

Event Viewer

File Action View Help

Event Viewer (Local)

- Custom Views
  - Cisco
    - Cisco Ar
    - Cisco Ar
    - Cisco Se
  - ServerRoles
  - Administrati
- Windows Logs
- Applications an
- Saved Logs
- Subscriptions

Cisco Secure Endpoint Number of events: 76

Level	Date and Time	Source	Event ID	Task Categ...
Information	11/16/2023 12:09:58 PM	CiscoSecu...	1300	Detection
Error	11/16/2023 12:09:58 PM	CiscoSecu...	1311	Quarantine
Information	11/16/2023 12:09:58 PM	CiscoSecu...	1300	Detection
Error	11/16/2023 12:09:58 PM	CiscoSecu...	1311	Quarantine
Information	11/14/2023 1:21:41 PM	CiscoSecu...	1300	Detection
Error	11/14/2023 1:21:41 PM	CiscoSecu...	1311	Quarantine
Information	11/14/2023 1:21:41 PM	CiscoSecu...	1300	Detection
Error	11/14/2023 1:21:41 PM	CiscoSecu...	1311	Quarantine

Event 1300, CiscoSecureEndpoint

General Details

☒ Friendly View ☐ XML View

+ System

- EventData

**DetectionName** Gen:Variant.Fugrafa.302351

**DetectionId** 7301946046790238210

**ParentName** pb220.exe

**DetectedFilePath** C:\Experiments\images\_icons\imageicontest\_cloud.exe

**DetectionEngine** 64

Event Viewer

File Action View Help

Event Viewer (Local)

- Custom Views
  - Cisco
    - Cisco AnyConnect Secure Mobility Client
    - Cisco AnyConnect Umbrella Roaming
    - Cisco Secure Endpoint
  - ServerRoles
  - Administrative Events
- Windows Logs
  - Application
  - Security
  - Setup
  - System
  - Forwarded Events
- Applications and Services Logs
  - Saved Logs
  - Subscriptions

Cisco Secure Endpoint Number of events: 55 (1) New events available

Level	Date and Time	Source	Event ID	Task Category
Error	11/13/2023 3:39:08 PM	CiscoSecureEndpoint	1311	Quarantine
Error	11/13/2023 3:39:08 PM	CiscoSecureEndpoint	1311	Quarantine
Information	11/13/2023 3:39:08 PM	CiscoSecureEndpoint	1300	Detection
Information	11/13/2023 3:39:08 PM	CiscoSecureEndpoint	1300	Detection
Error	11/13/2023 3:38:47 PM	CiscoSecureEndpoint	1311	Quarantine
Error	11/13/2023 3:38:47 PM	CiscoSecureEndpoint	1311	Quarantine
Information	11/13/2023 3:38:47 PM	CiscoSecureEndpoint	1300	Detection
Information	11/13/2023 3:38:47 PM	CiscoSecureEndpoint	1300	Detection

Event 1300, CiscoSecureEndpoint

General Details

☐ Friendly View ☒ XML View

```
<?xml version="1.0" encoding="UTF-8"?>
<Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event">
  <System>
    <Provider Name="CiscoSecureEndpoint" Guid="{0643104d-3c79-4ed5-9ed4-cd8e803fea9c}" />
    <EventID>1300</EventID>
    <Version>1</Version>
    <Level>4</Level>
    <Task>10</Task>
    <Opcode>0</Opcode>
    <Keywords>0x8000000000000000</Keywords>
    <TimeCreated SystemTime="2023-11-13T10:09:08.6021627Z" />
    <EventRecordID>52</EventRecordID>
    <Correlation />
    <Execution ProcessID="5636" ThreadID="8872" />
    <Channel>CiscoSecureEndpoint/Events</Channel>
    <Computer>[REDACTED]</Computer>
    <Security UserID="S-1-5-18" />
  </System>
  <EventData>
    <Data Name="DetectionName">Gen:Variant.Fugrafa.302351</Data>
    <Data Name="DetectionId">7300886693106679829</Data>
    <Data Name="ParentName">pb220.exe</Data>
    <Data Name="DetectedFilePath">C:\Experiments\myimageapp\RCXEE99.tmp</Data>
    <Data Name="DetectionEngine">64</Data>
  </EventData>
</Event>
```