Trellix

Cyberworld

Trellix 威胁情报交换 (TIE)

Trellix TIE (Threat Intelligence Exchange, 威胁情报交换) 作为信誉代理，可实现自适应威胁检测和响应。它结合了您企业内安全解决方案的本地情报和外部全球威胁数据，在您的安全生态系统中即时共享这些集体情报，使解决方案能够交换并根据共享情报采取行动。

创建一个协作威胁情报生态系统

作为信誉代理，Trellix TIE将全球各来源的威胁情报相结合，情报来源涵盖了Trellix GTI (Global Threat Intelligence, 全球威胁情报)、第三方威胁信息 (如VirusTotal)、以及本地的端点、网关和高级分析解决方案。

通过使用 Trellix DXL (Data Exchange Layer, 数据交换层)，可以在您的安全生态系统中即时共享这些集体情报，让安全解决方案作为一个整体运行，从而增强整个企业的网络安全性。

跨安全解决方案共享威胁情报

主要优势：

- 自适应威胁防护将高级针对性攻击从遭遇到遏制的时间从几天、几周和几个月缩短到几毫秒。
- 协作威胁情报是由全球情报数据源与本地威胁情报收集相结合而构建的。
- 相关的安全情报在端点、网关、网络和数据中心安全解决方案之间实时共享。
- 根据端点上下文（文件、进程和环境属性）与集体威胁情报相结合，对从未见过的文件做出决策。
- 通过TDXL简化了集成。将Trellix和非Trellix安全解决方案连接在一起，以实时操作威胁情报，可以降低实施和运营成本。

Trellix DXL实现了集成简便性，大大降低了大量直接应用程序编程接口(API)集成的实施和运营成本，并提供了无与伦比的安全性、有效性和运营效率。Trellix DXL采用开放框架设计，使所有安全解决方案都能够动态加入 Trellix TIE 生态系统，包括第三方安全产品。

自适应威胁防护

从网络各个位置检测到的每条共享见解，都能帮助企业更深入地了解针对性攻击的危害。由于这些威胁本质上是高度针对性的攻击，企业需要一个本地监察系统来捕捉趋势和任何独特的攻击。从遭遇中收集的本地上下文数据与全球威胁情报相结合，可以更好地对以前未见过的文件做出决策，从而更快地实现保护和检测。

当在网络上的任何位置遇到未识别的文件时，系统会联系 Trellix TIE 来确定该文件是否存在信誉。描述性元数据，例如普及率和时间，也会得到维护，并反映在集体情报中。

除了请求信誉，集成的安全解决方案还可以根据本地判定向Trellix TIE提供信誉更新。然后，更新后的信誉会实时反映到您的所有系统中。这些本地威胁情报会被存储起来以备将来使用，这意味着如果在另一台设备或服务器上再次发现该威胁，它将不再是未知威胁，而是会立即被检测到。

Trellix TIE 使管理员能够轻松定制威胁情报。安全管理员能够汇编、覆盖、增强和调整全面的情报信息，以定制针对其环境和企业的保护。这些本地优先和调整的威胁信息可为未来的任何遭遇提供即时响应。

加强保护实施点

整个网络的集成解决方案，从端点到网络边缘，根据可用的信誉、元数据或数据点组合应用策略。一个紧密集成的解决方案Trellix终端安全，运用组合的本地情报（文件元数据，例如普及率和时间，以及其他安全组件提供的本地信誉）和当前可用的全球威胁情报来做出准确的决策。

例如，一个没有全球信誉但在企业内具有高普及率的自定义应用程序不会产生恶意综合信誉，并且很可能会被允许运行。另一方面，一个在企业中从未见过的文件，没有全球或本地信誉，并且打包可疑，很可能会产生较低的信任级别，从而触发阻止或需要进一步调查，这些是通过Trellix终端安全引擎或Trellix智能沙箱进行。

Real Protect、Trellix 终端安全的机器学习功能和动态应用程序遏制功能进一步增强了端点检测和保护。Real Protect 通过执行前和执行后分析在云端查找最新的威胁情报，而动态应用程序遏制可防止端点上的恶意活动，保护第一台暴露于新威胁的机器，同时执行其他分析。

高级针对性攻击是现实世界中的挑战

高级针对性攻击旨在阻止检测，并在企业中建立持久立足点。它会持续困扰着企业，窃取高价值数据。

从协作中受益

高级威胁分析

如果需要更多关于文件的信息，可以自动从 Trellix TIE 发送到 Trellix 高级分析解决方案，如Trellix智能沙箱，以立即获得对潜在新威胁的额外见解，并确定相关文件的信誉。所有这些都是自动化的、记录在案的，并通过 Trellix DXL 集体共享，以保护您的整个安全生态系统。

安全事件管理

Trellix企业安全管理器使您能够深入调查由 Trellix TIE 识别的 IoC。访问历史安全信息和创建自动监视列表的能力可提高企业的安全效率。

Trellix

关于 Trellix

Trellix是一家重新定义网络安全未来的全球性公司。它的开放式原生扩展检测和响应（XDR）平台，可帮助企业抵御当今最先进的网络威胁攻击，并保护其业务不受影响。Trellix安全团队和庞大的合作伙伴生态系统，运用人工智能、机器学习和自动化加速技术创新，为 40,000 多家企业客户提供服务。