[Product name] Hero Scenarios for Security Copilot
January 24, 2024

[Team members]

How to use this template

What is this template for?

When building integrations into Security Copilot, it is important to consider how your plugin (skillset) will interact with the broader set of plugins available in the Security Copilot ecosystem to enable and enrich user scenarios and workflows. The Security Copilot standalone experience is an open narrative interface that creates value by bringing together data and insights from a variety of internal and external sources.

The first step to building new skills is to define the user scenarios that your plugin aims to support and the insights that your plugin will deliver for the user.

The **objectives** of completing this spec are to:

1. Define hero scenarios and user value that your plugin will enable.
2. Specify requirements for high level skill architecture from a user experience perspective.
3. Create alignment with stakeholders, allowing for ways that your plugin can maximize value for users.

Using the template document

This template guides you to follow these steps:

1. Define hero scenarios – what are users trying to achieve?
    a. Promptbooks are some good examples of user scenarios to reference. Promptbooks are a collection of prompts that have been put together to accomplish specific security-related tasks.
2. Understand and explain how your plugin will enable or enrich these hero scenarios.
    a. What insights can your product give users in these scenarios?
    b. How would this appear in a workflow and fit in with the insights and actions enabled by other plugins in Security Copilot?
3. Using your understanding from the above steps, sketch out requirements for high level skill architecture.

a. The goal of this is to do it from the lens of a user in Security Copilot (not from an engineering perspective). Generally, a skill will map to a use case / insight that a user is trying to get; what is the expected input and output for this? When it comes to actual implementation, different actions or API calls may be chained together to facilitate a skill – these details will be defined before implementation.

Create a copy of this document and fill in the following sections with your content. Once completed, remove the entire "How to use this template" section.

Overview

[Provide an overview of what your integration to Security Copilot is and what value you are bringing to users.]

Scenarios

Scenario 1: [scenario name]

User role	[Who is the user in this scenario?]
User story	[What is the situation and what is the user trying to achieve?]
Current practice	[What are users currently doing to achieve this? What are pain points in this process?]
Decomposition *[Stage]*	[Break down the scenario into the different stages using one row per stage – examples of stages are triage, enrich, reverse engineer, assess impact, get recommendations, manage posture, report. Within each stage, list out the user actions] [For each action, fill out: Prompt: [user prompt] Skillset/skill: [the skillset / skill that should be selected] Response: [expected contents of Copilot response]
Decomposition *[Stage]*	" "
Value from [your product name]	[What user value does your integration provide in this scenario?]
RAI harms/risks	[What are possible RAI harms/risks that your integration may have? Review Microsoft Responsible AI guidelines]

Example scenario: Investigate Defender incident

User role	SOC analyst
User story	Import a security incident from Defender, augment with data from key Microsoft systems, and enrich IOCs with threat intelligence.
Current practice	[What are users currently doing to achieve this? What are pain points in this process?]
Decomposition *Enrich*	**1. Load in incident context** Prompt: "Summarize Defender incident XXX" Skill/skillset: GetIncident (Fusion/Defender) Response: summary containing: • Severity • No. alerts • Incident date and time • Users and apps/devices involved • IP addresses **2. Get supporting info on entities involved** Prompt: "Tell me about the entities associated with that incident." Skill/Skillset: GetIncidentEntities (Fusion) Response: details of users (name, UPN), apps, IP addresses
Decomposition *Assess impact*	**3. Get reputation of IP addresses involved** Prompt: "What are the reputation scores for the IPv4 addresses on that incident?" Skill/skillset: GetReputationsByIpAddresses (ThreatIntelligence.DTI) Response: list of IPv4 addresses, their reputation scores and assessment of reputation **4. Get authentication information for users involved** Prompt: "Show the authentication methods set up for each user involved in that incident. Especially indicate whether they have MFA enabled." Skill/skillset: GetEntraUserDetails (Entra) Response: list of auth methods with details such as auth method ID, created date time, device type **5. Get compliance status of potential user devices involved in incident** Prompt: "If a user is listed in the incident details, show which devices they have used recently and indicate whether they are compliant with policies."

	Skillset/skill: GetIntuneDevices (Intune) Response: device info and compliance policies and compliance statuses **6. Check if user device is up to date** Prompt: "If any devices are listed in the previous output, show details from Intune on the one that checked in most recently. Especially indicate if it is current on all operating system updates." Skill/skillset: GetIntuneDevices (Intune) Response: device details, OS version and whether the device is up to date
Decomposition *Report*	**7. Write a report on findings** Prompt: "Write an executive report summarizing this investigation. It should be suited for a non-technical audience." Skill/skillset: SummarizeText (Generic) Response: brief report summary with key info from each preceding prompt and response, and assessment of incident.
Value from Intune	*(The example is assuming Intune is the author of this doc)*
RAI harms/risks	[What are possible RAI harms/risks that your integration may have?]

High level skill architecture

1. [skill name]

Description	[Explain what the skill does]
Scenarios	[List the scenarios that this skill contributes to]
Example prompts	[List some example prompts that this skill would support]
Required inputs	[List required inputs for the skill, if any]
Optional inputs	[List optional inputs for the skill, if any]
Data + source	[What data is needed for the skill and where is the data located?]
Expected output + skill behavior	[Describe expected contents of output + skill behavior. Also consider edge cases, exception/error behaviors, and how responses should be formatted for an ideal user experience.]

Value	[What are the insights and value that users get from the response from this skill?]

2. [skill name]

Description	[Explain what the skill does]
Scenarios	[List the scenarios that this skill contributes to]
Example prompts	[List some example prompts that this skill would support]
Required inputs	[List required inputs for the skill, if any]
Optional inputs	[List optional inputs for the skill, if any]
Data + source	[What data is needed for the skill and where is the data located?]
Expected output + skill behavior	[Describe expected contents of output + skill behavior. Also consider edge cases, exception/error behaviors, and how responses should be formatted for an ideal user experience.]
Value	[What are the insights and value that users get from the response from this skill?]