

Trellix Wise: GenAI能解决您面临的 最大安全运营挑战

主要特点

消除警报疲劳

Wise会自动调查您的所有警报,通过自动升级和警报评分,将最重要的警报置于顶部。

更快地做出正确决策

通过对1.5PB的威胁情报数据和多向量控制,进行深度自动化EDR调查,检测其他人错过的威胁,包括利用人工智能的威胁。

弥补安全人才缺口

使用日常语言让每个人都能创建GenAI内容,同时运用基于十年现实世界专业知识的提示来提升安全团队技能。

快速证明投资回报率

跟踪Wise为您节省的时间,并通过内置报告和仪表板轻松展示效率和效能的提升。每调查100条警报,Wise可节省8小时的安全运营中心(SOC)工作时间,使您能够从响应转向预防,并阻止更多威胁。

安全团队似乎每年都面临同样的问题:漏报威胁、警报数量增加和人才缺口。随着数据持续爆炸式增长、网络安全岗位空缺以及单点工具集合无法在业务受到影响之前检测到复杂的威胁,安全团队面临的问题只会越来越严重。

如今,这些问题终于有了答案,那就是 Trellix Wise。Trellix Wise 通过**分析、人工智能和自动化**来帮助客户转变其安全运营。安全团队可以使用Wise来**自动调查所有数据**,消除误报,自动修复,并使用对话式人工智能进行威胁搜寻,无论安全团队当前的专业水平如何。

再也不会错过警报

由于安全工具生成了大量警报且误报率较高,大多数安全团队成员仅查看大约 10% 的警报。如果安全团队使用了Trellix Wise,就能消除警报疲劳。Wise是建立在十多年的人工智能建模和25年的分析、机器学习经验之上,会自动调查每条警报,使用数据的完整上下文来决定安全团队何时需要采取行动。那么,安全团队不再被大量警报淹没,而是有机会深入挖掘并发现高级的人工智能攻击。

通过人工智能调查深入挖掘数据

一旦发现事件,Trellix Wise将自动调用Trellix丰富的端点检测和响应(EDR)数据。Wise运用端点、电子邮件、网络和沙箱产品中的33个机器学习模型,做出决策并为安全团队提供详细解释。警报评分会提高,以便分析师能够正确查看和确定其优先级。这通常需要3到5个人花几个小时才能完成,现在只需几秒钟即可完成!

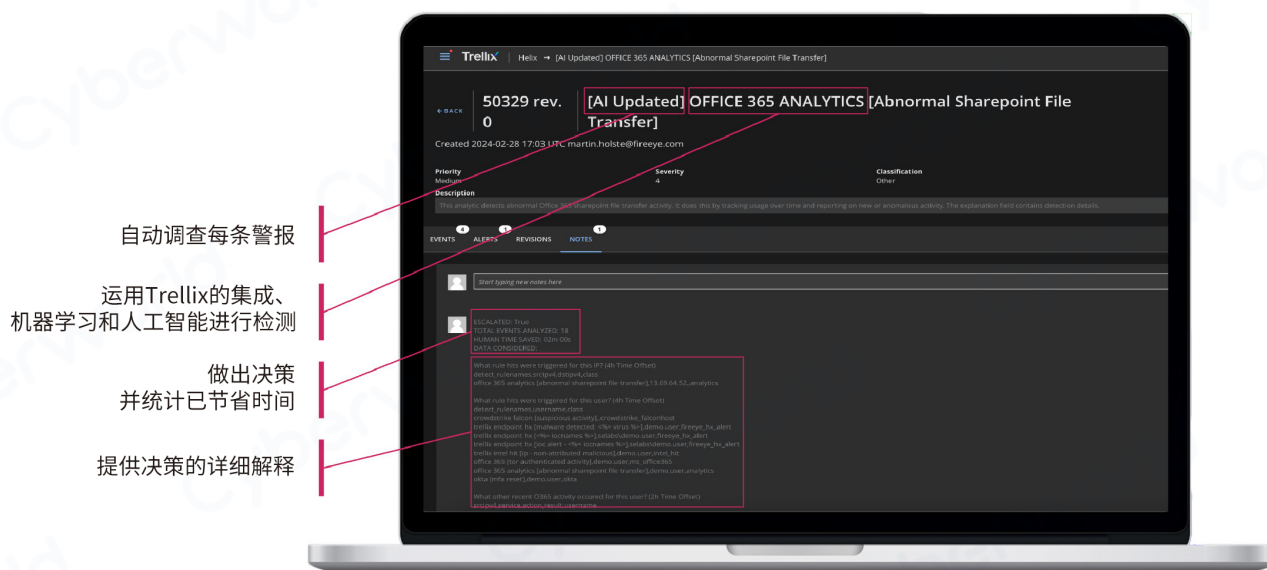


图 1: Trellix Wise 使用内置的机器学习、人工智能和 GenAI 在几秒钟内做出决策。

Trellix Wise 的不同之处

- 提供的第三方集成数量是行业同质解决方案的 3 倍, 将 GenAI 价值应用于更多环境, 并发现具有复杂杀伤链的高级威胁。
- 运用具有 1.5PB 遥测数据的大数据生态系统自动分类威胁, 以便根据正确的数据做出正确的决策。
- 每天使用来自 6.6 亿个端点的 600 亿次查询来获取实时的、现实世界的操作威胁情报。

让威胁搜寻变得触手可及, 并提升员工的技能

威胁搜寻和设置自动化操作不再依赖于获得高技能的分析师。通过 Trellix Wise, 任何级别的用户都可以使用常见语言查询进行交互、创建自动化流程和搜寻威胁。这几乎可以是任何内容, 例如“仅在星期五升级来自销售部门的警报”或“如果某个资产面向公众并且有超过10次登录失败尝试, 则始终升级警报”。

当 Trellix Wise 进行分析时, 它会提供发现的详细信息和采取的补救措施。即使是经验最少的安全团队成员, 也能进行调查、响应并在工作中学习威胁搜寻。

快速证明价值

通常，企业很难知道从任何特定的安全投资中获得多快或多少回报。Trellix Wise 会跟踪节省的时间，以便您可以在用户界面中查看或向领导团队报告效率和效能的提升。您可以在图形和列表格式的报告查看由人工智能节省的总时间、事件数量以及调查的速度和严重程度。

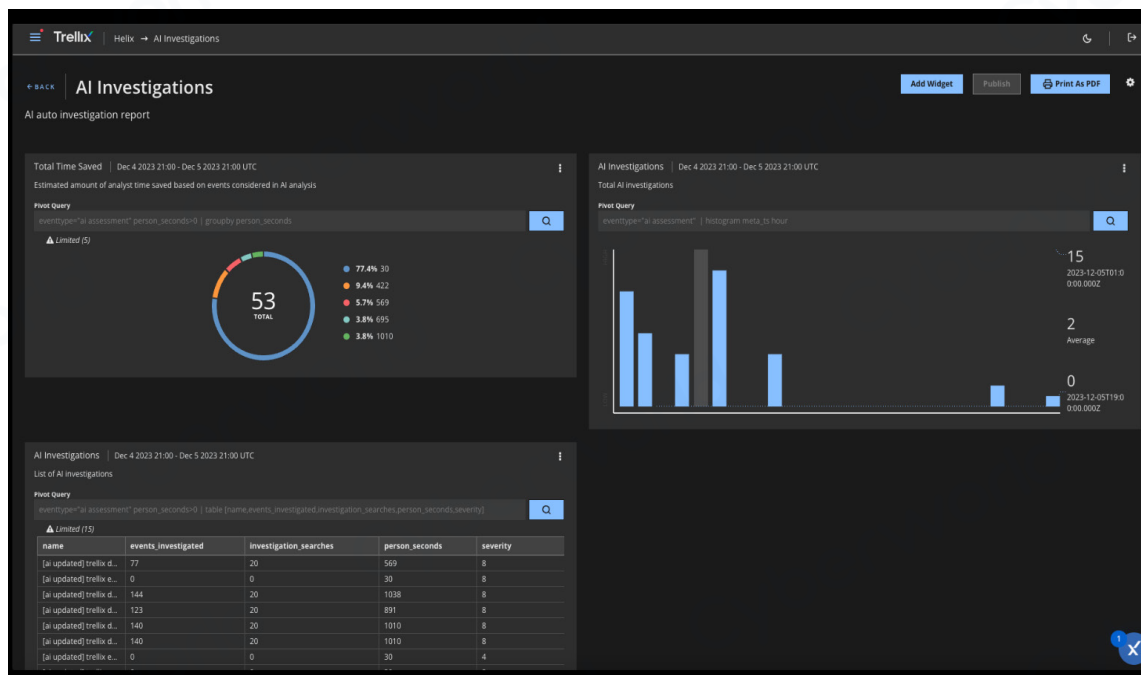


图 2: Trellix Wise 会跟踪为您节省的时间,并在 Trellix 的用户界面中以图形方式显示。

使用 Trellix Wise 解决当今最大的安全挑战

不要推迟那些可以真正提升您的效率和效能的改变,要更好地运用您现有的资源。Trellix Wise 连接了数百种安全工具,可以在本地、隔离网络和云环境中实施。使用 Trellix Wise,您的企业可以解决一些最常见的挑战:

- **在3分钟内自动进行警报调查:**确保在3分钟内对所有警报进行分类、范围界定和评估。
- **减少平均检测时间(MTTD):**对90%以上的警报进行分类、范围界定和调查,每天可节省 5 名分析师的工作量。
- **改进平均调查时间(MTTI):**自动化事件遏制和简化调查,使用风险评分和建议总结事件。
- **将平均修复时间(MTTR)提高多达300%:**使用由人工智能驱动响应,以更快、更准确的响应降低企业风险。
- **更好地运用现有资源:**通过自动化和加速的工作流程、安全内容创建以及自然语言人工智能交互。