

# Introduction to Splunk SOAR

# Course Objectives

- Define Security Orchestration, Automation and Response
- Identify good use cases for Splunk SOAR
- Describe Splunk SOAR capabilities

# Course Outline

- Topic 1: What is SOAR?
- Topic 2: How Splunk SOAR works

# What is SOAR?

0010  
01010  
0101



# Topic Objectives

- List orchestration goals
- List automation goals
- List Response goals

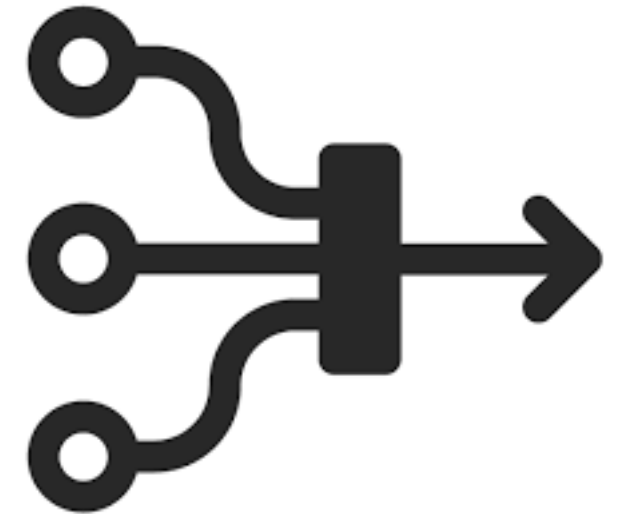
# Security Orchestration, Automation and Response

- The intent of SOAR is to make it as easy and fast as possible to detect and respond to security incidents
- SOAR provides tools for both manual and automated investigation and actions
- SOAR also incorporates tools to:
  - Respond in an organized and collaborative approach
  - Compile records of all stages of the response



# Initial Detection

- SOAR monitors networked environments for:
  - Security incidents (breaches, unauthorized access, malicious activity)
  - Vulnerabilities that could make security incidents more likely
- The monitored data can come from virtually any data source
- Typically, SOAR ingests data from a Splunk search head or Splunk Enterprise Security server



# Events

- Data ingested into SOAR is stored in a database and displayed as **events**
- The event contains information about the incident, like the date, time, objects and attributes that can help us understand what is happening
  - Example: At `10:15:20 AM` today, an unexpected process named "deepworm" began executing on server TCH1200-1, with hash ID 23ED3DAAHDE39D290
- Events also store descriptive information like status, owner, severity, comments, notes, and a record of all activities while the event is processed





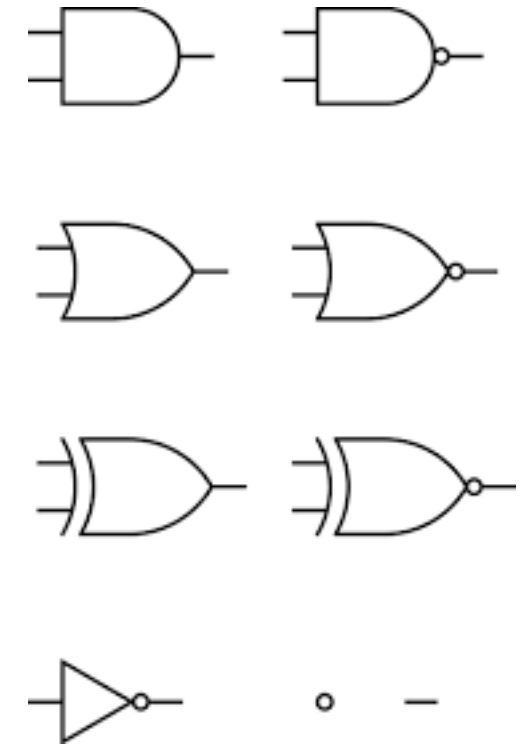
# Understanding What's Happening

- We can analyze the event information to plan a response
  - What servers or end-points are affected
  - What is the threat
  - Where did the threat come from
  - How serious is it
- All the information needs to be recorded
- Often many teams and systems are involved
- Time is always critical



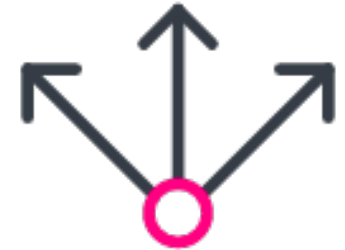
# Making Decisions

- We use the results of the analysis to make response decisions
- Decisions must be timely and based on good data
  - Some incidents are false positives
  - Others are real, but well understood, with known responses
  - Some might be new, or very complex, needing additional steps and analysis
- SOAR provides decision making via:
  - Human input
  - Automated scripts called **playbooks**



# Taking Action

- Decisions lead to actions:
  - Kill processes
  - Isolate servers
  - Disable user accounts
  - Delete files
  - Update event record and status
- Everything we learn and do must be recorded to improve our security posture



# Summary: Goals of SOAR

- Remember: **S**ecurity **O**rchestration, **A**utomation and **R**esponse
- Orchestration
  - Provide collaborative and open tools to work together on incidents
- Automation
  - Automate as much of the analysis, decision, and action steps as possible for rapid execution
- Response
  - Enable access to all available response tools via manual or automated methods

# Quiz 1

- Need help here, not sure how to create quiz

# How Splunk SOAR Works

0010  
01010  
0101

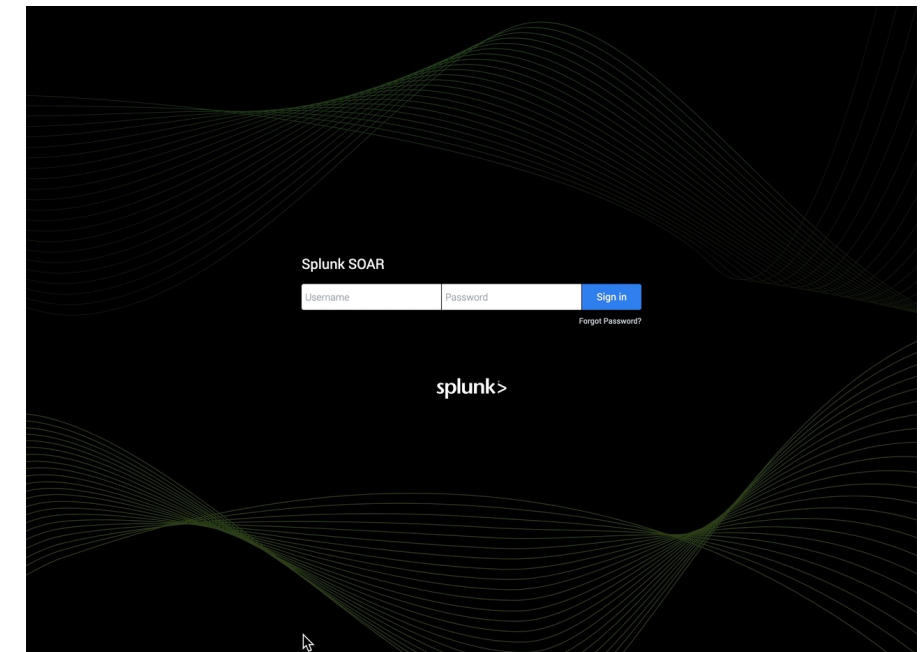


# Topic Objectives

- Define common Splunk SOAR objects
- Describe the SOAR event life cycle
- Identify manual, coordinated and automated response options

# SOAR User Interface

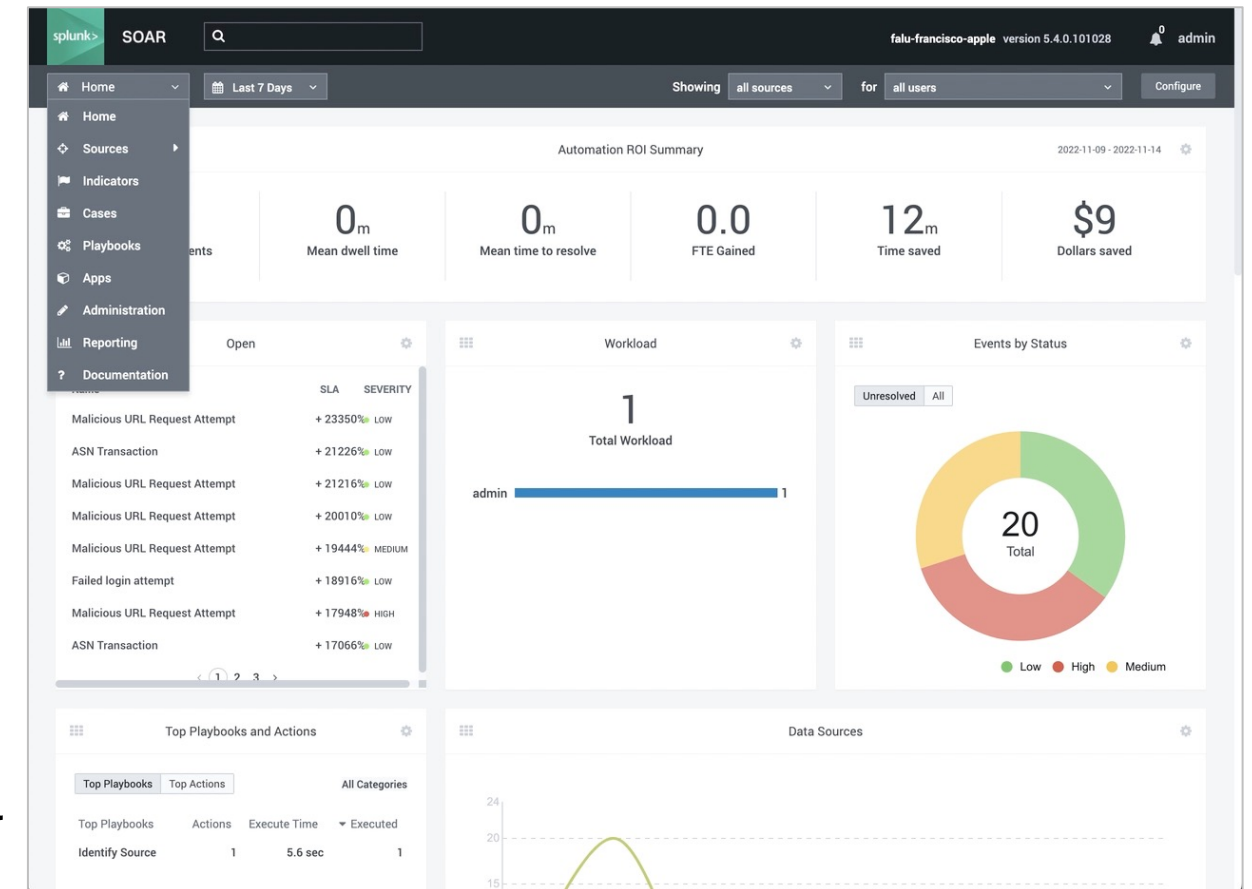
- SOAR is a web appliance
  - Cloud based or installed on premises
- A user name and password are required
  - Can be integrated with your enterprise authentication system
- After log on you'll see the **ROI Summary** and main menu
  - ROI summary is a dashboard showing current status of events in SOAR





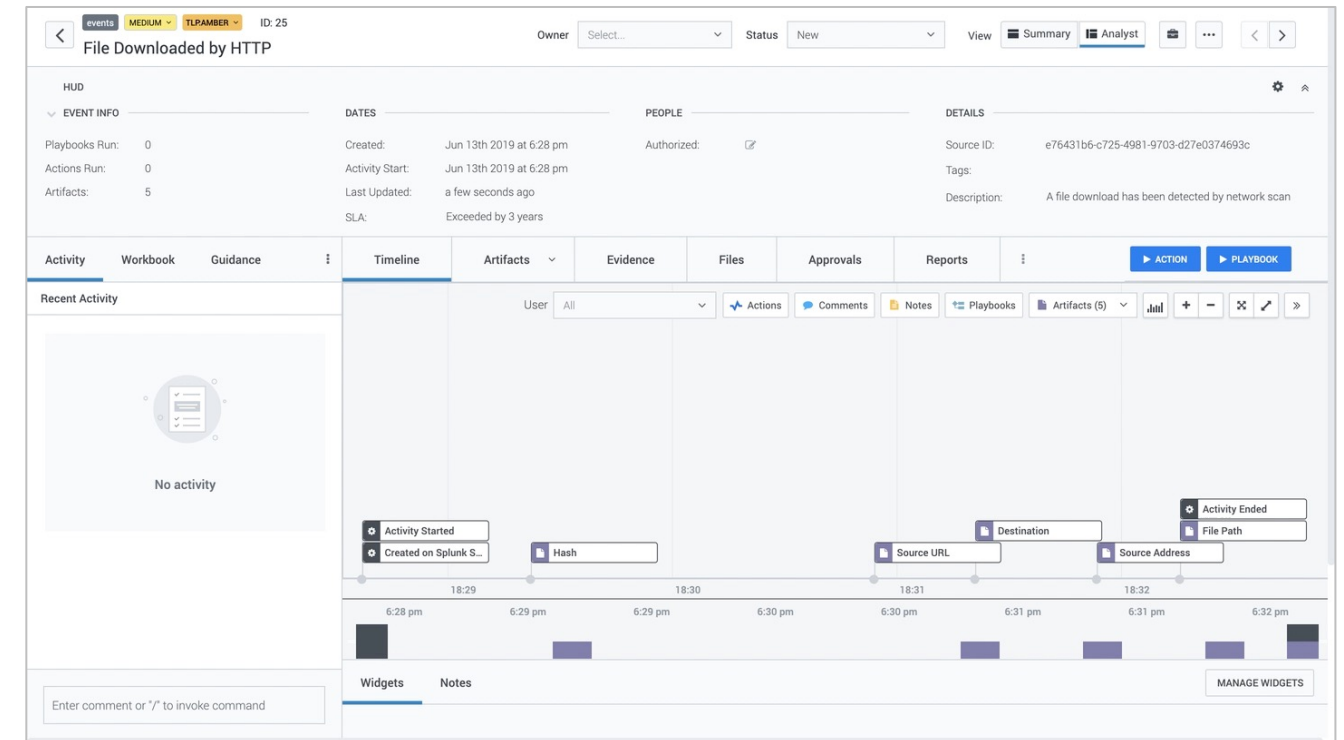
# Events in Splunk SOAR

- Data ingested into SOAR are displayed as events
- The events often come from Splunk Enterprise Security
  - Example: a virus has been detected
- Each event represents an incident or vulnerability
- The event will contain any relevant data sent by Splunk
  - Example: the infected host ID, how the virus was detected (files, processes, source addresses, etc.)



# Event Life Cycle



- Events go through status changes as they are processed
- **New**
  - The event has just been created
- **Open**
  - The event is being actively processed
- **Closed**
  - the incident has been resolved
- All artifact and action results, along with comments, notes, files, etc., are preserved in the event for later study







# Artifacts

- The event data is stored in **Artifacts**
- Each artifact contains one or more name/value pairs
- Artifact data provides the input for SOAR to work on to analyze the incident, make decisions, and take action to eliminate the threat

ARTIFACTS (5) Q

	ID	LABEL	NAME	SEVERITY	CREATED BY	TAGS
	32	path	File Path	MEDIUM	admin	
<div><div></div><div><div>Name</div><div>File Path</div><div>Start Time</div><div>Jun 13th 2019 at 6:32 pm</div></div><div><div>Label</div><div>path</div><div>Created</div><div>Jun 13th 2019 at 6:32 pm</div></div><div><div>Created by</div><div>admin</div><div>Type</div><div>N/A</div></div><div><div>Source ID</div><div>fc740748-179c-4221-bb47-9abb6d5d6e6</div><div>Severity</div><div>Medium</div></div></div>						
<div>Details</div>						
<div><div>filePath</div><div>/home/user/results</div></div>						

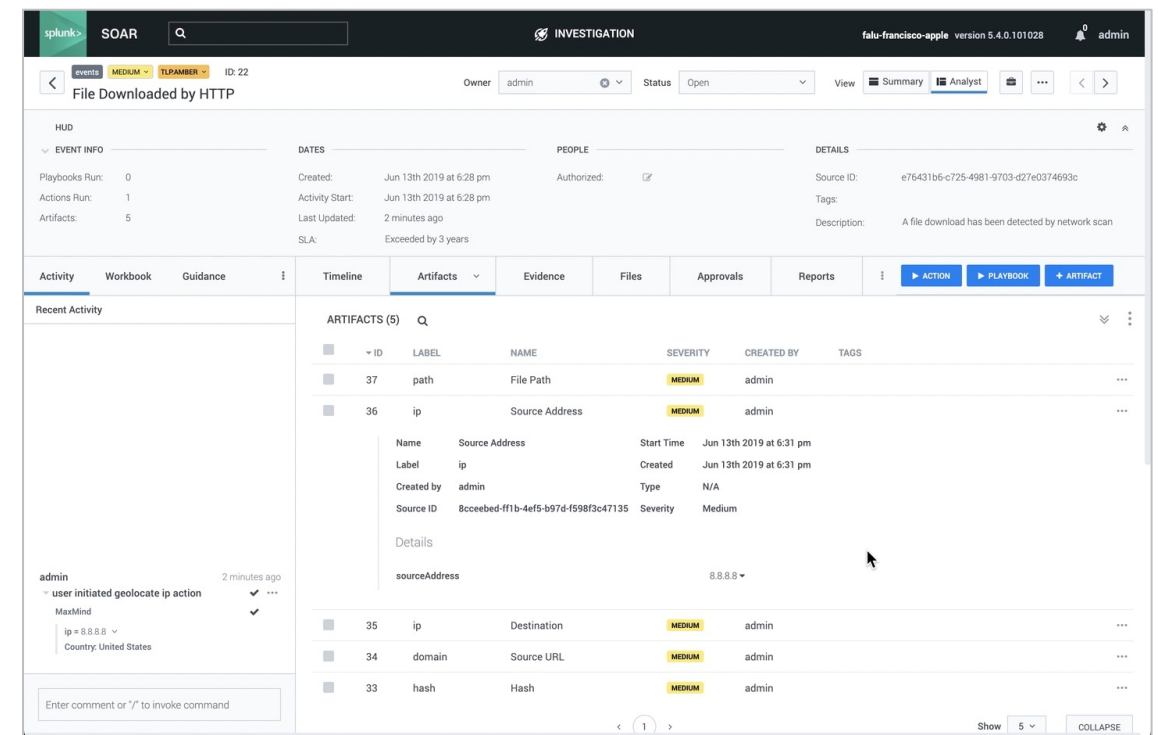
	31	ip	Source Address	MEDIUM	admin
	30	ip	Destination	MEDIUM	admin
	29	domain	Source URL	MEDIUM	admin
	28	hash	Hash	MEDIUM	admin

# Actions

- An **action** is an operation SOAR can conduct based on an event's artifact data
- Actions can gather more information
  - For instance: find out if a virus type is known, or if the source of the infection is known, or even test run (detonate) a virus sample in a safe environment
  - All action results are stored in the event and can be used for further analysis and decision making
- Actions can also make changes in the environment
  - For instance, kill processes started by the suspect virus file, and isolate the server
- Actions can be executed manually or automatically

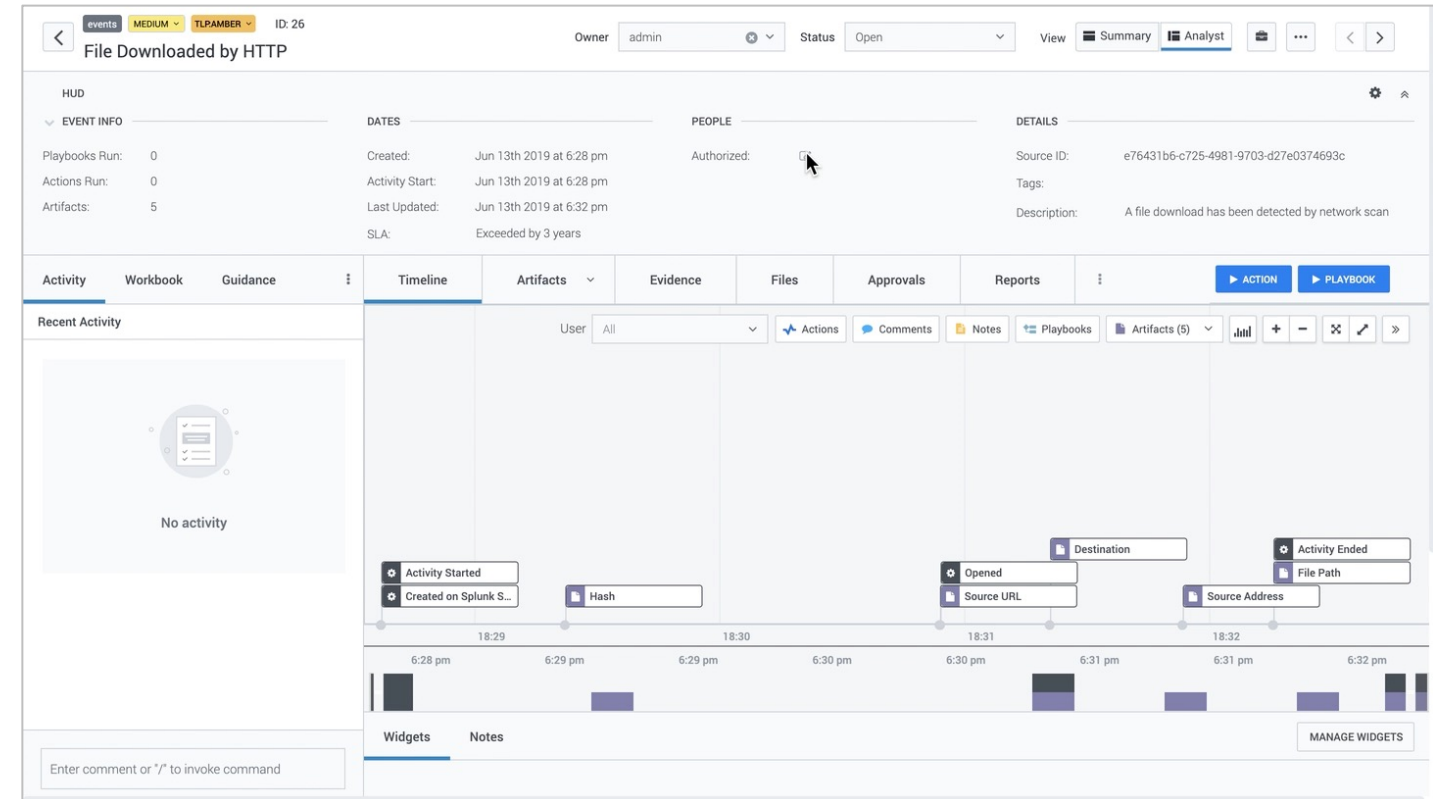
# Running Actions Manually

- Actions can be executed manually or automatically
- To run an action manually, click the artifact value, and select the action desired
- The choice of available actions will depend on the context, or type of data, and the action libraries (called **apps**) which have been configured for your server



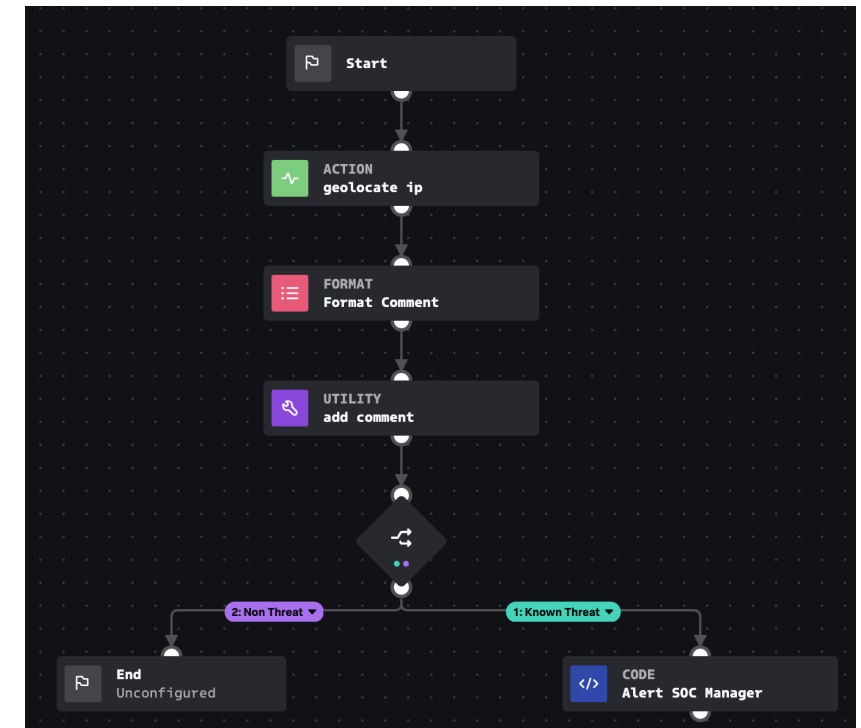
# Playbooks

- A **playbook** is a script that can:
  - Use event artifacts as input
  - Run actions to gather information
  - Use artifacts and action results to make decisions
  - Use actions to correct or contain the incident
- Playbooks can be run manually, or automatically when:
  - An event's artifact data is first ingested
  - Later, if new artifacts are added



# Visual Playbook Editor

- The VPE allows non-coding security professionals to build sophisticated automated responses
- In this example a simple playbook uses a **geolocate** action to identify the source country, formats the output from the action into human readable text, adds that as a comment to the event, and uses the decision block to check known threat records to decide if the SOC management team should be alerted



# VPE in Action

