로그 전달 개요

보안 이벤트 및 트래픽 로그

SIEM(Security Information Event Management) 시스템은 보안 정보 및 보안 이벤트 정보를 단일 관리 플랫폼으로 결합하는 것을 전문으로 하는 솔루션입니다. 보안 및 이벤트 정보는 이 정보를 SIEM에 전달하도록 구성된 서드파티 보안 솔루션에서 가져옵니다.

멀티 클라우드 방어에서는 UI 내에서 직접 보안 이벤트 정보 보기를 지원합니다. 이러한 이벤트는 **Investigate(**조사**)** > **Flow Analytics(**플로우 분석**)** 섹션에서 사용할 수 있습니다. 이벤트는 다음과 같이 분류되고 볼 수 있습니다.

카테고리	유형	설명
플로우 로그	FLOW_LOG	트래픽 흐름의 여러 단계와 관련된 정보

카테고리	유형	설명
방화벽 이벤트	APPID	애플리케이션 ID를 기준으로 일치하는 트래픽(OpenAppID)
	GEOIP	Geo IP에서 제공되거나 Geo IP로 전송되는 트래픽(MaxMind)
	L4_FW	레이어 4 정보(소스/대상 IP/포트 및 프로토콜)를 기반으로 일치하는 트래픽
	MALICIOUS_IP	악의적인 IP에서 발생하거나 악성 IP로 향하는 트래픽 (TrustWave)
	SNI	SNI 정보를 기준으로 일치하는 트래픽
네트워크 위협	AV	바이러스가 탐지된 트래픽 (ClamAV)
	DPI	IDS/IPS 위협이 탐지된 트래픽 (TALOS)
	DLP	민감한 데이터가 유출되는 트래픽
웹 보호	WAF	웹 애플리케이션 위협이 탐지된 트래픽(ModSecurity)
	L7DOS	Layer7 DOS 공격에 기여하는 트래픽
URL 필터링	URLFILTER	URL 범주 또는 URL과 일치하는 트래픽(BrightCloud)
FQDN 필터링	FQDNFILTER.	FQDN 범주 또는 FQDN과 일치하는 트래픽(BrightCloud)
HTTPS 로그	HTTP_REQUEST	웹 기반 트래픽 관련 정보(HTTP)
	TLS_ERROR	TLS 오류 관련 정보
	TLS_LOG	TLS 동작 관련 정보
트래픽 요약 로그	SESSION_SUMMARY	처리된 각 트래픽 세션에 대한 요약 정보

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

로그 전달 프로파일을 사용하여 각 이벤트 범주를 SIEM으로 전송할 수 있습니다. 현재 멀티 클라우드 방어에서 지원되는 SIEM은 다음과 같습니다.

- AWS S3 버킷
- Datadog
- GCP 로깅
- Microsoft Sentinel
- Splunk
- Sumo Logic
- Syslog

로그 전달 프로파일은 아래에 설명된 단계를 사용하여 작동할 수 있습니다.

독립형 이벤트 또는 트래픽 로그 프로파일 생성

단계 **1** **Manage(**관리**)** > **Profiles(**프로파일**)** > **Log Forwarding(**로그 전달**)**으로 이동합니다.
단계 **2** **Create(**생성**)**를 클릭합니다.
단계 **3** 프로파일 이름 및 설명을 지정합니다.
단계 **4** *Type(*유형*)*을 Standalone(독립형)으로 지정합니다.
단계 **5** 적절한 매개변수를 입력합니다(SIEM 관련 문서 참조).
단계 **6** **Save(**저장**)**를 클릭합니다.
단계 **7** 원하는 게이트웨이 연결을 추가합니다(게이트웨이에 이벤트, 트래픽 로그 전달 프로파일 또는 메트릭 전달 프로파일 추가 참조).

독립형 이벤트 또는 트래픽 로그 프로파일 편집

단계 **1** **Manage(**관리**)** > **Profiles(**프로파일**)** > **Log Forwarding(**로그 전달**)**으로 이동합니다.
단계 **2** 편집할 프로파일 옆의 상자를 선택합니다.
단계 **3** **Edit(**편집**)**를 클릭합니다.
단계 **4** 원하는 대로 매개변수를 수정합니다(SIEM 관련 문서 참조).
단계 **5** **Save(**저장**)**를 클릭합니다.

그룹 이벤트 또는 트래픽 로그 프로파일 생성

단계 **1** **Manage(**관리**)** > **Profiles(**프로파일**)** > **Log Forwarding(**로그 전달**)**으로 이동합니다.
단계 **2** **Create(**생성**)**를 클릭합니다.
단계 **3** 프로파일 이름 및 설명을 지정합니다.
단계 **4** *Type(*유형*)*을 Group(그룹)으로 지정합니다.
단계 **5** 그룹화하려는 독립형 프로파일의 수를 수용하기 위해 행을 필요한 만큼 추가합니다.
단계 **6** **Save(**저장**)**를 클릭합니다.
단계 **7** 원하는 게이트웨이 연결을 추가합니다(게이트웨이에 이벤트, 트래픽 로그 전달 프로파일 또는 메트릭 전달 프로파일 추가 참조).

그룹 이벤트 또는 트래픽 로그 프로파일 편집

단계 **1** **Manage(**관리**)** > **Profiles(**프로파일**)** > **Log Forwarding(**로그 전달**)**으로 이동합니다.
단계 **2** 편집할 프로파일 옆의 상자를 선택합니다.
단계 **3** **Edit(**편집**)**를 클릭합니다.
단계 **4** 독립형 프로파일을 수정, 추가 또는 제거합니다.
단계 **5** **Save(**저장**)**를 클릭합니다.

이벤트 또는 트래픽 로그 전달 프로파일 보기

단계 **1** **Manage(**관리**)** > **Profiles(**프로파일**)** > **Log Forwarding(**로그 전달**)**으로 이동합니다.
단계 **2** 세부 정보를 보려는 프로파일 링크를 선택합니다.
단계 **3** 세부 정보를 봅니다.

이벤트 또는 트래픽 로그 프로파일 삭제

대시보드에서 프로파일을 삭제하려면 다음 절차를 따르십시오.

Before you begin

대시보드에서 프로파일을 삭제하기 전에 이벤트 또는 프로파일과 게이트웨이 간의 연결을 반드시 제거해야 합니다. 자세한 내용은 게이트웨이에서 이벤트, 트래픽 로그 전달 프로파일 또는 메트릭 전달 프로파일 제거를 참조하십시오.

단계 **1** **Manage(**관리**)** > **Profiles(**프로파일**)** > **Log Forwarding(**로그 전달**)**으로 이동합니다.
단계 **2** 삭제할 프로파일 옆의 상자를 선택합니다.
단계 **3** **Delete(**삭제**)**를 클릭합니다.
단계 **4** **Yes(**예**)** 또는 **No(**아니요**)**를 클릭하여 삭제 작업을 확인합니다.

검색 로그

검색 로그는 SIEM(Security Information Event Management) 시스템으로 전달되어 단일 관리 플랫폼으로 집계될 수 있습니다.

멀티 클라우드 방어에서는 UI 내에서 직접 보안 이벤트 정보 보기를 지원합니다. 이러한 이벤트는 **Investigate(**조사**)** > **Traffic(**트래픽**)** 섹션에서 사용할 수 있습니다. 이벤트는 다음과 같이 분류되고 볼 수 있습니다.

카테고리	유형	설명
DNS 로그	DNS_LOG	클라우드 제공자로부터 수집된 DNS 로그 정보와 위협 인텔리전스의 상관 관계
VPC 로그	VPC_LOG	클라우드 제공자로부터 수집된 VPC/VNet 플로우 로그 정보와 위협 인텔리전스의 상관 관계

로그 전달 프로파일을 사용하고 온보딩된 클라우드 어카운트에 프로파일을 연결하여 각 범주를 SIEM으로 전송할 수 있습니다. 현재 멀티 클라우드 방어에서 지원하는 로그 전달 대상은 다음과 같습니다.

- AWS S3 버킷
- Datadog
- GCP 로깅
- Microsoft Sentinel
- Splunk
- Sumo Logic
- Syslog

검색 로그를 전달하려면 아래 단계를 사용합니다.

독립형 검색 로그 프로파일 생성

단계 **1** **Manage(**관리**)** > **Profiles(**프로파일**)** > **Log Forwarding(**로그 전달**)**으로 이동합니다.
단계 **2** **Create(**생성**)**를 클릭합니다.
단계 **3** 프로파일 이름 및 설명을 지정합니다.
단계 **4** *Type(*유형*)*을 Standalone(독립형)으로 지정합니다.
단계 **5** 적절한 매개변수를 입력합니다(SIEM 관련 문서 참조).
단계 **6** **Save(**저장**)**를 클릭합니다.
단계 **7** 로그 프로파일을 원하는 클라우드 어카운트에 연결합니다(클라우드 어카운트로 검색 로그 프로파일 추가 참조).

독립형 검색 로그 프로파일 편집

단계 **1** **Manage(**관리**)** > **Profiles(**프로파일**)** > **Log Forwarding(**로그 전달**)**으로 이동합니다.
단계 **2** 편집할 프로파일 옆의 상자를 선택합니다.
단계 **3** **Edit(**편집**)**를 클릭합니다.
단계 **4** 원하는 대로 매개변수를 수정합니다(SIEM 관련 문서 참조).
단계 **5** **Save(**저장**)**를 클릭합니다.

그룹 검색 로그 프로파일 생성

단계 **1** **Manage(**관리**)** > **Profiles(**프로파일**)** > **Log Forwarding(**로그 전달**)**으로 이동합니다.
단계 **2** **Create(**생성**)**를 클릭합니다.
단계 **3** 프로파일 이름 및 설명을 지정합니다.
단계 **4** *Type(*유형*)*을 Group(그룹)으로 지정합니다.
단계 **5** 독립형 프로파일을 연결할 행을 추가합니다.
단계 **6** **Save(**저장**)**를 클릭합니다.
단계 **7** 원하는 게이트웨이 연결을 추가합니다(게이트웨이에 이벤트, 트래픽 로그 전달 프로파일 또는 메트릭 전달 프로파일 추가 참조).

그룹 검색 로그 프로파일 편집

단계 **1** **Manage(**관리**)** > **Profiles(**프로파일**)** > **Log Forwarding(**로그 전달**)**으로 이동합니다.
단계 **2** 편집할 프로파일 옆의 상자를 선택합니다.
단계 **3** **Edit(**편집**)**를 클릭합니다.
단계 **4** 독립형 프로파일을 수정, 추가 또는 제거합니다.
단계 **5** **Save(**저장**)**를 클릭합니다.

검색 로그 프로파일 세부 정보 보기

단계 **1** **Manage(**관리**)** > **Profiles(**프로파일**)** > **Log Forwarding(**로그 전달**)**으로 이동합니다.
단계 **2** 세부 정보를 보려는 프로파일 링크를 선택합니다.
단계 **3** 세부 정보를 봅니다.

클라우드 어카운트로 검색 로그 프로파일 추가

단계 **1** **Manage(**관리**)** > **Cloud Accounts(**클라우드 어카운트**)** > **Accounts(**어카운트**)**로 이동합니다.
단계 **2** 프로파일을 연결할 클라우드 어카운트 옆의 확인란을 선택합니다.
단계 **3** **Actions(**작업**)** > **Update Log Profile(**로그 프로파일 업데이트**)**를 클릭합니다.
단계 **4** 클라우드 로그 전달 프로파일에 대한 **Log Profile(**로그 프로파일**)** 개체를 선택합니다.
단계 **5** **Save & Continue(**저장 후 계속**)**를 클릭합니다.

클라우드 어카운트에서 검색 로그 프로파일 제거

단계 **1** **Manage(**관리**)** > **Cloud Accounts(**클라우드 계정**)** > **Accounts(**계정**)**로 이동합니다.
단계 **2** 프로파일을 연결할 클라우드 어카운트 옆의 확인란을 선택합니다.
단계 **3** **Actions(**작업**)** > **Update Log Profile(**로그 프로파일 업데이트**)**를 클릭합니다.
단계 **4** *Cloud Logs Forwarding Profile(*클라우드 로그 전달 프로파일*)* 매개변수의 경우 *Profile(*프로파일*)* 옆에 있는 'X'를 클릭하여 제거합니다.
단계 **5** **Save & Continue(**저장 후 계속**)**를 클릭합니다.

검색 로그 프로파일 삭제

대시보드에서 프로파일을 삭제하려면 다음 절차를 따르십시오.

Before you begin

대시보드에서 프로파일을 삭제하기 전에 프로파일과 게이트웨이 간의 연결을 반드시 제거해야 합니다. 자세한 내용은 클라우드 어카운트에서 검색 로그 프로파일 제거를 참조하십시오.

단계 **1** **Manage(**관리**)** > **Profiles(**프로파일**)** > **Log Forwarding(**로그 전달**)**으로 이동합니다.

단계 **2** 삭제할 프로파일 옆의 상자를 선택합니다.

단계 **3** **Delete(**삭제**)**를 클릭합니다.

단계 **4** **Yes(**예**)** 또는 **No(**아니요**)**를 클릭하여 삭제 작업을 확인합니다.

게이트웨이 메트릭 전달 프로파일

이 프로파일은 데이터 모니터링 및 분석을 위해 멀티 클라우드 방어 게이트웨이에 의해 생성된 게이트웨이 메트릭을 전달하는 데 사용됩니다. 메트릭은 게이트웨이에 의해 생성되지만 메트릭을 서드파티 분석 애플리케이션에 전달하는 멀티 클라우드 방어 컨트롤러입니다. 이 전달 프로파일을 사용하면 멀티 클라우드 방어에 로그인하지 않고도 게이트웨이 메트릭을 모니터링, 분석 및 구성할 수 있습니다. 이 정보를 사용하여 게이트웨이 환경의 성능 및 동작을 측정합니다. 또한 환경 문제 해결을 위해 이 정보를 활용합니다.

참고 멀티 클라우드 방어 컨트롤러 버전 23.09부터는 DataDog만 서드파티 분석 애플리케이션으로 지원됩니다.

DataDog와 같이 사용 가능한 대부분의 분석 애플리케이션의 경우, 반드시 권한이 부여된 사용자여야 툴의 API 및 렌더링된 데이터에 액세스할 수 있습니다.

독립형 메트릭 전달 프로파일 생성

다음 절차에 따라 독립형 프로파일을 생성하고 서드파티에서 처리할 메트릭을 전달합니다.

시작하기 전에

이 프로파일을 생성하기 전에 메트릭을 전달할 서드파티 애플리케이션이 하나 이상 있어야 합니다.

단계 **1** **Manage(**관리**)** > **Profiles(**프로파일**)** > **Metrics Forwarding(**메트릭 전달**)**로 이동합니다.

단계 **2** **Create(**생성**)**를 클릭합니다.

단계 **3** 고유한 프로파일 이름을 입력합니다.

단계 **4** (선택 사항) **Description(**설명**)**을 입력합니다. 이렇게 하면 유사한 이름의 다른 프로파일과 구분할 수 있습니다.

단계 **5** **Type(**유형**)** 드롭다운 메뉴를 확장하고 **Standalone(**독립형**)**을 선택합니다.

단계 **6** **Destination(**대상**)** 드롭다운 메뉴를 확장하고 메트릭을 처리하고 분석할 서드파티 애플리케이션을 선택합니다.

단계 **7** 메트릭의 엔드포인트 위치로 사용할 **Endpoint(**엔드포인트**)**를 입력합니다.

단계 **8** **Save(**저장**)**를 클릭합니다.

분석 애플리케이션으로 DataDog를 선택하는 경우, 엔드포인트는 기본적으로 HTTP Webhook로 채워집니다. 이 항목이 기본값인 경우 프로파일을 저장하기 전에 수정할 수 있습니다.

다음에 수행할 작업

- 프로파일 세부 정보 보기
- 프로파일에 게이트웨이 연결 추가

독립형 메트릭 전달 프로파일 편집

이미 생성된 독립형 프로파일을 편집하려면 다음 절차를 사용합니다.

단계 **1** **Manage(**관리**)** > **Profiles(**프로파일**)**로 이동하고 적절한 프로파일 **Type(**유형**)**을 선택합니다.

단계 **2** 편집할 프로파일 옆의 상자를 선택합니다.

단계 **3** **Edit(**편집**)**를 클릭합니다.

단계 **4** 필요에 따라 매개변수를 수정합니다.

단계 **5** **Save(**저장**)**를 클릭합니다.

그룹 메트릭 전달 프로파일 생성

이 프로세스에서는 프로파일을 생성한 다음 특정 게이트웨이에 할당합니다. 그룹 프로파일은 최대 5개의 독립형 메트릭 전달 프로파일을 결합한 다음 단일 게이트웨이에 할당할 수 있습니다. 다음 절차를 사용하여 그룹화된 메트릭 전달 프로파일을 생성합니다.

시작하기 전에

- 이 프로파일을 생성하기 전에 메트릭을 전달할 서드파티 애플리케이션이 하나 이상 있어야 합니다.
- 둘 이상의 독립형 메트릭 전달 프로파일이 이미 생성되어 있어야 합니다. 자세한 내용은 독립형 메트릭 전달 프로파일 생성를 참조하십시오.

단계 **1** 멀티 클라우드 방어 컨트롤러 인터페이스에서 **Manager(**관리자**)** > **Profiles(**프로파일 **)** > **Metrics Forwarding(**메트릭 전달**)**으로 이동합니다.

단계 **2** **Create(**생성**)**를 클릭합니다.

단계 **3** 고유 **Profile Name(**프로파일 이름**)**을 입력합니다.

단계 **4** (선택 사항) **Description(**설명**)**을 입력합니다. 이렇게 하면 유사한 이름의 프로파일을 구분하는 데 도움이 될 수 있습니다.

단계 **5** **Type(**유형**)** 드롭다운 메뉴를 확장하고 **Group(**그룹**)**을 선택합니다.

단계 **6** **Group Details(**그룹 세부 정보**)**에서 프로파일에 추가해야 하는 모든 새 행에 대해 **Add(**추가**)**를 클릭합니다.

단계 **7** 각 행에 대한 드롭다운 메뉴를 확장하여 그룹에 추가할 프로파일을 선택합니다. 저장하기 전에 언제든지 프로파일을 제거하려면, 해당 프로파일의 확인란을 선택하고 **Remove(**제거**)**를 선택합니다.

단계 **8** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

- 프로파일 세부 정보 보기
- 프로파일에 게이트웨이 연결 추가

그룹 프로파일 편집

이미 생성된 그룹화된 프로파일 집합을 편집하려면 다음 절차를 사용합니다.

단계 **1** **Manage(**관리**)** > **Profiles(**프로파일**)**로 이동하고 적절한 프로파일 **Type(**유형**)**을 선택합니다.

단계 **2** 편집할 프로파일 옆의 상자를 선택합니다.

단계 **3** **Edit(**편집**)**를 클릭합니다.

단계 **4** 그룹 프로파일을 수정, 추가 또는 제거합니다.

단계 **5** **Save(**저장**)**를 클릭합니다.

프로파일 삭제

대시보드에서 프로파일을 삭제하려면 다음 절차를 따르십시오.

시작하기 전에

대시보드에서 프로파일을 삭제하기 전에 프로파일과 게이트웨이 간의 연결을 반드시 제거해야 합니다. 자세한 내용은 게이트웨이에서 이벤트, 트래픽 로그 전달 프로파일 또는 메트릭 전달 프로파일 제거를 참조하십시오.

단계 **1** **Manage(**관리**)** > **Profiles(**프로파일**)**로 이동하고 적절한 프로파일 **Type(**유형**)**을 선택합니다.
단계 **2** 삭제할 프로파일 옆의 상자를 선택합니다.
단계 **3** **Delete(**삭제**)**를 클릭합니다.
단계 **4** **Yes(**예**)** 또는 **No(**아니요**)**를 클릭하여 삭제 작업을 확인하거나 취소합니다.

게이트웨이에 이벤트, 트래픽 로그 전달 프로파일 또는 메트릭 전달 프로파일 추가

단계 **1** **Manage(**관리**)** > **Gateways(**게이트웨이**)**로 이동합니다.
단계 **2** 프로파일을 연결할 게이트웨이 옆의 확인란을 선택합니다.
단계 **3** **Edit(**편집**)**를 클릭합니다.
단계 **4** *Log Profile(*로그 프로파일*)* 매개변수에 대해서는 메뉴에서 원하는 프로파일을 선택합니다.
단계 **5** **Save(**저장**)**를 클릭합니다.

게이트웨이에서 이벤트, 트래픽 로그 전달 프로파일 또는 메트릭 전달 프로파일 제거

단계 **1** **Manage(**관리**)** > **Gateways(**게이트웨이**)**로 이동합니다.
단계 **2** 프로파일의 연결을 해제할 게이트웨이 옆의 확인란을 선택합니다.
단계 **3** **Edit(**편집**)**를 클릭합니다.
단계 **4** *Log Profile(*로그 프로파일*)* 매개변수의 경우 *Profile(*프로파일*)* 옆에 있는 'X'를 클릭하여 제거합니다.
단계 **5** **Save(**저장**)**를 클릭합니다.

Note 또한 로그 전달 프로파일을 게이트웨이 생성 시 게이트웨이와 연결할 수 있습니다. *Log Profile(*로그 프로파일*)* 매개변수는 게이트웨이 생성 프로세스 중에 사용할 수 있으며, 이 프로세스에서는 메뉴에서 원하는 프로파일을 선택할 수 있습니다.