You Won't Believe How Splunk Built This Mind-Blowing Plugin for Microsoft Security Copilot

cisco Live!

Wayne Brown
Sr. Global Partner Technical Manager
Splunk

DEVNET-2336

Cisco Webex App

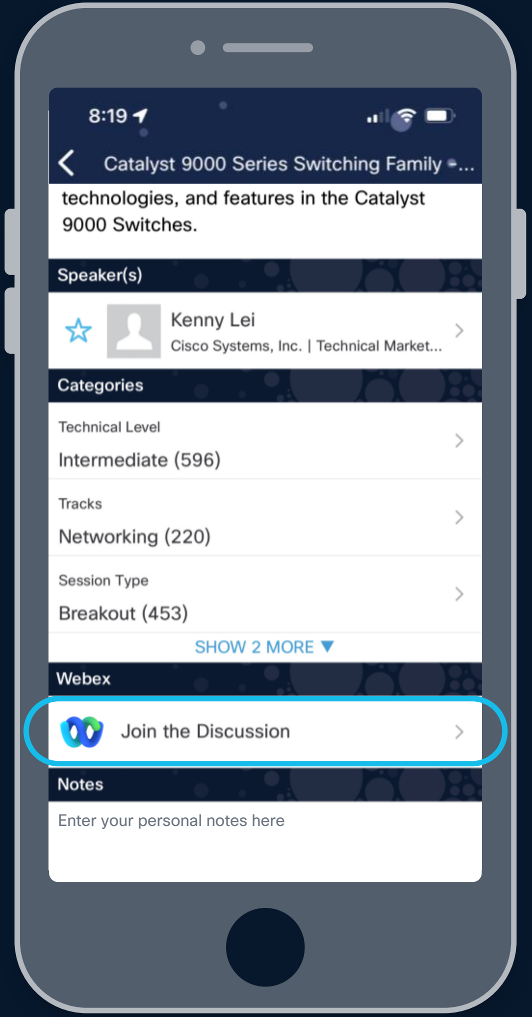
Questions?

Use Cisco Webex App to chat
with the speaker after the session

How

1. Find this session in the Cisco Live Mobile App
2. Click “Join the Discussion”
3. Install the Webex App or go directly to the Webex space
4. Enter messages/questions in the Webex space

Webex spaces will be moderated by the speaker until June 13, 2025.



8:19

Catalyst 9000 Series Switching Family •...

technologies, and features in the Catalyst 9000 Switches.

Speaker(s)

Kenny Lei
Cisco Systems, Inc. | Technical Market...

Categories

Technical Level
Intermediate (596)

Tracks
Networking (220)

Session Type
Breakout (453)

SHOW 2 MORE ▼

Webex

Join the Discussion

Notes

Enter your personal notes here

Poll Time

Do not edit

How to change the design

Join at slido.com
#DEVNET-2336

The Slido app must be installed on every computer you’re presenting from

Do not edit
How to change the design

How familar are you with Splunk?

ⓘ The Slido app must be installed on every computer you're presenting from

slido

Agenda

01 Quick Splunk Overview

02 Why We Built This Plugin

03 How It Works

04 Demo

05 Conclusion

Quick Splunk Overview

Our Purpose is to build a <u>safer</u> and more <u>resilient</u> digital world.

What the Splunk Platform Does

Get Data In

Files, Scripts, APIs, Wire
OTLP, Code, Network,
Local, Remote, Data Lakes

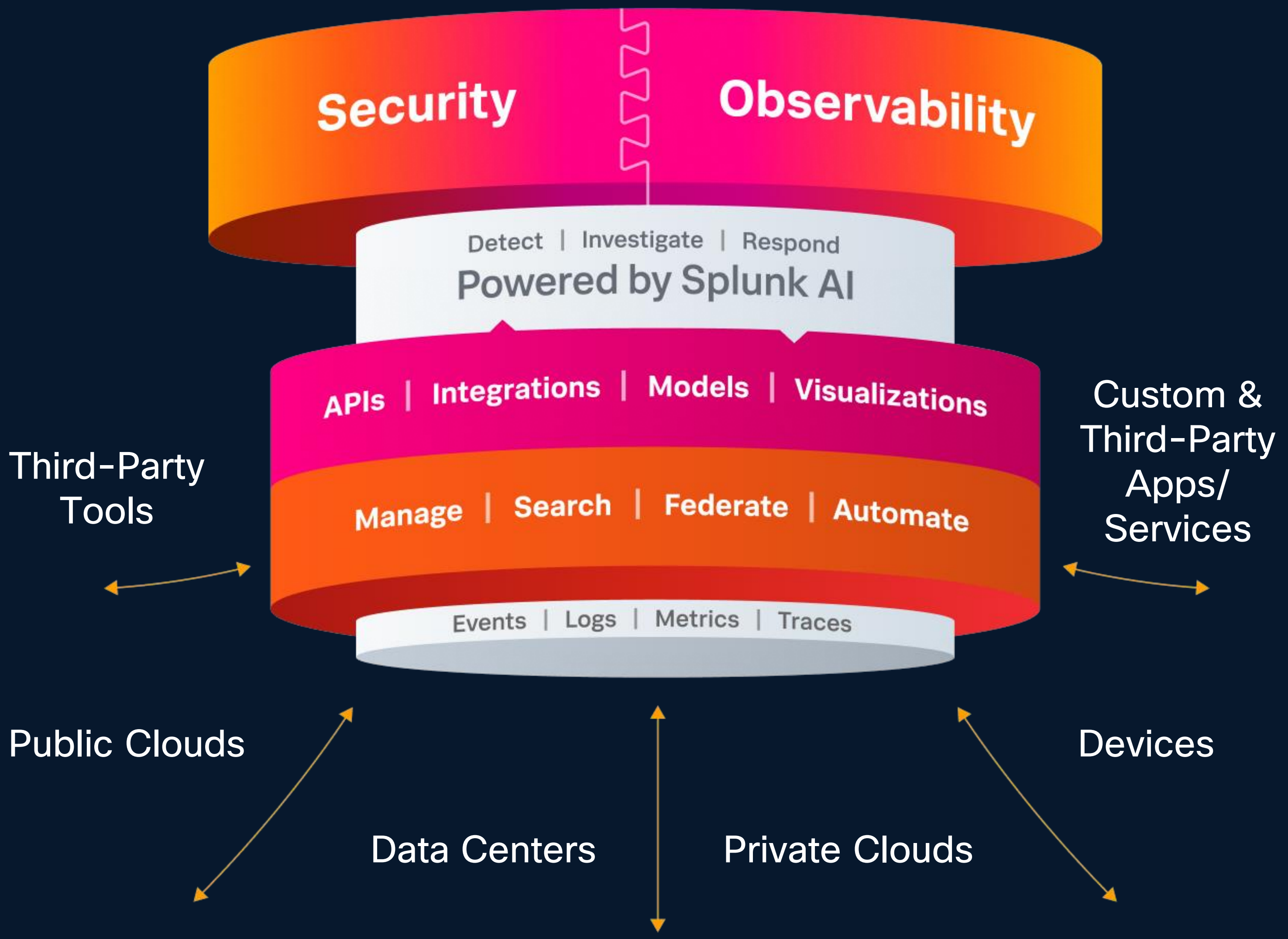
Ask Questions from Data

Ad-Hoc, Dashboards, SPL
Feeds, Security,
Observability, Assurance

Take Action on Data

Simple Actions,
Complex Workflows (SOAR),
3rd Party Systems

Any Data
Any Question
Any Action


Security
Observability
Detect | Investigate | Respond
Powered by Splunk AI
APIs | Integrations | Models | Visualizations
Manage | Search | Federate | Automate
Events | Logs | Metrics | Traces
Third-Party Tools
Custom & Third-Party Apps/ Services
Public Clouds
Data Centers
Private Clouds
Devices

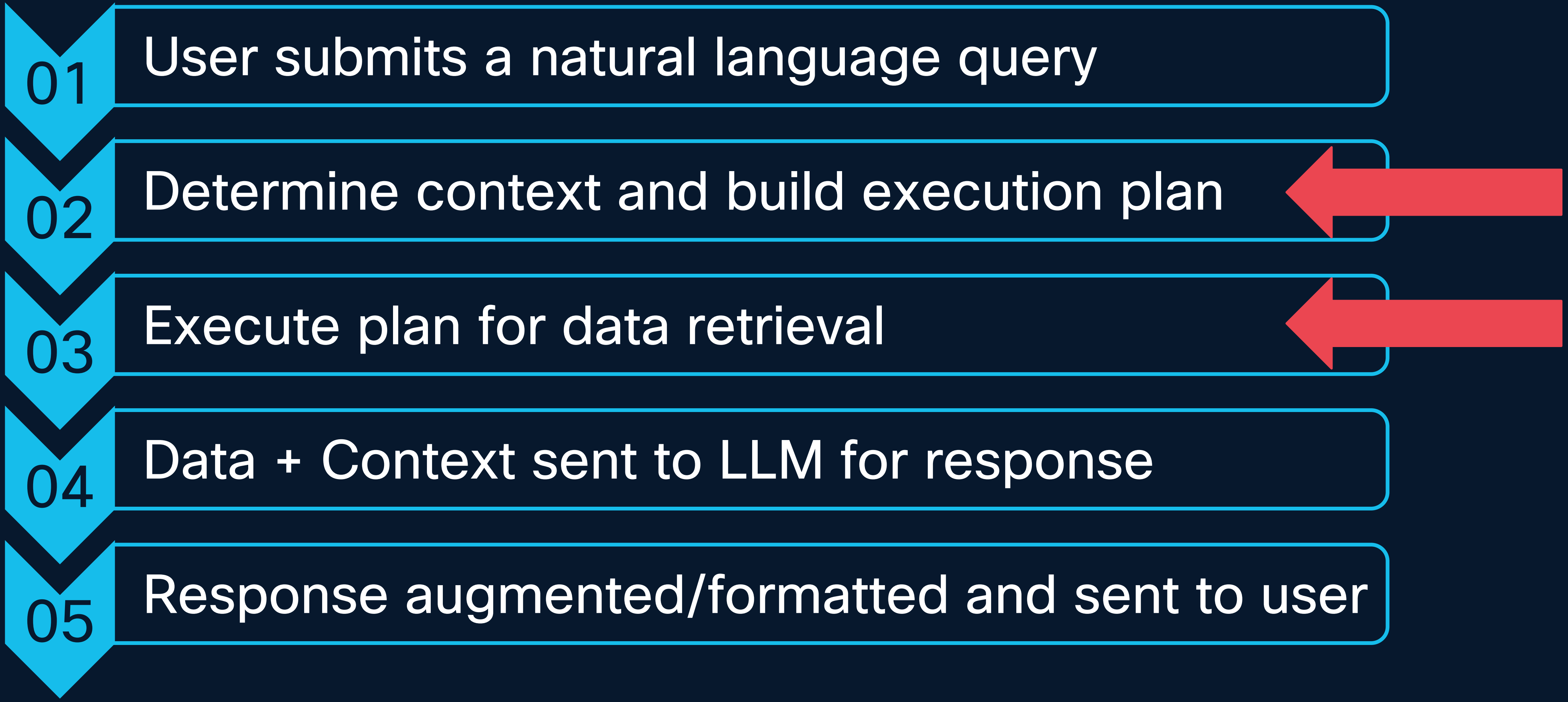
Why We Built This Plugin

Why We Built This Plugin

- Meet Our Customers Where They Are
- Grow the Splunk/Microsoft Partnership

How It Works

Process Flow (Very Simplified)



01 User submits a natural language query

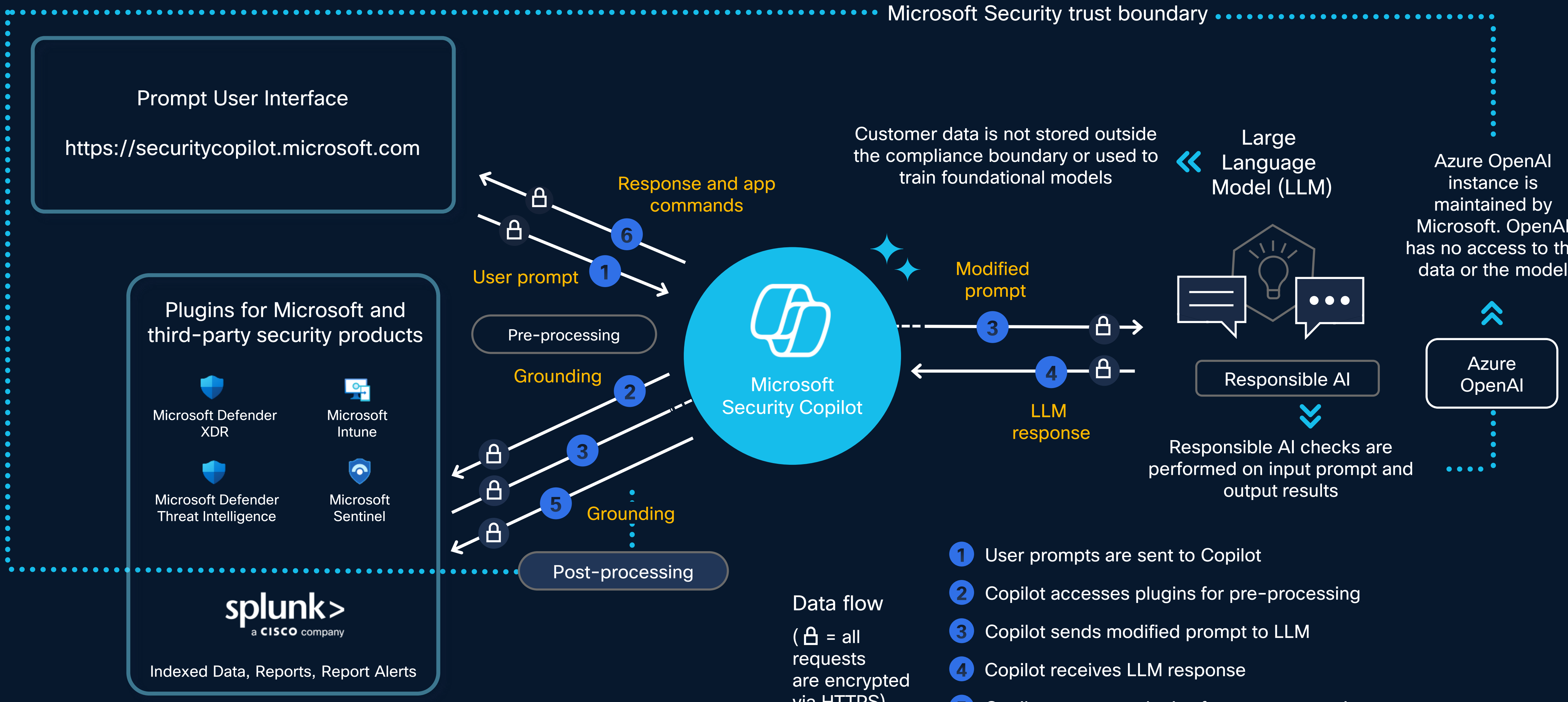
02 Determine context and build execution plan

03 Execute plan for data retrieval

04 Data + Context sent to LLM for response

05 Response augmented/formatted and sent to user

Data Flow



Microsoft Security trust boundary

Prompt User Interface

https://securitycopilot.microsoft.com

Response and app commands 6

User prompt 1

Pre-processing

Grounding 2

3

5 Grounding

Post-processing

Plugins for Microsoft and third-party security products

Microsoft Defender XDR

Microsoft Intune

Microsoft Defender Threat Intelligence

Microsoft Sentinel

splunk> a CISCO company

Indexed Data, Reports, Report Alerts

Microsoft Security Copilot

Modified prompt 3

4 LLM response

Customer data is not stored outside the compliance boundary or used to train foundational models

Large Language Model (LLM)

Responsible AI

Responsible AI checks are performed on input prompt and output results

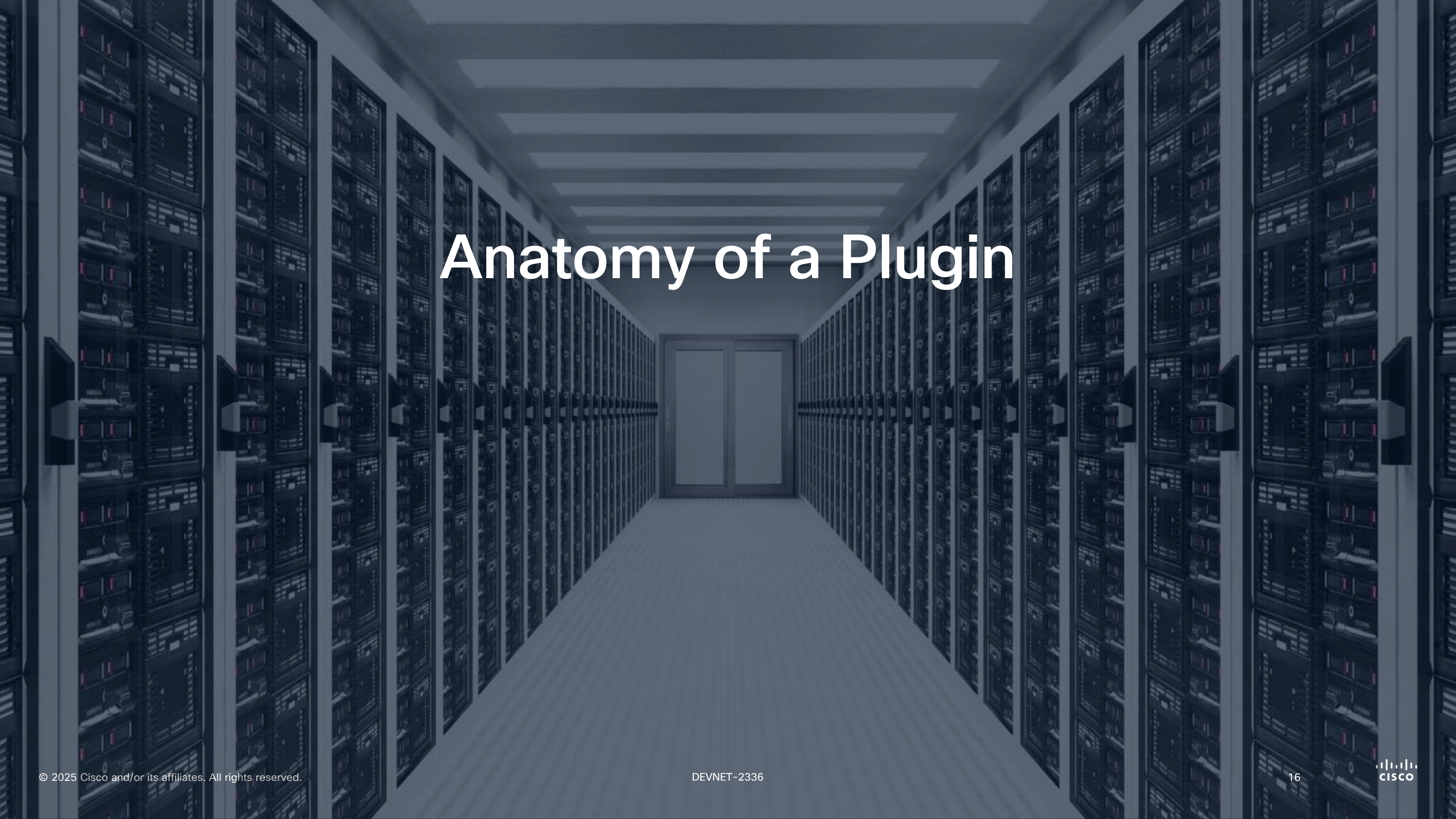
Azure OpenAI instance is maintained by Microsoft. OpenAI has no access to the data or the model

Azure OpenAI

Data flow

(🔒 = all requests are encrypted via HTTPS)

1. User prompts are sent to Copilot
2. Copilot accesses plugins for pre-processing
3. Copilot sends modified prompt to LLM
4. Copilot receives LLM response
5. Copilot accesses plugins for post-processing
6. Copilot sends the response back



Anatomy of a Plugin

Anatomy of a Plugin: Required Files

Plugin Version

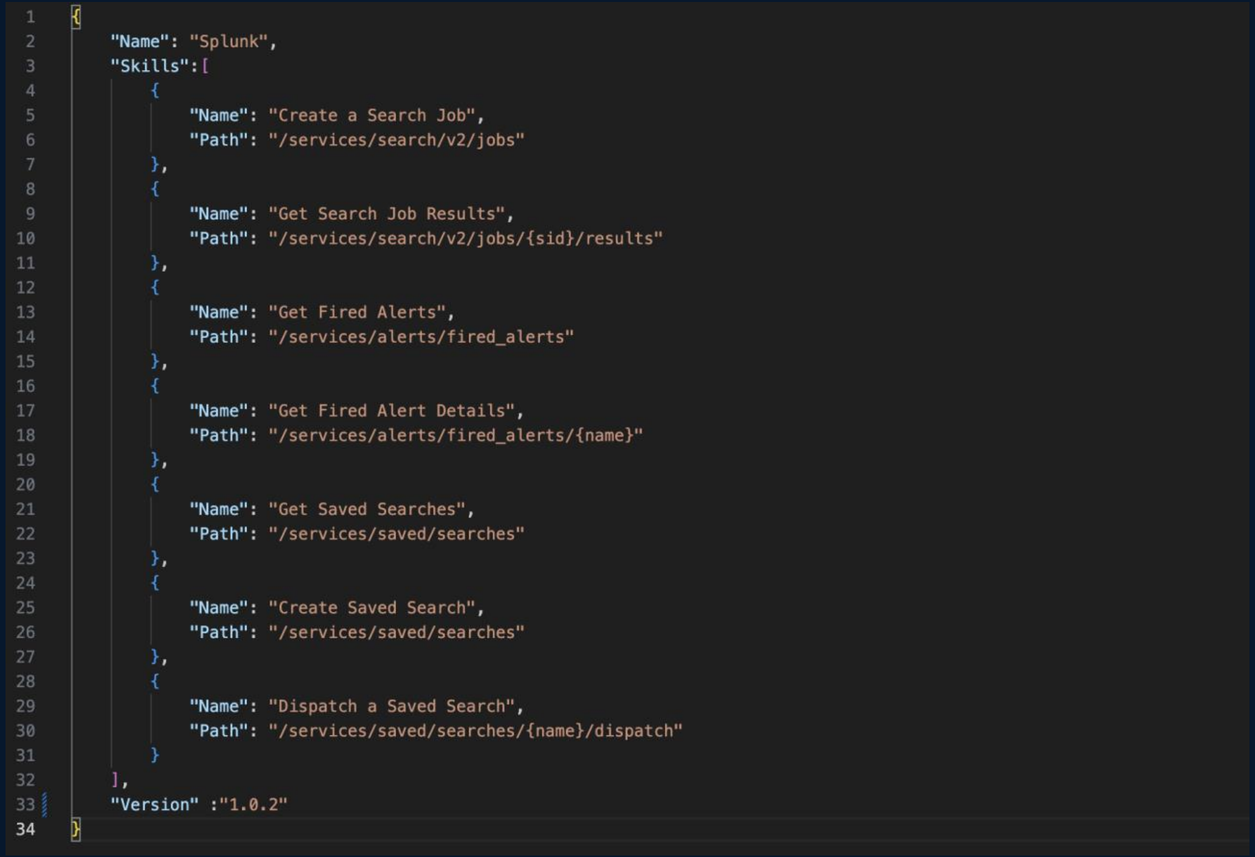
- JSON format
- Named *pluginVersion.json*
- Contains plugin name, version number, and skills published.

Manifest

- JSON or YAML format
- Named *manifest.json* or *manifest.yaml*
- Description and SkillGroups sections
  - Configuration settings
  - Auth types
- ** Version number must match version number in plugin version file**

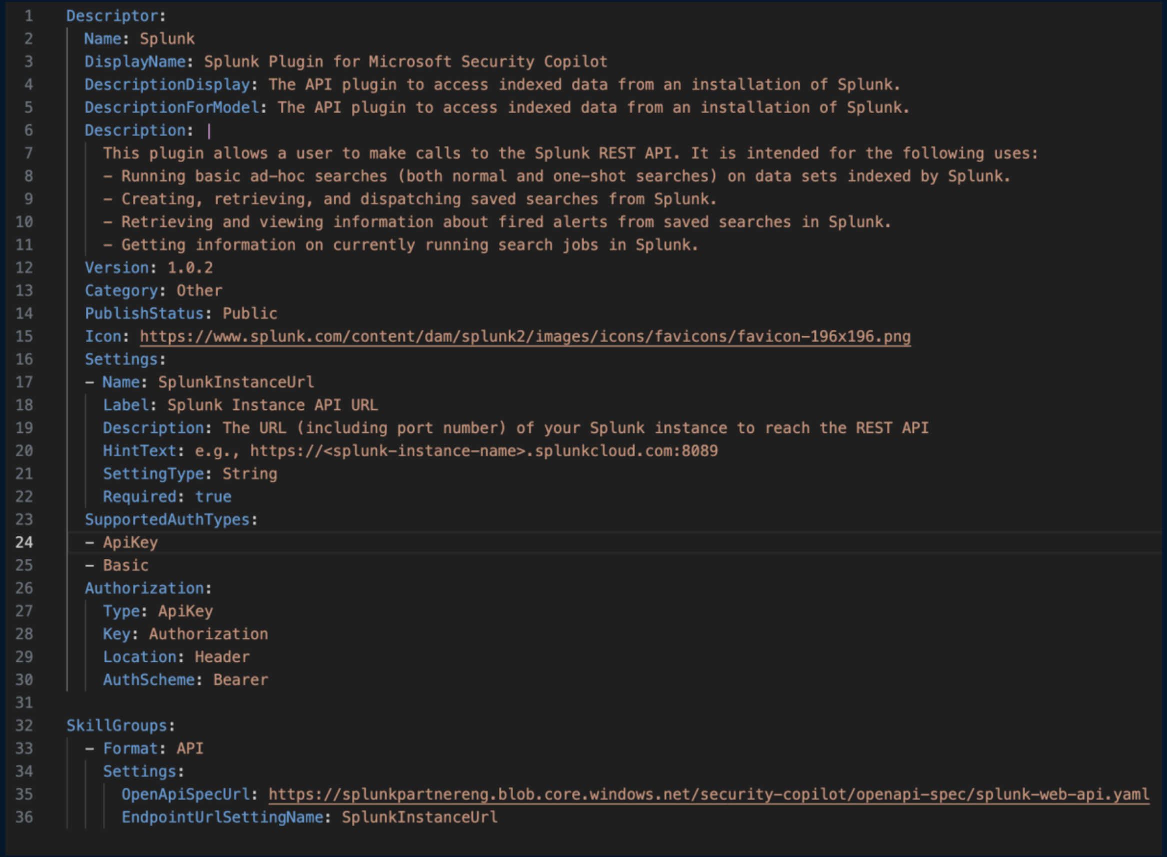
Anatomy of a Plugin: Required Files

pluginVersion.json



```json
{
    "Name": "Splunk",
    "Skills":[
        {
            "Name": "Create a Search Job",
            "Path": "/services/search/v2/jobs"
        },
        {
            "Name": "Get Search Job Results",
            "Path": "/services/search/v2/jobs/{sid}/results"
        },
        {
            "Name": "Get Fired Alerts",
            "Path": "/services/alerts/fired_alerts"
        },
        {
            "Name": "Get Fired Alert Details",
            "Path": "/services/alerts/fired_alerts/{name}"
        },
        {
            "Name": "Get Saved Searches",
            "Path": "/services/saved/searches"
        },
        {
            "Name": "Create Saved Search",
            "Path": "/services/saved/searches"
        },
        {
            "Name": "Dispatch a Saved Search",
            "Path": "/services/saved/searches/{name}/dispatch"
        }
    ],
    "Version" :"1.0.2"
}
```

manifest.yaml



```yaml
Descriptor:
  Name: Splunk
  DisplayName: Splunk Plugin for Microsoft Security Copilot
  DescriptionDisplay: The API plugin to access indexed data from an installation of Splunk.
  DescriptionForModel: The API plugin to access indexed data from an installation of Splunk.
  Description: |
    This plugin allows a user to make calls to the Splunk REST API. It is intended for the following uses:
    - Running basic ad-hoc searches (both normal and one-shot searches) on data sets indexed by Splunk.
    - Creating, retrieving, and dispatching saved searches from Splunk.
    - Retrieving and viewing information about fired alerts from saved searches in Splunk.
    - Getting information on currently running search jobs in Splunk.
  Version: 1.0.2
  Category: Other
  PublishStatus: Public
  Icon: https://www.splunk.com/content/dam/splunk2/images/icons/favicons/favicon-196x196.png
  Settings:
  - Name: SplunkInstanceUrl
    Label: Splunk Instance API URL
    Description: The URL (including port number) of your Splunk instance to reach the REST API
    HintText: e.g., https://<splunk-instance-name>.splunkcloud.com:8089
    SettingType: String
    Required: true
  SupportedAuthTypes:
  - ApiKey
  - Basic
  Authorization:
    Type: ApiKey
    Key: Authorization
    Location: Header
    AuthScheme: Bearer

SkillGroups:
  - Format: API
    Settings:
      OpenApiSpecUrl: https://splunkpartnereng.blob.core.windows.net/security-copilot/openapi-spec/splunk-web-api.yaml
      EndpointUrlSettingName: SplunkInstanceUrl
```

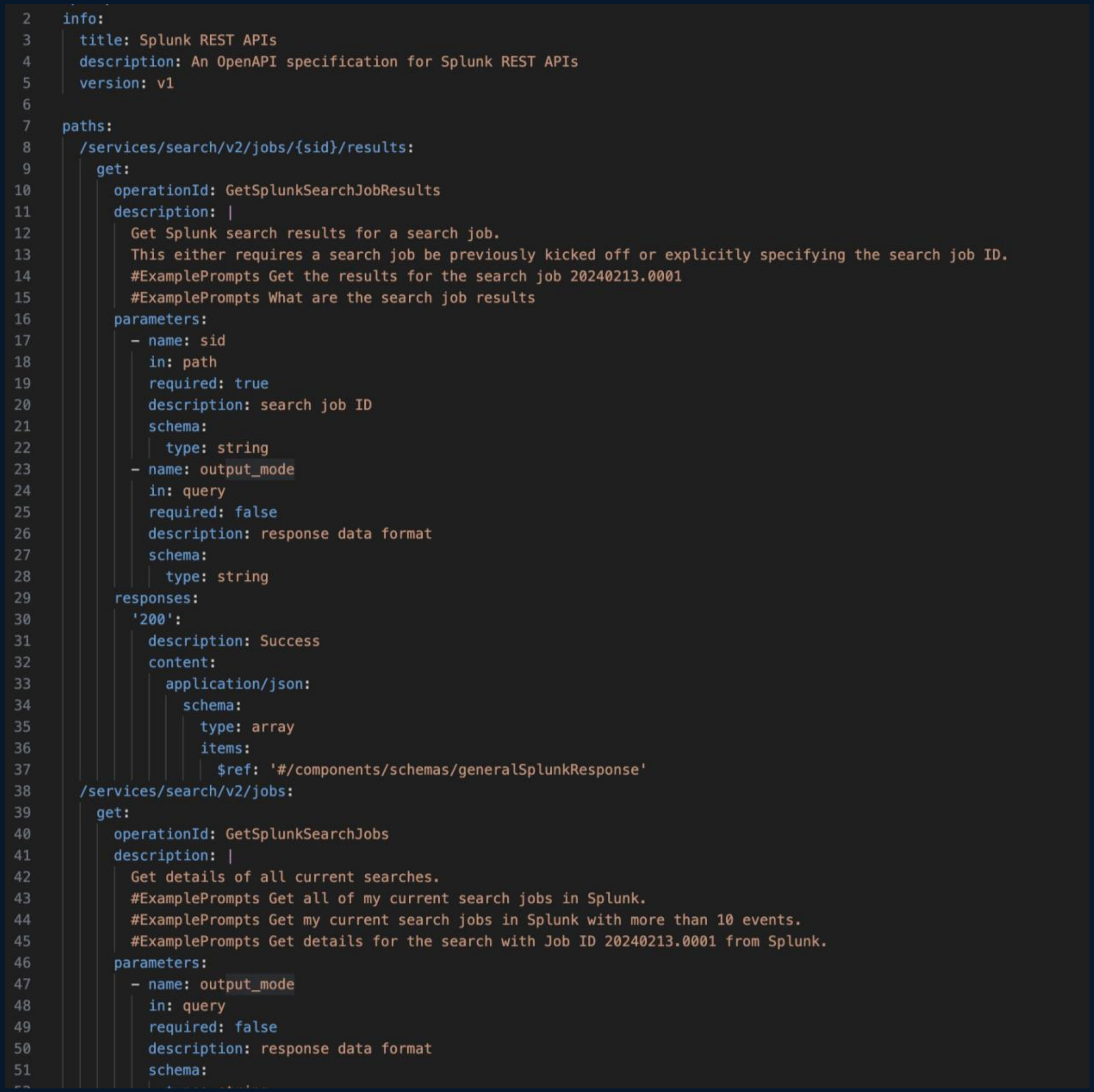
Anatomy of a Plugin: Skill Group Types

Subtitle placeholder

Type	Skill Group Description
KQL	Uses KQL to access specific data stored in Defender / Sentinel / Log Analytics / other Kusto endpoint
API	Interfaces with an API endpoint for data retrieval
GPT	Bases skills on GPT prompt templates – uses GPT 4o model

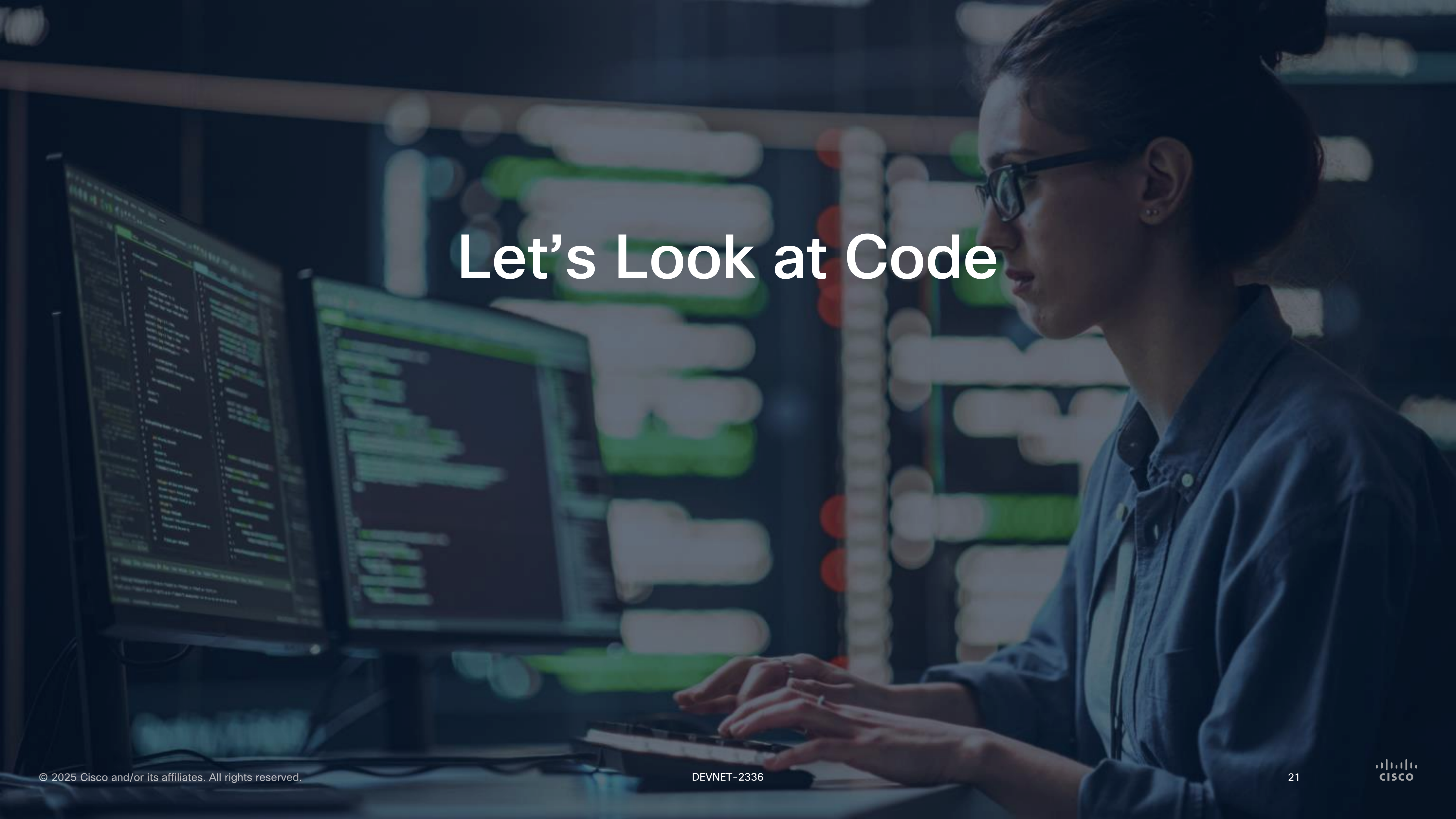
Anatomy of a Plugin: API Plugins

- Based on OpenAPI specification
- Description should also include sample prompts
- #ExamplePrompts



```
info:
  title: Splunk REST APIs
  description: An OpenAPI specification for Splunk REST APIs
  version: v1

paths:
  /services/search/v2/jobs/{sid}/results:
    get:
      operationId: GetSplunkSearchJobResults
      description: |
        Get Splunk search results for a search job.
        This either requires a search job be previously kicked off or explicitly specifying the search job ID.
        #ExamplePrompts Get the results for the search job 20240213.0001
        #ExamplePrompts What are the search job results
      parameters:
        - name: sid
          in: path
          required: true
          description: search job ID
          schema:
            type: string
        - name: output_mode
          in: query
          required: false
          description: response data format
          schema:
            type: string
      responses:
        '200':
          description: Success
          content:
            application/json:
              schema:
                type: array
                items:
                  $ref: '#/components/schemas/generalSplunkResponse'
  /services/search/v2/jobs:
    get:
      operationId: GetSplunkSearchJobs
      description: |
        Get details of all current searches.
        #ExamplePrompts Get all of my current search jobs in Splunk.
        #ExamplePrompts Get my current search jobs in Splunk with more than 10 events.
        #ExamplePrompts Get details for the search with Job ID 20240213.0001 from Splunk.
      parameters:
        - name: output_mode
          in: query
          required: false
          description: response data format
          schema:
```



Let’s Look at Code

Demo

Scan to See a Demo

https://app.vidcast.io/playlists/1a4bda3e-908c-42b9-a75b-7abaf0c8e763

Complete Your Session Evaluations

Complete a minimum of 4 session surveys and the Overall Event Survey to be entered in a drawing to win 1 of 5 full conference passes to Cisco Live 2026.

Earn 100 points per survey completed and compete on the Cisco Live Challenge leaderboard.

Level up and earn exclusive prizes!

Complete your surveys in the Cisco Live mobile app.

Continue your education

Visit the Cisco Showcase for related demos

Book your one-on-one Meet the Engineer meeting

Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs

Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand

Contact me at: waynbrow@cisco.com

Thank you

cisco Live!