© 2025 SPLUNK LLC

Practical SOAR Examples from the Field: Part 2

SEC1372

Richard Hampshire
Matthew Bennett

© 2025 SPLUNK LLC

Forward-looking statements

This presentation may contain forward-looking statements regarding future events, plans or the expected financial performance of our company, including our expectations regarding our products, technology, strategy, customers, markets, acquisitions and investments. These statements reflect management's current expectations, estimates and assumptions based on the information currently available to us. These forward-looking statements are not guarantees of future performance and involve significant risks, uncertainties and other factors that may cause our actual results, performance or achievements to be materially different from results, performance or achievements expressed or implied by the forward-looking statements contained in this presentation.

For additional information about factors that could cause actual results to differ materially from those described in the forward-looking statements made in this presentation, please refer to our periodic reports and other filings with the SEC, including the risk factors identified in our most recent quarterly reports on Form 10-Q and annual reports on Form 10-K, copies of which may be obtained by visiting the Splunk Investor Relations website at www.investors.splunk.com or the SEC's website at www.sec.gov. The forward-looking statements made in this presentation are made as of the time and date of this presentation. If reviewed after the initial presentation, even if made available by us, on our website or otherwise, it may not contain current or accurate information. We disclaim any obligation to update or revise any forward-looking statement based on new information, future events or otherwise, except as required by applicable law.

In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not be incorporated into any contract or other commitment. We undertake no obligation either to develop the features or functionalities described, in beta or in preview (used interchangeably), or to include any such feature or functionality in a future release.

Splunk, Splunk> and Turn Data Into Doing are trademarks and registered trademarks of Splunk Inc. in the United States and other countries. All other brand names, product names or trademarks belong to their respective owners.
© 2025 Splunk LLC. All rights reserved.

splunk> .conf25

Overview

Session Breakdown and Goals

Breakdown

- Introductions
- SOAR Intro and Refresher
- Cases Studies
- Additional Tips
- Wrap Up / Questions

Goals

- Inspire you to confidently handle automation
- Show you more real-world playbooks from the field
- Leave you with more ideas, tips and tricks on creating your own playbooks

© 2025 SPLUNK LLC

Introductions

© 2025 SPLUNK LLC

Richard Hampshire

Security Architect - Professional Services
Splunk

rich@splunk.com

.conf25
splunk>

© 2025 SPLUNK LLC

Matt Bennett

Co-Founder / Core Consultant
Hyperion3
matt@hyperion3.com.au

© 2025 SPLUNK LLC

SOAR Intro / Refresher

© 2025 SPLUNK LLC

Recap

SEC1579B - .conf24

Last year we covered:

- Best practice SOAR playbook implementation
- Playbook case studies from the field
- Bonus tips
- … and more

https://tinyurl.com/4r7afb9r

© 2025 SPLUNK LLC

Recap

SOAR Implementation Methodology

.conf24 SEC1579B

https://tinyurl.com/4r7afb9r

© 2025 SPLUNK LLC

Recap

SOAR Integration - Where do the analysts work?

Many options, with no right or wrong way

Splunk SOAR

Splunk ES

3rd Party

Mission Control

.conf24 SEC1579B
https://tinyurl.com/4r7afb9r

© 2025 SPLUNK LLC

Playbook Design Principles

© 2025 SPLUNK LLC

Design Principles

What we've discovered

- Detailed / Low Level Designs used for traditional Splunk deployments do no work for SOAR
  - Automation is complex area and legacy design principals do not translate across
- Effort is better spent prototyping the solution and iterating / adjusting on the fly
  - Automation aligns better with a DevOps / CICD approach
- A high level design can still be used to set goals and establish guardrails
  - Provides the 'commander's intent'
- It's impossible to gather all requirements and permutations of the automation flow up front
  - Often the customer cannot provide this until they've seen the solution in action

© 2025 SPLUNK LLC

Typical Legacy Approach

What's supposed to happen:

- Requirements are gathered and a design is created
- Customer reviews and if satisfied the design is approved and all playbook components are 'locked in'
- Playbook is developed in-line with the design
- Solution presented to customer, is tested, and signed off

© 2025 SPLUNK LLC

Typical Legacy Approach

What usually actually happens..

- Process proceeds up until playbook development stats, during which:
  - Environment specifics are discovered that conflict with the design
  - New questions are raised that could not have been predicted previously
  - Additional requirements are raised from the customer

- Re-design is required, more time is needed, and often deadlock occurs

- And most importantly, more time is spent on the design than developing the playbook itself.

© 2025 SPLUNK LLC

Best Practice Approach

How we've changed the approach

- Enhanced focus on discovery to draw out requirements, assumptions, and potential blockers
- High level design captures the general flow and overall intent - not every individual block / function
- Playbook developer then has freedom to innovate and develop the solution as long as it still reasonably meets the intent from the high level design.
- True up activity at the end uplifts documentation to reflect what was actually built

© 2025 SPLUNK LLC

Case Study: Agent Management Playbook Design

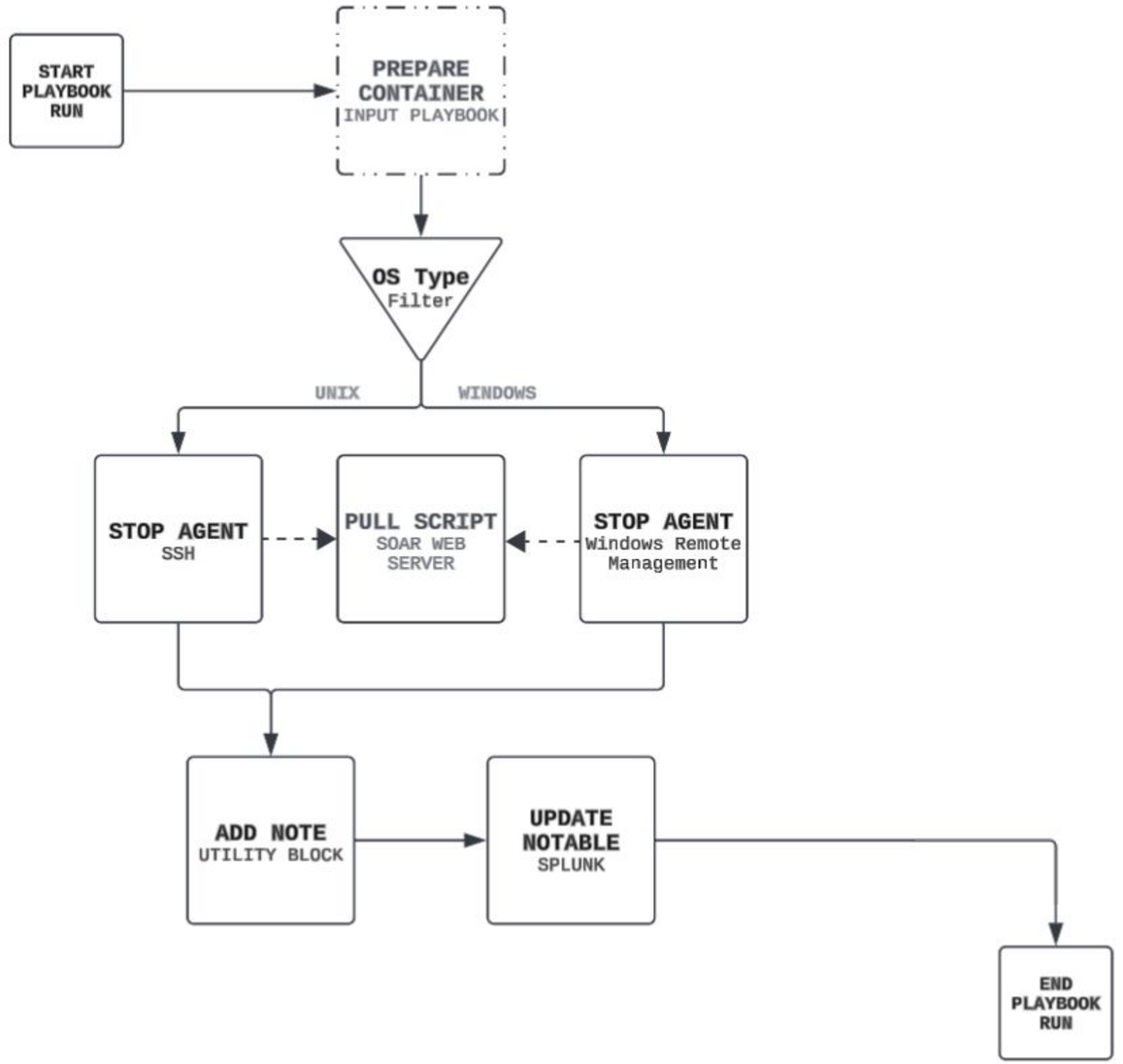
© 2025 SPLUNK LLC

Initial Design

Simple high level flow to determine the OS, stop the agent, add a note, and update the notable.

What more could you possibly need?

Required Apps:
SSH
Windows Remote Management
Splunk

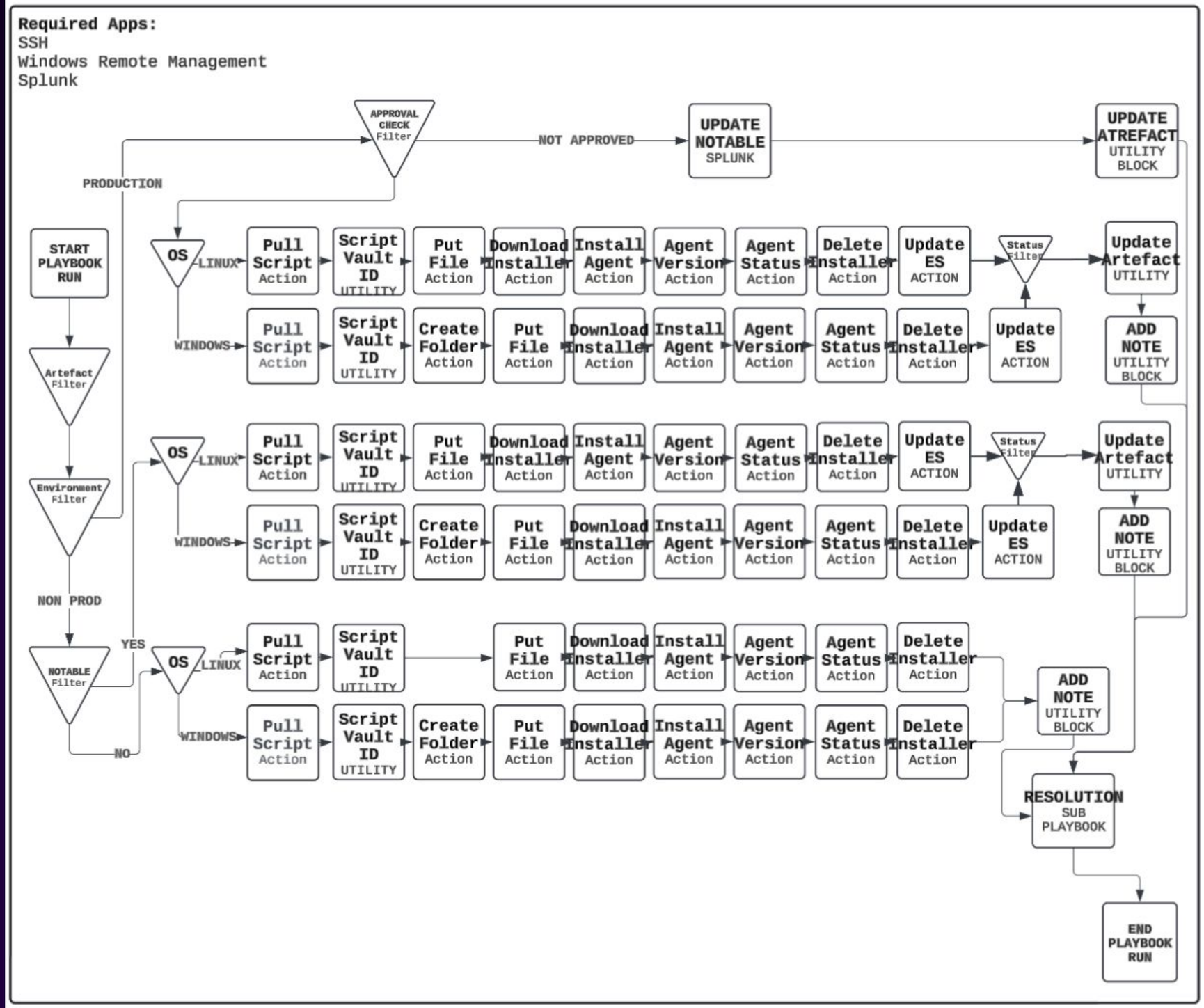


© 2025 SPLUNK LLC

Final Design

Well…

Same playbook,
Same requirements,
Just a higher level of detail unearthed once development commenced.



© 2025 SPLUNK LLC

Design Principles

Key Takeaways

- Legacy approach had been underway for over 24 months and completely stalled
  - Our new approach had customer design sign-off in < 1 week
- Employ high level design to capture the intent and establish automation goals / guardrails
- Low level / detailed designs are not practical to create in advance
  - Especially for complex automation - more time will be spent on design than build
- Perform a ‘true-up’ once the solution has been completed
  - Documentation as code will save time here

© 2025 SPLUNK LLC

Playbook Case Studies

© 2025 SPLUNK LLC

Custom ES Automation Workflow

© 2025 SPLUNK LLC

Custom ES Automation Workflow

Using ES notable status changes to trigger automation

What and why?

- Requirement to selectively initiate automation under heavy constraints
  - Automation must be triggered by a user
  - User must be able to select some container and omit others
  - Automation ‘requests’ must be reviewed and approved before execution
  - Solution must provide different workflows for PROD and NON-PROD systems
    - PROD runs as per the above
    - NON-PROD hosts follow a different flow

© 2025 SPLUNK LLC

Custom ES Automation Workflow

Using ES notable status changes to trigger automation

How?

- Correlation search creating notable events
- Custom notable statuses configured in ES
- Additional scheduled search monitoring for status change
- Send to SOAR adaptive response action

© 2025 SPLUNK LLC

Analyst queue Search findings & investigations All time

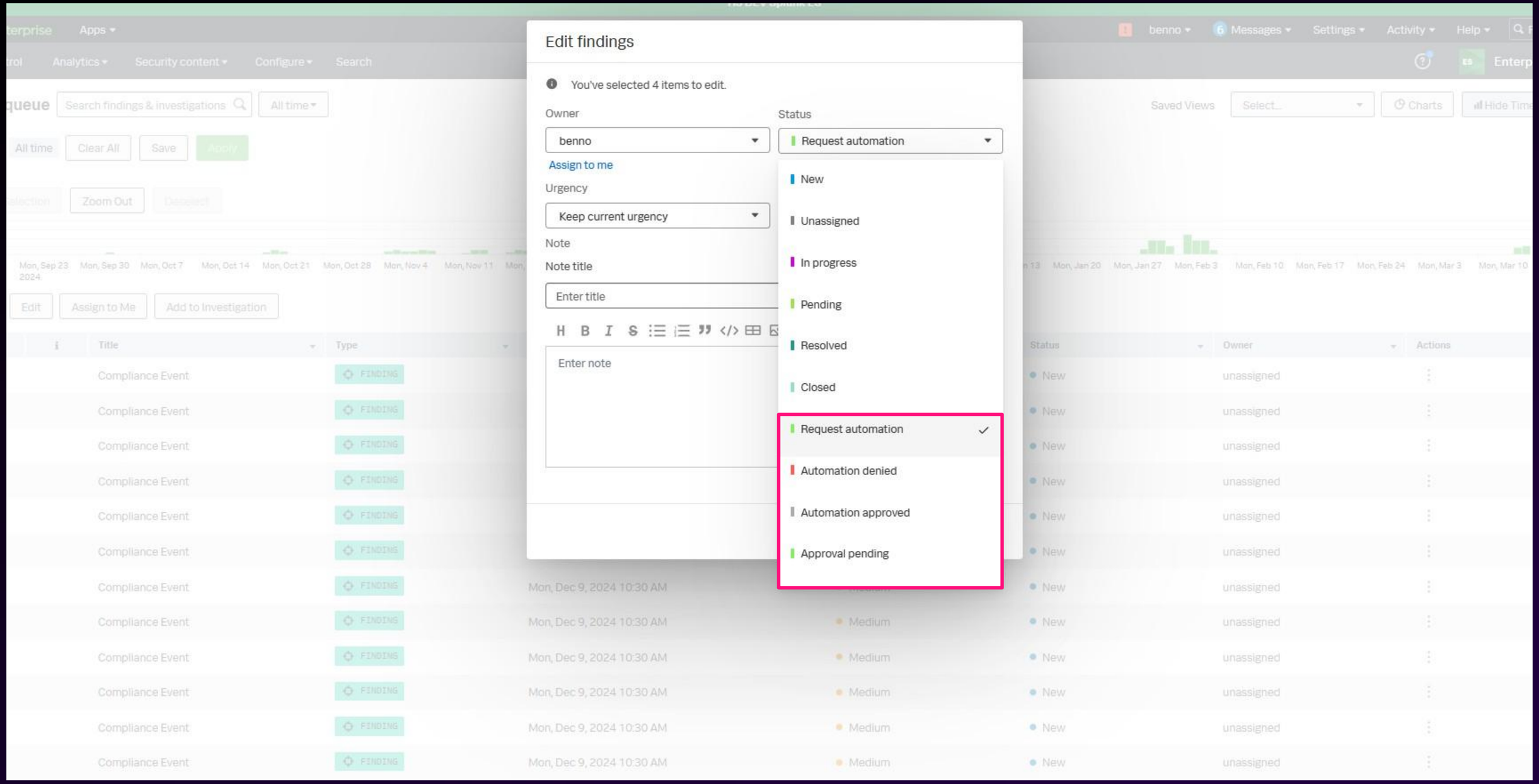
Time Range: All time | Clear All | Save | Apply

Zoom To Selection | Zoom Out | Deselect

4 selected | Edit | Assign to Me | Add to Investigation

	Title	Type	Status	Owner	Risk Object	Risk Score	Time	Disposition
☑	Compliance Event	FINDING	New	unassigned	HYP3SVR655	1	Tue, 18 Mar 2025 10:50	Undetermined
☑	Compliance Event	FINDING	New	unassigned	HYP3SVR542	1	Tue, 18 Mar 2025 10:50	Undetermined
☑	Compliance Event	FINDING	New	unassigned	HYP3SVR204	1	Tue, 18 Mar 2025 10:45	Undetermined
☑	Compliance Event	FINDING	New	unassigned	HYP3SVR193	1	Tue, 18 Mar 2025 10:45	Undetermined
☐	Compliance Event	FINDING	New	unassigned	HYP3SVR687	1	Tue, 18 Mar 2025 10:40	Undetermined
☐	Compliance Event	FINDING	New	unassigned	HYP3SVR609	1	Tue, 18 Mar 2025 10:40	Undetermined
☐	Compliance Event	FINDING	New	unassigned	HYP3SVR400	1	Tue, 18 Mar 2025 10:35	Undetermined
☐	Compliance Event	FINDING	New	unassigned	HYP3SVR627	1	Tue, 18 Mar 2025 10:30	Undetermined
☐	Compliance Event	FINDING	New	unassigned	HYP3SVR16	1	Tue, 18 Mar 2025 10:30	Undetermined
☐	Compliance Event	FINDING	New	unassigned	HYP3SVR17	1	Tue, 18 Mar 2025 10:25	Undetermined
☐	Compliance Event	FINDING	New	unassigned	HYP3SVR638	1	Tue, 18 Mar 2025 10:25	Undetermined
☐	Compliance Event	FINDING	New	unassigned	HYP3SVR727	1	Tue, 18 Mar 2025 10:25	Undetermined
☐	Compliance Event	FINDING	New	unassigned	HYP3SVR161	1	Tue, 18 Mar 2025 10:20	Undetermined
☐	Compliance Event	FINDING	New	unassigned	HYP3SVR171	1	Tue, 18 Mar 2025 10:20	Undetermined
☐	Compliance Event	FINDING	New	unassigned	HYP3SVR602	1	Tue, 18 Mar 2025 10:20	Undetermined
☐	Compliance Event	FINDING	New	unassigned	HYP3SVR979	1	Tue, 18 Mar 2025 10:10	Undetermined
☐	Compliance Event	FINDING	New	unassigned	HYP3SVR445	1	Tue, 18 Mar 2025 10:10	Undetermined
☐	Compliance Event	FINDING	New	unassigned	HYP3SVR592	1	Tue, 18 Mar 2025 10:10	Undetermined
☐	Compliance Event	FINDING	New	unassigned	HYP3SVR91	1	Tue, 18 Mar 2025 10:05	Undetermined

© 2025 SPLUNK LLC



© 2025 SPLUNK LLC

Automatically detecting the status change

Required SPL

```
`notable`
| search status_label="Request Automation"
| eval rule_name=if(isnull(rule_name),source,rule_name)
| eval rule_title=if(isnull(rule_title),rule_name,rule_title)
| eval rule_description=if(isnull(rule_description),source,rule_description)
| eval security_domain=if(isnull(security_domain),source,security_domain)
| stats values(urgency) as urgency, values(status_label) as status_label,
values(status_description) as status_description, values(event_hash) as event_hash,
values(event_id) as event_id, values(orig_raw) as orig_raw, values(rule_name) as rule_name,
values(rule_id) as rule_id, values(status_logger) as status_logger count by owner
| table *
```

© 2025 SPLUNK LLC

Automatically detecting the status change

Required SPL

```
`notable`
| search status_label="Request Automation"
| eval rule_name=if(isnull(rule_name),source,rule_name)
| eval rule_title=if(isnull(rule_title),rule_name,rule_title)
| eval rule_description=if(isnull(rule_description),source,rule_description)
| eval security_domain=if(isnull(security_domain),source,security_domain)
| stats values(urgency) as urgency, values(status_label) as status_label,
values(status_description) as status_description, values(event_hash) as event_hash,
values(event_id) as event_id, values(orig_raw) as orig_raw, values(rule_name) as rule_name,
values(rule_id) as rule_id, values(status_logger) as status_logger count by owner
| table *
```

Native macro to return all notable events within the time window searched

© 2025 SPLUNK LLC

Automatically detecting the status change

Required SPL

```
`notable`
| search status_label="Request Automation"
| eval rule_name=if(isnull(rule_name),source,rule_name)
| eval rule_title=if(isnull(rule_title),rule_name,rule_title)
| eval rule_description=if(isnull(rule_description),source,rule_description)
| eval security_domain=if(isnull(security_domain),source,security_domain)
| stats values(urgency) as urgency, values(status_label) as status_label,
values(status_description) as status_description, values(event_hash) as event_hash,
values(event_id) as event_id, values(orig_raw) as orig_raw, values(rule_name) as rule_name,
values(rule_id) as rule_id, values(status_logger) as status_logger count by owner
| table *
```

Filtering on the custom status created to return all notables pending approval

© 2025 SPLUNK LLC

Automatically detecting the status change

Required SPL

```
`notable`
| search status_label="Request Automation"
| eval rule_name=if(isnull(rule_name),source,rule_name)
| eval rule_title=if(isnull(rule_title),rule_name,rule_title)
| eval rule_description=if(isnull(rule_description),source,rule_description)
| eval security_domain=if(isnull(security_domain),source,security_domain)
| stats values(urgency) as urgency, values(status_label) as status_label,
values(status_description) as status_description, values(event_hash) as event_hash,
values(event_id) as event_id, values(orig_raw) as orig_raw, values(rule_name) as rule_name,
values(rule_id) as rule_id, values(status_logger) as status_logger count by owner
| table *
```

Eval functions to set required fields for downstream automation

© 2025 SPLUNK LLC

Automatically detecting the status change

Required SPL

```
`notable`
| search status_label="Request Automation"
| eval rule_name=if(isnull(rule_name),source,rule_name)
| eval rule_title=if(isnull(rule_title),rule_name,rule_title)
| eval rule_description=if(isnull(rule_description),source,rule_description)
| eval security_domain=if(isnull(security_domain),source,security_domain)
| stats values(urgency) as urgency, values(status_label) as status_label,
values(status_description) as status_description, values(event_hash) as event_hash,
values(event_id) as event_id, values(orig_raw) as orig_raw, values(rule_name) as rule_name,
values(rule_id) as rule_id, values(status_logger) as status_logger count by owner
| table *
```

Stats command to group notables by owner to support bulk approval request

© 2025 SPLUNK LLC

Automatically detecting the status change
Implementing the SPL

- Correlation Search scheduled to run every 5 minutes (`*/5 * * * *`)

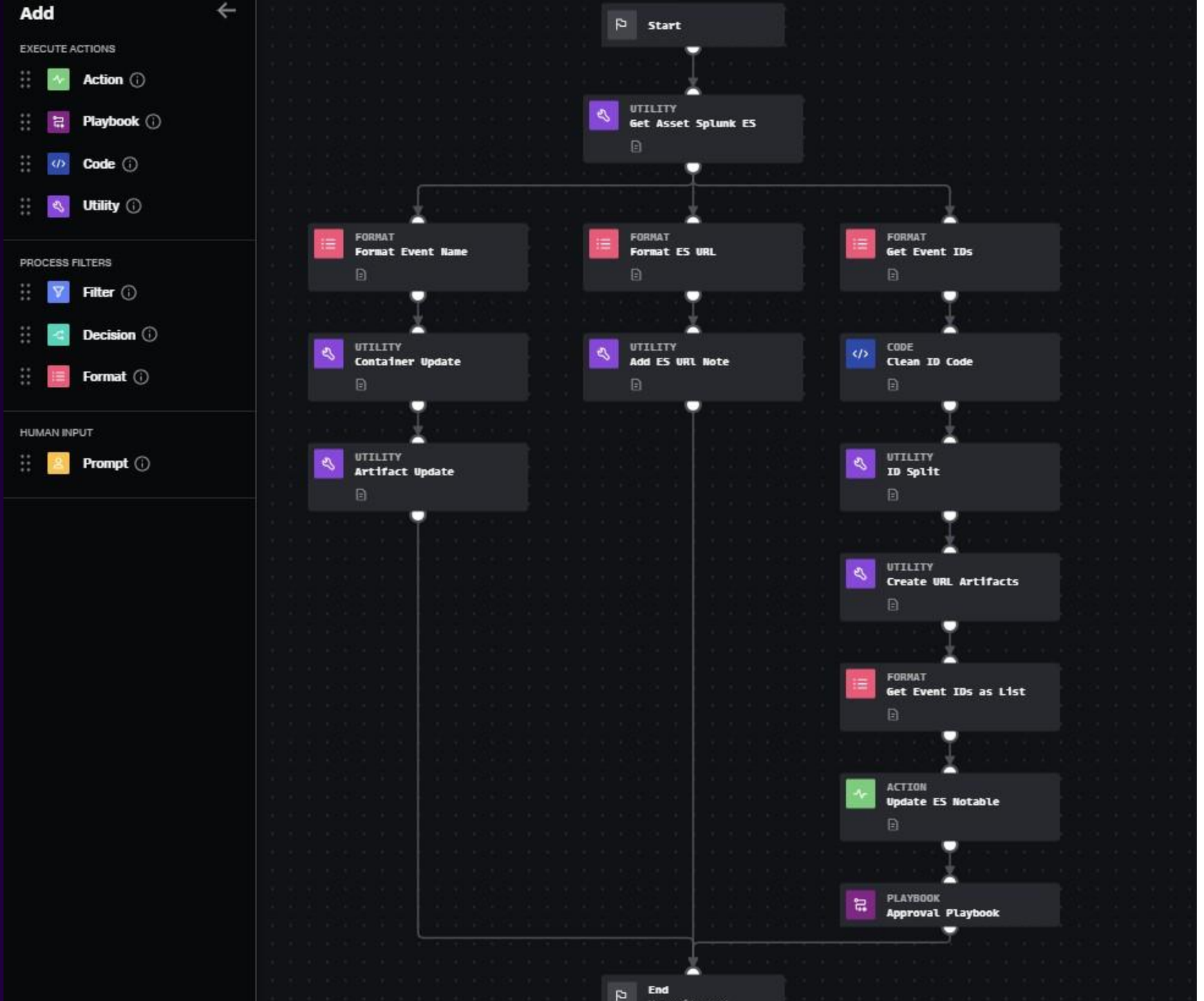
- Employ throttling on key fields
  - For this environment we used the ‘`host`’ field

- Run adaptive response ‘Send to SOAR’ with specific playbook and label selected
  - We used a specific label in SOAR named ‘`Approval`’ to store all approval containers

© 2025 SPLUNK LLC

Notable Onboarding Playbook

Shown in part 1, Previously developed playbook used again for a new customer to solve a problem!

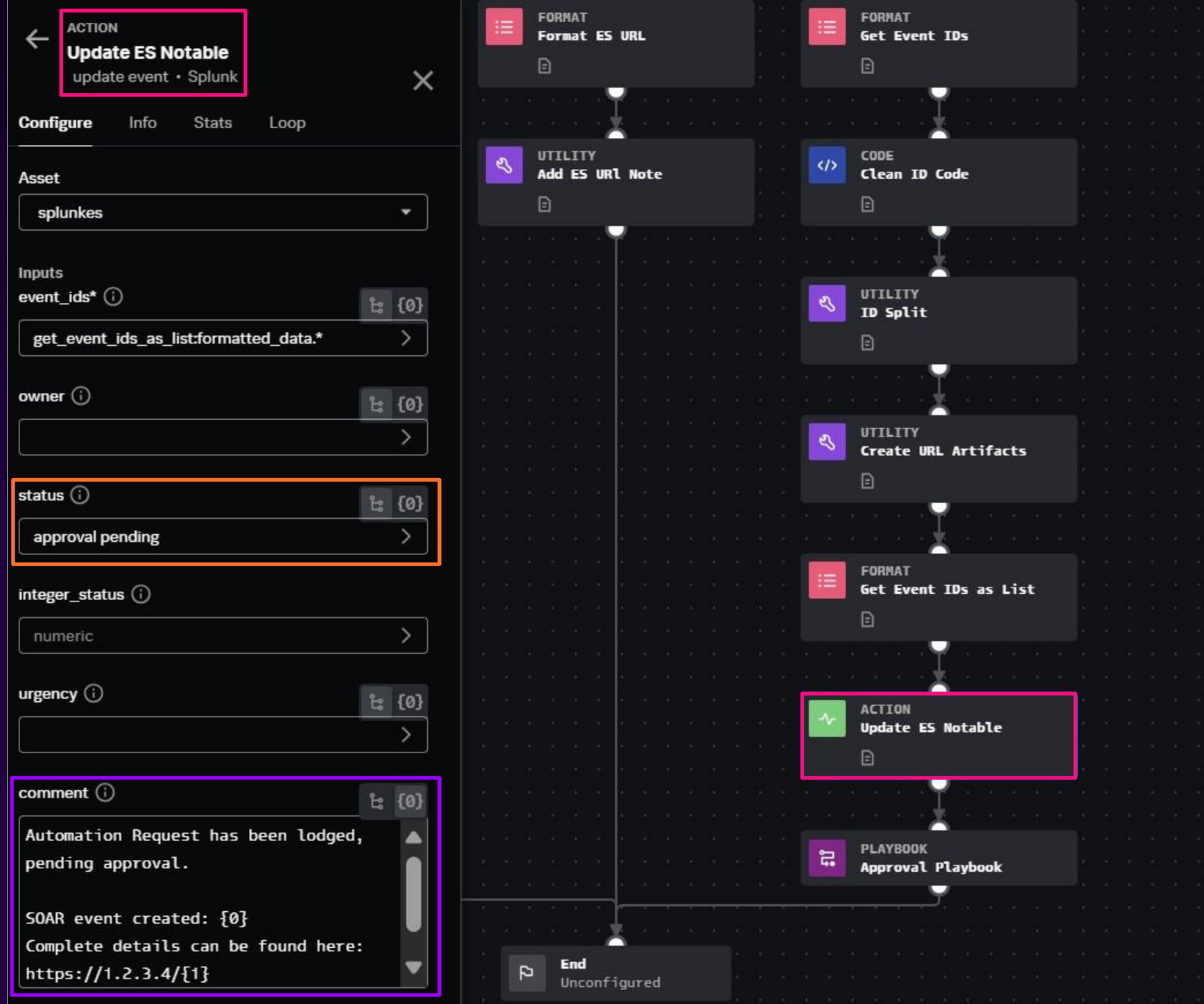


© 2025 SPLUNK LLC

Notable Onboarding Playbook

Action Block:
Splunk Update Event

Update status to approval pending and add comment

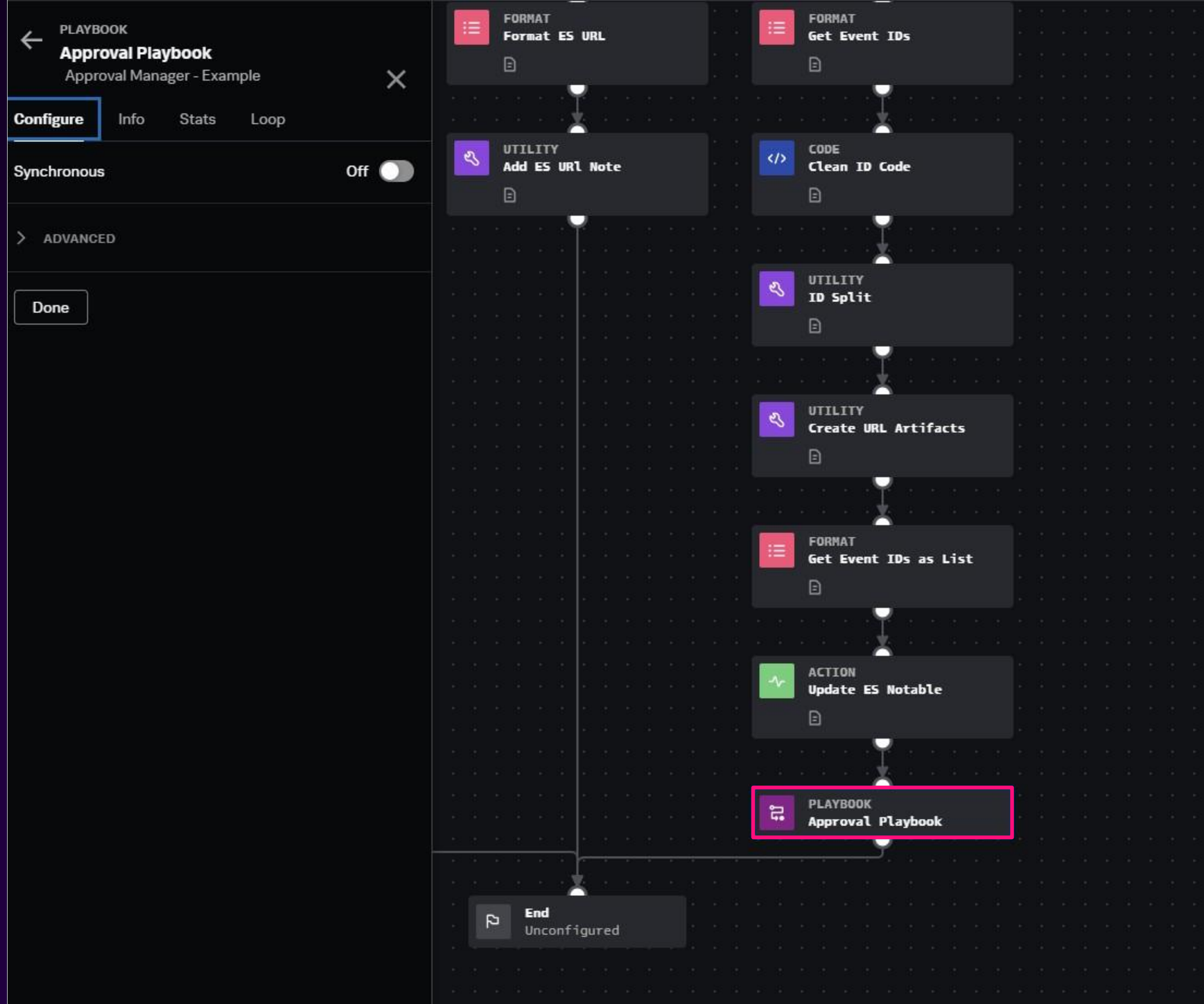


© 2025 SPLUNK LLC

Notable Onboarding Playbook

Playbook Block:

Run Approval Playbook as a sub playbook.

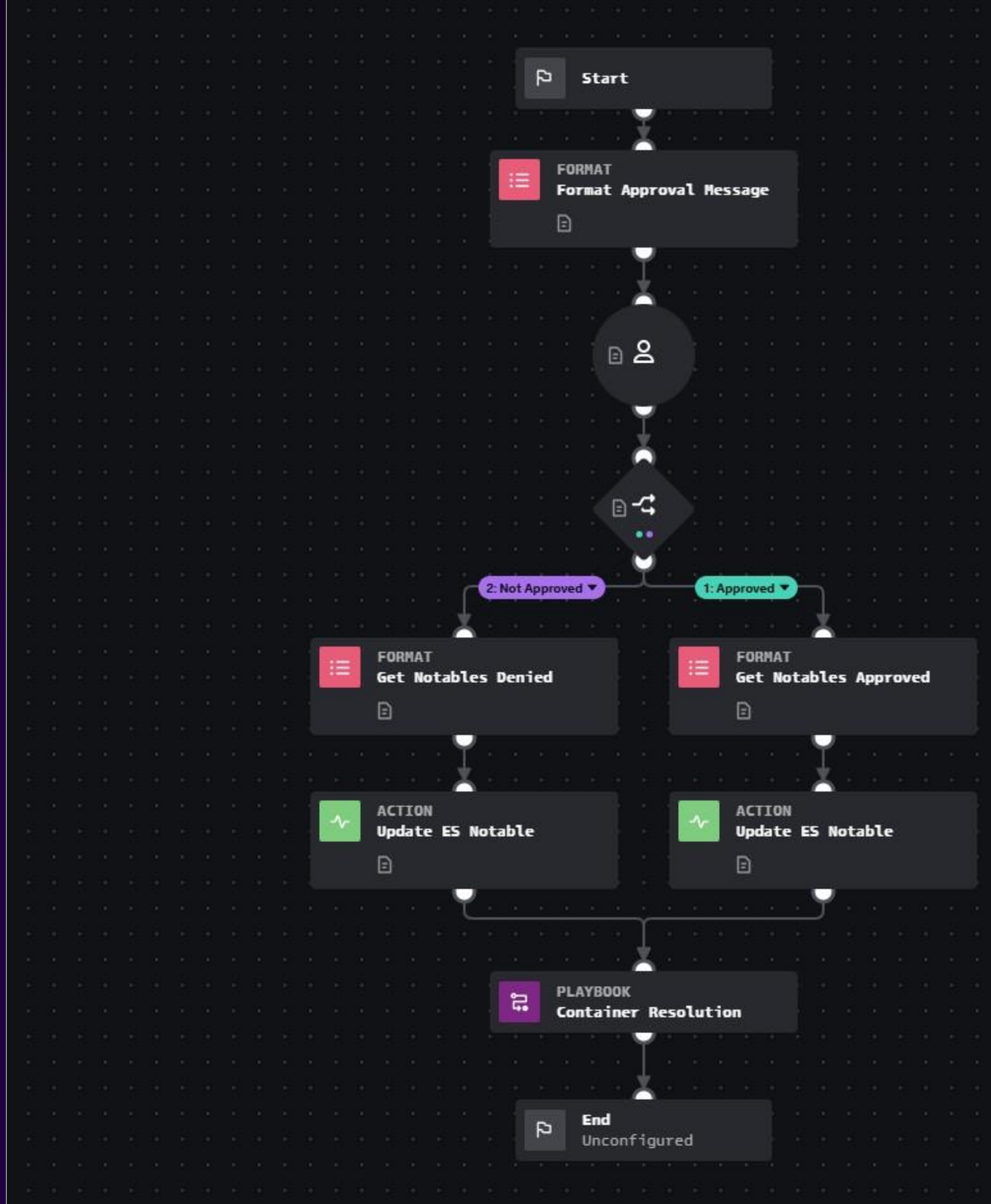


© 2025 SPLUNK LLC

Approval Playbook

New playbook created for the customer

Simple example of using prompts to capture an approval for automation and linking it back to ES!

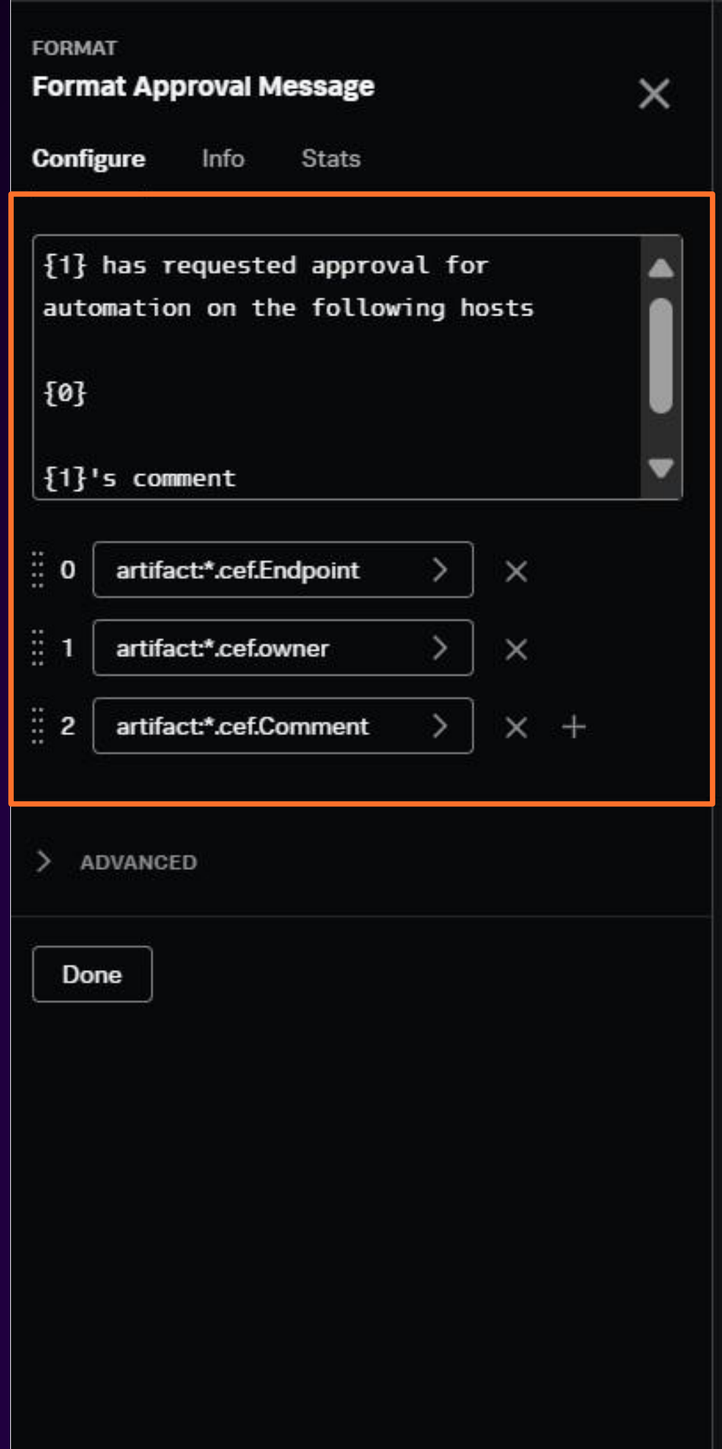


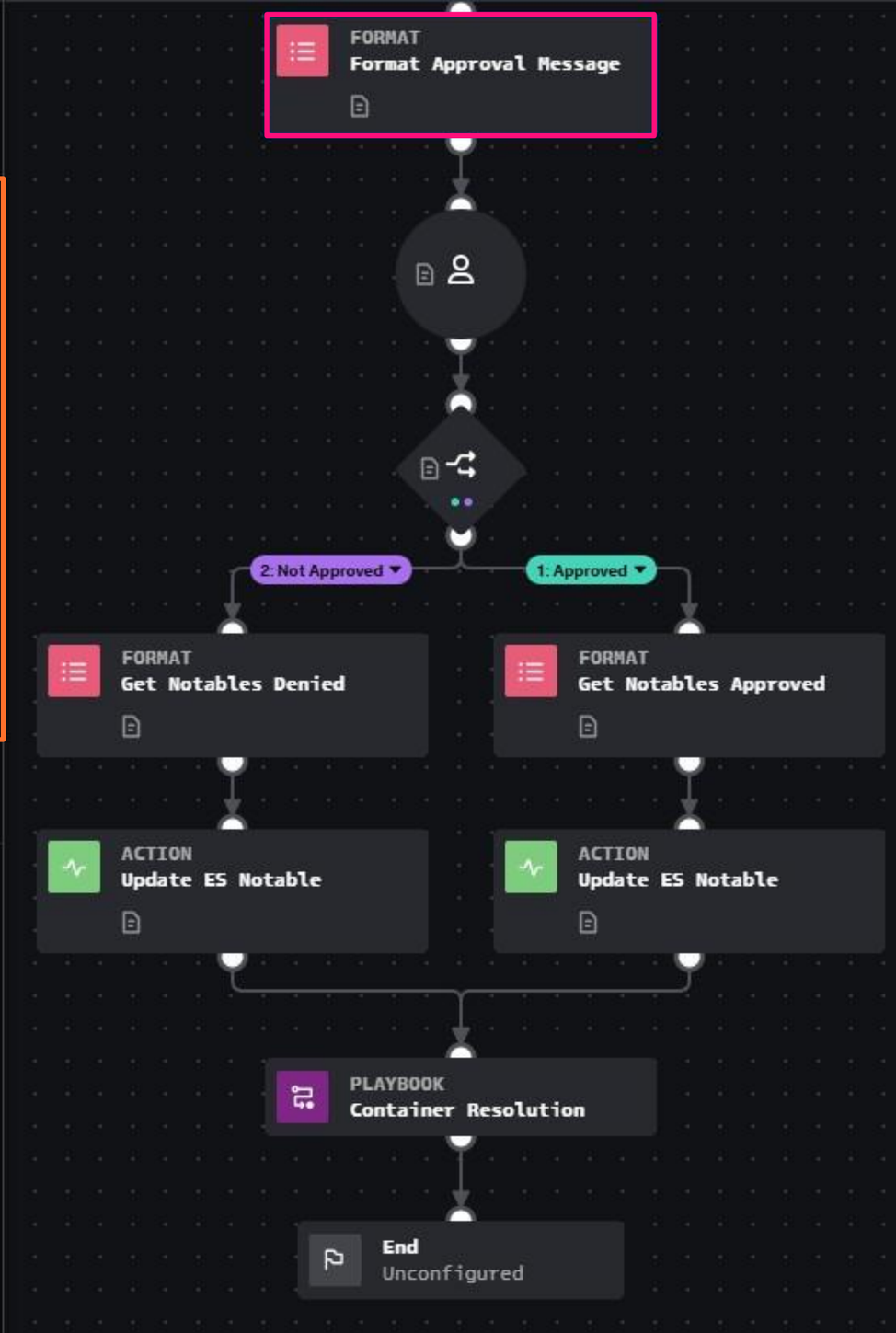
© 2025 SPLUNK LLC

Approval Playbook

Format Block:

Format custom message for the approver



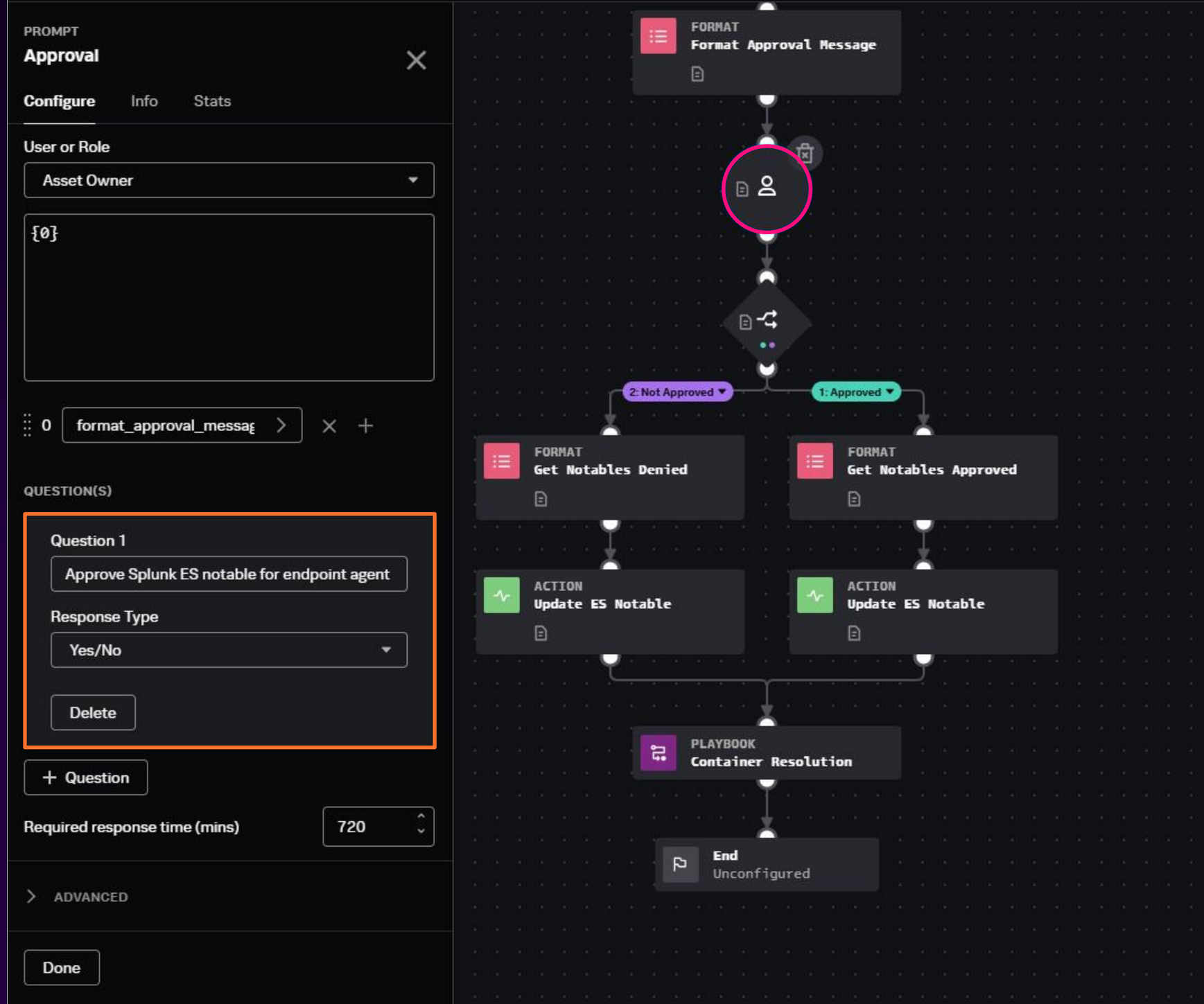


© 2025 SPLUNK LLC

Approval Playbook

Prompt Block:

Display formatted message and request Yes/No input from approver

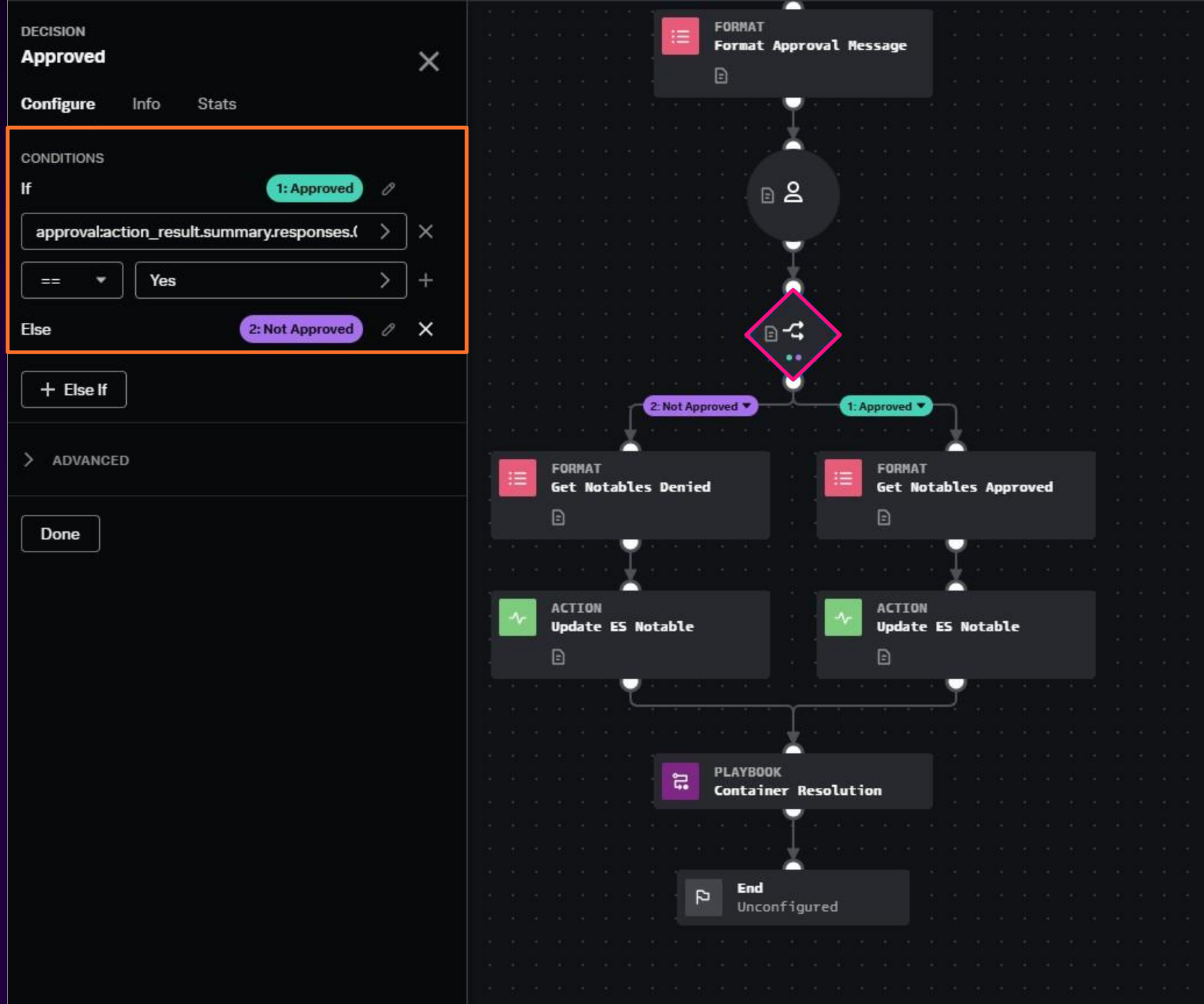


© 2025 SPLUNK LLC

Approval Playbook

Decision Block:

Based off approval prompt, perform required actions



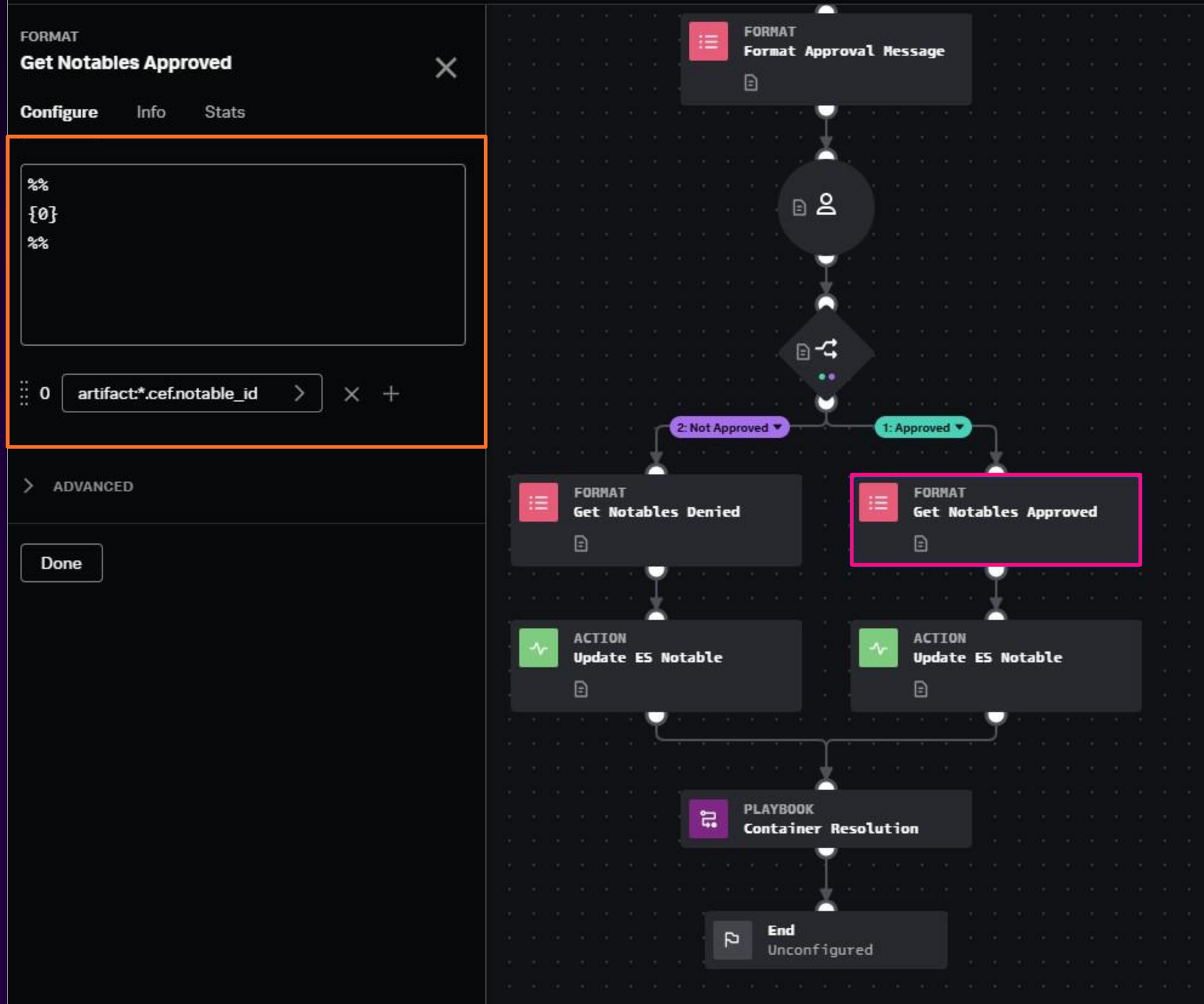
© 2025 SPLUNK LLC

Approval Playbook

Format Block:

List each Notable ID as a list

(See Part 1 on this)

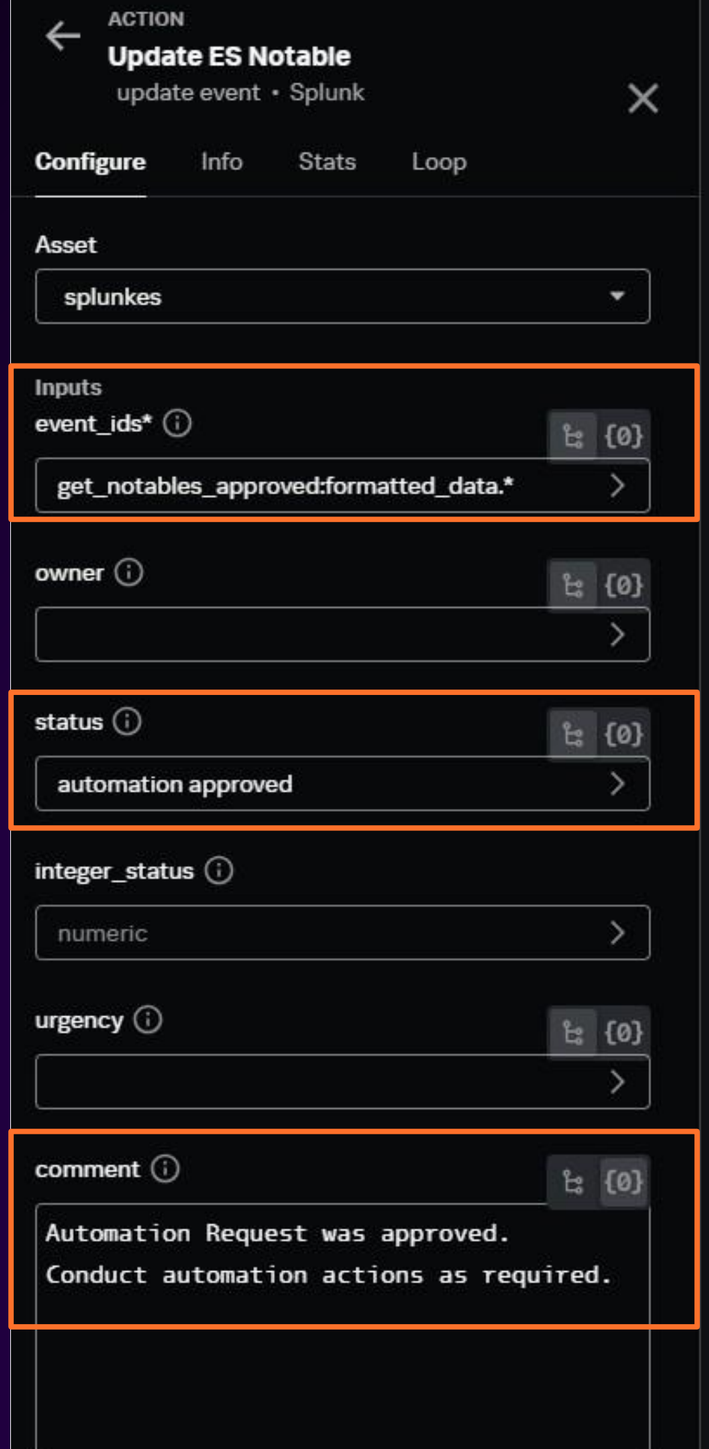


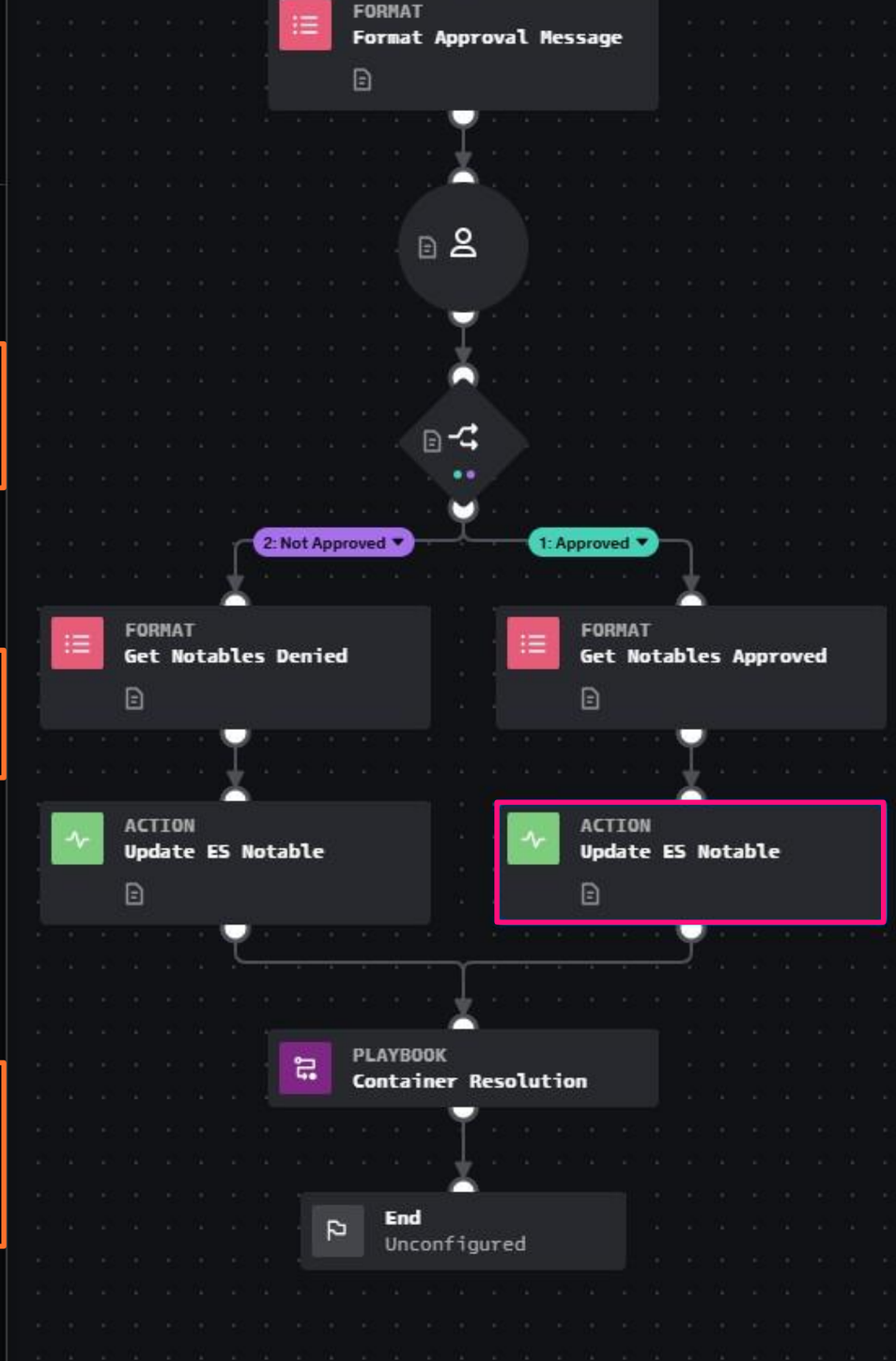
© 2025 SPLUNK LLC

Approval Playbook

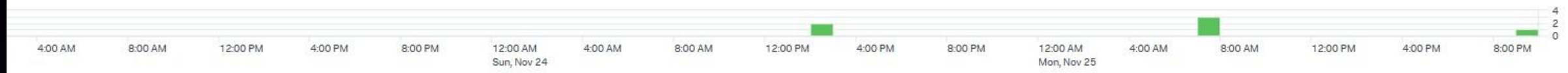
Action Block:
Splunk Update Event

Change status to desired state and provide message to end user





© 2025 SPLUNK LLC



Last refresh at 02:20 PM | Auto-refresh off | 20 per page

	Type	Time	Urgency	Status	Owner	Actions
	FINDING	Mon, Nov 25, 2024 9:05 PM	Medium	Automation Approved	rich	
	FINDING	Mon, Nov 25, 2024 7:40 AM	Medium	Automation Approved	benno	
	FINDING	Mon, Nov 25, 2024 7:40 AM	Medium	Automation Approved	benno	
	FINDING	Mon, Nov 25, 2024 7:40 AM	Medium	Automation Approved	benno	
	FINDING	Sun, Nov 24, 2024 2:33 PM	Informational	Automation Approved	benno	
	FINDING	Sun, Nov 24, 2024 2:33 PM	Informational	Automation Approved	benno	
	FINDING	Fri, Nov 22, 2024 3:52 PM	High	Automation Denied	benno	
	FINDING	Fri, Nov 22, 2024 3:26 PM	Critical	Automation Approved	benno	
	FINDING	Fri, Nov 22, 2024 2:42 PM	High	Automation Approved	benno	
	FINDING	Fri, Nov 22, 2024 1:43 PM	Informational	Automation Approved	benno	
	FINDING	Fri, Nov 22, 2024 1:28 PM	Informational	Automation Approved	benno	
	FINDING	Fri, Nov 22, 2024 1:27 PM	Informational	Automation Approved	benno	
	FINDING			Automation		

© 2025 SPLUNK LLC

Automation Approval Playbook

Key Takeaways

- Thinking outside the box to create a custom solution to a complex set of requirements
- Leveraged the strengths of both ES and SOAR where each is more appropriate
  - Steered the solution away from a fixation on SOAR doing everything
- Final implementation allowed for bulk automation runs while still meeting customer approval process requirements

© 2025 SPLUNK LLC

Remote Script / Command Execution

© 2025 SPLUNK LLC

Remote Script and Command Execution

Using SOAR to invoke native OS level commands

What and why?

- Requirement to remediate various agents across the environment from SOAR
  - Logging, AV, EDR, VM, etc
  - Extant approach completely manual and no longer viable
- Solution needed to be able to:
  - Start/stop agents
  - Install/remove agents
  - Perform automated troubleshooting remotely, and capture results

© 2025 SPLUNK LLC

Remote Script and Command Execution

Using SOAR to invoke native OS level commands

How?

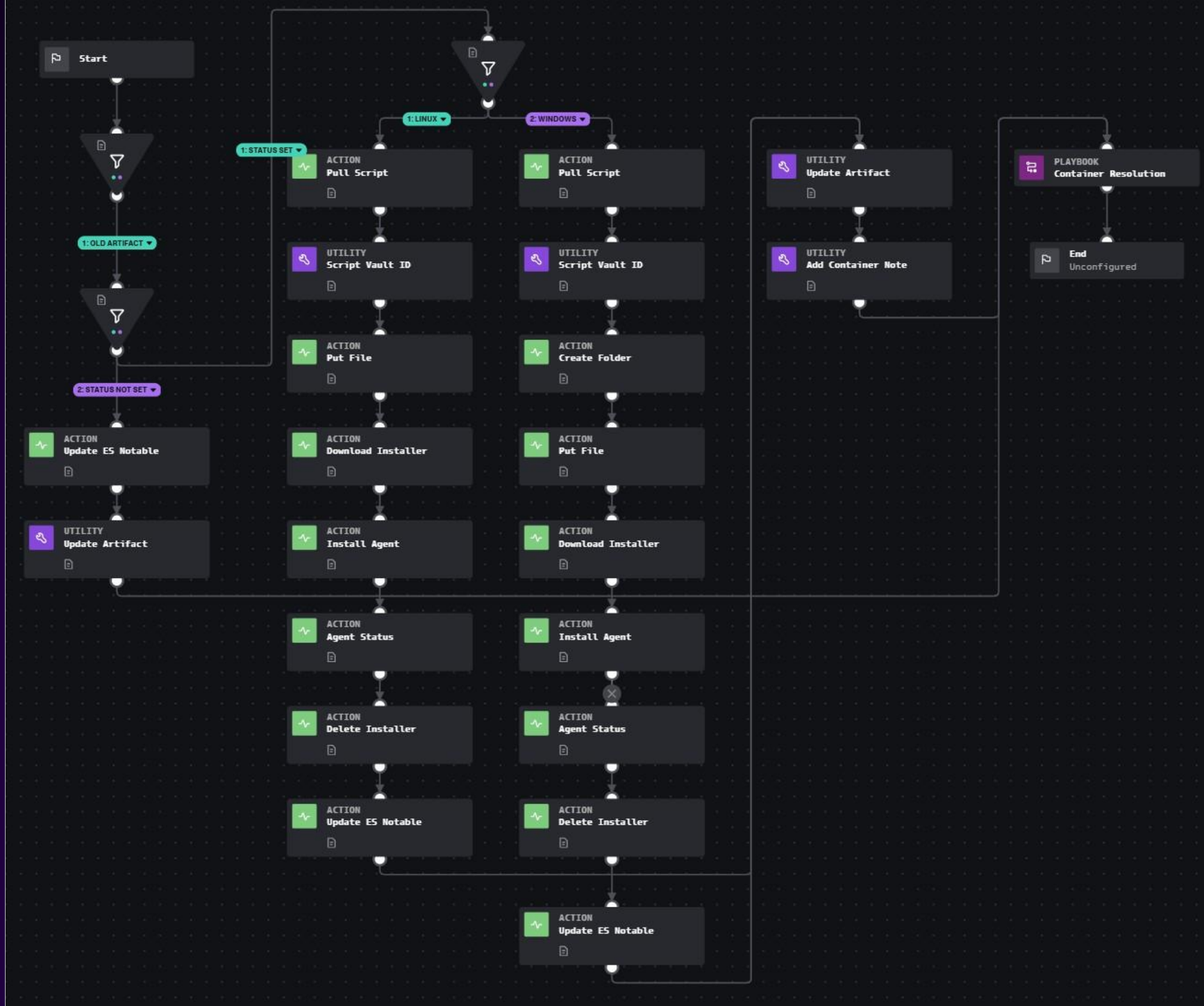
- Custom scripts to do heavy lifting on OS side
  - WinRM App in SOAR using the Run Script function
  - SSH App in SOAR using the Execute Program function

- Leverage Native SOAR functions

© 2025 SPLUNK LLC

Remote Script Example

Pushes a script to the remote endpoint and executes various scripted actions



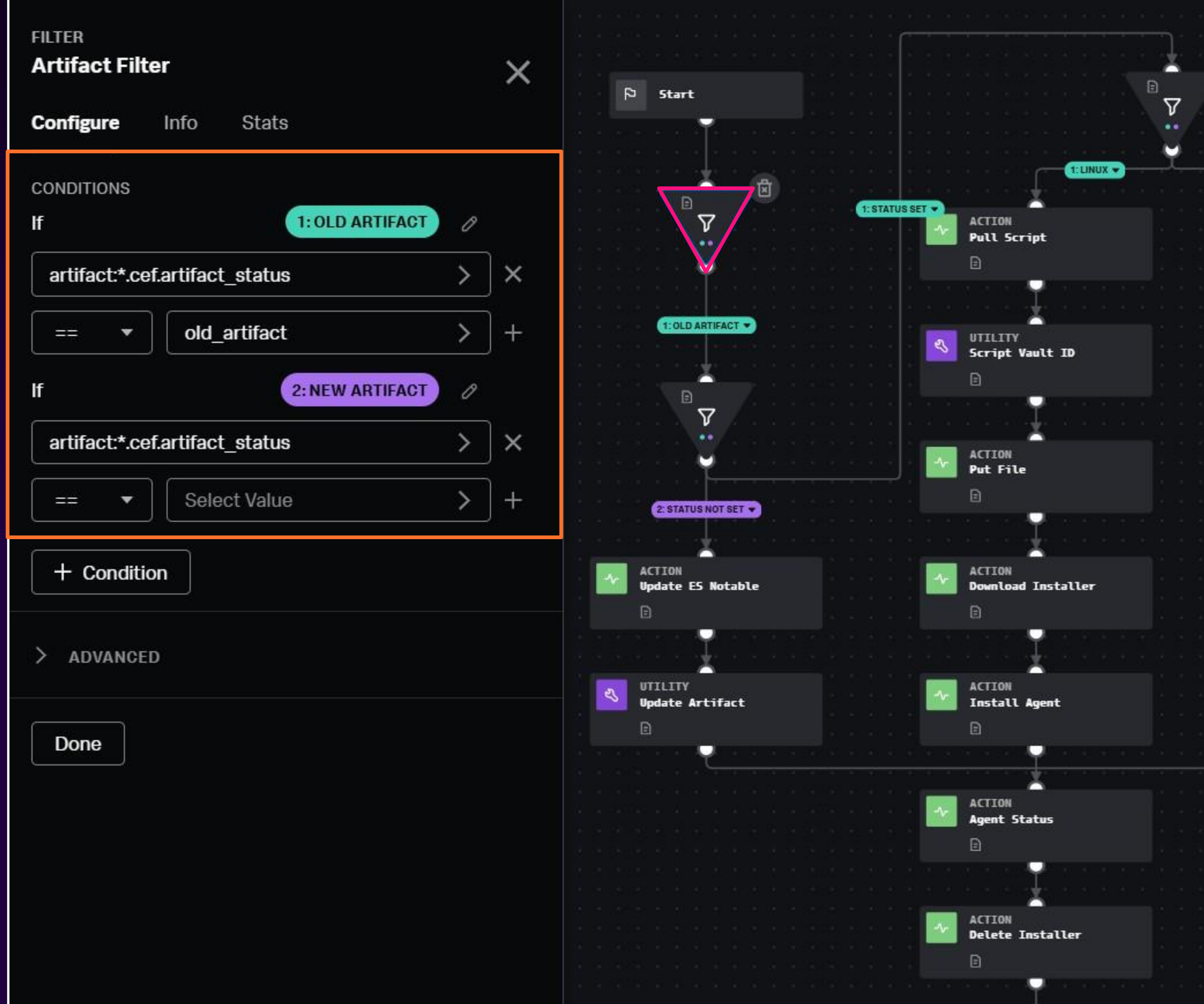
© 2025 SPLUNK LLC

Remote Script Example

Filter Block:

Checking if artifact is marked as old_artifact

Executing an adaptive response on an ES Notable re-opens the same container it originally created

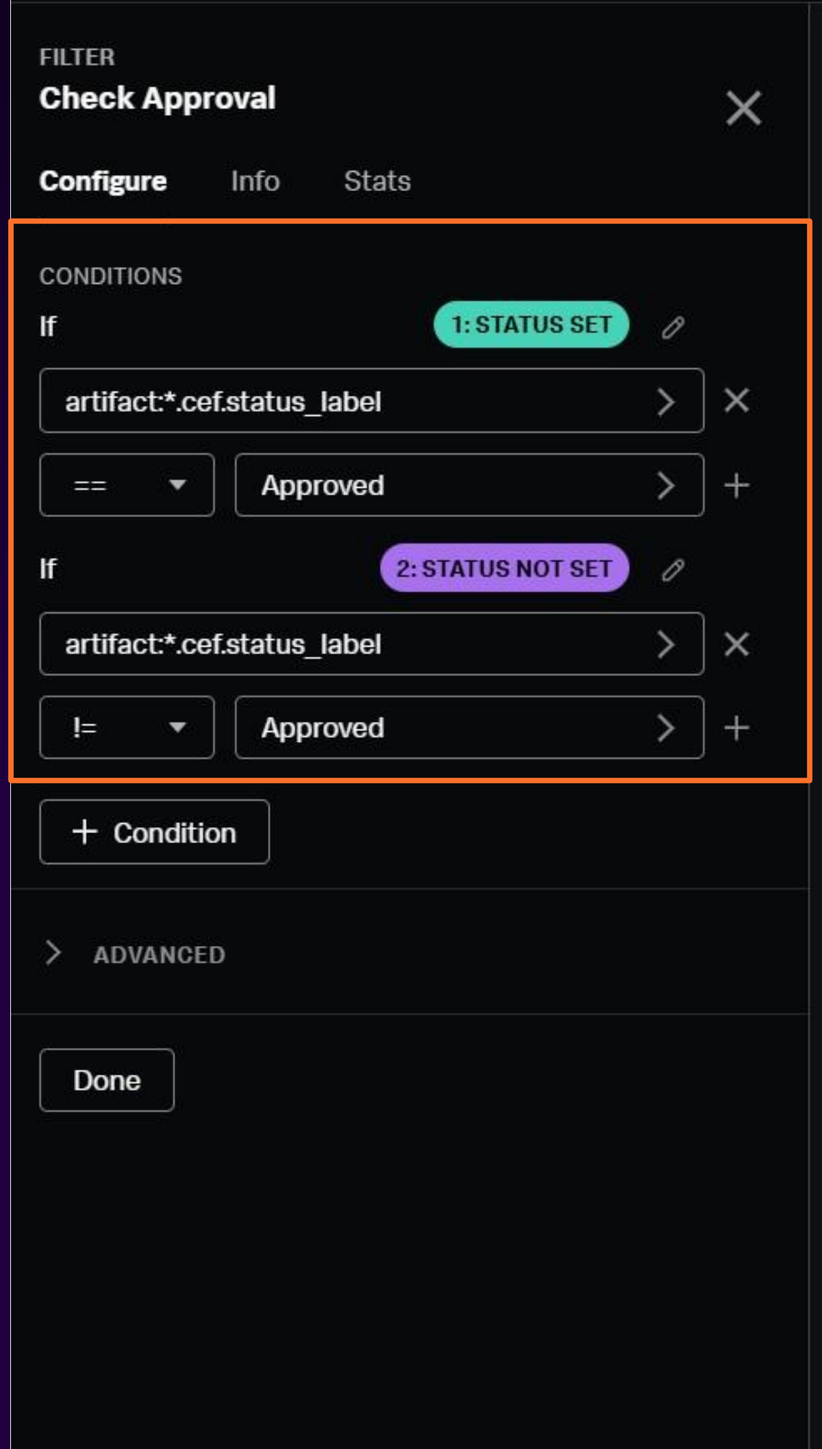


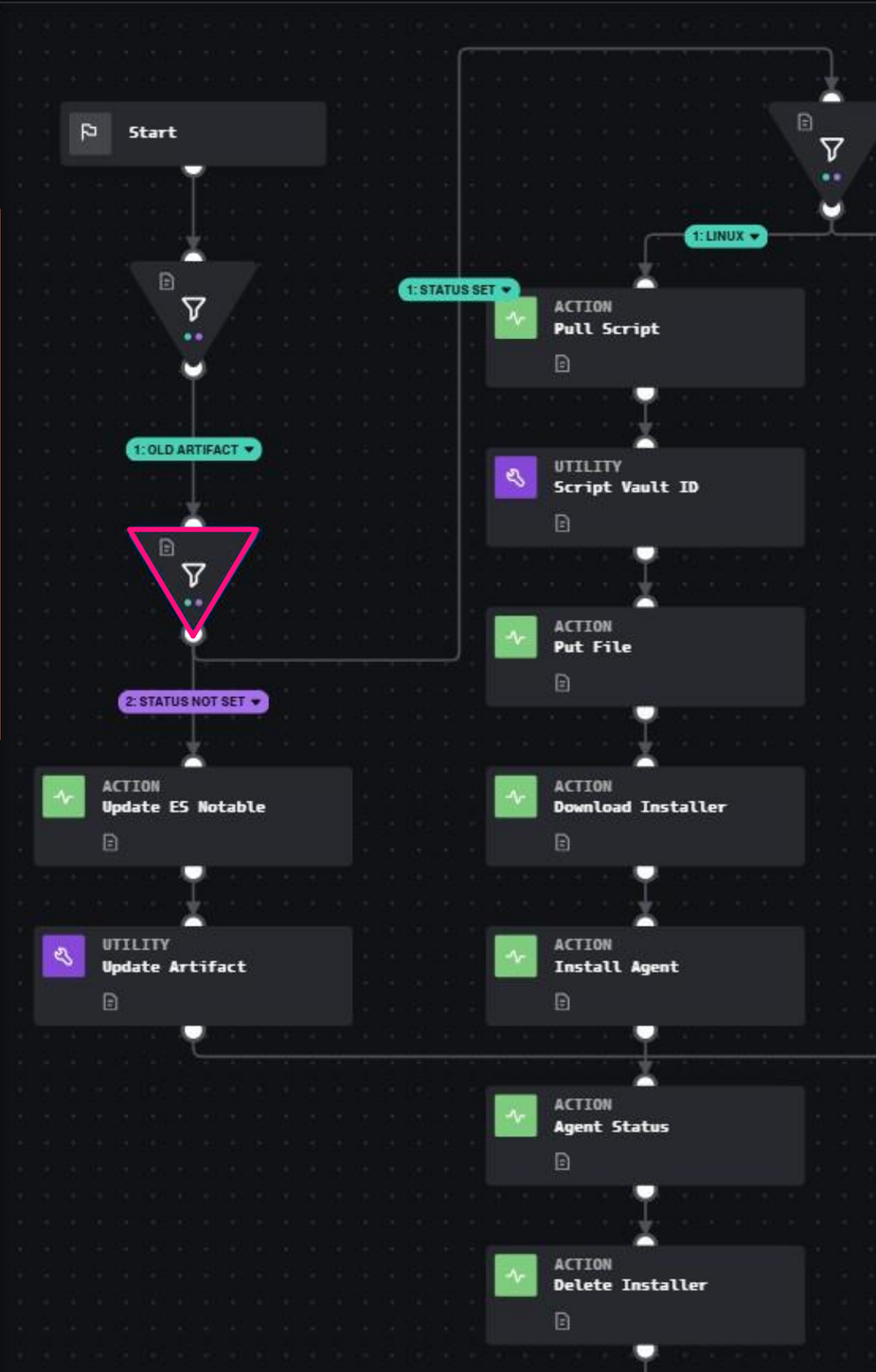
© 2025 SPLUNK LLC

Remote Script Example

Filter Block:

Check if artifact contains Approved field under status_label



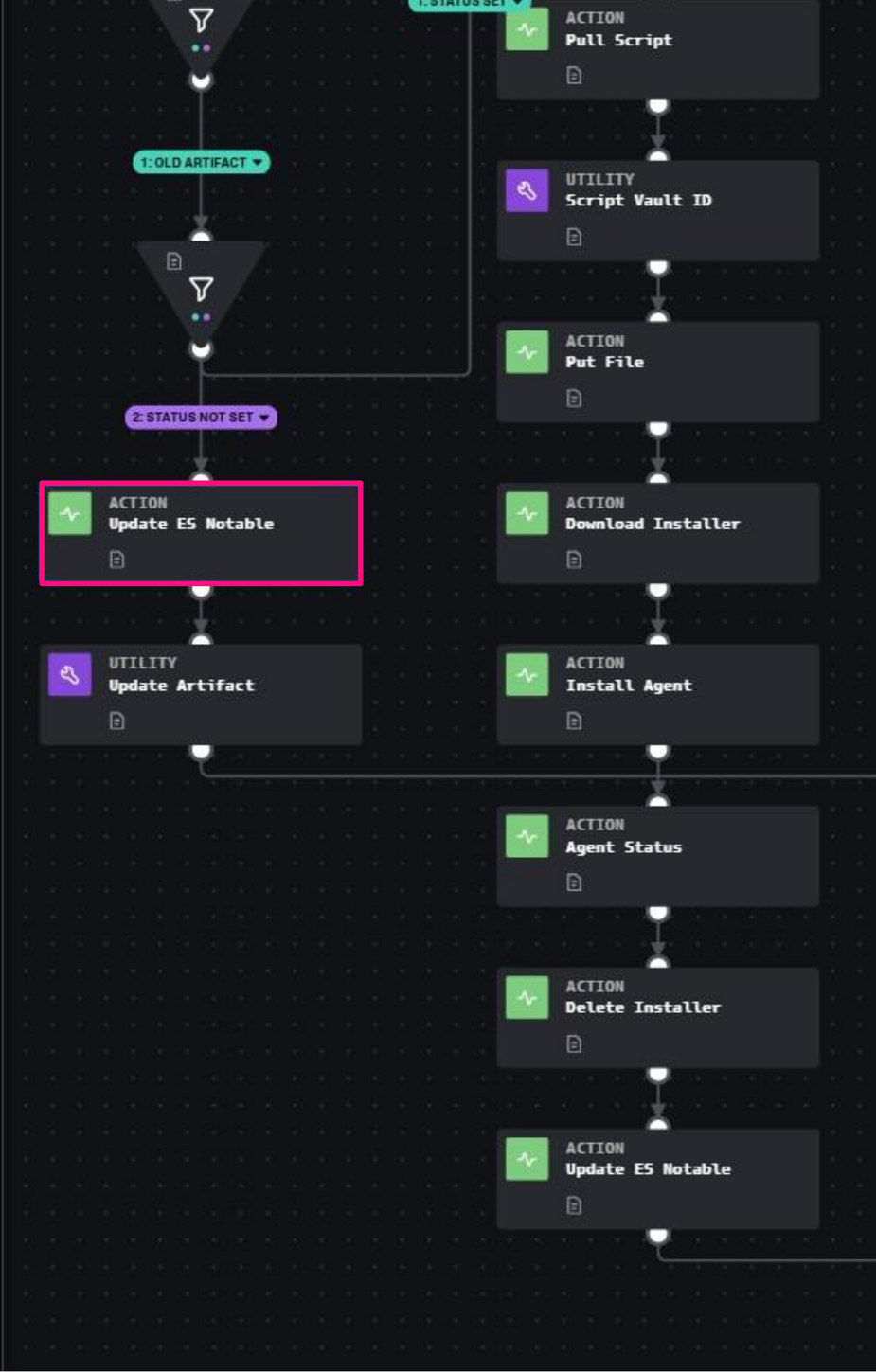


© 2025 SPLUNK LLC

Remote Script Example

Action Block:
Update Splunk

Send comment to Notable event stating automation not run due to approval state

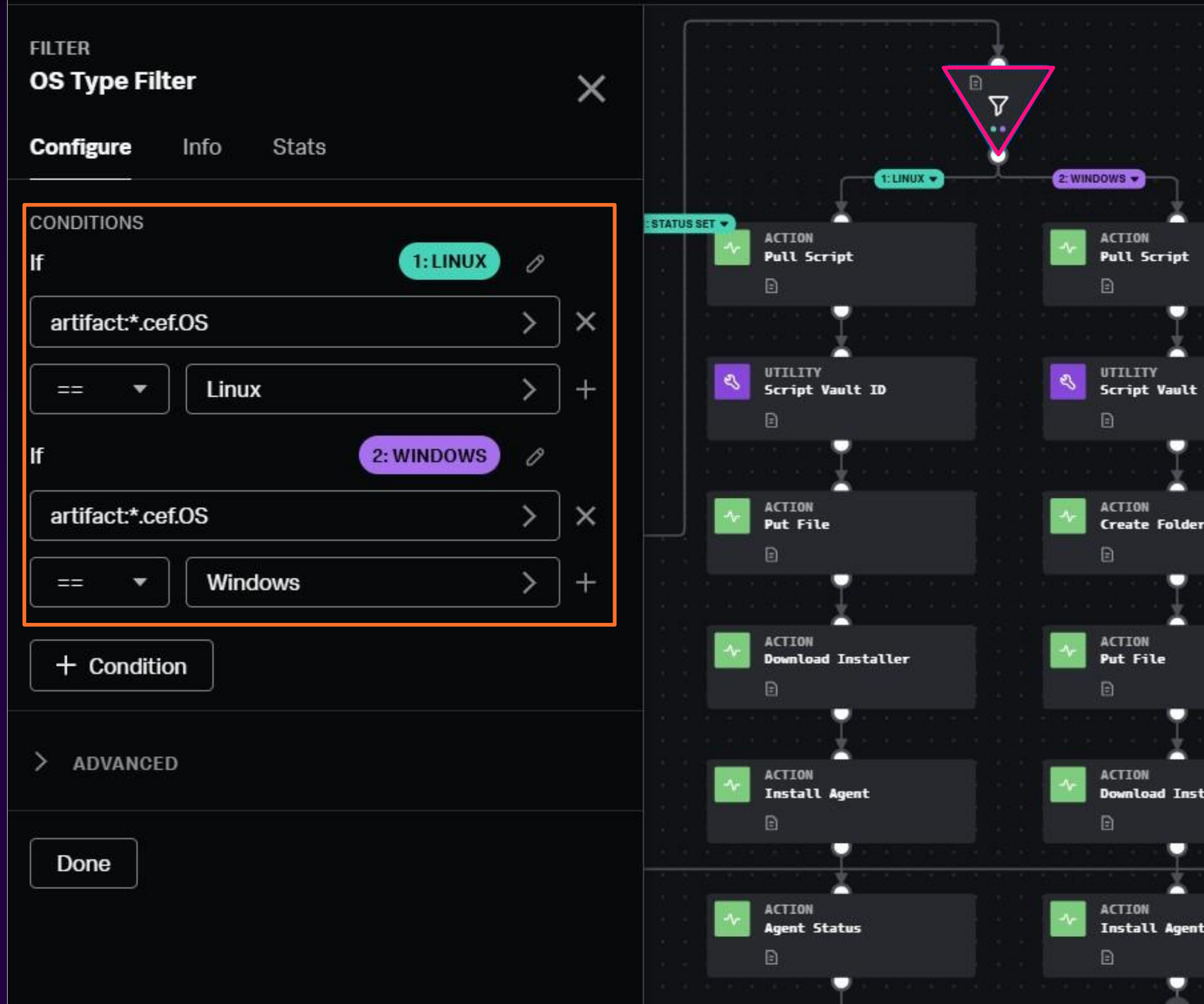


© 2025 SPLUNK LLC

Remote Script Example

Filter Block:

Check for OS to determine correct path

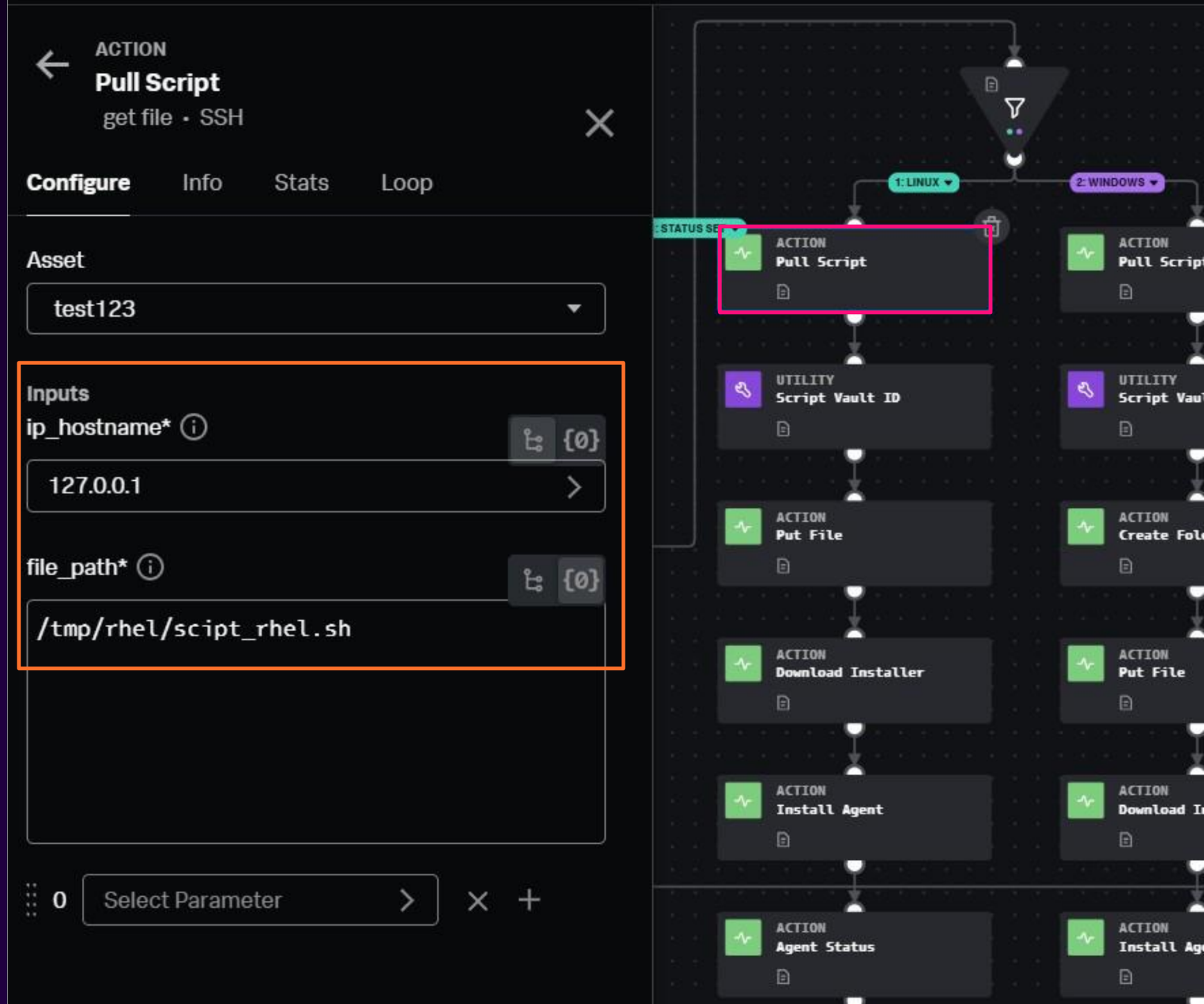


© 2025 SPLUNK LLC

Remote Script Example

Action Block:
SSH Get File

Use the SSH App and the get file action to connect SOAR itself using 127.0.0.1 to get the script

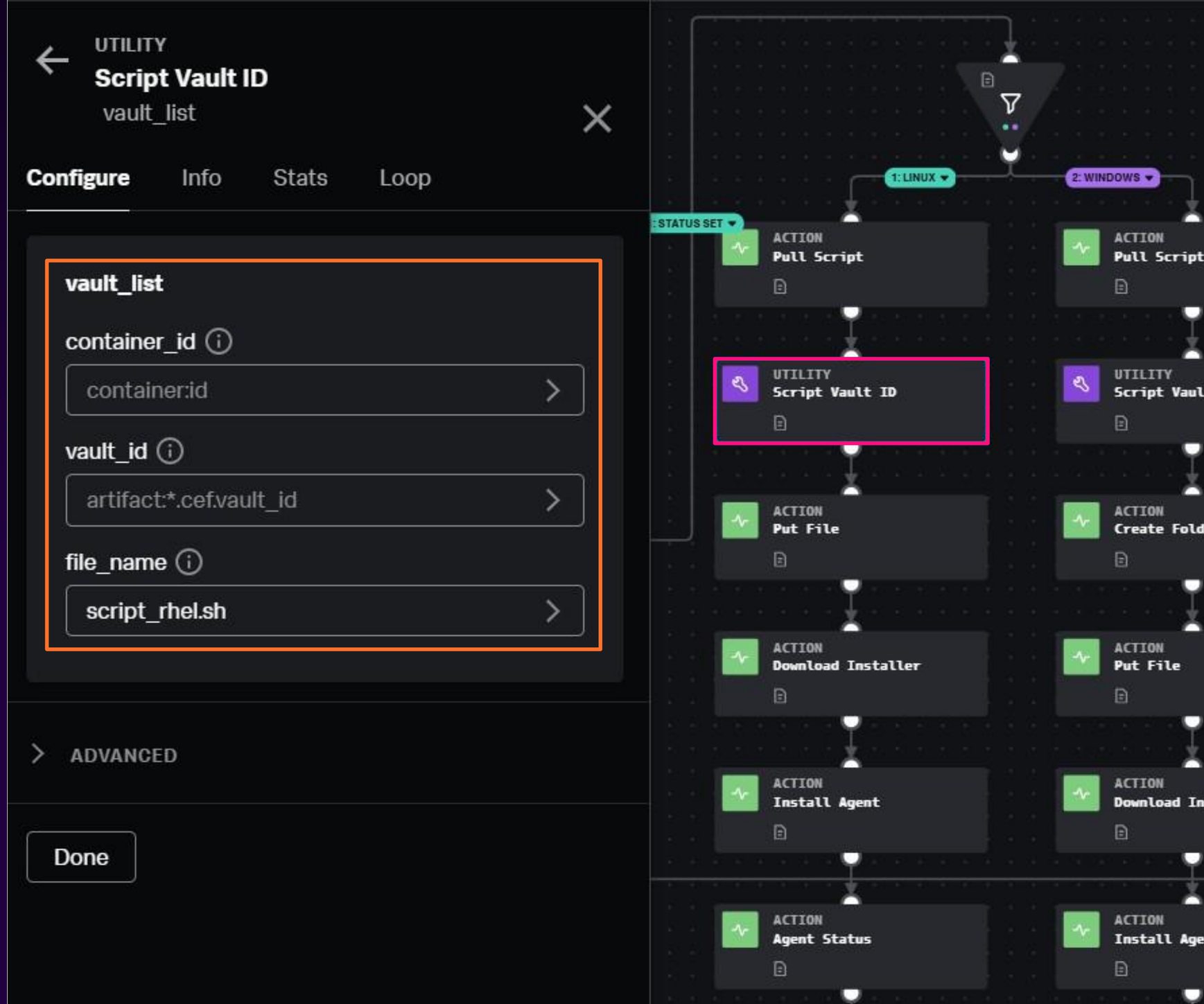


© 2025 SPLUNK LLC

Remote Script Example

Utility Block:
Vault List

Add the previously pulled script into the containers file vault

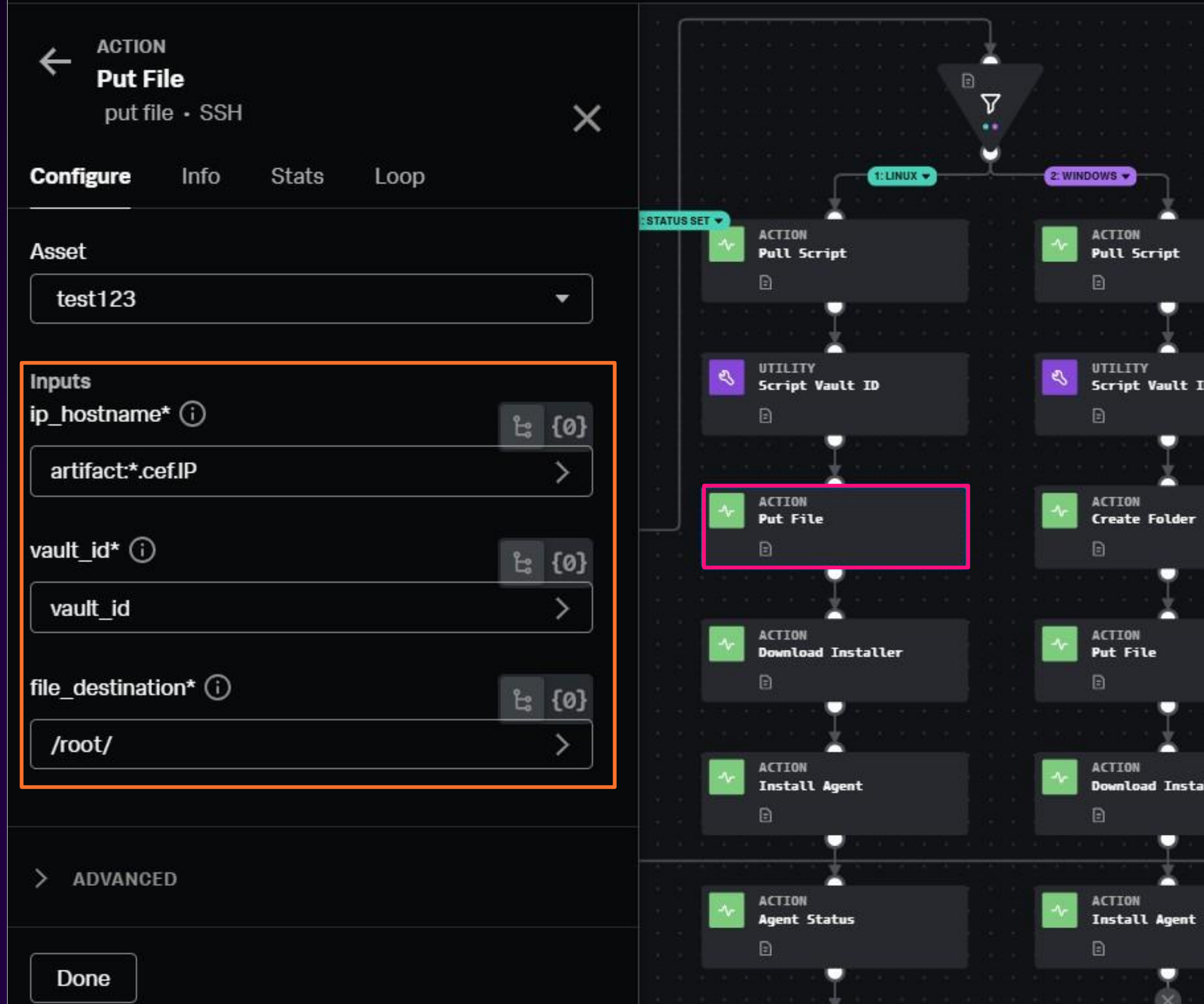


© 2025 SPLUNK LLC

Remote Script Example

Action Block:
SSH Put File

Now use SSH Put File action again to place the script on the target endpoint using the vault file.



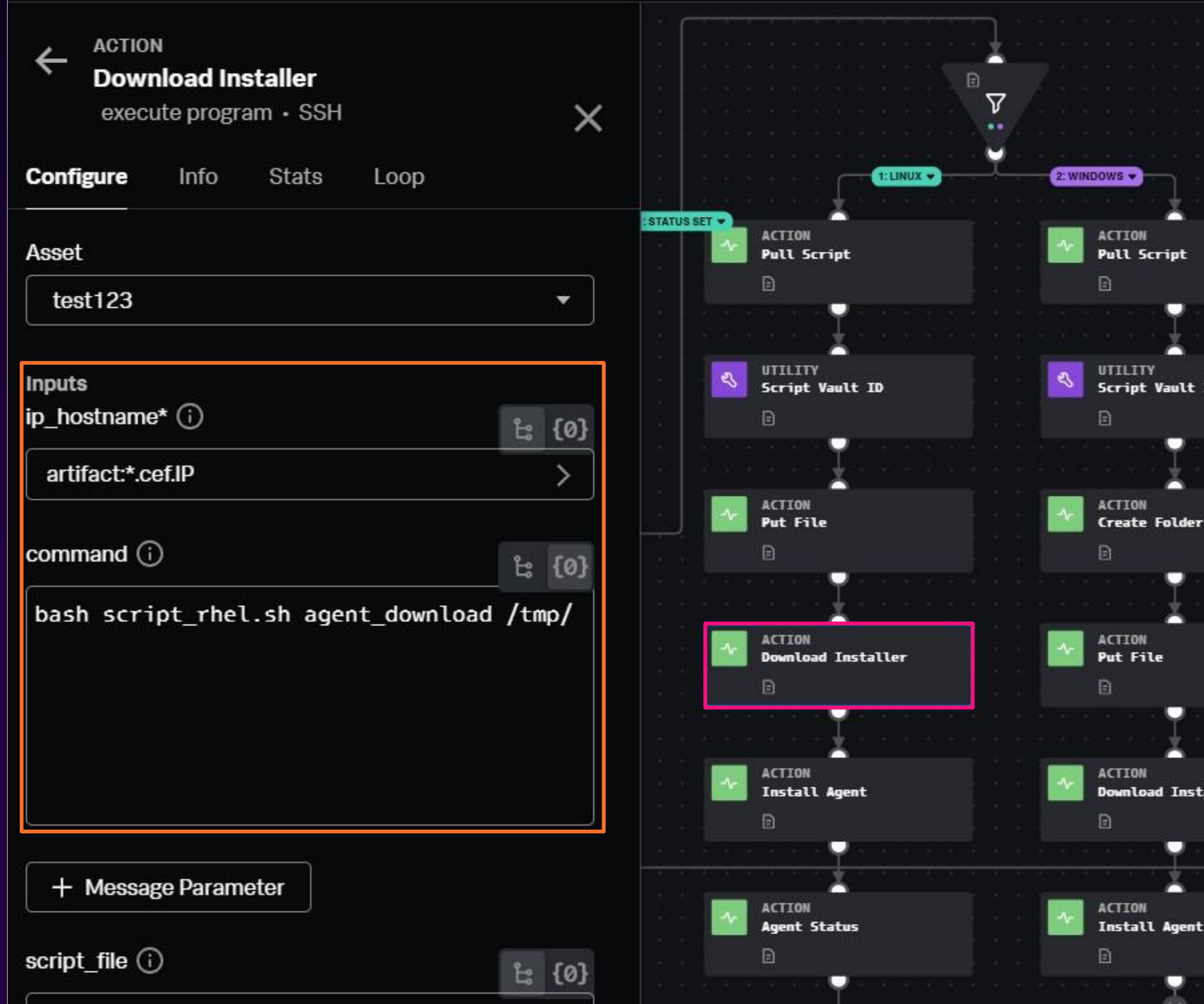
© 2025 SPLUNK LLC

Remote Script Example

Action Block:
SSH Execute Program

Using bash execute the script file placed on target host.

Note in this instance its called a specific function within the script.

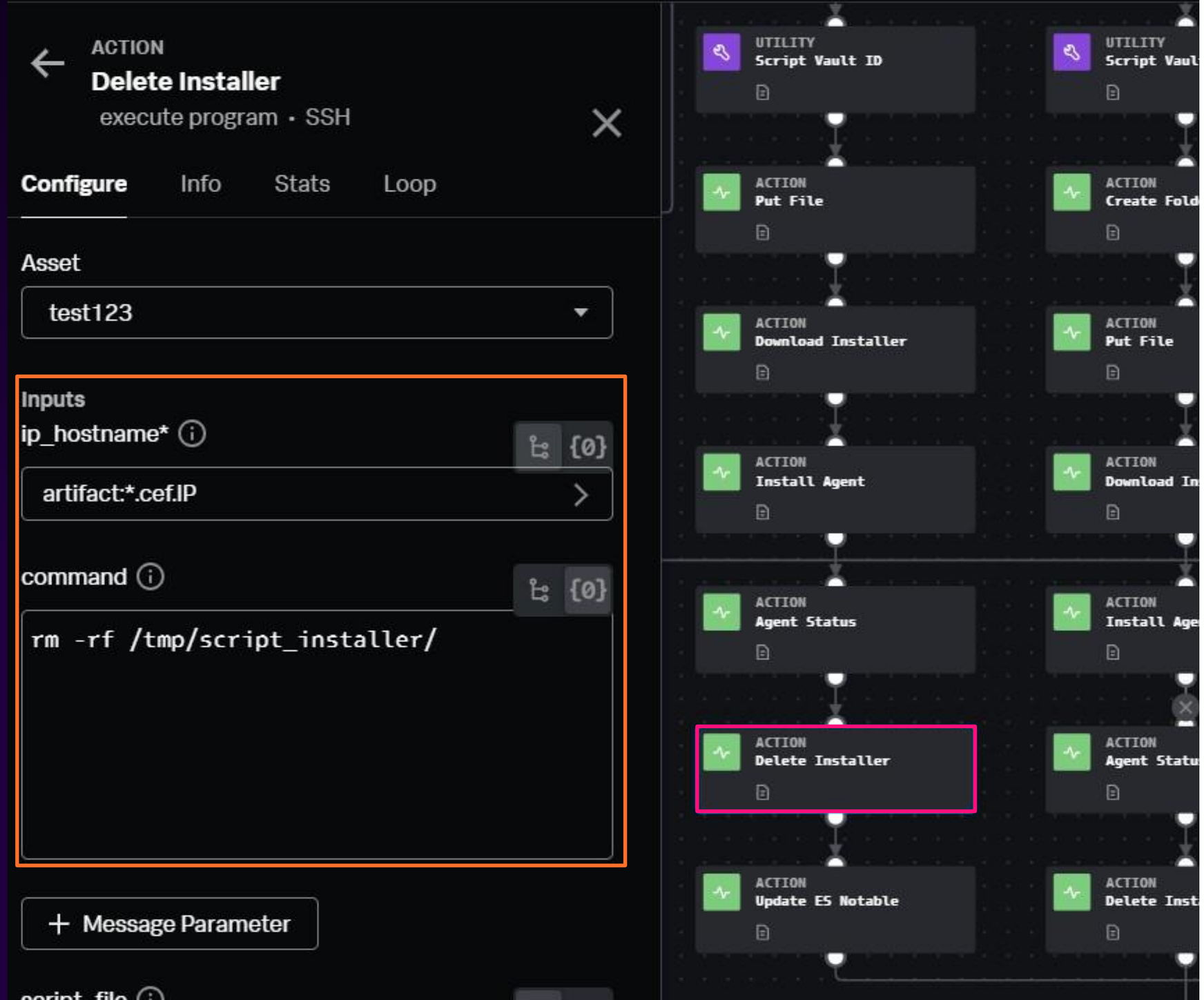


© 2025 SPLUNK LLC

Remote Script Example

Action Block:
SSH Execute Program

Remove the script from the end host



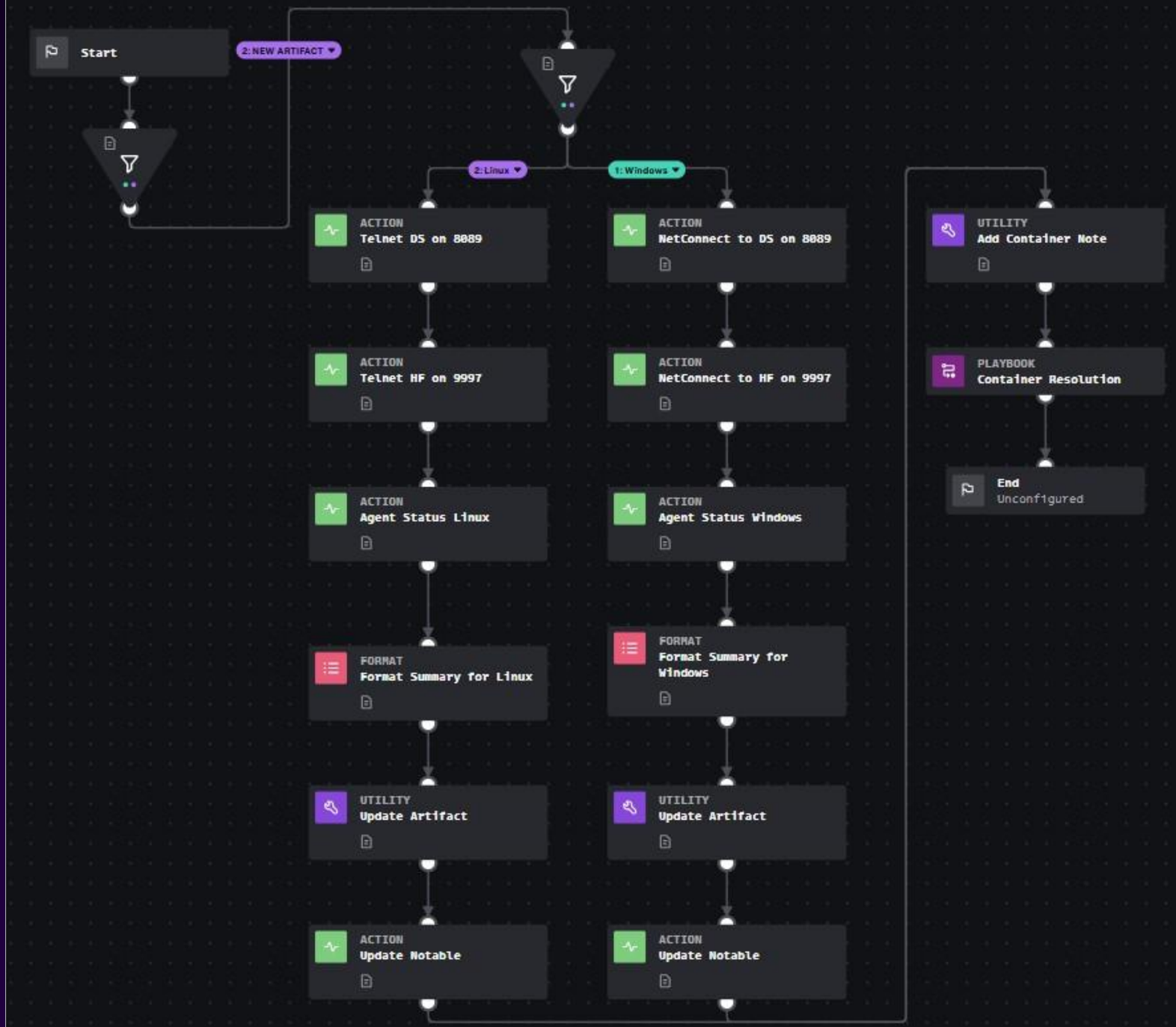
© 2025 SPLUNK LLC

Remote Command Example

Runs commands based off determined host OS

Command results are returned to SOAR

Results formatted



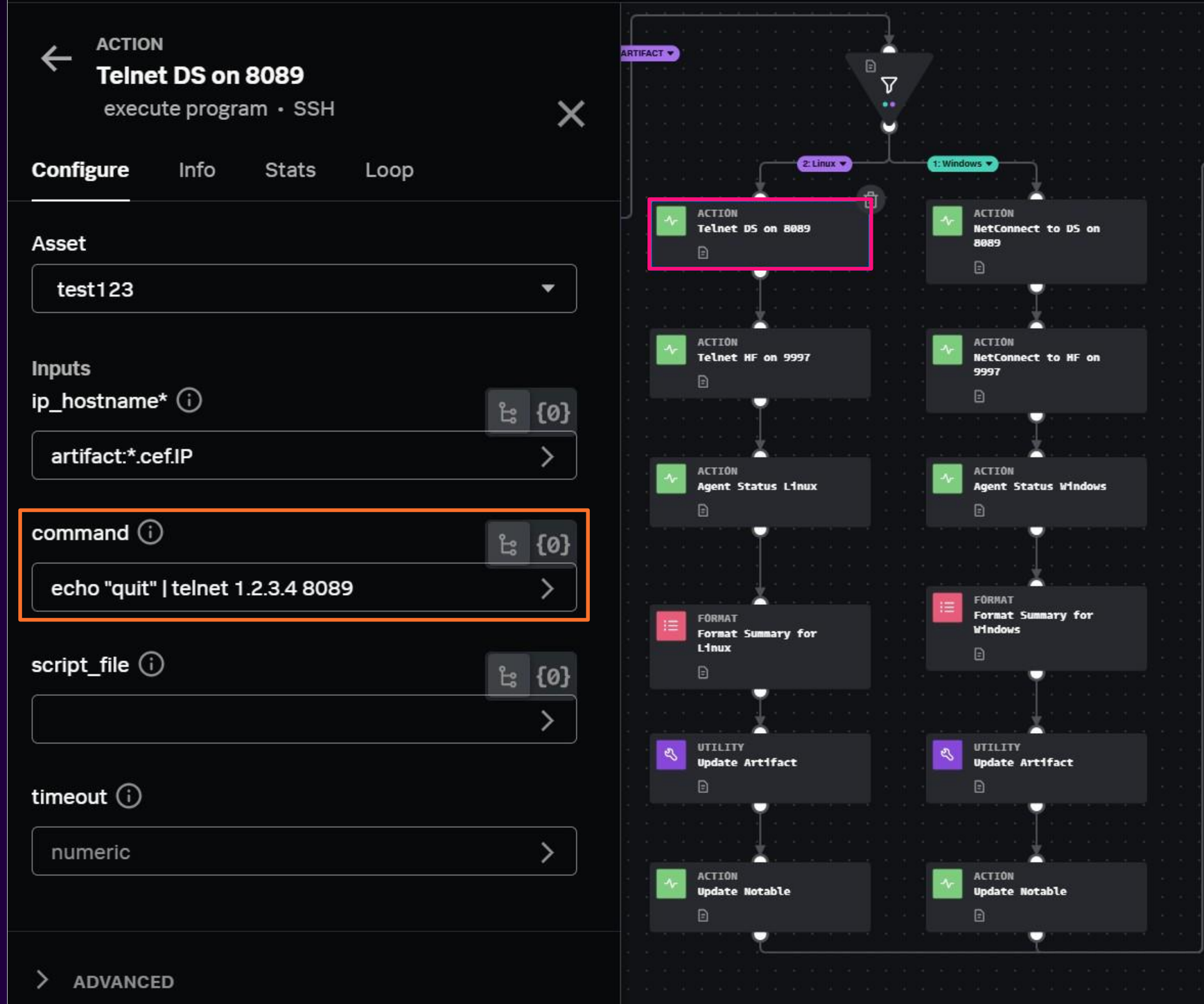
© 2025 SPLUNK LLC

Remote Command Example

Action Block:
SSH Execute Program

Run telnet command against IP and Port 8089 to test Splunk to Splunk

Results are automatically returned

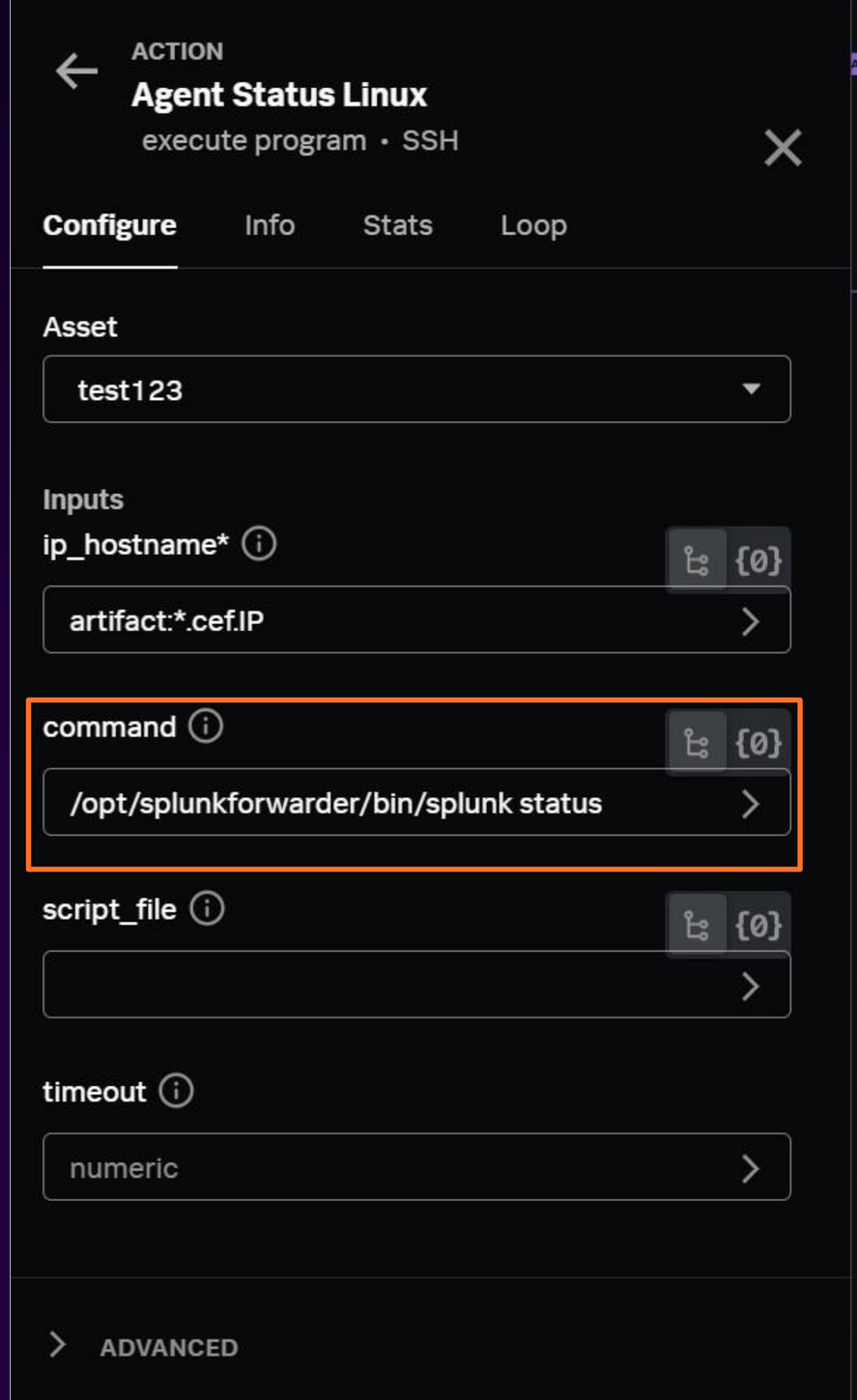


© 2025 SPLUNK LLC

Remote Command Example

Action Block:
SSH Execute Program

Run splunk status command



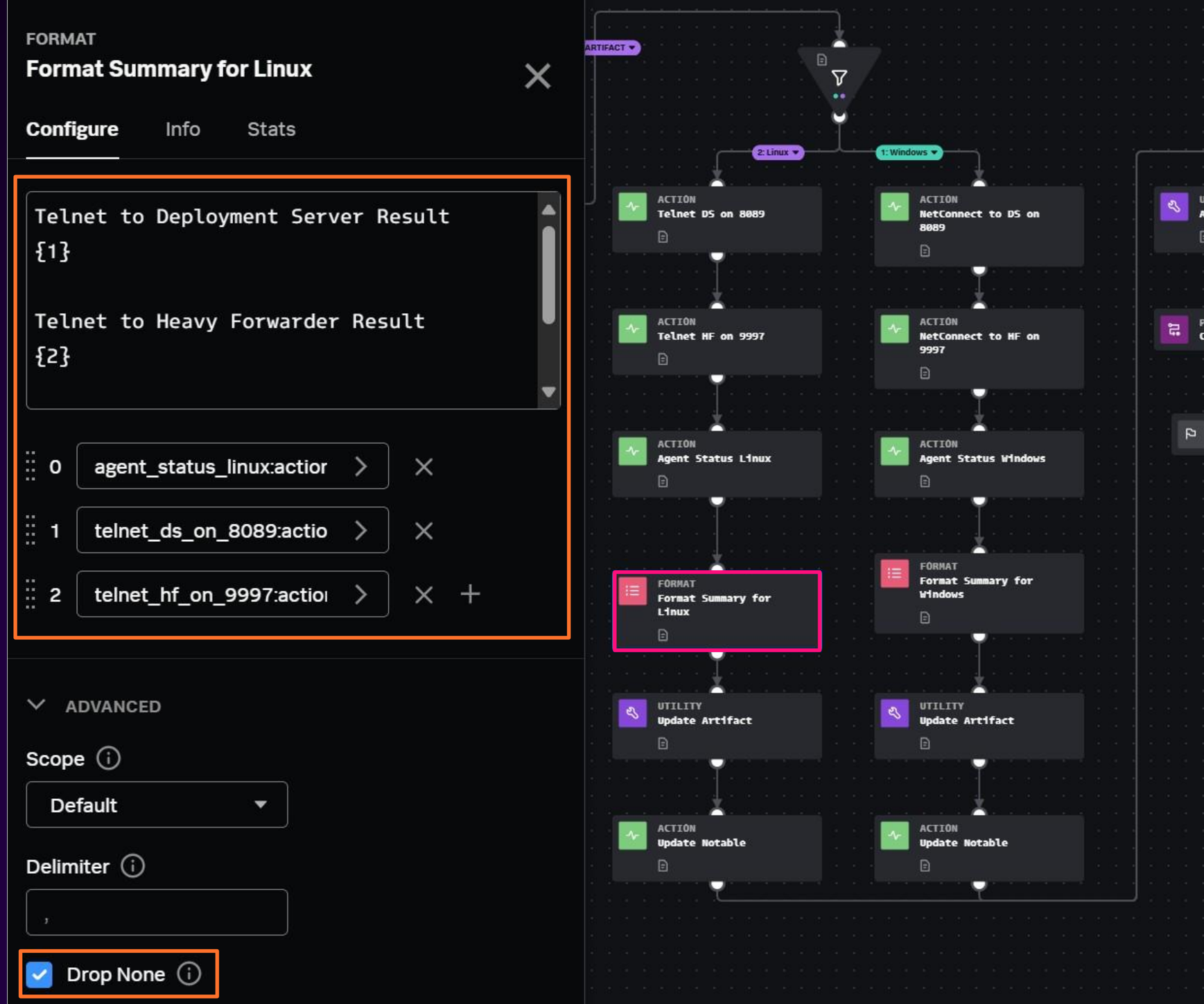
© 2025 SPLUNK LLC

Remote Command Example

Format Block:

Format a message using all the returned results from the previous action blocks

Note the drop none is selected

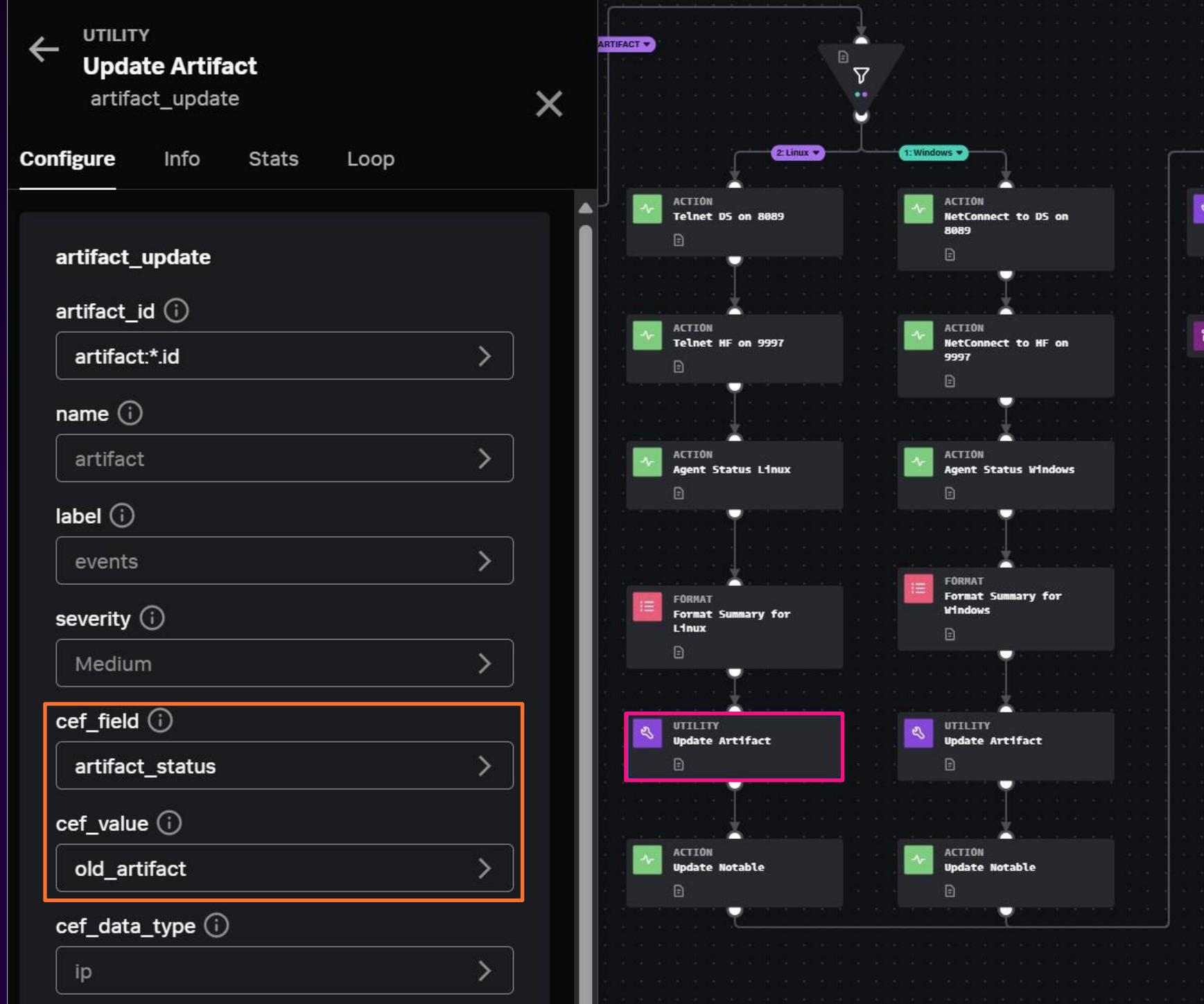


© 2025 SPLUNK LLC

Remote Command Example

Utility Block:
Artifact Update

Add custom field to artifact for future use/ filtering

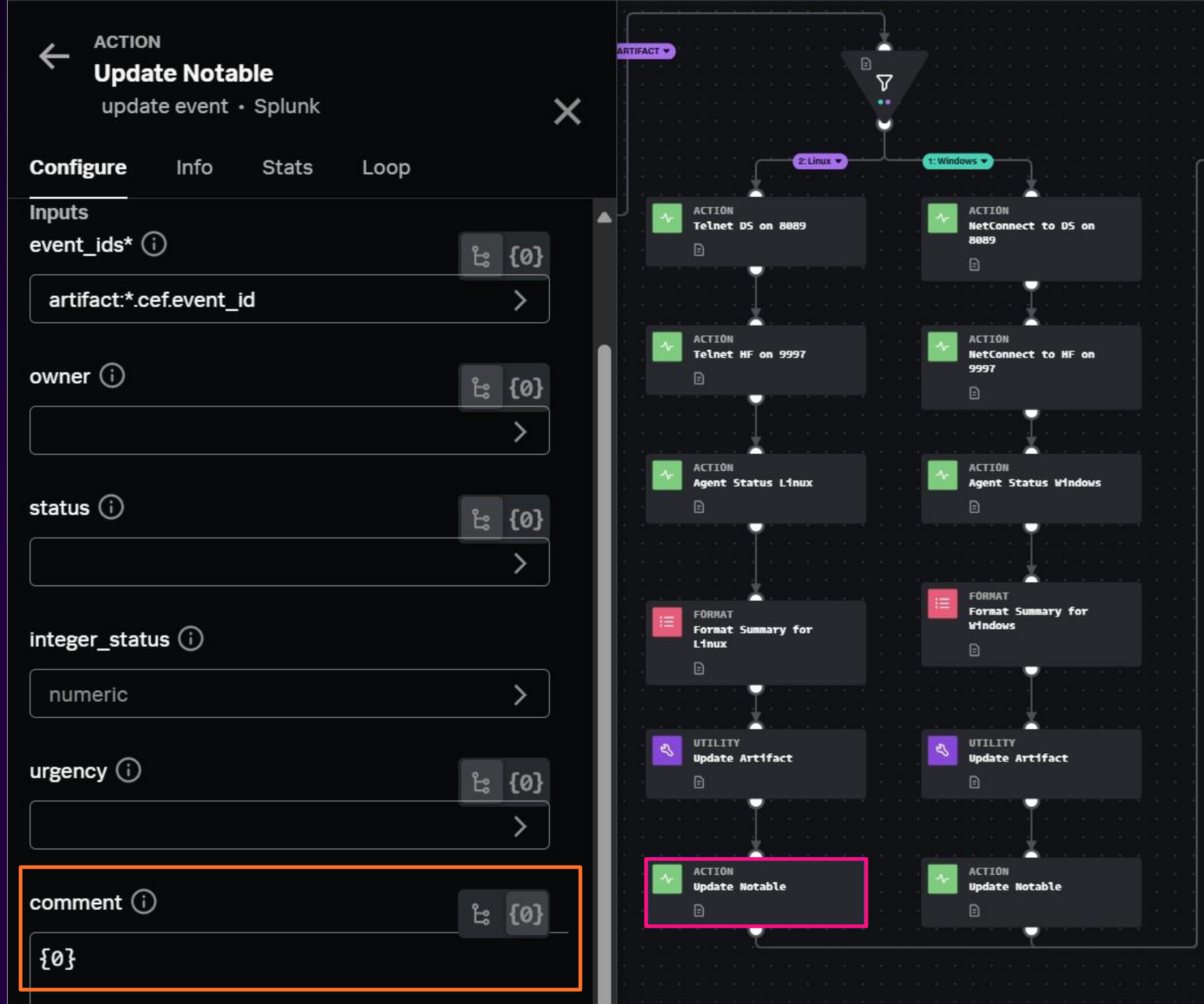


© 2025 SPLUNK LLC

Remote Command Example

Action Block:
Splunk Update Event

Send formatted results to ES as a comment for the analyst to review



© 2025 SPLUNK LLC

Remote Script / Command Execution

Key Takeaways

- Use the underlying Operating System to do the heavy lifting and return results to SOAR
- This initial phase was focused on compliance monitoring and troubleshooting agents
  - However the next phase will reuse this functionality to support automated investigations and incident response
- Consider how you might use these techniques with that in mind
  - Running native OS commands to gather evidence (ps, netstat, etc)
  - Running additional scripts to perform containment functions

© 2025 SPLUNK LLC

Bonus Tips

© 2025 SPLUNK LLC

Bonus Tip

Splunk Lookup Tables within* SOAR!

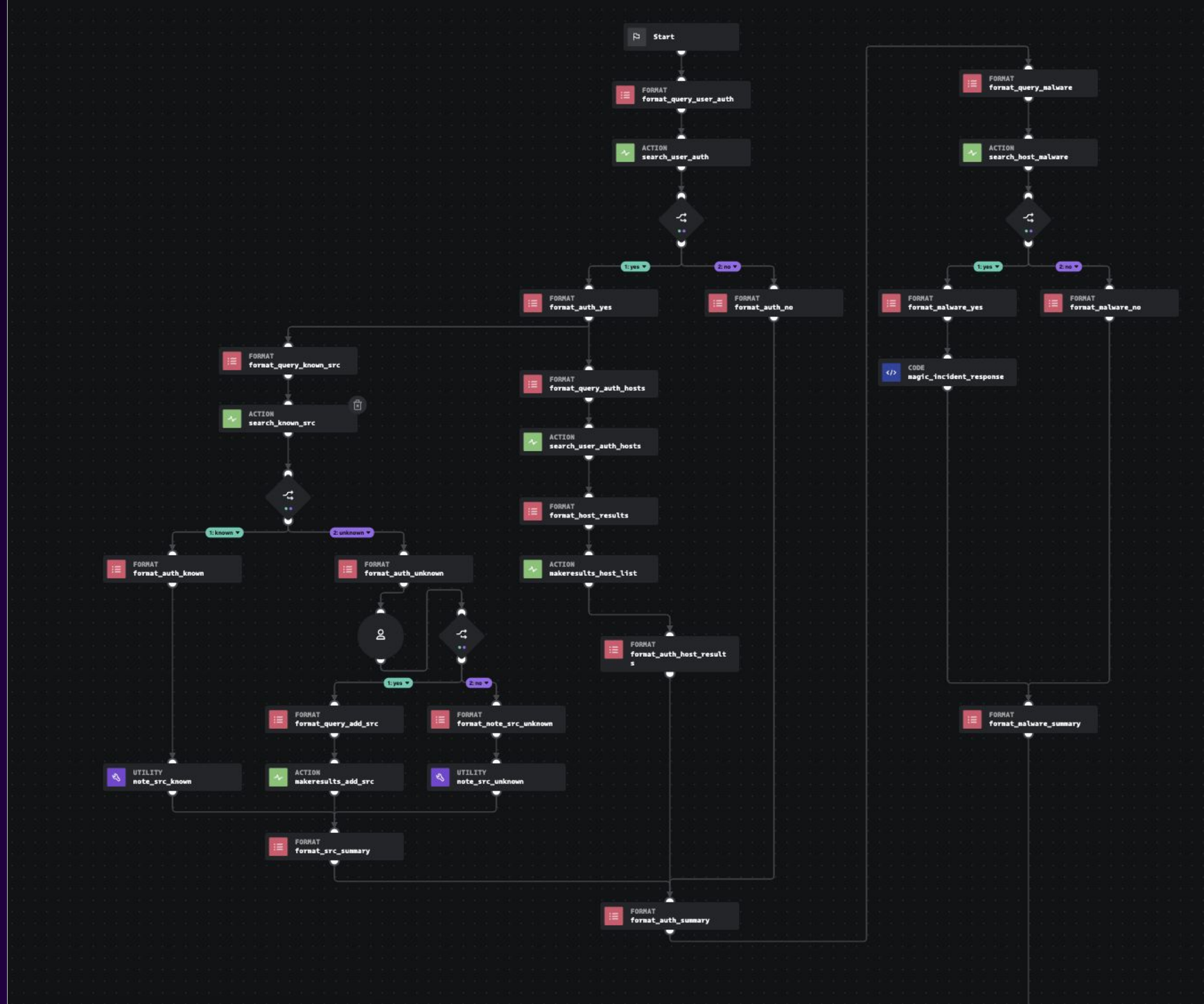
- *“SPL EVAL Functions within* SOAR”* was a fan favorite from our previous talk
  - See slide 40 of our previous talk
  - Lets extend on this, and use it to leverage lookup tables…
- “*This would be so much easier if I could could just use a Splunk Lookup table instead*”
  - Anyone who’s ever had to write python code in SOAR for to manage a custom list…
- SOAR Custom Lists are very powerful, but have limited out of the box functionality
  - Assumes playbook developer will write a custom function in python to handle their data
- What if we cheat and get Splunk to do the heavy lifting for us?

© 2025 SPLUNK LLC

Bonus Tip

Leverage Splunk Lookup Tables via SOAR

Additional branch for our user investigative playbook to check if their source IP(s) are known / trusted…

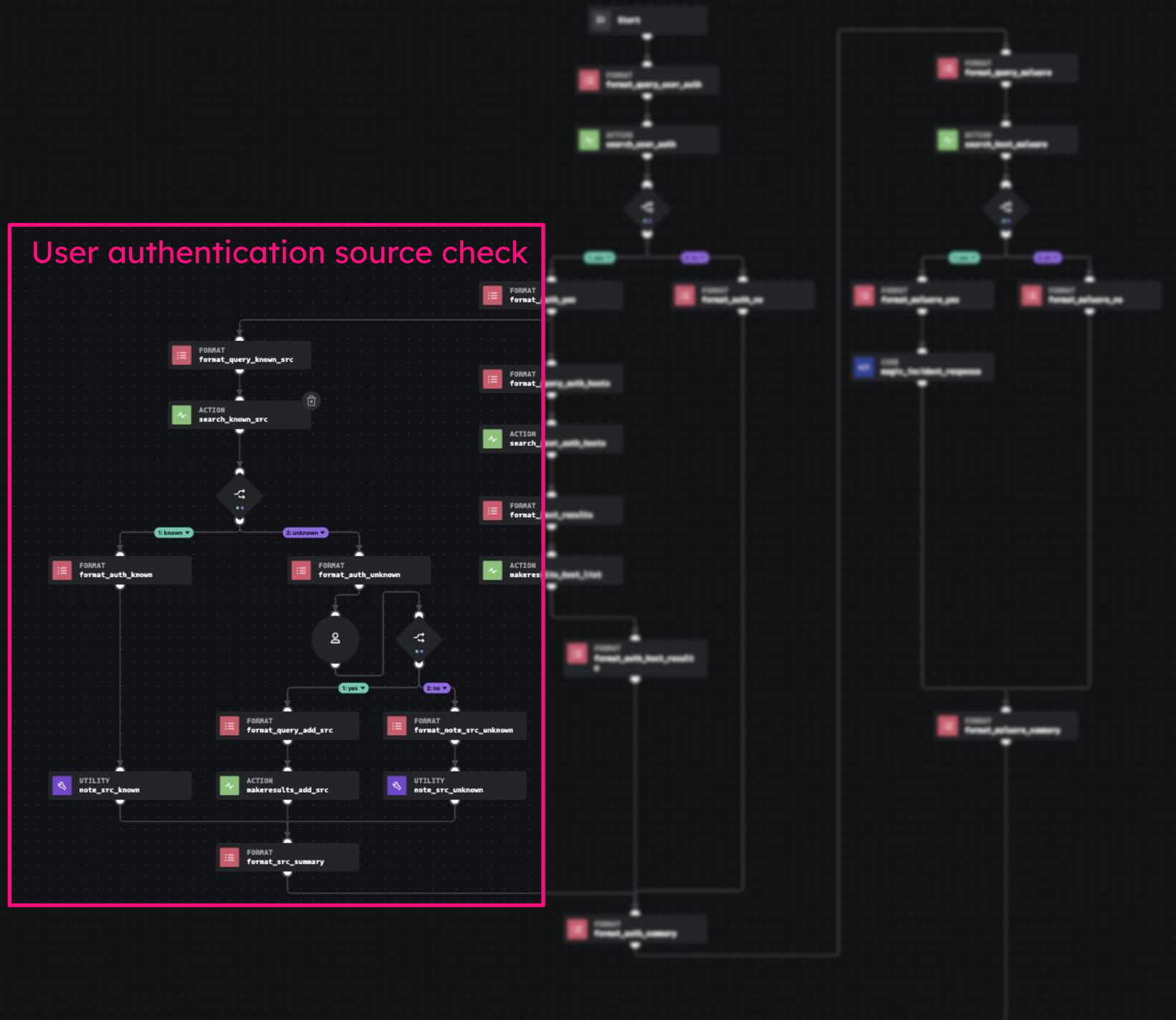


© 2025 SPLUNK LLC

Bonus Tip

Leverage Splunk Lookup Tables via SOAR

Additional branch for our user investigative playbook to check if their source IP(s) are known / trusted…

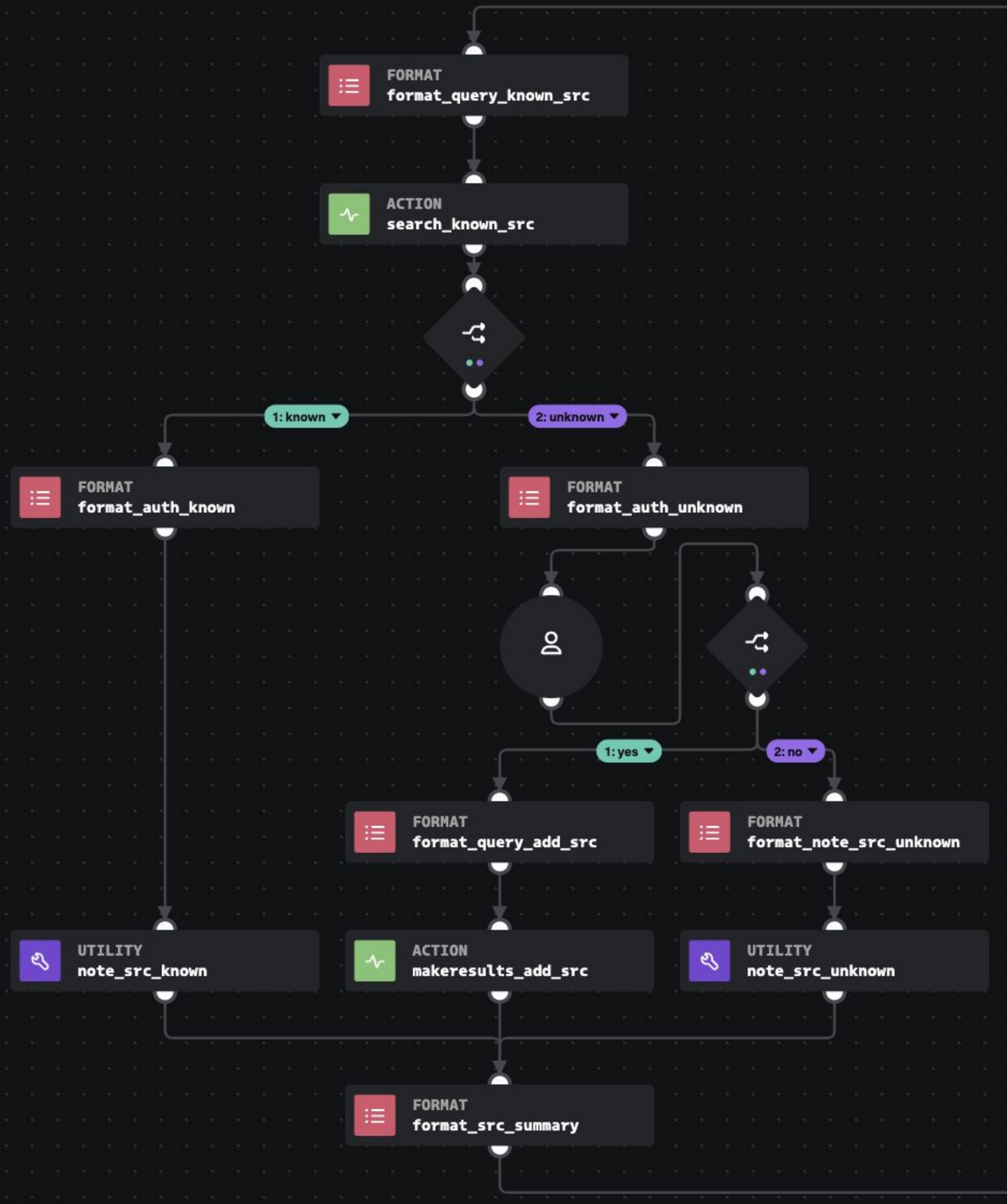


© 2025 SPLUNK LLC

Bonus Tip

Leverage Splunk Lookup Tables via SOAR

Additional branch for our user investigative playbook to check if their source IP(s) are known / trusted…

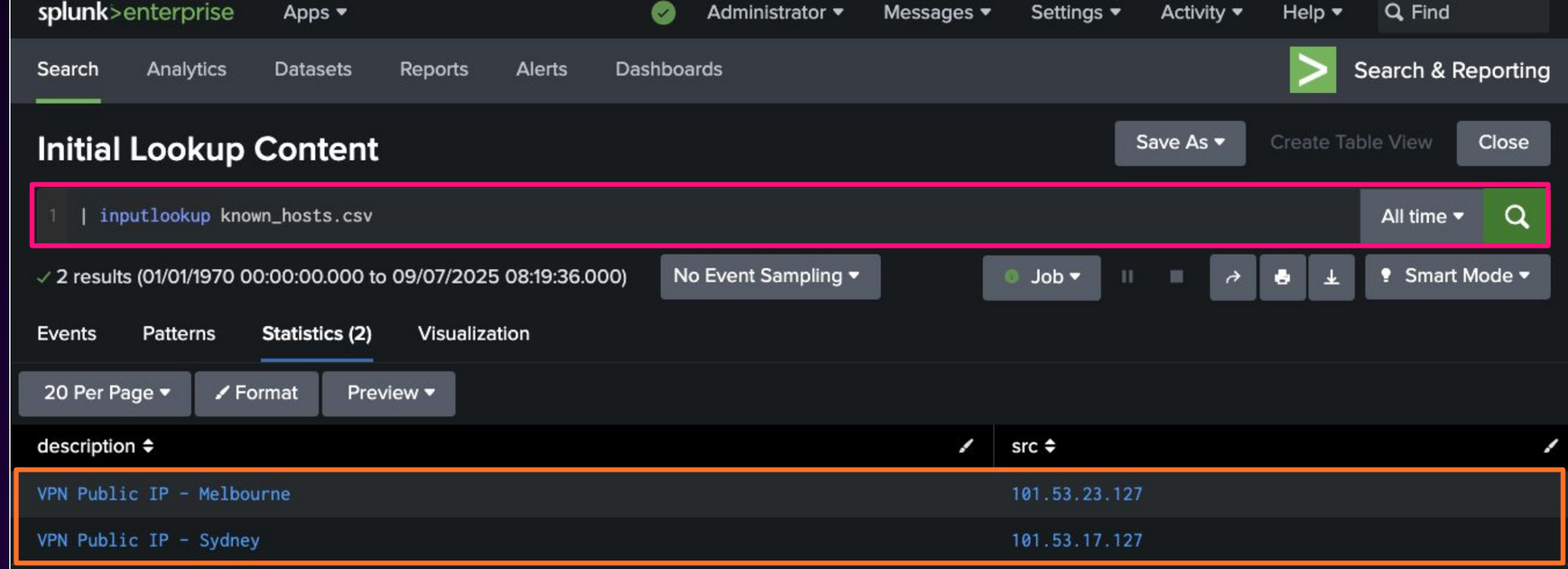


© 2025 SPLUNK LLC

Bonus Tip

Leverage Splunk Lookup Tables via SOAR

… with ‘trust’ based on a lookup table within Splunk, containing an IP address and a description.



© 2025 SPLUNK LLC

Bonus Tip

Leverage Splunk Lookup Tables via SOAR

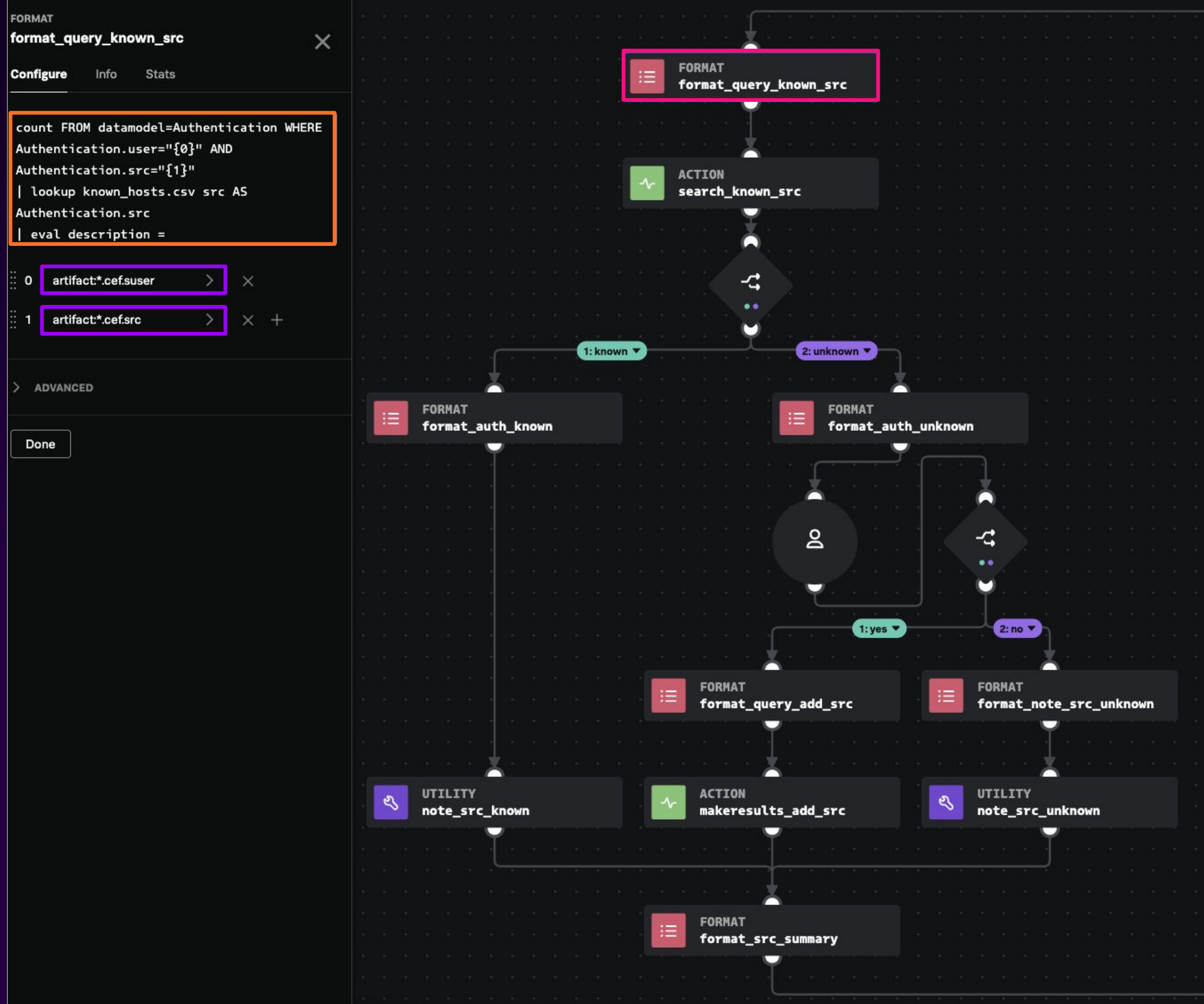
For this talk we'll use two demo containers to step through the example.

© 2025 SPLUNK LLC

Bonus Tip

Leverage Splunk Lookup Tables via SOAR

Format Block:
Write your SPL to search for the users activity, and cross-check against the lookup table.

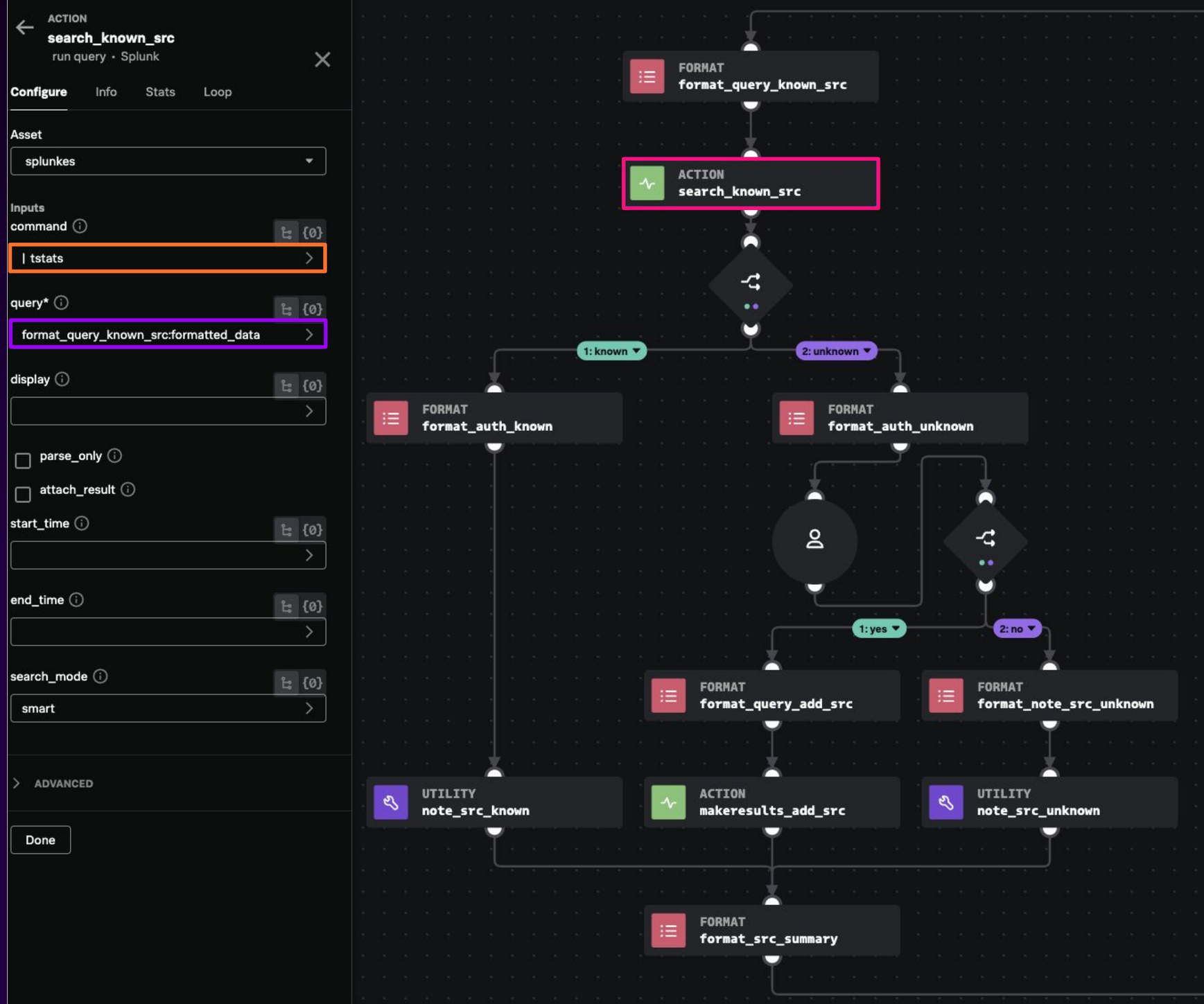


© 2025 SPLUNK LLC

Bonus Tip

Leverage Splunk Lookup Tables via SOAR

Action Block:
Pass this SPL into an action block with a leading | tstats



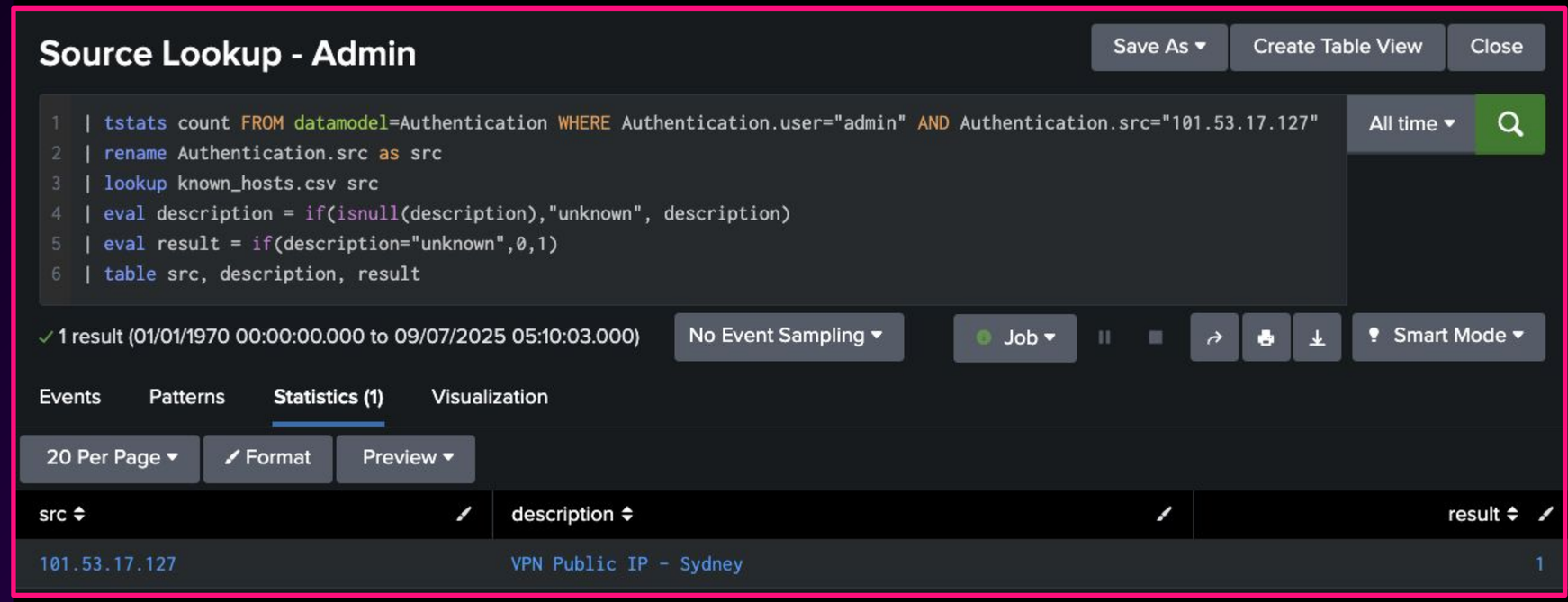
© 2025 SPLUNK LLC

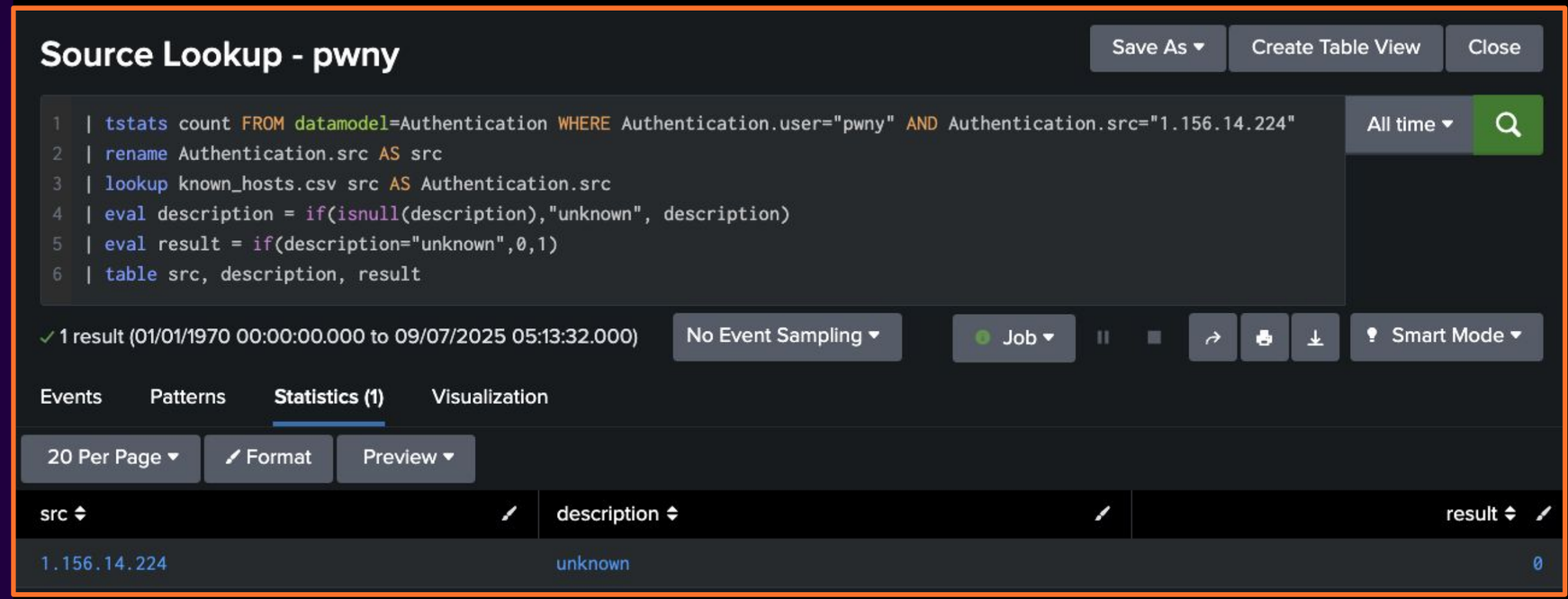
Bonus Tip

Leverage Splunk Lookup Tables via SOAR

Searches for the two users from Splunk's perspective.

Note the result field - this creates a binary condition used by the upcoming decision block.



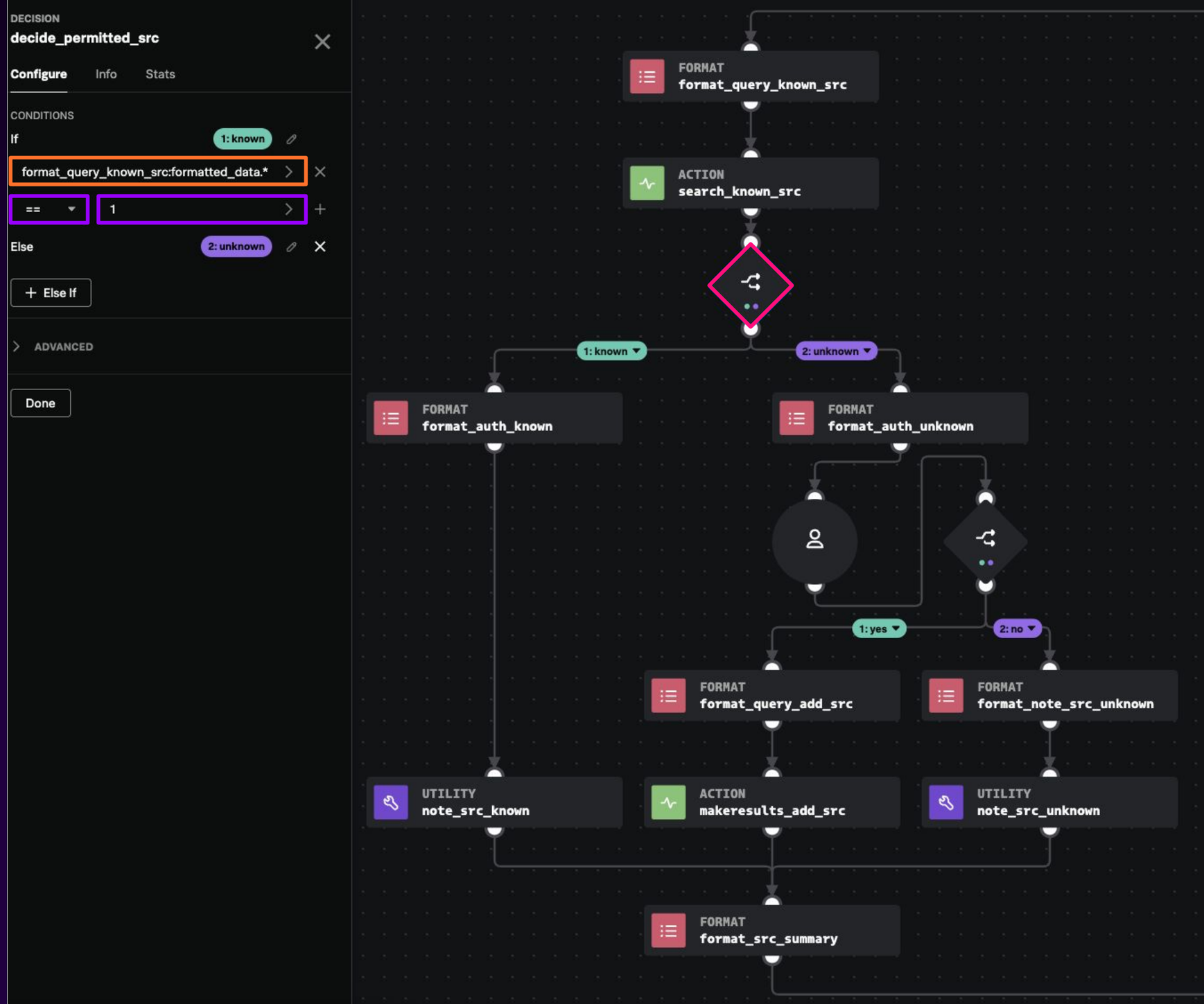


© 2025 SPLUNK LLC

Bonus Tip

Leverage Splunk Lookup Tables via SOAR

Decision Block:
Choose a path based on the result returned

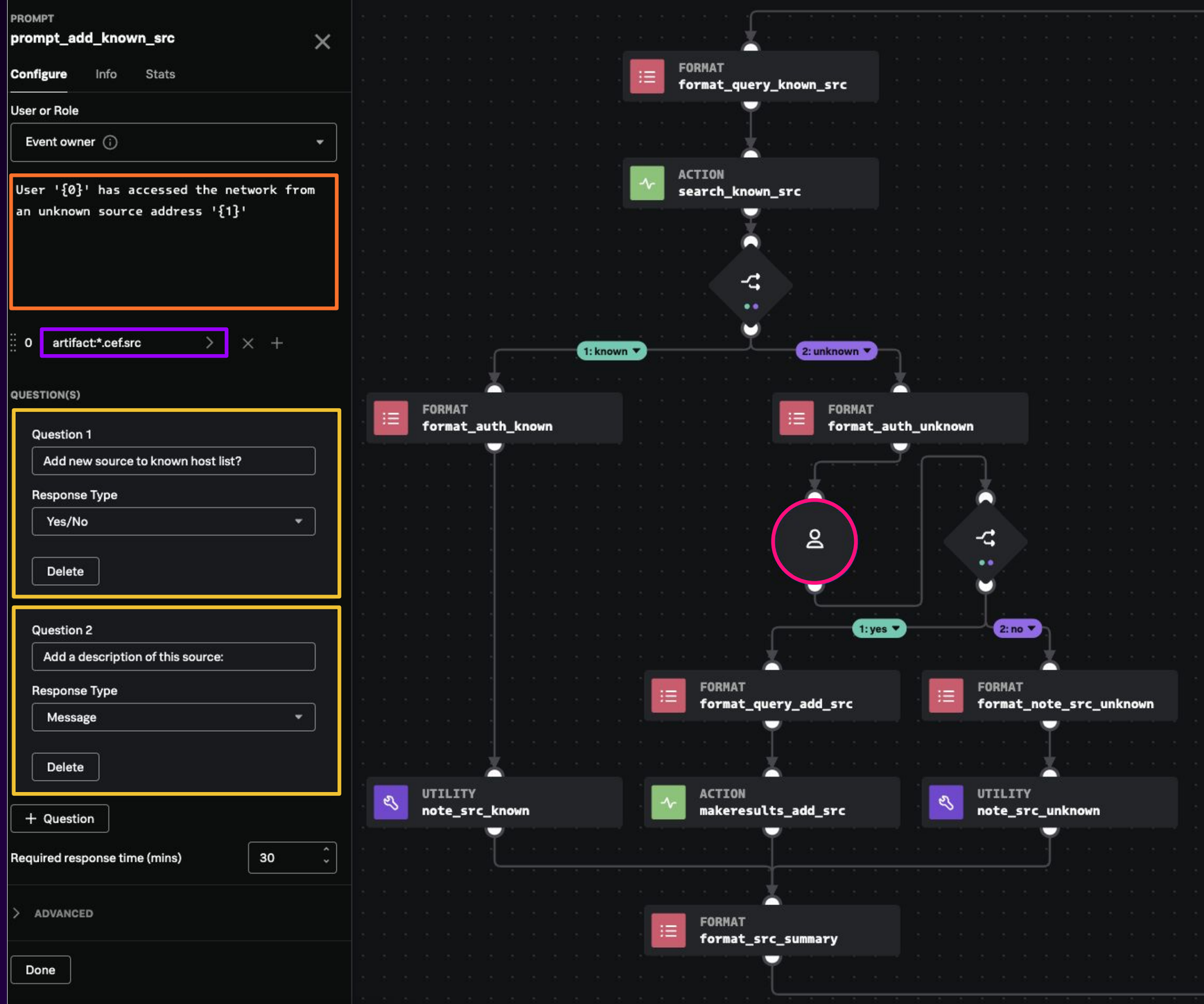


© 2025 SPLUNK LLC

Bonus Tip

Leverage Splunk Lookup Tables via SOAR

Prompt Block:
For unknown sources, have a user review and determine if the source is trusted.

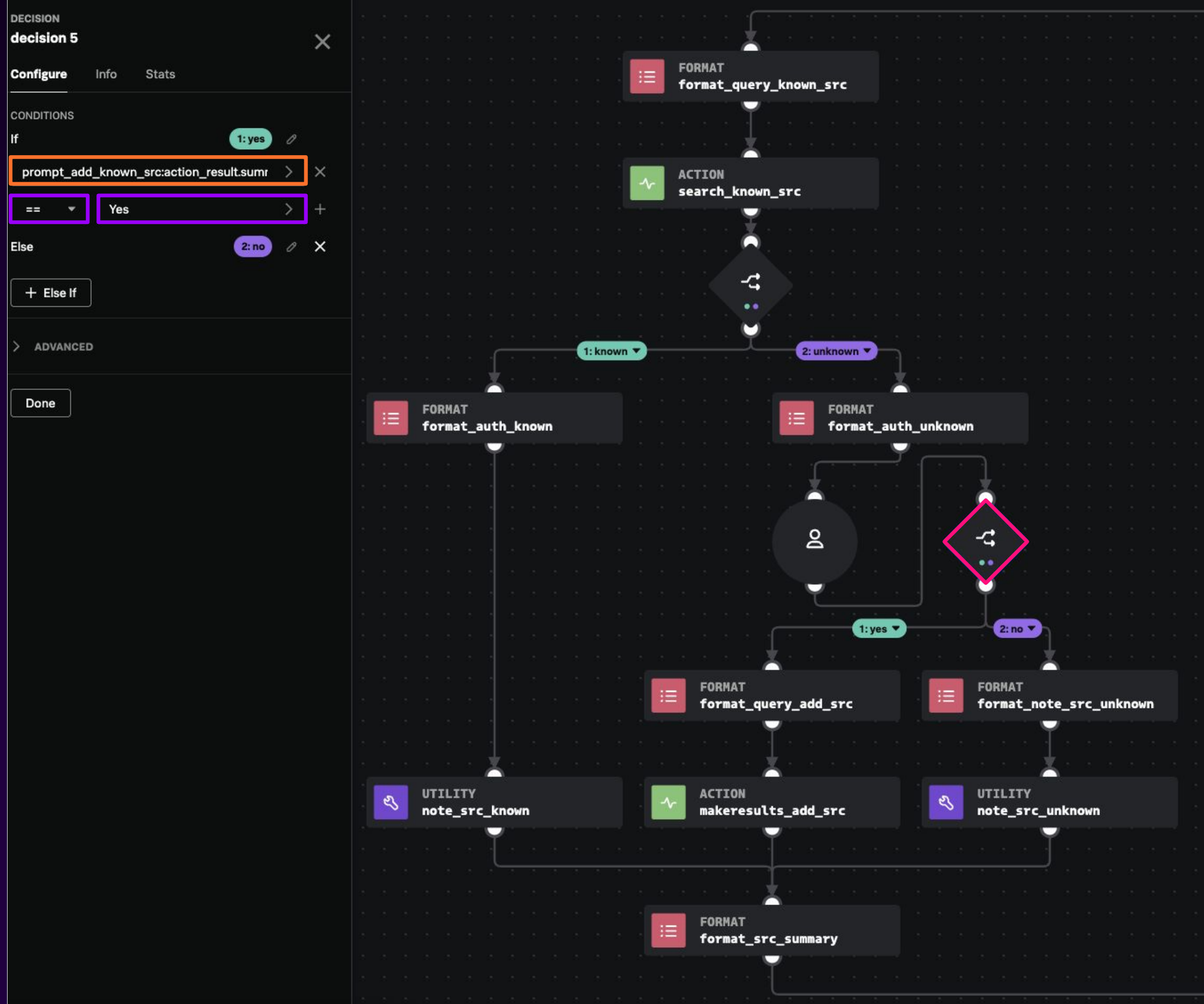


© 2025 SPLUNK LLC

Bonus Tip

Leverage Splunk Lookup Tables via SOAR

Decision Block:
Choose a path based on the prompt response

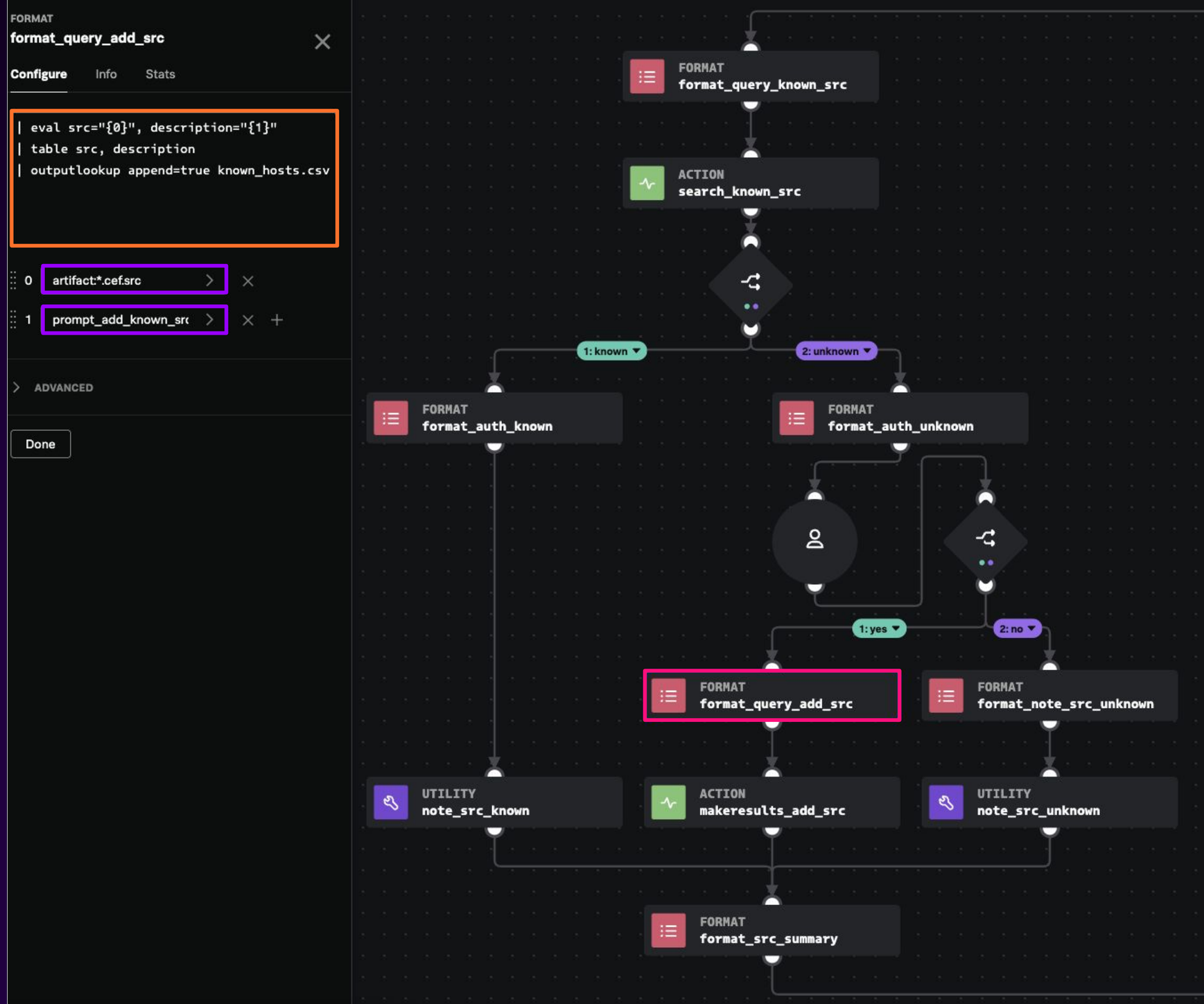


© 2025 SPLUNK LLC

Bonus Tip

Leverage Splunk Lookup Tables via SOAR

Format Block:
Write your SPL to create a search that will output into the lookup table.

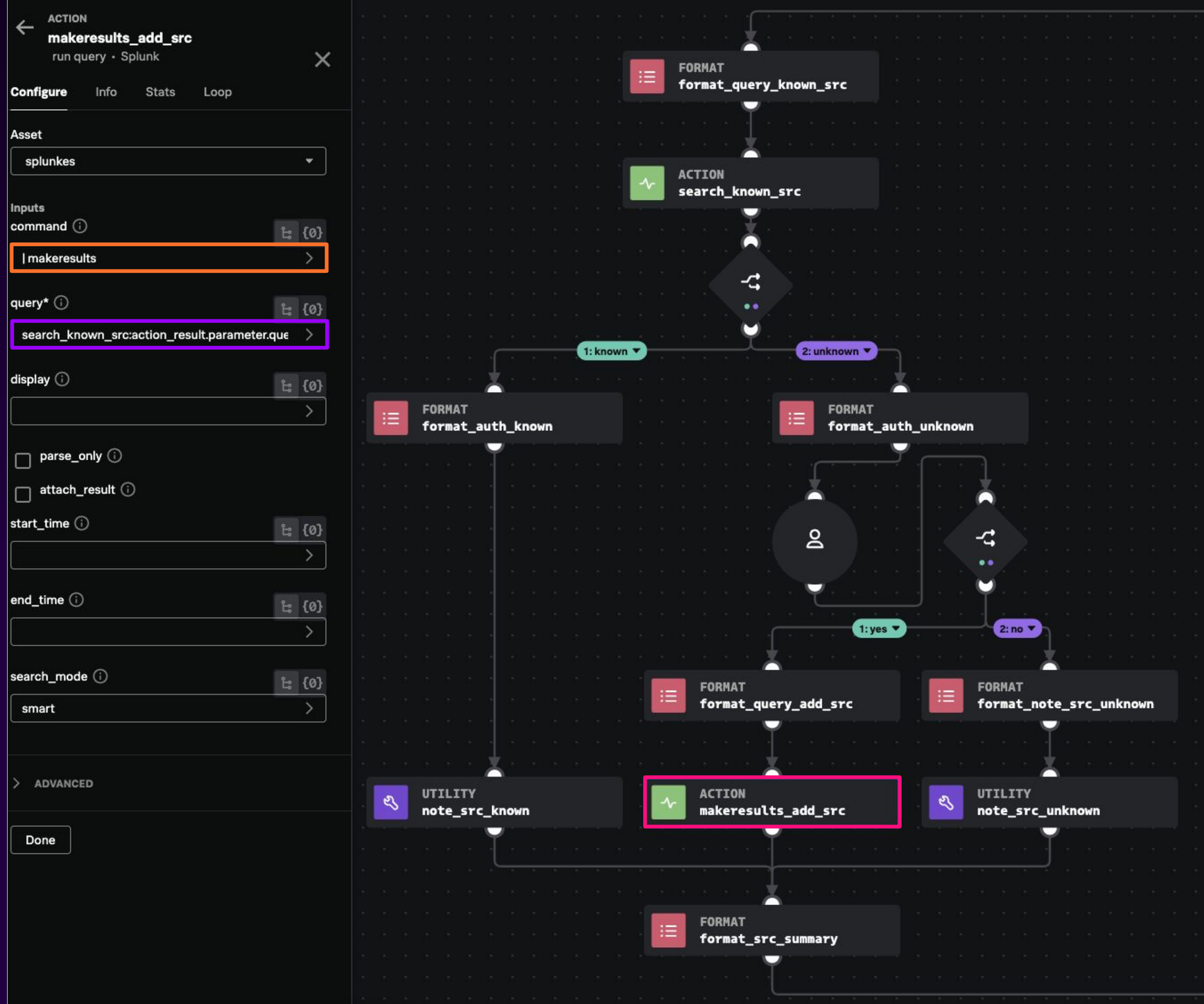


© 2025 SPLUNK LLC

Bonus Tip

Leverage Splunk Lookup Tables via SOAR

Action Block:
Pass this SPL into an action block with a leading | makeresults



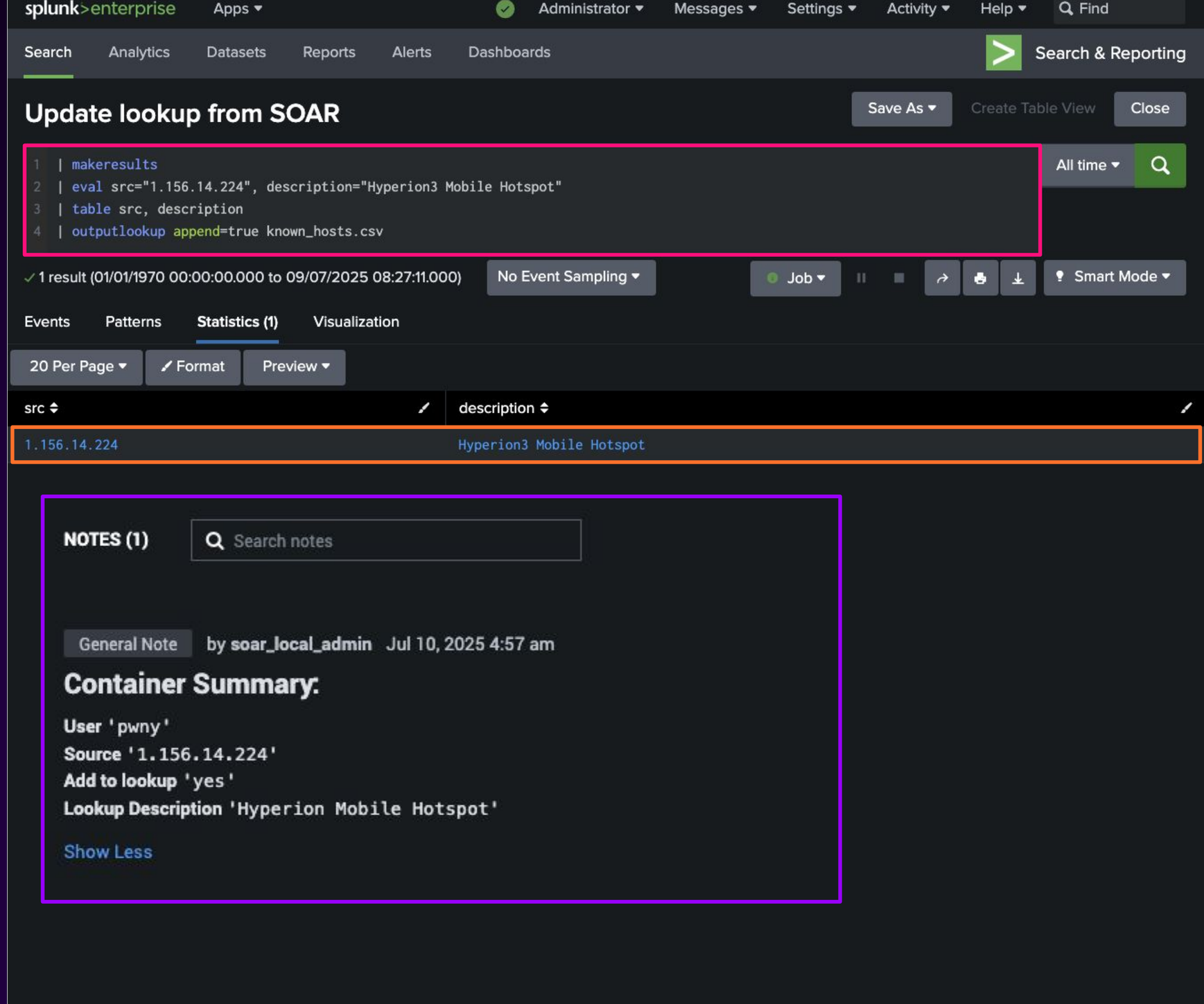
© 2025 SPLUNK LLC

Bonus Tip

Leverage Splunk Lookup Tables via SOAR

Equivalent SPL within Splunk, plus SOAR output via a note:

Data has now been written in a Splunk lookup table from SOAR with zero custom code!

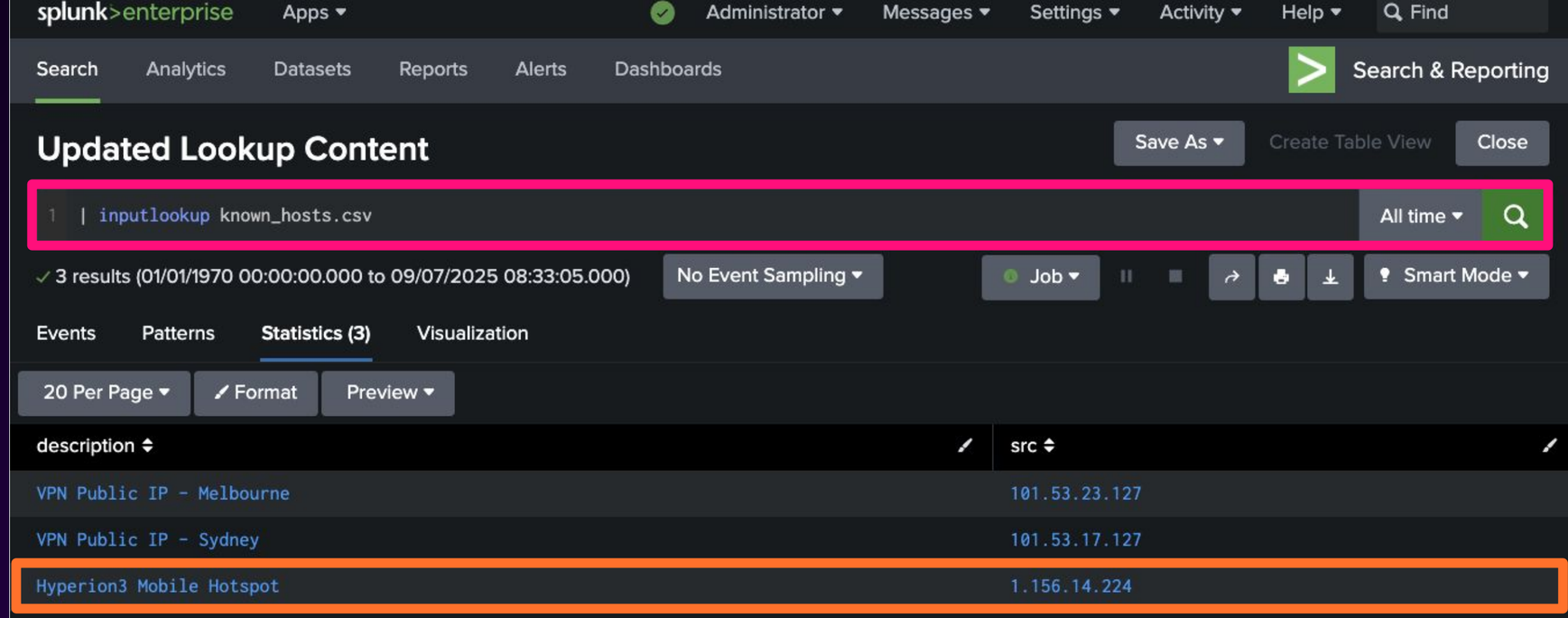


© 2025 SPLUNK LLC

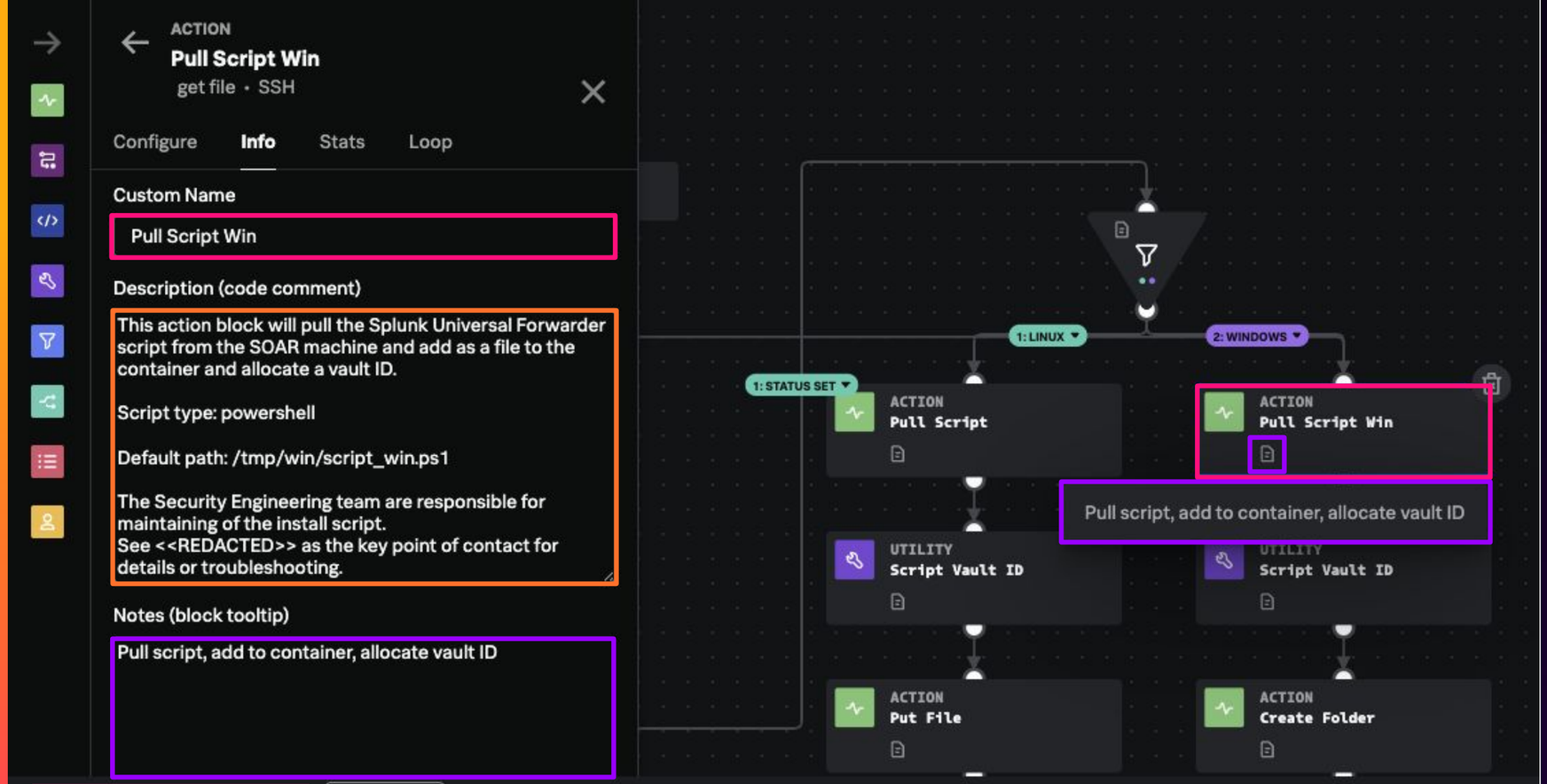
Bonus Tip

Leverage Splunk Lookup Tables via SOAR

Contents of the updated lookup table, showing the new entry from SOAR.



© 2025 SPLUNK LLC



pull_script_win Function Copy

```python
@phantom.playbook_block()
def pull_script_win(action=None, success=None, container=None, results=None, handle=None, filtered_artifacts=None, filtered_results=None
    phantom.debug("pull_script_win() called")

    # phantom.debug('Action: {0} {1}'.format(action['name'], ('SUCCEEDED' if success else 'FAILED')))

    ################################################################################
    # This action block will pull the Splunk Universal Forwarder script from the SOAR
    # machine and add as a file to the container and allocate a vault ID.
    #
    # Script type: powershell
    #
    # Default path: /tmp/win/script_win.ps1
    #
    # The Security Engineering team are responsible for maintaining of the install
    # script.
    # See <<REDACTED>> as the key point of contact for details or troubleshooting.
    #
    ################################################################################

    parameters = []
```

Bonus Tip

Documentation as Code

Save time by documenting automation as you build!

- Set a custom name to each block, this defines the function name
- Add a detailed description to each block, this becomes living documentation within the code
- Configure a note, this provides a tooltip to assist development / code reuse / debugging

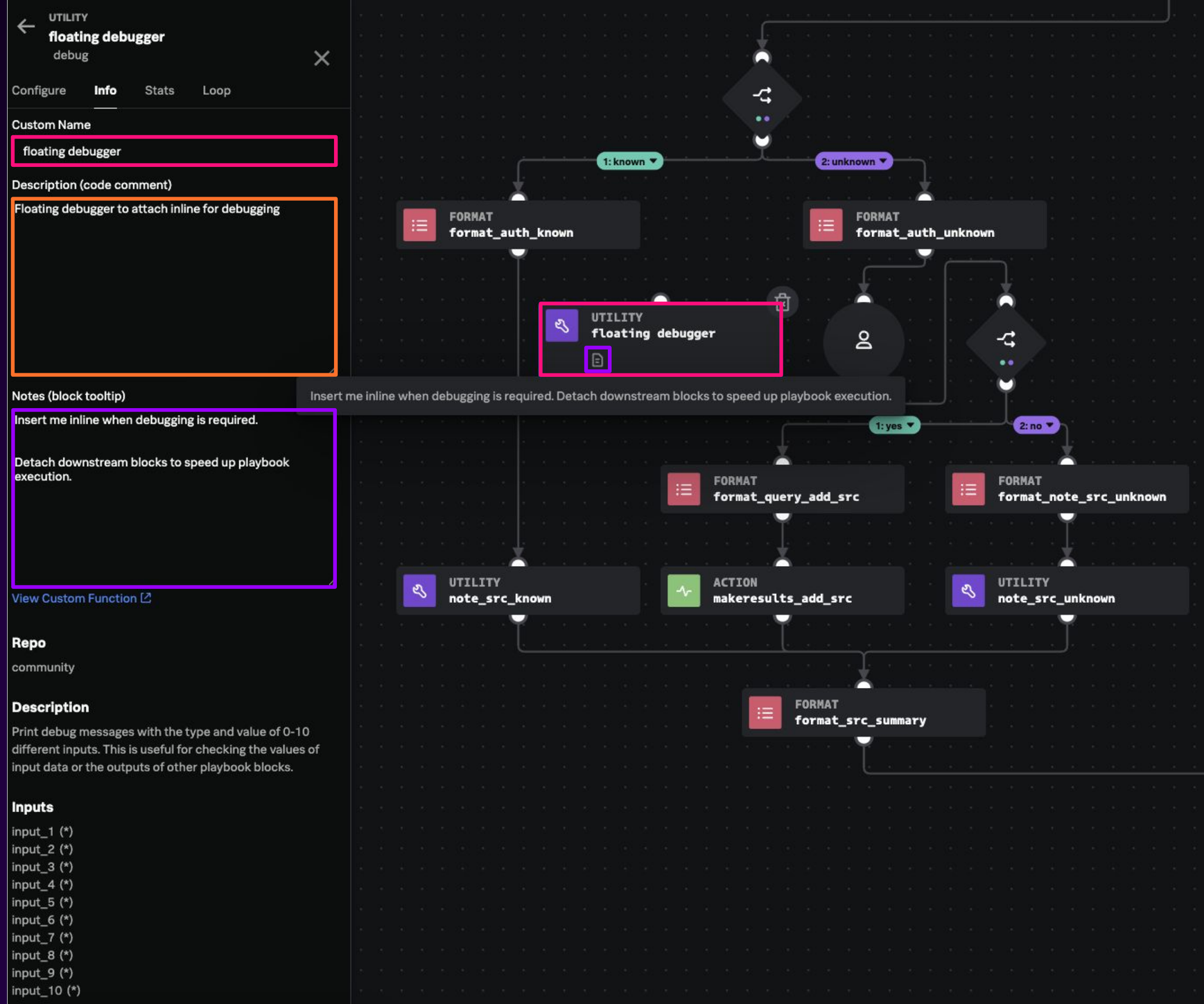
© 2024 SPLUNK INC.

Bonus Tip

Floating Debugger

Keep a ‘floating debugger’ close to wherever you are actively developing a playbook.

Name, description, and notes as per good coding practices.

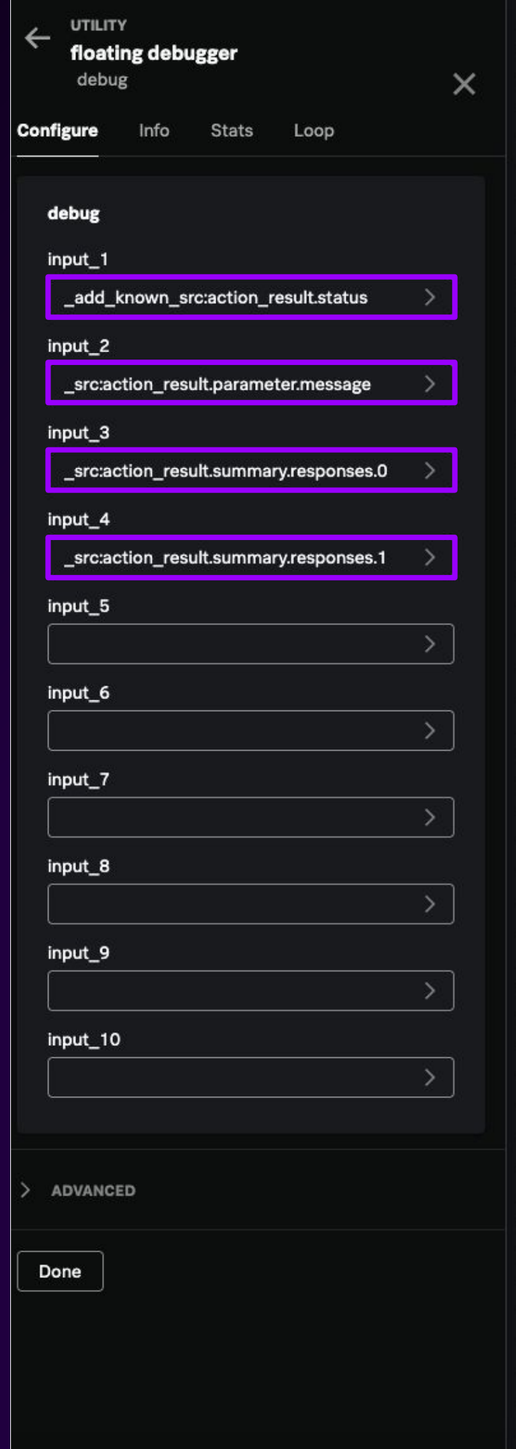


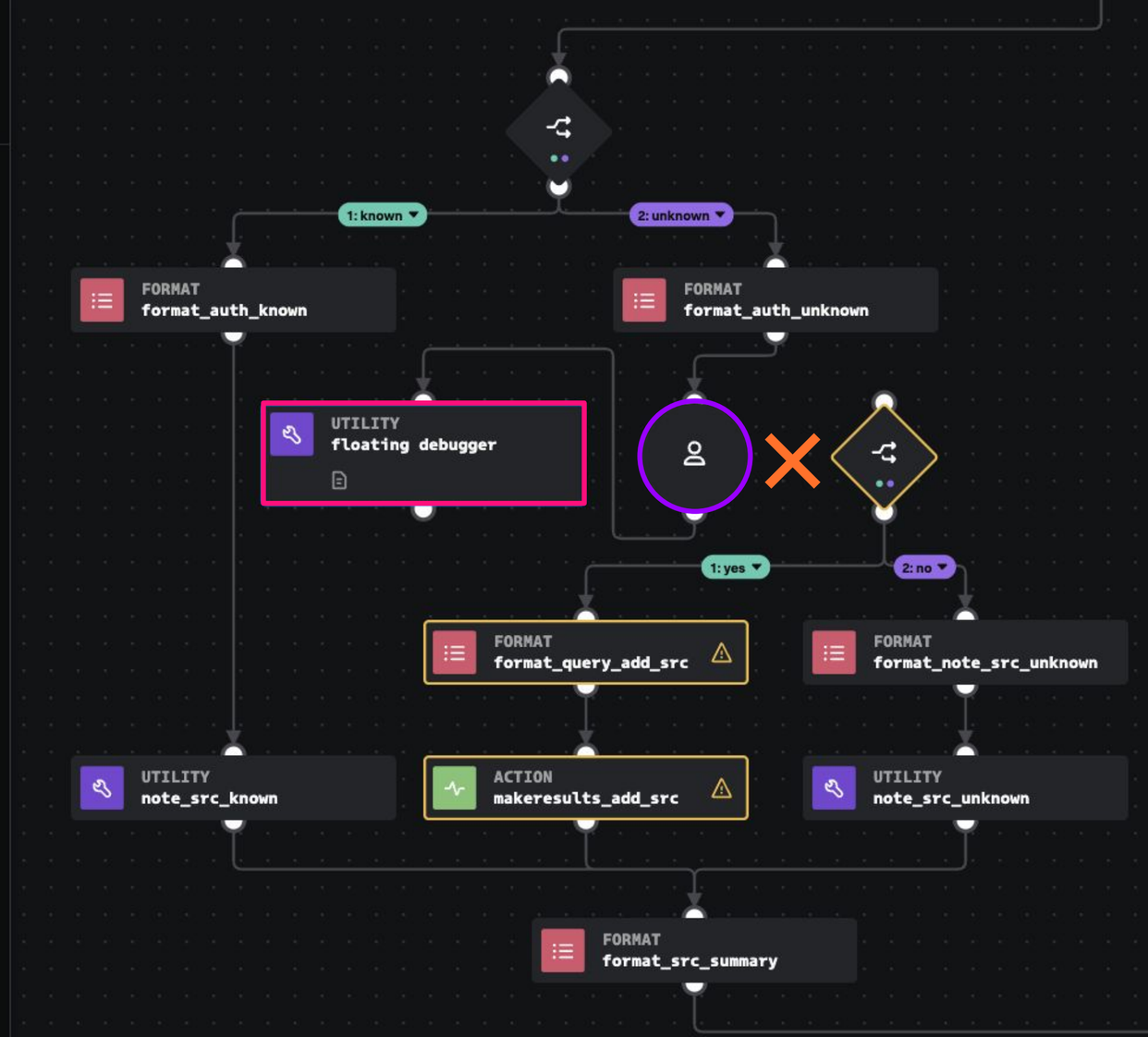
© 2025 SPLUNK LLC

Bonus Tip

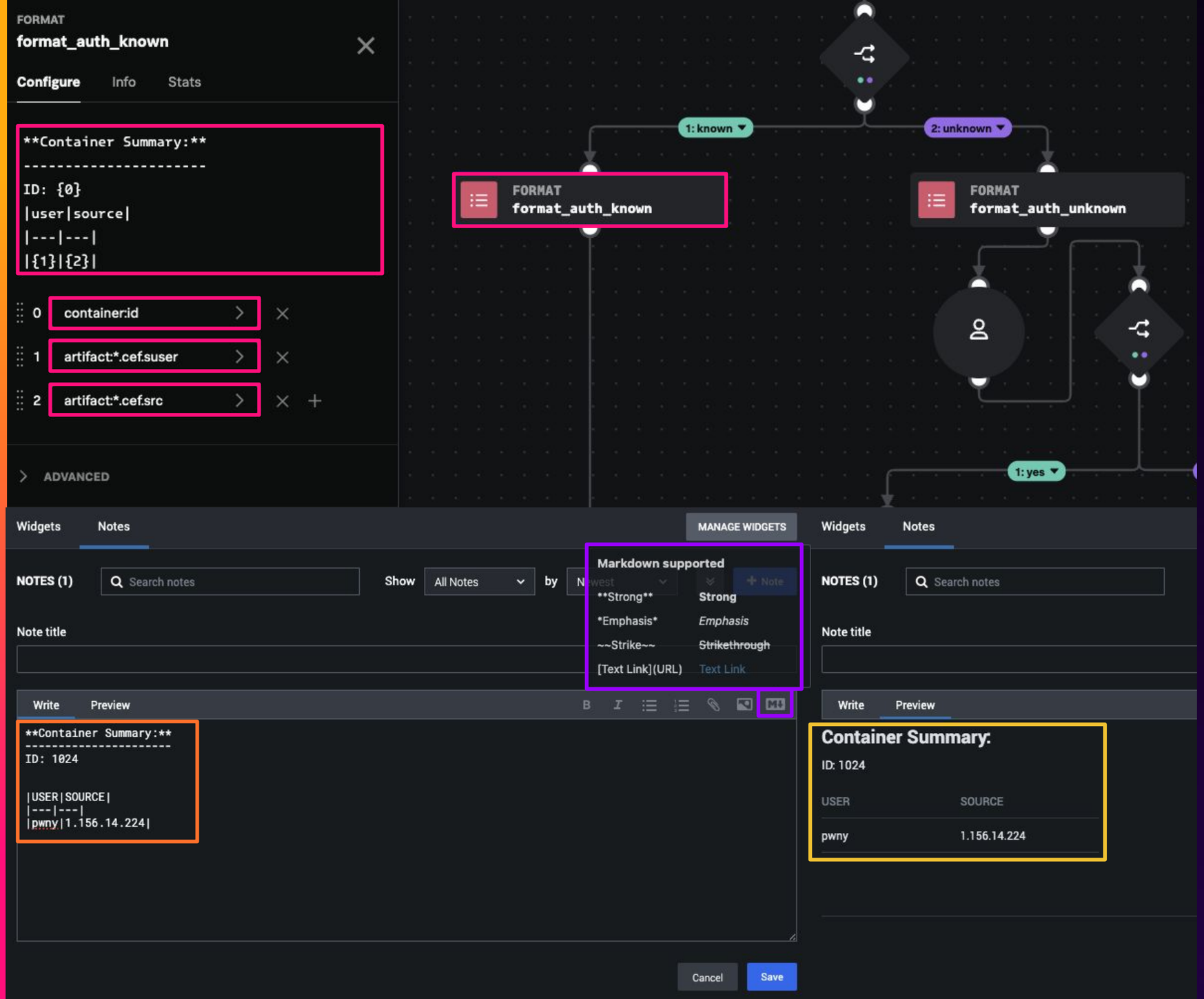
Floating Debugger

- Connect in-line when running the playbook debugger
- Disconnect downstream blocks to speedup execution
- Add up inputs in bulk in order to locate the fields relevant to your playbook





© 2025 SPLUNK LLC



Bonus Tip

Markdown Formatting

- Format blocks support markdown input, allowing for text formatting / tables
- The same applies for notes, where you can even insert images!
- Use the inbuilt markdown cheatsheet to get started
- Use note preview to test and adjust

© 2024 SPLUNK INC.

Wrap Up

Today we covered

- Refresher of some Part 1 content
- Example of out of the box thinking
- Example of remote code/script execution
- Tips and good practice

Watch Part 1 if you missed it!

© 2025 SPLUNK LLC

Hyperion3 SOAR
Git Repo

https://github.com/MattHyp3/Hyperion3_SOAR

© 2025 SPLUNK LLC

Questions?

Mic is open!

Or, come and see us afterwards / reach out to us at:

rich@splunk.com
matt@hyperion3.com.au

Thank you

© 2025 SPLUNK LLC