

Tenable.ot 規格書

系統規格

硬體：

Tenable.ot Security Platform

CPU: Intel Xeon 16Core (2.0G)

*1/32GB DDR 4 *2/2TB SATA3

HDD*2/

64GB SSD *1/Gigabit Ethernet LAN

COPPER RJ-45 *4

USB Port *2

Tenable.ot Configurable Sensor

CPU: Intel Xeon 4Core (2.0G) /4GB

DDR 4 *1/64GB SSD *1/Gigabit

Ethernet LAN

COPPER RJ-45 *5/USB Port *2

產品特性

Tenable.ot 能保護工業網路免於網路威脅、惡意內部人員及人為錯誤。從偵測及降低威脅到追蹤資產、弱點管理、組態控管及裝置完整性檢查，Tenable 的 ICS 安全性功能可在確保企業作業環境能見度、安全性與控管方面，發揮最大功效。

產品優勢

1.360 度可視性

您的OT基礎架構中多達50%包含IT資產。攻擊很容易在IT / OT基礎架構中傳播。Tenable.ot可提供對聚合攻擊面的完全可見性，同時可測量和控制整個OT和IT系統中的網路風險。Tenable.ot與Tenable產品組合以及領先的IT安全性和運營工具整合在一起，以實現可利用您整個安全基礎架構的一流的“信任生態系統”。

2.威脅偵測與緩解

Tenable.ot透過其多種檢測引擎，可以識別違規的事件，檢測異常行為並追蹤潛在高風險事件。可以在發生任何攻擊之前主動識別危險特徵。自訂政策使您可以設置和微調檢測方法，以便針對您的環境進行優化。借助內容豐富的警報，您可以快速回應並緩解影響您運營的威脅。

3.資產追蹤

Tenable.ot在不影響運營的情況下為您提供了對基礎架構的深刻探測和狀態感知。這種獲得專利的方法比單獨的被動監視收集的信息較多，包括識別沒有在網路上通信的設備。

4.弱點管理

Tenable.ot利用OT資產在工業安全領域的領域專業知識，以及IT資產在Nessus的領域。Tenable的VPR評分會利用ICS網路中的每項資產生成弱點和風險級別。

報告包括詳細的說明以及緩解建議。這使授權人員能夠在攻擊者利用弱點之前快速識別出最高優先級補救措施。

5.設定檔稽核

使用Tenable.ot，您可以追蹤被惡意軟體或使用者修改了設定檔，並提供了設備設定檔隨時間變化的完整歷史記錄，這使管理員可以建立具有“最新已知良好狀態”的備份快照，以更快地恢復並遵守行業法規