Netscout 威脅偵測平台

HIGHLIGHTS

- 用於快速檢測網路威脅和事件回應的創新平台
- 基於數據的可擴展專利ASI技術可提高分析的完整性，正確性和質量
- 提供安全分析和邏輯工作流程，以檢測，識別，驗證，調查和回應潛在的威脅和網路風險
- 直覺的工作流程，從高風險可視性深入到用於網路調查和主機調查的集中監控系統
- 可與大部分的SIEM平台做整合，實現了單一可視性平台分析方法
- 可與Netscout Arbor的指紋資料庫做整合

產品介紹

Netscout的Omnis™ Cyber Investigator (OCI) 是一個可以在企業範圍偵測網路威脅和風險調查的解決方案，可幫助減少網路威脅對企業的影響。它可作用於告警系統，能夠迅速有效地檢測，驗證，調查和回應網路威脅。唾手可得的經濟效益且可以高度擴展的路絡威脅分析解決方案將使企業受益，該解決方案還可以輕鬆地與許多公司使用的主流SIEM平台做整合。

ASI 技術

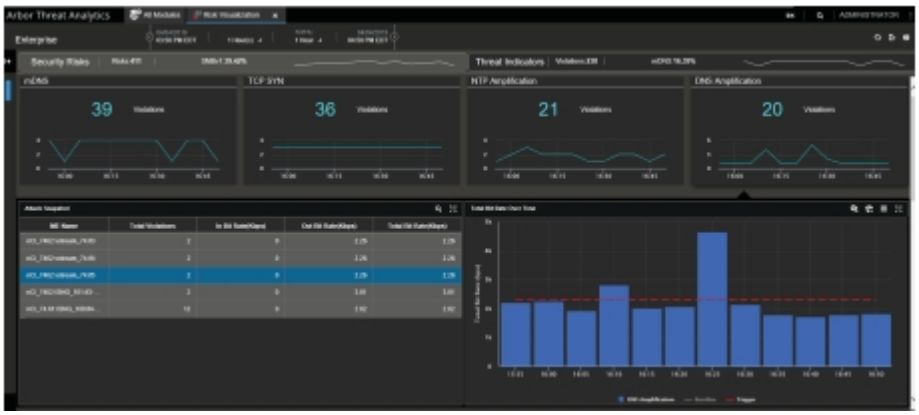
Omnis™ Cyber Investigator 基於NETSCOUT的專利Adaptive Service Intelligence™ （ASI） 技術構建，該技術利用數據可進行快速，上下文的獨立分析。對豐富且有意義的安全分析數據的訪問，結合高質量的檢測，可以提高調查速度，並以有效的方式簡化對威脅事件的評估。.

任何地方的可視性

ASI技術是NETSCOUT的數據來源分析技術的基礎，這些技術包括InfiniStreamNG （ISNG） 軟體和設備以及vSTREAM虛擬設備。通過ISNG和vSTREAM部署選擇，在各種私有雲，公有雲，常見的基礎架構以及虛擬化環境中實現全面且連續的可視性分析，而當這些環境需要完整的可試性以進行威脅檢測和故障排除。便可以與Omnis™ Cyber Investigator (OCI)一起使用。

可擴充性的架構

Omnis™ Cyber Investigator (OCI)具有可擴展及備援的系統結構，可支持大型分散式網路中的數據收集和分析。可用於擴展您的Omnis™ Cyber Investigator (OCI)部署，以實現更高的可擴展性或高可用性。

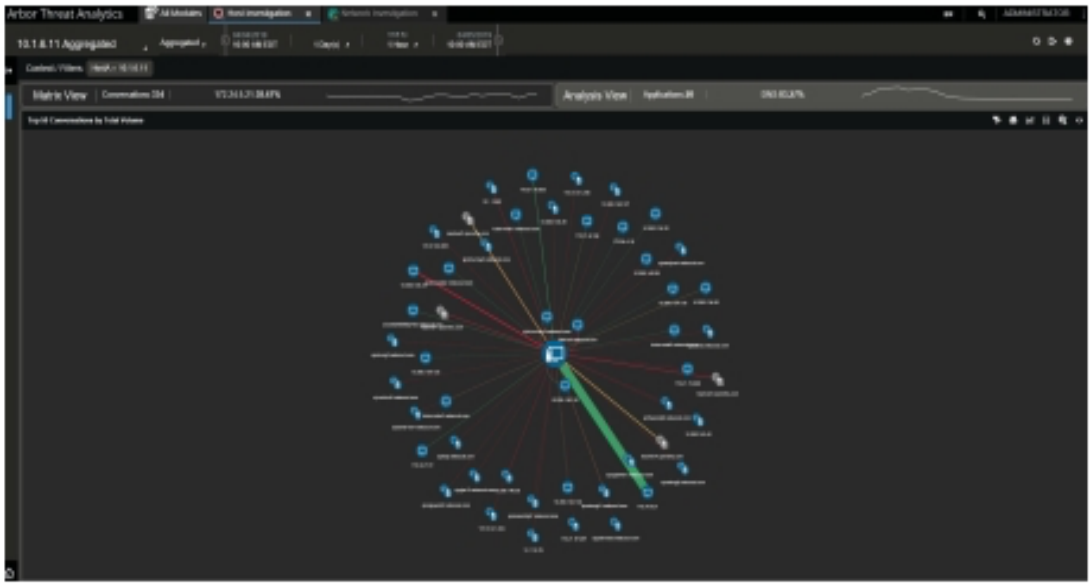


智慧型威脅偵測與偵查

Omnis™ Cyber Investigator (OCI)在數據中心和企業環境內部的深層和端點之間運行，這些地方其他工具無法提供網絡威脅可見性。安全分析師可以使用OCI)來解決當今大型，複雜的環境中可能會錯過的各種風險和威脅指標。

從威脅檢測的角度來看，Omnis™ Cyber Investigator (OCI)中會針對內部攻擊，與協議相關的風險和異常行為觸發安全事件。特定的協議風險評估包括檢測證書過期，較弱的SSL版本或密碼或使用未加密的協議。

通過使用靈活的工作流程，Omnis™ Cyber Investigator (OCI)的直觀用戶界面既強大又易於操作，無論是中級還是高級的安全分析師，都可以進行事件驅動型調查。



Corporate Headquarters
NETSCOUT Systems, Inc.
Westford, MA 01886-4105
Phone: +1 978-614-4000
www.netscout.com

Sales Information
Soll Free US: 800-309-4804
(International numbers below)

Product Support
Toll Free US: 888-357-7667
(International numbers below)

NETSCOUT