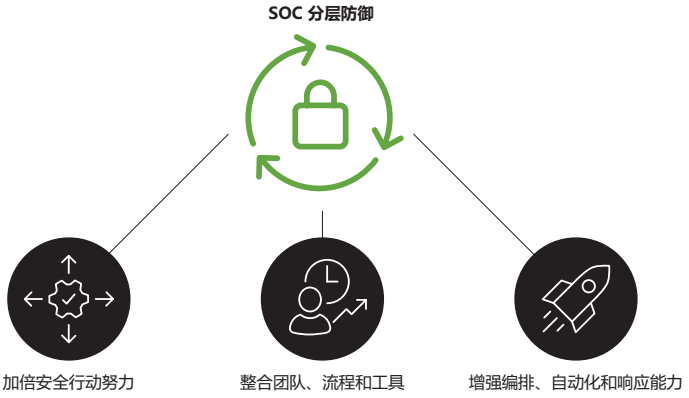
SPLUNK® PHANTOM

利用 SOLD 功能最大限度地提高您的 SOC 效率

- **通过加大安全运营力度，缩小安全技能差距**
- **整合您的团队、**流程和工具，提高 SOC 效率
- **借助高级编排、自动化和响应能力，**提升您的 SOC



安全团队正在努力识别、分析和减轻其组织面临的威胁。但是这些团队同样疲于将不同的安全产品拼接在一起，以及在互相没有编排的情况下对它们逐一操控。此外，大多数公司没有足够的安全人员来分析大量的日常事件，结果是安全事件的积压越来越多。

组织希望通过部署可以最大限度提高效率和规模的工具来更好地利用现有资源，同时创建统一的防御系统，实现一加一大于二的效果。

Phantom 将安全团队、流程和工具集成在一起，以便更智能地工作、更快地应对威胁并加强防御。

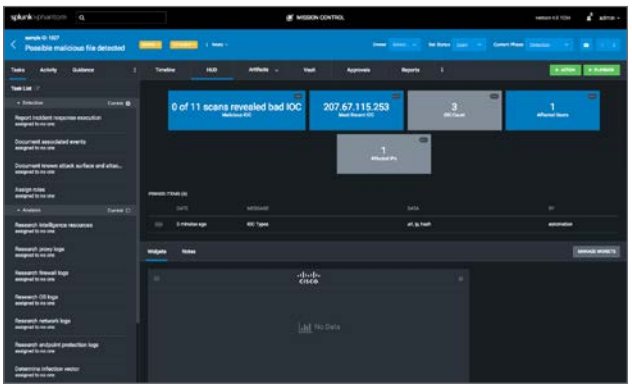
Splunk Phantom 提供了安全编排、自动化和响应 (SOAR) 功能，使分析师能够摆脱重复任务，并将注意力集中在做出最关键的任务决策上。通过将团队、流程和工具集成在一起，组织能够提高安全性和更好地管理风险。借助 Phantom，安全团队可以将任务自动化、将工作流编排起来并支持广泛的 SOC 功能，包括事件和案例管理、协作和报告。

SOC 自动化

使用 Phantom 进行事件丰富和程序化的分类，以消除噪音，以机器速度预获取威胁情报，支持决策，并为人类分析确定最关键事件的优先级。进行网络钓鱼调查，并在几秒钟内处理可疑的网络钓鱼电子邮件。通过自动执行恶意软件调查中的重复步骤来提高安全性，并降低总体平均解决时间 (MTTR)。

事件响应

Phantom 帮助安全团队更快地调查和应对威胁。从任务控制界面执行调查性质的安全动作，例如将文件提交到沙箱并查询威胁情报服务，而不会丢失调查的上下文。



使用 Phantom 进行案例管理，以提高与标准操作程序的一致性，编排人工和机器任务，并将所有与案例相关的数据和活动保存在一个集中的位置。增强合作，提高与其他团队成员就事件或案例交流的能力。还可以使用 Phantom 将事件案例和任务分配给适当的团队成员。

已准备了解更多?

下载 Splunk Phantom 的**免费社区版**，立即开始

splunk>

了解更多：www.splunk.com/asksales

www.splunk.com

PB-Splunk-Phantom-Maximize-Your-SOC-Efficiency-With-SOAR-106