

不正および aWIPS イベント通知

• 不正および aWIPS イベント通知, on page 1

不正および aWIPS イベント通知

不正または aWIPS 攻撃が発生するたびに通知を送信するように Cisco DNA Center を構成できます。これらのイベントは、Cisco DNA Center 通知センターに記録されません。不正の脅威または aWIPS 脅威に登録した後にイベントが発生した場合、REST API (ウェブフック、PagerDuty、および Webex)または syslog サーバーを介して通知を受信できます。

- ウェブフックおよび syslog の接続先を設定するには、『Cisco DNA Center Platform User Guide』の「Work with Events」トピックを参照してください。https://www.cisco.com/c/en/us/support/cloud-systems-management/dna-center/products-user-guide-list.html
- PagerDutyの接続先を設定するには、『Cisco DNA Center ITSM Integration Guide』の「Cisco DNA Center to Cisco WebEx Integration」のトピックを参照してください。
 https://www.cisco.com/c/en/us/support/cloud-systems-management/dna-center/
 products-user-guide-list.html
- Webex の接続先を設定するには、『Cisco DNA Center ITSM Integration Guide』の「Cisco DNA Center to Cisco WebEx Integration」のトピックを参照してください。https://www.cisco.com/c/en/us/support/cloud-systems-management/dna-center/products-user-guide-list.html

この手順を完了したら、不正または aWIPS イベントを選択し、登録していることを確認します。

Cisco DNA Center GUI で不正または aWIPS イベントに登録するには、メニューアイコン (≡) をクリックし、[Platform] > [Developer Toolkit] > [Events] を選択します。



Note

サブスクリプション後にのみイベント通知を受け取ります。サブスクリプション前に発生した 脅威の場合は、Cisco DNA Center GUI で、メニューアイコン (═) をクリックし、[Reports] > [Report Templates] > [Rogue and aWIPS] を選択します。

Webex および PagerDuty の接続先には、5 分あたり 100 件のイベント通知の制限があります。 5 分間に 100 件を超えるイベントを受信する場合は、ウェブフックまたは syslog の接続先を構成します。

不正イベント

不正イベントは、次の脅威レベルの高い不正に対してのみトリガーされます。

- ビーコン不正チャネル
- ビーコン DS 攻撃
- AP 偽装
- 有線ネットワーク上の不正
- ハニーポット
- 脅威レベルを高として作成されたカスタムルール

不正イベントは、次の場合にトリガーされます。

- ・脅威レベルの高い不正がネットワークで初めて発見された (ROGUE_NEW_THREAT_DETECTED)
- 脅威レベルの高い不正がネットワークで削除された (ROGUE THREAT DELETED)
- 脅威レベルが [High] から [Potential] または [Informational] に変更された (ROGUE_THREAT_LEVEL_CHANGED)
- 脅威レベルが [Potential] または [Informational] から [High] に変更された (ROGUE_THREAT_LEVEL_CHANGED)
- ・脅威レベルは [High] のままだが、脅威の種類が変わった (ROGUE_THREAT_TYPE_CHANGED)

不正イベントペイロードの詳細:

```
"detectingApLocation": "string",
"rssi": "int",
"threatMacAddress": "string",
"threatType": "string",
"detectingApMacAddress": "string",
"threatState": "string",
"wlcIp": "string",
"detectingApName": "string",
"containmentState": "string",
```

```
"vendorName": "string",
"ssid": "string",
"threatLevel": "string"
}
```

ペイロード内のコマンド:

- threatMacAddress: 不正 AP の MAC アドレス
- ThreatType: 不正の脅威のタイプ (ビーコン DS 攻撃、AP 偽装、有線ネットワーク上の不正、ハニーポット、または脅威レベルを高として作成されたカスタムルール)
- threatState: 不正の脅威の状態(ROGUE_NEW_THREAT_DETECTED、ROGUE_THREAT_DELETED、ROGUE_THREAT_LEVEL_CHANGED)、ROGUE_THREAT_LEVEL_CHANGED、またはROGUE_THREAT_TYPE_CHANGED
- threatLevel:不正の状態(高、潜在的、または情報)
- detecting Ap Name: 最も強力な検出 AP の名前
- detecting Ap Mac Address: 最も強力な検出 AP の MAC アドレス
- detectingApLocation:最も強力な検出 AP の場所
- rssi: 不正 AP を検出する検出 AP の RSSI 値
- containmentState:不正 AP の封じ込め状態 (PENDING、NOTCONTAINED、または CONTAINED)
- threat Vendor Name: 不正 AP のベンダー名
- ssid: 最新の SSID またはハニーポット SSID
- wlcIp: ワイヤレスコントローラ の IP アドレス

aWIPS イベント

aWIPS イベントは、ネットワーク内のすべての aWIPS 脅威に対してトリガーされます。

検出 AP ごとに通知が送信されます。複数の AP が同じ脅威を検出した場合、複数のイベント通知を受け取ります。

送信元ベースの aWIPS 脅威の場合、送信元情報が送信されます。接続先情報は [Not Applicabl] として送信されます。

接続先ベースのaWIPS 脅威の場合、接続先情報が送信されます。送信元情報は[Not Applicable] として送信されます。

ペアベースの aWIPS 脅威の場合、送信元と接続先の両方の情報が送信されます。

aWIPS イベントペイロードの詳細:

```
{
  "sourceVendorName": "string",
  "detectingApLocation": "string",
  "attackType": "string",
```

```
"sourceMacAddress": "string",
"detectingApMacAddress": "string",
"wlcIp": "string",
"detectingApName": "string",
"targetMacAddress": "string"
```

ペイロード内のコマンド:

• attackType: aWIPS 攻撃の種類

• sourceMacAddress: 攻撃者の MAC アドレス

• source Vendor Name: 攻撃者のベンダー名

• targetMacAddress: ターゲットの MAC アドレス

• detectingApLocation:検出APの場所

• detectingApMacAddress: 検出 APの MAC アドレス

• detectingApName: 検出 AP の名前

• wlcIp: ワイヤレスコントローラ の IP アドレス

翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。