CYBERSEC 2022 臺灣資安大會

# CHANGE

NOW

數位轉型 資安升級

SEP. 20-22 臺北南港展覽二館

# 制定有效的 XDR 戰略

## Defining an XDR Strategy

朱孟穎
亞太技術副總

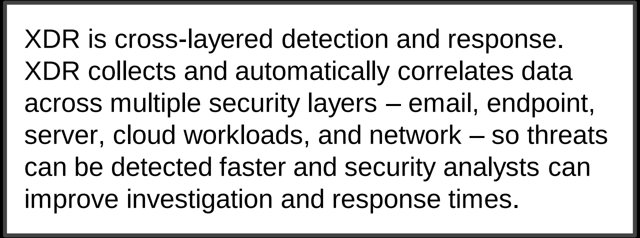
Daniel Chu

VP. Systems Engineering, APJ
ExtraHop

# 如何定義 XDR?

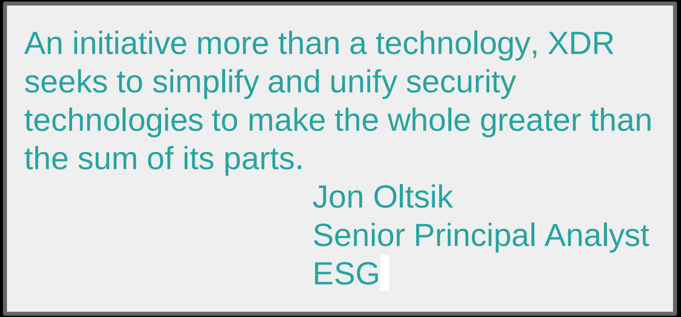
**(eXtended Detection & Response)**

# 業界分析師如何定義XDR?



XDR is cross-layered detection and response. XDR collects and automatically correlates data across multiple security layers – email, endpoint, server, cloud workloads, and network – so threats can be detected faster and security analysts can improve investigation and response times.

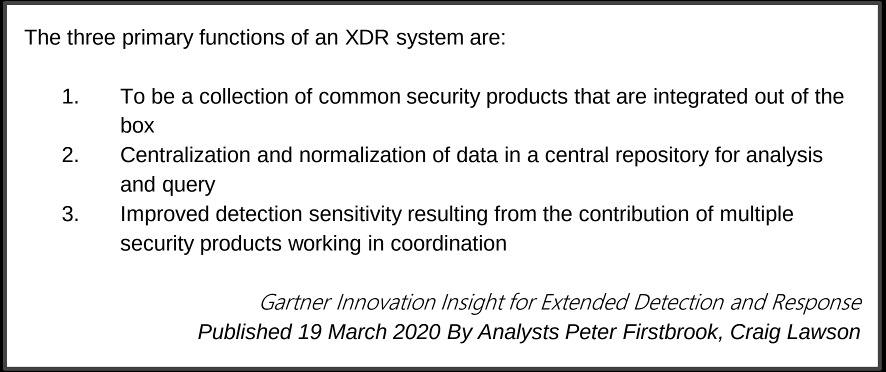
**XDR可整合: email、 端點、雲端、網路 的資料**



An initiative more than a technology, XDR seeks to simplify and unify security technologies to make the whole greater than the sum of its parts.

Jon Oltsik
Senior Principal Analyst
ESG

**XDR 非技術產品,而是新的主動方針，其精神為: 提供簡化與整合的資安產品使整體效益大於各個部分的總和**

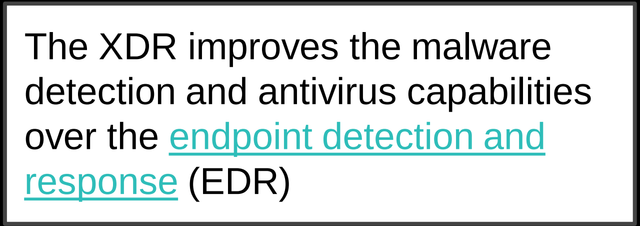


The three primary functions of an XDR system are:

1. To be a collection of common security products that are integrated out of the box
2. Centralization and normalization of data in a central repository for analysis and query
3. Improved detection sensitivity resulting from the contribution of multiple security products working in coordination

*Gartner Innovation Insight for Extended Detection and Response*
*Published 19 March 2020 By Analysts Peter Firstbrook, Craig Lawson*

**1. 容易整合各類的資安產品**
**2. 資料集中化＋正規化**
**3. 多產品協同工作下大幅提昇偵測效果**



The XDR improves the malware detection and antivirus capabilities over the endpoint detection and response (EDR)

**XDR可提昇EDR偵測惡意程式的效力**

# 業界廠商如何定義XDR?

## 資安廠商:

- “XDR = SIEM + EDR”
- “XDR 是進階的EDR” 或 “EDR+”
- “XDR = EDR + NDR”
- “XDR = SIEM + SOAR + EDR”
- “XDR = SIEM”

## 資安老鳥User:

- “XDR是無意義的行銷用語”
- “XDR是品牌重塑包裝”

# XDR的使命

1. **Improve Detection and Response**
   提昇偵測與回應功能

2. **Reduce Friction**
   減低執行摩擦：建置，維運，價位

3. **Consolidate Tools**
   簡化整合現有工具

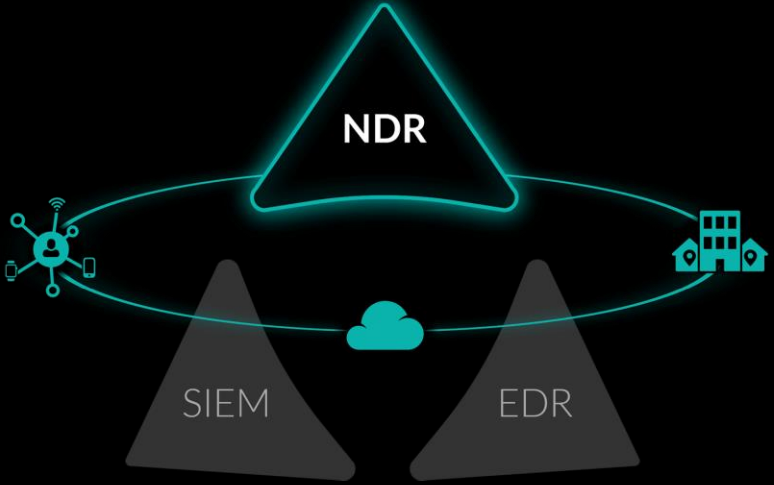
# eXtending Detection and Response

## 如何避免資安安全事件衍生成嚴重洩漏?

- Post-Compromise mindset
  防護+防止的心態到侵入後心態

- Fill in the gaps
  填補盲點

- Focus on reducing dwell time
  專注在降低潛伏期



ExtraHop

# XDR 偵測與回應 取決於資料來源

## NDR – 網路

高解析度俯視圖監視 (網路)

盲點: 端點內

## EDR - 檔案, 程序, 登錄檔

家中高解析監視 (端點)

盲點: 伺服器、Linux、IoT

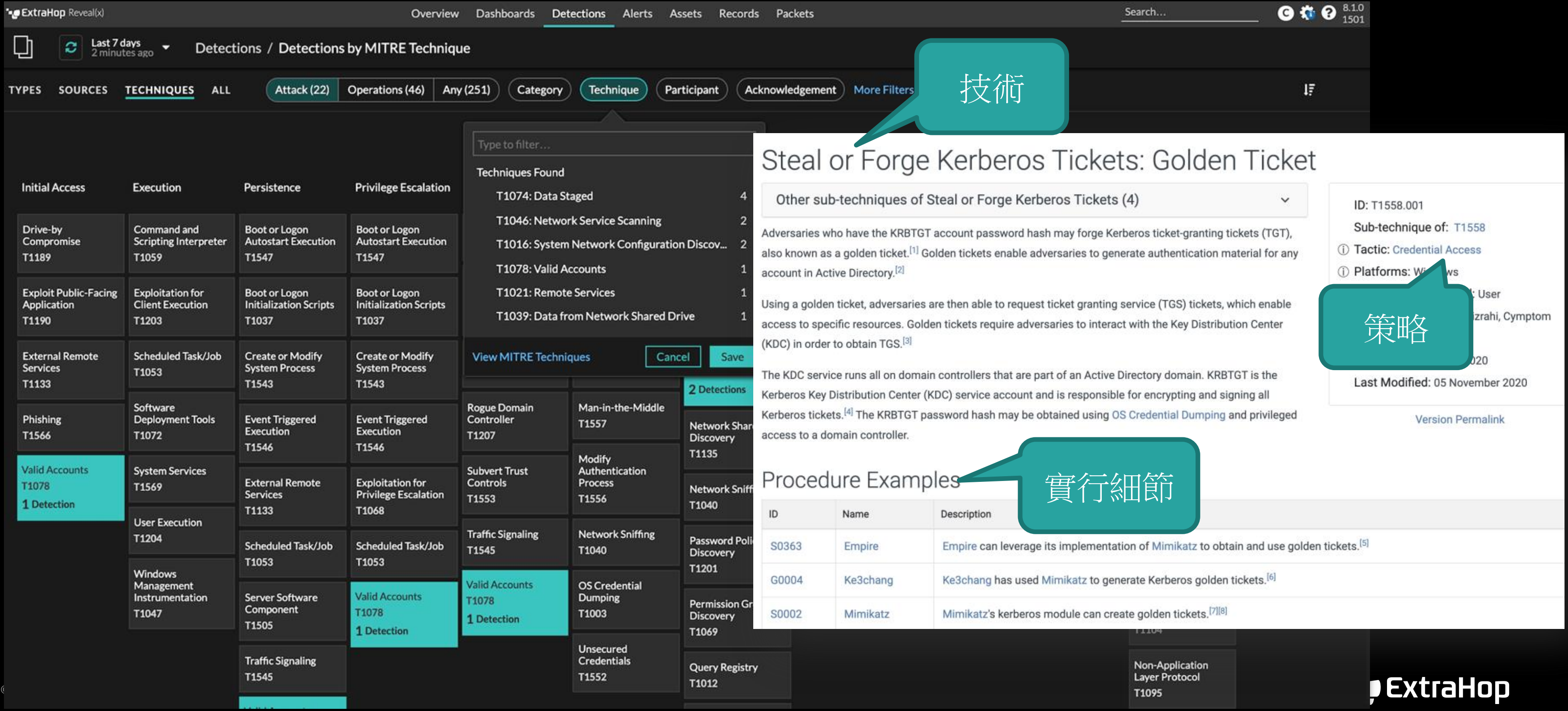
## SIEM – 日誌

房間裡高解析檢視 (應用層)

盲點: 沒裝日誌的系統

# MITRE ATT&CK 資安框架當Detection參考:

## TTP: 策略(Tactics), 技術(Techniques), 實行細節(Procedures)



Type to filter...

Techniques Found

| | |
|---|---|
| T1074: Data Staged | 4 |
| T1046: Network Service Scanning | 2 |
| T1016: System Network Configuration Discov... | 2 |
| T1078: Valid Accounts | 1 |
| T1021: Remote Services | 1 |
| T1039: Data from Network Shared Drive | 1 |

View MITRE Techniques Cancel Save

Initial Access
- Drive-by Compromise T1189
- Exploit Public-Facing Application T1190
- External Remote Services T1133
- Phishing T1566
- Valid Accounts T1078 1 Detection

Execution
- Command and Scripting Interpreter T1059
- Exploitation for Client Execution T1203
- Scheduled Task/Job T1053
- Software Deployment Tools T1072
- System Services T1569
- User Execution T1204
- Windows Management Instrumentation T1047

Persistence
- Boot or Logon Autostart Execution T1547
- Boot or Logon Initialization Scripts T1037
- Create or Modify System Process T1543
- Event Triggered Execution T1546
- External Remote Services T1133
- Scheduled Task/Job T1053
- Server Software Component T1505
- Traffic Signaling T1545

Privilege Escalation
- Boot or Logon Autostart Execution T1547
- Boot or Logon Initialization Scripts T1037
- Create or Modify System Process T1543
- Event Triggered Execution T1546
- Exploitation for Privilege Escalation T1068
- Scheduled Task/Job T1053
- Valid Accounts T1078 1 Detection

- Rogue Domain Controller T1207
- Subvert Trust Controls T1553
- Traffic Signaling T1545
- Valid Accounts T1078 1 Detection

- Man-in-the-Middle T1557
- Modify Authentication Process T1556
- Network Sniffing T1040
- OS Credential Dumping T1003
- Unsecured Credentials T1552

- 2 Detections
- Network Shar Discovery T1135
- Network Sniff T1040
- Password Poli Discovery T1201
- Permission Gr Discovery T1069
- Query Registry T1012

- Non-Application Layer Protocol T1095

### Steal or Forge Kerberos Tickets: Golden Ticket

Other sub-techniques of Steal or Forge Kerberos Tickets (4)

Adversaries who have the KRBTGT account password hash may forge Kerberos ticket-granting tickets (TGT), also known as a golden ticket.[1] Golden tickets enable adversaries to generate authentication material for any account in Active Directory.[2]

Using a golden ticket, adversaries are then able to request ticket granting service (TGS) tickets, which enable access to specific resources. Golden tickets require adversaries to interact with the Key Distribution Center (KDC) in order to obtain TGS.[3]

The KDC service runs all on domain controllers that are part of an Active Directory domain. KRBTGT is the Kerberos Key Distribution Center (KDC) service account and is responsible for encrypting and signing all Kerberos tickets.[4] The KRBTGT password hash may be obtained using OS Credential Dumping and privileged access to a domain controller.

ID: T1558.001

Sub-technique of: T1558

ⓘ Tactic: Credential Access

ⓘ Platforms: Wi ws

: User

zrahi, Cymptom

020

Last Modified: 05 November 2020

Version Permalink

### Procedure Examples

| ID | Name | Description |
|---|---|---|
| S0363 | Empire | Empire can leverage its implementation of Mimikatz to obtain and use golden tickets.[5] |
| G0004 | Ke3chang | Ke3chang has used Mimikatz to generate Kerberos golden tickets.[6] |
| S0002 | Mimikatz | Mimikatz's kerberos module can create golden tickets.[7][8] |

# APT Playbook

## 三幕劇: 開局，中局，殘局

### 1. 開局: 入侵初期

1. Initial Access

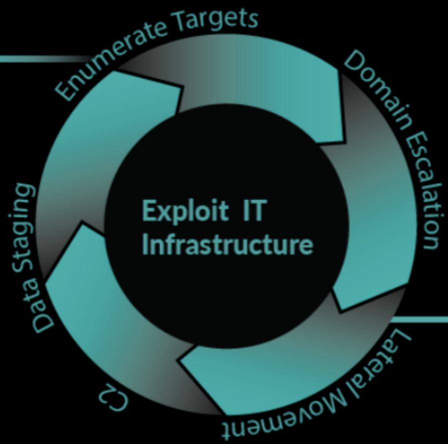
WIDE RANGE OF TECHNIQUES

- Phish
- Stolen credential
- Drive-by downloads
- RDP
- Initial Access Broker(IAB)
- Supply chain
- Trusted relationships
- Vulnerability exploit
- ...

Initial Access (入侵初期)

### 2. 中局

2. Midgame



Execution (執行)
Persistence (持續潛伏)
Privilege Escalation (權限提升)
Defense Evasion (防禦逃避)
Credential Access (憑證存取)
Discovery (發現)
Lateral Movement (橫向移動)
Collection (收集)

### 3.殘局: 衝擊

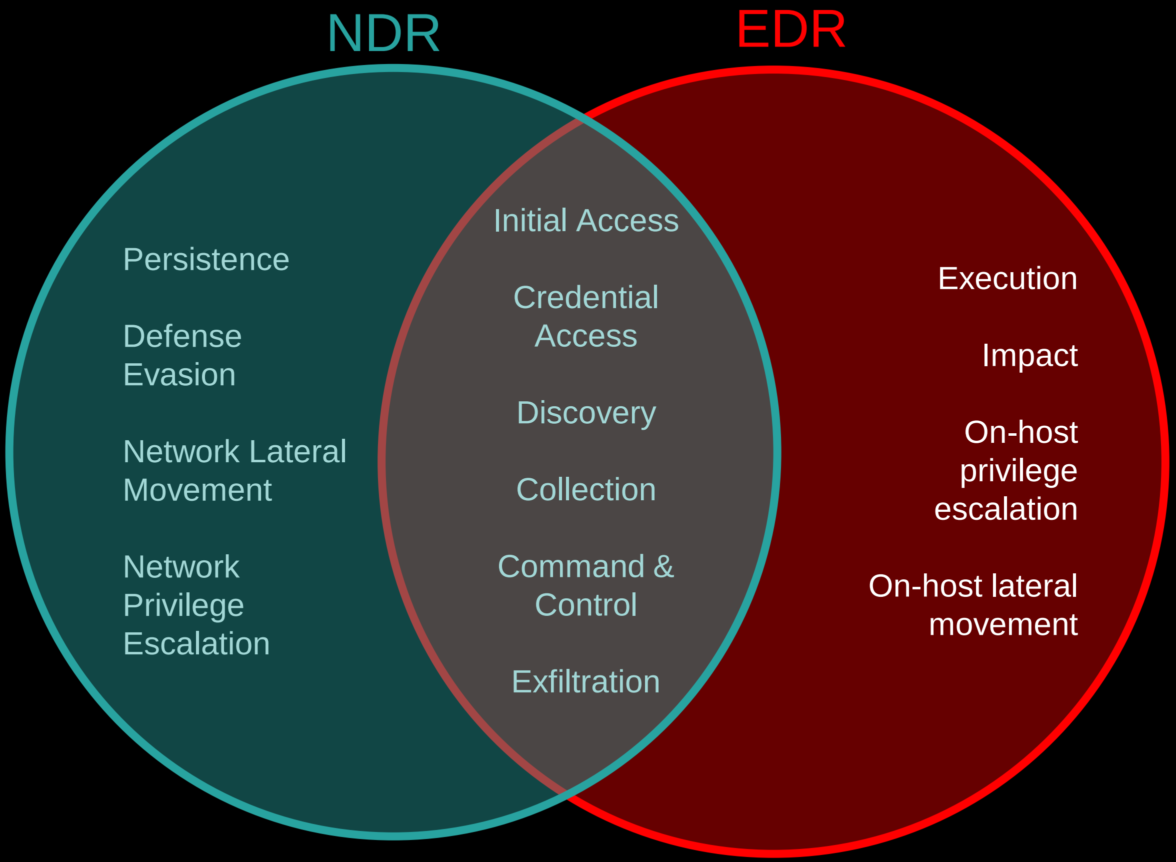
3. Extortion Cycle

TARGETED VALUABLES

- Apps Services
- DB Services
- Files Shares
- OT
- IoT

Exfiltration (滲透)
Command and Control (指揮與控制)
Impact (衝擊)

# NDR + EDR 可覆蓋的MITRE策略



NDR

EDR

Persistence

Defense Evasion

Network Lateral Movement

Network Privilege Escalation

Initial Access

Credential Access

Discovery

Collection

Command & Control

Exfiltration

Execution

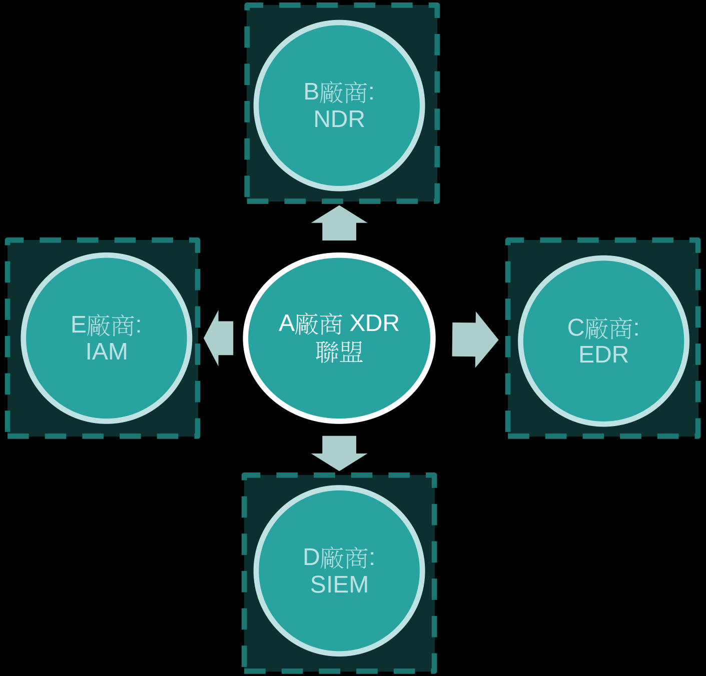
Impact

On-host privilege escalation

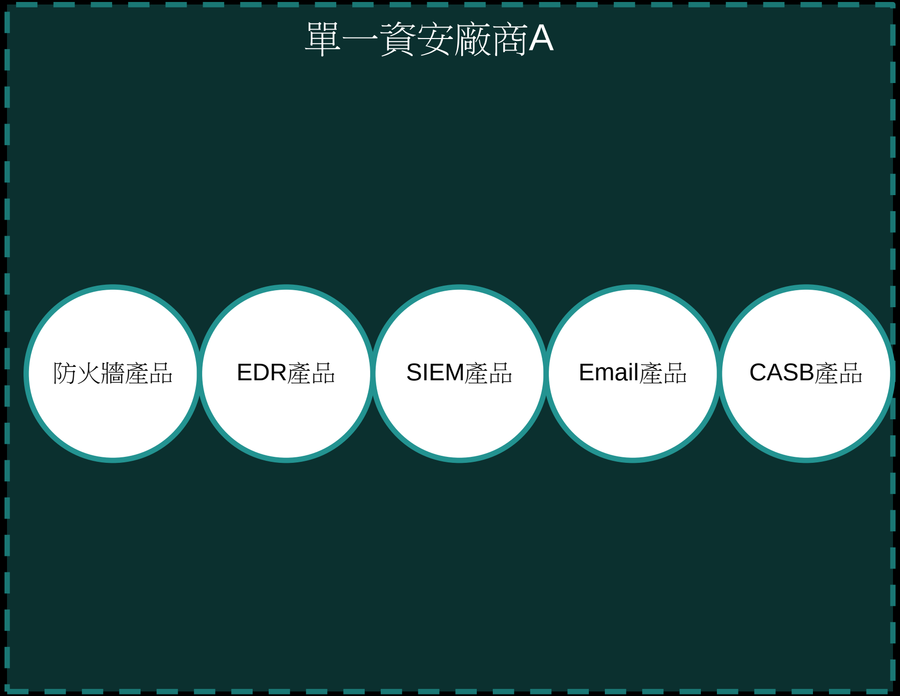
On-host lateral movement

# 市場上推展XDR 模式

## Open XDR 聯盟

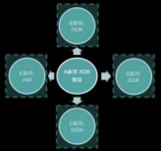


## 資安廠商產品線 (Security Portfolio)



# XDR 不是一個產品, 是一個策略

## Open XDR 策略



### 優點

- 可使用最先進的技術及專業的服務
(Best-of-Breed Product & Focused services)

- 不被單一廠商套牢
- 採購價優化

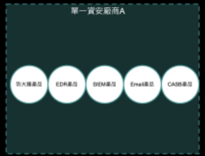
### 缺點:

- 需個別簽約
- 整合多廠商的複雜度

### 評估:

- 是表面的還是緊密的整合?
- 各別簽約/供應商的負擔有多少?

## 單一廠商 XDR 策略



### 優點

- 單一管理
- 單一合約

### 缺點:

- 套裝產品 品質不一
- 併購後的產品時常沒有新的研發
- 不符合用戶需求的擴充產品

### 評估:

- 同場商是否真的有緊密整合?
- 可整合第三方廠商資料/程序?
- XDR 供應的其他產品是否符合你環境需求?

# 制定有效的 XDR 戰略

1. **Post-Compromise mindset**
   防護+防止的心態到侵入後心態
   資安組織的復原能力

2. **Improve Detection and Response**
   提昇偵測與回應功能
   取決於資料來源
   了解並彌補盲點 (參考MITRE)

3. 找出適合的XDR的策略:
   OpenXDR vs 單一廠商

# 謝謝