로그 전달 대상/SIEM

로그 전달 - AWS S3 버킷

멀티 클라우드 방어에서는 처리, 저장, 액세스 및 상관관계를 위해 보안 이벤트 및 트래픽 로그를 AWS S3 버킷으로 전송하여 보안 이벤트 및 트래픽 로그 정보를 전송할 수 있습니다. 전송되는 정보는 속성-값 쌍을 액세스하고 처리할 수 있는 준정형 JSON 형식으로 전송됩니다.

요구 사항

AWS S3 버킷에 이벤트/로그를 전달하려면 다음이 필요합니다.

1. 새 AWS 버킷을 만들거나 기존 AWS S3 버킷을 사용합니다.
2. 다음 정책을 AWS S3 버킷에 적용하여 멀티 클라우드 방어 컨트롤러이(가) 버킷에 대한 액세스 및 쓰기를 허용합니다.

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

```
    ]
}
```

프로필 매개변수

매개변수	정확도	기본값	설명
프로필 이름	필수		프로파일을 참조하는 데 사용할 고유한 이름입니다.
설명	선택 사항		프로필에 대한 설명입니다.
대상	필수	AWS S3	AWS S3 버킷
CSP 계정	필수		AWS S3 버킷이 있는 CSP 계정입니다.
S3 버킷	필수		이벤트/로그가 전달할 AWS S3 버킷 이름입니다.

로그 전달 - Datadog

DataDog는 많은 기업에서 사용하는 매우 일반적이고 강력한 SIEM입니다. 멀티 클라우드 방어은(는) DataDog로의 로그 전달을 지원하여 처리, 저장, 액세스 및 상관 관계를 위해 보안 이벤트 및 트래픽 로그 정보를 전송합니다. 전송되는 정보는 속성-값 쌍을 액세스하고 처리할 수 있는 준정형 JSON 형식으로 전송됩니다.

요구 사항

DataDog에 로그를 전달하려면 다음 정보가 필요합니다.

- DataDog 계정
- 엔드포인트 URL
- API 키

Tip

- Datadog 계정에 등록하려면 **Datadog** 계정(https://www.datadoghq.com/)을 참조하십시오.
- Datadog API 키를 생성하려면 **Datadog API** 키(https://app.datadoghq.com/account/login?next=%2Faccount%2Fsettings#api)를 참조하십시오.

프로필 매개변수

매개변수	정확도	기본값	설명
프로필 이름	필수		프로파일을 참조하는 데 사용할 고유한 이름입니다.
설명	선택 사항		프로필에 대한 설명입니다.
대상	필수	Datadog	프로파일에 사용되는 SIEM입니다.
인증서 확인 건너뛰기	선택 사항	선택 취소됨	인증서의 신뢰성 확인을 건너뛸지 여부입니다.
API 키	필수		통신 인증을 위한 DataDog API 키입니다.
엔드포인트	필수	https://http-intake.logs.datadoghq.com/	전달된 이벤트/로그를 수신하는 데 사용되는 URL 엔드포인트

로그 전달 - GCP 로깅

GCP Stack드라이버 로깅은 애플리케이션 및 서비스에서 로그 수집 및 저장을 위해 GCP(Google Cloud Provider)가 제공하는 서비스입니다. 멀티 클라우드 방어은(는) GCP Stack드라이버 로깅으로의 로그 전달을 지원하여 처리, 저장, 액세스 및 상관관계를 위해 보안 이벤트 및 트래픽 로그 정보를 전송합니다. 전송되는 정보는 속성-값 쌍을 액세스하고 처리할 수 있는 준정형 JSON 형식으로 전송됩니다.

요구 사항

게이트웨이에서 GCP StackDriver 로그에 이벤트를 기록하려면 GCP 멀티 클라우드 방어-*firewall* 서비스 계정에 로그 작성자 역할이 할당되어야 합니다.

프로필 매개변수

매개변수	정확도	기본값	설명
프로필 이름	필수		프로파일을 참조하는 데 사용할 고유한 이름입니다.
설명	선택 사항		프로필에 대한 설명입니다.

매개변수	정확도	기본값	설명
대상	필수	GCP 로깅(게이트웨이에서)	프로파일에 사용되는 SIEM입니다.
로그 이름	필수	ciscomcd -gateway-logs	이벤트를 저장하는 데 사용되는 Stackdriver 로그의 이름입니다.

필드 정수 대 문자열 매핑

이벤트가 컨트롤러에서 전달되면 컨트롤러는 이벤트 필드 값을 식별 이름에 매핑합니다. 이벤트가 게이트웨이에서 직접 전달될 경우(예: GCP 로깅) 컨트롤러는 관련되지 않으며, 따라서 이벤트 필드 값은 식별 이름에 매핑되지 않습니다. 이러한 필드를 해석하려면 사용자는 식별 이름 매핑에 대한 필드 값을 수행해야 합니다.

식별 매핑에 대한 필드, 하위 필드 및 해당 값은 아래에 나와 있습니다.

필드	정수	문자열
action	0	DUMMY_ACTION
	1	ALLOW
	2	DENY
	3	DROP
	4	REDIRECT
	5	PROXY
	6	LOG
	7	OTHER
	8	DELAY
	9	DETECT_SIG

필드	정수	문자열
gatewaySecurityType	1	INGRESS_FIREWALL
	2	EAST_WEST_AND_EGRESS_FIREWALL

필드	정수	문자열
level	1	DEBUG
	2	INFO
	3	NOTICE
	4	WARNING
	5	ERROR
	6	CRITICAL
	7	ALERT
	8	EMERGENCY

필드	정수	문자열
policyMatchInfo.serviceType	0	UNKNOWN
	1	PROXY
	2	FORWARDING
	3	REVERSE_PROXY
	4	FORWARD_PROXY

필드	정수	문자열
protocol **sessionSummaryInfo.egressConnection.protocol** **sessionSummaryInfo.ingressConnect.protocol**	0	DUMMY
	1	ICMP
	6	TCP
	17	UDP
	252	HTTP

필드	정수	문자열
rule.type	0	DUMMY_RULE_TYPE
	1	THIRD_PARTY
	2	USER_DEFINED

필드	정수	문자열
statusText **ingressConnectionStates.state**	0	CLOSED
	1	SYN_SENT
	2	SYN_RECV
	3	ESTABLISHED
	4	FIN_WAIT
	5	CLOSE_WAIT
	6	LAST_ACK
	7	TIME_WAIT
	8	CLOSE

필드	정수	문자열
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	AV

로그 전달 - Microsoft Sentinel

Microsoft Sentinel은 많은 기업에서 사용하는 강력한 SIEM입니다. 멀티 클라우드 방어은(는) Microsoft Sentinel로의 로그 전달을 지원하여 처리, 저장, 액세스 및 상관 관계를 위해 보안 이벤트 및 트래픽 로그 정보를 전송합니다. 전송되는 정보는 속성-값 쌍을 액세스하고 처리할 수 있는 준정형 JSON 형식으로 전송됩니다.

요구 사항

Microsoft Sentinel에 로그를 전달하려면 다음 정보가 필요합니다.

- Azure 로그 분석 작업 영역을 생성합니다.
- Azure 로그 테이블을 정의합니다.

프로필 매개변수

매개변수	정확도	기본값	설명
프로필 이름	필수		프로파일을 참조하는 데 사용할 고유한 이름입니다.
설명	선택 사항		프로필에 대한 설명입니다.
대상	필수	Microsoft Sentinel	프로파일에 사용되는 SIEM입니다.
Azure 로그 분석 작업 영역 ID	필수		Azure 로그 분석 작업 영역의 ID입니다.
공유 키	필수		통신 인증에 사용되는 공유 키입니다.
Azure 로그 테이블 이름	필수		로그/이벤트가 저장될 Azure 로그 테이블의 이름입니다.

로그 전달 - Splunk

Splunk는 많은 기업에서 사용하는 매우 일반적이고 강력한 SIEM입니다. 멀티 클라우드 방어은(는) Splunk로의 로그 전달을 지원하여 처리, 저장, 액세스 및 상관 관계를 위해 보안 이벤트 및 트래픽 로그 정보를 전송합니다. 전송되는 정보는 속성-값 쌍을 액세스하고 처리할 수 있는 준정형 JSON 형식으로 전송됩니다.

요구 사항

Splunk에 로그를 전달하려면 다음 정보가 필요합니다.

- Splunk 계정
- Splunk 컬렉터 URL
- 이벤트 컬렉터 키
- 색인 이름

Tip Splunk 이벤트 컬렉터에 대한 자세한 내용은 **Splunk HTTP** 이벤트 컬렉터(https://docs.splunk.com/Documentation/Splunk/8.1.0/Data/UsetheHTTPEventCollector)를 참조하십시오.

프로필 매개변수

매개변수	정확도	기본값	설명
프로필 이름	필수		프로파일을 참조하는 데 사용할 고유한 이름입니다.
설명	선택 사항		프로필에 대한 설명입니다.
대상	필수	Datadog	프로파일에 사용되는 SIEM입니다.
인증서 확인 건너뛰기	선택 사항	선택 취소됨	인증서의 신뢰성 확인을 건너뛸지 여부입니다.
엔드포인트	필수		HTTP 이벤트 컬렉터에 액세스하는 데 사용되는 URL입니다.
토큰	필수		멀티 클라우드 방어에 Splunk와 통신에 허용하는 Splunk 토큰입니다.
색인	필수	기본	이벤트를 저장하는 데 사용되는 Splunk 인덱스의 이름입니다.

로그 전달 - Sumo Logic

Sumo Logic은 많은 기업에서 사용하는 매우 일반적이고 강력한 SIEM입니다. 멀티 클라우드 방어은(는) Sumo Logic으로의 로그 전달을 지원하여 처리, 저장, 액세스 및 상관 관계를 위해 보안 이벤트 및 트래픽 로그 정보를 전송합니다. 전송되는 정보는 속성-값 쌍을 액세스하고 처리할 수 있는 준정형 JSON 형식으로 전송됩니다.

요구 사항

Sumo Logic에 로그를 전달하려면 다음 정보가 필요합니다.

- Sumo Logic 계정
- Sumo Logic 컬렉터 엔드포인트

Tip Sumo Logic 컬렉터 설정 방법에 대한 자세한 내용은 **Sumo Logic** 설정 가이드(https://help.sumologic.com/docs/send-data/setup-wizard/)를 참조하십시오.

프로필 매개변수

매개변수	정확도	기본값	설명
프로필 이름	필수		프로파일을 참조하는 데 사용할 고유한 이름
설명	선택 사항		프로필에 대한 설명
대상	필수	Sumo Logic	프로파일에 사용되는 SIEM
엔드포인트	필수		전달된 이벤트/로그를 수신하는 데 사용되는 URL 엔드포인트

로그 전달 - 시스템 로그

시스템 로그 서버는 표준 형식의 시스템 로그 메시지를 수락하는 공통 로그 컬렉터입니다. 각 시스템 로그 메시지에는 시설, 심각도, 메시지에 대한 필드가 포함되어 있습니다. 대부분의 SIEM은 다른 메시지 형식을 지원하지만 거의 모든 SIEM은 시스템 로그 형식의 메시지를 수락할 수 있습니다. 멀티 클라우드 방어에서는 보안 이벤트 및 트래픽 로그를 시스템 로그 서버로 전송하도록 지원합니다. 전달할 수 있는 이벤트 및 로그의 목록은 다음과 같습니다.

- 플로우 로그(트래픽 요약)

- 방화벽 이벤트(AppID, L4FW, GeoIP, MaliciousIP, SNI)
- HTTPS 로그(HTTP, TLS)
- 네트워크 위협(AV, DLP, IDS/IPS)
- 웹 보호(WAF, L7 DoS)

Note 플로우 로그는 게이트웨이 버전 2.10 이상 릴리스에서 더 이상 사용되지 않습니다. 각 플로우 로그에 포함된 정보는 **Traffic Summary(**트래픽 요약**)** > **Logs(**로그**)**에서 제공되는 세션 정보의 일부로 제공됩니다.

이벤트는 로그 전달 프로파일을 사용하여 시스템 로그 서버로 전달할 수 있습니다. 생성된 프로파일을 새 게이트웨이 또는 기존 게이트웨이와 연결해야 이벤트가 시스템 로그 서버로 전송됩니다. 로그 전달 프로파일의 게이트웨이 연결을 생성, 수정 또는 변경하려면 로그 전달 - 보안 이벤트 및 트래픽 로그를 참조하십시오.

프로필 매개변수

매개변수	정확도	기본값	설명
프로필 이름	필수		프로파일을 참조하는 데 사용할 고유한 이름입니다.
설명	선택 사항		프로필에 대한 설명입니다.
SIEM 벤더	필수	시스템 로그	프로파일에 사용되는 SIEM입니다.
서버 IP	필수		시스템 로그 서버의 IP 주소입니다.
프로토콜	필수	UDP	메시지를 전송할 때 사용할 프로토콜(TCP/UDP)입니다.
포트	필수		메시지를 전송할 때 사용할 포트입니다.
형식	필수	IETF	메시지의 형식입니다(IETF만 지원됨).
플로우 로그	필수	아니요	플로우 로그를 보낼지 여부(예/아니요)입니다.

매개변수	정확도	기본값	설명
방화벽 이벤트	필수	아니요	방화벽 이벤트를 전송할지 여부(예/아니요)입니다.
HTTPS 로그	필수	아니요	HTTPS 로그를 전송할지 여부(예/아니요)입니다.
네트워크 위협	필수	긴급	가장 낮은 심각도 수준으로 네트워크 위협을 전송할 수 있습니다.
웹 공격	필수	긴급	웹 공격을 전송할 가장 낮은 심각도 레벨입니다.

Note 다음의 심각도 레벨(가장 높은 것부터 가장 낮은 것)을 사용할 수 있습니다.

- 긴급
- 알림
- 심각
- 오류
- 경고
- 알림
- 정보
- 디버그

지정한 심각도 레벨 이상을 포함하는 범주에 대한 모든 이벤트는 시스템 로그 서버로 전송됩니다.