什麼是OT資安？

OT Security Lesson 1: Top Threats to Industrial Control Systems

Forcepoint

OT資安的定義、解釋和探討

OT資訊安全定義

據Gartner稱，營運技術（OT）是透過直接監視，和/或控制企業中的實體設備、流程和事件，來檢測或引起更改的硬體和軟體。OT在諸如SCADA系統的工業控制系統（ICS）中很常見。在關鍵基礎設施領域中，OT可用於控制電站或公共交通。隨著這項技術的發展和與網路技術的融合，對OT安全的需求，呈指數成長。

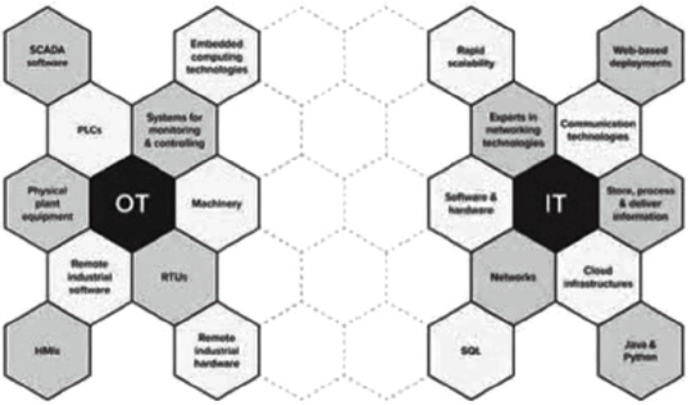
IT-OT的融合

多年來，工業系統依賴於專有協議和軟體，由人為人工管理和監視，並且與外界沒有任何聯繫。因此，對於駭客來說，它們是微不足道的目標，因為沒有網路介面接口可以攻擊，也沒有獲得或破壞的介面接口。滲透到這些系統的唯一方法，是獲得對終端的實體入侵，這絕非易事。OT和IT整合很少，並且沒有處理相同類型的漏洞。

今天，這是一個截然不同的故事，因為我們看到越來越多的工業系統上網，以交付大數據和智慧分析，並透過技術整合採用新的

功能和效率。IT-OT的融合，為組織提供了工業系統的單一視圖，以及流程管理解決方案，這些流程管理解決方案，可確保在正確的時間，以最佳格式，將準確的資訊傳遞給人員、機器、交換機、感測器和設備。當IT和OT系統協同工作時，可以發現新的效率，可以對系統進行遠端監控和管理，組織可以實現與管理IT系統，相同的安全優勢。

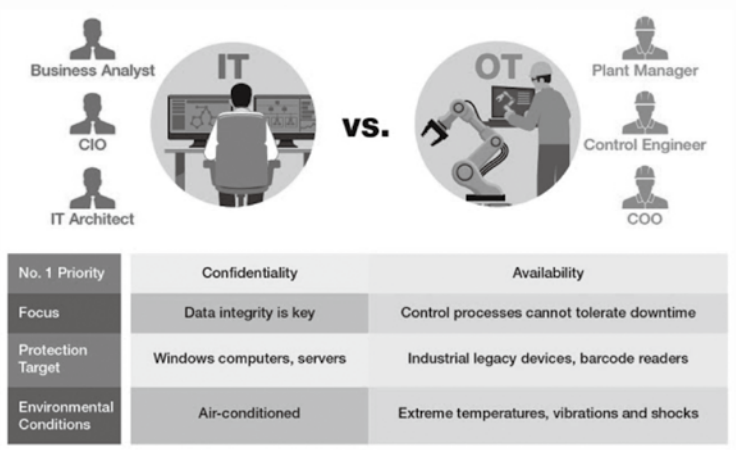
從封閉系統到開放系統的這種轉變，產生了許多新的安全風險，需要解決。



OT的資安為何重要？

隨著工業系統之間的聯繫越來越緊密，它們也更容易受到攻擊。工業設備的高成本，以及攻擊可能對社區和經濟造成的破壞，是尋求保護其工業網路的組織的關鍵因素。添加舊設備，可能禁止對設備進行任何修改的安全法規，以及要求將敏感數據提供給第三方的合規法規，你將面臨很大的挑戰。

好消息是，可以保護工業網路而不會中斷營運，或冒違規風險。透過使用可以完全看到的，網路控制流量的解決方案，並建立正確的安全策略，你可以製訂有效的OT策略，以保護你的流程、人員和利潤，並顯著減少安全漏洞和事件。



No. 1 Priority	Confidentiality	Availability
Focus	Data integrity is key	Control processes cannot tolerate downtime
Protection Target	Windows computers, servers	Industrial legacy devices, barcode readers
Environmental Conditions	Air-conditioned	Extreme temperatures, vibrations and shocks

保護當今的工業網路

更好的消息是，工業環境通常比IT環境，具有較低的流量。許多流量在確定的端點之間傳播，因此，與IT網路上生成的流量相比，可以更輕鬆地對其進行基線和盤點。使用監視和分析工具，可以幫助辨識，並防止未經授權的更改，和其他異常現象，這些異常或異常現象，可能預示著攻擊已全面展開，或處於初始階段。

新一代的防火牆（NGFW），提供了策略驅動的集中式管理，使你可以完全控制工業環境。

無論你需要分析成千上萬的端點，還是更小的網路，都可以動態配置新一代的防火牆來查找意外，或未經授權的流量，以及工業系統上其他。