semperis

目錄管理服務保護器

業界最全面的 Active Directory 威脅偵測及應變平台。

一個讓您放心的平台。Semperis 目錄服務保護器（DSP）是一個全方位平台，持續監控 Active Directory 和 Azure Active Directory 的暴險指標、偵測進階攻擊，並啟用快速應變。

- 阻止攻擊者存取內部部署的 AD 和 Azure AD
- 自動化威脅防護和應變
- 持續驗證您的 AD 安全性狀態

如果您的AD不安全，那麼就沒有什麼是安全的。

內部部署和雲端中的商務應用程式依賴 Active Directory 和 Azure Active Directory，因此它是您 IT 基礎結構的關鍵部分。但其不斷變化、數量龐大的設定，加上日益複雜的威脅類型，保護 Active Directory 非常困難。許多攻擊從內部部署開始，後移至雲端，為確保混合式系統的安全帶來額外挑戰。Semperis 目錄服務保護器（DSP）持續監控 Active Directory 和 Azure Active Directory 的暴險指標，並提供內部部署和雲端中活動的單一檢視。

主動保護 AD 和 Azure AD 免於網路攻擊。

比攻擊者更早掌握 AD 和 AZURE AD 漏洞

攻擊者針對混合式 AD 系統中的弱點，利用內部部署 AD 的弱點進入環境，然後移至線上的 Azure AD 速度愈來愈快。

→ DSP 持續監控威脅 AD 和 Azure AD 的暴險和危害指標——由 Semperis 公司威脅研究團隊所揭露。

消除混合式 ACTIVE DIRECTORY 的盲點安全性

攻擊者使用強大的駭客攻擊和探索工具，在混合式 Active Directory 內部建立後門程式並設立持續性存取權——避開傳統 SIEM 解決方案的偵測。

→ DSP 使用多個資料來源——包括 AD 複製流——以擷取逃過代理程式型或記錄型偵測的變化。

啟用快速復原

入侵者和惡意系統管理員可迅速對您的系統造成嚴重破壞，規模難以透過人為介入進行有效監控和補救。

→ Semperis 的 DSP 提供一個整合儀表板，顯示內部部署的 Active Directory 和 Azure Active Directory 中的惡意變更，讓您能在攻擊者襲擊之前縮小安全性缺口。

semperis

混合式身份系統已成為攻擊的對象。

混合式身份系統，即結合Active Directory和Azure Active Directory的系統，越來越普遍地被組織採用以部署本地資產和雲服務最佳組合。但是，隨著這種靈活性的增加，複雜性也隨之而來 – 特別是在Microsoft環境下管理混合身份安全性方面。

保護Active Directory與保護Azure Active Directory需要不同的方法：工具、流程和威脅都是不同的。

在混合式場景下，攻擊者的潛在攻擊面會擴大。

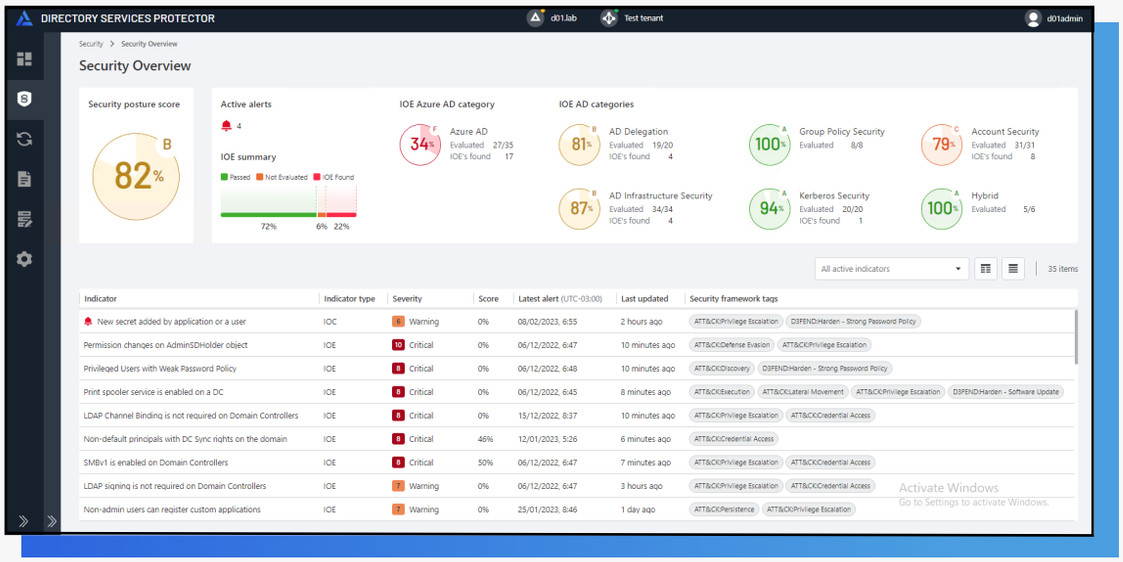
現在攻擊往往從本地開始，然後轉移到雲端，就像SolarWinds攻擊；或者從雲端轉移到本地。管理混合身份系統的安全性是複雜的。由於Azure AD是安全拼圖的關鍵部分，採用混合身份模型的組織必須防範無數潛在的入口點。Directory Services Protector通過追踪Azure AD變更、在Azure AD中手動回復惡意更改以及對環境的混合檢視來保護混合AD環境免受網路攻擊。這有助於比對本地AD和Azure AD中的更改。

透過Directory Services Protector輕鬆追蹤AD和Azure AD的安全狀態。

清晰地傳達混合AD的整體安全狀態並管理AD和Azure AD的威脅偵測和回應：

- 檢視整體分數和各個安全類別的分數，包括AD帳戶安全、群組原則安全、Kerberos安全、AD委派、AD基礎架構、Azure AD和混合安全
- 深入瞭解特定的風險指標（IOEs）和威脅指標（IOCs）
- 使用優先排序的修復指南立即減少AD的攻擊面
- 追蹤和手動回復在Azure AD中的惡意更改
- 在單一的混合檢視中視覺化並相關聯Azure AD和本地AD中的變更
- 偵測會繞過傳統偵測(基於日誌和事件監控，例如SIEM)的進階AD攻擊

針對本地AD及Azure AD的漏洞評估、變更追蹤及變更回復的解決方案



semperis

漏洞評估
持續監控可導致混合式 AD 環境遭受安全性危害的「暴險指標」。利用來自安全性研究人員社群的內建威脅情報。

自動補救
建立敏感 AD 和 Azure AD 物件和屬性變更的稽核通知，並有自動復原選取變更的選項。

防竄改追蹤
即使安全性記錄被關閉、記錄被刪除、代理程式被停用或停止運作，或變更被直接插入 AD 或 Azure AD，也能擷取變更。

即時發現和修復
使用 Semperis DSP 的線上資料庫，在兩分鐘或更短的時間內，發現和修復不需要的混合式 AD 物件和屬性變更。

細微回復
還原對個別屬性、群組成員、物件和容器的變更——並且至任何時間點，不僅僅至之前的備份。

鑑定分析
識別可疑的變更，隔離遭入侵帳戶所進行的變更等等。使用 DSP 資料來支援數位鑑定和事件回應（DFIR）作業，以追蹤事件的來源和詳細資料。

SIEM 代理程式擴充
以獨特整合消除安全性資訊和事件管理（SIEM）系統中的盲點。

代理
利用健全的角色型存取控制（RBAC）和豐富的網路使用者介面，為系統管理員提供針對其特定控制範圍的檢視和還原功能。

強大的報告
使用 AD 專家所建立的內建報告，以深入了解您的混合式 AD 環境的運作、最佳做法、合規性和安全性等。根據精確的 LDAP 和 DSP 資料庫查詢建立自訂報告。

即時通知
當混合式 AD 環境中發生與作業和安全性有關的變更時，透過電子郵件通知接收警示。

POWERSHELL 支援
使用 DSP PowerShell 模組將流程自動化，並將 DSP 操作和管理整合至現有的工具組。

支援法規遵循
Semperis 公司 DSP 為主要法規和架構提供預先設定的規範模組，讓報告自動化。

- PCI
- HIPAA
- SOX
- GDPR

持續的安全性驗證
自動監控對抗由設定偏移造成的安全性狀態迴歸——隨時間累積而遭入侵的組態設定，讓您容易受到攻擊。

追蹤 AZURE AD 變更
在 Azure AD 模組適用的 DSP 中使用近即時變更追蹤，以監控角色指派、群組成員資格和使用者屬性的變更。

讓混合式 AD 安全性變得可見
利用 Azure AD 模組適用的DSP，輕鬆檢視來自 Azure AD 的變化，並使用混合式檢視讓內部部署 AD 和 Azure AD 之間的變化產生關聯。

您的混合式 AD 環境是否安全？

Semperis Purple Knight 安全性評估工具使用者的安全性分數顯示，組織未能關閉混合式 AD 系統中的安全性缺口，平均分數為 61%——勉強及格——讓他們容易受到從內部部署開始並移至 Azure AD、數量日增的攻擊。

Semperis在應對針對Active Directory和其他基於身份的網路攻擊方面擁有無與倫比的經驗。Semperis的解決方案重視人員和流程的最佳實踐和指導，不僅僅關注他們的優秀技術以應對客戶的挑戰，這使他們與競爭對手有所區別。

Semperis
IT 防衛協調流程

5 ★★★★★

資料來源：Gartner Peer Insights 平台

info@semperis.com
www.semperis.com

Semperis 公司總部
221 River Street 9th Floor
Hoboken, NJ 07030

+1-703-918-4884

semperis iSecurity The Hub of Security Innovations

marketing@isecurity.com.tw
www.isecurity.com.tw

數位資安系統股份有限公司 11493
台北市內湖科技園區堤頂大道二段293號8樓

+886-2-7702-1088

Microsoft 合作夥伴
企業雲端聯盟
Microsoft 加速器校友
Microsoft 共同銷售

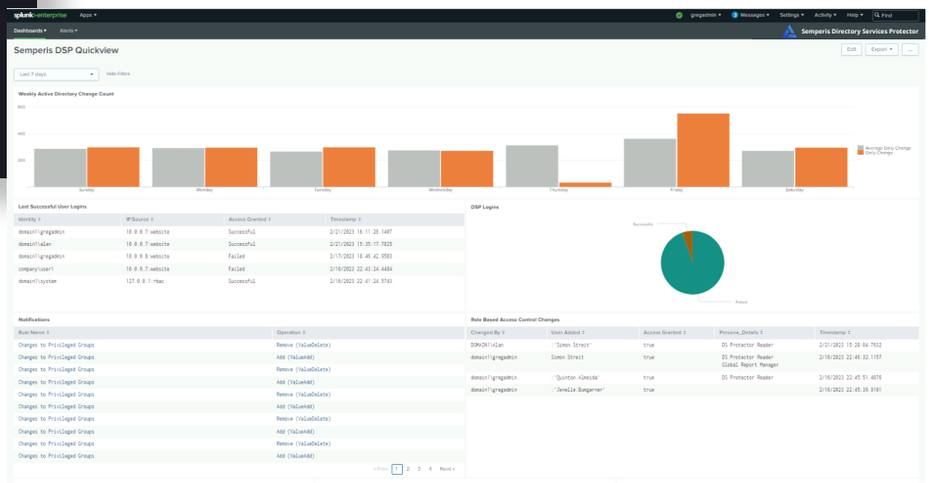
讓您的SIEM恢復可見性

越來越多的攻擊規避安全性稽核

不同於過往的追蹤工具，僅依賴於安全日誌和位於每個網域控制器的agent，Semperis DSP 監控多個資料來源，包括Active Directory複寫串流。AD複寫串流是捕捉每個變更唯一可靠的方法，無論攻擊者如何試圖隱藏他們的蹤跡，所作的變更一定會透過複寫串流複寫到其他DC上。Semperis DSP會將可疑的AD更改帶有有意義的上下文轉發到您的SIEM系統中，從而大大減輕安全分析師的負擔。您可以使用針對Microsoft Sentinel、Splunk和其他SIEM和SOAR工具的預定義警報，並為SecOps工具和像ServiceNow這樣的ticket系統建立自定義警報。

開箱即用，現成的SIEM整合

DSP透過現成的整合，簡化了威脅檢測和回應，將之前隱藏的AD安全資料以可用、熟悉的視圖呈現給Sentinel和Splunk使用者。



DSP將AD安全資料轉換成Splunk熟悉的檢視方式

splunk> Microsoft Sentinel