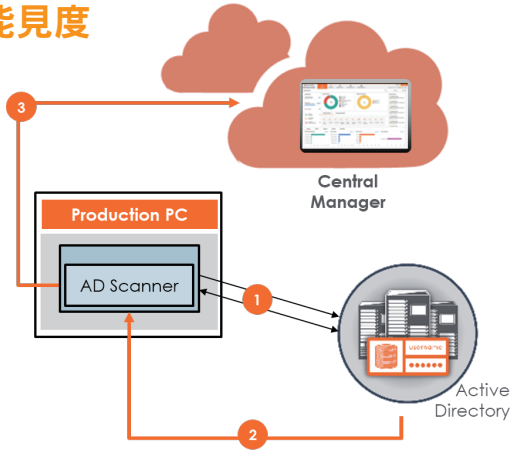
RiskView Active Directory為 AD 曝露風險和攻擊行為提供絕不間斷的超高能見度

微軟的產品 Active Directory (簡稱 AD) 是所有企業資源的主要資訊來源，並且與商業應用程式緊密整合，因此成為攻擊者的高價值目標。然而，要保障 AD 的安全並不簡單，因為除非企業組織執行詳盡且昂貴的審核機制，否則許多漏洞是不明顯的。

RiskView- 針對曝露風險和即時攻擊持續提供能見度

- 針對關鍵性網域、電腦和使用者等級的曝露風險提供能見度，以迅速修正弱點
- 持續或依需求對 AD 進行主動監控，以迅速發現當中有可能的攻擊活動
- 分析潛在風險的變化並提供風險評分
- 識別有可能存在惡意活動的新曝露風險



RiskView Active Directory流程示意圖

效益

- 針對 AD 安全基本防護 (Security Hygiene) 問題提供能見度，並對網域、電腦和身份等級的主要曝露發出可採取行動的告警
- 即時針對 AD 權限提升進行偵測，並對 AD 資訊的存取提供更精細的限制，而不會影響企業商務營運
- 持續深入地了解與憑證、權限帳戶、老舊帳戶、共享憑證和身份攻擊路徑有關的身份和服務帳戶風險

建置

- 易於部署：輕量級的程式庫，不需要權限憑證就能從單一端點執行
- 具有靈活性：可選擇公共雲或就地部署的管理和控制台
- 自動化：只需在網域控制器訂閱變更告警機制，即可即時偵測攻擊

RISKVIEW

RiskView 智能數位資產風險防護解決方案

數位攻擊面盤點

數位攻擊面盤點模組可識別企業組織的數位足跡(Digital Footprint)，並持續監控外圍的資產，以確保提供該資產的能見度，方法是依據嚴重性將要處理的問題以優先順序排列，從而突顯出相關的威脅、漏洞和弱點。

威脅情資蒐集和分析

即時監控開放網路、深網 (Deep Web) 和暗網中成千上萬個威脅來源，蒐集數以百萬計的情資項目。

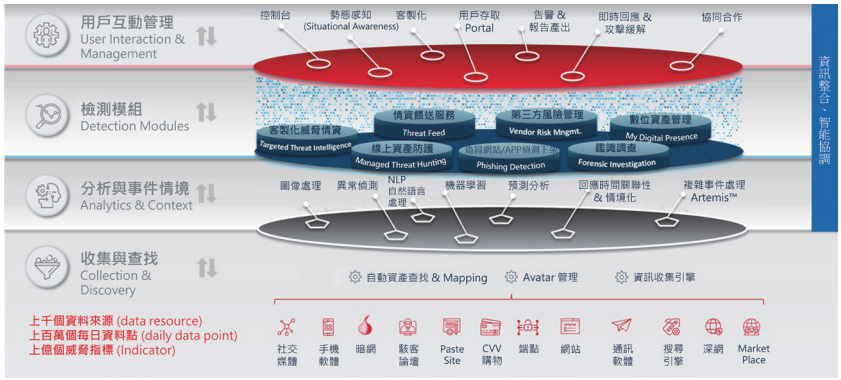
原始情資項目會自動與企業組織的資產 (包括 IP、網域、品牌、主管等等) 相互關聯，並根據特定的使用個案進行分類，範疇包括釣魚網站 (Phishing)、惡意軟體活動、憑證填充(Credential Stuffing)、資料洩漏、欺詐活動等等。

威脅情資蒐集和分析

再利用專業的機器學習演算法，根據潛在風險和影響對此原始情資依優先順序排列，進而提供智慧型且具成本效益的分析。自動化和半自動化的分析引擎會建立可採取行動的告警，然後透過深入的分析、豐富的背景信息、威脅參與者分析等向資安團隊發出告警，讓企業組織能採取有效的行動。

鑑識資料視覺化 (Forensic Viewer)

鑑識資料視覺化模組能識別及分析威脅參與者，並深入調查他們使用的工具、戰術和流程 (TTPs; Tools, Tactics and Procedures)。鑑識資料視覺化模組的利用有助於使特定或多個入侵指標 (IOC)的背景信息更加充實，進而將多項服務整合成統一的調查平台，以支援各種連線，包括威脅情資、WHOIS 服務、被動域名系統 (DNS)、社交探索(Social Discovery)、惡意程式碼偵測等等。



RiskView智能數位資產風險防護解決方案總覽

橙鎵科技公司旗下的RiskView是資訊安全軟體供應商，致力於發展最符合台灣企業組織需求的網路安全解決方案。我們正在改寫資安防禦的規則，協助客戶在日益嚴峻的網路威脅中，不只能全身而退，更能提前部署、即時偵測，達到100%安全防護。

RISKVIEW