日志记录转发概述

日志转发 - 安全事件和流量日志

安全信息事件管理 (SIEM) 系统是专门将安全信息和安全事件信息整合到一个管理平台中的解决方案。安全和事件信息将来自配置为将此信息转发到 SIEM 的第三方安全解决方案。

多云防御 支持直接在 UI 中查看安全事件信息。这些事件在“ **调查** > **流分析** ”部分下可用。事件分类和查看方式如下：

类别	类型	说明
流日志	FLOW_LOG	与流量的不同阶段相关的信息
防火墙事件	APPID	根据应用 ID (OpenAppID) 匹配的流量
	GEOIP	源自或发往 Geo IP 的流量 (MaxMind)
	L4_FW	基于第 4 层信息（源/目标 IP/端口和协议）匹配的流量
	MALICIOUS_IP	源自或发往恶意 IP 的流量 (Trustwave)
	SNI	根据 SNI 信息匹配的流量

类别	类型	说明
网络威胁	防病毒	检测到病毒的流量 (ClamAV)
	DPI	检测到 IDS/IPS 威胁的流量 (TALOS)
	DLP	敏感数据被泄露的流量
Web 保护	WAF	检测到 Web 应用威胁的流量 (ModSecurity)
	L7DOS	导致第 7 层 DOS 攻击的流量
URL 过滤	URLFILTER	与 URL 类别或 URL 匹配的流量 (BrightCloud)
FQDN 过滤	FQDNFILTER	与 FQDN 类别或 FQDN (BrightCloud) 匹配的流量
HTTPS 日志	HTTP_REQUEST	与基于 Web 的流量 (HTTP) 相关的信息
	TLS_ERROR	与 TLS 错误相关的信息
	TLS_LOG	与 TLS 行为相关的信息
流量摘要日志	SESSION_SUMMARY	有关每个已处理流量会话的摘要信息

Note 流日志在 2.10 及更高版本的网关中已弃用。每个流日志中包含的信息作为 **流量摘要** > **日志**中可用的会话信息的一部分提供。

可以使用日志转发配置文件将每个事件类别发送到 SIEM。 多云防御 当前支持的 SIEM 包括：

- AWS S3 存储桶
- Datadog
- GCP 日志记录
- Microsoft Sentinel
- Splunk
- Sumo Logic
- 系统日志

可以使用下面列出的步骤操作日志转发配置文件：

创建独立事件或流量日志配置文件

步骤 1 导航至 **管理** > **配置文件** > **日志转发**。
步骤 2 点击**创建 (Create)**。
步骤 3 指定配置文件名称和说明。
步骤 4 将 类型 指定为独立。
步骤 5 填写适当的参数（请参阅 SIEM 特定文档）。
步骤 6 点击**保存**。
步骤 7 添加所需的网关关联（请参阅 将事件、流量日志转发配置文件或指标转发配置文件添加到网关）。

编辑独立事件或流量日志配置文件

步骤 1 导航至 **管理** > **配置文件** > **日志转发**。
步骤 2 选中要 编辑的配置文件旁边的复选框。
步骤 3 点击**编辑**。
步骤 4 根据需要修改参数（请参阅 SIEM 特定文档）。
步骤 5 点击**保存 (Save)**。

创建组事件或流量日志配置文件

步骤 1 导航至 **管理** > **配置文件** > **日志转发**。
步骤 2 点击**创建 (Create)**。
步骤 3 指定配置文件名称和说明。
步骤 4 将 类型 指定为组。
步骤 5 根据需要添加尽可能多的行，以适应要分组的独立配置文件的数量。
步骤 6 点击**保存**。
步骤 7 添加所需的 **网关关联** （请参阅 将事件、流量日志转发配置文件或指标转发配置文件添加到网关）。

编辑组事件或流量日志配置文件

步骤 1 导航至 **管理** > **配置文件** > **日志转发**。

步骤 2 选中要 编辑的配置文件旁边的复选框。

步骤 3 点击**编辑**。

步骤 4 修改、添加或删除独立配置文件。

步骤 5 点击**保存 (Save)**。

查看事件或流量日志转发配置文件

步骤 1 导航至 **管理** > **配置文件** > **日志转发**。

步骤 2 选择要查看 详细信息的配置文件链接。

步骤 3 查看 详细 信息。

删除事件或流量日志配置文件

使用以下程序从控制面板删除配置文件：

Before you begin

在从控制面板中删除配置文件之前，**必须**删除事件或配置文件与网关之间的关联。有关详细信息，请参阅 从网关中删除事件、流量日志转发配置文件或指标转发配置文件 。

步骤 1 导航至 **管理** > **配置文件** > **日志转发**。

步骤 2 选中要 编辑的配置文件旁边的复选框。

步骤 3 点击**删除 (Delete)**。

步骤 4 点击 **是** 或 **否** 确认 删除操作。

网关指标转发配置文件

此配置文件旨在转发 多云防御网关 生成的网关指标，以进行数据监控和分析。虽然指标由网关生成，但 多云防御控制器 会将指标转发到第三方分析应用。使用此转发配置文件，您无需登录 多云防御即可监控、分析和组织网关指标。使用此信息来衡量网关环境的性能和行为；您还可以利用此信息进行环境故障排除。

注释 从 多云防御控制器 版本 23.09 开始，仅支持 Datadog 作为第三方分析应用。

对于大多数可用的分析应用（例如 Datadog），您必须已经是授权用户才能访问该工具的 API 和呈现的数据。

创建独立指标转发配置文件

使用以下程序为指标转发创建独立配置文件：

开始之前

在创建此配置文件之前，您必须至少有一个第三方应用来转发指标。

步骤 1 导航到 **管理器** > **配置文件** > **指标转发**。

步骤 2 点击**创建 (Create)**。

步骤 3 输入唯一的 **名称**。

步骤 4 （可选）输入**说明 (Description)**。这可能有助于与具有相似名称的其他配置文件区分开来。

步骤 5 展开 **类型** 下拉菜单，然后选择 **独立**。

步骤 6 拓展 **目标** 下拉菜单，然后选择第三方应用来处理和分析指标。

步骤 7 输入要用作指标的 **终端** 位置的终端。

步骤 8 点击**保存**。

如果选择 Datadog 作为分析应用，则默认情况下会使用 HTTPS Webhook 填充 **终端** 。如果默认设置，可以在保存配置文件之前修改此条目。

下一步做什么

- 查看配置文件详细信息
- 将网关关联添加到配置文件

编辑独立指标转发配置文件

使用以下程序编辑已创建的独立配置文件。

步骤 1 导航至 **管理** > **配置文件** ，然后选择相应的配置文件 **类型**。

步骤 2 选中要编辑的配置文件旁边的复选框。

步骤 3 点击**编辑**。

步骤 4 根据需要修改参数。

步骤 5 点击**保存 (Save)**。

创建组指标转发配置文件

在此过程中，您需要创建一个配置文件，然后将其分配给特定网关。组配置文件最多组合五个独立的指标转发配置文件，然后可以将其分配给单个网关。使用以下程序创建分组指标转发配置文件：

开始之前

- 在创建此配置文件之前，您必须至少有一个第三方应用来转发指标。
- 您必须至少创建两个独立的指标转发配置文件。有关详细信息，请参阅创建独立指标转发配置文件。

步骤 1 在 多云防御控制器 界面中，导航到 **管理器** > **配置文件** > **指标转发**。

步骤 2 点击**创建 (Create)**。

步骤 3 输入唯一的 **配置文件名称**。

步骤 4 （可选）输入**说明 (Description)**。这可能有助于区分具有相似名称的配置文件。

步骤 5 展开 **类型** 下拉菜单，然后选择 **组**。

-
- **说明** - 输入说明以帮助将此配置文件与其他独立配置文件区分开来。
- **类型** - 选择 **组**。

步骤 6 在组详细信息下，为需要添加到配置文件的每个新行点击 **添加** 。

步骤 7 展开每行的下拉菜单，选择要添加到组的配置文件。如果要在保存之前删除配置文件，请选中配置文件的复选框，使其突出显示，然后选择 **删除**。

步骤 8 点击**保存 (Save)**。

下一步做什么

- 查看配置文件详细信息
- 将网关关联添加到配置文件

编辑组配置文件

使用以下程序编辑已创建的一组分组配置文件：

步骤 1 导航至 **管理** > **配置文件** ，然后选择相应的配置文件 **类型**。

步骤 2 选中要 编辑的配置文件旁边的复选框。

步骤 3 点击**编辑**。

步骤 4 修改、添加或删除组配置文件。

步骤 5 点击**保存 (Save)**。

删除配置文件

使用以下程序从控制面板删除配置文件：

开始之前

您**必须先**删除配置文件和网关之间的关联，然后才能从控制面板中删除配置文件。有关详细信息，请参阅 从网关中删除事件、流量日志转发配置文件或指标转发配置文件 。

步骤 1 导航至 **管理** > **配置文件** ，然后选择相应的配置文件 **类型**。

步骤 2 选中要删除的配置文件旁边的复选框。

步骤 3 点击**删除 (Delete)**。

步骤 4 点击 **是** 或 **否** 以确认或取消删除操作。

将事件、流量日志转发配置文件或指标转发配置文件添加到网关

步骤 1 导航至 **管理** > **网关**。

步骤 2 选中要与 配置文件关联的网关旁边的框。

步骤 3 点击**编辑**。

步骤 4 对于 日志配置文件 参数，请从菜单中选择所需的 配置文件 。

步骤 5 点击**保存 (Save)**。

从网关中删除事件、流量日志转发配置文件或指标转发配置文件

步骤 1 导航至 **管理** > **网关**。

步骤 2 选中要取消关联 配置文件的网关旁边的框。

步骤 3 点击**编辑**。

步骤 4 对于 日志配置文件 参数，请点击 配置文件 旁边的“X”将其删除。

步骤 5 点击**保存**。

Note 日志转发配置文件也可以在创建网关时与网关关联。 日志配置文件 参数在网关创建过程中可用，其中可以从菜单中选择所需的 配置文件 。

日志转发 - 发现日志

发现日志可以转发到安全信息事件管理 (SIEM) 系统，以汇聚到单个管理平台中。

多云防御 支持直接在 UI 中查看安全事件信息。这些事件在 **调查** > **流量** 部分下可用。事件分类和查看方式如下：

类别	类型	说明
DNS 日志	DNS_LOG	威胁情报与从云提供商收集的 DNS 日志信息的关联
VPC 日志	VPC_LOG	威胁情报与从云提供商收集的 VPC/VNet 流日志信息的关联

可以使用日志转发配置文件将每个类别发送到 SIEM，并将配置文件附加到自行激活的云账户。 多云防御 当前支持的日志转发目标包括：

- AWS S3 存储桶
- Datadog
- GCP 日志记录
- Microsoft Sentinel
- Splunk
- Sumo Logic
- 系统日志

要转发发现日志，请执行以下步骤：

创建独立发现配置文件

步骤 1 导航至 **管理** > **配置文件** > **日志转发**。

步骤 2 点击**创建 (Create)**。

步骤 3 指定配置文件名称和说明。

步骤 4 将 类型 指定为独立。
步骤 5 填写适当的参数（请参阅 SIEM 特定文档）。
步骤 6 点击**保存**。
步骤 7 将日志配置文件关联到所需的云账户（请参阅 使用云账户添加发现日志配置文件）。

编辑独立发现日志配置文件

步骤 1 导航至 **管理** > **配置文件** > **日志转发**。
步骤 2 选中要 编辑的配置文件旁边的复选框。
步骤 3 点击**编辑**。
步骤 4 根据需要修改参数（请参阅 SIEM 特定文档）。
步骤 5 点击**保存 (Save)**。

创建组发现日志配置文件

步骤 1 导航至 **管理** > **配置文件** > **日志转发**。
步骤 2 点击**创建 (Create)**。
步骤 3 指定配置文件名称和说明。
步骤 4 将 类型 指定为组。
步骤 5 添加一行以关联独立配置文件。
步骤 6 点击**保存**。
步骤 7 添加所需的网关关联（请参阅 将事件、流量日志转发配置文件或指标转发配置文件添加到网关）。

编辑组发现日志配置文件

步骤 1 导航至 **管理** > **配置文件** > **日志转发**。
步骤 2 选中要 编辑的配置文件旁边的复选框。
步骤 3 点击**编辑**。
步骤 4 修改、添加或删除独立配置文件。
步骤 5 点击**保存 (Save)**。

查看发现日志配置文件详细信息

步骤 1 导航至 **管理** > **配置文件** > **日志转发**。
步骤 2 选择要查看 详细信息的配置文件链接。
步骤 3 查看 详细 信息。

使用云账户添加发现日志配置文件

步骤 1 导航至 **管理** > **云** > **账户**。
步骤 2 选中要与 配置文件关联的云账户旁边的复选框。
步骤 3 点击 **操作** > **更新日志配置文件**。
步骤 4 为云日志转发配置文件选择 **日志配置文件** 对象。
步骤 5 点击**保存并继续**。

从云账户中删除发现日志配置文件

步骤 1 导航至 **管理** > **云** > **账户**。
步骤 2 选中要取消关联 配置文件的云账户旁边的框。
步骤 3 点击 **操作** > **更新日志配置文件**。
步骤 4 对于 云日志转发配置文件 参数，请点击 配置文件 旁边的 “X” 将其删除。
步骤 5 点击**保存并继续**。

删除发现日志配置文件

使用以下程序从控制面板删除配置文件：

Before you begin

您 **必须先** 删除配置文件和网关之间的关联，然后才能从控制面板中删除配置文件。有关详细信息，请参阅 从云账户中删除发现日志配置文件 。

步骤 1 导航至 **管理** > **配置文件** > **日志转发**。
步骤 2 选中要 编辑的配置文件旁边的复选框。

步骤 3 点击**删除 (Delete)**。

步骤 4 点击 **是** 或 **否** 确认 删除操作。

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。