日志转发目标/SIEM

日志转发 - AWS S3 存储桶

多云防御 支持将安全事件和流量日志转发到 AWS S3 存储桶，以发送安全事件和流量日志信息进行处理、存储、访问和关联。发送的信息采用半结构化 JSON 格式，可以访问和处理属性-值对。

要求

要将事件/日志转发到 AWS S3 存储桶，需要满足以下条件：

1. 创建新的或使用现有的 AWS S3 存储桶。
2. 将以下策略应用于 AWS S3 存储桶，以允许 多云防御控制器 访问和写入存储桶：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "<controller-role-arn>"
      },
      "Action": "s3:*",
      "Resource": [
        "arn:aws:s3:::<s3bucketname>/*",
        "arn:aws:s3:::<s3bucketname>"
      ]
    }
  ]
}
```

配置文件参数

参数	义务性	默认值	说明
配置文件名称	必需		用于引用配置文件的唯一名称。
说明	可选		配置文件的说明。
目标	必填	AWS S3	AWS S3 存储桶。
CSP 账户	必需		AWS S3 存储桶所在的 CSP 账户。
S3 桶	必需		将转发事件/日志的 AWS S3 存储桶名称。

日志转发 - Datadog

Datadog 是许多公司使用的一种非常常见且功能强大的 SIEM。多云防御 支持将日志转发到 Datadog，以发送安全事件和流量日志信息，以进行处理、存储、访问和关联。发送的信息采用半结构化 JSON 格式，可以访问和处理属性-值对。

要求

要将日志转发到 Datadog，需要以下信息：

- Datadog 账户
- 终端 URL
- API 密钥

Tip

- 要注册 Datadog 账户，请参阅 **Datadog 账户** (https://www.datadoghq.com/)。
- 要创建 Datadog API 密钥，请参阅 **Datadog API 密钥** (https://app.datadoghq.com/account/login?next=%2Faccount%2Fsettings#api)。

配置文件参数

参数	义务性	默认值	说明
配置文件名称	必需		用于引用配置文件的唯一名称。
说明	可选		配置文件的说明。

参数	义务性	默认值	说明
目标	必填	Datadog	用于配置文件的 SIEM。
跳过验证证书	可选	已取消选中	是否跳过验证证书的真实性。
API 密钥	必需		用于对通信进行身份验证的 Datadog API 密钥。
终端	必需	https://http-intake.logs.datadoghq.com/	用于接收转发的事件/日志的 URL 终端。

日志转发 - GCP 日志记录

GCP Stackdriver Logging 是 Google 云提供商 (GCP) 提供的一项服务，用于从应用和服务收集和存储日志。 多云防御 支持将日志转发到 GCP Stackdriver Logging，以发送安全事件和流量日志信息以进行处理、存储、访问和关联。发送的信息采用半结构化 JSON 格式，可以访问和处理属性-值对。

要求

必须为 GCP 多云防御-防火墙 服务账户分配 **日志编写者** 角色，网关才能将事件写入 GCP Stackdriver 日志。

配置文件参数

参数	义务性	默认值	说明
配置文件名称	必需		用于引用配置文件的唯一名称。
说明	可选		配置文件的说明。
目标	必填	GCP 日志记录（从网关）	用于配置文件的SIEM。
日志名称	必需	ciscomcd -gateway-logs	用于存储事件的 Stackdriver 日志的名称。

字段整数到字符串的映射

从控制器转发事件时，控制器会引入事件字段值到友好名称的映射。当事件直接从网关转发（例如，GCP 日志记录）时，不涉及控制器，因此事件字段值不会映射到友好名称。为了解释这些字段，用户负责执行字段值到友好名称的映射。

下面提供了友好映射的字段、子字段及其值：

字段	整数	字符串
action	0	DUMMY_ACTION
	1	允许
	2	拒绝
	3	DROP
	4	REDIRECT
	5	代理
	6	日志
	7	其他
	8	DELAY
	9	DETECT_SIG

字段	整数	字符串
gatewaySecurityType	1	INGRESS_FIREWALL
	2	EAST_WEST_AND_EGRESS_FIREWALL

字段	整数	字符串
水平	1	DEBUG
	2	INFO
	3	通知
	4	警告
	5	错误
	6	严重
	7	ALERT
	8	危急

字段	整数	字符串
policyMatchInfo.serviceType	0	未知
	1	代理
	2	转发
	3	REVERSE_PROXY
	4	FORWARD_PROXY

字段	整数	字符串
protocol **sessionSummaryInfo.egressConnection.protocol** **sessionSummaryInfo.ingressConnect.protocol**	0	虚拟
	1	ICMP
	6	TCP
	17	UDP
	252	HTTP

字段	整数	字符串
rule.type	0	DUMMY_RULE_TYPE
	1	THIRD_PARTY
	2	USER_DEFINED

字段	整数	字符串
statusText **ingressConnectionStates.state**	0	已关闭
	1	SYN_SENT
	2	SYN_RECV
	3	ESTABLISHED
	4	FIN_WAIT
	5	CLOSE_WAIT
	6	LAST_ACK
	7	TIME_WAIT
	8	拉近距离

字段	整数	字符串
type	1	WAF
	2	DPI
	3	HTTP_REQUEST
	4	L4_FW
	5	FLOW_LOG
	6	MALICIOUS_IP
	7	TLS_ERROR
	8	TLS_LOG
	9	L7DOS
	10	SNI
	11	APPID
	12	URLFILTER
	13	SESSION_SUMMARY
	14	DLP
	15	FQDNFILTER
	16	防病毒

日志转发 - Microsoft Sentinel

Microsoft Sentinel 是许多公司使用的强大 SIEM。 多云防御 支持向 Microsoft Sentinel 转发日志，以发送安全事件和流量日志信息以进行处理、存储、访问和关联。发送的信息采用半结构化 JSON 格式，可以访问和处理属性-值对。

要求

要将日志转发到 Microsoft Sentinel，需要以下信息：

- 创建 Azure 日志分析工作空间。
- 定义 Azure 日志表。

配置文件参数

参数	义务性	默认值	说明
配置文件名称	必需		用于引用配置文件的唯一名称。
说明	可选		配置文件的说明。
目标	必填	Microsoft Sentinel	用于配置文件的SIEM。
Azure 日志分析工作空间 ID	必需		Azure Log Analytics 工作空间的 ID。
共享密钥	必需		用于对通信进行身份验证的共享密钥。
Azure 日志表名称	必需		将存储日志/事件的 Azure 日志表的名称。

日志转发 - Splunk

Splunk 是许多公司使用的一种非常常见且功能强大的 SIEM。 多云防御 支持将日志转发到 Splunk，以发送安全事件和流量日志信息以进行处理、存储、访问和关联。发送的信息采用半结构化 JSON 格式，可以访问和处理属性-值对。

要求

要将日志转发到 Splunk，需要以下信息：

- Splunk 帐户
- Splunk 收集器 URL
- 事件收集器密钥
- 索引名称

Tip 有关 Splunk 事件收集器的信息，请参阅 **Splunk HTTP 事件收集器** (https://docs.splunk.com/Documentation/Splunk/8.1.0/Data/UsetheHTTPEventCollector)。

配置文件参数

参数	义务性	默认值	说明
配置文件名称	必需		用于引用配置文件的唯一名称。
说明	可选		配置文件的说明。
目标	必填	Datadog	用于配置文件的SIEM。
跳过验证证书	可选	已取消选中	是否跳过验证证书的真实性。
终端	必需		用于访问 HTTP 事件收集器的 URL。
令牌	必需		允许 多云防御 与 Splunk 通信的 Splunk 令牌。
索引	必需	main	用于存储事件的 Splunk 索引的名称。

日志转发 - Sumo Logic

Sumo Logic 是许多公司使用的一种非常常见且功能强大的 SIEM。 多云防御 支持将日志转发到 Sumo Logic，以发送安全事件和流量日志信息以进行处理、存储、访问和关联。发送的信息采用半结构化 JSON 格式，可以访问和处理属性-值对。

要求

要将日志转发到 Sumo Logic，需要以下信息：

- Sumo Logic 账户
- Sumo Logic 收集器终端

Tip 有关如何设置 Sumo Logic 收集器的信息，请参阅 **Sumo Logic 设置指南** （https://help.sumologic.com/docs/send-data/setup-wizard/）。

配置文件参数

参数	义务性	默认值	说明
配置文件名称	必需		用于引用配置文件的唯一名称

参数	义务性	默认值	说明
说明	可选		配置文件的说明
目标	必填	Sumo Logic	用于配置文件的 SIEM
终端	必需		用于接收转发的事件/日志的 URL 终端

日志转发 - 系统日志

系统日志服务器是接受标准格式的系统日志消息的常见日志收集器。每个系统日志消息都包含设施、严重性和消息字段。几乎任何 SIEM 都可以接受系统日志格式的消息，但大多数 SIEM 支持其他消息格式。多云防御支持将安全事件和流量日志发送到系统日志服务器。以下是可以转发的事件和日志的列表：

- 流日志（流量摘要）
- 防火墙事件（AppID、L4FW、GeoIP、MaliciousIP、SNI）
- HTTPS 日志（HTTP、TLS）
- 网络威胁（AV、DLP、IDS/IPS）
- Web 保护（WAF、L7 DoS）

Note 流日志在网关版本 2.10 及更高版本中已弃用。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事件转发到系统日志服务器。创建后，配置文件需要与新的或现有的网关关联，以便将事件发送到系统日志服务器。要创建、修改或更改日志转发配置文件的网关关联，请参阅 日志转发 - 安全事件和流量日志。

配置文件参数

参数	义务性	默认值	说明
配置文件名称	必需		用于引用配置文件的唯一名称。
说明	可选		配置文件的说明。
SIEM 供应商	必需	系统日志	用于配置文件的SIEM。
服务器 IP	必需		系统日志服务器的IP地址。

参数	义务性	默认值	说明
Protocol	必需	UDP	发送消息时使用的协议(TCP/UDP)。
端口	必需		发送消息时使用的端口。
格式	必填	IETF	消息的格式（仅支持IETF）。
流日志	必需	不兼容	是否发送流日志（是/否）。
防火墙事件	必需	不兼容	是否发送防火墙事件（是/否）。
HTTPS 日志	必需	不兼容	是否发送 HTTPS 日志（是/否）。
网络威胁	必需	紧急	发送网络威胁的最低严重性级别。
Web 攻击	必需	紧急	发送 Web 攻击的最低严重性级别。

Note 提供以下严重性级别（从最高到最低）：

- 紧急
- 警报
- 严重
- 错误
- 警告
- 通知
- 信息
- 调试

包含指定或更高严重性级别的类别的所有事件都将发送到系统日志服务器。

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。