云可视性报告

报告提供有价值的统计信息，您可以使用这些信息了解网络及其一般运行状况，并相应地做出决策。多云防御 提供生成以下类型报告的功能：

发现

通过从 DNS 查询和 VPC 流日志获取带外流量信息，并将数据与威胁情报和云资产信息相关联，生成 生成发现报告 。仅当您将云服务提供商的 VPC 配置为将日志发送到 S3 存储桶，然后将其直接传输到 多云防御控制器时，这些日志才可用。

威胁指标快照

生成威胁和云分析报告 报告是有关网关实例的数据的汇编。您可以使用此报告通过检查流量模式、满足阈值的时间和方式、攻击趋势和特定实例来确定网关在威胁下的持久性。该报告包括以下要点：

- **IDS/IPS 检测** - 此数据是在所选时间范围内检测到的攻击数量、攻击类型、检测到的攻击的时间以及前十个 IDS/IPS 签名。
- **WAF 检测** - 此数据是 WAF 规则检测到的攻击数量、检测到的攻击的时间以及所选时间范围内的前十个 WAF 签名。
- **按数量划分的威胁地理位置** - 此区域分布图按国家/地区显示 WAF 和 IDS/IPS 事件的攻击量。
- **按数量和时间划分的前十个攻击国家/** 地区 - 此水平条形图描绘了在整个时间跨度内产生最多事件的前 10 个国家/地区的数量，然后按时间间隔内发生事件的时间增量显示该数量。
- **策略和预防** - 此数据图表显示网关安全类型在其部署的任何 CSP 环境中采取的操作。这包括操作类型、操作生成的事件数量、网关安全类型等。

请注意，您 **必须** 在策略中启用 Web 应用防火墙 (WAF)、入侵检测和保护 (IDS/IPS) 规则， 多云防御网关 才能收集和轮询数据。

有关其他信息：

- 生成发现报告, on page 2
- 生成威胁和云分析报告 ， 第 2 页

生成发现报告

通过获取在由 多云防御控制器处理之前已发送到 S3 存储桶的 DNS 查询和 VPC 流日志来生成发现报告。

使用以下程序生成执行发下报告：

步骤 1 在 多云防御控制器 页面中，导航至 **报告**。

步骤 2 选择 **工具**。

步骤 3 点击 **生成** 按钮。报告将在新选项卡中生成。

步骤 4 报告已生成。要在本地保存报告，请点击 **打印报告** 并导航至要在本地服务器上保存报告的位置。

生成威胁和云分析报告

威胁和云分析报告是使用 多云防御网关收集和检查的流量生成的 **威胁指标快照** 。这提供了更全面的报告，因为 多云防御 现在位于数据路径中，并补充发现报告。

请注意，无法生成当天的报告，因为在一天结束、月末、季度末或年末之前，无法对事件进行定性汇总。

注释 您 **必须** 在策略中启用 Web 应用防火墙 (WAF)、入侵检测和保护 (IDS/IPS) 规则， 多云防御网关 才能收集和轮询数据。有关详细信息，请分别参阅以下链接：

- Web 应用防火墙
- 网络入侵 (IDS/IPS) 配置文件

使用以下程序生成具有威胁指标快照的威胁和云分析：

步骤 1 在 多云防御控制器 页面中，导航至 **报告**。

步骤 2 选择 **威胁指标快照**。

步骤 3 使用下拉菜单选择提取数据的 **频率** ：每天、每周、每月、每季度或每年。

- **每天** - 从上午 12 点开始，持续 24 小时。这是 UTC 时间。
- **每周** - 从星期一到星期日。
- **每月** - 通常是从月初到月末。
- **季度** - 从一夸脱的开始到结束。季度通常定义为1月1日至3月31日、4月1日至6月30日、7月1日至9月30日和10月1日至12月31日。

- **每年** - 从所选年份的 1 月 1 日到 12 月 31 日。

步骤 4 使用下拉 **列表** 选择要收集数据的时间范围或特定日期。灰显的天数没有要编译的数据。如果没有可用于生成报告的数据，请确认您的策略包含 WAF 和 IDS/IPS 规则。

步骤 5 点击**生成报告**。

步骤 6 报告已生成。要在本地保存报告，请点击 **打印报告** 并导航至要在本地服务器上保存报告的位置。

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。