Guided-SaaS NDR

您專屬的安全專家服務

安全團隊的管理者正面臨著雙線作戰。一方面，他們必須對其網路上的對手活動的可視化有所掌握。另一方面，他們也面臨著提高 SOC 效率且同時需減少分析師過勞的挑戰。 Gigamon ThreatINSIGHT™ Guided-SaaS NDR 縮小了 SOC 可視化差距並提供高真實呈現度的對抗式偵測，以達到快速且即時掌握消息的回應。 ThreatINSIGHT Guided-SaaS NDR 重新定義了基於 SaaS 的資訊安全實現方式，可確保安全團隊：

不再孤軍作戰
Guided-SaaS 提供 ThreatINSIGHT 安全分析師和事件應變專家在高風險事件期間獲得諮詢指導服務以減少過勞

不再困惑分心
Guided-SaaS 意味著只需要最少的維護以及免除偵測調整的負擔，從而提高 SOC/IR 效率和有效性

不再霧裡看花
Guided-SaaS 彌補在任何網路、設備與流量中有效識別敵人所需的 SOC 可視化落差

作為公司在面對網路上的對手活動的第一線處理者，安全維運和事件應變 (IR) 團隊應精通快速應變。然而，在兩線作戰中，成熟的安全團隊除了找尋了解 SOC/IR 工作重點的供應商，還需要設計不僅考慮到分析師的效率還有減輕過勞的解決方案。具體來說，理想的網路偵測和應變 (NDR) 解決方案應減輕：

可視化落差使得 SOC 搜尋就像霧裡看花

分析師需要的有效可視化正逐漸消失:

+ SIEM 和 EDR 存在可視化落差（設備、網路和流量）
+ 勞動力正逐漸轉變為在家工作 (WFH)
+ 加密流量快速增長，偵測難度提高

不必要的工具干擾

分析師正不知所措，因為:

+ 他們一直面臨著沒停過的誤報警
+ 耗時的偵測調整負擔落在安全團隊而不是供應商身上
+ 解決方案偵測暗藏著隱型成本（維護、更新、可視化優化）

孤軍奮戰的壓力

分析師常獨自面對高壓事件：

+ 告警缺乏有關下一步操作的上下文或指導
+ 供應商對產品專業知識的支援必須額外收費
+ 供應商對威脅知識或事件調查指導必須額外收費

69%

的 SOC 分析師認為缺乏對網路流量的可視化是 SOC 效率低下的首要原因[1]

可視化是基本需求

84%

的 SOC 分析師表示將 “誤告警最小化” 列為最重要的 SOC 任務（偵測微調） [2]

減少誤

告警本應是供應商的責任

43%

的 SOC 分析師表示維護、調整和提供安全工具更新是核心工作[2]

SecOps 的核心工作應該放在最重要的焦點。。。威脅管理

70%

的 SOC 分析師指出，由於常處於高壓環境，他們常常過勞倦怠[2]

SecOps 團隊急需信賴的專家顧問協助

ThreatINSIGHT 帶來的新科技

Gigamon ThreatINSIGHT Guided-SaaS NDR 是一個獨特且具有創新的 SaaS 產品，其中最重要的是包含了將人類智慧結晶與資訊安全專業人才經驗緊密結合，打造一個來用於偵測和回應攻擊者的平台。 Gigamon 技術成功管理 (TSM) 團隊聚集了具有豐富現場經驗的安全分析師和事件應變處理人員，他們與 Gigamon 應用威脅研究部門 (ATR) 一起合作，以確保 ThreatINSIGHT 客戶對於敵人手法具有應變能力。

減少 SOC 可視化落差

雖然 SIEM 和 EDR 提高了 SOC/IR 團在隊識別感染活動的效率，但設備、網路和流量的可視化落差仍舊存在。結果是，在試圖分類識別 MITRE ATT&CK 框架中描述的所有對手活動時，分析師都一無所知。
ThreatINSIGHT Guided – SaaS NDR 解決方案：

+ 提供接近封包級別metadata的可視化和記錄

任何設備、任何網路和任何流量，包括東西南北向流量和加密流量

+ 提供高真實呈現度的對抗式偵測

融合機器學習、行為分析和群眾外包威脅情報

+ 快速且全方位的分類和調查搜索功能

7 天、30 天或無限日數訪問豐富的網路metadata

+ 為分析師和事件處理人員提供有用建議

針對事件應變管理提供應對威脅的具體後續步驟

消除干擾

購買資訊安全解決方案後，安全專家應該能夠更專注於保護他們的組織。然而事與願違，資訊安全供應商提供的解決方案，實際結果與想像的往往有所差距。許多 NDR 解決方案在提供關注和訓練、解決方案熟練度、解決誤告警和執行偵測調整方面存在隱性的金錢成本和時間成本——這與當初它們被期待的價值存在落差。
ThreatINSIGHT Guided-SaaS NDR 包括專業知識從產品和威脅專家那裡消除干擾並確保：

+ 快速見效

Gigamon 技術成功經理 (TSMs) 提供部署、配置和運行狀況檢查協助以及持續的產品支援，以維持高客戶配合熟練程度

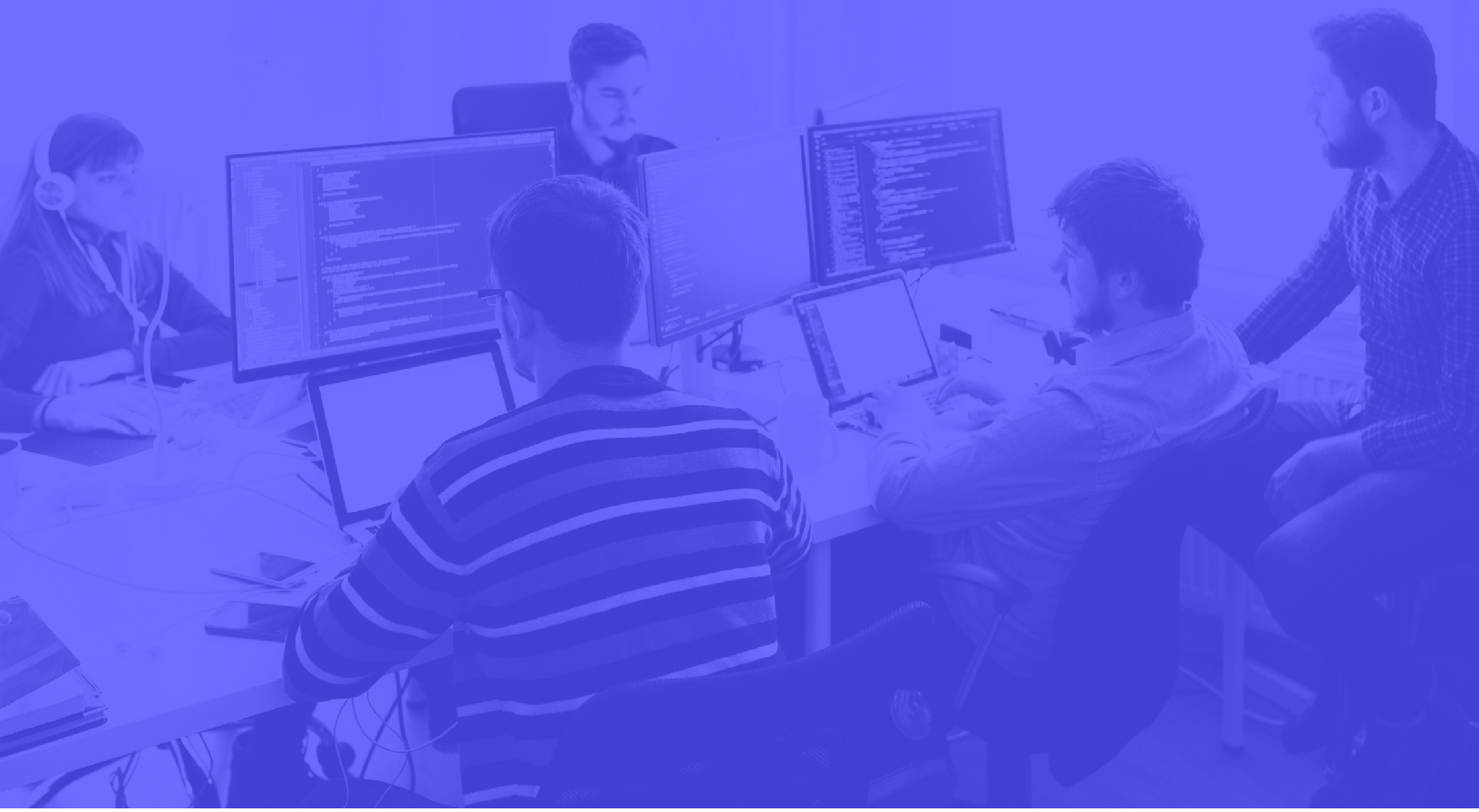
+ 最少的維護

Gigamon TSM 和 SaaS 維運團隊提供傳感器和流量診斷、完全託管的 ThreatINSIGHT 入口網站和自動化軟體更新

+ 使用 true-positive 偵測技術以減少偵測調整

ATR 對所有機器學習、行為分析和威脅情報偵測引擎進行持續的偵測調整和 QA

> 重要之事，絕不可受小事煩瑣牽絆. -佚名



面對網路攻擊事件對於 SOC/IR 分析師來說是一種高壓情況，他們正在與時間賽跑以保護他們的企業。由於對對手的意圖、策略、技術或程序資訊有限，並且在沒有外部建議的情況下工作，安全團隊通常必須孤單面對。外部威脅知識庫通常有限，而且安全工具傳統上只提供一般性建議。大多數工具並無提供必要的上下文和搜索功能，無法深入了解攻擊者入侵的系統、訪問的數據或獲得的身份和驗證資訊。這些限制使 SOC/IR 團隊難以制定全面的威脅應變計劃。

ThreatINSIGHT Guided-SaaS NDR 得到 Gigamon ATR 威脅研究人員和 Gigamon TSM 的技術支援，他們都是經驗豐富的安全分析師和事件應變處理人員，他們都專注於確保客戶處於最佳位置以面對及反擊對手

+ ATR 執行逆向工程、追踪和詳細說明對手的行為

建立關於對手的第一手知識，以強化 ThreatINSIGHT 和 TSMs

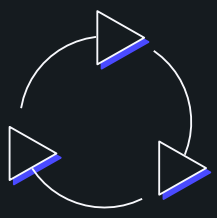
+ TSMs 客戶緊密合作，根據要求提供專家諮詢指導

在高壓關注工作期間共享威脅資訊和事件應變最佳作法和參考指南

ThreatINSIGHT Guided-SaaS NDR

專用定製化 NDR 科技

無與倫比的可視化
+
高真實呈現的對抗式偵測
+
快速、掌握資訊的應變



不須分心的 SaaS 管理

最少的維護
+
免偵測調整
+
自動化軟體更新

最重要的諮詢指導

威脅/對手知識資料庫
+
事件應變管理指導
+
分類和搜尋最佳作法

ThreatINSIGHT Guided-SaaS NDR

ThreatINSIGHT 提供了應有的 NDR。以事件應變處理人員為中心的解決方案，為事件應變處理人員提供:

+ 透過網路偵測和事件應變增強您的 SIEM 和 EDR，以完整 SOC 可視化三要素，分類識別 ATT&CK 框架中其他技術無法觀察到的威脅者行為，因此您的團隊不再只是霧裡看花
+ 提供免偵測調整的 NDR 技術和需要最少解決方案管理與維護的 SaaS 方式，您的團隊不再被干擾分心
+ 借助 Guided-SaaS 專業知識為您減輕安全分析師在高壓狀況下的負擔，讓您的團隊從此不再孤軍作戰

取得更多相關資訊請點擊 gigamon.com/threatinsight.

需要現場介紹請點擊 GIGAMON.COM/DEMO.

[1] Ponemon: Improving the Effectiveness of the SOC, 2020
[2] Ponemon: The Economics of Security Operations Centers, 2020

Gigamon®

全球總部
3300 Olcott Street, Santa Clara, CA 95054 USA
+1 (408) 831-4000 | www.gigamon.com