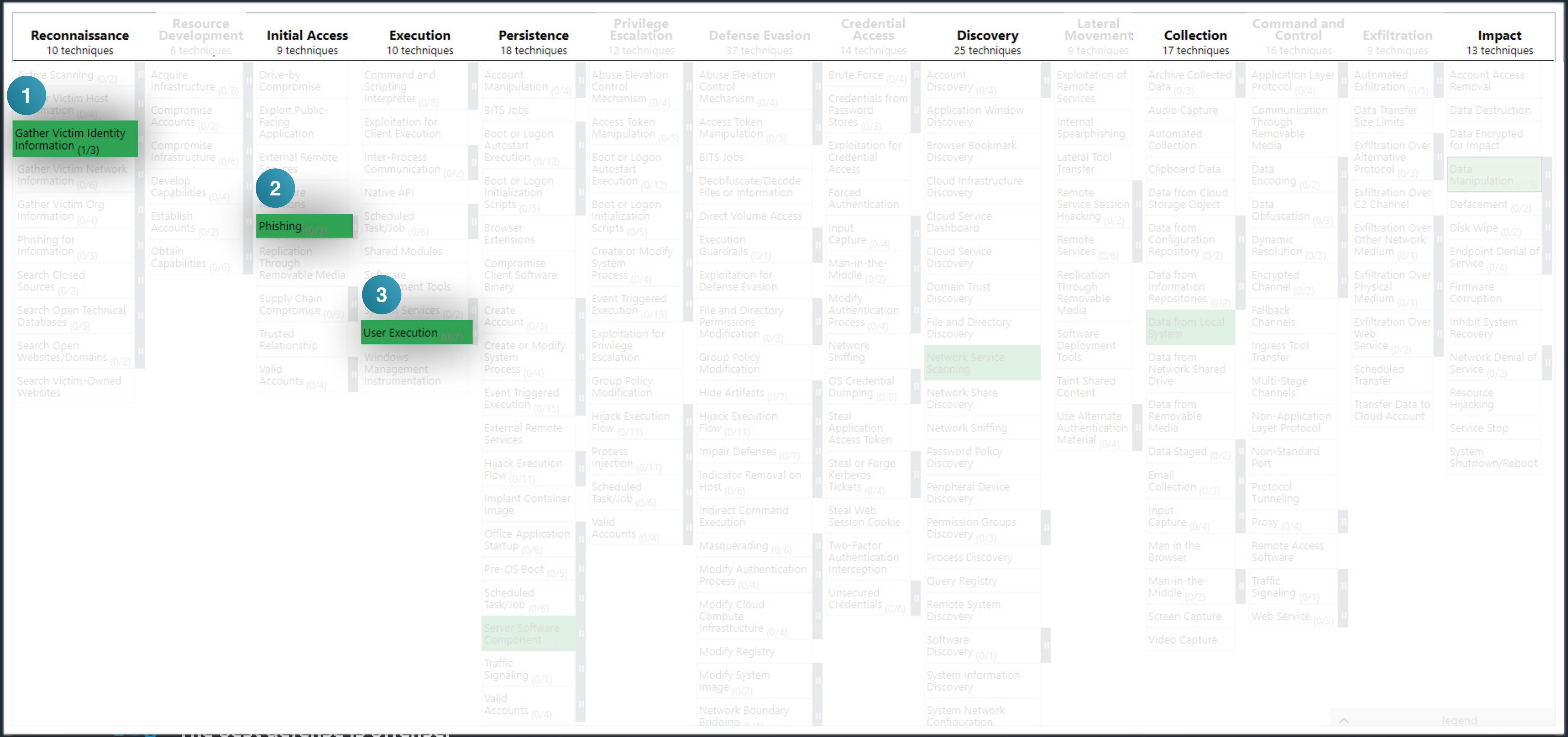
金融資安事件 - MITRE ATT&CK



Reconnaissance 10 techniques	Resource Development 6 techniques	Initial Access 9 techniques	Execution 10 techniques	Persistence 18 techniques	Privilege Escalation 12 techniques	Defense Evasion 37 techniques
Active Scanning (0/2)	Acquire Infrastructure (0/6)	Drive-by Compromise	Command and Scripting Interpreter (0/8)	Account Manipulation (0/4)	Abuse Elevation Control Mechanism (0/4)	Abuse Elevation Control Mechanism (0/4)
Gather Victim Host Information (0/4)	Compromise Accounts (0/2)	Exploit Public-Facing Application	Exploitation for Client Execution	BITS Jobs	Access Token Manipulation (0/5)	Access Token Manipulation (0/5)
Gather Victim Identity Information (1/3)	Compromise Infrastructure (0/6)	External Remote Services	Inter-Process Communication (0/2)	Boot or Logon Autostart Execution (0/12)	Boot or Logon Autostart Execution (0/12)	BITS Jobs
Gather Victim Network Information (0/6)	Develop Capabilities (0/4)	Hardware Additions	Native API	Boot or Logon Initialization Scripts (0/5)	Boot or Logon Initialization Scripts (0/5)	Deobfuscate/Decode Files or Information
Gather Victim Org Information (0/4)	Establish Accounts (0/2)	Phishing (0/3)	Scheduled Task/Job (0/6)	Browser Extensions	Create or Modify System Process (0/4)	Direct Volume Access
Phishing for Information (0/3)	Obtain Capabilities (0/6)	Replication Through Removable Media	Shared Modules	Compromise Client Software Binary	Event Triggered Execution (0/15)	Execution Guardrails (0/1)
Search Closed Sources (0/2)		Supply Chain Compromise (0/3)	Software Deployment Tools	Create Account (0/3)	Exploitation for Privilege Escalation	Exploitation for Defense Evasion
Search Open Technical Databases (0/5)		Trusted Relationship	System Services (0/2)	Create or Modify System Process (0/4)	Group Policy Modification	File and Directory Permissions Modification (0/2)
Search Open Websites/Domains (0/2)		Valid Accounts (0/4)	User Execution	Event Triggered Execution (0/15)	Hijack Execution Flow (0/11)	Group Policy Modification
Search Victim-Owned Websites			Windows Management Instrumentation	External Remote Services	Process Injection (0/11)	Hide Artifacts (0/7)
				Hijack Execution Flow (0/11)	Scheduled Task/Job (0/6)	Hijack Execution Flow (0/11)
				Implant Container Image	Valid Accounts (0/4)	Impair Defenses (0/7)
				Office Application Startup (0/6)		Indicator Removal on Host (0/6)
				Pre-OS Boot (0/5)		Indirect Command Execution
				Scheduled Task/Job (0/6)		Masquerading (0/6)
				Server Software Component		Modify Authentication Process (0/4)
				Traffic Signaling (0/1)		Modify Cloud Compute Infrastructure (0/4)
				Valid Accounts (0/4)		Modify Registry
						Modify System Image (0/2)
						Network Boundary Bridging (0/1)

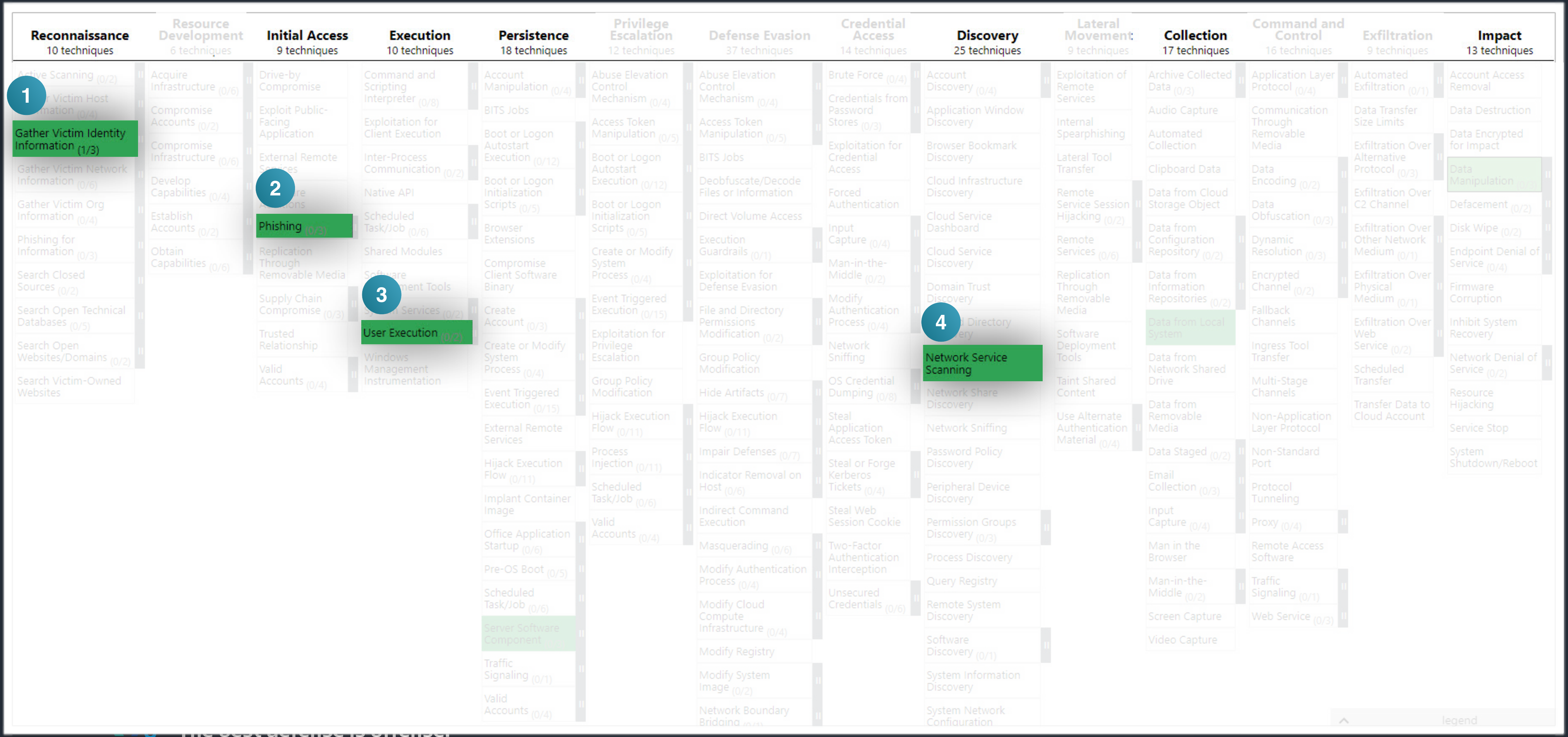
Credential Access 14 techniques	Discovery 25 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 16 techniques	Exfiltration 9 techniques	Impact 13 techniques
Brute Force (0/4)	Account Discovery (0/4)	Exploitation of Remote Services	Archive Collected Data (0/3)	Application Layer Protocol (0/4)	Automated Exfiltration (0/1)	Account Access Removal
Credentials from Password Stores (0/3)	Application Window Discovery	Internal Spearphishing	Audio Capture	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Exploitation for Credential Access	Browser Bookmark Discovery	Lateral Tool Transfer	Automated Collection	Data Encoding (0/2)	Exfiltration Over Alternative Protocol (0/3)	Data Encrypted for Impact
Forced Authentication	Cloud Infrastructure Discovery	Remote Service Session Hijacking (0/2)	Clipboard Data	Data Obfuscation (0/3)	Exfiltration Over C2 Channel	Data Manipulation (0/3)
Input Capture (0/4)	Cloud Service Dashboard	Remote Services (0/6)	Data from Cloud Storage Object	Dynamic Resolution (0/3)	Exfiltration Over Other Network Medium (0/1)	Defacement (0/2)
Man-in-the-Middle (0/2)	Cloud Service Discovery	Replication Through Removable Media	Data from Configuration Repository (0/2)	Encrypted Channel (0/2)	Exfiltration Over Physical Medium (0/1)	Disk Wipe (0/2)
Modify Authentication Process (0/4)	Domain Trust Discovery	Software Deployment Tools	Data from Information Repositories (0/2)	Fallback Channels	Exfiltration Over Web Service (0/2)	Endpoint Denial of Service (0/4)
Network Sniffing	File and Directory Discovery	Taint Shared Content	Data from Local System	Ingress Tool Transfer	Scheduled Transfer	Firmware Corruption
OS Credential Dumping (0/8)	Network Service Scanning	Use Alternate Authentication Material (0/4)	Data from Network Shared Drive	Multi-Stage Channels	Transfer Data to Cloud Account	Inhibit System Recovery
Steal Application Access Token	Network Share Discovery		Data from Removable Media	Non-Application Layer Protocol		Network Denial of Service (0/2)
Steal or Forge Kerberos Tickets (0/4)	Network Sniffing		Data Staged (0/2)	Non-Standard Port		Resource Hijacking
Steal Web Session Cookie	Password Policy Discovery		Email Collection (0/3)	Protocol Tunneling		Service Stop
Two-Factor Authentication Interception	Peripheral Device Discovery		Input Capture (0/4)	Proxy (0/4)		System Shutdown/Reboot
Unsecured Credentials (0/6)	Permission Groups Discovery (0/3)		Man in the Browser	Remote Access Software		
	Process Discovery		Man-in-the-Middle (0/2)	Traffic Signaling (0/1)		
	Query Registry		Screen Capture	Web Service (0/3)		
	Remote System Discovery		Video Capture			
	Software Discovery (0/1)					
	System Information Discovery					
	System Network Configuration					

金融資安事件 - MITRE ATT&CK



Reconnaissance 10 techniques	Resource Development 6 techniques	Initial Access 9 techniques	Execution 10 techniques	Persistence 18 techniques	Privilege Escalation 12 techniques	Defense Evasion 37 techniques	Credential Access 14 techniques	Discovery 25 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 16 techniques	Exfiltration 9 techniques	Impact 13 techniques
Active Scanning (0/2)	Acquire Infrastructure (0/6)	Drive-by Compromise	Command and Scripting Interpreter (0/8)	Account Manipulation (0/4)	Abuse Elevation Control Mechanism (0/4)	Abuse Elevation Control Mechanism (0/4)	Brute Force (0/4)	Account Discovery (0/4)	Exploitation of Remote Services	Archive Collected Data (0/3)	Application Layer Protocol (0/4)	Automated Exfiltration (0/1)	Account Access Removal
Gather Victim Host Information (0/4)	Compromise Accounts (0/2)	Exploit Public-Facing Application	Exploitation for Client Execution	BITS Jobs	Access Token Manipulation (0/5)	Access Token Manipulation (0/5)	Credentials from Password Stores (0/3)	Application Window Discovery	Internal Spearphishing	Audio Capture	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Gather Victim Identity Information (1/3)	Compromise Infrastructure (0/6)	External Remote Services	Inter-Process Communication (0/2)	Boot or Logon Autostart Execution (0/12)	Boot or Logon Autostart Execution (0/12)	BITS Jobs	Exploitation for Credential Access	Browser Bookmark Discovery	Lateral Tool Transfer	Automated Collection	Data Encoding (0/2)	Exfiltration Over Alternative Protocol (0/3)	Data Encrypted for Impact
Gather Victim Network Information (0/6)	Develop Capabilities (0/4)	Hardware Additions	Native API	Boot or Logon Initialization Scripts (0/5)	Boot or Logon Initialization Scripts (0/5)	Deobfuscate/Decode Files or Information	Forced Authentication	Cloud Infrastructure Discovery	Remote Service Session Hijacking (0/2)	Clipboard Data	Data Obfuscation (0/3)	Exfiltration Over C2 Channel	Data Manipulation (0/3)
Gather Victim Org Information (0/4)	Establish Accounts (0/2)	Phishing (0/3)	Scheduled Task/Job (0/6)	Browser Extensions	Create or Modify System Process (0/4)	Direct Volume Access	Input Capture (0/4)	Cloud Service Dashboard	Remote Services (0/6)	Data from Cloud Storage Object	Dynamic Resolution (0/3)	Exfiltration Over Other Network Medium (0/1)	Defacement (0/2)
Phishing for Information (0/3)	Obtain Capabilities (0/6)	Replication Through Removable Media	Shared Modules	Compromise Client Software Binary	Event Triggered Execution (0/15)	Execution Guardrails (0/1)	Man-in-the-Middle (0/2)	Cloud Service Discovery	Replication Through Removable Media	Data from Configuration Repository (0/2)	Encrypted Channel (0/2)	Exfiltration Over Physical Medium (0/1)	Disk Wipe (0/2)
Search Closed Sources (0/2)		Supply Chain Compromise (0/3)	Software Deployment Tools	Create Account (0/3)	Exploitation for Privilege Escalation	Exploitation for Defense Evasion	Modify Authentication Process (0/4)	Domain Trust Discovery	Software Deployment Tools	Data from Information Repositories (0/2)	Fallback Channels	Exfiltration Over Web Service (0/2)	Endpoint Denial of Service (0/4)
Search Open Technical Databases (0/5)		Trusted Relationship	System Services (0/2)	Create or Modify System Process (0/4)	Group Policy Modification	File and Directory Permissions Modification (0/2)	Network Sniffing	File and Directory Discovery	Taint Shared Content	Data from Local System	Ingress Tool Transfer	Scheduled Transfer	Firmware Corruption
Search Open Websites/Domains (0/2)		Valid Accounts (0/4)	User Execution (0/2)	Event Triggered Execution (0/15)	Hijack Execution Flow (0/11)	Group Policy Modification	OS Credential Dumping (0/8)	Network Service Scanning	Use Alternate Authentication Material (0/4)	Data from Network Shared Drive	Multi-Stage Channels	Transfer Data to Cloud Account	Inhibit System Recovery
Search Victim-Owned Websites			Windows Management Instrumentation	External Remote Services	Process Injection (0/11)	Hide Artifacts (0/7)	Steal Application Access Token	Network Share Discovery		Data from Removable Media	Non-Application Layer Protocol		Network Denial of Service (0/2)
				Hijack Execution Flow (0/11)	Scheduled Task/Job (0/6)	Hijack Execution Flow (0/11)	Steal or Forge Kerberos Tickets (0/4)	Network Sniffing		Data Staged (0/2)	Non-Standard Port		Resource Hijacking
				Implant Container Image	Valid Accounts (0/4)	Impair Defenses (0/7)	Steal Web Session Cookie	Password Policy Discovery		Email Collection (0/3)	Protocol Tunneling		Service Stop
				Office Application Startup (0/6)		Indicator Removal on Host (0/6)	Two-Factor Authentication Interception	Peripheral Device Discovery		Input Capture (0/4)	Proxy (0/4)		System Shutdown/Reboot
				Pre-OS Boot (0/5)		Indirect Command Execution	Unsecured Credentials (0/6)	Permission Groups Discovery (0/3)		Man in the Browser	Remote Access Software		
				Scheduled Task/Job (0/6)		Masquerading (0/6)		Process Discovery		Man-in-the-Middle (0/2)	Traffic Signaling (0/1)		
				Server Software Component (0/3)		Modify Authentication Process (0/4)		Query Registry		Screen Capture	Web Service (0/3)		
				Traffic Signaling (0/1)		Modify Cloud Compute Infrastructure (0/4)		Remote System Discovery		Video Capture			
				Valid Accounts (0/4)		Modify Registry		Software Discovery (0/1)					
						Modify System Image (0/2)		System Information Discovery					
						Network Boundary Bridging (0/1)		System Network Configuration					

金融資安事件 - MITRE ATT&CK



Reconnaissance 10 techniques
- Active Scanning (0/2)
- Gather Victim Host Information (0/4)
- Gather Victim Identity Information (1/3)
- Gather Victim Network Information (0/6)
- Gather Victim Org Information (0/4)
- Phishing for Information (0/3)
- Search Closed Sources (0/2)
- Search Open Technical Databases (0/5)
- Search Open Websites/Domains (0/2)
- Search Victim-Owned Websites

Resource Development 6 techniques
- Acquire Infrastructure (0/6)
- Compromise Accounts (0/2)
- Compromise Infrastructure (0/6)
- Develop Capabilities (0/4)
- Establish Accounts (0/2)
- Obtain Capabilities (0/6)

Initial Access 9 techniques
- Drive-by Compromise
- Exploit Public-Facing Application
- External Remote Services
- Hardware Additions
- Phishing (0/3)
- Replication Through Removable Media
- Supply Chain Compromise (0/3)
- Trusted Relationship
- Valid Accounts (0/4)

Execution 10 techniques
- Command and Scripting Interpreter (0/8)
- Exploitation for Client Execution
- Inter-Process Communication (0/2)
- Native API
- Scheduled Task/Job (0/6)
- Shared Modules
- Software Deployment Tools
- System Services (0/2)
- User Execution (0/2)
- Windows Management Instrumentation

Persistence 18 techniques
- Account Manipulation (0/4)
- BITS Jobs
- Boot or Logon Autostart Execution (0/12)
- Boot or Logon Initialization Scripts (0/5)
- Browser Extensions
- Compromise Client Software Binary
- Create Account (0/3)
- Create or Modify System Process (0/4)
- Event Triggered Execution (0/15)
- External Remote Services
- Hijack Execution Flow (0/11)
- Implant Container Image
- Office Application Startup (0/6)
- Pre-OS Boot (0/5)
- Scheduled Task/Job (0/6)
- Server Software Component
- Traffic Signaling (0/1)
- Valid Accounts (0/4)

Privilege Escalation 12 techniques
- Abuse Elevation Control Mechanism (0/4)
- Access Token Manipulation (0/5)
- Boot or Logon Autostart Execution (0/12)
- Boot or Logon Initialization Scripts (0/5)
- Create or Modify System Process (0/4)
- Event Triggered Execution (0/15)
- Exploitation for Privilege Escalation
- Group Policy Modification
- Hijack Execution Flow (0/11)
- Process Injection (0/11)
- Scheduled Task/Job (0/6)
- Valid Accounts (0/4)

Defense Evasion 37 techniques
- Abuse Elevation Control Mechanism (0/4)
- Access Token Manipulation (0/5)
- BITS Jobs
- Deobfuscate/Decode Files or Information
- Direct Volume Access
- Execution Guardrails (0/1)
- Exploitation for Defense Evasion
- File and Directory Permissions Modification (0/2)
- Group Policy Modification
- Hide Artifacts (0/7)
- Hijack Execution Flow (0/11)
- Impair Defenses (0/7)
- Indicator Removal on Host (0/6)
- Indirect Command Execution
- Masquerading (0/6)
- Modify Authentication Process (0/4)
- Modify Cloud Compute Infrastructure (0/4)
- Modify Registry
- Modify System Image (0/2)
- Network Boundary Bridging (0/1)

Credential Access 14 techniques
- Brute Force (0/4)
- Credentials from Password Stores (0/3)
- Exploitation for Credential Access
- Forced Authentication
- Input Capture (0/4)
- Man-in-the-Middle (0/2)
- Modify Authentication Process (0/4)
- Network Sniffing
- OS Credential Dumping (0/8)
- Steal Application Access Token
- Steal or Forge Kerberos Tickets (0/4)
- Steal Web Session Cookie
- Two-Factor Authentication Interception
- Unsecured Credentials (0/6)

Discovery 25 techniques
- Account Discovery (0/4)
- Application Window Discovery
- Browser Bookmark Discovery
- Cloud Infrastructure Discovery
- Cloud Service Dashboard
- Cloud Service Discovery
- Domain Trust Discovery
- File and Directory Discovery
- Network Service Scanning
- Network Share Discovery
- Network Sniffing
- Password Policy Discovery
- Peripheral Device Discovery
- Permission Groups Discovery (0/3)
- Process Discovery
- Query Registry
- Remote System Discovery
- Software Discovery (0/1)
- System Information Discovery
- System Network Configuration

Lateral Movement 9 techniques
- Exploitation of Remote Services
- Internal Spearphishing
- Lateral Tool Transfer
- Remote Service Session Hijacking (0/2)
- Remote Services (0/6)
- Replication Through Removable Media
- Software Deployment Tools
- Taint Shared Content
- Use Alternate Authentication Material (0/4)

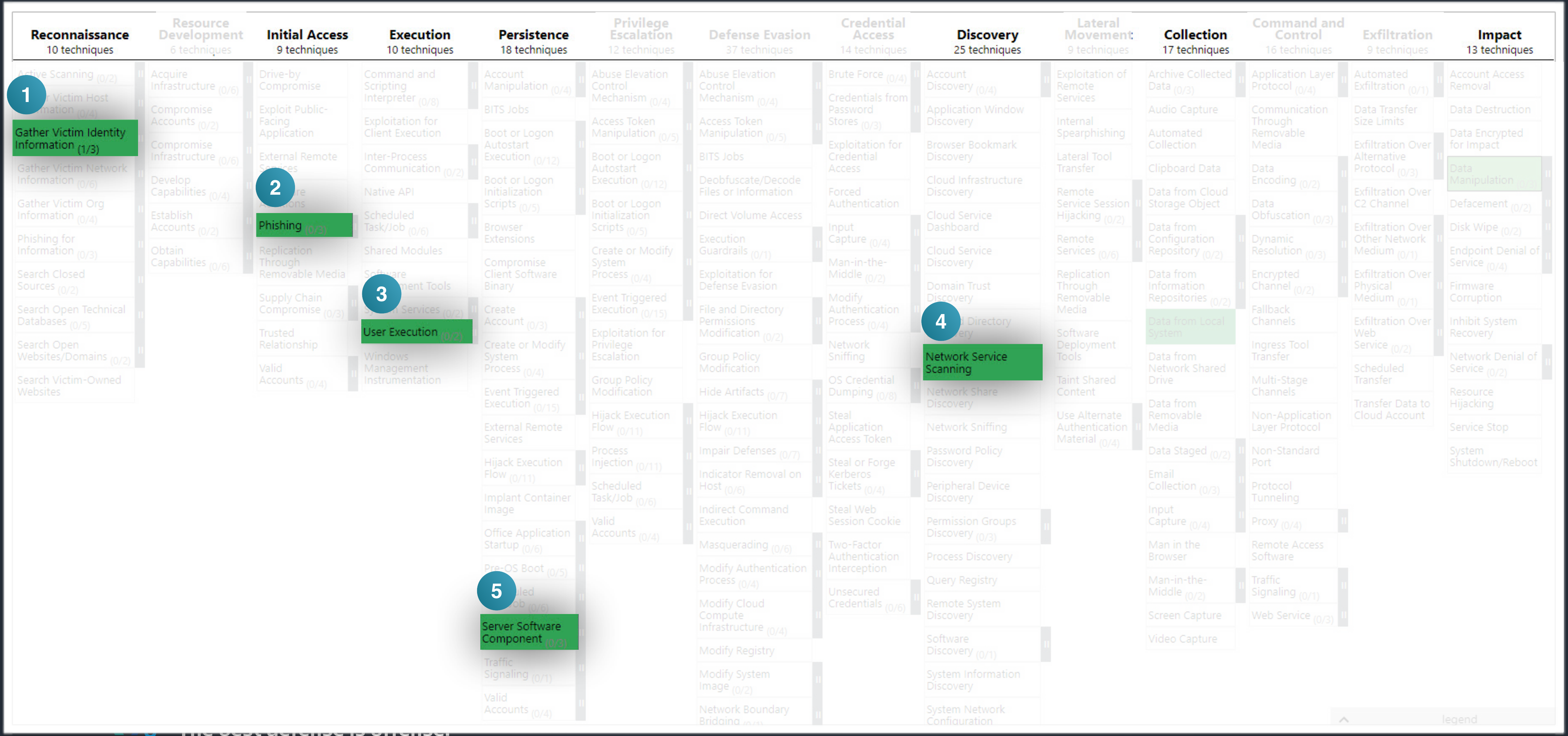
Collection 17 techniques
- Archive Collected Data (0/3)
- Audio Capture
- Automated Collection
- Clipboard Data
- Data from Cloud Storage Object
- Data from Configuration Repository (0/2)
- Data from Information Repositories (0/2)
- Data from Local System
- Data from Network Shared Drive
- Data from Removable Media
- Data Staged (0/2)
- Email Collection (0/3)
- Input Capture (0/4)
- Man in the Browser
- Man-in-the-Middle (0/2)
- Screen Capture
- Video Capture

Command and Control 16 techniques
- Application Layer Protocol (0/4)
- Communication Through Removable Media
- Data Encoding (0/2)
- Data Obfuscation (0/3)
- Dynamic Resolution (0/3)
- Encrypted Channel (0/2)
- Fallback Channels
- Ingress Tool Transfer
- Multi-Stage Channels
- Non-Application Layer Protocol
- Non-Standard Port
- Protocol Tunneling
- Proxy (0/4)
- Remote Access Software
- Traffic Signaling (0/1)
- Web Service (0/3)

Exfiltration 9 techniques
- Automated Exfiltration (0/1)
- Data Transfer Size Limits
- Exfiltration Over Alternative Protocol (0/3)
- Exfiltration Over C2 Channel
- Exfiltration Over Other Network Medium (0/1)
- Exfiltration Over Physical Medium (0/1)
- Exfiltration Over Web Service (0/2)
- Scheduled Transfer
- Transfer Data to Cloud Account

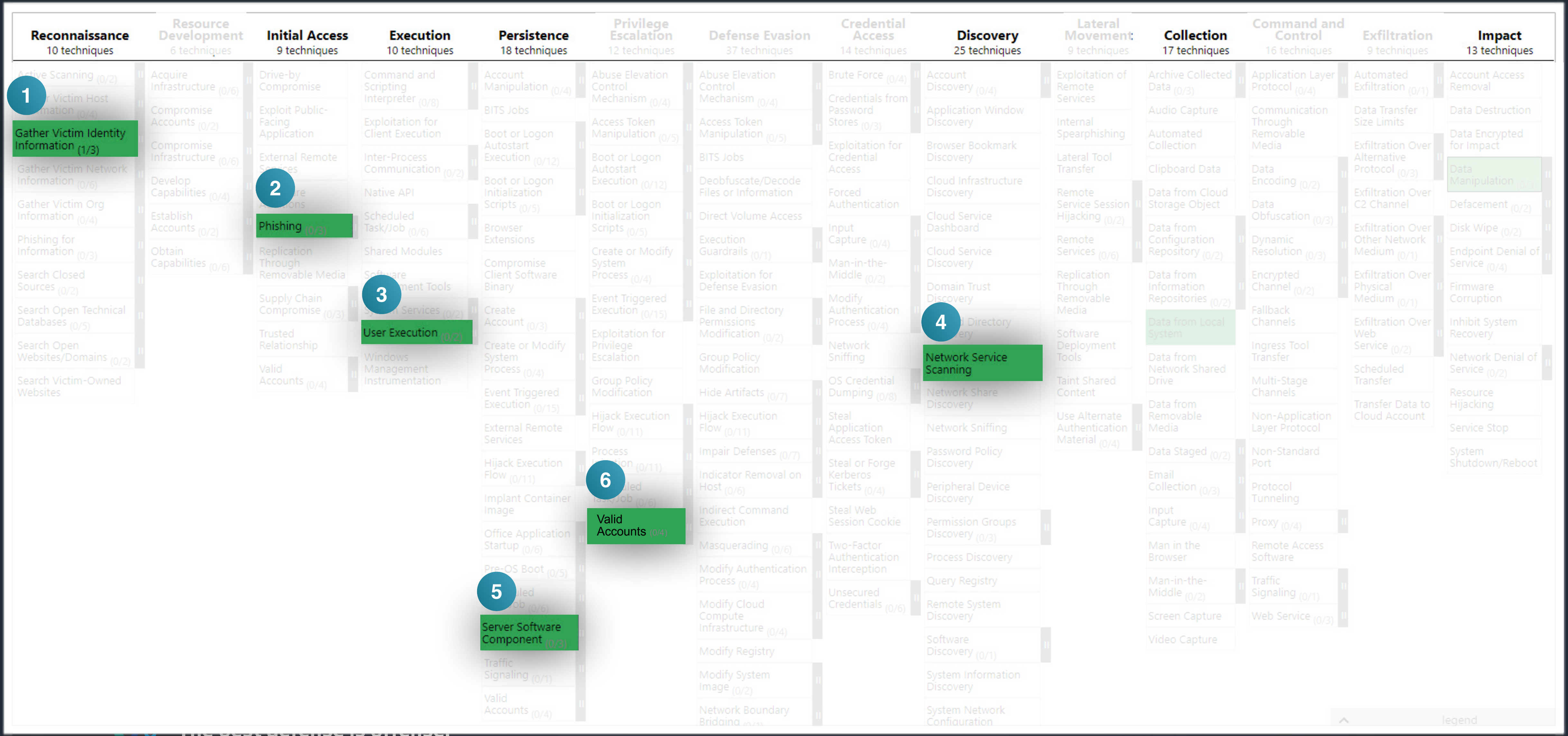
Impact 13 techniques
- Account Access Removal
- Data Destruction
- Data Encrypted for Impact
- Data Manipulation (0/3)
- Defacement (0/2)
- Disk Wipe (0/2)
- Endpoint Denial of Service (0/4)
- Firmware Corruption
- Inhibit System Recovery
- Network Denial of Service (0/2)
- Resource Hijacking
- Service Stop
- System Shutdown/Reboot

金融資安事件 - MITRE ATT&CK



Reconnaissance 10 techniques	Resource Development 6 techniques	Initial Access 9 techniques	Execution 10 techniques	Persistence 18 techniques	Privilege Escalation 12 techniques	Defense Evasion 37 techniques	Credential Access 14 techniques	Discovery 25 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 16 techniques	Exfiltration 9 techniques	Impact 13 techniques
Active Scanning (0/2)	Acquire Infrastructure (0/6)	Drive-by Compromise	Command and Scripting Interpreter (0/8)	Account Manipulation (0/4)	Abuse Elevation Control Mechanism (0/4)	Abuse Elevation Control Mechanism (0/4)	Brute Force (0/4)	Account Discovery (0/4)	Exploitation of Remote Services	Archive Collected Data (0/3)	Application Layer Protocol (0/4)	Automated Exfiltration (0/1)	Account Access Removal
Gather Victim Host Information (0/4)	Compromise Accounts (0/2)	Exploit Public-Facing Application	Exploitation for Client Execution	BITS Jobs	Access Token Manipulation (0/5)	Access Token Manipulation (0/5)	Credentials from Password Stores (0/3)	Application Window Discovery	Internal Spearphishing	Audio Capture	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Gather Victim Identity Information (1/3)	Compromise Infrastructure (0/6)	External Remote Services	Inter-Process Communication (0/2)	Boot or Logon Autostart Execution (0/12)	Boot or Logon Autostart Execution (0/12)	BITS Jobs	Exploitation for Credential Access	Browser Bookmark Discovery	Lateral Tool Transfer	Automated Collection	Data Encoding (0/2)	Exfiltration Over Alternative Protocol (0/3)	Data Encrypted for Impact
Gather Victim Network Information (0/6)	Develop Capabilities (0/4)	Hardware Additions	Native API	Boot or Logon Initialization Scripts (0/5)	Boot or Logon Initialization Scripts (0/5)	Deobfuscate/Decode Files or Information	Forced Authentication	Cloud Infrastructure Discovery	Remote Service Session Hijacking (0/2)	Clipboard Data	Data Obfuscation (0/3)	Exfiltration Over C2 Channel	Data Manipulation (0/3)
Gather Victim Org Information (0/4)	Establish Accounts (0/2)	Phishing (0/3)	Scheduled Task/Job (0/6)	Browser Extensions	Create or Modify System Process (0/4)	Direct Volume Access	Input Capture (0/4)	Cloud Service Dashboard	Remote Services (0/6)	Data from Cloud Storage Object	Dynamic Resolution (0/3)	Exfiltration Over Other Network Medium (0/1)	Defacement (0/2)
Phishing for Information (0/3)	Obtain Capabilities (0/6)	Replication Through Removable Media	Shared Modules	Compromise Client Software Binary	Event Triggered Execution (0/15)	Execution Guardrails (0/1)	Man-in-the-Middle (0/2)	Cloud Service Discovery	Replication Through Removable Media	Data from Configuration Repository (0/2)	Encrypted Channel (0/2)	Exfiltration Over Physical Medium (0/1)	Disk Wipe (0/2)
Search Closed Sources (0/2)		Supply Chain Compromise (0/3)	Software Deployment Tools	Create Account (0/3)	Exploitation for Privilege Escalation	Exploitation for Defense Evasion	Modify Authentication Process (0/4)	Domain Trust Discovery	Software Deployment Tools	Data from Information Repositories (0/2)	Fallback Channels	Exfiltration Over Web Service (0/2)	Endpoint Denial of Service (0/4)
Search Open Technical Databases (0/5)		Trusted Relationship	System Services (0/2)	Create or Modify System Process (0/4)	Group Policy Modification	File and Directory Permissions Modification (0/2)	Network Sniffing	File and Directory Discovery	Taint Shared Content	Data from Local System	Ingress Tool Transfer	Scheduled Transfer	Firmware Corruption
Search Open Websites/Domains (0/2)		Valid Accounts (0/4)	User Execution (0/2)	Event Triggered Execution (0/15)	Hijack Execution Flow (0/11)	Group Policy Modification	OS Credential Dumping (0/8)	Network Service Scanning	Use Alternate Authentication Material (0/4)	Data from Network Shared Drive	Multi-Stage Channels	Transfer Data to Cloud Account	Inhibit System Recovery
Search Victim-Owned Websites			Windows Management Instrumentation	External Remote Services	Process Injection (0/11)	Hide Artifacts (0/7)	Steal Application Access Token	Network Share Discovery		Data from Removable Media	Non-Application Layer Protocol		Network Denial of Service (0/2)
				Hijack Execution Flow (0/11)	Scheduled Task/Job (0/6)	Hijack Execution Flow (0/11)	Steal or Forge Kerberos Tickets (0/4)	Network Sniffing		Data Staged (0/2)	Non-Standard Port		Resource Hijacking
				Implant Container Image	Valid Accounts (0/4)	Impair Defenses (0/7)	Steal Web Session Cookie	Password Policy Discovery		Email Collection (0/3)	Protocol Tunneling		Service Stop
				Office Application Startup (0/6)		Indicator Removal on Host (0/6)	Two-Factor Authentication Interception	Peripheral Device Discovery		Input Capture (0/4)	Proxy (0/4)		System Shutdown/Reboot
				Pre-OS Boot (0/5)		Indirect Command Execution	Unsecured Credentials (0/6)	Permission Groups Discovery (0/3)		Man in the Browser	Remote Access Software		
				Scheduled Task/Job (0/6)		Masquerading (0/6)		Process Discovery		Man-in-the-Middle (0/2)	Traffic Signaling (0/1)		
				Server Software Component (0/3)		Modify Authentication Process (0/4)		Query Registry		Screen Capture	Web Service (0/3)		
				Traffic Signaling (0/1)		Modify Cloud Compute Infrastructure (0/4)		Remote System Discovery		Video Capture			
				Valid Accounts (0/4)		Modify Registry		Software Discovery (0/1)					
						Modify System Image (0/2)		System Information Discovery					
						Network Boundary Bridging (0/1)		System Network Configuration					

金融資安事件 - MITRE ATT&CK



Reconnaissance 10 techniques
- Active Scanning (0/2)
- Gather Victim Host Information (0/4)
- Gather Victim Identity Information (1/3)
- Gather Victim Network Information (0/6)
- Gather Victim Org Information (0/4)
- Phishing for Information (0/3)
- Search Closed Sources (0/2)
- Search Open Technical Databases (0/5)
- Search Open Websites/Domains (0/2)
- Search Victim-Owned Websites

Resource Development 6 techniques
- Acquire Infrastructure (0/6)
- Compromise Accounts (0/2)
- Compromise Infrastructure (0/6)
- Develop Capabilities (0/4)
- Establish Accounts (0/2)
- Obtain Capabilities (0/6)

Initial Access 9 techniques
- Drive-by Compromise
- Exploit Public-Facing Application
- External Remote Services
- Hardware Additions
- Phishing (0/3)
- Replication Through Removable Media
- Supply Chain Compromise (0/3)
- Trusted Relationship
- Valid Accounts (0/4)

Execution 10 techniques
- Command and Scripting Interpreter (0/8)
- Exploitation for Client Execution
- Inter-Process Communication (0/2)
- Native API
- Scheduled Task/Job (0/6)
- Shared Modules
- Software Deployment Tools
- System Services (0/2)
- User Execution (0/2)
- Windows Management Instrumentation

Persistence 18 techniques
- Account Manipulation (0/4)
- BITS Jobs
- Boot or Logon Autostart Execution (0/12)
- Boot or Logon Initialization Scripts (0/5)
- Browser Extensions
- Compromise Client Software Binary
- Create Account (0/3)
- Create or Modify System Process (0/4)
- Event Triggered Execution (0/15)
- External Remote Services
- Hijack Execution Flow (0/11)
- Implant Container Image
- Office Application Startup (0/6)
- Pre-OS Boot (0/5)
- Scheduled Task/Job (0/6)
- Server Software Component (0/3)
- Traffic Signaling (0/1)
- Valid Accounts (0/4)

Privilege Escalation 12 techniques
- Abuse Elevation Control Mechanism (0/4)
- Access Token Manipulation (0/5)
- Boot or Logon Autostart Execution (0/12)
- Boot or Logon Initialization Scripts (0/5)
- Create or Modify System Process (0/4)
- Event Triggered Execution (0/15)
- Exploitation for Privilege Escalation
- Group Policy Modification
- Hijack Execution Flow (0/11)
- Process Injection (0/11)
- Scheduled Task/Job (0/6)
- Valid Accounts (0/4)

Defense Evasion 37 techniques
- Abuse Elevation Control Mechanism (0/4)
- Access Token Manipulation (0/5)
- BITS Jobs
- Deobfuscate/Decode Files or Information
- Direct Volume Access
- Execution Guardrails (0/1)
- Exploitation for Defense Evasion
- File and Directory Permissions Modification (0/2)
- Group Policy Modification
- Hide Artifacts (0/7)
- Hijack Execution Flow (0/11)
- Impair Defenses (0/7)
- Indicator Removal on Host (0/6)
- Indirect Command Execution
- Masquerading (0/6)
- Modify Authentication Process (0/4)
- Modify Cloud Compute Infrastructure (0/4)
- Modify Registry
- Modify System Image (0/2)
- Network Boundary Bridging

Credential Access 14 techniques
- Brute Force (0/4)
- Credentials from Password Stores (0/3)
- Exploitation for Credential Access
- Forced Authentication
- Input Capture (0/4)
- Man-in-the-Middle (0/2)
- Modify Authentication Process (0/4)
- Network Sniffing
- OS Credential Dumping (0/8)
- Steal Application Access Token
- Steal or Forge Kerberos Tickets (0/4)
- Steal Web Session Cookie
- Two-Factor Authentication Interception
- Unsecured Credentials (0/6)

Discovery 25 techniques
- Account Discovery (0/4)
- Application Window Discovery
- Browser Bookmark Discovery
- Cloud Infrastructure Discovery
- Cloud Service Dashboard
- Cloud Service Discovery
- Domain Trust Discovery
- File and Directory Discovery
- Network Service Scanning
- Network Share Discovery
- Network Sniffing
- Password Policy Discovery
- Peripheral Device Discovery
- Permission Groups Discovery (0/3)
- Process Discovery
- Query Registry
- Remote System Discovery
- Software Discovery (0/1)
- System Information Discovery
- System Network Configuration

Lateral Movement 9 techniques
- Exploitation of Remote Services
- Internal Spearphishing
- Lateral Tool Transfer
- Remote Service Session Hijacking (0/2)
- Remote Services (0/6)
- Replication Through Removable Media
- Software Deployment Tools
- Taint Shared Content
- Use Alternate Authentication Material (0/4)

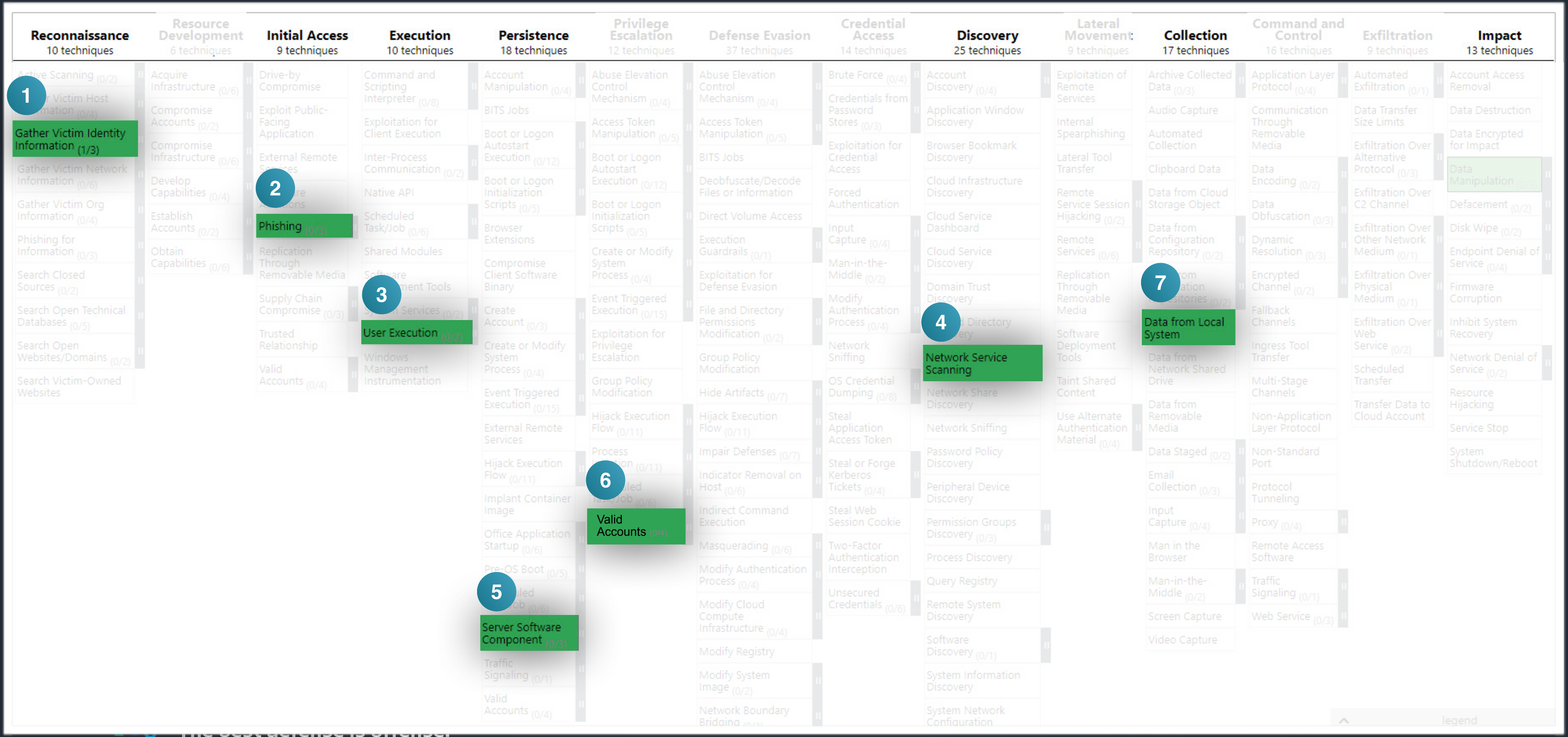
Collection 17 techniques
- Archive Collected Data (0/3)
- Audio Capture
- Automated Collection
- Clipboard Data
- Data from Cloud Storage Object
- Data from Configuration Repository (0/2)
- Data from Information Repositories (0/2)
- Data from Local System
- Data from Network Shared Drive
- Data from Removable Media
- Data Staged (0/2)
- Email Collection (0/3)
- Input Capture (0/4)
- Man in the Browser
- Man-in-the-Middle (0/2)
- Screen Capture
- Video Capture

Command and Control 16 techniques
- Application Layer Protocol (0/4)
- Communication Through Removable Media
- Data Encoding (0/2)
- Data Obfuscation (0/3)
- Dynamic Resolution (0/3)
- Encrypted Channel (0/2)
- Fallback Channels
- Ingress Tool Transfer
- Multi-Stage Channels
- Non-Application Layer Protocol
- Non-Standard Port
- Protocol Tunneling
- Proxy (0/4)
- Remote Access Software
- Traffic Signaling (0/1)
- Web Service (0/3)

Exfiltration 9 techniques
- Automated Exfiltration (0/1)
- Data Transfer Size Limits
- Exfiltration Over Alternative Protocol (0/3)
- Exfiltration Over C2 Channel
- Exfiltration Over Other Network Medium (0/1)
- Exfiltration Over Physical Medium (0/1)
- Exfiltration Over Web Service (0/2)
- Scheduled Transfer
- Transfer Data to Cloud Account

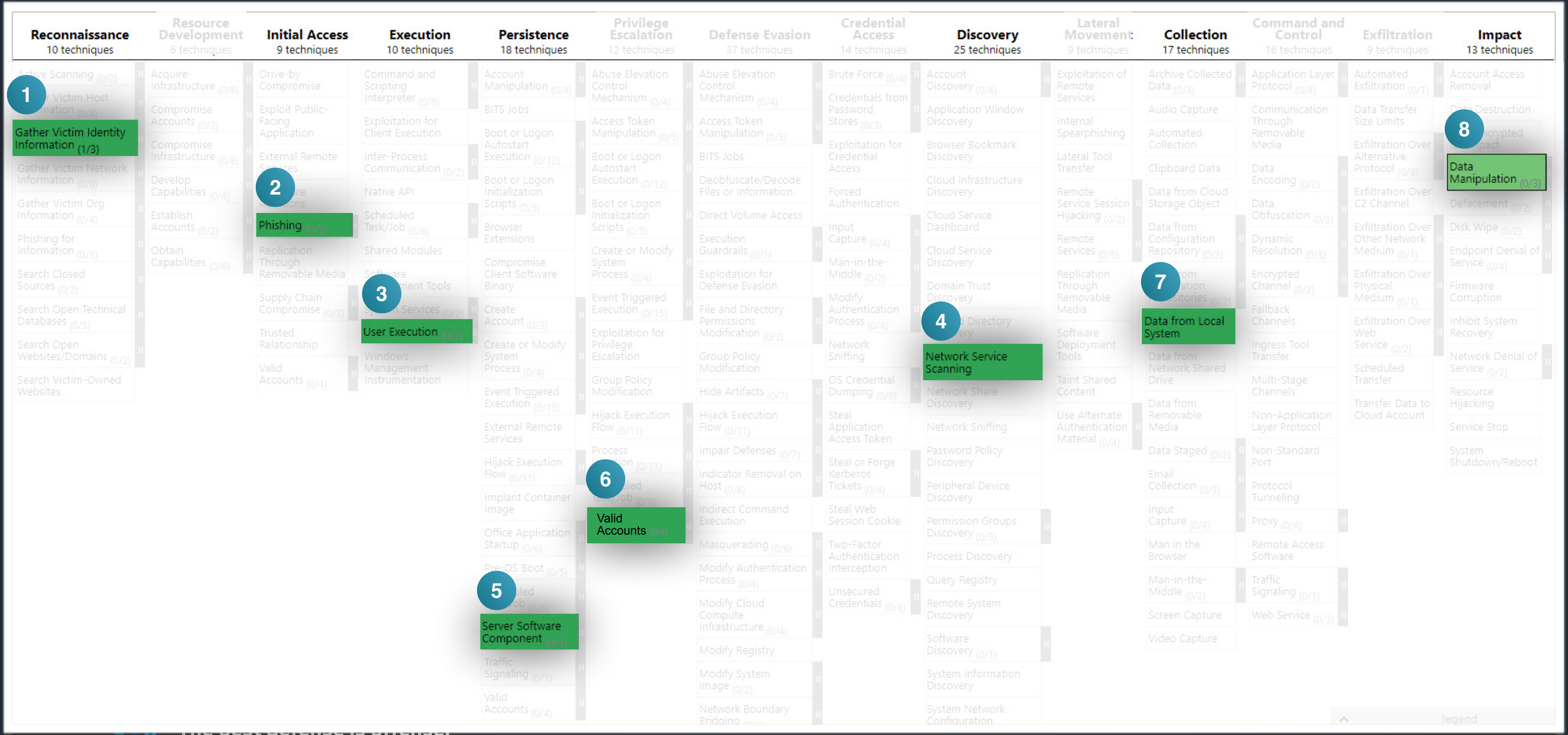
Impact 13 techniques
- Account Access Removal
- Data Destruction
- Data Encrypted for Impact
- Data Manipulation (0/3)
- Defacement (0/2)
- Disk Wipe (0/2)
- Endpoint Denial of Service (0/4)
- Firmware Corruption
- Inhibit System Recovery
- Network Denial of Service (0/2)
- Resource Hijacking
- Service Stop
- System Shutdown/Reboot

金融資安事件 - MITRE ATT&CK



Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
10 techniques	6 techniques	9 techniques	10 techniques	18 techniques	12 techniques	37 techniques	14 techniques	25 techniques	9 techniques	17 techniques	16 techniques	9 techniques	13 techniques
Active Scanning (0/2)	Acquire Infrastructure (0/6)	Drive-by Compromise	Command and Scripting Interpreter (0/8)	Account Manipulation (0/4)	Abuse Elevation Control Mechanism (0/4)	Abuse Elevation Control Mechanism (0/4)	Brute Force (0/4)	Account Discovery (0/4)	Exploitation of Remote Services	Archive Collected Data (0/3)	Application Layer Protocol (0/4)	Automated Exfiltration (0/1)	Account Access Removal
1 r Victim Host mation (0/4)	Compromise Accounts (0/2)	Exploit Public-Facing Application	Exploitation for Client Execution	BITS Jobs	Access Token Manipulation (0/5)	Access Token Manipulation (0/5)	Credentials from Password Stores (0/3)	Application Window Discovery	Internal Spearphishing	Audio Capture	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Gather Victim Identity Information (1/3)	Compromise Infrastructure (0/6)	External Remote Services	Inter-Process Communication (0/2)	Boot or Logon Autostart Execution (0/12)	Boot or Logon Autostart Execution (0/12)	BITS Jobs	Exploitation for Credential Access	Browser Bookmark Discovery	Lateral Tool Transfer	Automated Collection	Data Encoding (0/2)	Exfiltration Over Alternative Protocol (0/3)	Data Encrypted for Impact
Gather Victim Network Information (0/6)	Develop Capabilities (0/4)	2 re ons	Native API	Boot or Logon Initialization Scripts (0/5)	Boot or Logon Initialization Scripts (0/5)	Deobfuscate/Decode Files or Information	Forced Authentication	Cloud Infrastructure Discovery	Remote Service Session Hijacking (0/2)	Clipboard Data	Data Obfuscation (0/3)	Exfiltration Over C2 Channel	Data Manipulation (0/3)
Gather Victim Org Information (0/4)	Establish Accounts (0/2)	Phishing (0/3)	Scheduled Task/Job (0/6)	Browser Extensions	Create or Modify System Process (0/4)	Direct Volume Access	Input Capture (0/4)	Cloud Service Dashboard	Remote Services (0/6)	Data from Cloud Storage Object	Dynamic Resolution (0/3)	Exfiltration Over Other Network Medium (0/1)	Defacement (0/2)
Phishing for Information (0/3)	Obtain Capabilities (0/6)	Replication Through Removable Media	Shared Modules	Compromise Client Software Binary	Event Triggered Execution (0/15)	Execution Guardrails (0/1)	Man-in-the-Middle (0/2)	Cloud Service Discovery	Replication Through Removable Media	Data from Configuration Repository (0/2)	Encrypted Channel (0/2)	Exfiltration Over Physical Medium (0/1)	Disk Wipe (0/2)
Search Closed Sources (0/2)		Supply Chain Compromise (0/3)	Software ment Tools	Create Account (0/3)	Exploitation for Privilege Escalation	Exploitation for Defense Evasion	Modify Authentication Process (0/4)	Domain Trust Discovery	Software Deployment Tools	7 rom ation sitories (0/2)	Fallback Channels	Exfiltration Over Web Service (0/2)	Endpoint Denial of Service (0/4)
Search Open Technical Databases (0/5)		Trusted Relationship	3 S n Services (0/2)	Create or Modify System Process (0/4)	Group Policy Modification	File and Directory Permissions Modification (0/2)	Network Sniffing	4 d Directory ery	Taint Shared Content	Data from Local System	Ingress Tool Transfer	Scheduled Transfer	Firmware Corruption
Search Open Websites/Domains (0/2)		Valid Accounts (0/4)	User Execution (0/2)	Event Triggered Execution (0/15)	Hijack Execution Flow (0/11)	Group Policy Modification	OS Credential Dumping (0/8)	Network Service Scanning	Use Alternate Authentication Material (0/4)	Data from Network Shared Drive	Multi-Stage Channels	Transfer Data to Cloud Account	Inhibit System Recovery
Search Victim-Owned Websites			Windows Management Instrumentation	External Remote Services	Process tion (0/11)	Hide Artifacts (0/7)	Steal Application Access Token	Network Share Discovery		Data from Removable Media	Non-Application Layer Protocol		Network Denial of Service (0/2)
				Hijack Execution Flow (0/11)	6 uled Task/Job (0/6)	Hijack Execution Flow (0/11)	Steal or Forge Kerberos Tickets (0/4)	Network Sniffing		Data Staged (0/2)	Non-Standard Port		Resource Hijacking
				Implant Container Image	Valid Accounts (0/4)	Impair Defenses (0/7)	Steal Web Session Cookie	Password Policy Discovery		Email Collection (0/3)	Protocol Tunneling		Service Stop
				Office Application Startup (0/6)		Indicator Removal on Host (0/6)	Two-Factor Authentication Interception	Peripheral Device Discovery		Input Capture (0/4)	Proxy (0/4)		System Shutdown/Reboot
				Pre-OS Boot (0/5)		Indirect Command Execution	Unsecured Credentials (0/6)	Permission Groups Discovery (0/3)		Man in the Browser	Remote Access Software		
				5 uled ob (0/6)		Masquerading (0/6)		Process Discovery		Man-in-the-Middle (0/2)	Traffic Signaling (0/1)		
				Server Software Component (0/3)		Modify Authentication Process (0/4)		Query Registry		Screen Capture	Web Service (0/3)		
				Traffic Signaling (0/1)		Modify Cloud Compute Infrastructure (0/4)		Remote System Discovery		Video Capture			
				Valid Accounts (0/4)		Modify Registry		Software Discovery (0/1)					
						Modify System Image (0/2)		System Information Discovery					
						Network Boundary Bridging (0/1)		System Network Configuration					

金融資安事件 - MITRE ATT&CK



Reconnaissance
10 techniques

- Active Scanning (0/2)
- r Victim Host mation (0/4)
- Gather Victim Identity Information (1/3)
- Gather Victim Network Information (0/6)
- Gather Victim Org Information (0/4)
- Phishing for Information (0/3)
- Search Closed Sources (0/2)
- Search Open Technical Databases (0/5)
- Search Open Websites/Domains (0/2)
- Search Victim-Owned Websites

Resource Development
6 techniques

- Acquire Infrastructure (0/6)
- Compromise Accounts (0/2)
- Compromise Infrastructure (0/6)
- Develop Capabilities (0/4)
- Establish Accounts (0/2)
- Obtain Capabilities (0/6)

Initial Access
9 techniques

- Drive-by Compromise
- Exploit Public-Facing Application
- External Remote Services
- re ons
- Phishing (0/3)
- Replication Through Removable Media
- Supply Chain Compromise (0/3)
- Trusted Relationship
- Valid Accounts (0/4)

Execution
10 techniques

- Command and Scripting Interpreter (0/8)
- Exploitation for Client Execution
- Inter-Process Communication (0/2)
- Native API
- Scheduled Task/Job (0/6)
- Shared Modules
- Software ment Tools
- Sy m Services (0/2)
- User Execution (0/2)
- Windows Management Instrumentation

Persistence
18 techniques

- Account Manipulation (0/4)
- BITS Jobs
- Boot or Logon Autostart Execution (0/12)
- Boot or Logon Initialization Scripts (0/5)
- Browser Extensions
- Compromise Client Software Binary
- Create Account (0/3)
- Create or Modify System Process (0/4)
- Event Triggered Execution (0/15)
- External Remote Services
- Hijack Execution Flow (0/11)
- Implant Container Image
- Office Application Startup (0/6)
- Pre-OS Boot (0/5)
- uled ob (0/6)
- Server Software Component (0/3)
- Traffic Signaling (0/1)
- Valid Accounts (0/4)

Privilege Escalation
12 techniques

- Abuse Elevation Control Mechanism (0/4)
- Access Token Manipulation (0/5)
- Boot or Logon Autostart Execution (0/12)
- Boot or Logon Initialization Scripts (0/5)
- Create or Modify System Process (0/4)
- Event Triggered Execution (0/15)
- Exploitation for Privilege Escalation
- Group Policy Modification
- Hijack Execution Flow (0/11)
- Process tion (0/11)
- uled Task/Job (0/6)
- Valid Accounts (0/4)

Defense Evasion
37 techniques

- Abuse Elevation Control Mechanism (0/4)
- Access Token Manipulation (0/5)
- BITS Jobs
- Deobfuscate/Decode Files or Information
- Direct Volume Access
- Execution Guardrails (0/1)
- Exploitation for Defense Evasion
- File and Directory Permissions Modification (0/2)
- Group Policy Modification
- Hide Artifacts (0/7)
- Hijack Execution Flow (0/11)
- Impair Defenses (0/7)
- Indicator Removal on Host (0/6)
- Indirect Command Execution
- Masquerading (0/6)
- Modify Authentication Process (0/4)
- Modify Cloud Compute Infrastructure (0/4)
- Modify Registry
- Modify System Image (0/2)
- Network Boundary Bridging (0/1)

Credential Access
14 techniques

- Brute Force (0/4)
- Credentials from Password Stores (0/3)
- Exploitation for Credential Access
- Forced Authentication
- Input Capture (0/4)
- Man-in-the-Middle (0/2)
- Modify Authentication Process (0/4)
- Network Sniffing
- OS Credential Dumping (0/8)
- Steal Application Access Token
- Steal or Forge Kerberos Tickets (0/4)
- Steal Web Session Cookie
- Two-Factor Authentication Interception
- Unsecured Credentials (0/6)

Discovery
25 techniques

- Account Discovery (0/4)
- Application Window Discovery
- Browser Bookmark Discovery
- Cloud Infrastructure Discovery
- Cloud Service Dashboard
- Cloud Service Discovery
- Domain Trust Discovery
- d Directory ery
- Network Service Scanning
- Network Share Discovery
- Network Sniffing
- Password Policy Discovery
- Peripheral Device Discovery
- Permission Groups Discovery (0/3)
- Process Discovery
- Query Registry
- Remote System Discovery
- Software Discovery (0/1)
- System Information Discovery
- System Network Configuration

Lateral Movement
9 techniques

- Exploitation of Remote Services
- Internal Spearphishing
- Lateral Tool Transfer
- Remote Service Session Hijacking (0/2)
- Remote Services (0/6)
- Replication Through Removable Media
- Software Deployment Tools
- Taint Shared Content
- Use Alternate Authentication Material (0/4)

Collection
17 techniques

- Archive Collected Data (0/3)
- Audio Capture
- Automated Collection
- Clipboard Data
- Data from Cloud Storage Object
- Data from Configuration Repository (0/2)
- rom ation ositories (0/2)
- Data from Local System
- Data from Network Shared Drive
- Data from Removable Media
- Data Staged (0/2)
- Email Collection (0/3)
- Input Capture (0/4)
- Man in the Browser
- Man-in-the-Middle (0/2)
- Screen Capture
- Video Capture

Command and Control
16 techniques

- Application Layer Protocol (0/4)
- Communication Through Removable Media
- Data Encoding (0/2)
- Data Obfuscation (0/3)
- Dynamic Resolution (0/3)
- Encrypted Channel (0/2)
- Fallback Channels
- Ingress Tool Transfer
- Multi-Stage Channels
- Non-Application Layer Protocol
- Non-Standard Port
- Protocol Tunneling
- Proxy (0/4)
- Remote Access Software
- Traffic Signaling (0/1)
- Web Service (0/3)

Exfiltration
9 techniques

- Automated Exfiltration (0/1)
- Data Transfer Size Limits
- Exfiltration Over Alternative Protocol (0/3)
- Exfiltration Over C2 Channel
- Exfiltration Over Other Network Medium (0/1)
- Exfiltration Over Physical Medium (0/1)
- Exfiltration Over Web Service (0/2)
- Scheduled Transfer
- Transfer Data to Cloud Account

Impact
13 techniques

- Account Access Removal
- Data Destruction
- ncrypted pact
- Data Manipulation (0/3)
- Defacement (0/2)
- Disk Wipe (0/2)
- Endpoint Denial of Service (0/4)
- Firmware Corruption
- Inhibit System Recovery
- Network Denial of Service (0/2)
- Resource Hijacking
- Service Stop
- System Shutdown/Reboot

legend

隱形的差距

常見攻擊鏈+ 通常金融業**不太會有明顯**影響業務情況

初始進入 → 持久化 → 提權 → 橫向移動 → 取得資料 → 影響業務

01. 可視性

02. 風險認知

03. 合規落差

04. 行為視角

05. 流程碎片化

01. 可視性

- 日誌缺：關鍵入口 / 身份鑑別 / 雲端 與 供應鏈 沒被納入同一條線
- 日誌散：欄位不一致、時間線對不起來、關聯不起來
  - SOC 看見的是「告警」，但攻擊者走的是「行為軌跡」

網站相關弱點或設定不當高度相關

凸顯 Web 攻擊面之防護成熟度，將直接影響整體內網安全風險。

01. 可視性 自評問答

- 你能否 回答：哪些關鍵入口「沒有/例外」MFA？
- 你能否 看見：非典型裝置/地點/時間的登入行為？
- 你能否 串起：登入 → 橫向移動 → 取得資料酷 的同一條時間線？

02. 錯誤的風險認知

- 「沒被打」≠「很安全」：最大的危險是你不知道你已被滲透
- 風險不只在漏洞，也在流程、人、例外狀況以及業務邏輯
- 安全決策要權衡風險/成本/影響，而不是只追求「越快越好」

高價資產（資料庫 / 核心資料 / 交易關聯）

常見弱點：MFA 例外、缺條件式存取、缺行為監控與異常告警

攻擊者策略：先偷憑證 → 再用最短路徑直達高價資產

02. 錯誤的風險認知 自評問答

- 你們最可能被利用的 3 個入口點？
  - 依據是什麼？（事件、情資、資產曝露、例外清單）

03. 合規 vs 實戰落差

- 合規是底線，不是終點（合規檢驗「是否具備」）
- 實戰要回答「能否抵禦」：時間窗內能否偵測、阻斷、減少損害

稽核範圍外資產：影子系統/測試環境/外包介面/供應商通道
業務邏輯：流程可被繞過、API 被濫用但不觸發傳統告警
橫向移動路徑未演練：AD/管理平台/跳板主機成為必經跳點

04. 設備導向 vs 行為導向

- 設備導向問法：EDR 裝了嗎？WAF 開了嗎？
- 行為導向問法：誰在「不該」的時間/地點/方式做事？
- 攻擊者看行為：橫向移動、提權、取資料的行為與關聯

Identity：異常登入、條件式存取、Token 濫用與會話劫持跡象
Lateral：遠端服務、憑證傾倒、權限擴大、異常列舉與掃描
Data：查詢量/匯出行為/壓縮/資料傳輸與目的異常

05. 事件處理流程碎片化

- 告警在 SOC、證據在各系統、決策在不同單位（資訊與責任分散）
- 交接期 = 攻擊者黃金時間（協調越慢，攻擊越順）
- 工單式處理常跟不上攻擊節奏：看見 ≠ 來得及

用業務語言定義嚴重分級：交易/個資/核心系統＝最高優先
權責：誰能斷線？誰能封帳？誰能停服務？（避免臨場爭論）
證據鏈：哪些 log 必保全、保存多久、誰能取用與回溯

01. 可視性

身分 / SaaS /API 納入同一狩獵面
（關聯與回溯）

02. 風險認知

入口分級 ＋ 例外治理
（最小例外、最高監控）

03. 合規落差

用情境化演練驗證控制有效性
（不是只驗證存在）

04. 行為視角

建立基線＋關聯
（把事件串成鏈）

05. 流程碎片化

playbook＋紅隊演練＋跨單位節奏
（縮短協調期 ）

執行者

架構設計者：能預判攻擊路徑、設計偵測與回應

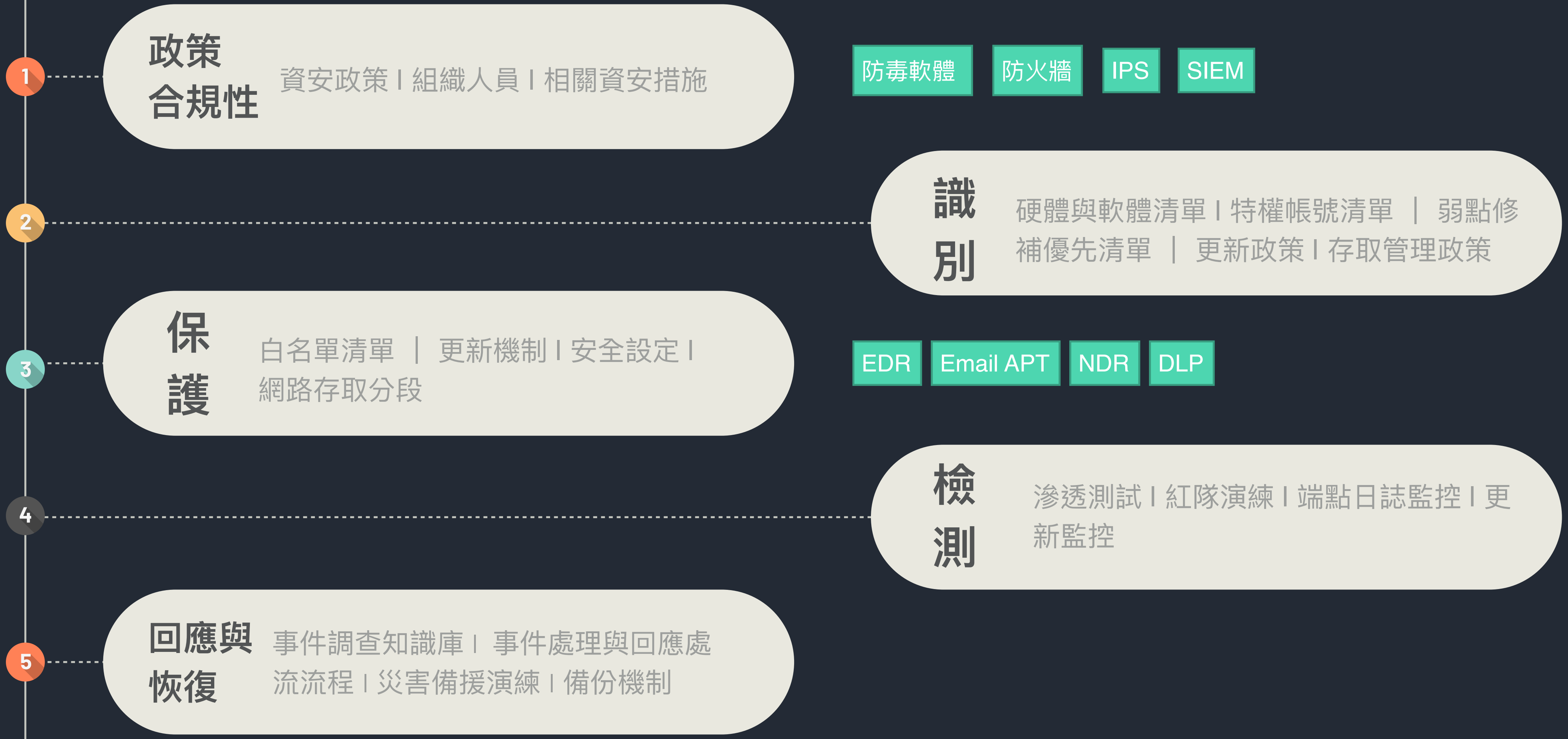
技術專家

業務詮釋者：用業務語言說清「為何必須優先」

事故響應者

風險管理者：把重心前移到威脅建模與風險評估

落實資安相關措施與持續推展



1 政策合規性

資安政策 | 組織人員 | 相關資安措施

防毒軟體 防火牆 IPS SIEM

2 識別

硬體與軟體清單 | 特權帳號清單 ｜ 弱點修補優先清單 ｜ 更新政策 | 存取管理政策

3 保護

白名單清單 ｜ 更新機制 | 安全設定 | 網路存取分段

EDR Email APT NDR DLP

4 檢測

滲透測試 | 紅隊演練 | 端點日誌監控 | 更新監控

5 回應與恢復

事件調查知識庫 | 事件處理與回應處流流程 | 災害備援演練 | 備份機制

藍隊人員

防禦者擁抱攻擊者心態

被動防禦 逐漸提升 主動防禦

很重要

ZUSO Generation
The best defense is offense.

臺灣證券交易所
115年證券商資通安全會議
攻擊者眼中的資安團隊隱形差距

紅隊演練並非萬靈藥

但是！可以 提早發現問題 ｜入侵途徑｜影響範圍

也可以知道哪些是冤望錢

如梭世代股份有限公司
sales@zuso.ai

2026.03.20

Thank You!

工具不是答案，理解才是槓桿：用攻擊者視角重排優先序
把縫縮小：可視性補齊、例外收斂、行為關聯、流程劇本化

下一步：選 1 條最高風險路徑做攻擊驅動 PoC
（先把一條線打穿）

連絡我們

Email

sales@zuso.ai

Facebook

https://FB.com/ZUSOGeneration

Website

https://zuso.ai

ZUSO Generation
The best defense is offense.