splunk> .conf2017

Security Hands-on @ Pavilion

Automate Security Operations with Phantom & Splunk

Splunk | Security Markets

September 26 | Washington, DC

The Leader in Security Automation & Orchestration

RSAC Innovation Sandbox 2016 WINNER

2016 SINET 16 INNOVATOR

THE CHANNEL CO. CRN SECURITY 100 2017

Forbes 2017 THE Cloud100 RISING STARS

Phantom Community Growing Larger Each Day

- Phantom Community Edition (free)
- Share Community Playbooks
- Contribute Apps
- Documentation, Training, KB Articles
- Q&A

phantom.us/join

phantom-community

blog.phantom.us

Objective

- **OBJECTIVE**
  - Learn to triage a security event using a Phantom Automation Playbook triggered by an event in Splunk.

- **USE-CASE**
  - Phantom ingests a security event from Splunk.
  - Event requires triage; Phantom Automation Playbook is launched.
  - Results are reviewed in Phantom Mission Control; additional on demand actions launched.
  - Data is posted back to Splunk for archival purposes.

- **BENEFITS**
  - Splunk integrated with Phantom automates event triage and streamlines security functions like investigation, hunting, enrichment, containment & recovery. This is Splunk Adaptive Response in action.

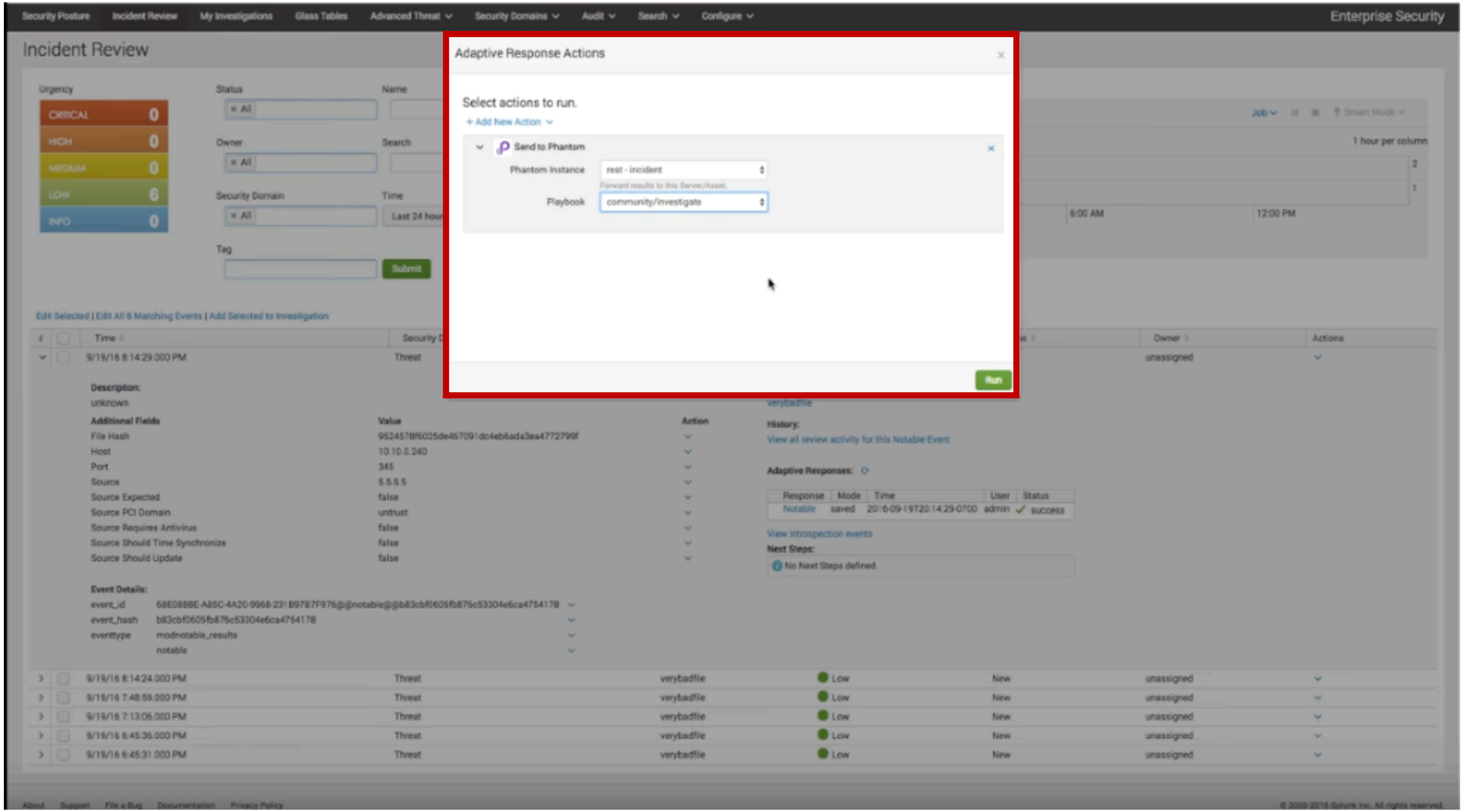
SET-UP INSTRUCTION

- Access information :
  - https://54.215.195.107/

- Login :
  - ID : (shared during session)
  - Pass : (shared during session)

- Other Instruction :
  - Ensure Chrome browser is in use

Ingest Event from Splunk



Incident Review

Urgency

CRITICAL	0
HIGH	0
MEDIUM	0
LOW	6
INFO	0

Status: × All

Owner: × All

Security Domain: × All

Time: Last 24 hour

Name

Search

Tag

Adaptive Response Actions

Select actions to run.

+ Add New Action

Send to Phantom

Phantom Instance: rest - incident

Forward results to this Server/Asset.

Playbook: community/investigate

1 hour per column

6:00 AM

12:00 PM

Edit Selected | Edit All 6 Matching Events | Add Selected to Investigation

i		Time	Security D				Owner	Actions
⌄	□	9/19/16 8:14:29.000 PM	Threat				unassigned	⌄

Description:

unknown

Additional Fields	Value	Action
File Hash	952457Bf6025de467091dc4eb6ada3ea4772799f	⌄
Host	10.10.0.240	⌄
Port	345	⌄
Source	5.5.5.5	⌄
Source Expected	false	⌄
Source PCI Domain	untrust	⌄
Source Requires Antivirus	false	⌄
Source Should Time Synchronize	false	⌄
Source Should Update	false	⌄

Event Details:

event_id	68E0888E-A85C-4A20-9968-231B9787F976@@notable@@b83cbf0605fb876c53304e6ca4754178
event_hash	b83cbf0605fb876c53304e6ca4754178
eventtype	modnotable_results
	notable

verybadfile

History:

View all review activity for this Notable Event

Adaptive Responses:

Response	Mode	Time	User	Status
Notable	saved	2016-09-19T20:14:29-0700	admin	✓ success

View introspection events

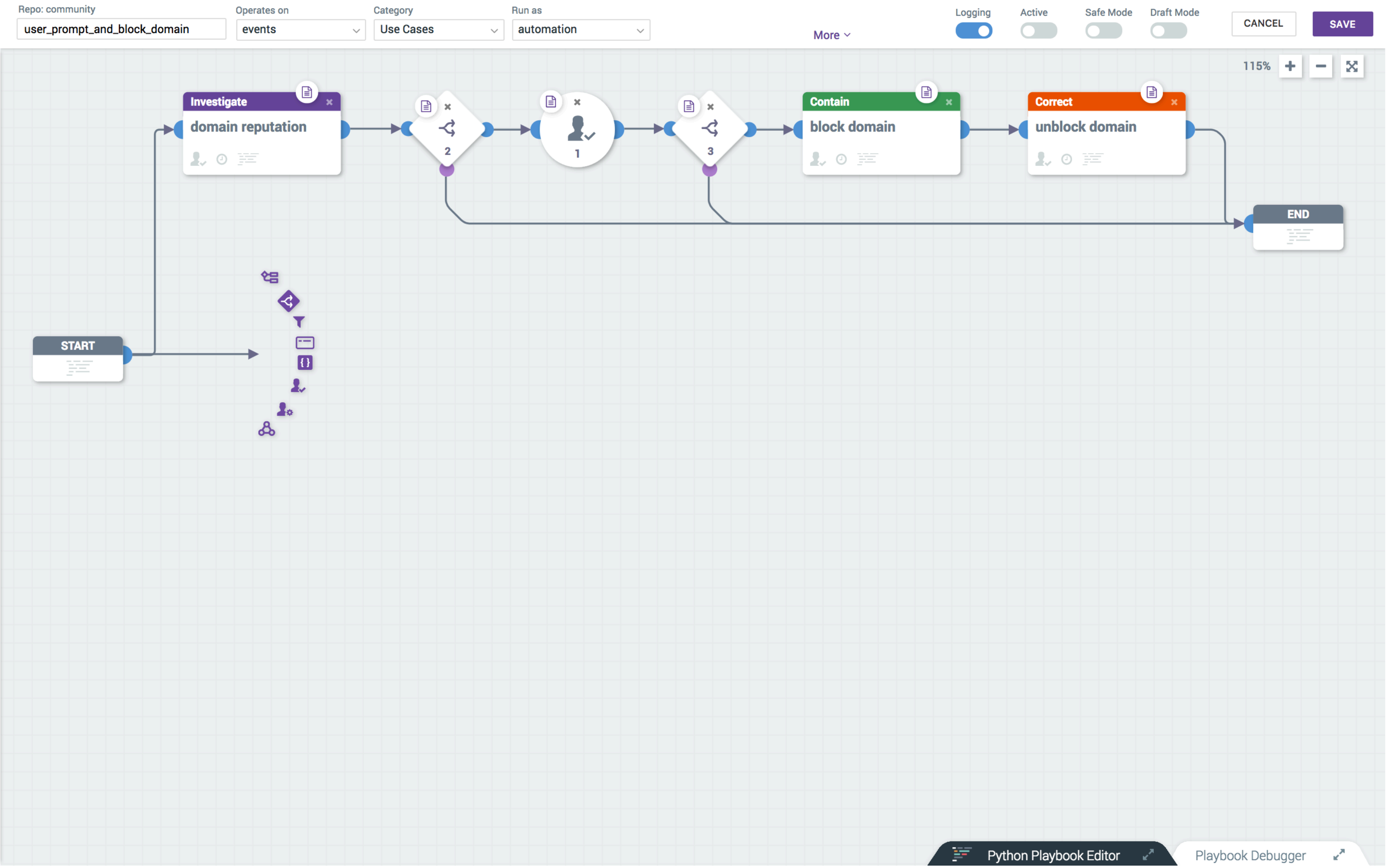
Next Steps:

No Next Steps defined.

›	□	9/19/16 8:14:24.000 PM	Threat	verybadfile	● Low	New	unassigned	⌄
›	□	9/19/16 7:48:59.000 PM	Threat	verybadfile	● Low	New	unassigned	⌄
›	□	9/19/16 7:13:06.000 PM	Threat	verybadfile	● Low	New	unassigned	⌄
›	□	9/19/16 6:45:36.000 PM	Threat	verybadfile	● Low	New	unassigned	⌄
›	□	9/19/16 6:45:31.000 PM	Threat	verybadfile	● Low	New	unassigned	⌄

© 2005-2016 Splunk Inc. All rights reserved.

Phantom Automation Playbook



Repo: community: user_prompt_and_block_domain

Operates on: events

Category: Use Cases

Run as: automation

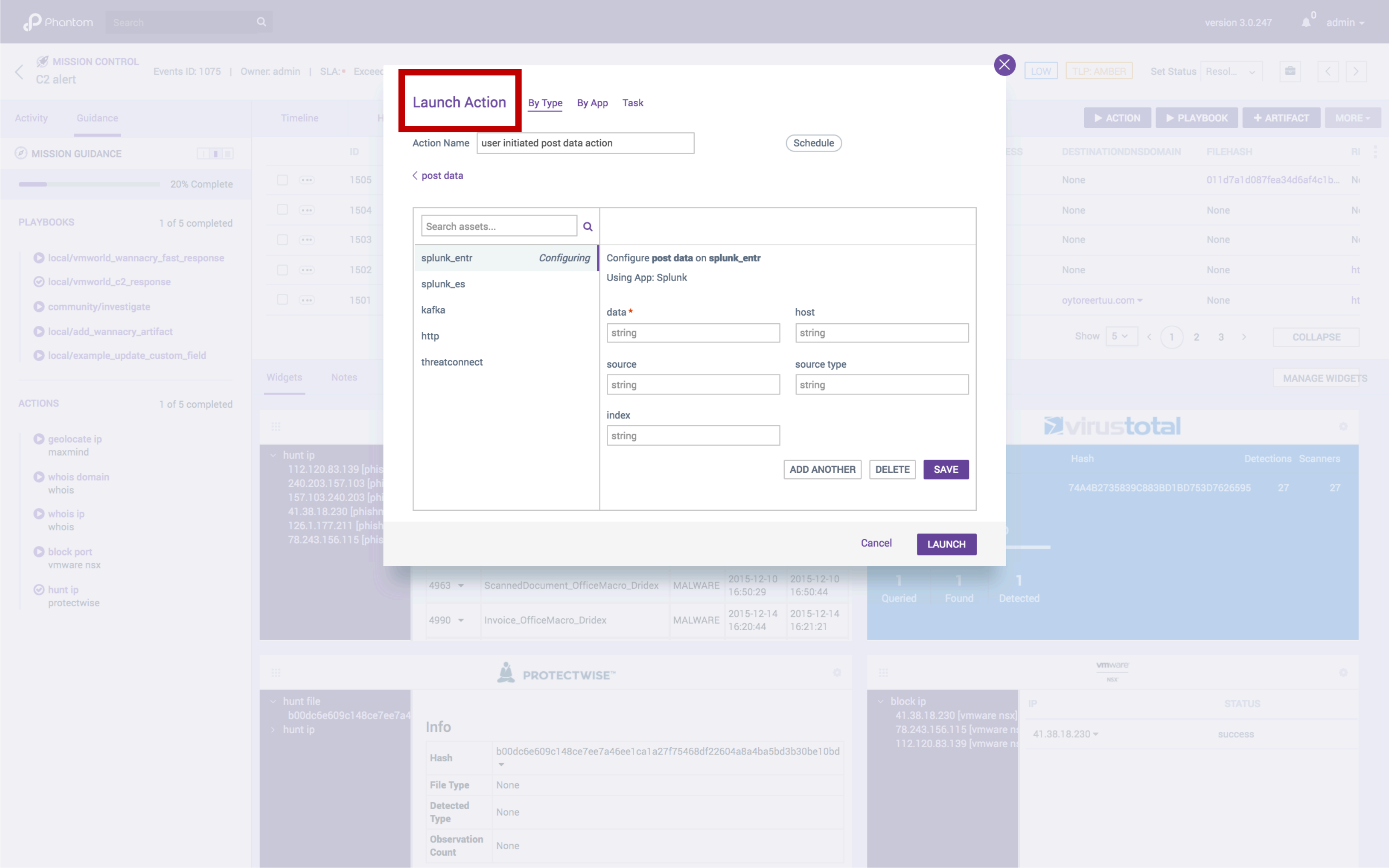
Logging: ● on

Active: ○ off

Safe Mode: ○ off

Draft Mode: ○ off

Phantom Mission Control



Launch Action

By Type | By App | Task

Action Name: user initiated post data action

Schedule

‹ post data

Search assets...

splunk_entr	*Configuring*
splunk_es	
kafka	
http	
threatconnect	

Configure **post data** on **splunk_entr**

Using App: Splunk

data *: string

host: string

source: string

source type: string

index: string

ADD ANOTHER | DELETE | SAVE

Cancel | LAUNCH

ID		DESTINATIONDNSDOMAIN	FILEHASH
1505		None	011d7a1d087fea34d6af4c1b...
1504		None	None
1503		None	None
1502		None	None
1501		oytoreertuu.com	None

hunt ip
112.120.83.139 [phis
240.203.157.103 [ph
157.103.240.203 [ph
41.38.18.230 [phishn
126.1.177.211 [phish
78.243.156.115 [phis

4963	ScannedDocument_OfficeMacro_Dridex	MALWARE	2015-12-10 16:50:29	2015-12-10 16:50:44
4990	Invoice_OfficeMacro_Dridex	MALWARE	2015-12-14 16:20:44	2015-12-14 16:21:21

Hash	Detections	Scanners
74A4B2735839C883BD1BD753D7626595	27	27

1 Queried | 1 Found | 1 Detected

hunt file
b00dc6e609c148ce7ee7a4
hunt ip

Info

Hash	b00dc6e609c148ce7ee7a46ee1ca1a27f75468df22604a8a4ba5bd3b30be10bd
File Type	None
Detected Type	None
Observation Count	None

block ip
41.38.18.230 [vmware nsx]
78.243.156.115 [vmware n
112.120.83.139 [vmware n

IP	STATUS
41.38.18.230	success

STEP BY STEP GUIDE

1. Ingest event data from Splunk
   - Open Splunk Incident Review
   - Choose the “Send to Phantom” action for an event
   - Select the Phantom Investigate Playbook; click “Run”

2. Review Phantom Automation Playbook
   - Open Phantom UI
   - Chose “Playbooks” from menu and the “Investigate” Playbook from listing
   - Review Playbook to ensure process is correct for future automations

3. Navigate to Phantom Mission Control
   - Select the file or IP address to execute additional actions
   - Choose additional actions to run on ”Launch Action” pane (e.g. block hash, block IP)