알림 대상/SIEM

Datadog 통합

설정이 완료되면 정의된 알림 서비스 프로파일 및 알림 규칙을 사용하여 멀티 클라우드 방어 알림이 DataDog로 전송됩니다.

알림 프로파일 서비스 생성

Before you begin

DataDog에 알림을 전송하려면 다음 정보가 필요합니다.

- DataDog 계정
- 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.

단계 **1** **Administration**(관리) > **Alert Profiles**(알림 프로파일) > **Services**(서비스)로 이동합니다.

단계 **2** **Create**(생성)를 클릭합니다.

단계 3 **Name(**이름**)** - 알림 통합의 고유한 이름을 입력합니다. 예: `멀티 클라우드 방어-Datadog-profile`.
단계 4 **Description(**설명**)**(선택 사항) - 알림 통합에 대한 설명을 입력합니다.
단계 5 **Type(**유형**)** - 풀다운을 사용하여 **Datadog**를 선택합니다.
단계 6 **API Key(API** 키**)** - 통신 인증에 사용되는 DataDog API 키를 지정합니다.
단계 7 **Save(**저장**)**를 클릭합니다.

What to do next

이 새 프로필로 알림 규칙을 생성합니다.

알림 규칙 생성

Before you begin

DataDog에 알림을 전송하려면 다음 정보가 필요합니다.

- DataDog 계정
- 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.

단계 1 **Settings(**설정**)** > **Alert Profiles(**알림 프로파일**)** > **Alert Rules(**알림 규칙**)**으로 이동합니다.
단계 2 **Create(**생성**)**를 클릭합니다.
단계 3 **Profile Name(**프로파일 이름**)** - 통합의 고유한 이름을 입력합니다. 예: `멀티 클라우드 방어-DataDog-alert-rule`.
단계 4 **Description(**설명**)**(선택 사항) - 알림 규칙에 대한 설명을 입력합니다.
단계 5 **Alert Profile(**알림 프로파일**)** - 풀다운을 사용하여 PagerDuty 알림 프로파일을 선택합니다. 예를 들어 `멀티 클라우드 방어-DataDog-profile`에서 생성된 프로파일을 선택합니다.
단계 6 **Type(**유형**)** - 풀다운을 사용하여 **System Logs(**시스템 로그**)** 또는 **Discovery(**검색**)**를 선택합니다.
단계 7 **Sub Type(**하위 유형**)** - **System Logs(**시스템 로그**)**의 경우 하위 유형 풀다운 옵션은 **Gateway(**게이트웨이**)** 또는 **Account(**계정**)** 중 하나입니다. **Discovery(**검색**)**의 경우 하위 유형 풀다운 옵션은 **Insights Rule(**인사이트 규칙**)**입니다.
단계 8 **Severity(**심각도**)** - 선택한 유형 **System Logs(**시스템 로그**)**에 대해 풀다운을 사용하여 `Info Warning Medium High(정보 경고 중간 높음)` 또는 `Critical(위험)` 옵션에서 심각도 레벨을 선택합니다. 유형 **Discovery(**검색**)**의 경우, `Info Medium Critical(정보 중간 위험)` 옵션에서 Severity(심각도) 레벨을 선택합니다.
단계 9 **Enabled(**활성화됨**)** - 확인란을 사용하여 이 알림 프로파일을 활성화합니다.

단계 **10** **Save(**저장**)**를 클릭합니다.

Microsoft Sentinel 통합

구성한 멀티 클라우드 방어 알림은 정의된 알림 서비스 프로파일 및 알림 규칙을 사용하여 Microsoft Sentinel로 전송됩니다.

알림 프로파일 서비스 생성

Before you begin

Microsoft Sentinel에 알림을 전송하려면 다음 정보가 필요합니다.

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

단계 **1** **Administration(**관리**)** > **Alert Profiles(**알림 프로파일**)** > **Services(**서비스**)**로 이동합니다.

단계 **2** **Create(**생성**)**를 클릭합니다.

단계 **3** **Name(**이름**)** - 알림 통합의 고유한 이름을 입력합니다. 예: `mcd-mssentinel-profile`.

단계 **4** **Description(**설명**)**(선택 사항) - 알림 통합에 대한 설명을 입력합니다.

단계 **5** **Type(**유형**)** - 풀다운을 사용하여 **Microsoft Sentinel**을 선택합니다.

단계 **6** **API Key(API** 키**)** - Azure 로그 분석 작업 공간에 대해 Azure에서 생성된 공유 키를 지정합니다.

단계 **7** **Azure Log Table Name(Azure** 로그 테이블 이름**)** - Azure 로그 분석 작업 공간을 생성할 때 정의된 Azure 로그의 이름을 지정합니다.

단계 **8** **Azure Log Analytics Workspace ID(Azure** 로그 분석 작업 공간 **ID)** - Azure 로그 분석 작업 공간의 ID를 지정합니다.

단계 **9** **Save(**저장**)**를 클릭합니다.

What to do next

이 새 프로필로 알림 규칙을 생성합니다.

알림 규칙 생성

Before you begin

Microsoft Sentinel에 알림을 전송하려면 다음 정보가 필요합니다.

- Azure 로그 분석 작업 영역을 생성합니다.

• Azure 로그 테이블을 정의합니다.

단계 1 **Settings(**설정**)** > **Alert Profiles(**알림 프로파일**)** > **Alert Rules(**알림 규칙**)**으로 이동합니다.

단계 2 **Create(**생성**)**를 클릭합니다.

단계 3 **Profile Name(**프로파일 이름**)** - 통합의 고유한 이름을 입력합니다. 예: `mcd-mssentinel-alert-rule`.

단계 4 **Description(**설명**)**(선택 사항) - 알림 규칙에 대한 설명을 입력합니다.

단계 5 **Alert Profile(**알림 프로파일**)** - 풀다운을 사용하여 PagerDuty 알림 프로파일을 선택합니다. 예를 들어 위에서 생성한 프로파일을 선택합니다`mcd-mssentinel-profile`.

단계 6 **Type(**유형**)** - 풀다운을 사용하여 **System Logs(**시스템 로그**)** 또는 **Discovery(**검색**)**를 선택합니다.

단계 7 **Sub Type(**하위 유형**)** - **System Logs(**시스템 로그**)**의 경우 하위 유형 풀다운 옵션은 **Gateway(**게이트웨이**)** 또는 **Account(**계정**)** 중 하나입니다. **Discovery(**검색**)**의 경우 하위 유형 풀다운 옵션은 **Insights Rule(**인사이트 규칙**)**입니다.

단계 8 **Severity(**심각도**)** - 선택한 유형 **System Logs(**시스템 로그**)**에 대해 풀다운을 사용하여 `Info Warning Medium High(정보 경고 중간 높음)` 또는 `Critical(위험)` 옵션에서 심각도 레벨을 선택합니다. 유형 **Discovery(**검색**)**의 경우, `Info Medium Critical(정보 중간 위험)` 옵션에서 Severity(심각도) 레벨을 선택합니다.

단계 9 **Enabled(**활성화됨**)** - 확인란을 사용하여 이 알림 프로파일을 활성화합니다.

단계 10 **Save(**저장**)**를 클릭합니다.

PagerDuty 통합

구성이 완료되면 멀티 클라우드 방어 알림이 정의된 알림 서비스 프로필 및 알림 규칙을 사용하여 PagerDuty API 게이트웨이로 전송됩니다.

알림 프로파일 서비스 생성

Before you begin

이 가이드의 단계를 완료하려면 다음이 필요합니다.

• API 키가 구성된 PagerDuty 계정.

Tip

• PagerDuty 계정에 등록합니다(https://www.servicenow.com/my-account/sign-up.html 참조).

• API 키(https://developer.pagerduty.com/api-reference)를 설정합니다.

단계 1 **Administration(**관리**)** > **Alert Profiles(**알림 프로파일**)** > **Services(**서비스**)**로 이동합니다.

단계 2 **Create(**생성**)**를 클릭합니다.

단계 **3** **Name(**이름**)** - 알림 통합의 고유한 이름을 입력합니다. 예: `mcd-pagerduty-profile`.
단계 **4** **Description(**설명**)**(선택 사항) - 알림 통합에 대한 설명을 입력합니다.
단계 **5** **Type(**유형**)** - 풀다운을 사용하여 **PagerDuty**를 선택합니다.
단계 **6** **API Key(API** 키**)** - 위에서 생성한 PagerDuty API 키 또는 원하는 다른 PagerDuty API 키를 복사합니다.
단계 **7** **Save(**저장**)**를 클릭합니다.

What to do next

이 새 프로필로 알림 규칙을 생성합니다.

알림 규칙 생성

Before you begin

이 가이드의 단계를 완료하려면 다음이 필요합니다.

API 키가 구성된 PagerDuty 계정.

Tip

- PagerDuty 계정에 등록합니다(https://www.servicenow.com/my-account/sign-up.html 참조).
- API 키(https://developer.pagerduty.com/api-reference)를 설정합니다.

단계 **1** **Administration(**관리**) Alert Profiles(**알림 프로파일**) Services(**서비스**)**로 이동합니다.
단계 **2** **Create(**생성**)**를 클릭합니다.
단계 **3** **Profile Name(**프로파일 이름**)** - 통합의 고유한 이름을 입력합니다. 예: `mcd-pagerduty-alert-rule`.
단계 **4** **Description(**설명**)**(선택 사항) - 알림 규칙에 대한 설명을 입력합니다.
단계 **5** **Alert Profile(**알림 프로파일**)** - 풀다운을 사용하여 PagerDuty 알림 프로파일을 선택합니다. 예를 들어 위에서 생성한 프로파일을 선택합니다`mcd-pagerduty-profile`.
단계 **6** **Type(**유형**)** - 풀다운을 사용하여 **System Logs(**시스템 로그**)** 또는 **Discovery(**검색**)**를 선택합니다.
단계 **7** **Sub Type(**하위 유형**)** - **System Logs(**시스템 로그**)**의 경우 하위 유형 풀다운 옵션은 **Gateway(**게이트웨이**)** 또는 **Account(**계정**)** 중 하나입니다. **Discovery(**검색**)**의 경우 하위 유형 풀다운 옵션은 **Insights Rule(**인사이트 규칙**)**입니다.
단계 **8** **Severity(**심각도**)** - 선택한 유형 **System Logs(**시스템 로그**)**에 대해 풀다운을 사용하여 `Info Warning Medium High or Critical(정보 경고 중간 높음 또는 위험)` 옵션에서 심각도 레벨을 선택합니다. 유형 **Discovery(**검색**)**의 경우, `Info Medium Critical(정보 중간 위험)` 옵션에서 Severity(심각도) 레벨을 선택합니다.
단계 **9** **Enabled(**활성화됨**)** - 확인란을 사용하여 이 알림 프로파일을 활성화합니다.
단계 **10** **Save(**저장**)**를 클릭합니다.

ServiceNow 통합

구성한 멀티 클라우드 방어 알림은 정의된 알림 서비스 프로파일 및 알림 규칙을 사용하여 ServiceNow API 게이트웨이로 전송됩니다.

알림 프로파일 서비스 생성

Before you begin

이 가이드의 단계를 완료하려면 다음이 필요합니다.

- 수신 Webhook URL이 있는 ServiceNow 계정.
- API 키가 구성되었습니다.

Tip

- ServiceNow 계정(https://www.servicenow.com/my-account/sign-up.html)에 등록
- Webhook 및 API 키(https://docs.servicenow.com/search?q=setup%20webhook) 설정

단계 **1** **Administration(**관리**)** > **Alert Profiles(**알림 프로파일**)** > **Services(**서비스**)**로 이동합니다.

단계 **2** **Create(**생성**)**를 클릭합니다.

단계 **3** **Name(**이름**)** - 알림 통합의 고유한 이름을 입력합니다. 예: `mcd-servicenow-profile`.

단계 **4** **Description(**설명**)**(선택 사항) - 알림 통합에 대한 설명을 입력합니다.

단계 **5** **Type(**유형**)** - 풀다운을 사용하여 **ServiceNow**를 선택합니다.

단계 **6** **API Key(API** 키**)** - 위에서 생성한 ServiceNow API 키 또는 다른 ServiceNow API 키를 지정합니다.

단계 **7** **API URL** - 위에서 생성한 ServiceNow Webhook URL 또는 원하는 경우 다른 ServiceNow Webhook URL을 지정합니다.

단계 **8** **Save(**저장**)**를 클릭합니다.

What to do next

이 새 프로필로 알림 규칙을 생성합니다.

알림 규칙 생성

Before you begin

이 가이드의 단계를 완료하려면 다음이 필요합니다.

- 수신 Webhook URL이 있는 ServiceNow 계정.
- 구성된 API 키.

Tip

- ServiceNow 계정(https://www.servicenow.com/my-account/sign-up.html)에 등록
- Webhook 및 API 키(https://docs.servicenow.com/search?q=setup%20webhook) 설정

단계 **1** **Administration(**관리**)** > **Alert Profiles(**알림 프로파일**)** > **Services(**서비스**)**로 이동합니다.

단계 **2** **Create(**생성**)**를 클릭합니다.

단계 **3** **Profile Name(**프로파일 이름**)** - 통합의 고유한 이름을 입력합니다. 예: `mcd-servicenow-alert-rule`.

단계 **4** **Description(**설명**)**(선택 사항) - 알림 규칙에 대한 설명을 입력합니다.

단계 **5** **Alert Profile(**알림 프로파일**)** - 풀다운을 사용하여 ServiceNow 알림 프로파일을 선택합니다. 예를 들어 위에서 생성한 프로파일을 선택합니다`mcd-servicenow-profile`.

단계 **6** **Type(**유형**)** - 풀다운을 사용하여 **System Logs(**시스템 로그**)** 또는 **Discovery(**검색**)**를 선택합니다.

단계 **7** **Sub Type(**하위 유형**)**을 선택합니다.

- **System Logs(**시스템 로그**)** 유형의 경우 옵션은 **Gateway(**게이트웨이**)** 또는 **Account(**계정**)** 중 하나입니다.
- **Discovery(**검색**)** 유형의 경우 유일한 옵션은 **Insights Rule(**인사이트 규칙**)**입니다.

단계 **8** **Severity(**심각도**)**를 선택합니다.

- 선택한 유형 **System Logs(**시스템 로그**)**에 대해 풀다운을 사용하여 **Info Warning Medium High or Critical(**정보 경고 중간 높음 또는 위험**)** 옵션에서 심각도 레벨을 선택합니다.
- 유형 **Discovery(**검색**)**의 경우 **Info Medium Critical(**정보 미디어 중요**)**을 선택합니다.

단계 **9** **Enabled(**활성화됨**)** - 확인란을 사용하여 이 알림 프로파일을 활성화합니다.

단계 **10** **Save(**저장**)**를 클릭합니다.

Slack 통합

구성되면 정의된 알림 서비스 프로파일 및 규칙을 사용하여 멀티 클라우드 방어 알림이 Slack 수신 Webhook URL로 전송됩니다.

알림 프로파일 서비스 생성

Before you begin

이 가이드의 단계를 완료하려면 다음이 필요합니다.

- 수신 Webhook URL이 구성된 Slack 계정.

Tip

1. Slack 계정(https://slack.com/get-started#/create)을 생성합니다.
2. 수신 Webhook(https://slack.com/help/articles/115005265063-Incoming-webhooks-for-Slack#set-up-incoming-webhooks)을 생성합니다.

단계 **1** **Administration(**관리**)** > **Alert Profiles(**알림 프로파일**)** > **Services(**서비스**)**로 이동합니다.
단계 **2** **Create(**생성**)**를 클릭합니다.
단계 **3** **Name(**이름**)** - 알림 통합의 고유한 이름을 입력합니다. 예: `mcd-slack-profile`.
단계 **4** **Description(**설명**)**(선택 사항) - 알림 통합에 대한 설명을 입력합니다.
단계 **5** **Type(**유형**)** - 풀다운을 사용하여 **Slack**을 선택합니다.
단계 **6** **API URL** - 위에서 생성한 Slack Webhook URL 또는 원하는 경우 다른 Slack Webhook URL을 지정합니다.

What to do next

이 새 프로필로 알림 규칙을 생성합니다.

알림 규칙 생성

Before you begin

이 가이드의 단계를 완료하려면 다음이 필요합니다.

수신 Webhook URL이 구성된 Slack 계정.

Tip

1. Slack 계정(https://slack.com/get-started#/create)을 생성합니다.
2. 수신 Webhook(https://slack.com/help/articles/115005265063-Incoming-webhooks-for-Slack#set-up-incoming-webhooks)을 생성합니다.

단계 **1** **Administration(**관리**)** > **Alert Profiles(**알림 프로파일**)** > **Services(**서비스**)**로 이동합니다.

단계 **2** **Create(**생성**)**를 클릭합니다.

단계 **3** **Profile Name(**프로파일 이름**)** - 통합의 고유한 이름을 입력합니다. 예: `mcd-slack-alert-rule`.

단계 **4** **Description(**설명**)**(선택 사항) - 알림 규칙에 대한 설명을 입력합니다.

단계 **5** **Alert Profile(**알림 프로파일**)** - 풀다운을 사용하여 Slack 알림 프로파일을 선택합니다. 예를 들어 위에서 생성한 프로파일을 선택합니다`mcd-slack-profile`.

단계 **6** **Type(**유형**)** - 풀다운을 사용하여 **System Logs(**시스템 로그**)** 또는 **Discovery(**검색**)**를 선택합니다.

단계 **7** **Sub Type(**하위 유형**)** - **System Logs(**시스템 로그**)**의 경우 하위 유형 풀다운 옵션은 **Gateway(**게이트웨이**)** 또는 **Account(**계정**)** 중 하나입니다. **Discovery(**검색**)**의 경우 하위 유형 풀다운 옵션은 **Insights Rule(**인사이트 규칙**)**입니다.

단계 **8** **Severity(**심각도**)** - 선택한 유형 **System Logs(**시스템 로그**)**에 대해 풀다운을 사용하여 `Info Warning Medium High or Critical(정보 경고 중간 높음 또는 위험)` 옵션에서 심각도 레벨을 선택합니다. 유형 **Discovery(**검색**)**의 경우, `Info Medium Critical(정보 중간 위험)` 옵션에서 Severity(심각도) 레벨을 선택합니다.

단계 **9** **Enabled(**활성화됨**)** - 확인란을 사용하여 이 알림 프로파일을 활성화합니다.

단계 **10** **Save(**저장**)**를 클릭합니다.

Webex 통합

구성이 완료되면 멀티 클라우드 방어 알림이 정의된 알림 서비스 프로필 및 알림 규칙을 사용하여 Webex API 게이트웨이로 전송됩니다.

알림 프로파일 서비스 생성

시작하기 전에

이 가이드의 단계를 완료하려면 다음이 필요합니다.

- 수신 Webhook URL이 있는 Webex 계정.
- API 키가 구성되었습니다.

참고

1. Webex 계정을 생성하거나 액세스합니다.
2. Webex 수신 Webhook을 생성합니다.
3. 수신 Webhook 권한을 수락합니다.
4. 이름을 제공하고 Webex Space를 선택합니다.
5. 알림 서비스 프로파일의 설정에 사용할 Webex Webhook URL을 복사합니다.

단계 **1** **Administration(**관리**)** > **Alert Profiles(**알림 프로파일**)** > **Services(**서비스**)**로 이동합니다.

단계 **2** **Create(**생성**)**를 클릭합니다.

단계 **3** **Name(**이름**)** - 알림 통합의 고유한 이름을 입력합니다. `mcd-servicenow-profile`을(를) 예로 들 수 있습니다.

단계 **4** (선택 사항) **Description(**설명**)** - 알림 통합에 대한 설명을 입력합니다.

단계 **5** **Type(**유형**)** - 풀다운을 사용하여 **Webex**를 선택합니다.

단계 **6** **API URL** - 사전 요구 사항의 일부로 생성된 Webex Webhook URL 또는 원하는 경우 다른 Webhook URL을 지정합니다.

다음에 수행할 작업

이 새 프로필로 알림 규칙을 생성합니다.

알림 규칙 생성

단계 **1** **Administration(**관리**)** > **Alert Profiles(**알림 프로파일**)** > **Services(**서비스**)**로 이동합니다.

단계 **2** **Create(**생성**)**를 클릭합니다.

단계 **3** **Profile Name(**프로파일 이름**)** - 통합의 고유한 이름을 입력합니다. `mcd-servicenow-alert-rule`을(를) 예로 들 수 있습니다.

단계 **4** (선택 사항) **Description(**설명**)** - 알림 규칙에 대한 설명을 입력합니다.

단계 **5** **Alert Profile(**알림 프로파일**)** - 풀다운을 사용하여 **Webex** 알림 프로파일을 선택합니다. 예를 들어 위의 mcd-servicenow-profile에서 생성한 프로파일을 선택합니다.

단계 **6** **Type(**유형**)** - 풀다운을 사용하여 **System Logs(**시스템 로그**)** 또는 **Discovery(**검색**)**를 선택합니다.

단계 **7** **Sub Type(**하위 유형**)**을 선택합니다.

- System Logs(시스템 로그) 유형의 경우 옵션은 **Gateway(**게이트웨이**)** 또는 **Account(**계정**)** 중 하나입니다.
- Discovery(검색) 유형의 경우 유일한 옵션은 **Insights Rule(**인사이트 규칙**)**입니다.

단계 **8** **Severity(**심각도**)**를 선택합니다.

- 선택한 유형 System Logs(시스템 로그)에 대해 풀다운을 사용하여 **Info Warning Medium High(**정보 경고 중간 높음**)** 또는 **Critical(**위험**)**을 선택합니다.
- 유형 Discovery(검색)의 경우 **Info Medium Critical(**정보 미디어 중요**)**을 선택합니다.

단계 **9** **Enabled(**활성화됨**)** - 확인란을 사용하여 이 알림 프로파일을 활성화합니다.

단계 **10** **Save(**저장**)**를 클릭합니다.