ExtraHop

安全

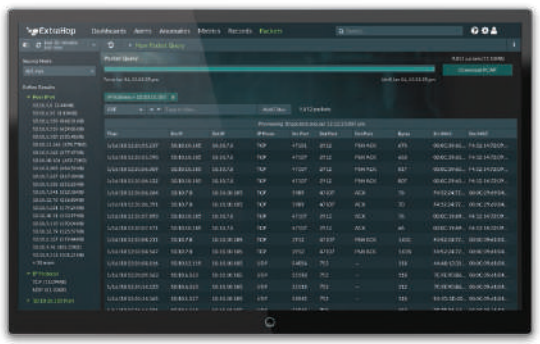
偵測一切 自動調查
減少威脅停留時間 進化資安能力

在 ExtraHop，我們創造了一種全新方法，分析網路上發生的每一個數位交易，將該洞察轉化為資安團隊的可付諸行動情報。 我們稱之為Wire data，也就是即時分析的決定性來源。

無與倫比的企業可視性

ExtraHop 使資安團隊能夠全面查看本地端及分點端、公有雲以及混合環境（甚至是加密環境）的通訊。

- 自動探索與分類公司資產，達到全面檢視所有連接的設備
- 50個以上企業通訊協定的全面化的封包內容分析，具備深度與廣度
- 橫跨多個應用程式網路流量分析，自動將內容上下文比對之能力，進而達到網路流量自動關聯及相依性對應。



進階行為分析

憑藉 ExtraHop 的即時分析與 Wire data-driven 網路異常偵測，您可以發現在整個企業網路中任何地方發掘的異常的行為模式。

- 具有東西向網路流量分析的進階威脅偵測
- 適用於勒索軟體、身份驗證等的即用型解決方案
- 與 Splunk、Phantom、Palo Alto、ServiceNow 等整合

自動化調查

只需點擊幾下，ExtraHop的優先分析工作流程即可將您從問題轉移到相關封包，節省故障排除時間並啟用即時洞察與快速威脅功能

- 始終啟用的機器學習在異常擊中纜線的瞬間即自動顯現異常
- 開放式且可擴展的平台，因此您可以使工作流程自動化
- 無縫深層探究，從偵測到的事件到所需的詳細資訊

ExtraHop

安全

安全分析
- 東西向流量分析
- 勒索軟體偵測
- 自動威脅獵殺
- 即時調整的自訂指標

法規遵循
- 個人識別資訊（PII）與明文傳輸
- 加密與密碼強度
- 能夠遵循《通用資料保護規章》（GDPR）
- 連續封包擷取

整合
- 安全資訊與事件管理（SIEM）與次世代防火牆（NGFW）
- 運用 Phantom、Ansible、Cisco Tetration、Moogsoft 已達到自動化的聯合防禦
- 運用 ServiceNow 或 Slack的事件回應

雲端
- 混合式資安監控
- 公有雲與私有雲的使用
- AWS API 整合

ExtraHop decrypts SSL and PFS traffic enhancing visibility

即時安全分析
ExtraHop使資安團隊能夠根據背景全面查看在其混合環境中所發生的所有交易。這使得網路成為最全面與高傳真的可用資料源，所有資料皆為即時性。

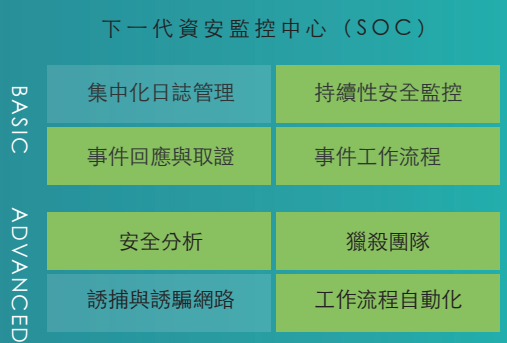
解密
ExtraHop 解密 SSL與PFS 流量，增強整個企業的可視性與背景，同時保持您的資安態勢。

機器學習
以線路資料驅動的ExtraHop 無人監督機器學習，能在您環境中的確切異常與威脅影響業務之前即先使其顯現。始終啟用並不斷學習，我們的機器學習服務隨著威脅出現與發佈新變體而逐步發展。

智慧型取證
ExtraHop 「全域搜尋與索引」提供資安洞察的立即存取權限，包括即時指標、交易紀錄以及用於取證回溯的封包。運用自動化工作流程與即時活動映射調查異常，按兩下即可將您從問題轉移到根本原因。

自動探索與分類
透過Agents與Log企圖覆蓋整個網路，但是事實上，並沒有辦法達到全面性的覆蓋到整個網路上，因此造成無法透視化的黑暗網路。ExtraHop 探索與分類在您的環境中通訊的所有端點。透過惡意節點、物聯網設備以及自攜設備系統在網路上通訊時將其識別，消除無法透視的黑暗網路。

整合與自動化
ExtraHop 與您現有的資安基礎架構整合，將線路資料串流到您的安全資訊與事件管理（SIEM），以進行關聯與自動事件回應，從而簡化您的資安工作流程。



關於 EXTRAHOP NETWORKS

ExtraHop 使資料驅動的IT成真。透過將即時分析與機器學習應用於所有數位互動，ExtraHop提供即時且無偏見的洞察。IT 主管首先求助於 ExtraHop幫助他們作出更快速、更明智的決策，從而提高效能、安全及數位體驗。只需詢問包括Sony、Lockheed Martin、Microsoft、Adobe及Google在內的全球數百家ExtraHop 客戶。

ExtraHop

520 Pike Street, Suite 1700
Seattle, WA 98101
877-333-9872 (voice)
206-274-6393 (fax)
info@extrahop.com
www.extrahop.com