Splunk Phantom Ignition

Mhike Funderburk
Senior Security Engineer | Stage 2 Security

splunk> .conf19

Brandon Robinson
Senior Security Architect | Stage 2 Security

Luke Summers
Security Engineer | Stage 2 Security

splunk> .conf19

Forward-Looking Statements

During the course of this presentation, we may make forward-looking statements regarding future events or plans of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results may differ materially. The forward-looking statements made in the this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, it may not contain current or accurate information. We do not assume any obligation to update any forward-looking statements made herein.

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. Splunk undertakes no obligation either to develop the features or functionalities described or to include any such feature or functionality in a future release.

Why Bother?

Automation is a lot of work and cost to implement

Houston, We Have a Problem

Everything is growing except your team

IT Platform Infrastructure

Security Stack

Threat Landscape

Privacy and Regulatory Reqs

Getting Ready

"Read all instructions before starting your exam"

splunk> .conf19

Before You Do Anything

Know where you are going

Implementation

- Interactive
  - Analysts work in the platform
- Non-Interactive
  - Analysts work elsewhere

Choose carefully, migrating later is messy

Content

- Triggers
  - Logs & Alerts
- Automation
  - Time
  - Effort

Automation isn't for everything

Documentation

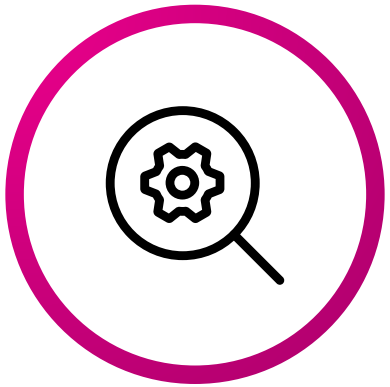
- What are you doing now?
  - Is it specific?
  - Is it effective?
  - Are you actually doing it that way?

You can't automate what you don't know

Blueprints

Because everyone hates you when you wing it

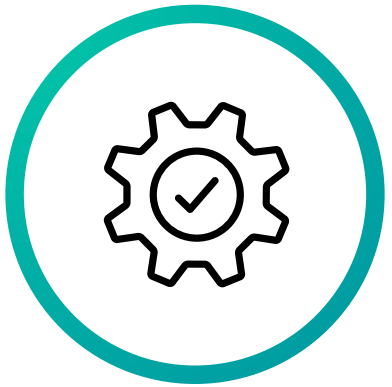
Scope Your Operations



Break Down Your Dependencies

Specify Human Interactions

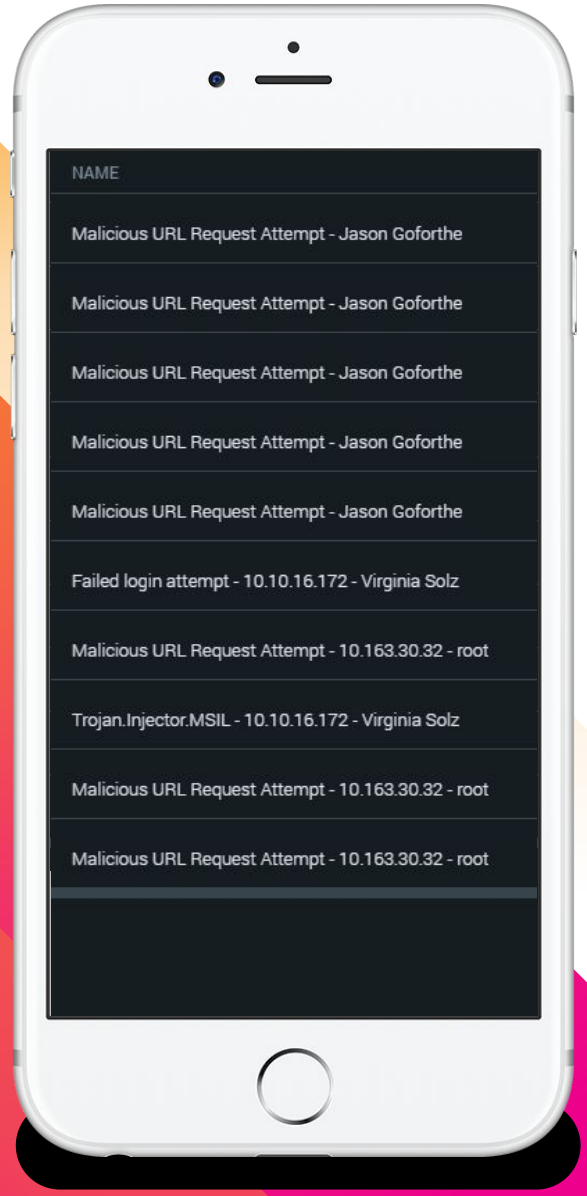
Automate Closure



Data Presentation

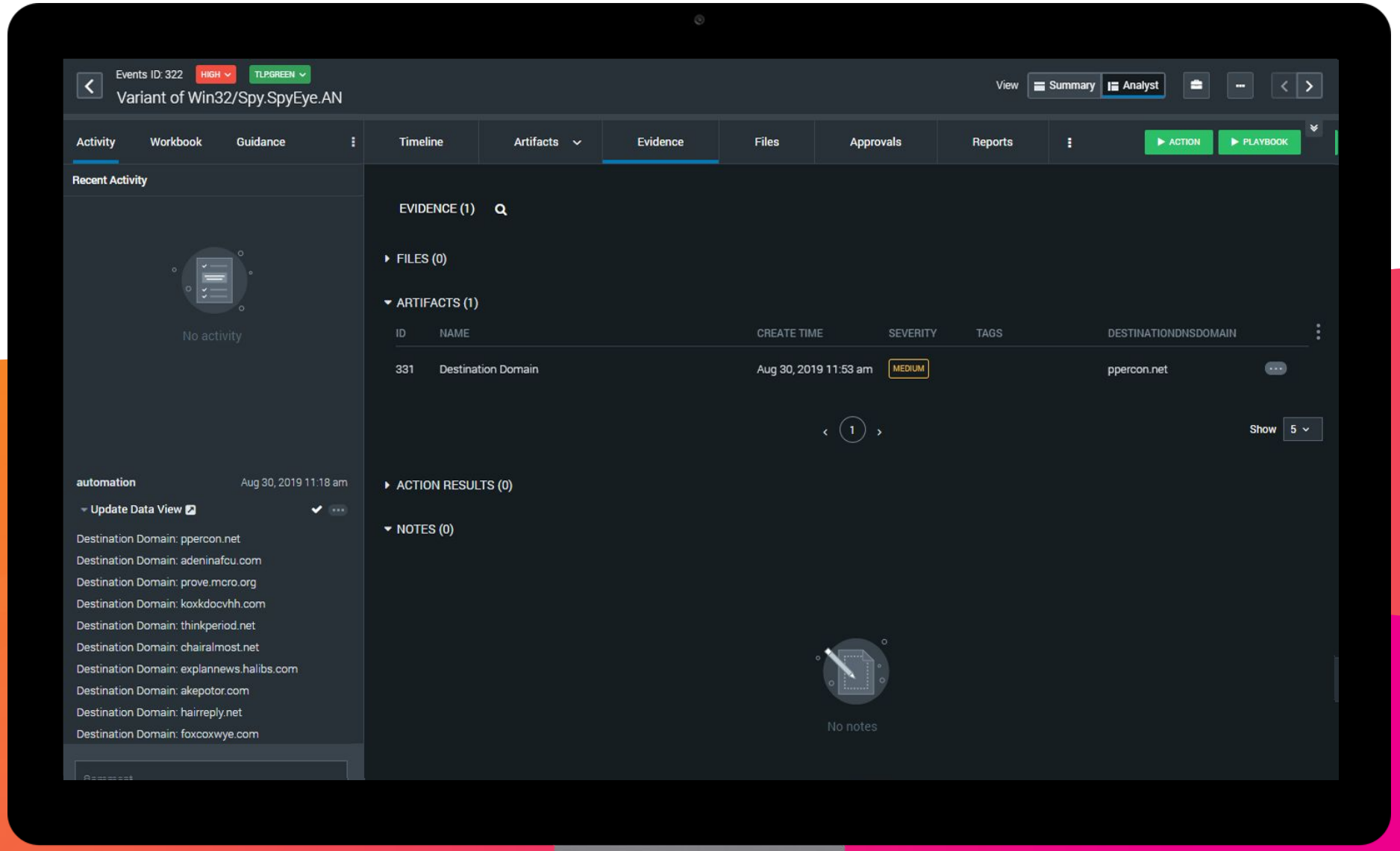
How will you present data to support the way you work?

splunk> .conf19



Automate Data Tasks

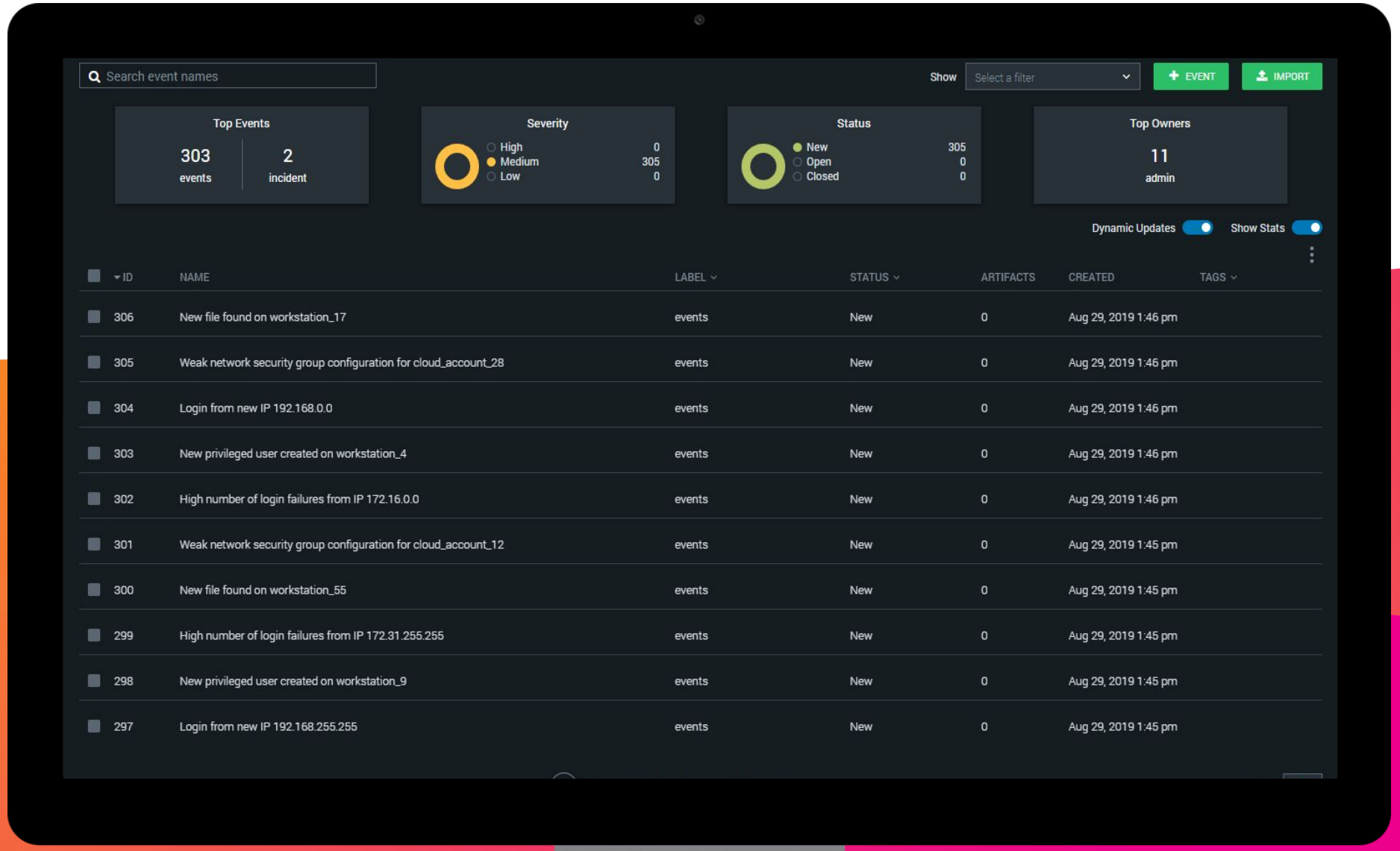
- Rename your containers with context
- Push the most important details to the visible locations
- Duplicate action data into artifacts, evidence, or comments



splunk> .conf19

Where is the Value?

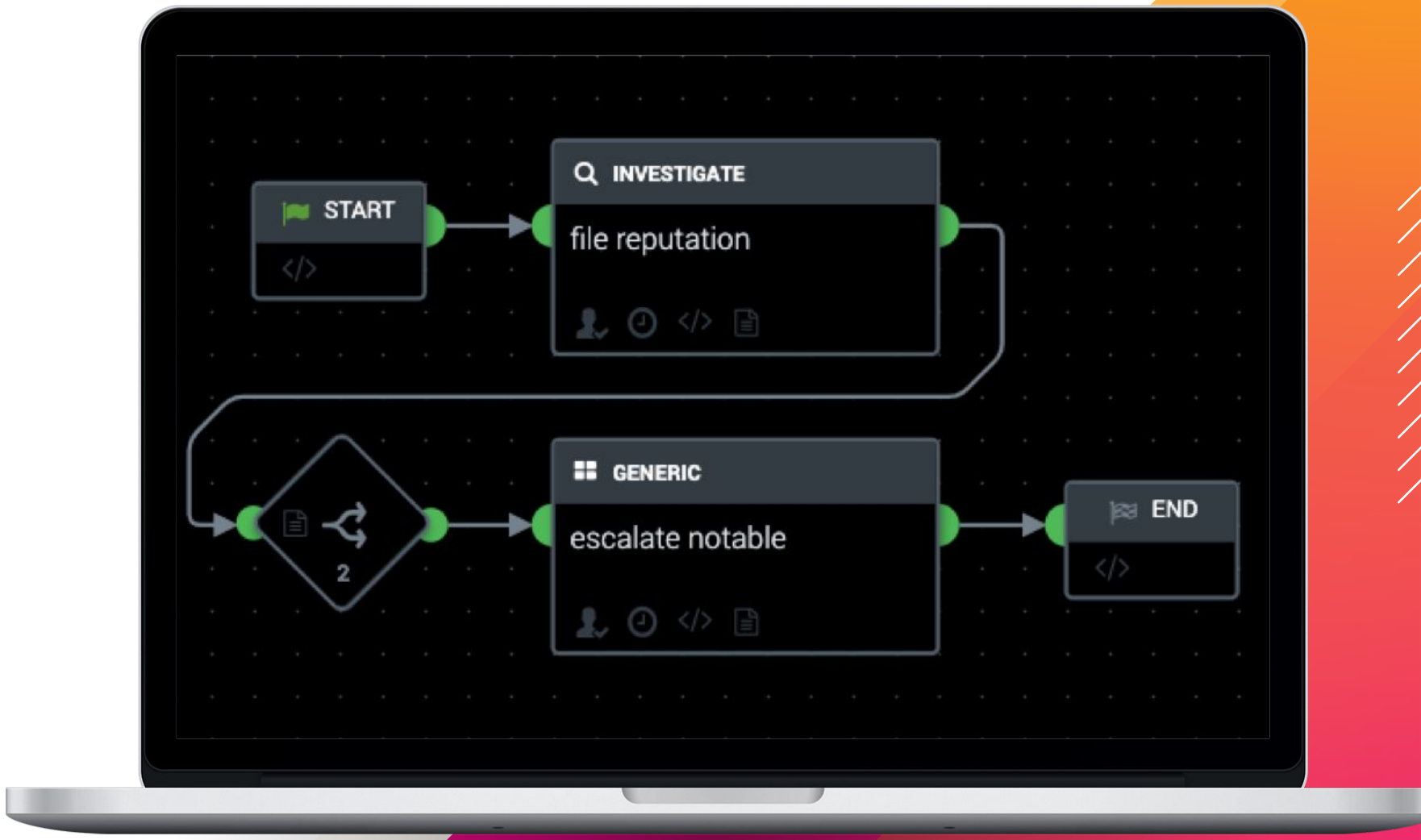
Seriously, this is a lot of work.
What can it do?

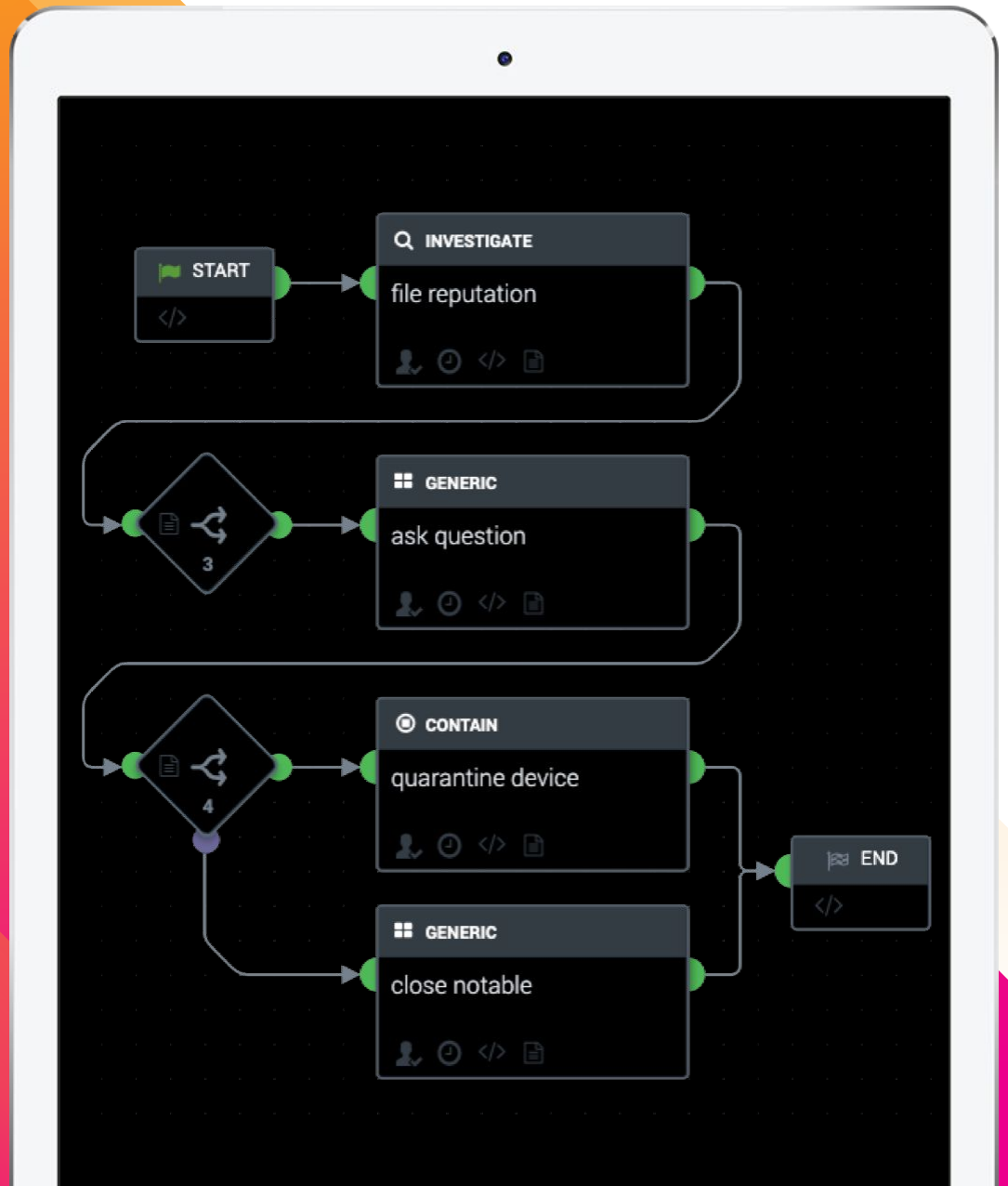


splunk> .conf19

Automate the Busy Work

- Automatic remediation isn't a requirement of automation
- Intelligently enrich your notables and alerts for your analysts
- Enjoy flexibility and functionality beyond Splunk ES





Take the Next Step

- Take advantage of non-analyst user interaction
- Build trust in the automation to perform advanced actions
- Avoid alert fatigue
- Identify and close false positives

Gotchas

We wish we knew this on day one

splunk> .conf19

"Build **trust** in the system. Don't automate remediation over night."

— Broken System Admin

"Be **conservative** in initial **volumes**."

— Overwhelmed Security Analyst

"Minimize active playbooks and **manage** execution **intelligently**."

— Executive Shelling Out For Unnecessary Licenses

“**Time.sleep** is the **devil**.”

— Support Staff After A Dev Broke The System

"It's all **python**. We should have a python **developer** on staff."

— Frustrated Security Analyst

"Don't use **proper names** for system objects in **action names**."

— Developer After A Very Confusing Support Ticket

"If you don't **scope properly**, nothing will work the way you are expecting."

— Admin Helping Debug

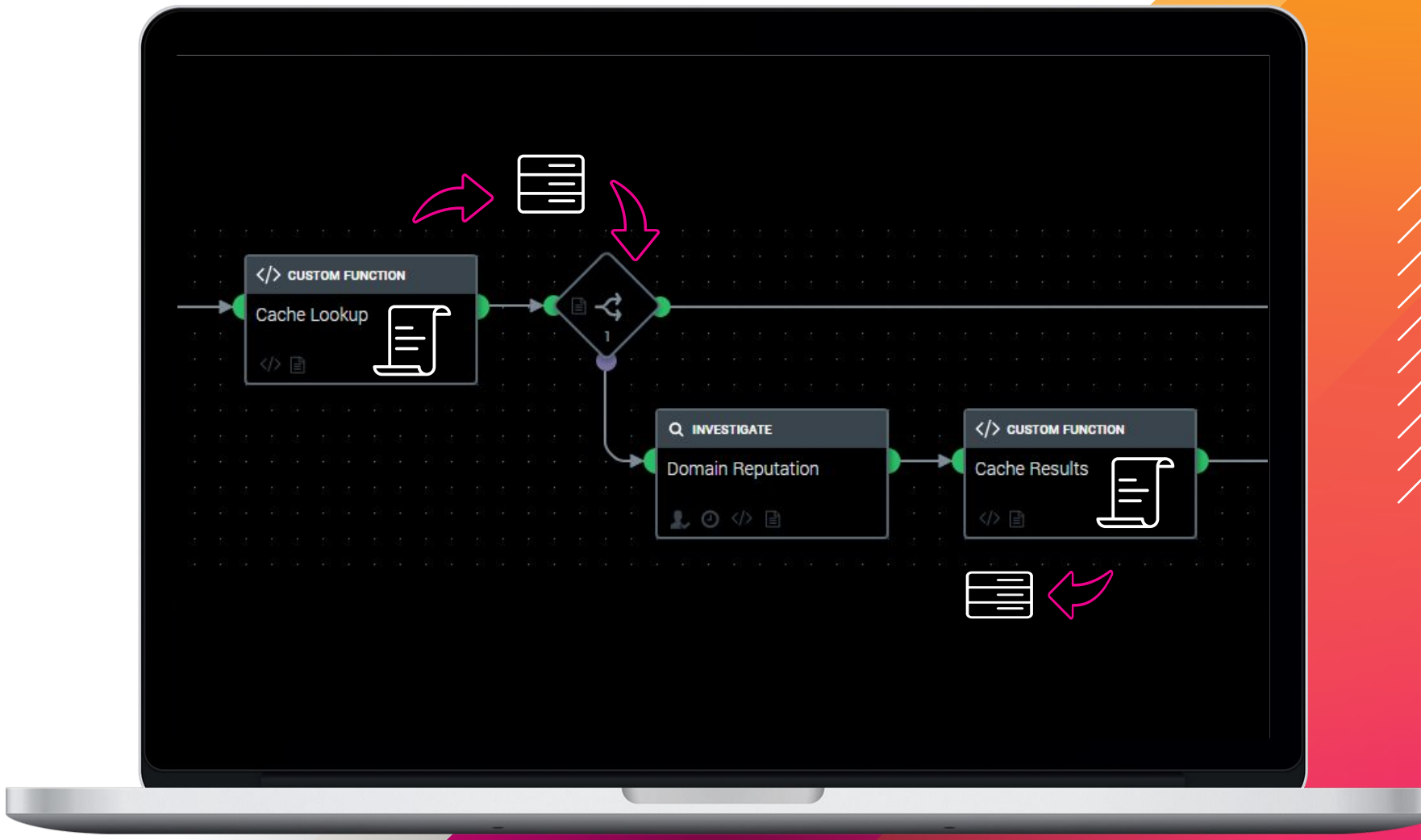
Going Deep

Developing beyond standard automation

splunk> .conf19

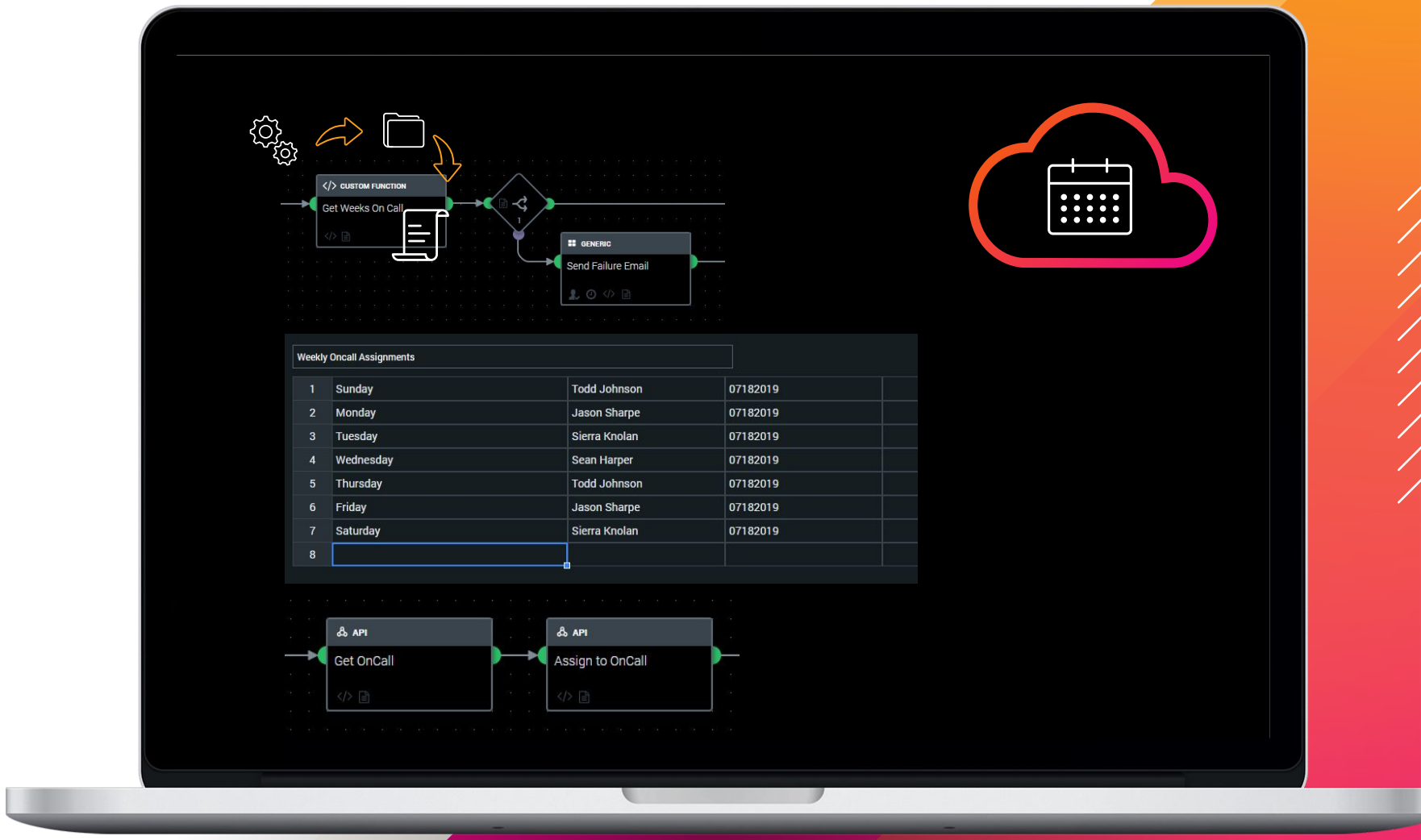
Cache App Results

- Limited API call
- Slow response from source
- Elements Required
  - Playbook actions
  - Custom Lists



Assign To On-Call

- Your on-call calendar is in an inconvenient location
- Elements Required
  - Timer App
  - Container
  - Playbooks
  - Calendar API
  - Custom Lists



Q&A

Mhike Funderburk — Senior Security Engineer
Luke Summers — Security Engineer
Brandon Robinson — Senior Security Architect

splunk> .conf19

.conf19

splunk>

Thank You !

Go to the .conf19 mobile app to

RATE THIS SESSION