英國 Dounreay 核能機構使用 OPSWAT MetaDefender 確保整體檔案安全

Politico最近的一份報告指出，「根據美國能源部發布的數據，今年上半年美國電網遭受的攻擊增加，共有 94 起物理和電腦化的威脅或攻擊事件。最新數據再次證明，針對電網基礎設施的攻擊正逐步上升。」

對於世界各地核能設施的安全管理人員來說，這樣的消息特別值得擔憂。因為這些設施若受到駭客、民族國家或恐怖組織的攻擊，可能會對員工和周圍社區造成危險的後果。這就是為什麼世界各地的安全專業人員，都在尋求最佳的網路安全解決方案，以確保核能設備的數據網路採用最高級別的網路安全。

在這方面，位於蘇格蘭的 Dounreay Site Restoration Limited （DSRL） 核能機構正在樹立最佳的典範。這五十年來，透過三個核子反應爐原型，Dounreay 一直處於英國核子反應爐發展的最前線。然而，經過半個世紀的服務，該設施正進行退役。

DSRL 是受英國核退役管理局（NDA）管轄的營運公司之一，NDA 是一個負責監督英國核能設施退役和清理工作的政府機構，該機構已採取大膽的措施加強其網路抵禦網路威脅之能力。

識別風險並實施解決方案

NDA 發現檔案有被帶入 Dounreay 實體隔離網路的風險，並實施風險緩解計劃，其中包括購買 13 台 OPSWAT Kiosk（每間營運公司兩台）作為試點項目的一部分。

Dounreay 購買了多款 OPSWAT Kiosks，包括 K1000 系列和 K3000 系列型號，以提供更好的跨域通訊，並授予第三方對掃描檔案的存取許可權，來防止網路攻擊並確保所有檔案的安全。這些 Kiosk 目前已連接 Dounreay 的 IT 網路，讓第三方在進入 Dounreay 網路之前需要先掃描他們的 USB 設備。

應對舊系統所帶來的挑戰

在採用 OPSWAT 技術之前，Dounreay 依靠過時的“Sheep Dip”系統來確保檔案安全，並面臨重大挑戰：

- 單一的防病毒引擎會帶來巨大的問題，因為單一的防病毒引擎使用單一的演算法，無法檢測不同類型的威脅。這就是為什麼需要多個防病毒引擎來最大化威脅檢測。
- 員工不得不手動使用「Sheep Dip」系統來掃描檔案。
- 驗證檔案需要幾天時間才能完成。
- 難以消化大型檔案和多個檔案。
- 該系統不可審計。

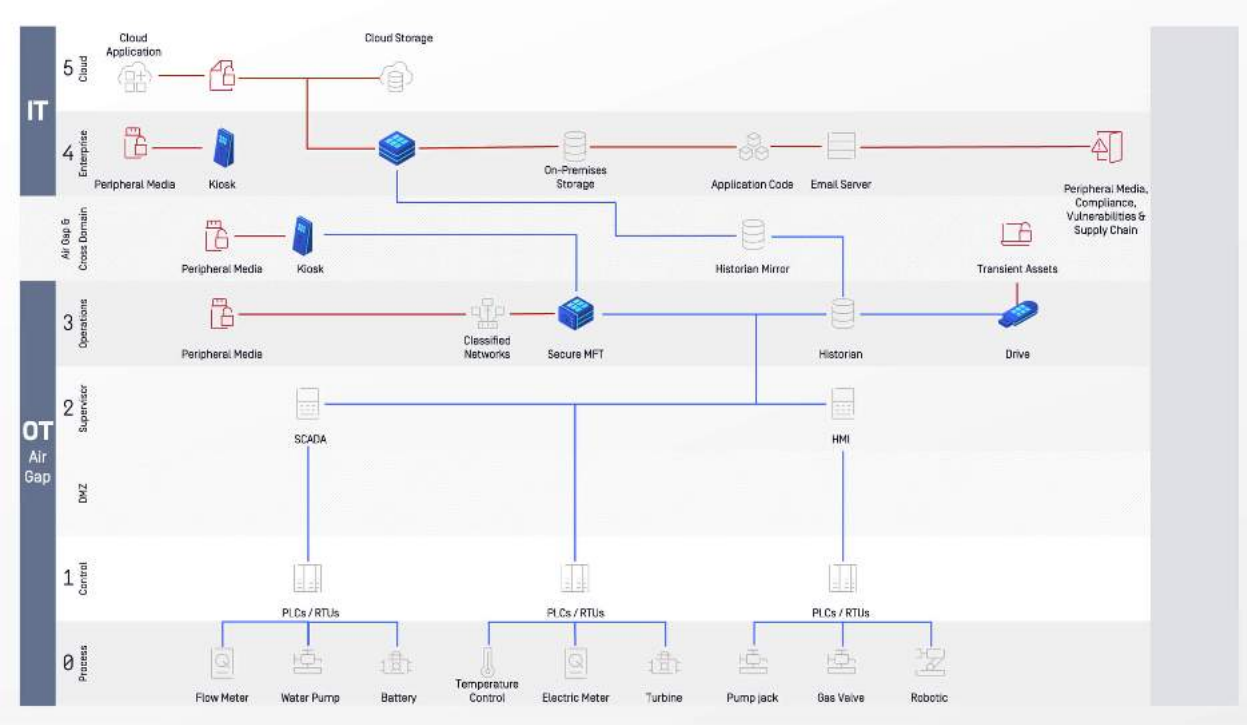
OPSWAT 技術堆疊解決方案

Dounreay為了增強其 IT 和 OT 系統的進階檔案安全，採納了 OPSWAT 的技術堆疊解決方案，正是為了其超越傳統防毒和端點安全解決方案的能力。已部署的解決方案包括MetaDefender Core, MetaDefender Kiosk （K1000 和 K3000 系列）， MetaDefender Drive 和 MetaDefender Managed File Transfer.

這些領先業界的解決方案，共同為 Dounreay 提供了一個完整的檔案安全系統，並打造了一條能供全球能源供應商，以及核能設施為確保檔案安全可以遵

循的路徑。該解決方案也使得 DSRL 符合旨在保護歐洲公民的隱私和個人數據的《通用數據保護條例》（GDPR）。

DOUNREAY SITE 資深安全經理理查·貝瑞表示：「我們需要確保在資料傳輸的過程中設有安全屏障，才能使得我們能夠安心地傳遞、分享、接收或提供資訊……OPSWAT 已成為對付特別艱鉅之技術挑戰時的可靠解方。」



提供更好的結果

OPSWAT 的技術解決方案為 Dounreay 提供了許多他們以前的系統無法提供的關鍵優勢：

- 使用 OPSWAT 多防毒引擎掃描技術，同時使用 16 種不同的防病毒引擎進行檔案掃描，顯著提高了威脅檢測率。正如 Dounreay Site 的 CSA Alan Taylor 所解釋的，「我認為進行多防毒引擎掃描很重要，因為不是每個引擎都能檢測到每一個惡意軟體或惡意檔案。透過多個引擎的廣泛檢測，我們可以確信檔案已經被完整、正確地掃描過。」

- Dounreay 現在可以有兩種選擇，來從第三方上傳媒體到他們的網路上。「他們可以使用互聯網將數據直接上傳到 Dounreay's OPSWAT 環境，然後對其進行掃描，並傳送到他們的公司網路」，Taylor 繼續說道：「他們也可以透過 MetaDefender Kiosk 實體的訪問網路，第三方或員工可以將可移動媒體輸入，掃描數據，然後上傳到企業網路。」

- Taylor 繼續解釋說：「我們還有另一個由OPSWAT提供的解決方案叫做 MetaDefender Drive，在第三方筆記型電腦進入我們的網站之前，我們能夠進行全面掃描，確保它們不會接觸到我們的任何基礎設施。」這可以防止外部供應商引入任何惡意軟體到該網站。

- 透過在非軍事區 （DMZ） 使用 MetaDefender Managed File Transfer ，第三方現在可以提前上傳大型或多個檔案並進行掃描。乾淨的檔案可以從外部網路傳輸到內部網路，當第三方需要使用網站時，這些檔案已經在網路上可供使用。

- 能夠通過非軍事區（DMZ） 安全地傳輸到網路中，已經大大加快了檔案驗證過程。掃描現在可以在幾個小時內完成，而不是三到五天。

- 有了 OPSWAT 部署後，Dounreay 已從單純阻擋可移動媒體，轉變為可以處理掃描和保護可移動媒體的完全整合解決方案。

- OPSWAT 的技術最終能夠顯著地提高檢測、效率和檔案保護能力。

DOUNREAY SITE 網路安全專家邁克·裡奇表示「僅使用一個防毒引擎來驗證特定檔案並不理想。有了我們目前與 OPSWAT 所使用的解決方案，每個檔案都會被 16 個不同的防毒引擎掃描。」

將安全作為應對未來威脅的優先事項

能源供應商和核能設施管理者需要明白，他們很有可能在未來的某個時候遭受網路攻擊。然而，抵禦此類攻擊的關鍵，是立即採用正確的技術解決方案，並透過經適當培訓的人員來構建關鍵基礎設施的韌性，以便在攻擊來臨時，擁有應對計劃，可以有效和高效地處理攻擊。

Alan Taylor 解釋說：「網路安全需要被視為是推動者，而不是阻礙者，提供使企業能夠執行其日常業務的系統對我們來說至關重要。」「Barrier 和OPSWAT提出的現代化安全控制方案正是我們所需要的」Mike Richie 補充道。

Alan Taylor 繼續說道：「OPSWAT對我們來說是一個重要的基礎設施，讓我們能夠進行日常業務。它使我們處理可移動媒體的方式，從非常老舊傳統的方案轉變為現代化的解決方案……現在，我們解決方案已經從單純阻擋可移動媒體，到擁有獨立系統，再到擁有可以掃描和保護可移動媒體的全面整合解決方案。」

網路攻擊總會發生，但正如 Dounreay 的安全專家所證明的，正確的技術可以提供堅實的防禦，以防止此類攻擊成為災難性事件。

瞭解 OPSWAT 的創新解決方案可以如何確保您的關鍵基礎設施安全，立即諮詢專家。