校園網管研習 / 教職員資安分享

特權使用者監控（PUM／UAM）導入概念

用 Syteca 守住校園網路裡，那些「權限最大、卻最少被看見」的帳號

開場情境

這個情境，你一定不陌生

委外廠商工程師

用「萬用」管理員帳號連進校務系統維護，做了什麼、改了什麼，事後完全說不清楚。

資訊組長離職交接

離職前用的管理員密碼到底有沒有改？他在離職前一週做過什麼操作？沒有人知道。

系統異常後追查

教務系統資料被異動，要回溯「誰、何時、做了什麼」，卻只有事後的結果，沒有過程紀錄。

這些，都是「特權帳號」缺乏監控所造成的盲區。

今天的 30 分鐘

議程

01	**為什麼校園需要這個** 資安現況數據 + 校園 IT 環境的特殊痛點	5 分鐘
02	**基礎概念建立** 什麼是特權帳號？監控 ≠ 偷窺，怎麼界定？	4.5 分鐘
03	**Syteca 核心功能** 看得到、攔得住、查得回去三個層次	9.5 分鐘
04	**校園情境與導入** 實際應用場景、部署方式、下一步行動	7 分鐘

教育機構，其實是熱門攻擊目標

2,297 次 / 週

全球教育機構平均每週遭受攻擊次數

Check Point, 2022

365 萬美元

教育產業單次資料外洩的平均成本

IBM Security, 2023

- 校園系統存放的，是學生與教職員的個資、學籍、成績、健康與財務資料
- 攻擊者看重的不只是「錢」，也包含資料量大、防護資源相對有限

校園 IT 環境的四個現實

網管人力極度有限

往往一人或兼任身分要扛起全校系統，沒有專責資安團隊全天候盯著日誌。

委外廠商頻繁進出

校務系統、設備維護常委外，廠商工程師持有高權限帳號，行為難以掌握。

系統新舊並陳

教育雲、學籍系統、自建伺服器、教室電腦並存，管理介面與紀錄格式不統一。

合規壓力上升

個資法、校安通報、教育部資安規範要求留存軌跡與舉證能力，但人力跟不上。

什麼是「特權使用者」？

能存取系統核心、修改設定、查看大量敏感資料的帳號，就是特權帳號——權限越大，一旦出問題影響範圍就越大。

資訊組長／網管教師

全校網路設備、伺服器、AD 帳號的管理權限

委外維運廠商工程師

校務系統、機房設備的遠端維護存取權

教務 / 學籍系統管理員

可查看、修改全校學生個資與成績資料

雲端服務管理帳號

教育雲、Office 365 / Google Workspace 管理者

Syteca 同時也能監看一般使用者與外部使用者，但特權帳號永遠是風險最高、最該優先掌握的一群。

監控 ≠ 偷窺：兩者的關鍵差異

常見的誤解

- 「裝了就是要抓人小辮子」
- 個人隱私一定會被赤裸看光
- 老師、職員會覺得被針對、不信任

PUM／UAM 的實際定位

- 聚焦在「高權限操作」，不是逐字看每個人的私事
- 預設可將個資去識別化，事件發生才還原查證
- 目的是留下「可舉證的軌跡」，保護學校也保護當事人

Syteca 是什麼？

一套「使用者活動監控（UAM）+ 特權存取管理（PAM）」平台，讓你看得到誰在做什麼、攔得住風險動作、查得回完整過程。

跨平台支援

Windows、macOS、Linux / Unix、VDI（VMware、Citrix）

部署彈性

On-premise、Azure、AWS，或 SaaS 雲端版本

上線速度

最快 20 分鐘內可完成基本部署並開始監看

產業認可

Gartner、KuppingerCole 報告均有列名，已用於教育機構

看得到

完整可視化使用者行為

攔得住

即時告警與自動回應

查得回

錄影存證、可供稽核

第三段　核心功能（一）看得到

完整看見特權帳號在做什麼

螢幕畫面操作

瀏覽的網址

開啟的應用程式

鍵盤輸入 / 剪貼簿

視窗標題

檔案上傳行為

USB 裝置連接

Linux 指令執行

不論是不間斷連線監看，或設定條件（如輸入特定關鍵字）才觸發錄製，皆可彈性配置。

異常發生時，即時告警與自動回應

即時規則式告警

依預設規則偵測可疑行為或違反政策的操作，第一時間通知。

自動／手動回應

可彈出警告訊息、強制中斷連線，或直接終止異常程序。

離線仍持續記錄

即使與伺服器斷線，仍會在本機持續記錄，恢復連線後同步。

可與 SIEM（如 Splunk）、工單系統（ServiceNow）整合，串接學校既有的通報流程。

第三段　核心功能（三）查得回

事後能完整回放、禁得起稽核

Session 完整錄影

RDP / SSH 連線與操作畫面全程錄製存檔，可回放查證每一步操作。

一鍵搜尋追蹤

依使用者、時間、關鍵字快速定位可疑片段，大幅縮短調查時間。

不可篡改格式匯出

需要對外提供證據（如報案、司法調查）時，匯出格式具備防竄改特性。

完整稽核軌跡

符合個資法、教育主管機關對留存軌跡與舉證能力的要求。

監控的同時，如何保護師生與職員隱私？

原始監控資料

畫面、輸入、操作紀錄

→

預設去識別化

個人身分資訊自動遮蔽

→

正常情況下

管理者僅看得到匿名化結果

唯有發生安全事件，經授權後才能解密還原為真實身分資料，作為調查依據。

這個機制讓校方同時做到「落實監督」與「保障教職員個人資料權利」，呼應《個人資料保護法》最小化與目的限縮原則。

放到校園裡，可以怎麼用？

委外廠商遠端維護

廠商工程師遠端連線維護校務系統或機房設備時，全程錄影留存，維護結束即可確認操作範圍是否如約定。

資訊組值班交接

多位網管教師共用管理帳號時，仍可區分「誰在哪個時段做了什麼」，交接更清楚，問題歸屬不再含糊。

教育雲／雲端服務帳號

教育雲、Google Workspace / M365 管理者帳號的關鍵操作（如大量帳號異動）受到監看與告警。

導入會很複雜嗎？

最快 20 分鐘可上線

輕量化代理程式（agent），安裝後即可開始監看，不需大規模改造現有架構。

部署方式彈性

可選擇校內機房 On-premise，或 Azure / AWS / SaaS 雲端部署，依學校資源彈性選擇。

對效能影響極小

在背景安靜運作，資料以優化過的影音與文字格式儲存，不拖慢教學與行政電腦。

常見部署模式

校內機房 On-premise

資料留在校內，掌控度最高

公有雲（Azure / AWS）

彈性擴充，適合多校共管

SaaS 雲端版

免維運硬體，快速上線

今天想留給大家的三件事

1 特權帳號（網管、廠商、雲端管理者）是校園資安最該優先掌握的風險來源

2 監控可以與隱私保護並存——去識別化機制讓「落實監督」不等於「侵犯隱私」

3 工具的價值在「事後查得回去」：完整錄影與軌跡，是出事時最重要的舉證依據

Q&A ／ 歡迎交流與提問

延伸資源：syteca.com/en/solutions/privileged-user-monitoring