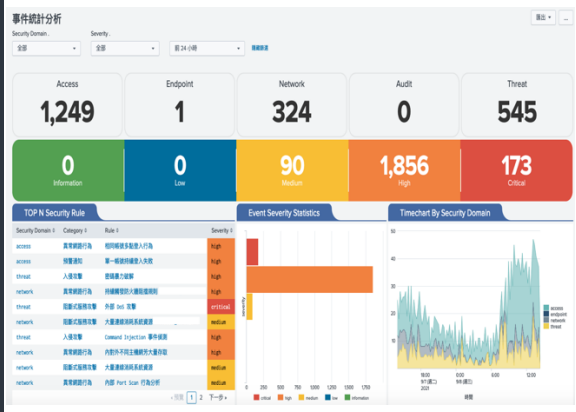
豪勉科技

NG-SOAR Information Security 資訊安全模組



資訊安全監控儀表板功能

- ✓ 資訊安全即時營運中心 - 戰情即時監控
- ✓ 資訊安全即時營運中心 - 事件統計分析
- ✓ 資訊安全即時營運中心 - 告警事件查詢
- ✓ 資訊安全即時營運中心 - 資安規則管理

1. 日誌收集功能：
   集成日誌的綜合分析平台，提供日誌搜尋，日誌 調查，產出定期報告。
2. 資料欄位正規化功能：
   透過 **Common Information Model (CIM)**幫助您規範化數據以匹配通用標準，對來自不同來源或供應商的等效事件使用相同的字段名稱和事件標籤。允許您定義事件數據中的關係，同時保持原始機器數據不變。
   對來自多個不同源類型的數據進行規範化後，可以快速開發報告、關聯搜索和視覺化儀表板。
3. 資訊安全監控規則：
   資訊安全監控規則定義與開發客製化服務，依據國家資通安全研究院 **N-SOC** 情資類別十大項監控內容包含：惡意內容、惡意程式、資訊蒐集、入侵嘗試、入侵攻擊、服務阻斷、資訊內容安全、詐欺攻擊、系統弱點、其他。

系統硬體規格需求

伺服器一台

- CPU, Intel® Xeon® Silver 4214R 等級以上 *2 above (一台)
- Memory, 32GB RDIMM, 2933MT/s,*4 above
- HDD, 1.2TB 10K RPM SAS 12Gbps 512n 2.5in Hot-plug Hard Drive,*8 above
- Power, Dual, Hot-plug, Redundant Power Supply (1+1), 750W above
- Network, 1GbE BASE-T *4

安裝於虛擬機環境硬體需求 Virtual Machine System Requirements (2 套)

The reference configuration for a virtual machine is as follows:

- 12 vCPU
- 32 GB RAM
- Full reservations for vCPU and vRAM (No CPU and memory overcommit)Minimum 800 random seek operations per second disk performance (sustained)
- Use VMware Tools in the guest VM
- Use VMXNET3 network adapter
- Provision virtual disks as Eager Zero Thick when not on an array that supports the appropriate VAAI primitives (“Write Same” and “ATS”)
- NFS and iSCSI disks are not recommended due to higher latency and file locking issues.

TECHNICAL SUPPORT

Email:

TechSupport@hauman.com.tw

Service phone number:

099-1122-160

Any Source , Any Data

資料收集不限來源格式，不限廠牌型號，只要是明碼即可。

Schema at Read

資料收集時不須事先定義欄位名稱，可讀取資料時再動態賦予欄位名稱定義。

台北市 大同區 承德路一段 70 號 3F

TEL: +886-2-2559-6163

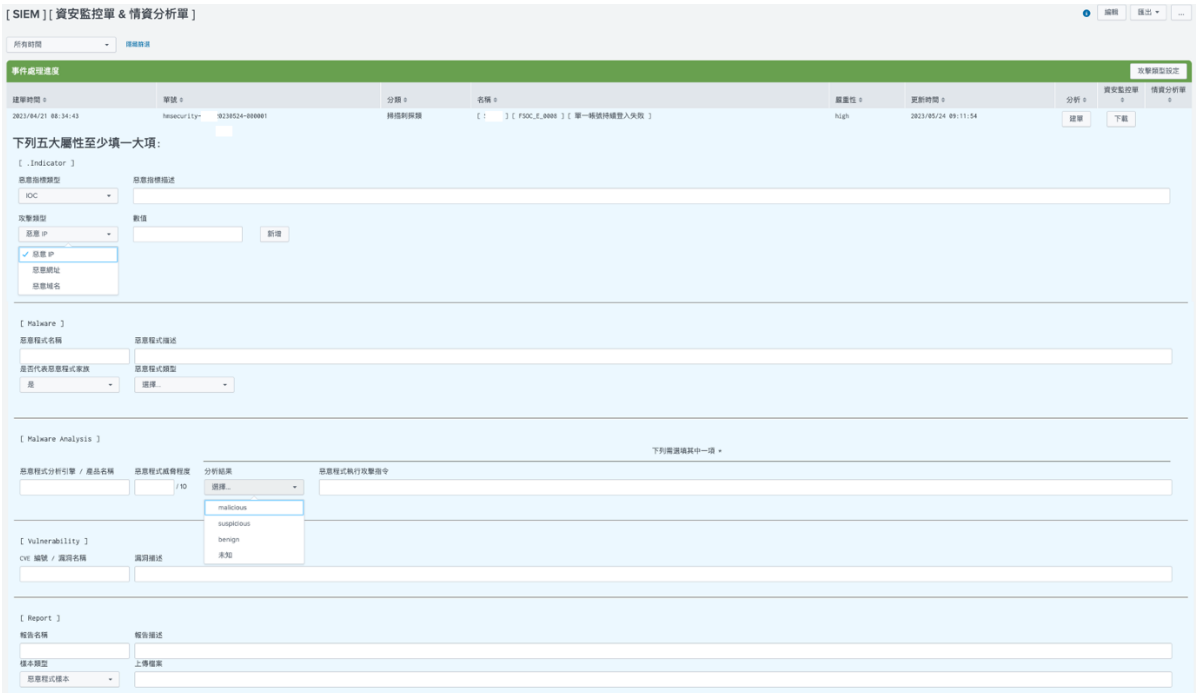
Fax: +886-2-2559-7406

Hauman 豪勉科技

豪勉科技

NG-SOAR Information Security 資訊安全模組

聯防監控情資整合功能模組



聯防監控情資開單模組

依照國家資通安全研究院政府 112 年頒布政府領域聯防監控作業規範進行功能開發。

監控執行單位即時回傳資安監控單和情資分析單，格式規範依照「聯防監控資安情資回傳 STIX 格式規範」文件進行開發 ，內容包含：

(1) 資安監控單

提供彙整開單系統資安告警事件成資安監控單。

(2) 情資分析單

提供彙整開單系統資安告警事件成情資分析單。

3 監控設備狀態單

提供彙整開單系統監控設備狀態告警事件成監控設備狀態單。

TECHNICAL SUPPORT

Email:

TechSupport@hauman.com.tw

Service phone number:

099-1122-160

Customized Service

依照國家資通安全研究院頒布最新的政府領域資安聯防監控作業規範進行開發，提供 GUI 介面，友善的操作介面。

提供監控資安事件整合MITRE ATT&CK 的攻擊類型設定。

提供資安監控單，情資分析單下載功能，檔案自動輸出為 STIX2.1 格式封裝。

台北市 大同區 承德路一段 70 號 3F

TEL: +886-2-2559-6163

Fax: +886-2-2559-7406

Hauman 豪勉科技