這 完全的 指導 到

安全 編排, 自動化 和 響應 (SOCGUARD)

經過

Andisheh Pardazan Goya System

(+98)9219427704

安全營運中心GUARD（SOCGUARD）

介紹

加特納公司 定義 翱翔 作為 A 科技 那 使 這
組織從各種來源獲取輸入並應用工作流程 對齊 到 過程 和 程式.

這些可以透過與其他整合來協調 技術和自動化來實現期望的結果和更大的可見性。附加功能 包括 案件 和 事件 管理 特徵, 這 能力管理威脅情報、儀表板和報告, 分析 那 能 是 應用 穿過 各種各樣的 功能。

SOCGUARD 工具 提供 機器驅動的 協助 到 人類 分析師 到 提升 這 效率 和 一致性 的 人們 和 流程 經過 顯著地 增強 安全 營運 活動 喜歡 威脅 偵測 和 回覆.

為什麼 SOCGUARD？

喜歡 許多 新的 工具 為了網路安全, 它 是 至關重要的 到 知道 什麼 問題 開車為了 發明 的 SOCGUARD 前 深的 潛水 進入 這 定義 的 SOCGUARD。
這 五 鑰匙 問題 這 SOCGUARD 市場 有 進化的 到 地址 是 作為 如下：

01

Organizations are being forced to achieve workload with less skilled analysts and high expectations.

02

Alerts consume most of the analyst time with similar analysis and false alarms and performing the same tasks to determine the accuracy of the alerts.

03

Security incidents are becoming more expensive, pushing organizations to find new ways to reduce the meantime to detection and the meantime to resolution further.

04

Security operations are naturally difficult to measure and manage effectively.

05

Tribal knowledge is genetically difficult to codify and often leaves the organization with personnel changes.

什麼 SOCGUARD 能 做？

一 的 這 添加 優點 的 SOCGUARD 是 它是 靈活性。 SOCGUARD 能 是 用過的 到 簡化 任何 數位 的 常見的 任務， 喜歡 更新中 威脅 資料庫 和 回應 到 警報。

鑰匙 應用：

管理 漏洞： 關聯日誌數據和 威脅 智力 到 理解 什麼 攻擊者正在使用並識別漏洞 元素 的 您之前的基礎設施 他們 能 是 妥協了。

協調調查：統一安全 數據 容易地 和 取回 相關的 第三者 威脅 智力 什麼時候 你 需要 它。 立即的存取外部資料來源有助於 分析師 在 製作 A 精確的 決定 在 每個 調查。

回應 到 事件： 劇本、 A 放 的 規則使 SOCGUARD 平台 到 行為 自動地 當事件發生時。這個功能 幫助 在 環境 向上 一個 自動化的 回覆 為了 這 最多 常見的 事件 類型。

簡化協作：事件 調查和其他安全流程 能 研磨 到 A 停 什麼時候 團隊 不是 有能力的 到 輕鬆協作，例如團隊合作時 整個組織將資料儲存在 不同的 格式 和 使用 不同的 軟體. SOCGUARD 幫助 你 排除 這些障礙 到 合作。

什麼 SOCGUARD 是 不是：

SOCGUARD 解決方案並不能取代熟練的分析師。部署 SOCGUARD 解決方案更換分析師將不可避免地帶來更多風險，而不是緩解風險。相反，SOCGUARD 解決方案應被視為安全計劃和安全分析師的推動者 一樣。

SOCGUARD 解決方案 是 不是 設計的 到 攝取 A 大的 體積 的 生的 事件。 反而， SOCGUARD 解決方案 是 設計的 到 挑選 向上 這 事件 在哪裡 SIEM 功能性 結束， 提供 一個自動化的 和 精心策劃的 回覆 自始至終 這 鑑別 階段， 作為 出色地 作為 這遏制， 根除 和 恢復 階段。

SOCGUARD 是一種透過自動化減輕安全威脅的解決方案 程式 到 C收集 數據 關於 安全 威脅 從 各種各樣的 來源 和 回應迅速地 到 這 低級 安全 事件 沒有 人類 協助。

SOCGUARD 功能：

聚合： 這 能力 到 總計的 數據 穿過 不同的 來源 在 這 形式 的 警報，或其他輸入 技術，例如來自 SIEM 工具的警報或發送至 郵箱。

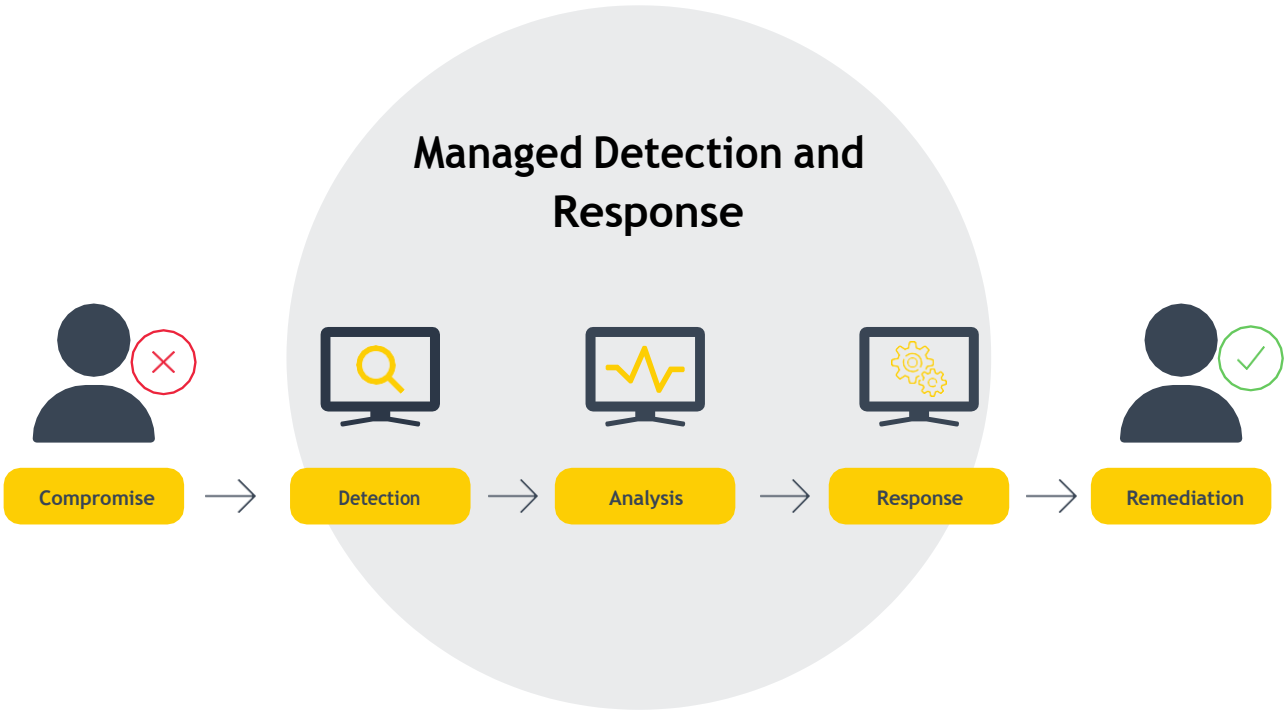
豐富： 額外的 期間的見解 數據 收集和處理，SOCGUARD 解決方案 幫助整合外部威脅情報 溫柔地 執行內部 上下文查找或運行進程來收集更多數據 渲染 到 定義的 行動。

編排： 整理 任務 到 最佳化 A 結構化的 工作流程 經過 蒐集 資訊從 A 不同的 來源 和 鞏固 它。 SOCGUARD 解決方案整合了不同的安全性 工具 和 平台 所以 他們 能 工作 一起。科技 整合 是 這 最好的 和 最多常見的 方法 用過的 到 支援 科技 編排。

自動化： 這 概念 使 軟體 到 完全的 A 單身的 任務 或者 功能 沒有人類的參與。自動化不是一個 人類分析師的替代方案。相反，它 減少 這 分析師的 時間 花費 在 簡單的， 重複的 任務。

反而 的 浪費 時間 在 乏味 手動的 任務並調查誤報， SOC（安全運營 中心）團隊可以利用他們的專業知識 回應 到 事件 迅速地 和 有效地。

響應： 手動或自動響應 提供 罐頭的 解決 到 以程式設計方式定義的 活動。 SOCGUARD 自動化 重複的 任務， 優先考慮 批判的 事件 和 流線型 安全 流程 到 減少回覆 次 徹底地。



SOCGUARD 好處 為了 交付 多重抗藥性 服務。

SOCGUARD 的 能力 到 編排 和 自動化 是 行動 採取 經過 安全 產品 沒有任何需要 人類的 干涉。這 是一 其 最大的力量 那 允許 SOCGUARD 到 整合 和 任何 安全 過程 或者 工具 那 是 已經 在 使用 那能 提高 這 表現 到 添加 用處 到 每個 產品。

為了解決可擴展性問題，SOCGUARD 融合的 和 現存的 安全 技術。

這 一體化 的 SOCGUARD 改善 這 能力的 MSSP 的 到 探測 和 中和 威脅 和 攻擊。

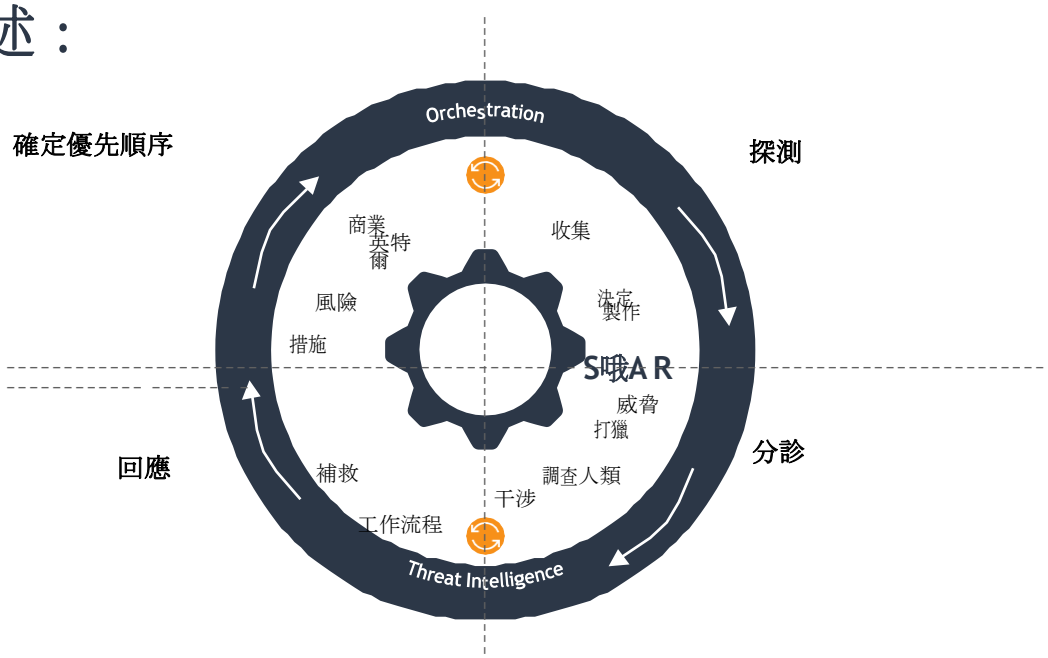
統一資產資料庫、幫助台 系統、設定管理 系統，和 其他 它 管理 工具 它行為 作為 A 單身的 「窗格 的 玻璃」。

SOCGUARD 加速 反應能力 到 警報 觸發的 經過 武裝 MSSP 的 和 這 能見度 和 能力 到 反應 果斷地 到 新的威脅 或者 攻擊 這樣的 作為 SOCGUARD 自動化的 威脅情報的工作流程 透過 這 案件 和 票 管理 並提供風險和相關性 警報。

MSSP 的 過量的 一個 充足 數量 的 時間 交易 和 錯誤的 正面的一面， 因為 那裡 每天都會有更多數量的警報。 SOCGUARD 能 自動化 這 處理 的 這樣的 警報，幫助分析師集中精力 在哪裡 決定 是 需要。

SOCGUARD 自動化 手動的 工作 的 這 分析師到 證實 這 合法性 的 這 警報 這樣的 作為在基礎設施中發現的新用戶或 刪除和更新規則，從而 減少 這 時間 消耗。

SOCGUARD 概述：



管理 偵測 和 回覆 （多重抗藥性） 安全 送貨 服務 提供者 臉 許多
先進技術帶來的技術和人類相關問題的挑戰 安全 威脅。

依賴靜態簽章和模式匹配的解決方案無法 偵測 和 回應 到 今天的 先進的 安全 威脅。 因此，
許多 MSSP 的 （管理 安全 服務 提供者） 是 去 在後面 SOCGUARD 解決方案 到 提升 他們的
偵測 和 回覆 能力。

動態 在 SOCGUARD

SOCGUARD 是 一個 編排、自動化 和 回應 系統 哪個 能 是
從資料注入階段到回應階段的所有 3 層均已開發 指控稱，SOCGUARD
平台可以透過以下方式擴展其軟體的功能： 機器學習等技術。機器學習補充了現有的 SOCGUARD
功能性 經過 給予 這 軟體 這 方法 到 適應 到 變化 在 這 環境。SOCGUARD 平台 能 學習 什麼
是 和 不是 普通的 為了 自動化 反而 的 依靠 在靜止的 基於閾值的 規則。 一次 這些 基線 是
已確立的， 軟體 更新 他們 定期地 作為 和 什麼時候 這 環境 變化， 增加 它是 準確性 和 減少 這
數位 的 錯誤的 正面的一面。

SOCGUARD 取得了重大改進，包括流程編排、 任務或工作流程的自動化。這有幫助
資料完整性並提供 更好的警報上下文，減少了必要的手動工作量 糾正威脅。也使用 SOCGUARD
的安全團隊成員 舒服的 和 腳本編寫 語言 能 使用 圖形化的 劇本 創建 工具， 儘管和 先進的
腳本編寫 知識 保持 這 能力 到 寫 腳本 經過 手。

批判的 成分 的SOCGUARD 技術：

什麼時候 評估 不同的 SOCGUARD 平台， 每個 成分 應該 是 經過考慮的 作為 它戲劇
一個 重要的 角色 在 這 功能。

01

可自訂性 和 靈活性： 一個 有效的 SOCGUARD 解決方案 應該 是
足以成為安全堆疊之上的單一工具。它 應該啟用 到 以針對 CSIRT
最佳化的方式實施團隊， 作為 出色地 作為 SOC 的， MSSP 的 和 安全 團隊。
數據 輸入 從 A 不同的來源，包括機器對機器、電子郵件、使用者提交、和
手動的 輸入 應該 是 支持的。

在每個 SOCGUARD 解決方案中，很少有預設集成 可用的 但 不是 全部 這組織的 安全 產品 支持， 為了那 原因 SOCGUARD 解決方案 應該 是 靈活的 足夠的 到 創造
與安全和分析平台的雙向集成 這 顧客 要求。

02

流程工作流程： SOCGUARD 解決方案的主要優勢之一是它 能力 的 自動化 和 編排 的 流程 工作流程 到 實現力量倍增，減輕重複性任務的負擔 執行的 經過 分析師 日復一日。 這 流程 工作流程 執行 應該 是 靈活的 足夠的 到 支援 幾乎 任何 過程 哪個 可能 需要 到被編碼在解決方案中。工作流程應支援兩者的使用 風俗 和 內建 集成， 作為 出色地 作為 這 手動的 任務 創作 哪個到 是 完全的 經過 一個 分析師。

03

事件 管理： 編排 和 自動化 的 安全 產品 為任何安全計劃提供明確的價值。 SOCGUARD 解決方案應包括 附加功能可管理整個 IR 生命週期並最大限度地提高 時間 和 貨幣 投資。 這 應該 包括 案件 管理
其中涉及收集、分發和分析與特定相關的數據 安全 事件， 到 允許 團隊 到 有效地 回應。 A SOCGUARD 平台 幫助組織減少時間 檢測並平均時間 回應 經過 使能 警報 到 是 合格的 和 補救的 在 分分鐘 相當比 天 和 幾週。

04

威脅 智力： 威脅 智力 是 A 批判的 成分 在 有效的
和高效率的事件響應。這些技術支援漏洞修復。 威脅 智力 必須 去 多於 和 超過 謙虛的 飼料 到 是 確實 有效的 在 今天的 威脅 景觀， 作為 A SOCGUARD 解決方案不僅可以存取指標，還可以存取事件
可以提供附加上下文的信息，它是不可模仿的 位置 到 收集 可執行的 威脅 智力。

05

協作與資訊共享：安全事件回應 警報 是 一個 平等的 潛在的 責任 的 一個 個人 在 一個 組織相似地 SOCGUARD 解決方案需要支援協作和資訊 分享 之中 團隊 會員 在 A 受控 方式。

SOCGUARD 應用：

01

積極主動的 威脅 打獵： 自從 威脅 打獵 通常 需要 分析師 到 多種安全工具之間的快速協調，提供了很好的 機會 為了 編排 和 即時 影響。 SOCGUARD 工具 能 啟用安全性 團隊 攝取 第三者 威脅來源 和 自動化 '搜尋 和 破壞' 工作流程 那 掃描 為了 潛在的 漏洞 穿過環境。

02

標準化與迭代事件流程：安全團隊需要 最大限度地減少事件管理和回應中的「品質差異」。 SOCGUARD 工作流程是朝這個方向邁出的重要第一步，允許部分/全部 最佳實踐流程的編纂並保證安全 分析師不必在每次遇到問題時從頭開始 具體的 事件。 和 部署 到期， SOCGUARD 工具 將要 也 允許 團隊 到 迅速地 迭代 之上 這些 流程 經過 發現 差距 和 地區為了 改進。

03

提升 調查 品質: 多種的 數據 點 在 這 報告 建議 那 安全 團隊 鬥爭 和 蒐集 事件 情境 和 槓桿作用數據在其許可時完全可見。 SOCGUARD 工具可以幫助改進 透過更快地解決誤報來提高調查質量, 透過來自多個方面的相關資訊對事件和風險進行優先排序 工具 和 釋放 向上 分析師 時間 經過 排除 這 需要 到 學習 這 詳細的白話 的 許多 安全 產品。

04

加速 和 規模 事件 回覆: SOCGUARD 提供協調一致的服務 自動化對當前受到重要但影響的行業的影響 可重複的、高數量的任務。 SOCGUARD 工具讓 SOC 可以信賴 自動化 為了 這 繁重的工作 和 槓桿作用 富有的， 相關的 資訊 為了決策 和 調查。

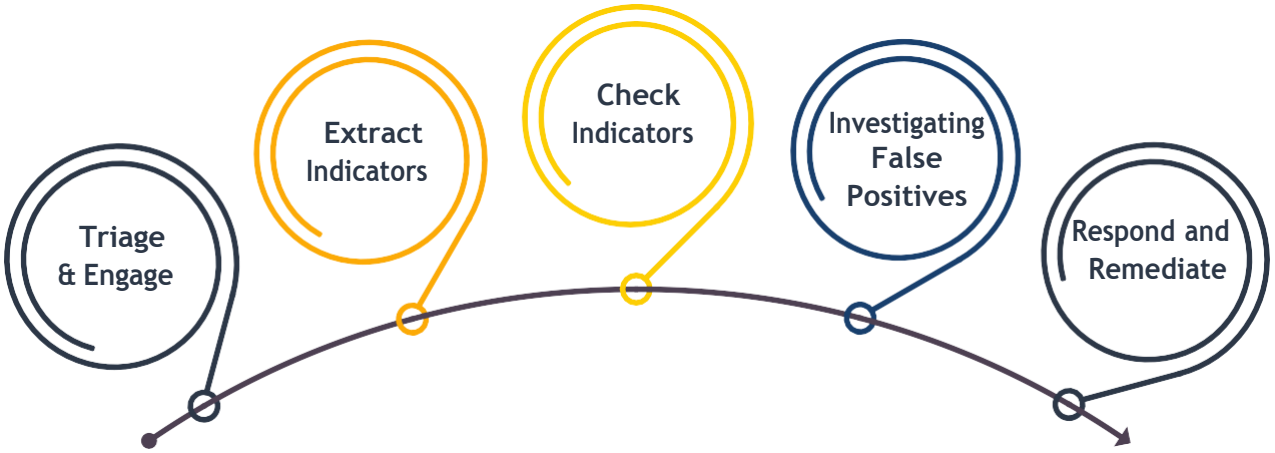
05

安全 營運 和 維護： 除了自動化重複的工作 任務、SOCGUARD 工具 也能 幫助安全 團隊簡化 系統檢查， 維護、升級、 和 一般的 安全 營運. 這些 實踐 依賴工作流程 盡可能多 作為回應， 和標準化 需要。 自動化 執行 將要 增加 準確性 和 更好的 插頭 差距 那 離開系統 易受傷害的。

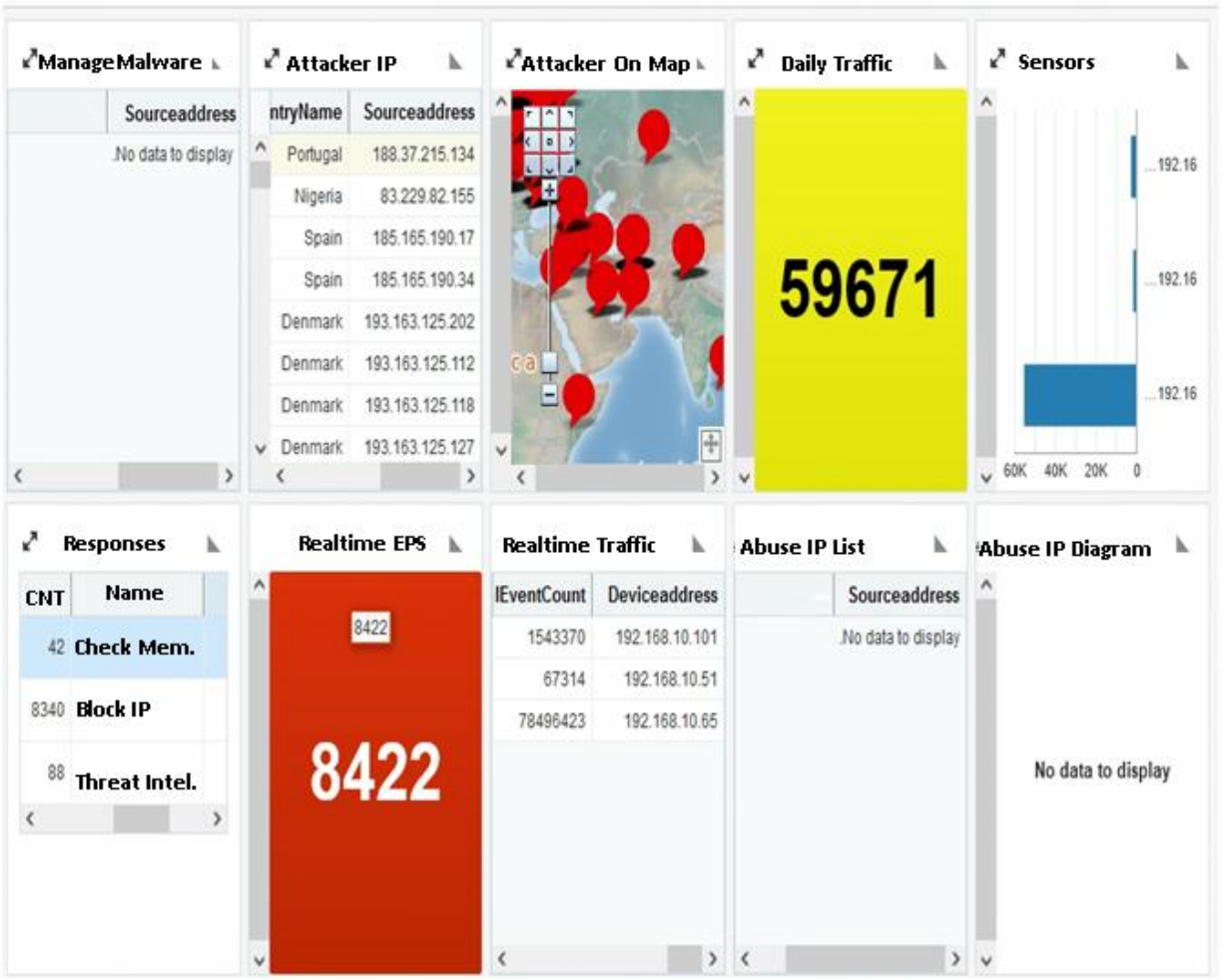
SOCGUARD 使用 案例：

使用 案例 為了 SOCGUARD 將要 各不相同 取決於 在 這 環境 和 是 有限的 僅有的 經過這 創造力 的 這 組織 建築學。

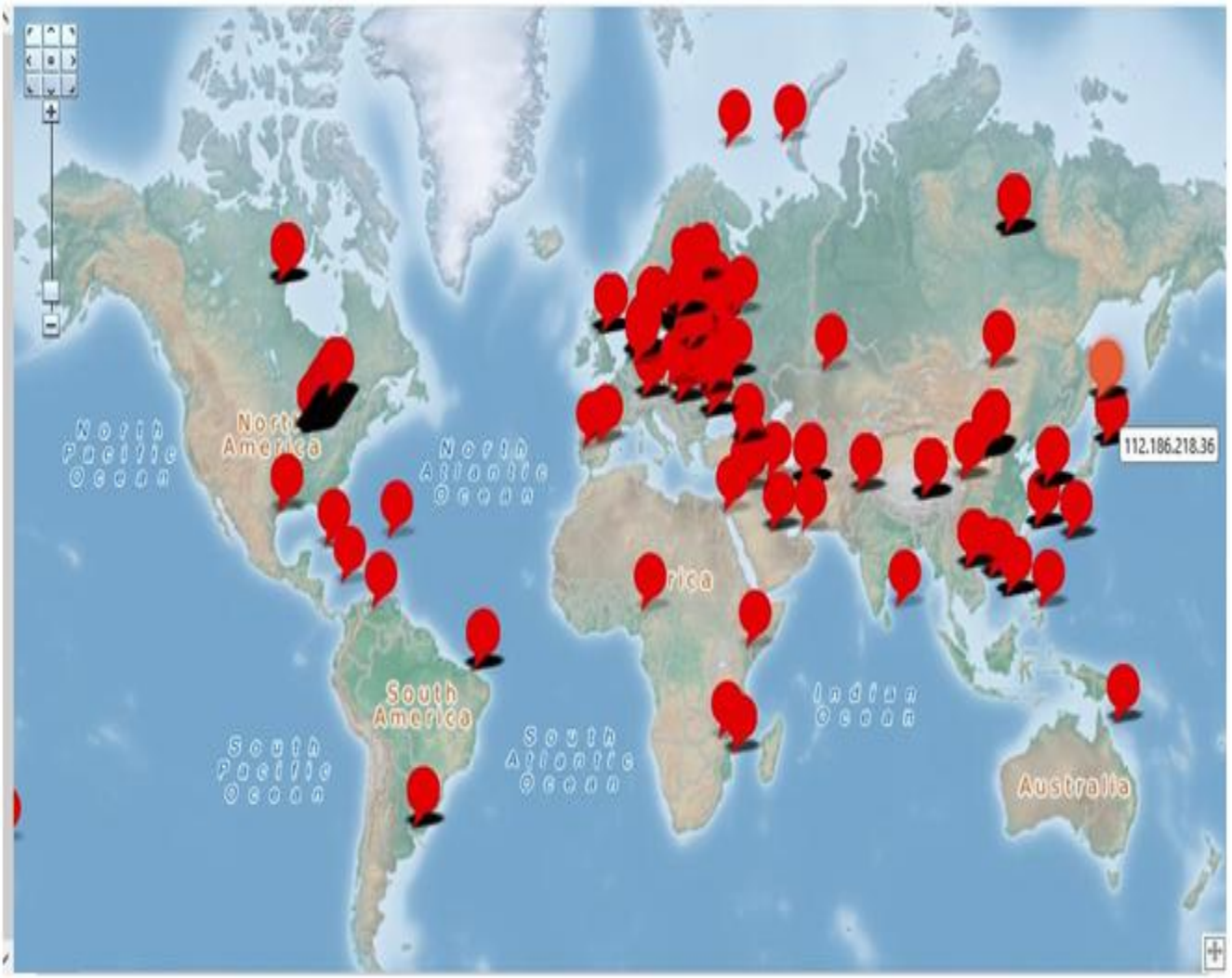
這裡 是 這 我們可以定義的工作流程：



管理報告：


ManageMalware
Sourceaddress
No data to display
Attacker IP
ntryName
Sourceaddress
Portugal 188.37.215.134
Nigeria 83.229.82.155
Spain 185.165.190.17
Spain 185.165.190.34
Denmark 193.163.125.202
Denmark 193.163.125.112
Denmark 193.163.125.118
Denmark 193.163.125.127
Attacker On Map
Daily Traffic
59671
Sensors
192.16
192.16
192.16
60K 40K 20K 0
Responses
CNT
Name
42 Check Mem.
8340 Block IP
88 Threat Intel.
Realtime EPS
8422
8422
Realtime Traffic
lEventCount
Deviceaddress
1543370 192.168.10.101
67314 192.168.10.51
78496423 192.168.10.65
Abuse IP List
Sourceaddress
No data to display
Abuse IP Diagram
No data to display

攻擊者地圖報告


North Pacific Ocean
North America
North Atlantic Ocean
South America
South Pacific Ocean
South Atlantic Ocean
Indian Ocean
Australia
112.186.218.36

翱翔 產品比較：

社會衛士	Q雷達	弧光瞄準器	史普朗克	太陽的風	產品/指標
好的	好的	好的	好的	好的	使用案例
大多	400+	400+	大多	-	資料來源
1000000	1000000	100000	每日 PB	每天 2500 萬	最大每股收益
機器學習、UEBA 和取證	機器學習、UEBA 和取證	機器學習	機器學習和 UEBA	例外行為	智力
軟體或雲端	裝置或軟體或雲	裝置或軟體或雲	軟體或雲端	虛擬設備	送貨
SC、UF、系統日誌、自訂	Wincollect、系統日誌	SC、系統日誌	超濾	掃描電鏡	支援代理
基於最大每日數據或 EPS	每月	基於最大每日數據或 EPS	基於每日最大數據 GB/天	每個節點	價錢

聯絡我們

銷售經理：

卡里米先生

+989219427704

info@socguard.ir