Threat Intelligence Director

优势

- 使用开放式行业标准接口获取威胁情报
- 通过第三方情报增强网络传感器的效用
- 将危害表现传输到思科安全传感器以自动阻止或监控可疑活动
- 关联网络传感器的观察结果并发送事件警报
- 根据改进的安全情报改善安全状态

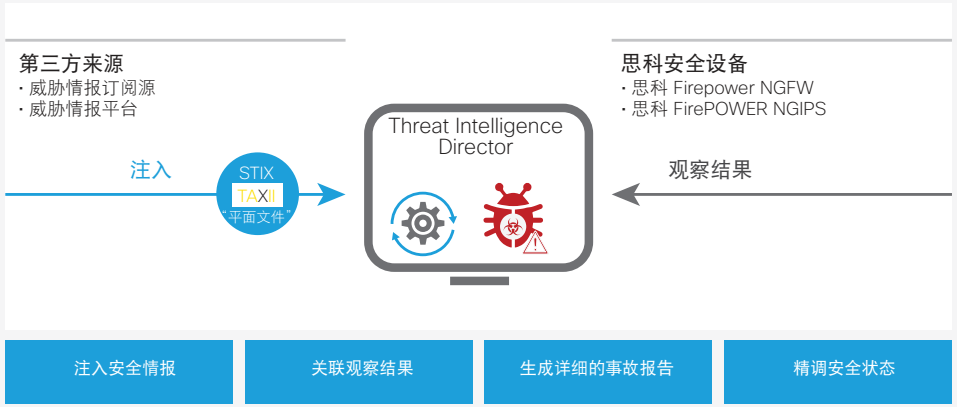
利用众多来源的情报

您的组织可能受到方方面面的威胁。恶意攻击者可能欺骗员工无意中下载恶意软件。组织中心怀不满的员工可能为获得经济利益而窃取公司资产。监控网络异常可能占用大量资源。

但是如果可以利用资源帮助您证实可疑行为的证据，然后自动采取行动遏制威胁会怎么样？Threat Intelligence Director 的目标正在于此。它首先会注入来自第三方威胁订阅源和威胁情报平台的威胁情报，然后将之与来自思科安全传感器的观察结果相关联，以检测安全事件并发出警报。您无需人工调查可能是良性的警报，因而可以专注处理已被自动阻止或监控的真实事件。

Threat Intelligence Director 不同于完全依赖本地威胁情报的安全设备，它可以利用第三方威胁订阅源提供更有效的安全。通过将情报转换为能够采取行动消除的危害表现，您的网络防御工具可以阻止或监控更多威胁，减少待审核的警报数量，改善整体安全状态。通过注入和分发更多来源的威胁情报，降低了管理复杂性以及查看和追踪误警报的必要性。

集成第三方安全情报



加快事件响应速度并实现自动化

利用第三方情报自动关联危害表现并采取行动。

请访问思科技术联盟合作伙伴列表，查看有助确保情报更切实可行的第三方威胁情报来源和威胁情报平台合作伙伴最新列表。