Trellix

Cyberworld

Trellix Helix Connect

通过由人工智能引导的调查和响应进行多向量和多供应商检测

原生和开放集成

- 端点检测和响应 (EDR)
- 身份管理平台
- 移动设备安全
- 威胁情报
- 漏洞管理
- 云安全
- 保护数据
- 网络安全
- 云原生安全解决方案，例如：云访问安全代理(CASB)和云工作负载保护平台(CWPP)
- 电子邮件和协作
- 欺诈检测

单点解决方案和多种工具集合使检测和响应变得冗长且手动化，导致威胁行为者未被检测到。扩展检测和响应 (XDR) 解决方案集成来自多个来源的数据，分析这些数据以提供上下文，从而更快地检测和响应事件。但并非所有解决方案都提供相同水平的上下文。

当您评估适合您业务的解决方案时，了解产品在集成和分析方面的表现，以及如何运用数据（无论是来自供应商的技术还是第三方）是非常重要的。解锁您已拥有的数据、供应商工具中的数据的能力，是衡量解决方案在 XDR 中创建 “X” 的标准。

Trellix Helix Connect 是如何运作的？

Trellix Helix Connect 集成了来自安全工具（Trellix 原生控件和 490 多个第三方）的数据，以全面讲述攻击的全过程。数据从多个来源采集，然后通过预构建的分析和规则进行关联，以创建多向量、多供应商检测。新检测在部署后数小时内就会出现，并根据严重程度进行优先级排序，50%到70%的误报已被移除。内置的自动化功能还可以消除常规威胁，并执行数据整合、设备控制、禁用用户、为工单系统和数百个第三方组件创建事件等任务。

人工智能可帮助任何经验水平的用户进行调查、威胁搜寻和事件响应。其中包括为分析师构建的多个自动化 Playbook，可进一步提高效率。来自Trellix高级研究中心团队的持续性机器学习、监察和洞察，确保最新的攻击向量、行为和更改建议，只需点击一下即可获得。

图 1：数据被采集、关联并与威胁情报进行情境化。内置 Playbook 为分析师提供了一个集成的工作体验，并实现自动化修复。

Trellix Helix Connect 有何独特之处？

- **深度集成：**Trellix Helix Connect 通过与 230 家供应商的 490 多个集成来满足您的需求，以便您使用更多的已有数据。
- **开箱即用的检测：**数据以实时方式采集，使用 2,000 多条规则和 50 种分析方法创建上下文，无需数月的检测工程。
- **无破坏性要求：**Trellix Helix Connect 是开放的，没有原生控件要求，您可以使用现有工具或 Trellix XDR 平台，并从中获得更多价值。
- **为每位分析师提供编排和自动化：**Trellix Helix Connect 配备了跨 250 个第三方组件编排和交付自动化的功能。增强您的SIEM，并通过人工智能引导和UI驱动的点击操作来实现自动化流程，使更多的安全团队成员能够调查威胁。
- **您环境中的安全综合视图：**通过使用统一的分析体验，减少手动调整，将非响应活动所花费的时间减少 90% 。

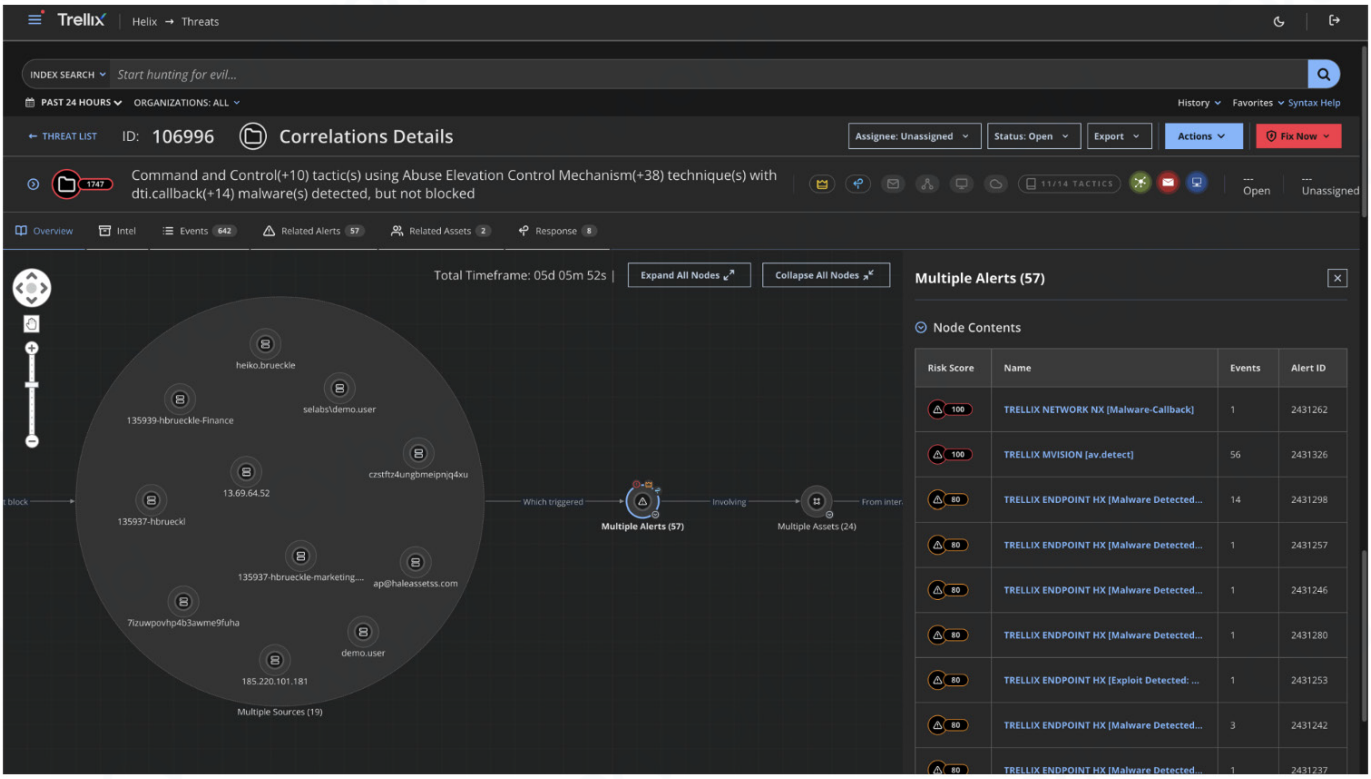

图 2：Trellix Helix Connect 一目了然地显示与威胁关联的多个警报。

Trellix Helix Connect 能为您的业务做什么？

- **加快您的平均检测时间（MTTD）和平均修复时间（MTTR）：**得益于 Trellix Helix Connect 的深度分析、人工智能和用户友好的体验，调查威胁和采取响应措施的平均时间不到 10 分钟，您的安全团队还可以消除跨点工具的枢轴，从而将效率提高 20%！

- **提高您的安全团队效率：**误报会浪费大量时间。在误报到达之前，Trellix Helix Connect 就阻止了50%到70%的误报，并根据严重程度对重要警报进行优先级排序，为您节省数小时或数天的时间。

- **缩小安全人才和技能差距：** Trellix Helix Connect 拥有比行业同质解决方案更多的预构建Playbook，能够根据您的需求进行定制，可以帮助您提升经验不足的分析师的技能。他们可以点击关联详细信息，使用引导式调查，通过最佳实践来执行数据整合或修复步骤，从而提高他们的专业知识。

- **快速实现价值：** Trellix Helix Connect 开箱即用，可在一周内完成部署。用户在部署后几个小时内就能发现之前遗漏的检测和新见解。相比之下，行业同质解决方案需要数周或数月的检测工程、集成工作或产品更换才能使用其XDR产品。Trellix Helix Connect 能够满足您的需求，并且可以在任何平台或环境中使用，从云端到本地或隔离环境。