Microsoft Advanced Threat Analytics

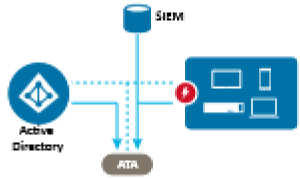
偵測內部 ID 所進行的非法存取

Microsoft Advanced Threat Analytics (ATA) 運用機器學習技術，分析登入 Active Directory 時的驗證狀況並預測使用者之後續動作，可早期發現從公司內部/外部進行非法存取或惡意攻擊的行為，是可確保網路安全性的解決方案。

輕鬆迅速掌握網路上發生的情況

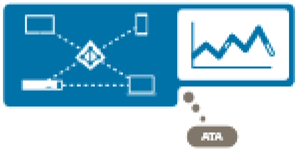
Microsoft Advanced Threat Analytics 可自動分析、學習及判別使用者或裝置的可疑動作，可保護企業及資料以避免遭到先進的目標型攻擊。ATA 運用封包檢查技術，以來自安全性情報、事件管理、內部 Active Directory 等各種資料來源的資訊為基礎，建立組織資訊安全關係，能夠幾近即時偵測到先進的目標型攻擊。ATA 可偵測到針對內部 Active Directory 的認證資料進行的攻擊以及非法活動或行為，可在發生重大損失之前防禦先進的安全性攻擊。

1.分析



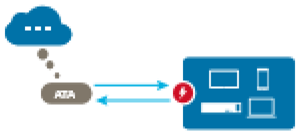
- Active Directory 網路流量之擷取與分析
- Deep Packet Inspection (DPI)
- 從 SIEM 收集記錄的事件

2.學習



- 自動學習使用者及 PC 的活動動作

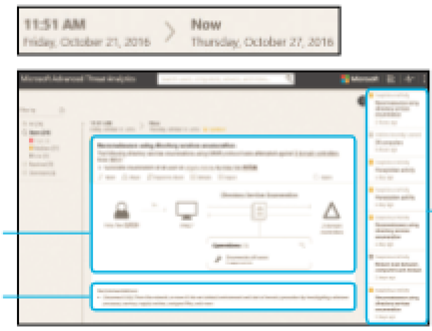
3.偵測



- 偵測發現惡意的攻擊、異常行為及安全性威脅
- 建立攻擊時間軸視覺，以掌握哪位使用者在何時如何進行攻擊

何時、從何處進行何種攻擊

可透過時間軸（時序）以可視化方式檢視攻擊者何時、從何處進行何種攻擊。Microsoft Advanced Threat Analytics 持續針對 Active Directory 上的 ID 進行分析、學習，並偵測是否有異常的行為，因此可迅速避免安全威脅。



詳細的安全性警示

Microsoft Advanced Threat Analytics 可針對 Pass-The-Ticket 或 Pass-The-Hash 等惡意攻擊並運用機器學習，進行使用者異常行為、安全問題及風險等詳細的警示偵測。

警示

惡意攻擊

在無需設定下就能即時偵測出已知的惡意攻擊

- Pass-the-Ticket (PtT)
- Pass-the-Hash (PtH)
- Overpass-the-Hash
- 偽造 PAC (MS14-068)
- Silver PAC (MS11-013)
- Golden Ticket
- Skeleton Key惡意軟體
- 偵察行為 (DNS、SMB)
- Bruteforce (NTLM、Kerberos、LDAP)
- 遠端執行

異常行為

利用機器學習進行行為分析，以發現可疑的活動或異常行為

- 異常的登入
- 利用 Honeytoken 帳戶
- 異常的資源存取
- 密碼共用
- 橫向移動

安全性問題與風險

識別已知的安全性問題

- 信任關係的異動
- 脆弱的通訊協定
- 異常的通訊協定
- 已知的通訊協定安全漏洞