这 完全的 指导 到

安全 编排, 自动化 和 响应(SOCGUARD)

经过

安迪舍·帕尔达赞戈雅体系

(+98)9219427704

安全运营中心 GUARD

（社会卫士）

介绍

高德纳公司 定义 翱翔 作为 A 技术 那 启用 这 组织从各种来源获取输入并加以应用工作流程 对齐 到 过程 和 程序。

这些可以通过与其他的集成来协调 技术和自动化来实现预期 成果和更高的可视性。附加功能 包括 案件 和 事件 管理 特征, 这 能力管理威胁情报、仪表板和报告， 分析 那 能 是 应用 穿过 各种各样的 功能。
安全卫士 工具 提供 机械驱动 协助 到 人类 分析师 到 提升 这 效率 和 一致性 的 人们 和 进程 经过 显著地 增强 安全运营 活动 喜欢 威胁 检测 和 回复。

为什么 SOCGUARD？

喜欢 许多 新的 工具 为了网络安全， 它 是 至关重要的 到 知道 什么 问题 开车为了 发明 的 安全卫士 前 深的 潜水 进入 这 定义 的 安全卫士。

这 五 钥匙 问题 这 安全卫士 市场 有 进化 到 地址 是 作为 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.

什么 安全卫士 能 做？

一 的 这 添加 优点 的 安全卫士 是 它是 灵活性。 安全卫士 能 是 用过的 到 简化 任何 数字 的 常见的 任务， 喜欢 更新 威胁 数据库 和 回应 到 警报。

钥匙 应用：

管理 漏洞： 关联日志数据和 威胁 智力 到 理解 什么 攻击者正在使用并识别漏洞 元素 的 你的基础设施 他们 能 是 妥协。

协调调查：统一安全 数据 容易地 和 取回 相关的 第三者 威胁 智力 什么时候 你 需要 它。 立即的访问外部数据源有助于 分析师 在 制作 A 精确的 决定 在 每个 调查。

回应 到 事件： 剧本， A 放 的 规则启用 安全卫士 平台 到 行为 自动地 当事件发生时。此功能 帮助 在 环境 向上 一个 自动化 回复 为了 这 最多 常见的 事件 类型。

简化协作：事件 调查和其他安全流程 能 研磨 到 A 停 什么时候 团队 不是 有能力的 到 轻松协作， 例如当团队 在整个组织中存储数据 不同的 格式 和 使用 不同的 软件。 安全卫士 帮助 你 排除 这些障碍 到 合作。

什么 安全卫士 是 不是：

SOCGUARD 解决方案不能替代熟练的分析师。部署 SOCGUARD 解决方案到更换分析师将不可避免地带来更多风险，而不是缓解风险。相反，SOCGUARD 解决方案应被视为安全计划和安全分析师的推动者 一样。

安全卫士 解决方案 是 不是 设计 到 摄取 A 大的 体积 的 生的 事件。 反而， 安全卫士 解决方案 是 设计 到 挑选 向上 这 事件 在哪里 安全信息与事件管理 功能 结束， 提供 一个自动化 和 精心策划 回复 自始至终 这 鉴别 阶段， 作为 出色地 作为 这遏制， 根除 和 恢复 阶段。

SOCGUARD 是一种通过自动化减轻安全威胁的解决方案， 程序 到 C 收集 数据 关于 安全 威胁 从 各种各样的 来源 和 回应迅速地 到 这 低级 安全 事件 没有 人类 协助。

安全卫士 功能：

聚合： 这 能力 到 总计的 数据 穿过 不同的 来源 在 这 形式 的 警报，或来自其他的输入 诸如来自 SIEM 工具的警报或发送到 邮箱。

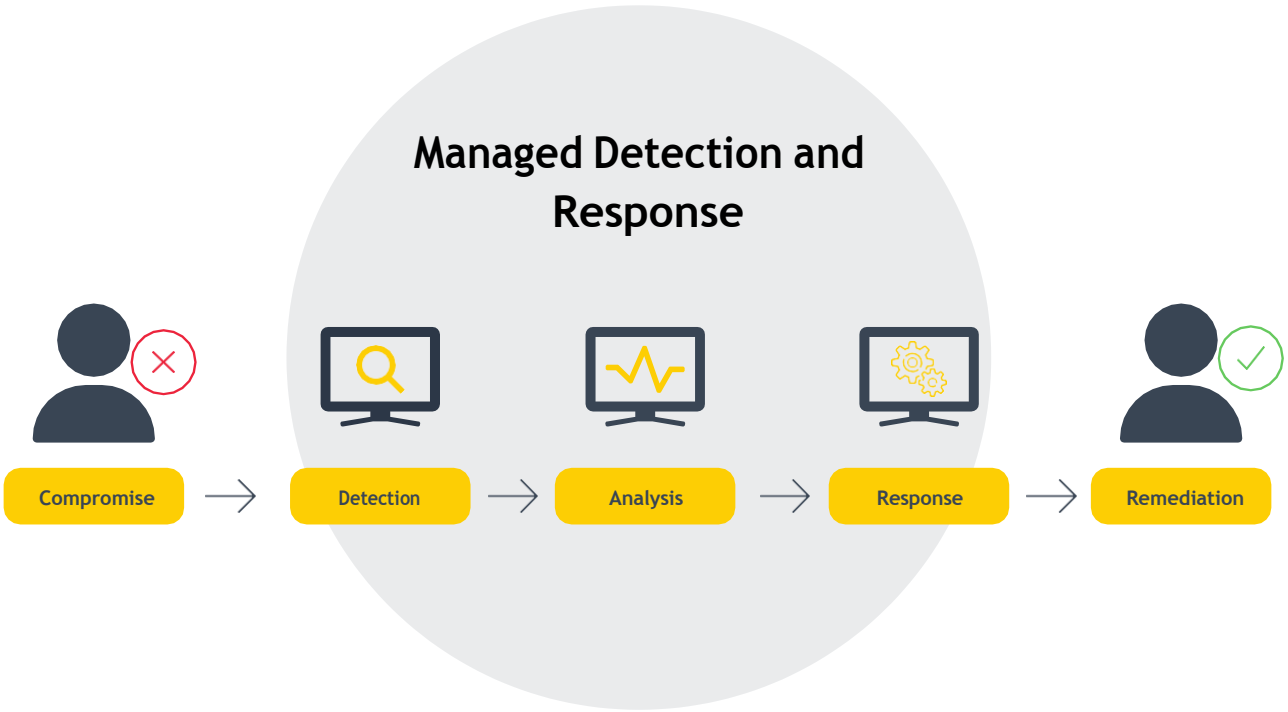
丰富： 额外的 洞察 数据 收集和处理，SOCGUARD解决方案 帮助整合外部威胁情报 起源于 执行内部 上下文查找或运行流程来收集更多数据 渲染 到 定义 动作。

编排： 安排 任务 到 优化 A 结构化的 工作流程 经过 搜集 信息从 A 不同的 来源 和 巩固 它。 SOCGUARD 解决方案集成了不同的安全 工具 和 平台 所以 他们 能 工作 一起。技术 整合 是 这 最好的 和 最多常见的 方法 用过的 到 支持 技术 编排。

自动化： 这 概念 启用 软件 到 完全的 A 单身的 任务 或者 功能 没有人类参与。自动化并不是 人类分析师的替代方案。相反，它 减少 这 分析师的 时间 花费 在 简单的， 重复 任务。

反而 的 消瘦 时间 在 乏味 手动的 任务和调查误报， SOC（安全运营 中心）团队可以利用他们的专业知识 回应 到 事件 迅速地 和 有效地。

响应：手动或自动响应 提供 罐头 解决 到 以编程方式 定义 活动。 安全卫士 自动化 重复 任务， 优先考虑 批判的 事件 和 流线型 安全 进程 到 减少回复 次 急剧地。



安全卫士 好处 为了 交付 耐多药 服务。

SOCGUARD 的 能力 到 精心策划 和 自动化 是 行动 已采取 经过 安全 产品 无需 人类的 干预。这 是一个 它的 最大的力量 那 允许 安全卫士 到 整合 和 任何 安全 过程 或者 工具 那 是 已经 在 使用 那能 提高 这 表现 到 添加 用处 到 每个 产品。

为了解决可扩展性问题，SOCGUARD 融合的 和 现存的 安全 技术。

这 一体化 的 安全卫士 改善 这 能力的 MSSP 到 探测 和 中和 威胁 和 攻擊。

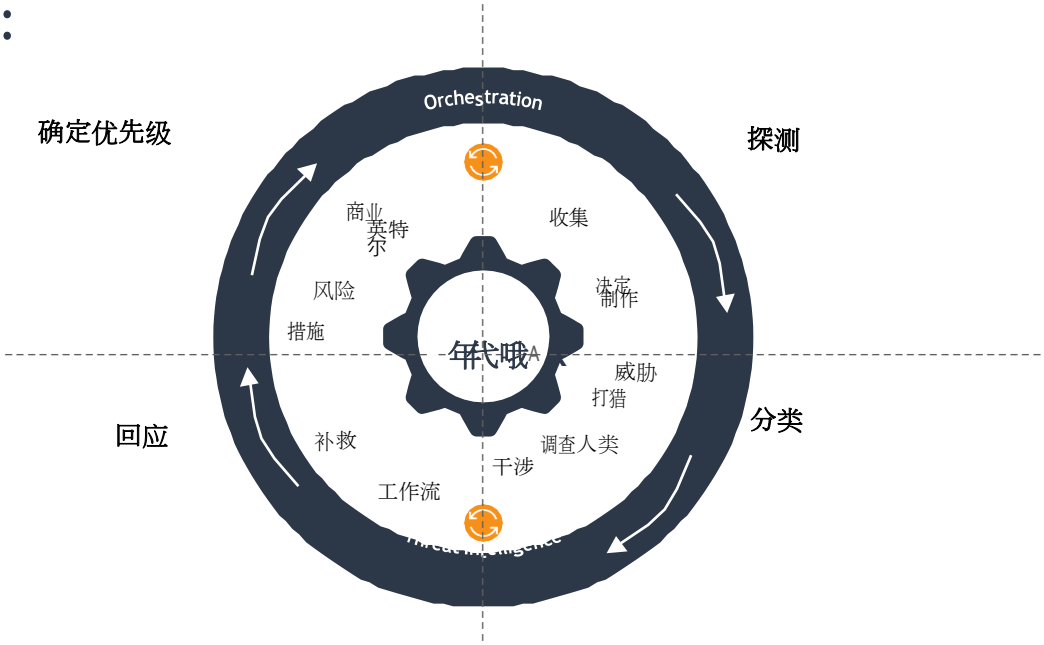
统一资产数据库、帮助台 系统、配置管理 系统，和 其他 它 管理 工具 它行为 作为 A 单身的 “窗格 的 玻璃”。

安全卫士 加速 响应能力 到 警报 触发 经过 武装 MSSP 和 这 能见度 和 能力 到 反应 果断地 到 新的威胁 或者 攻击 这样的 作为 安全卫士 自动化 威胁情报的工作流程跨度 通过 这 案件 和 票 管理 并提供风险和相关性 警报。

MSSP 过量的 一个 充足 数量 的 时间 交易 和 错误的 积极因素， 因为 那里 每天的警报数量都在增加。 安全卫士 能 自动化 这 处理 的 这样的 警报，帮助分析师关注 在哪里 决定 是 需要。

安全卫士 自动化 手动的 工作 的 这 分析师到 证实 这 合法性 的 这 警报 这样的 随着基础设施中发现新用户或 删除并更新规则，从而 减少 这 时间 消耗。

安全卫士 概述：



管理 检测 和 回复 （耐多药） 安全 送货 服务 提供商 脸 许多由于先进的 安全 威胁。

依赖于静态签名和模式匹配的解决方案无法 检测 和 回应 到 今天的 先进的 安全 威胁。 因此，许多 MSSP （管理 安全 服务 提供者） 是 去 在后面 安全卫士 解决方案 到 提升 他们的检测 和 回复 能力。

发展 在 安全卫士

安全卫士 是 一个 编排、自动化 和 回应 系统 哪个 能 是
从数据注入阶段到响应阶段，其所有 3 个层次都得到了发展
指控，SOCGUARD平台可以扩展其软件的功能 机器学习等技术。机器学习补充了现有的 SOCGUARD 功能 经过 给予 这 软件 这 方法 到 适应 到 变化 在 这 环境。安全卫士 平台 能 学习 什么 是 和 不是 普通的 为了 自动化 反而 的 依靠 在静止的 基于阈值 规则。 一次 这些 基线 是 已确立的， 软件 更新 他们 定期 作为 和 什么时候 这 环境 变化， 增加 它是 准确性 和 减少 这 数字 的 错误的 积极的方面。

SOCGUARD 取得了显著的进步，包括流程编排、 任务或工作流程的自动化。这有助于 数据完整性并提供 更好的警报上下文，从而减少手动工作量 补救威胁。此外，使用 SOCGUARD 的安全团队成员没有 舒服的 和 脚本 语言 能 使用 图形 剧本 创建 工具， 尽管和 先进的 脚本 知识 保持 这 能力 到 写 脚本 经过 手。

批判的 成分 的安全卫士 技术：

什么时候 评估 不同的 安全卫士 平台， 每个 成分 应该 是 经过考虑的 作为 它戏剧 一个 重要的 角色 在 这 功能。

01

可定制性 和 灵活性： 一个 有效的 安全卫士 解决方案 应该 是 足以成为安全堆栈顶部的单一工具。它 应该启用 到 以针对 CSIRT 进行优化的方式实施团队， 作为 出色地 作为 SOC， MSSP 和 安全 團隊。 数据 输入 从 A 不同的来源，包括机器对机器、电子邮件、用户提交，和 手动的 输入 应该 是 支持的。

在每个 SOCGUARD 解决方案中，都会有一些默认集成 可用的 但 不是 全部 这 组织的 安全 产品 支持， 为了那 原因 安全卫士 解决方案 应该 是 灵活的 足够的 到 创造
与安全和分析平台进行双向集成 这 顾客 要求。

02

流程工作流： SOCGUARD 解决方案的主要优势之一是其 能力 的 自动化 和 编排 的 进程 工作流程 到 实现力量倍增，减少重复任务的负担 执行 经过 分析师 日复一日。 这 过程 工作流程 执行 应该 是 灵活的 足够的 到 支持 几乎 任何 过程 哪个 可能 需要 到在解决方案中编纂。工作流程应支持使用 风俗 和 内置 整合， 作为 出色地 作为 这 手动的 任务 创作 哪个到 是 完全的 经过 一个 分析师。

03

事件 管理： 编排 和 自动化 的 安全 产品
为任何安全程序提供明确的价值。SOCGUARD 解决方案应包括 附加功能来管理整个 IR 生命周期，并最大限度地提高 时间 和 货币 投资。 这 应该 包括 案件 管理 涉及收集、分发和分析与特定 安全 事件， 到 允许 团队 到 有效地 回应。 A 安全卫士 平台 帮助组织减少 检测和平均时间 回应 经过 启用 警报 到 是 合格的 和 已补救 在 分钟 相当比 天 和 周。

04

威胁 智力： 威胁 智力 是 A 批判的 成分 在 有效的
以及高效的事件响应。这些技术支持漏洞修复。 威胁 智力 必须 去 多于 和 超过 谦虚的 供稿 到 是 确实 有效的 在 今天的 威胁 景观， 作为 A 安全卫士 解决方案不仅可以访问指标，还可以访问事件
这些信息可以提供额外的背景，它以一种独特的方式 位置 到 收集 可操作性 威胁 智力。

05

协作和信息共享：安全事件响应 警报 是 一个 平等的 潜在的 责任 的 一个 个人 在 一个 组织相似地 SOCGUARD 解决方案需要支持协作和信息 分享 之中 团队 成员 在 A 受控 方式。

安全卫士 应用：

01

积极主动的 威胁 打猎： 自从 威胁 打猎 通常 需要 分析师 到 在多种安全工具之间快速协调，它提供了极大的 机会 为了 编排 和 即时 影响。安全卫士 工具 能 启用安全性 团队 摄取 第三者 威胁源 和 自动化 '搜索 和 破坏' 工作流程 那 扫描 为了 潜在的 漏洞 穿过环境。

02

标准化和迭代事件流程：安全团队需要最大限度地减少事件管理和响应中的"质量差异"。SOCGUARD 工作流程是朝着这个方向迈出的重要的第一步，允许部分/全部编纂最佳实践流程并保证安全 分析师不必每次遇到 具体的 事件。 和 部署 到期，SOCGUARD 工具 将要 还 允许 团队 到 迅速地 迭代 之上 这些 进程 经过 点滴 差距 和 区域为了 改进。

03

提升 调查 质量： 多种的 数据 点 在 这 报告 建议 那 安全 团队 斗争 和 搜集 事件 语境 和 杠杆作用确保数据在清关时完全可见。SOCGUARD 工具可以帮助改善通过更快地解决误报来提高调查质量，通过来自多个系统的相关信息确定事件和风险的优先顺序 工具 和 释放 向上 分析师 时间 经过 避免 这 需要 到 学习 这 详细的白话 的 许多 安全 产品。

04

加速 和 规模 事件 回复： SOCGUARD 提供协调 自动化对目前受到重要但可重复、高质量的任务。SOCGUARD 工具允许 SOC 依靠 自动化 为了 这 繁重的工作 和 杠杆作用 富有的， 相关的 信息 为了决策 和 调查。

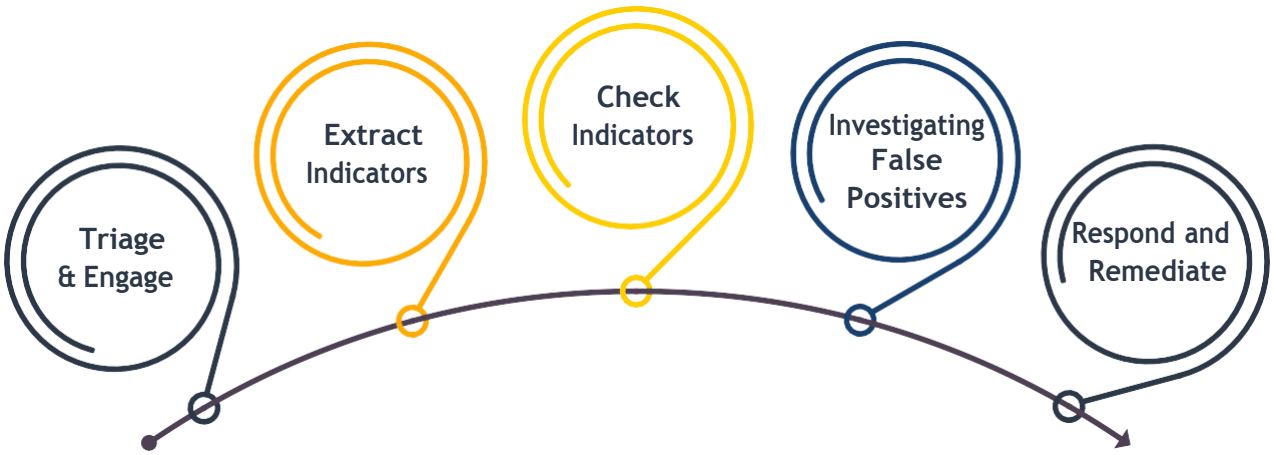
05

安全 运营 和 维护： 除了自动执行重复性工作 任务，SOCGUARD 工具 也能 帮助安全 团队简化 系统检查， 维护、升级、 和 一般的 安全 运营。 这些 实践 依赖工作流程 尽可能多 作为回应， 和标准化 是需要的。 自动化 执行 将要 增加 准确性 和 更好的 插头 差距 那 离开系统 易受伤害的。

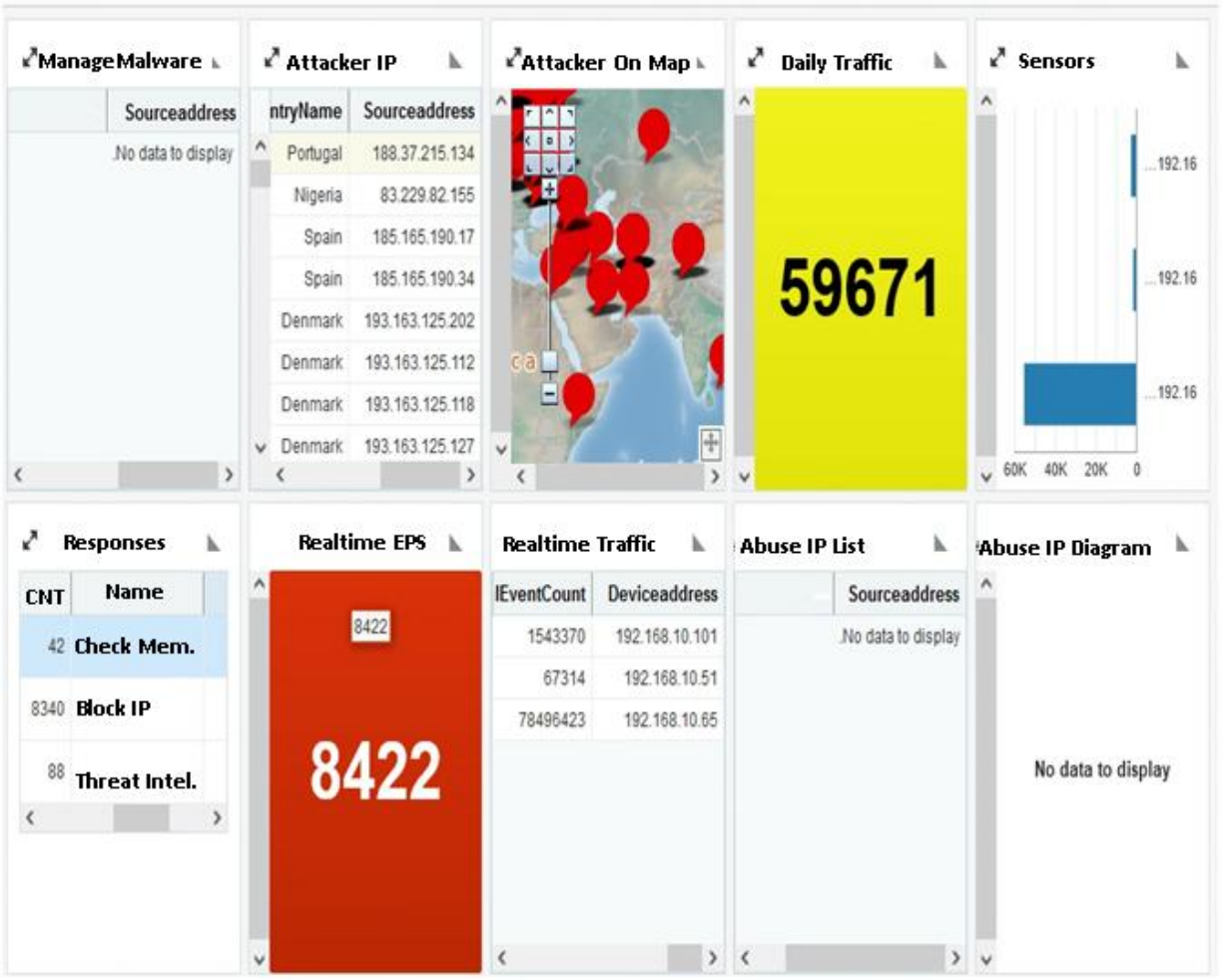
安全卫士 使用 案例：

使用 案例 为了 安全卫士 将要 各不相同 取决于 在 这 环境 和 是 有限的 仅有的 经过这 创造力 的 这 组织 建筑学。

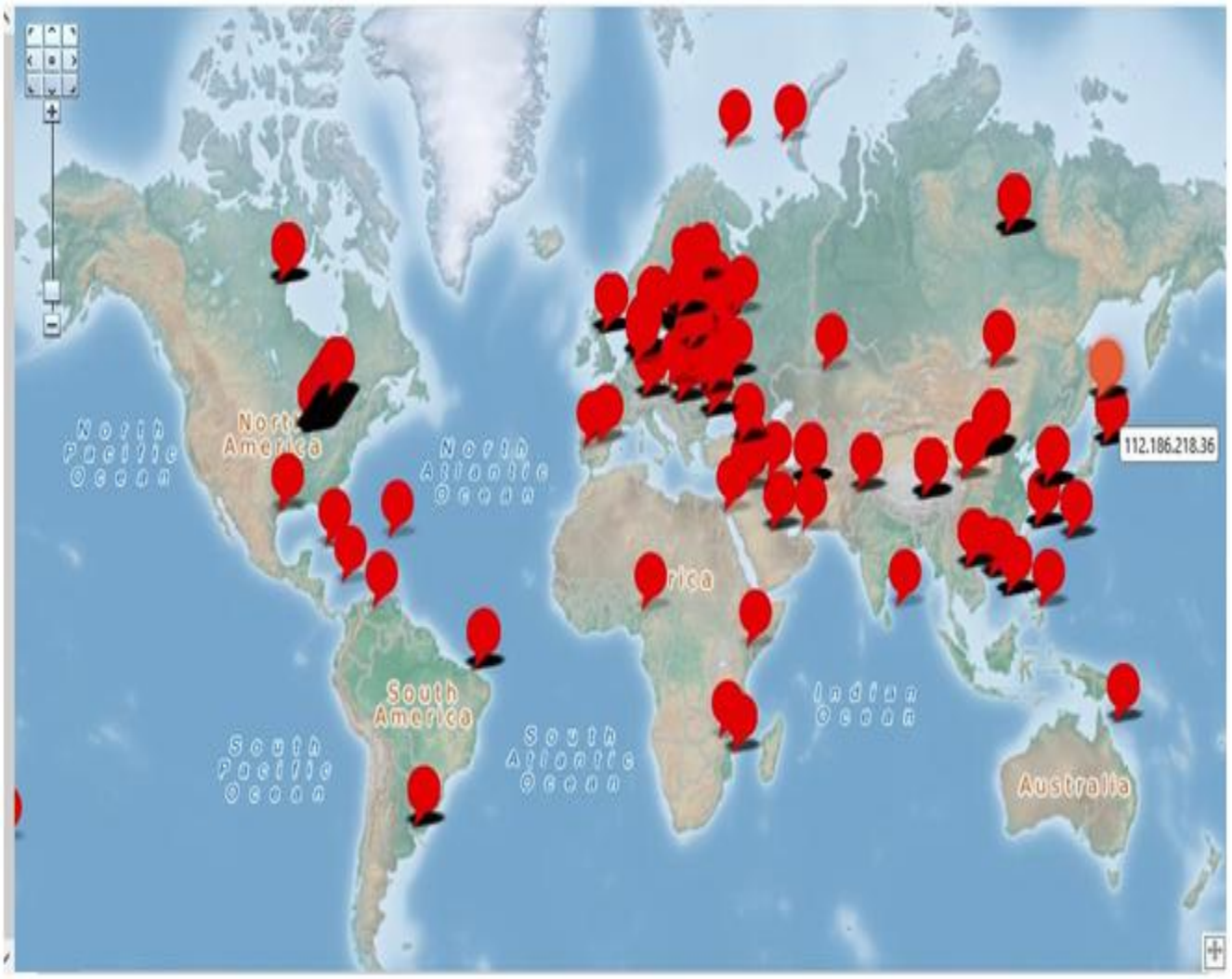
这里 是 这 我们可以定义的工作流程：



管理报告：


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

上的攻击者报告



翱翔 产品比较：

社会卫士	雷达	弧光	Splunk	太阳的风	产品/指标
好的	好的	好的	好的	好的	使用案例
大多	400+	400+	大多	-	数据源
1000000	1000000	100000	每日 PB 级数据	每天 2500 万	最大每股收益
机器学习、UEBA 和取证	机器学习、UEBA 和取证	机器学习	机器学习和 UEBA	异常行为	智力
软件或云	设备、软件或云	设备、软件或云	软件或云	虚拟设备	送货
SC、UF、系统日志、自定义	Wincollect，系统日志	SC、系统日志	超滤	扫描电子显微镜	支持代理
根据每日最大数据或每股收益	每月	根据每日最大数据或每股收益	根据每日最大数据英镑/天	每个节点	价钱

联系我们

销售经理：

卡里米先生

+989219427704

信息@socguard.ir