

# 使用XDR配置邮件通知自动化工作流程

## 目录

---

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[配置](#)

[从Cisco XDR Exchange安装 workflows](#)

[步骤1.安装终端隔离 workflows](#)

[创建自动化规则](#)

[步骤2.配置自动化规则](#)

[验证 workflows 功能](#)

[步骤3.验证 workflows 执行](#)

[步骤4.确认电子邮件通知](#)

---

## 简介

本文档介绍如何创建自动 workflows 以发送新事故的电子邮件通知。

## 先决条件

### 要求

本文档没有任何特定的要求。

### 使用的组件

本文档不限于特定的软件和硬件版本。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

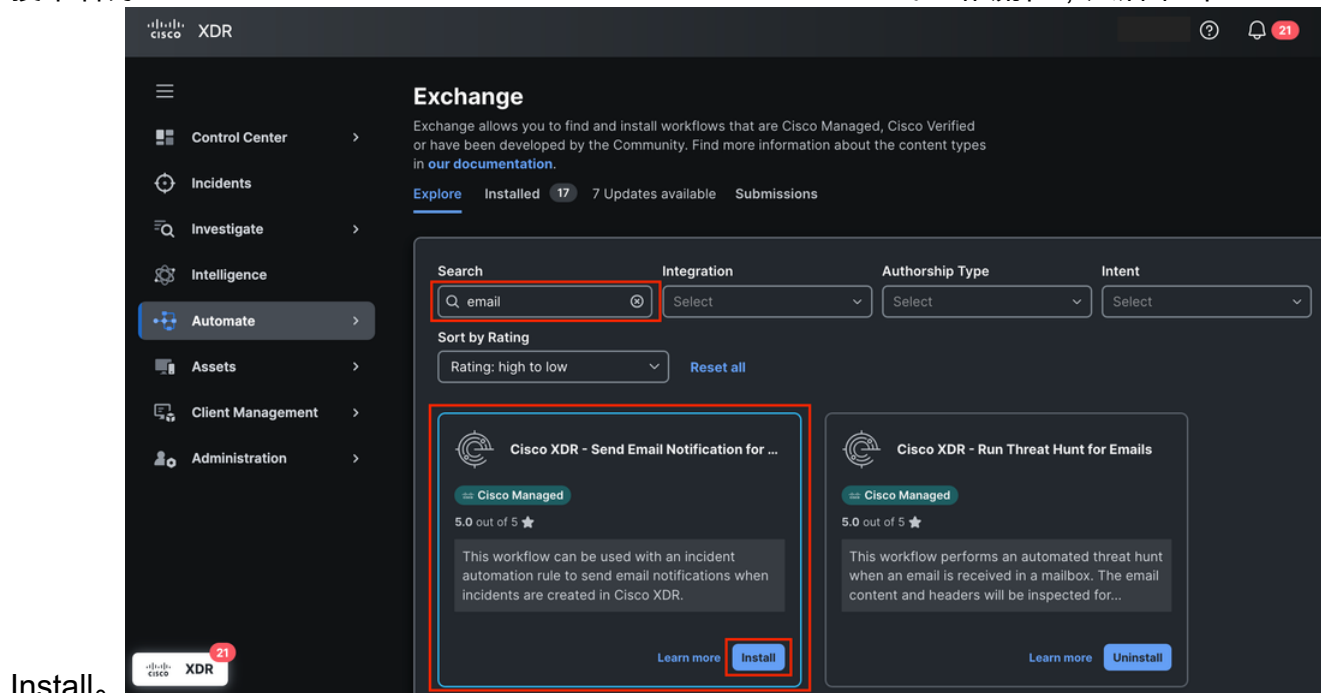
## 配置

本指南详细介绍配置和激活 workflows 的必要步骤，以便在发生事故时自动发送电子邮件通知。具体步骤如下。

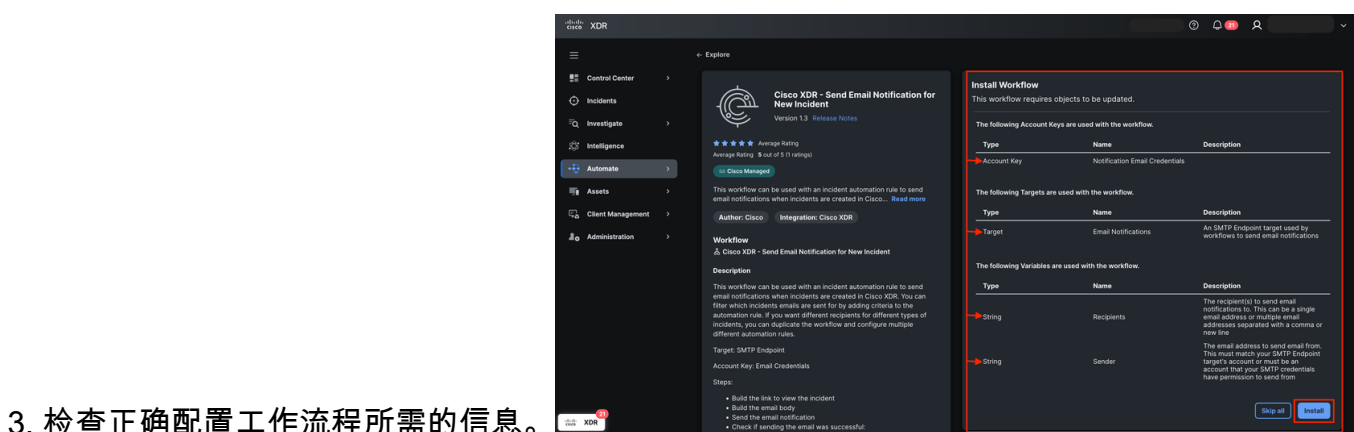
### 从Cisco XDR Exchange安装 workflows

#### 步骤1.安装终端隔离 workflows

1. 登录到Cisco XDR并导航到自动> Exchange。
2. 搜索名为Cisco XDR - Send Email Notification for New Incident的工作流程，然后单击

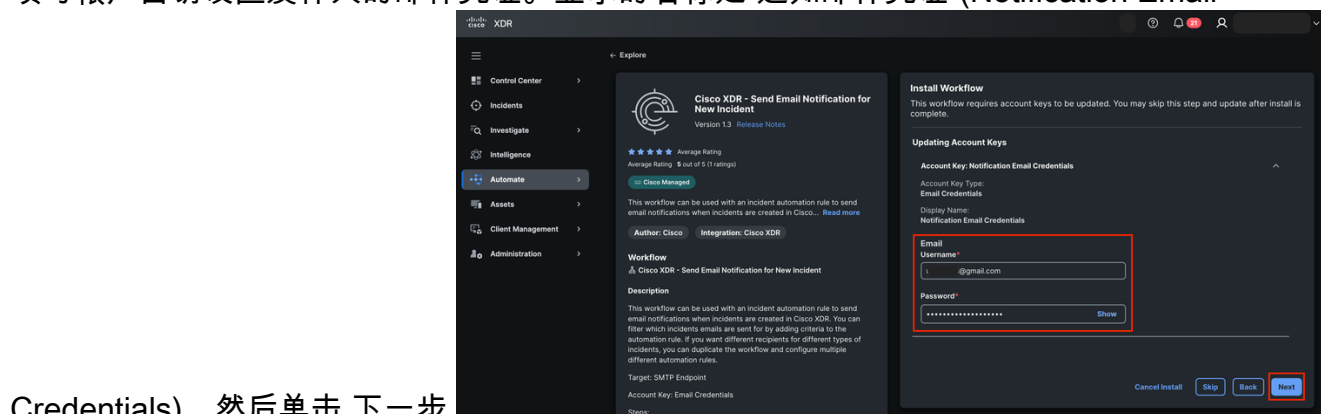


从Exchange发送电子邮件通知工作流



发送电邮通知工作流程概述

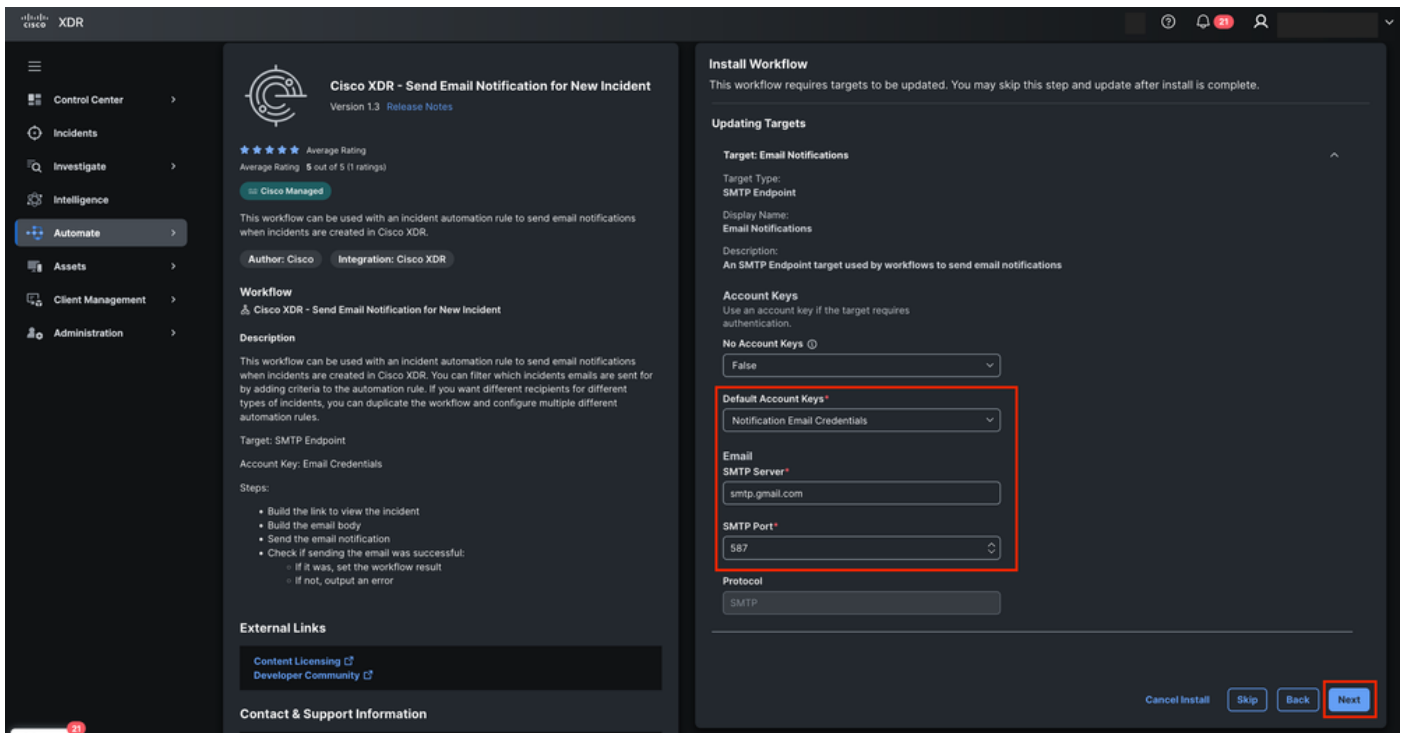
4. 填写帐户密钥设置发件人的邮件凭证。显示的名称是“通知邮件凭证”(Notification Email



工作流的帐户密钥

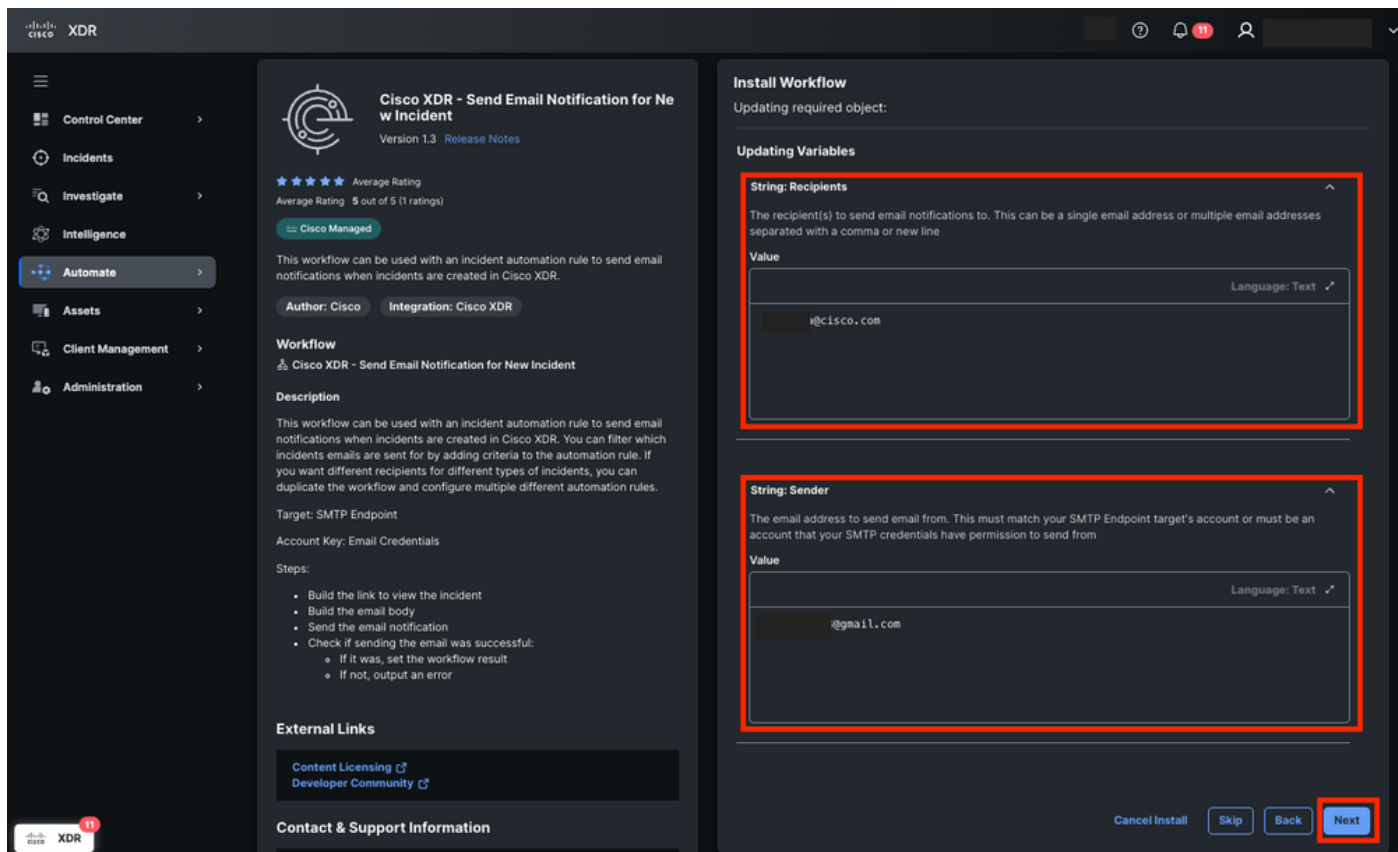
## 5. 使用以下设置配置目标信息：

- 帐户密钥：通知邮件凭据
- 发送邮件
  - SMTP服务器：smtp.gmail.com
  - SMTP端口：587



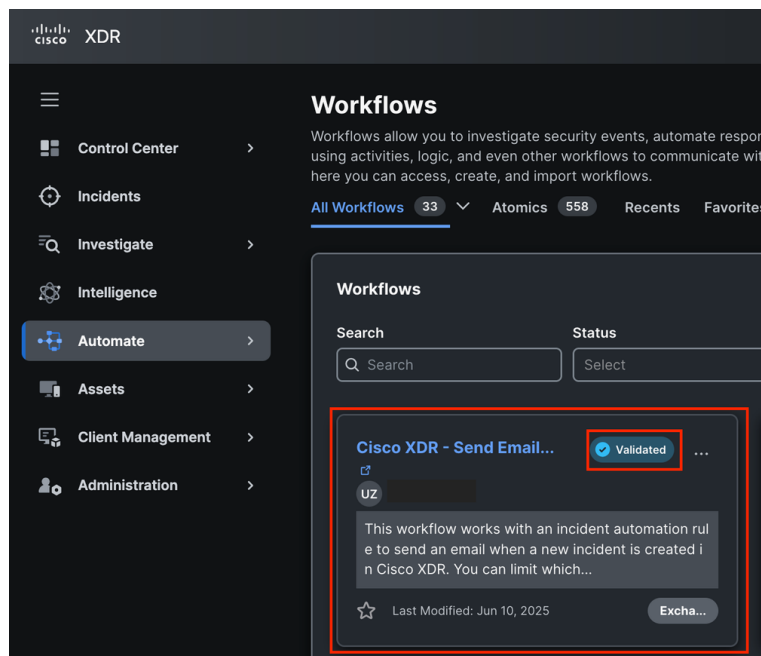
### 工作流程的目标配置

1. 单击 Next。
2. 更新以下项的变量：
  - 收件人
  - 发件人



为工作流分配变量

8.单击“下一步”。



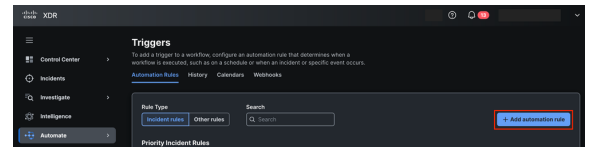
9.定位至自动>工作流，以检查“已验证”状态。

工作流验证状态

创建自动化规则

步骤2.配置自动化规则

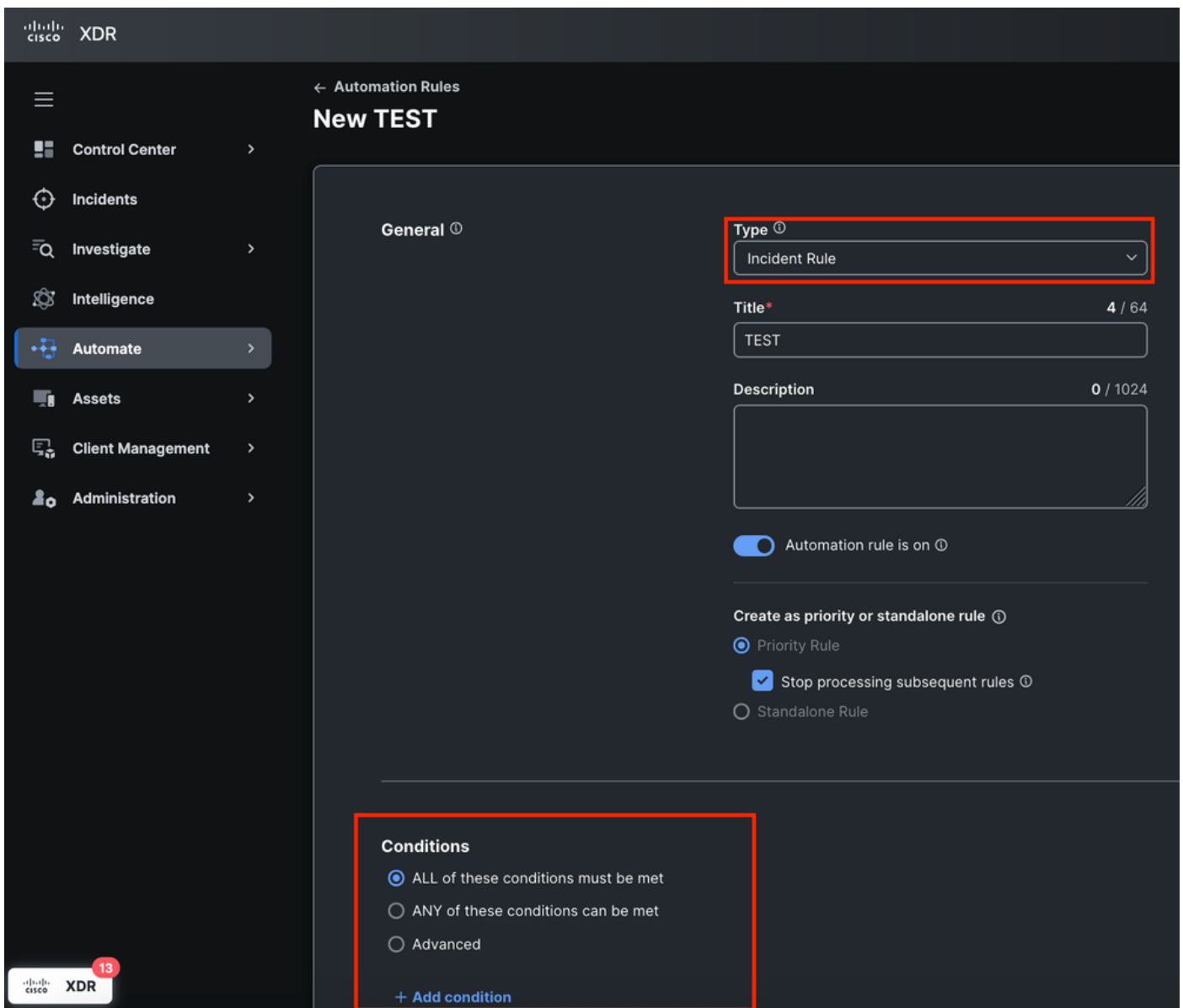
1. 导航到自动化>触发器部分。



2. 创建新规则。单击Add automation rule并分配名称。

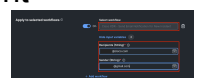
从触发器添加自动化规则

3. 选择Incident Rule类型并定义触发条件。您可以继续操作，而无需添加规则条件，这样可确保任何突发事件都会激活此规则。如有必要，请自定义条件。



自动化规则类型和条件

4.将自动化规则应用于之前安装的Cisco XDR - Send Email Notification for New Incident workflow(Cisco XDR — 发送新事件工作流程的电邮)。设置Recipients和Sender变量。



将自动化规则应用于工作流程并分配变量

5.保存规则。

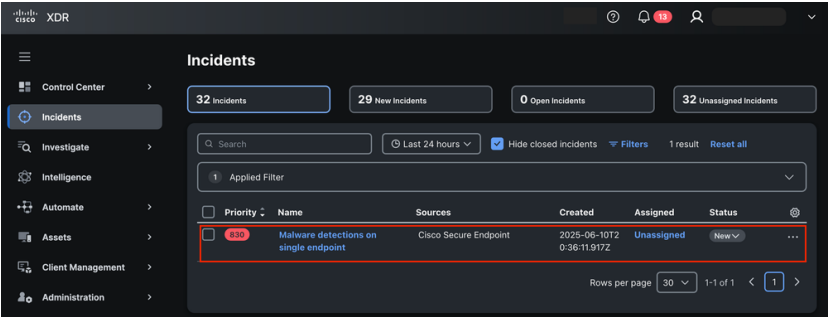
# 验证 workflow 功能

## 步骤3.验证 workflow 执行

1. 生成或等待符合规则条件的事件。

检测到Cisco XDR中的新事件

2. 单击Incident，然后单击View Incident Detail。



# Malware detections on single endpoint



Priority **830** Status **New**

Reported by  
**Cisco XDR Analytics**

on 2025-06-10T20:36:11.917Z

Unassigned

MITRE

## Priority score breakdown



**830**

**83**

Detection  
Risk

**10**

Asset  
Value at Risk

## Sources



Cisco Secure Endpoint



[View Incident Detail](#)

---

基于第一次检测生成初始事件名称；但是，如果发生其他检测或新信息丰富了事故，则情况可能会发生变化。

---

## 关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。