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> .conf22

Ready, Set, SOAR: How Utility Apps Can Up Level Your Playbooks!

SEC1700C

Daniel Federschmidt

Forward Deployed Software Engineering | Splunk

Erica Pescio

Forward Deployed Software Engineering
Splunk

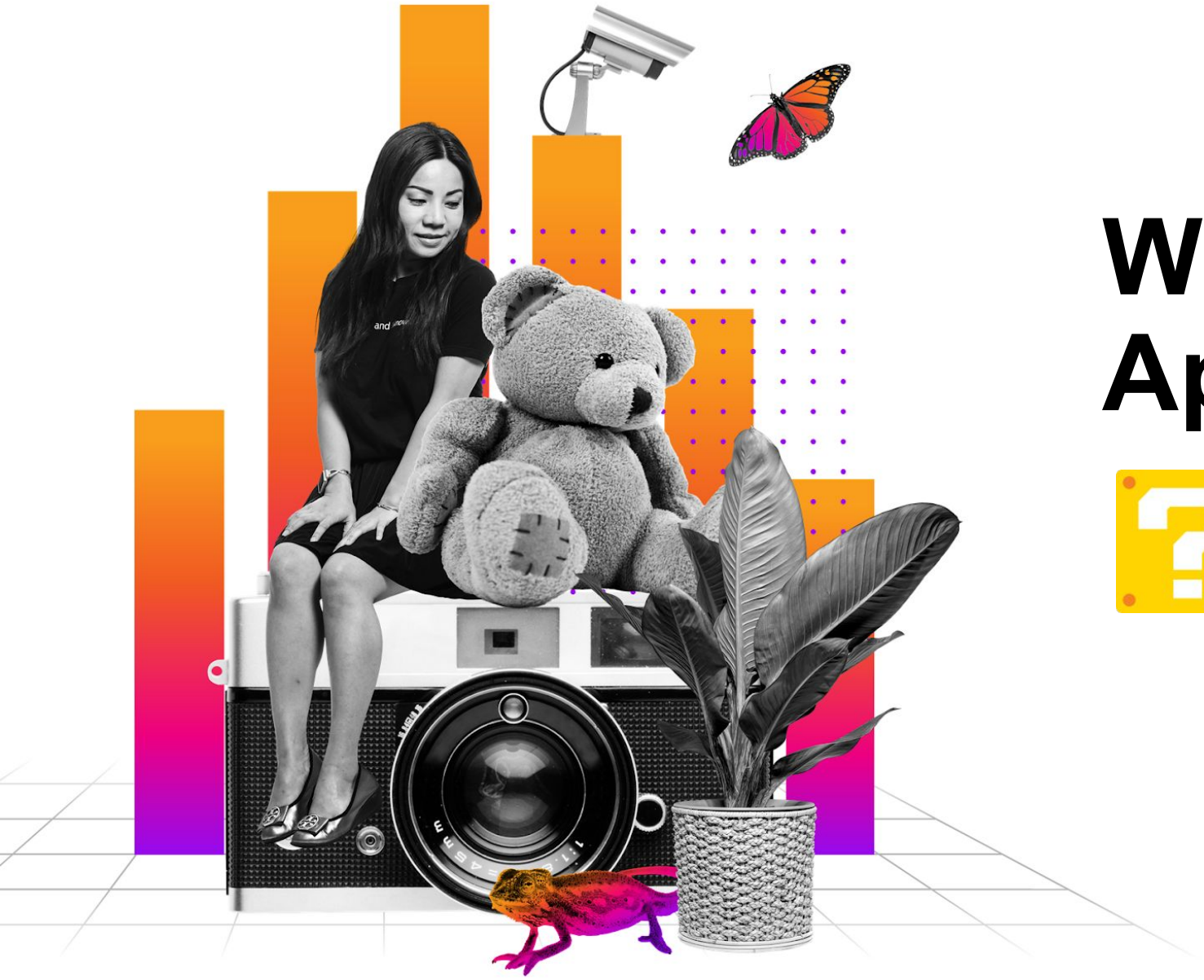
Daniel Federschmidt

Forward Deployed Software Engineer | Splunk

Erica Pescio

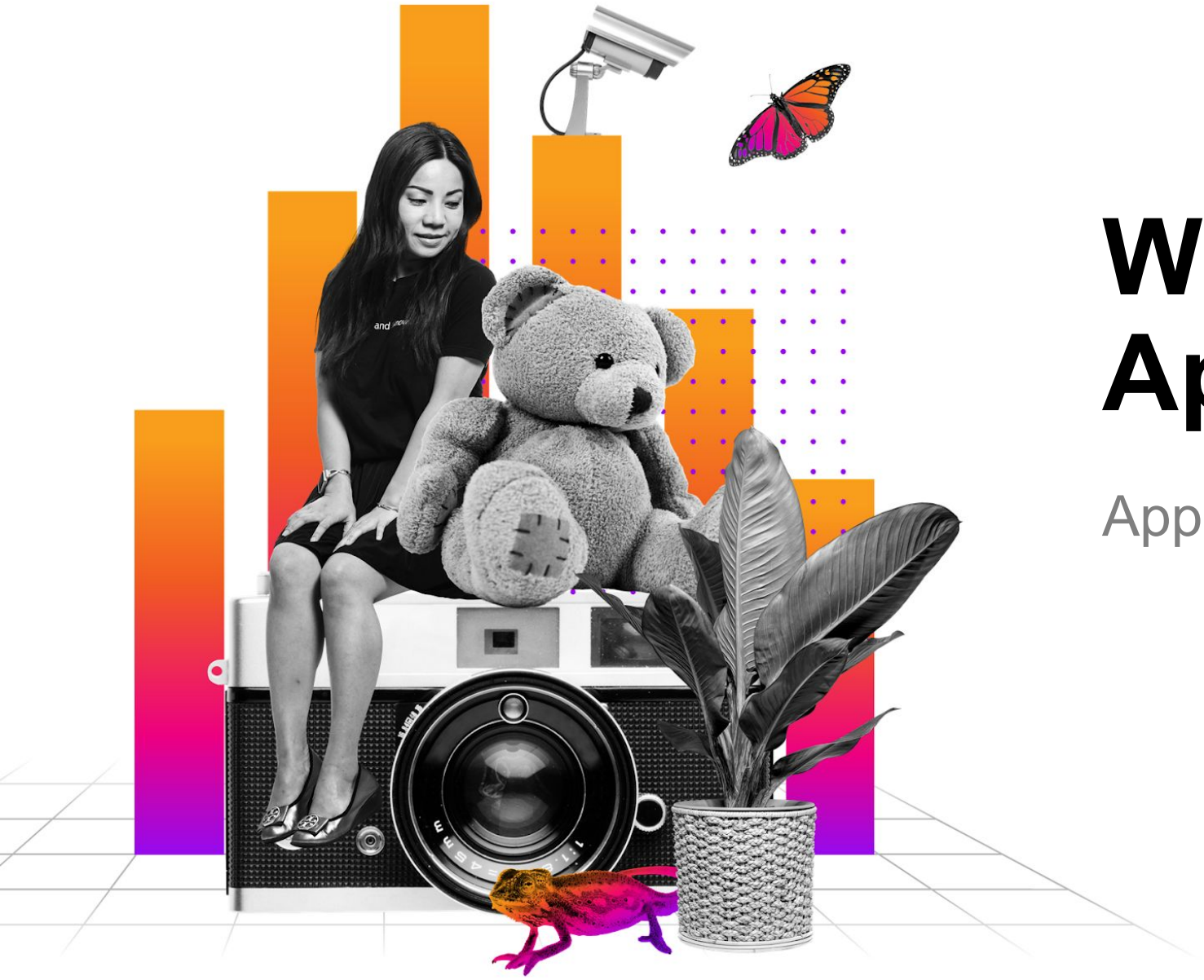
Forward Deployed Software Engineer | Splunk

splunk> .conf22



What Are Utility Apps?

splunk> .conf22



What Are Utility Apps?

Apps that do **more**

splunk> .conf22

SOAR Apps

350+ SOAR Apps on Splunkbase

Most apps integrate with a single remote API

- Crowdstrike OAuth
- VirusTotal v3
- Splunk

Utility Apps do more than that!

- Generic across APIs
- Advanced data processing
- May or may not wrap an existing utility

Think beyond integration with 3rd party systems!

splunk> .conf22

And Custom Functions?

Utility Apps

- Secret management
- Generic across use cases
- Natural grouping of related logic in actions

Custom Functions

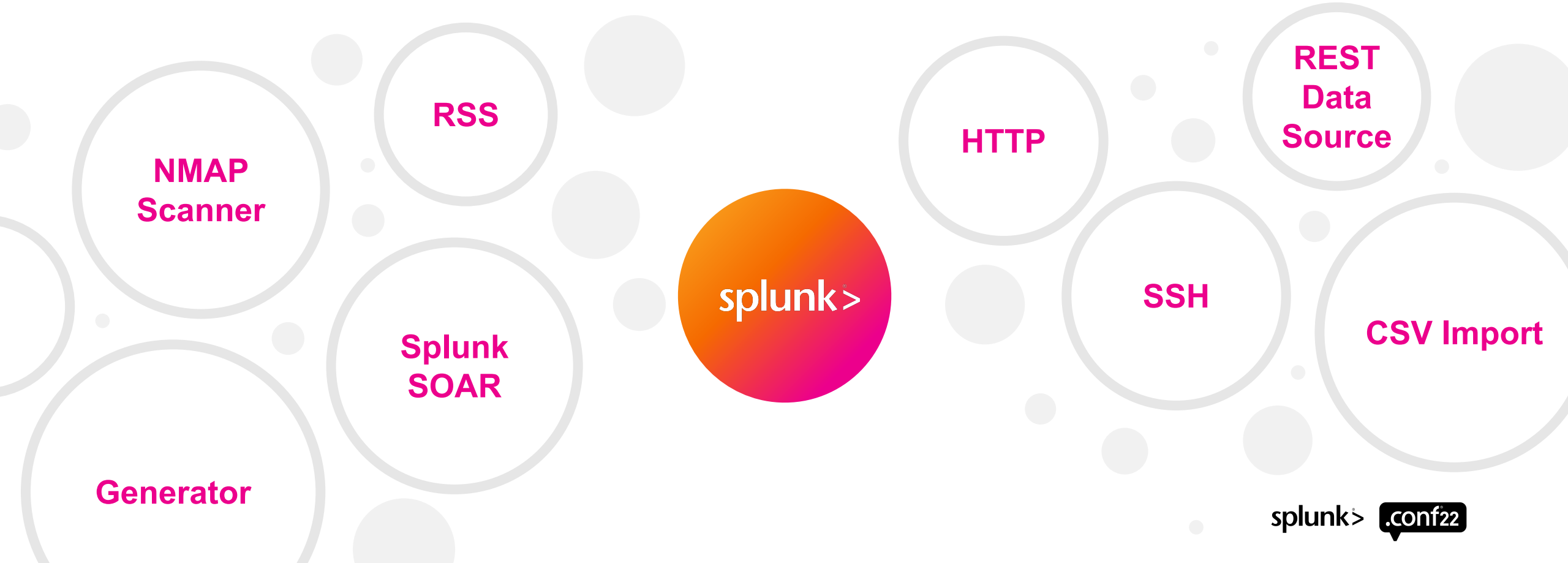
- No secrets to be managed
- Use-case specific data transformation
- Grouping by convention (prefix, tags,...)

Your Favs & Our Favs

What Utility Apps do we have?

splunk> .conf22

Popular Utility Apps



Our Top 3 Utilities in SOAR

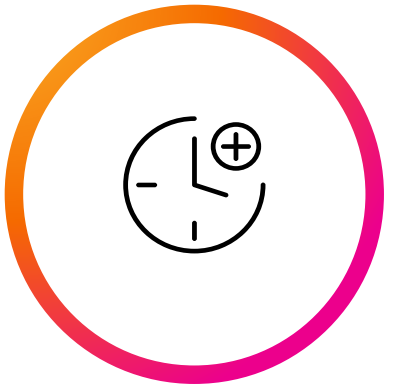
Splunk® SOAR

Exposes Splunk® SOAR APIs as actions

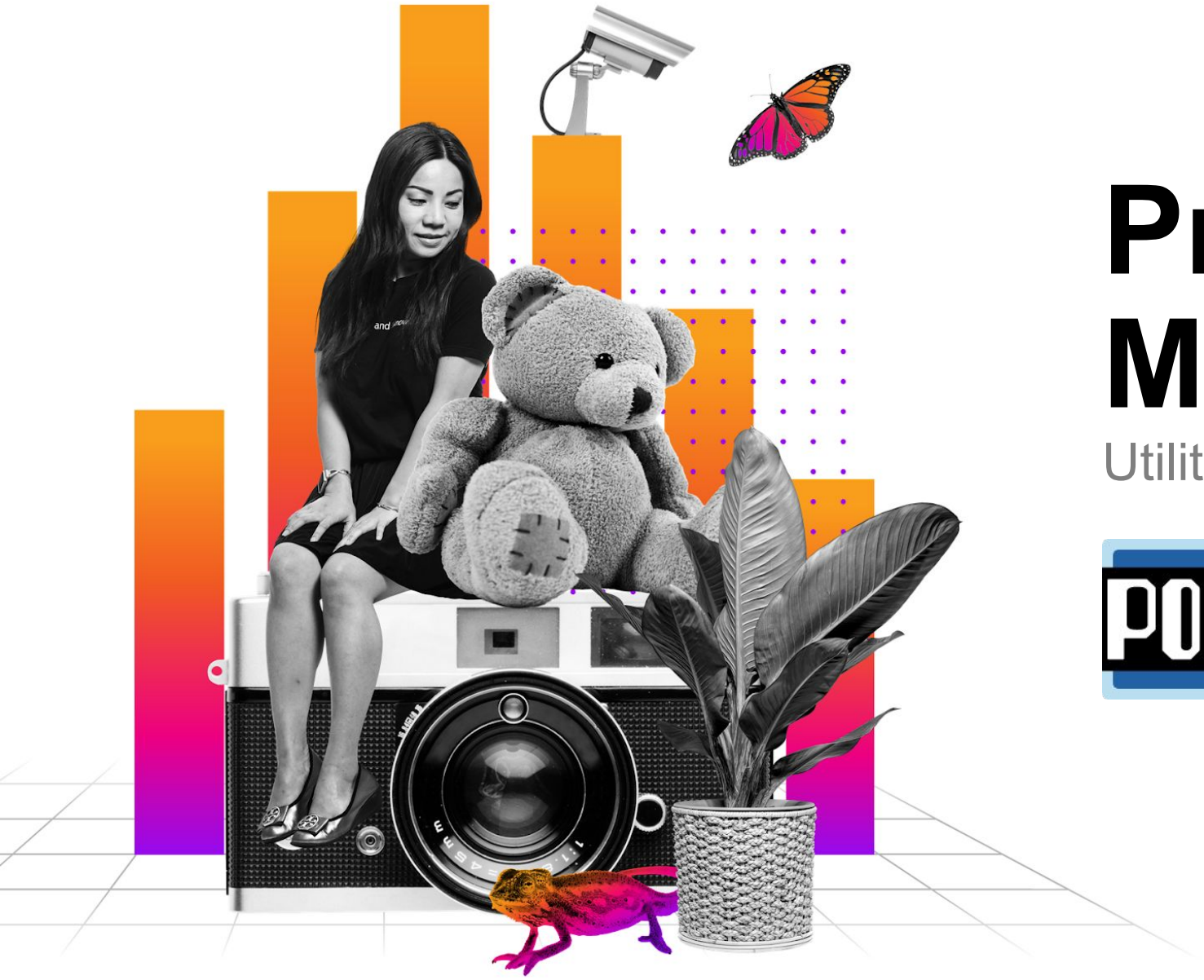
Parser

Extracts IOCs from various file formats

Timer



Kicks playbooks at scheduled intervals



Practice Makes Perfect

Utility Apps in action!

splunk> .conf22

Buttercup Games

Gaming Company

(Fictional)

Welcome to Buttercup Games

The Security team at Buttercup Games must provide a record time solution for these **3 scenarios**

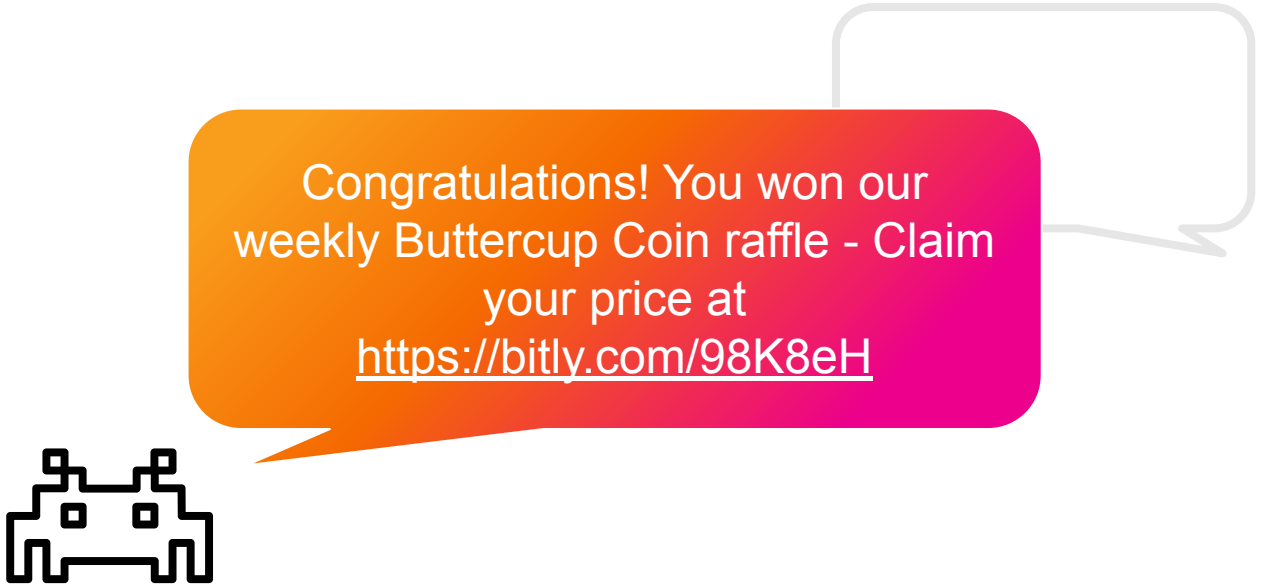
1. Tackle **phishing** through in-game chat
2. Onboard new **alert** sources
3. Improve **reporting** capabilities

Their knowledge of the Splunk® SOAR ecosystem and their playbook development skills will help them through these challenges

Phishing through in-game chat

Scenario 1

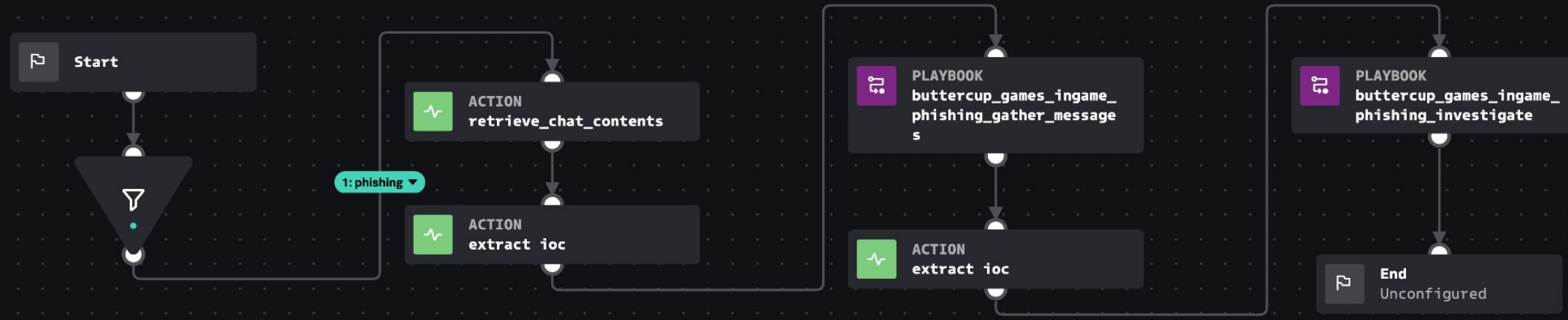
Malicious actors try to steal digital currency via in-game chat. The security team needs a way to triage and enrich reported messages.



Utility Apps

Parser

HTTP



Fetch chat content via HTTP App and save to Vault

Use the Parser to extract message artifacts from CSV

Collect CSV details as artifacts

Extract URL IOCs on added artifacts

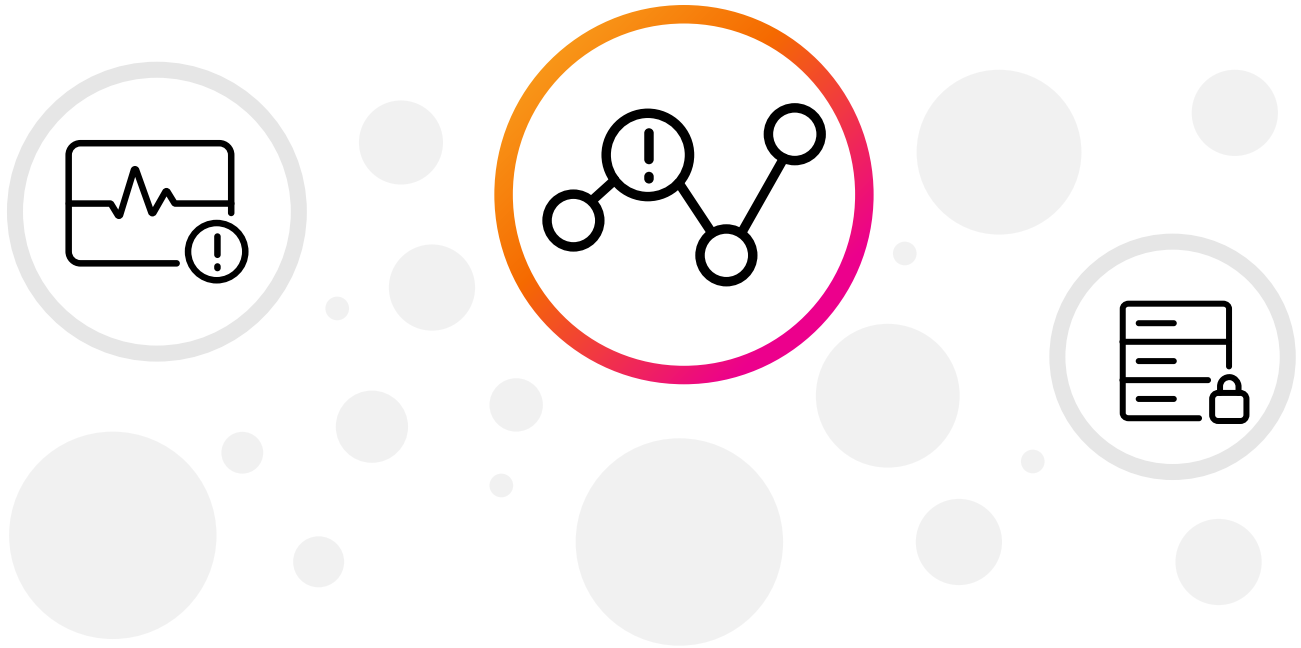
Run phishing investigation playbook

Notify analysts of potentially malicious URLs and further actions

Onboard new alert sources

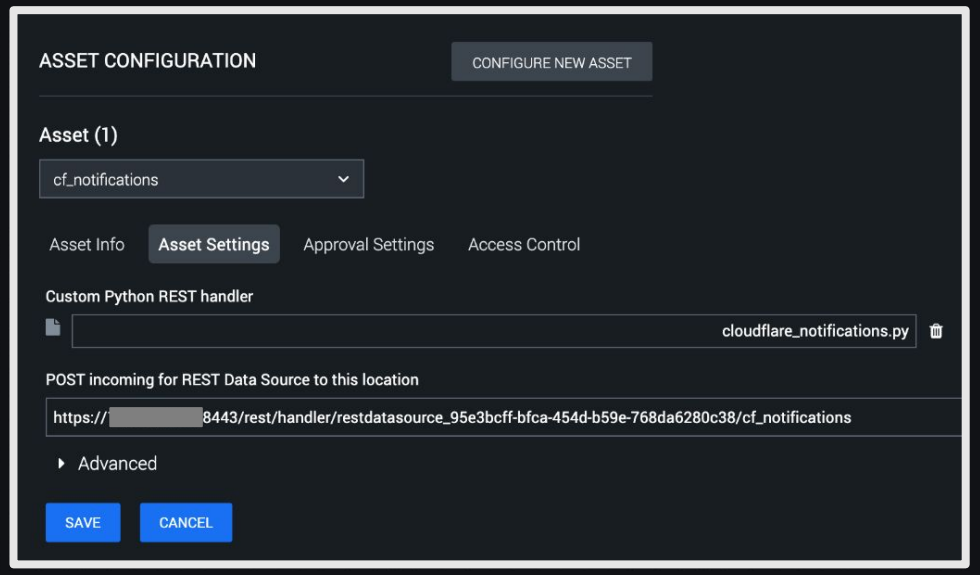
Scenario 2

Buttercup Go servers need to run stable, smoothly and securely to ensure the best player experience



Utility Apps

REST Data Source



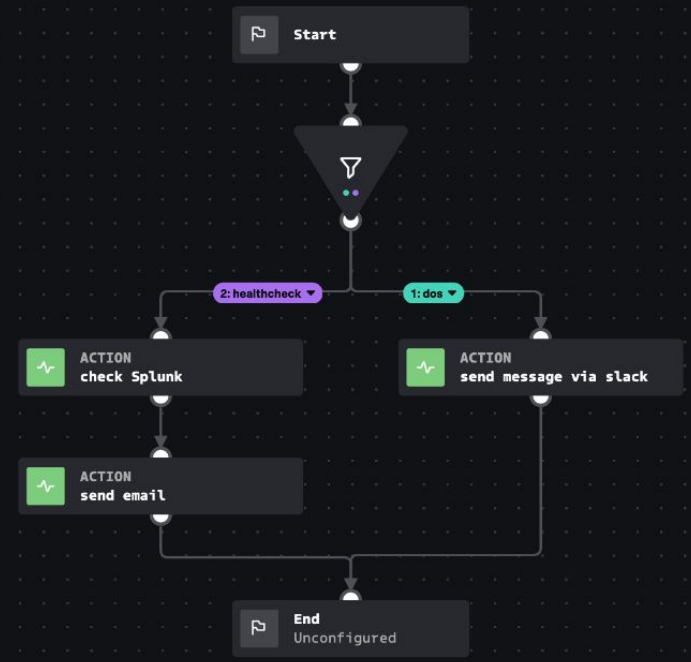
REST Data Source can consume webhook data from any source!

Packaged handlers for FireEye, STIX

Deploy your own custom handlers

Enrich alert with additional information

Notify stakeholders via appropriate communication channels



Improve reporting capabilities

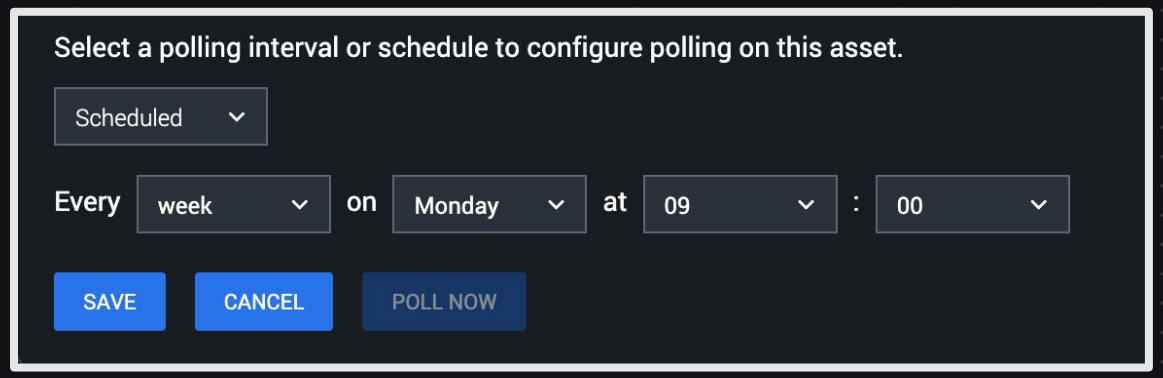
Scenario 3

Weekly report of suspicious activity to Buttercup Go management to keep them informed of security operations affecting the gaming platform

Utility Apps

Timer

SMTP

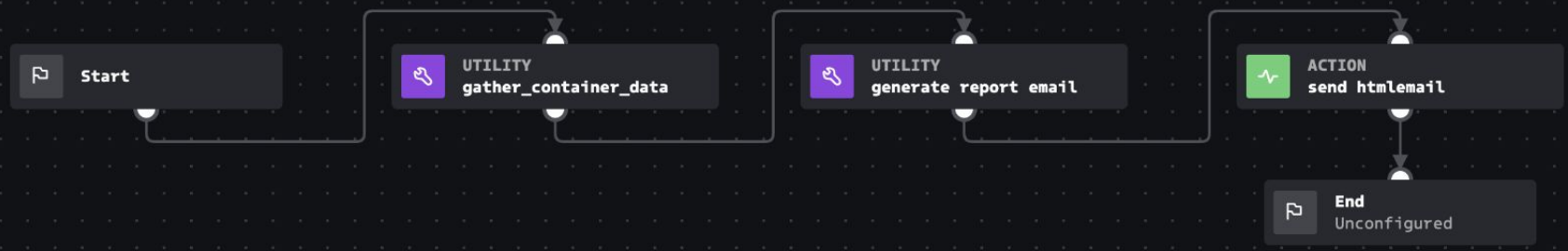


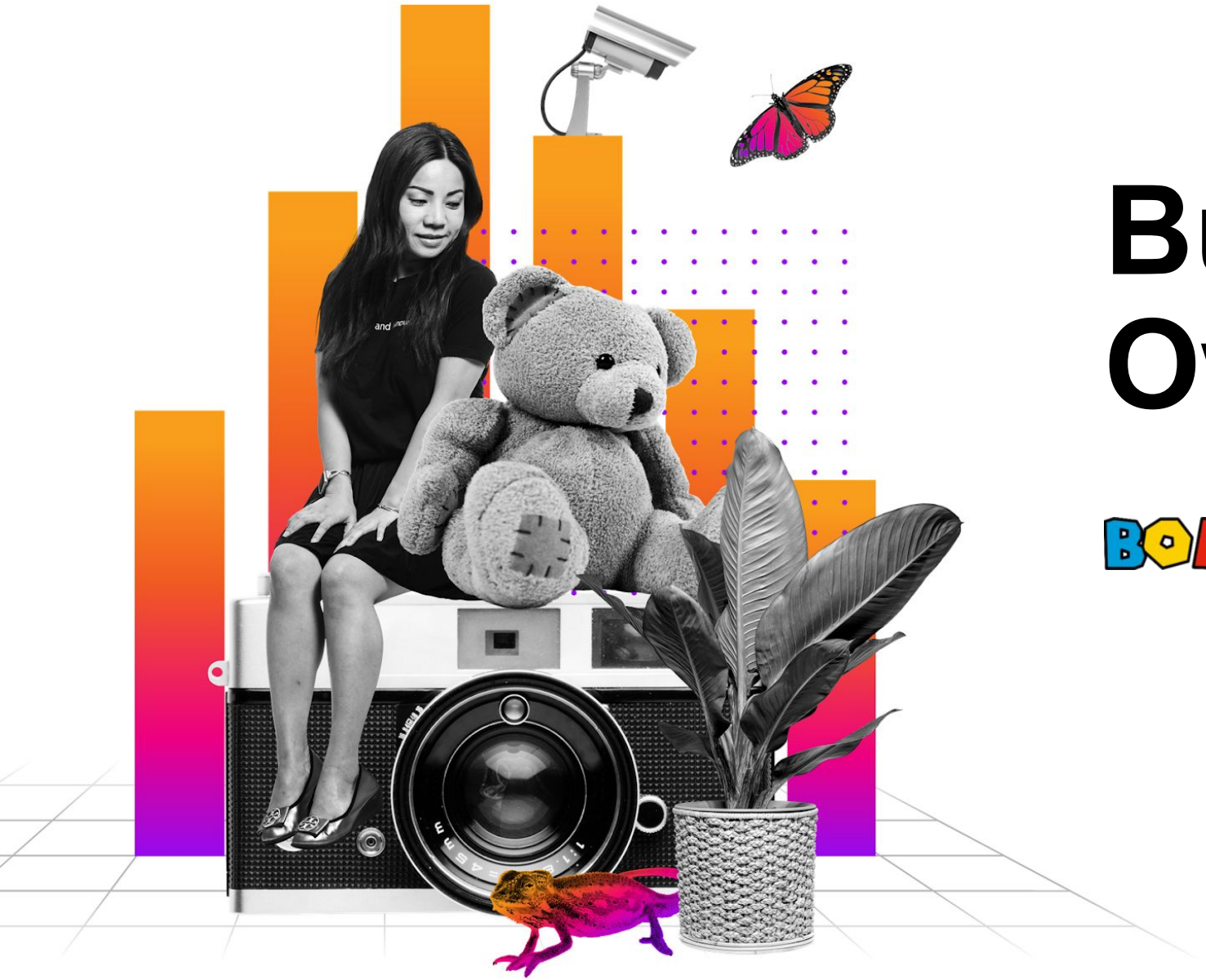
Create a new Timer asset with the required cadence

An individual Timer asset can be used across use cases!

Generate HTML mail containing report using SOAR REST API and custom functions

Send Email via SMTP app

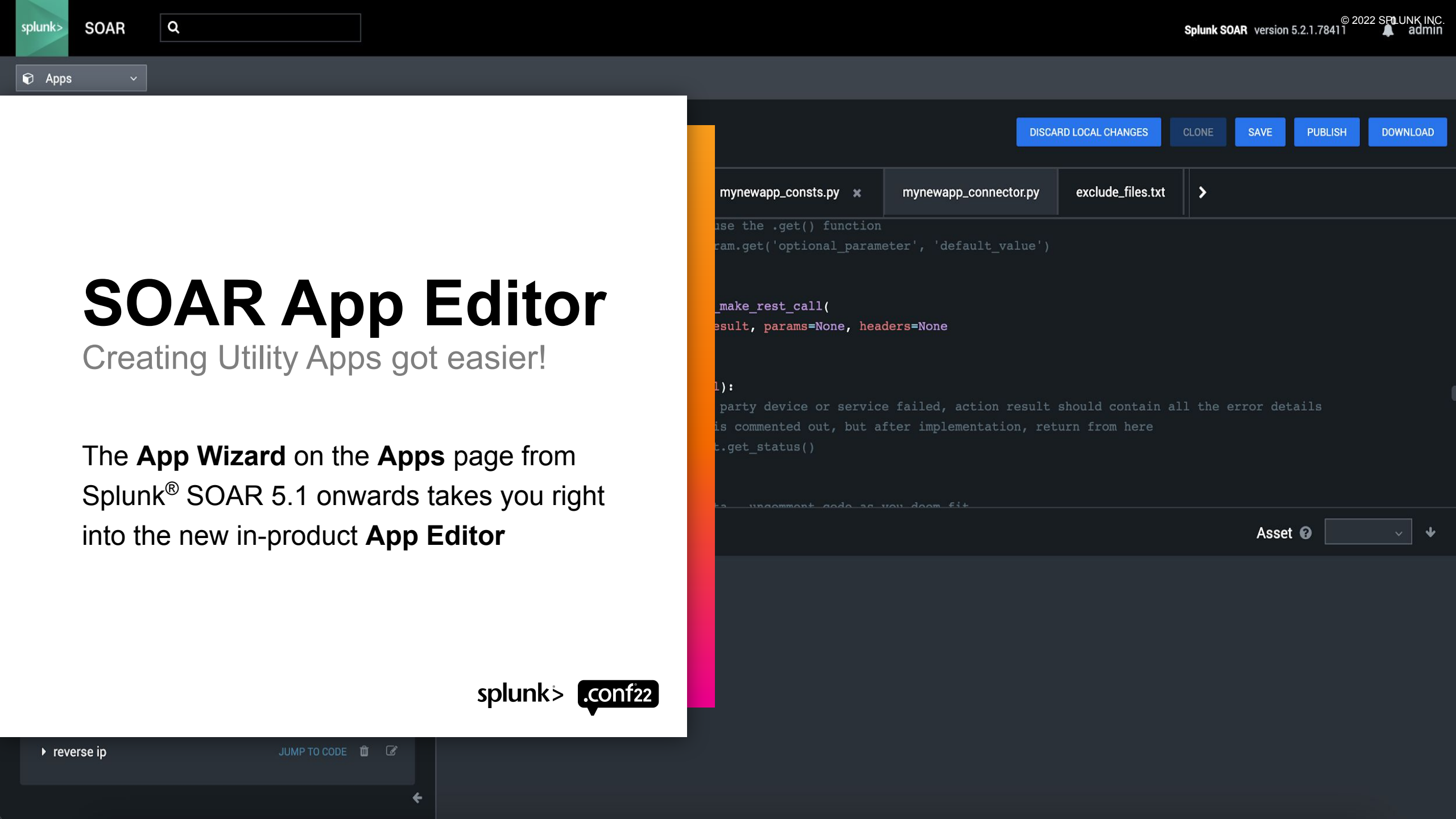




Build Your Own App!

BONUS LEVEL

splunk> .conf22

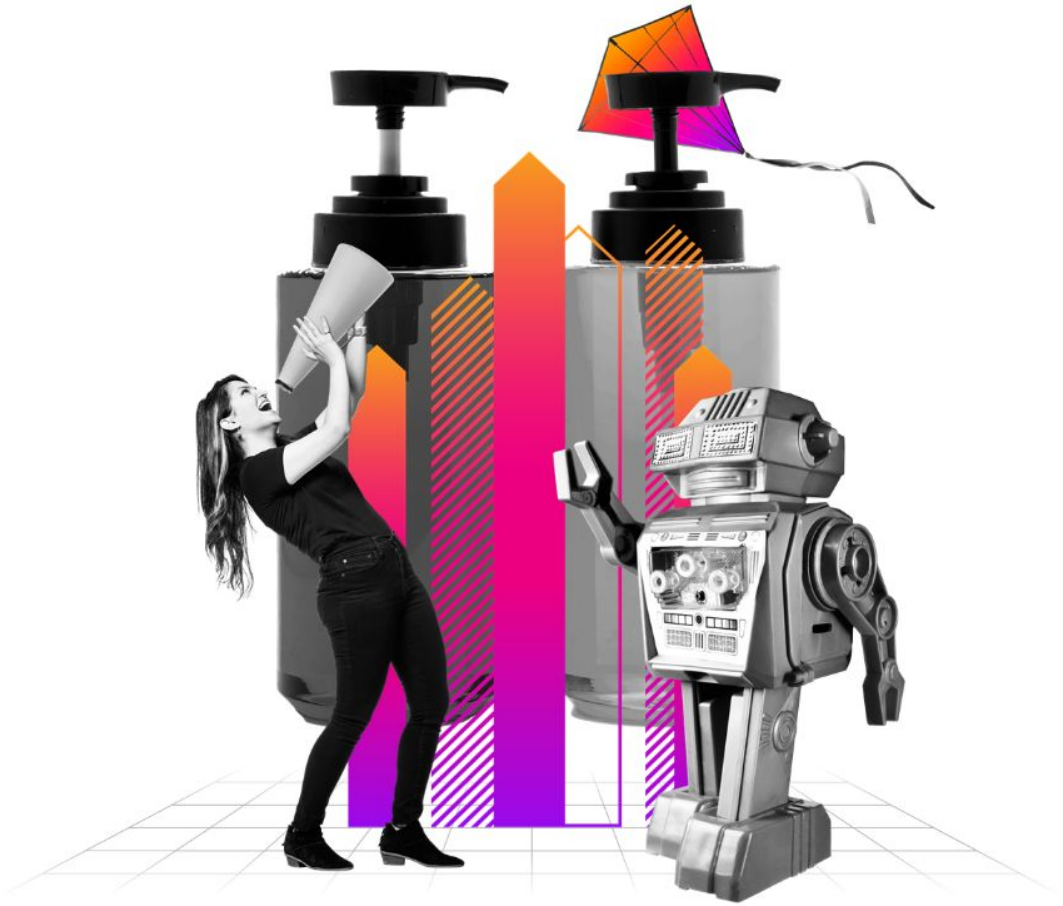


SOAR App Editor

Creating Utility Apps got easier!

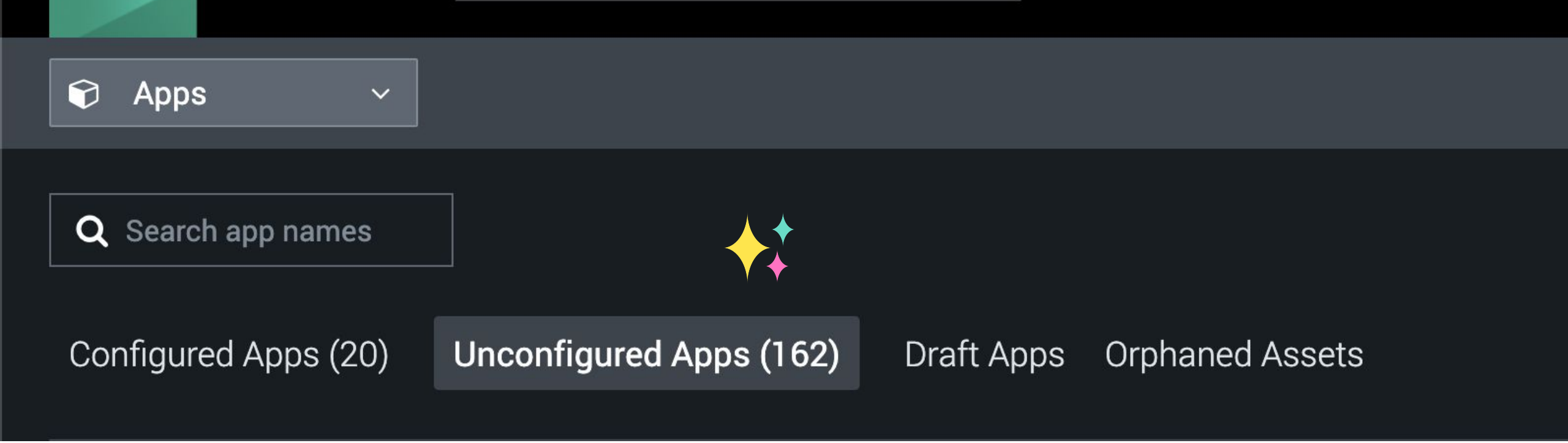
The **App Wizard** on the **Apps** page from Splunk® SOAR 5.1 onwards takes you right into the new in-product **App Editor**

splunk> .conf22



What Are You Waiting For?

splunk> .conf22



Explore Your Unconfigured SOAR Apps!

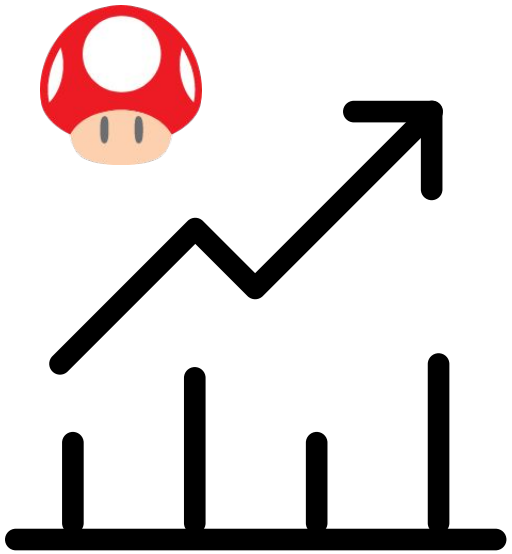
SOAR Apps on GitHub

The **splunk-soar-connectors** Github organization hosts over 380 repositories with SOAR Apps

splunk> .conf22

Above And Beyond

Bring your playbooks to the next level



By using **Utility Apps** you can

- Integrate with new data sources and systems without developing net-new apps
- Reduce your need for custom code blocks
- Speed up playbook development for new use cases

Thank You

splunk> .conf22