paloalto NETWORKS | CORTEX BY PALO ALTO NETWORKS

CORTEX CITY

SOC基拉 VS FUTURESOC的較量

第 01 期

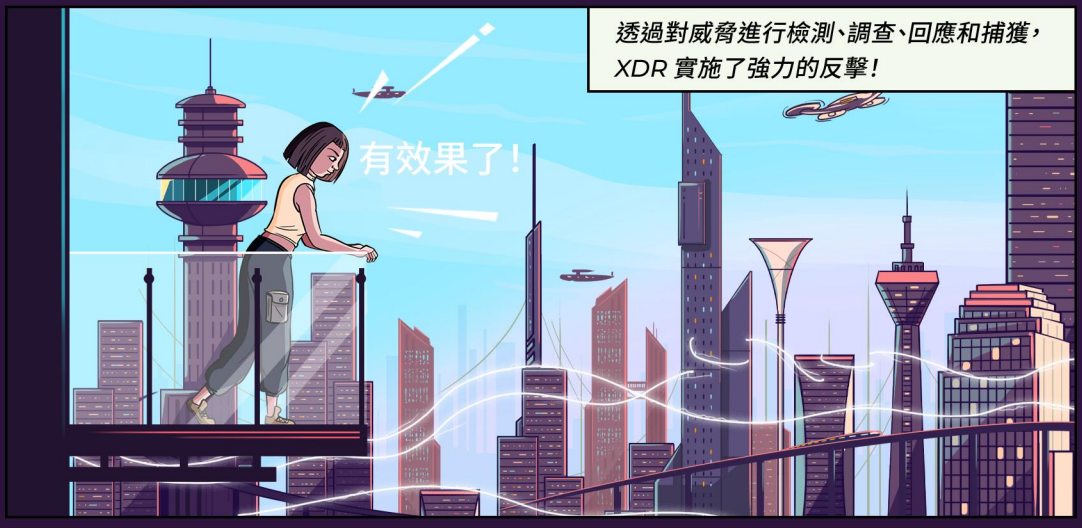

在一個清新、明朗的早晨，Cortex City 熙熙攘攘，大家又開始了新的一天。
不知從何而來的危險濃霧籠罩了整座城市，並將攻擊面暗藏其中。這只能是…
!!


SOC基拉
是 SOC 基拉!SecOps 團隊的死敵!
慧娜,那是什麼?
?
網路攻擊
到處都是警報!
團隊傳統的端點保護系統開始崩潰!無法收集和聯接不同來源的資料,對威脅進行檢測、調查和回應。

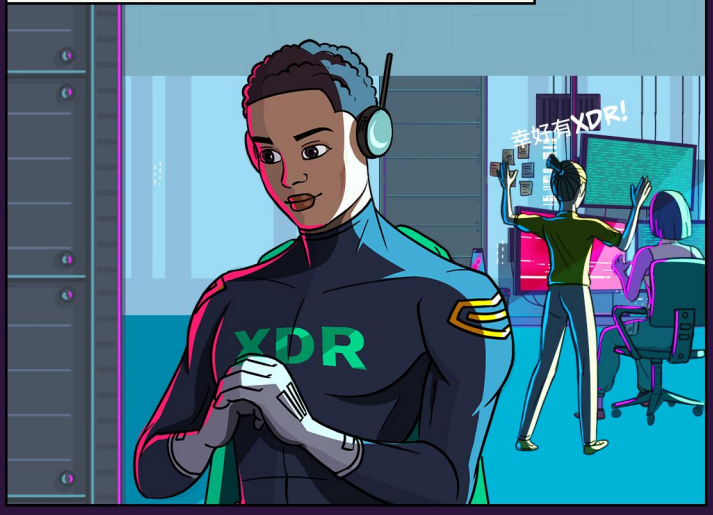

於是，慧娜快速呼叫最好的團隊！
她想求助抵禦這次網路攻擊…
FUTURESOC,
我們急需你們的幫助！
在 FutureSOC 總部…
XDR
該你出場了！
XDR
XDR 立即採取行動，監控網路是否有任何入侵跡象並且迅速確定攻擊源。
XDR

他對端點進行了分析，找到攻擊點。然後給出了整座城市的攻擊點視圖。之後，他將相關的端點遙測和事件數據發送給 BigTech Inc.。

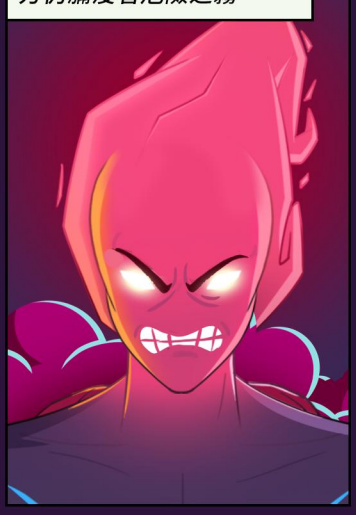
透過對威脅進行檢測、調查、回應和捕獲，XDR 實施了強力的反擊！



他在檢測、回應和擴展到雲端環境的實力超群，爲慧娜的團隊提供了抵禦攻擊所需的資訊。



可別小看 SOC 基拉，他並沒那麼好對付！城裡很多地方仍瀰漫著危險之霧…



慧娜和 XDR 呼叫 FutureSOC 團隊，尋求進一步的保護。

Xpanse 搶在 SOC基拉之前找到了漏洞，並不斷尋找資產、進行持續監控，以主動降低風險。同時，將資產情況與由外而內的映射交聯，然後…


她把所有資訊彙集在一起，瞭解遭曝露在新攻擊之下的原因，及攻擊展開的方式。此時，危險之霧已被驅散殆盡！
Xpanse
XSOAR 也前來助 Xpanse 一臂之力，將危險徹底清除！
XSOAR
Xpanse
XSOAR

強力調查與回應

自動回應未來事件

跨部門協調行動

人工任務自動

與所有SOC工具相容

XSOAR 可立即從慧娜的工具中提取警報，獲取有關端點、用戶、主機、漏洞、惡意軟體和攻擊者情報的資訊，以即時進行遏制。

啟動

XSOAR

XSOAR 驅散了危險之霧！整體攻擊面最終遭到減少和清除，這讓慧娜及其團隊得以重新監控全局！

呼！

擊退 SOC 基拉的攻擊，一切恢復如初後，XSOAR 向慧娜及其團隊說明如何增加自動化武器，以及抵禦供應鏈攻擊、國家級攻擊和零日攻擊的方式。

FutureSOC 團隊則幫助慧娜的團隊確定傳入警報的優先級別，並簡化其工作流程，以透過人工智慧和機器學習加快修復速度。

他們之所以能取得成功，祕訣在於 Cortex 的全套組合產品。慧娜及團隊藉助端點安全、檢測、回應、自動化和攻擊面管理，不僅減少了繁忙的工作時間，甚至可以悠閒享受晚間和週末時光！

總結

利用網路、雲端和身份資料，以及互聯網曝露資產風險的單一資料源來準確檢測威脅，慧娜及其團隊甚至可以發現最隱密的 SOC 基拉攻擊，並藉助 SOC 的全部力量進行回應。

FutureSOC 團隊證明，只要採用恰當的安全技術，即使是 SOC 基拉最新的威脅也能成功抵禦。

使安全事件具有全面的可見性，並採取協調一致的回應，也可以主動防禦和保護網路和資產，打造美好的未來。

我們歡迎你現在開始未來 SOC 之旅！和 Cortex 一起應對雲原生世界不斷變化的需求。

請點擊鏈接要求示範:
www.paloaltonetworks.tw/cortex/request-demo