



Examining Splunk Phantom's Architecture

Sourabh Satish

VP & Distinguished Engineer | Splunk

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.

Splunk, Splunk>, Turn Data Into Doing, The Engine for Machine Data, Splunk Cloud, Splunk Light and SPL 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. © 2019 Splunk Inc. All rights reserved.



Splunk Phantom Overview

Architecture

Why should you care?

Architecture details shall enable and empower you to better use the platform

- Strategize your phantom usage
- Strategize your workloads & use cases
- Strategize your playbooks

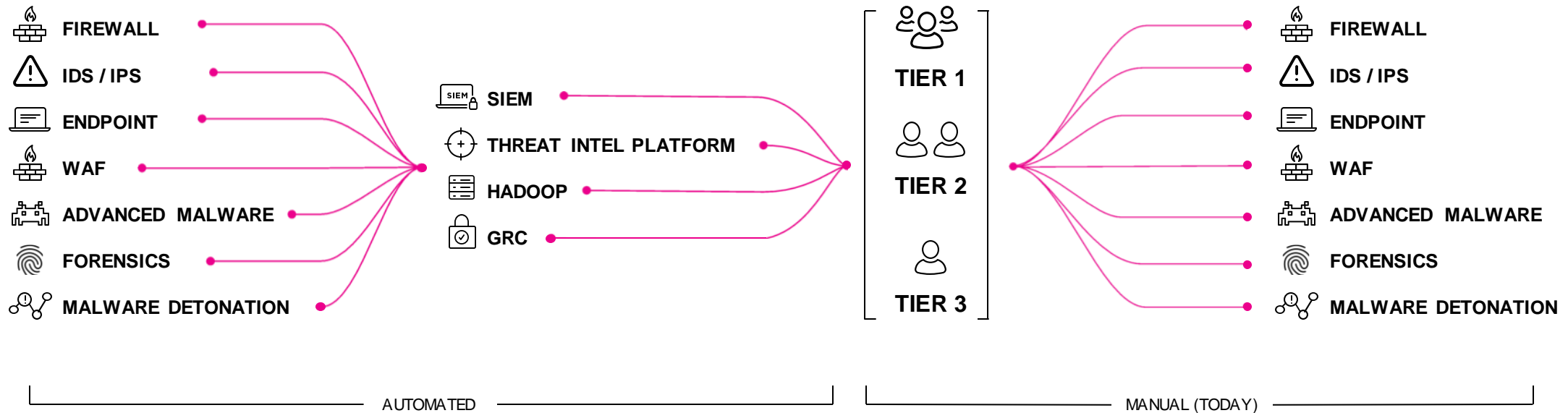
Better understand how to make best use of the platform and be successful!



Key Concepts

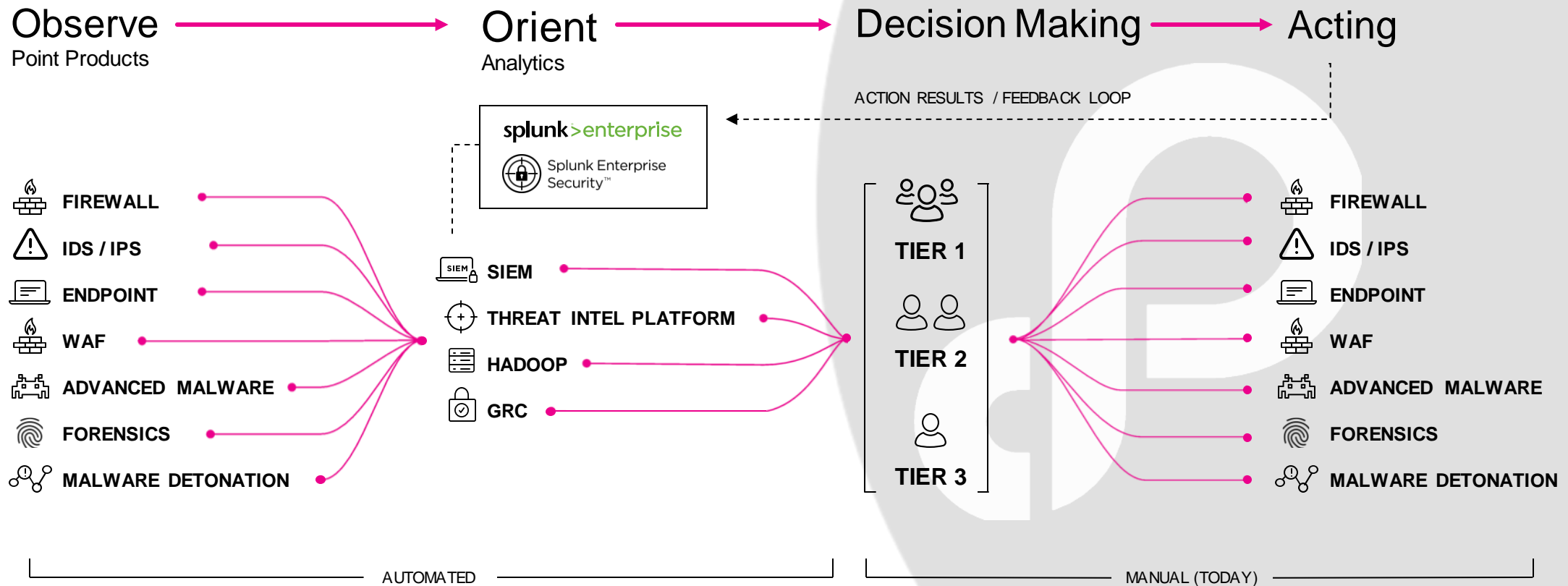
SOAR for Security Operations

Faster execution through the loop yields better security



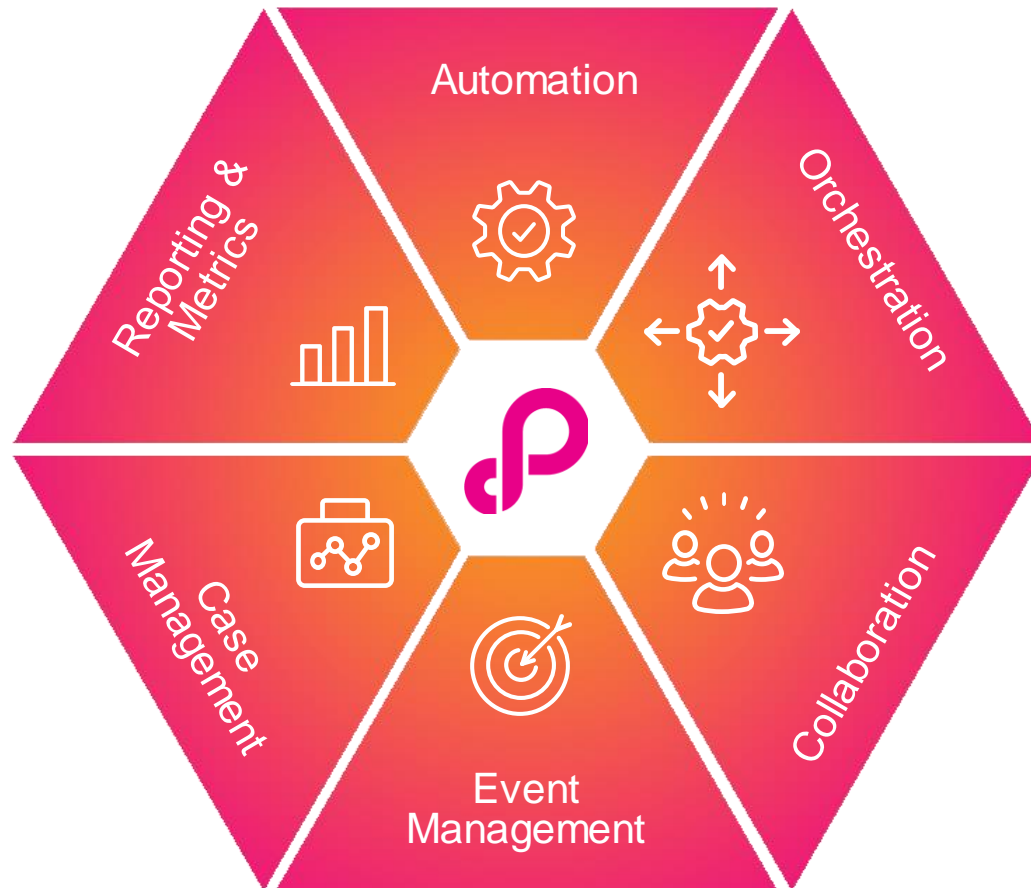
SOAR for Security Operations

Faster execution through the loop yields better security



Operationalizing Security

with Phantom

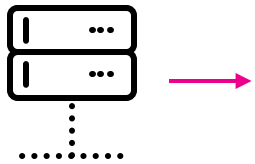


Integrate your team, processes, and tools together.

- Work smarter by automating repetitive tasks allowing analysts to focus on more mission-critical tasks.
- Respond faster and reduce dwell times with automated detection, investigation, and response.
- Strengthen defenses by integrating existing security infrastructure together so that each part is an active participant.

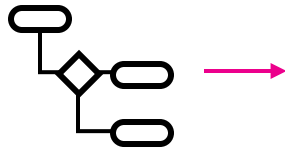
Key Concepts

Data Sources



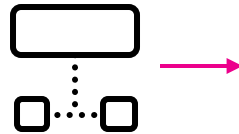
SIEM
Data Lake
Message Bus
Email
Threat Intelligence
Incident
Vulnerability

Playbooks



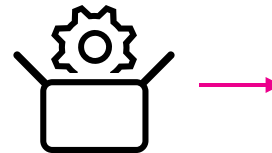
Investigate Endpoint
Reimage Endpoint
Deploy Indicators
Investigate Phishing

Actions



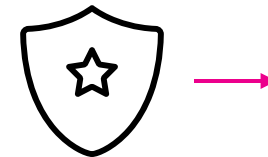
"Block IP"
"Disable User"
"Geolocate IP"
"Detonate File"
"Get Events"
"Send email"
"File Reputation"
"List Processes"
"Snapshot VM"

Apps



Splunk
Microsoft Ad
MaxMind
Cuckoo
ThreatGrid
Pan FW
SMTP
Tanium

Assets



Perimeter_FW
Primary_DC
Primary_SIEM
Exchange Server
CFO_Laptop

Owners

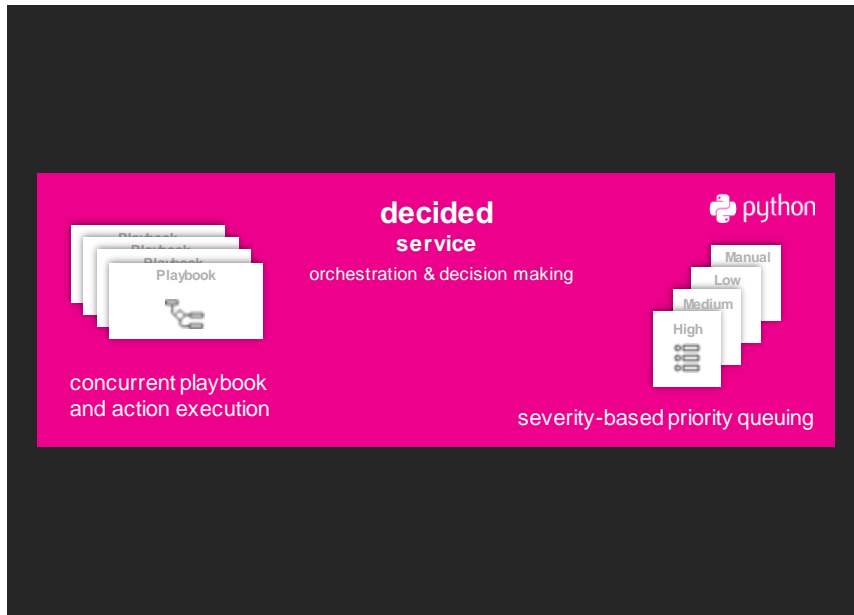


Bob
Judy
Fred





Architecture

Phantom Platform Architecture

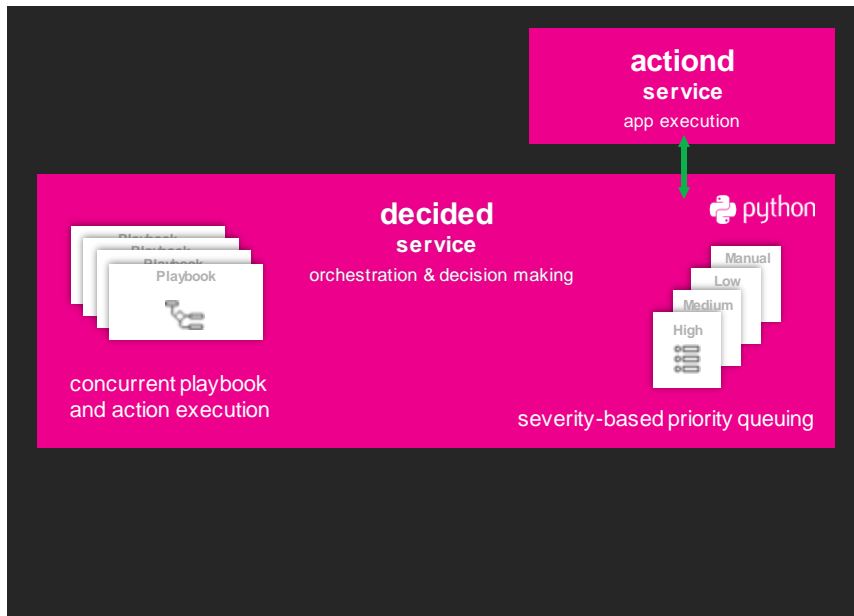


Phantom Services

LEGEND

-  = External Communication
-  = IPC

Phantom Platform Architecture

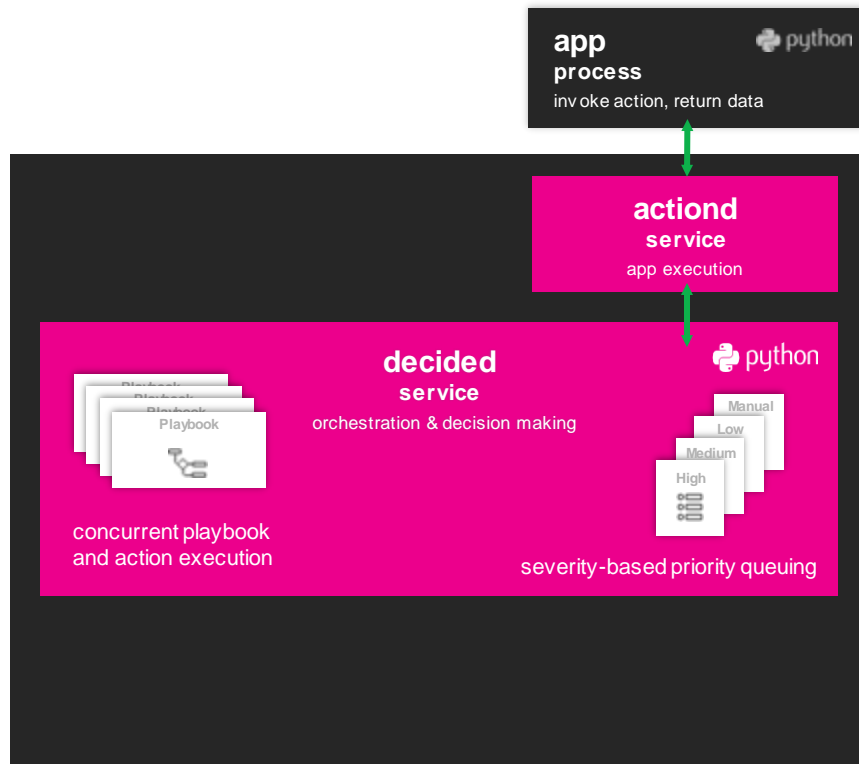


Phantom Services

LEGEND

- = External Communication
- = IPC

Phantom Platform Architecture



Phantom Services

LEGEND

- = External Communication
- = IPC

Phantom Platform Architecture



Phantom Services

LEGEND

- ↕ = External Communication
- ↕ = IPC

Phantom Platform Architecture

External Platforms & Services



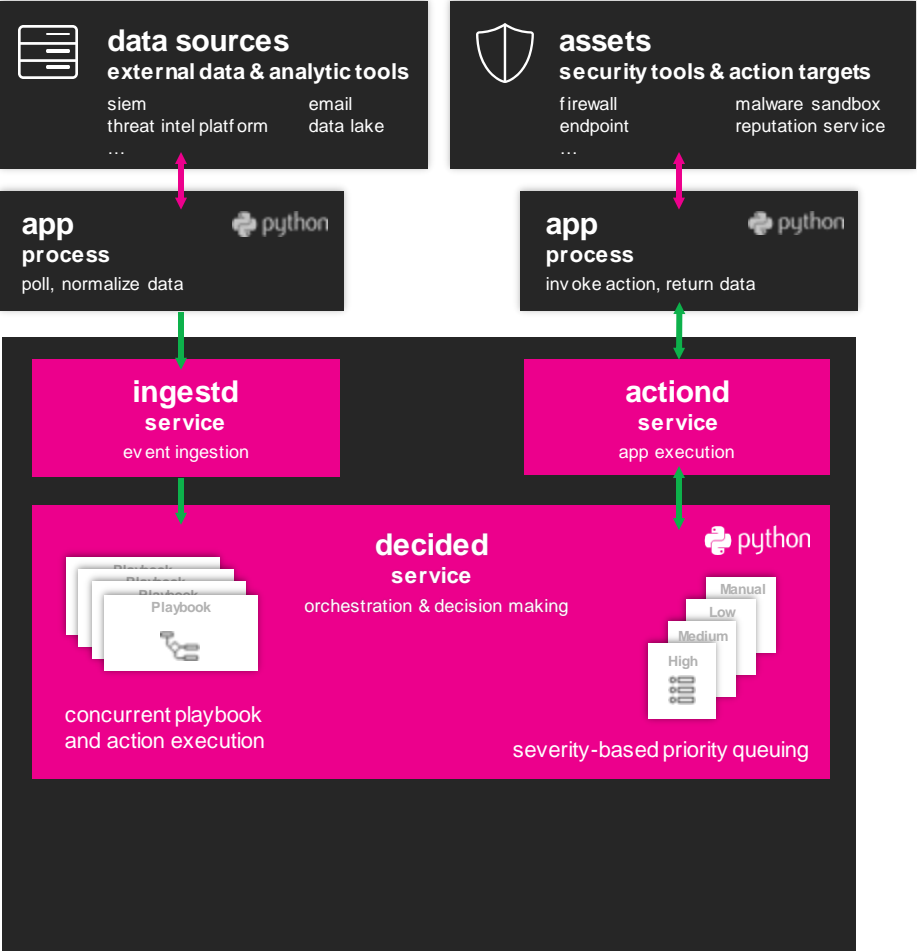
Phantom Services

LEGEND

- = External Communication
- = IPC

Phantom Platform Architecture

External Platforms & Services



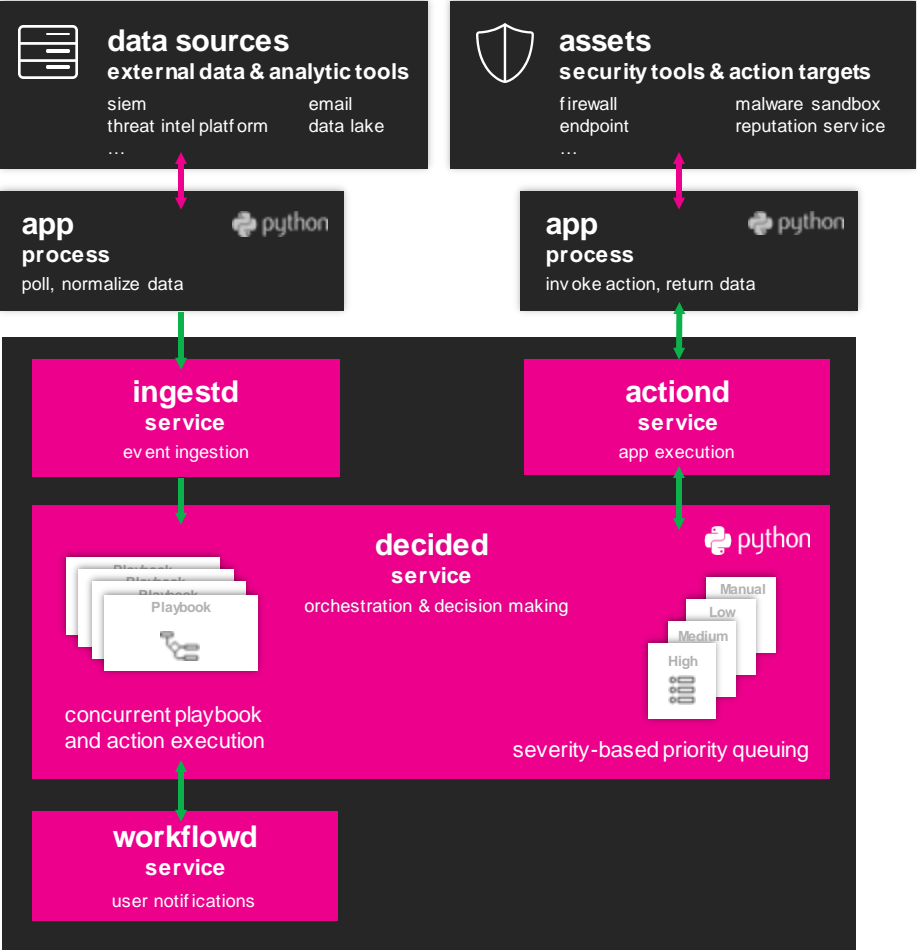
Phantom Services

LEGEND

- ↕ = External Communication
- ↕ = IPC

Phantom Platform Architecture

External Platforms & Services



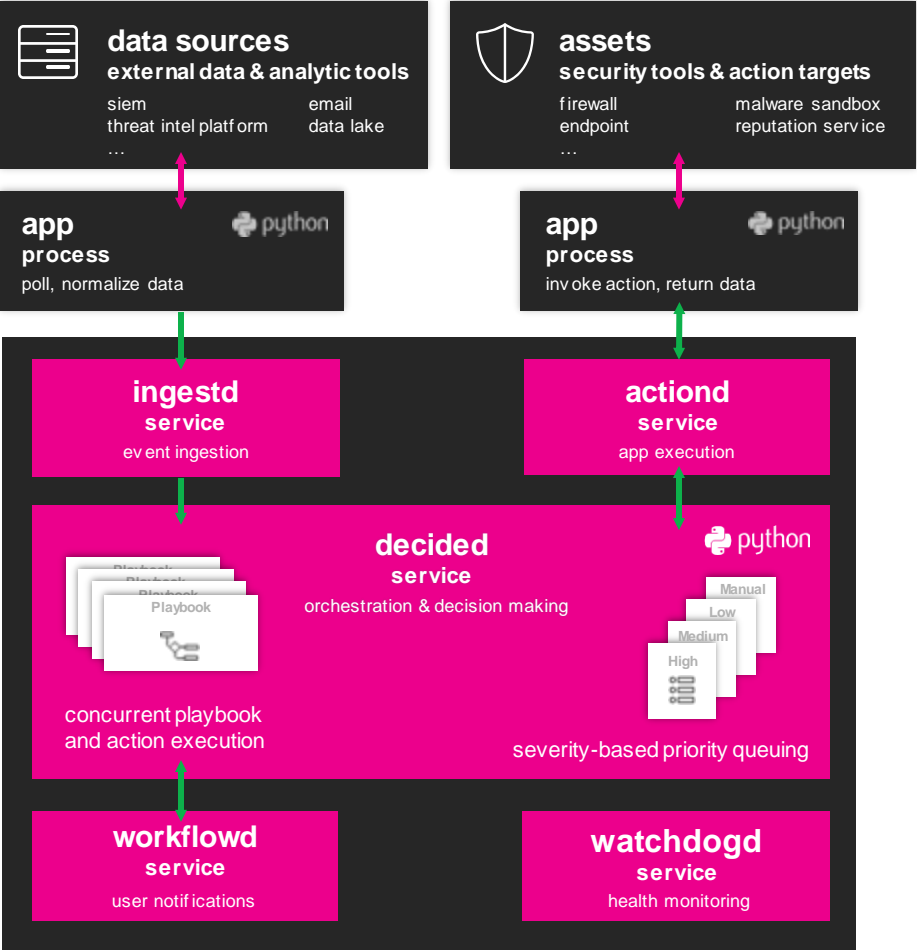
Phantom Services

LEGEND

- External Communication
- IPC

Phantom Platform Architecture

External Platforms & Services



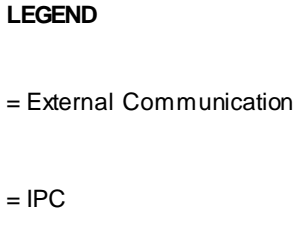
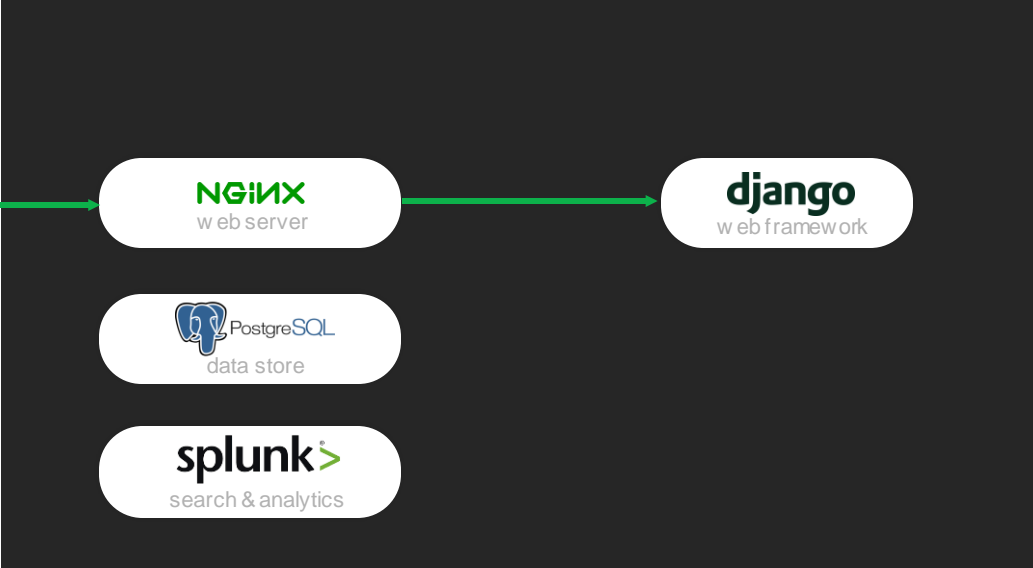
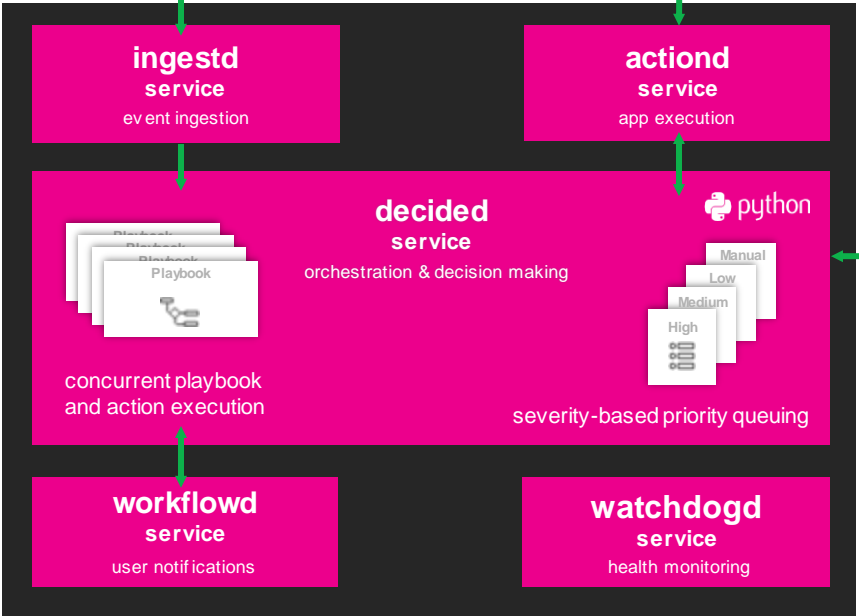
Phantom Services

LEGEND

- ↕ = External Communication
- ↕ = IPC

Phantom Platform Architecture

External Platforms & Services

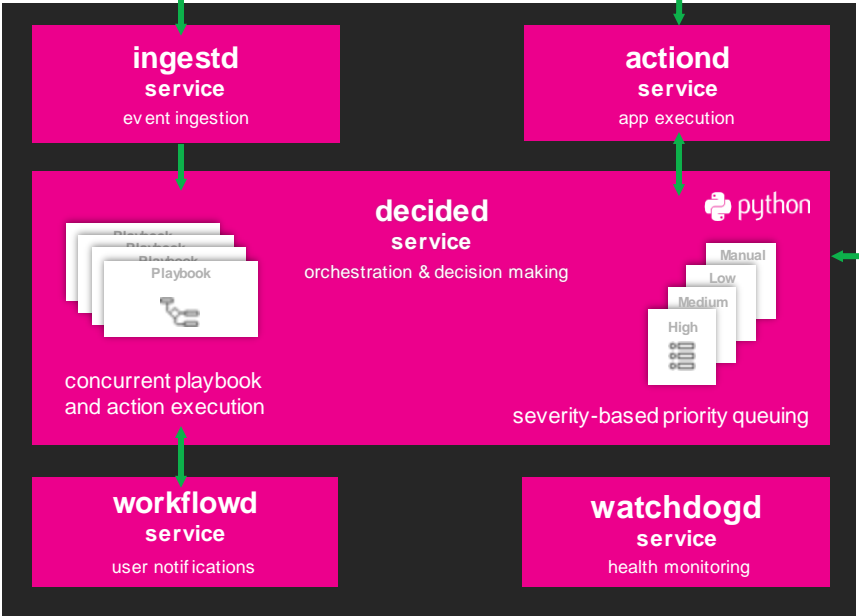
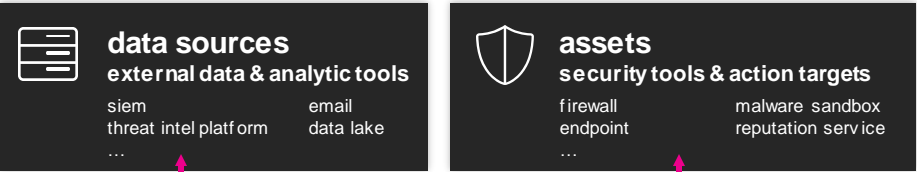


Phantom Services

Platform Services

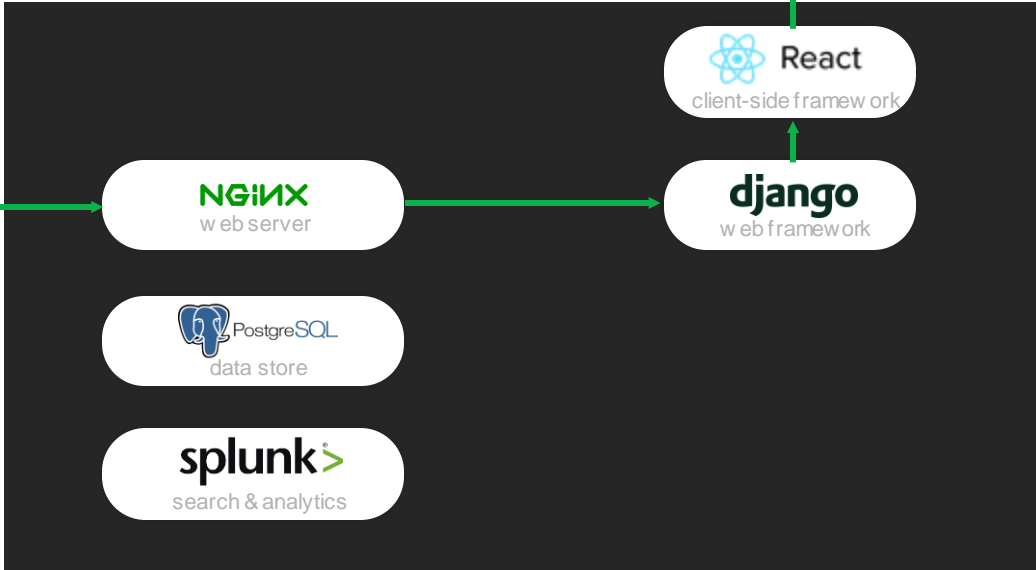
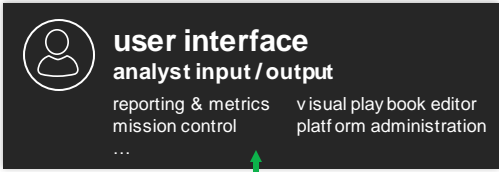
Phantom Platform Architecture

External Platforms & Services



Phantom Services

Human-Machine Interfaces



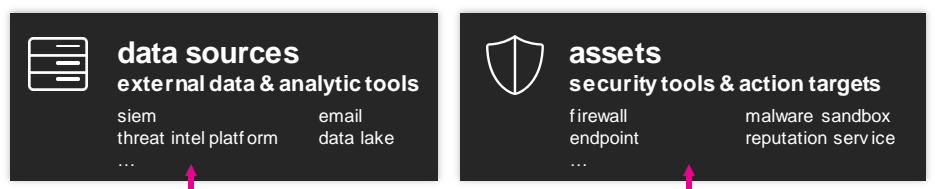
Platform Services

LEGEND

- ↕ = External Communication
- ↕ = IPC

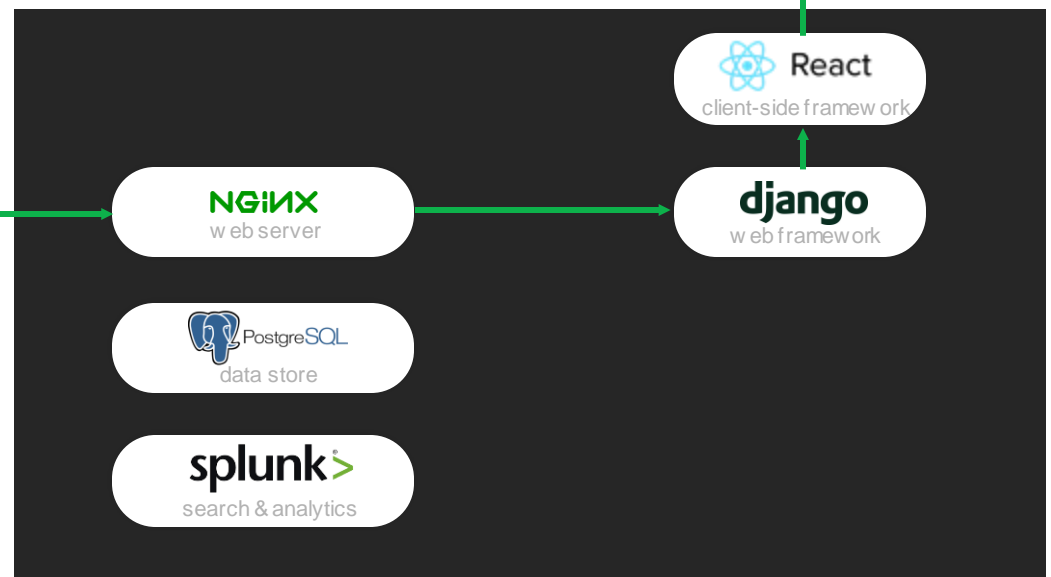
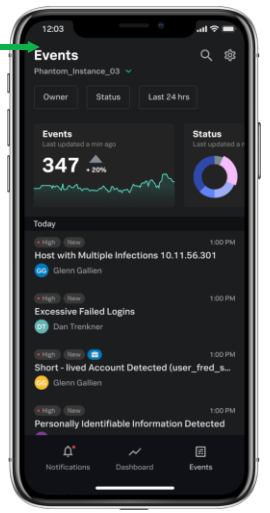
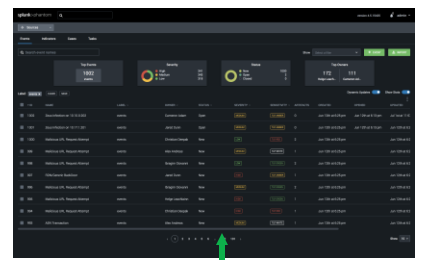
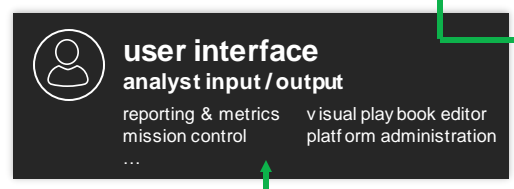
Phantom Platform Architecture

External Platforms & Services



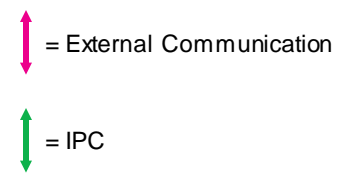
Phantom Services

Human-Machine Interfaces



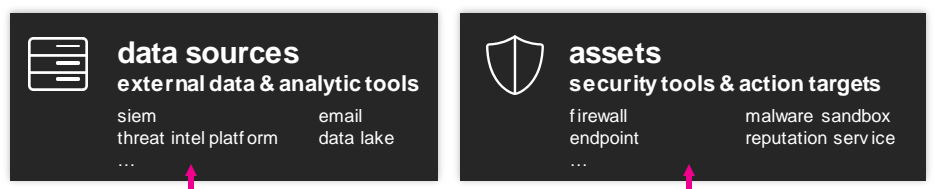
Platform Services

LEGEND



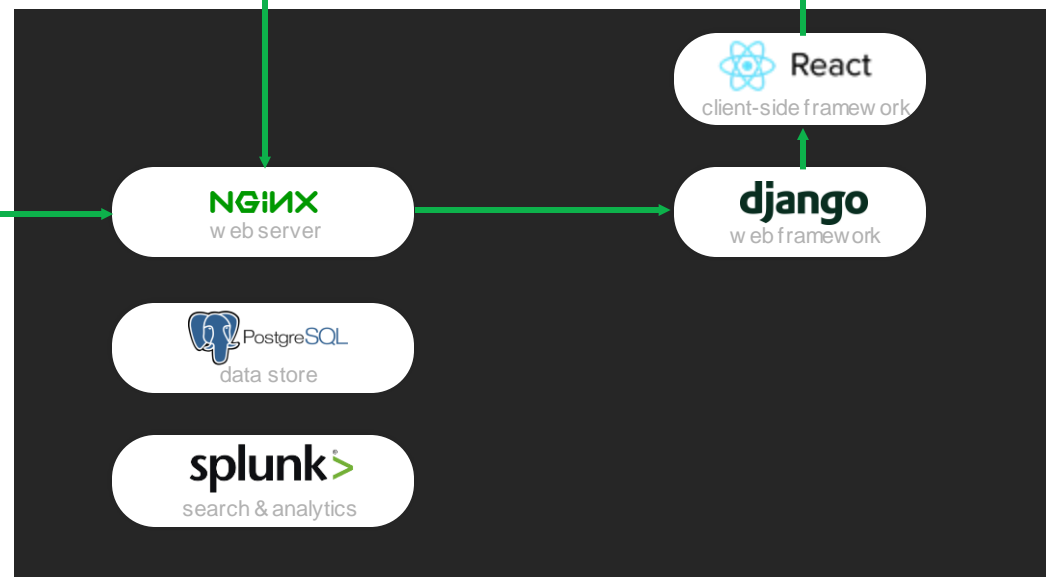
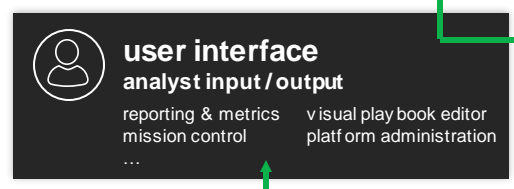
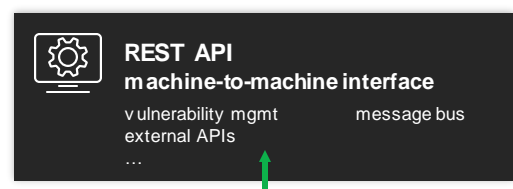
Phantom Platform Architecture

External Platforms & Services

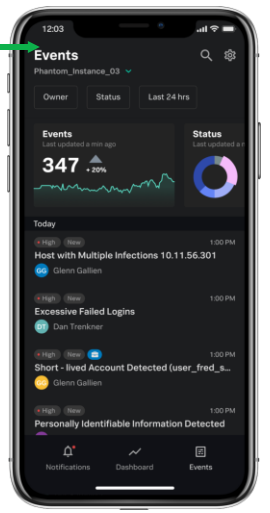
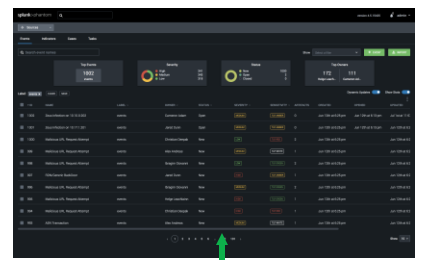


Phantom Services

Human-Machine Interfaces



Platform Services



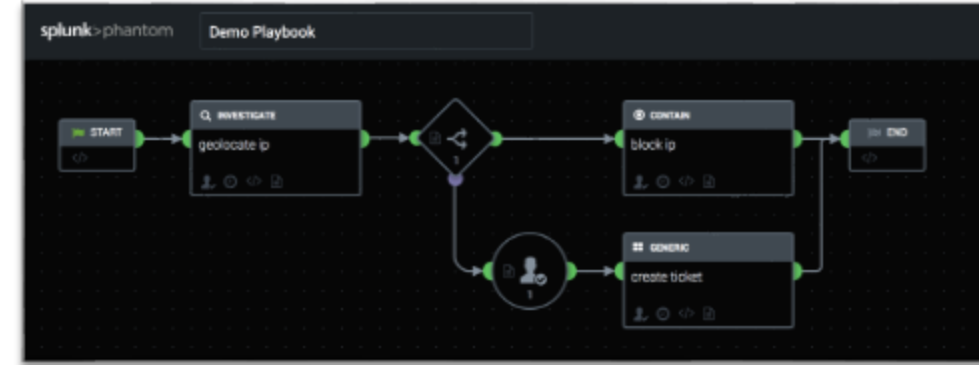
LEGEND

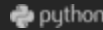
- ↕ = External Communication
- ↕ = IPC



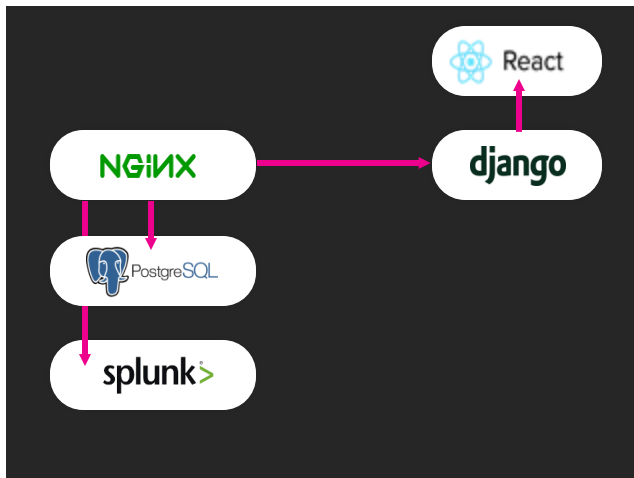
Playbook Execution

Playbook Execution

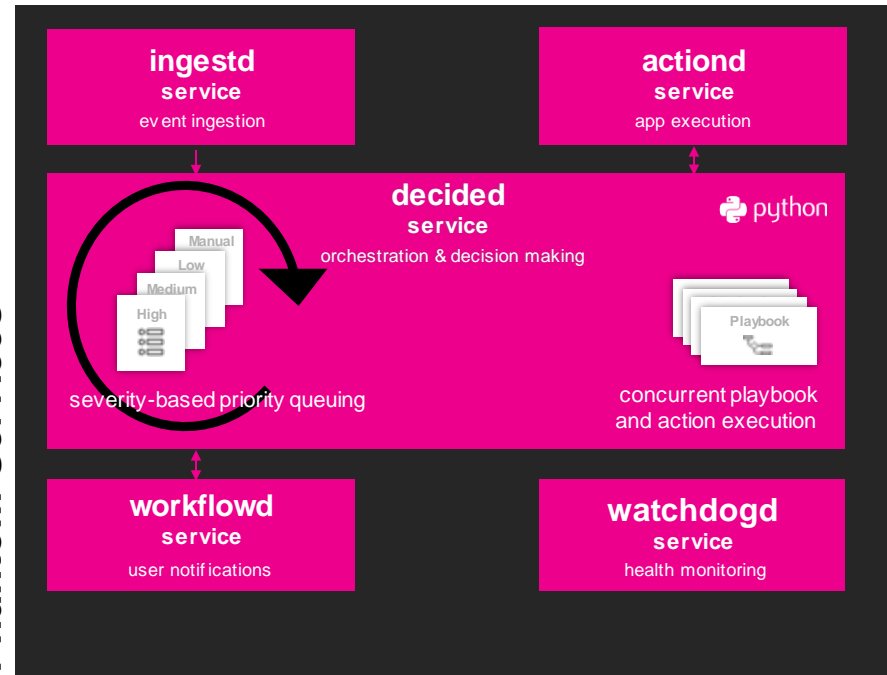


app process 
invoke action, return data

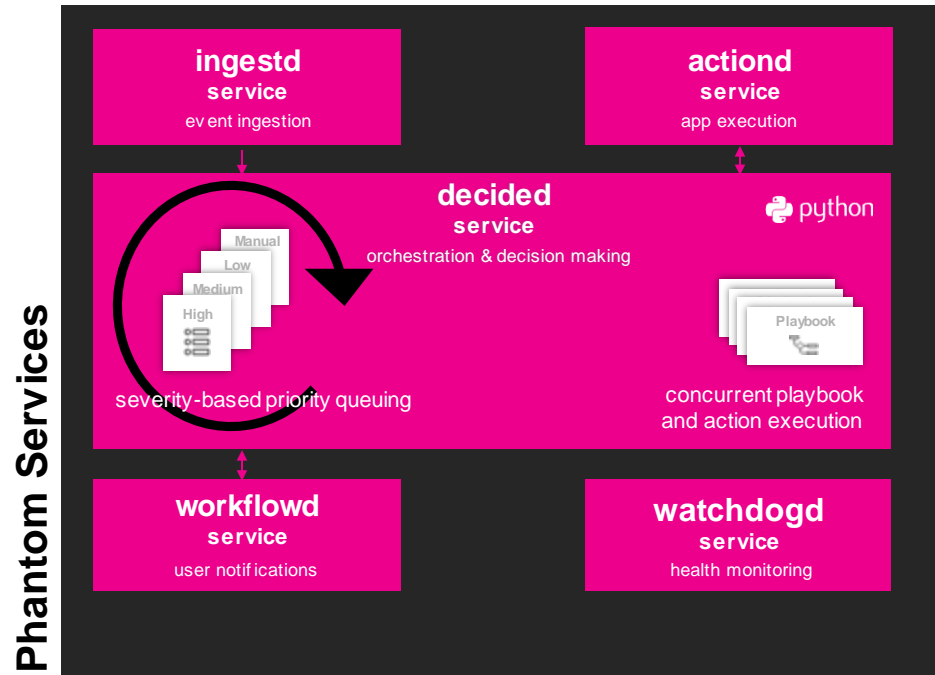
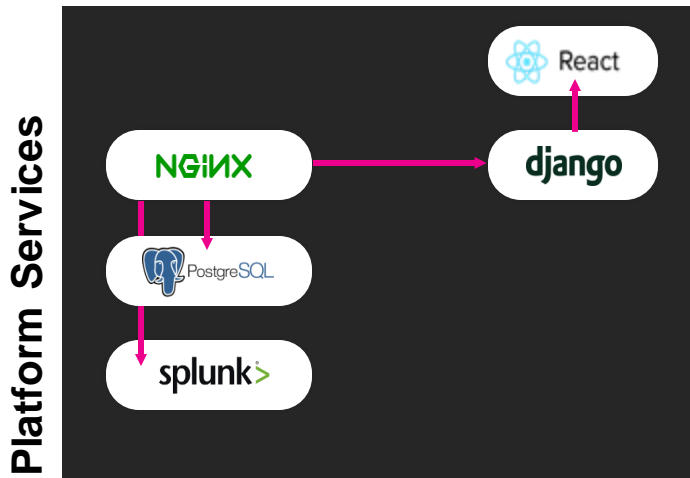
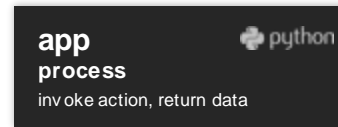
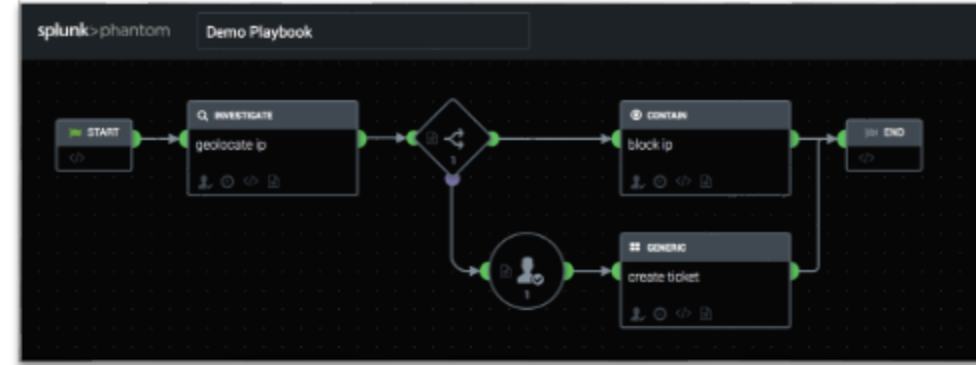
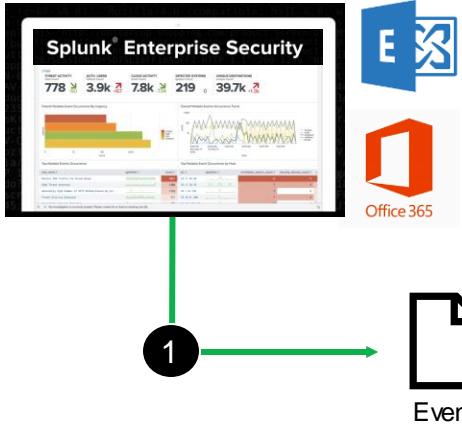
Platform Services



Phantom Services



Playbook Execution



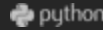
Playbook Execution

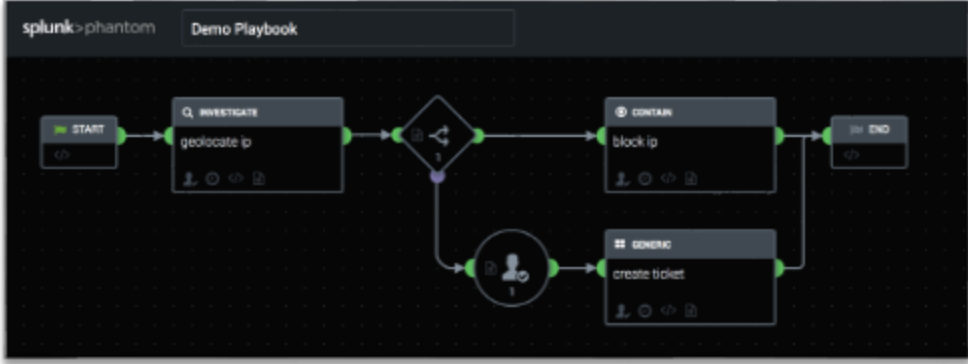


1

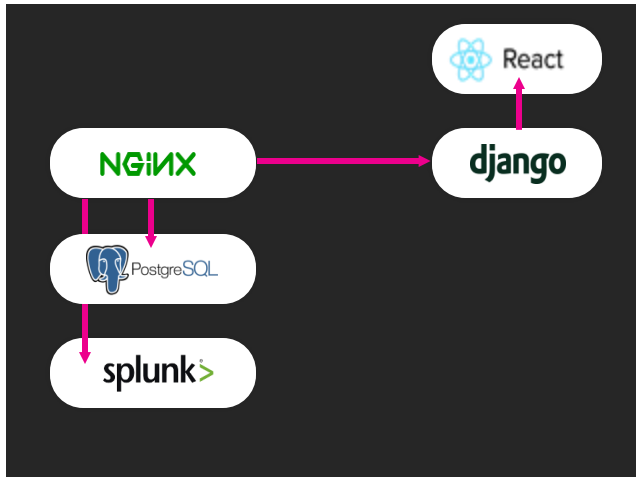


2

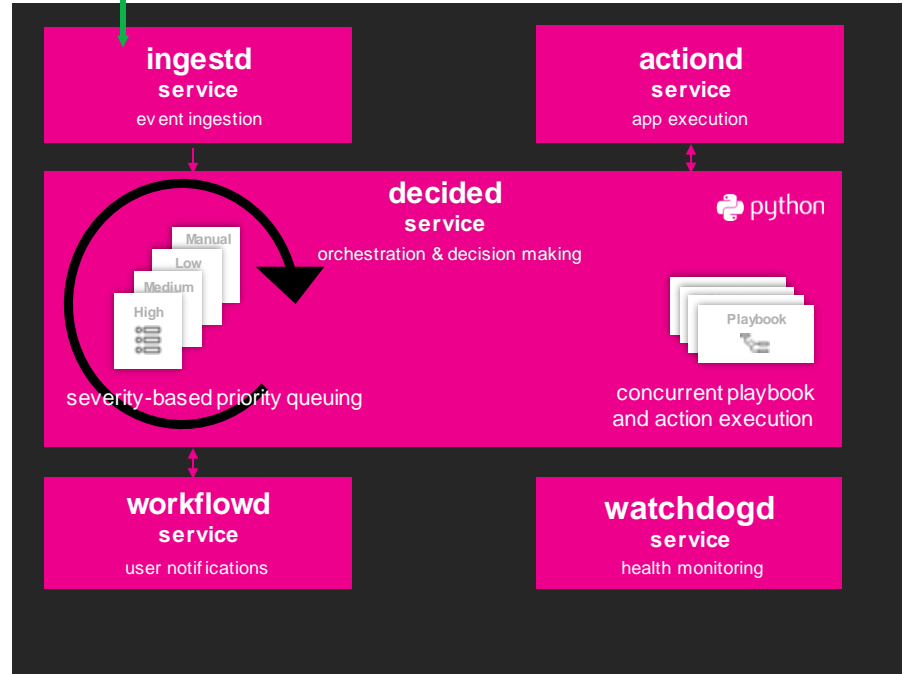
app process 
invoke action, return data



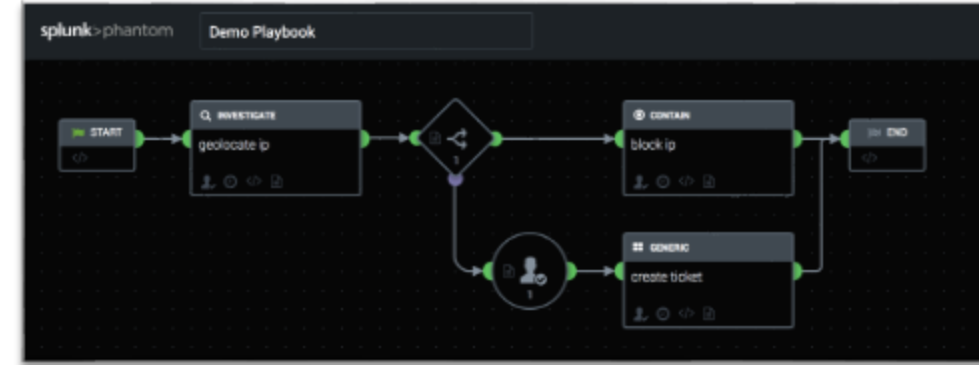
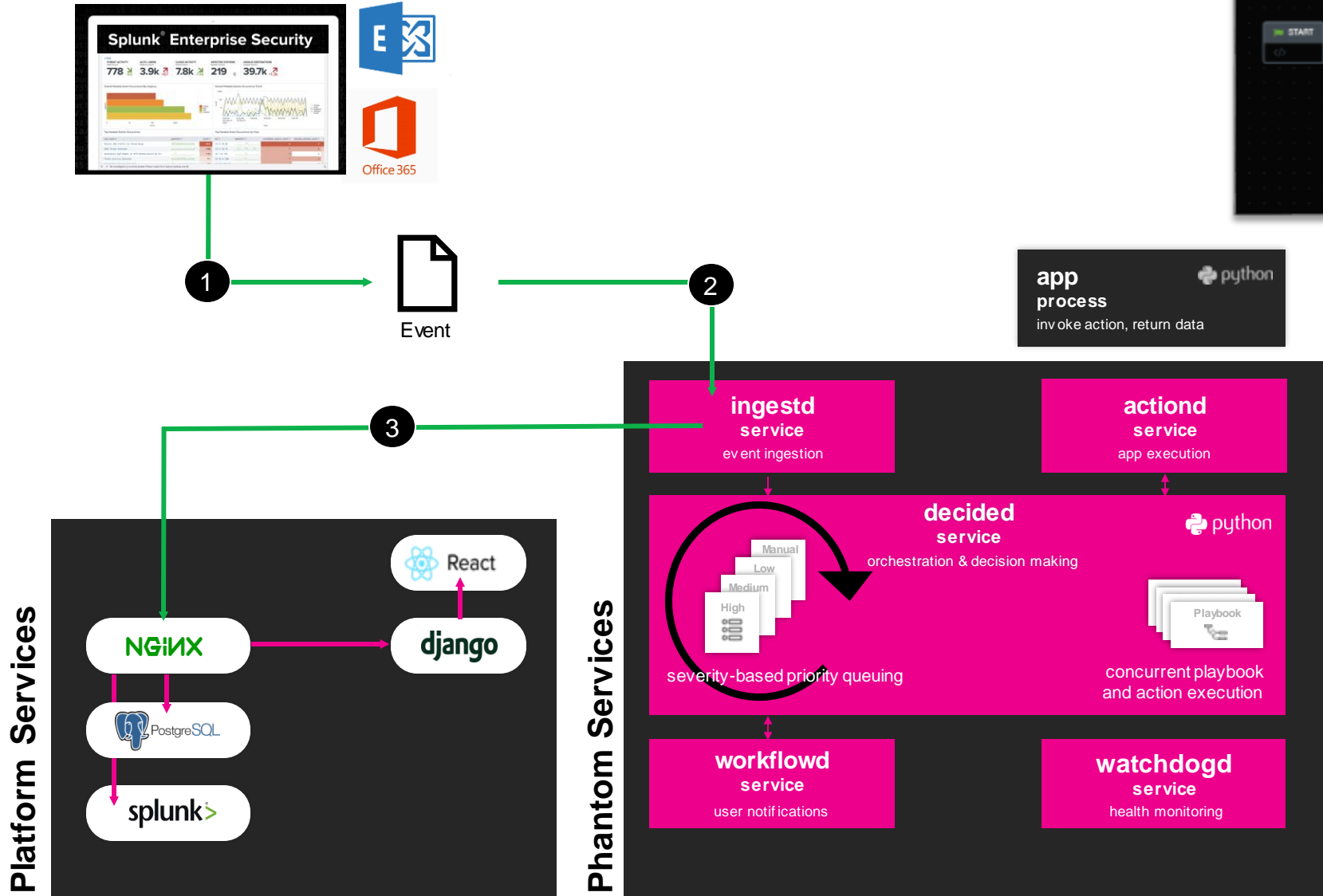
Platform Services



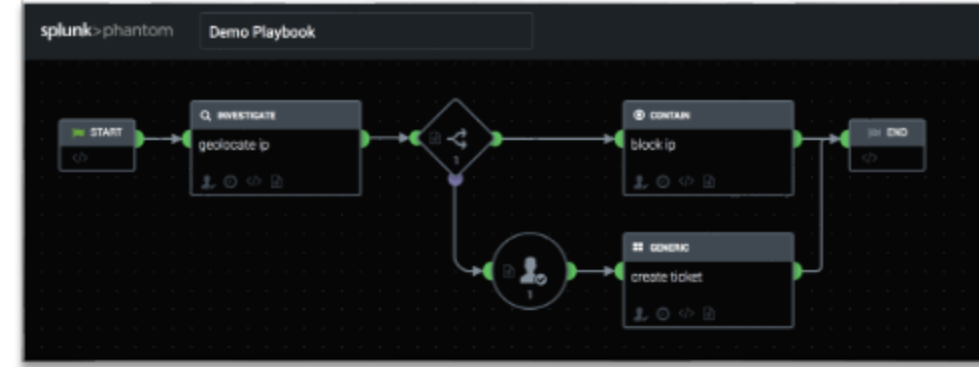
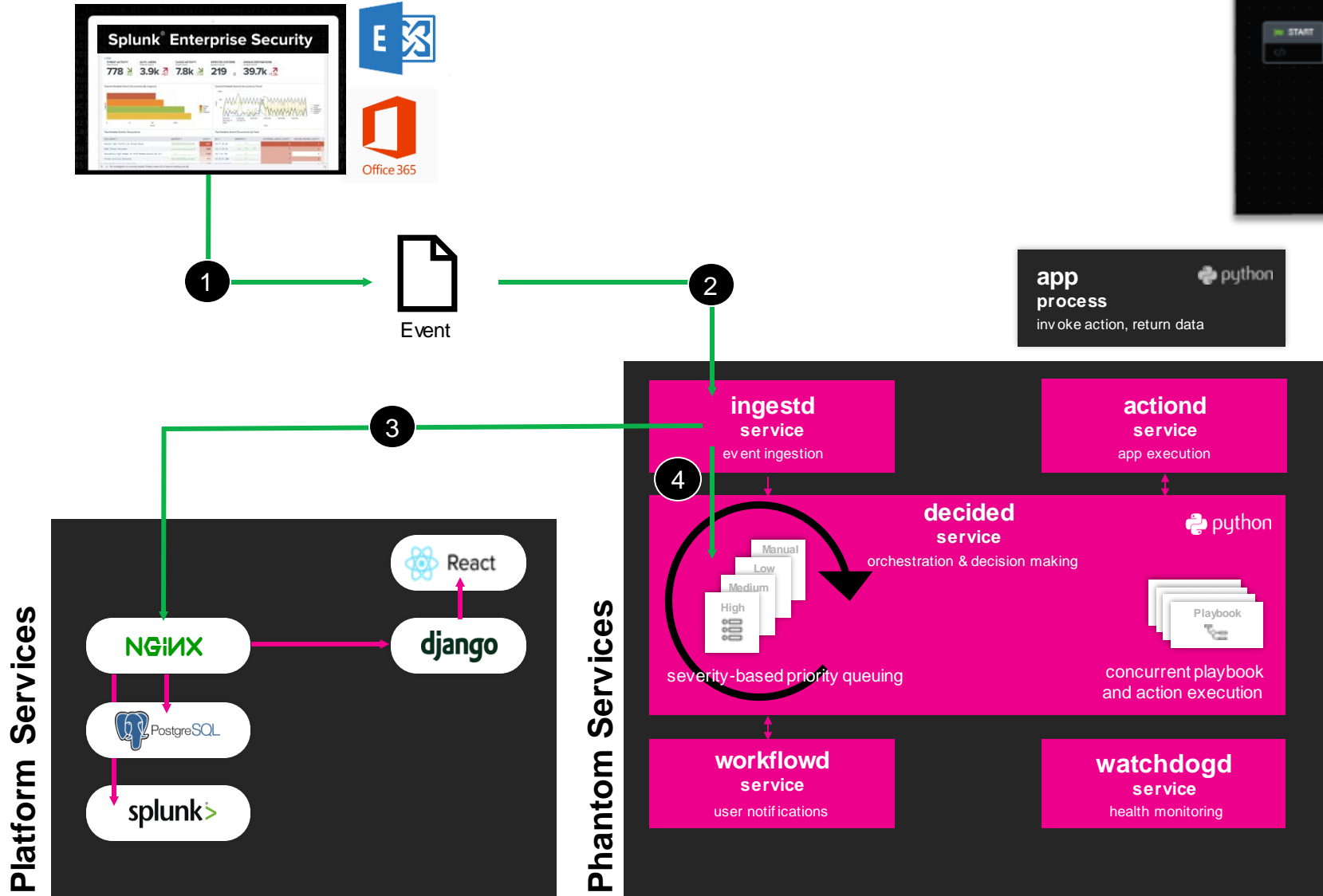
Phantom Services



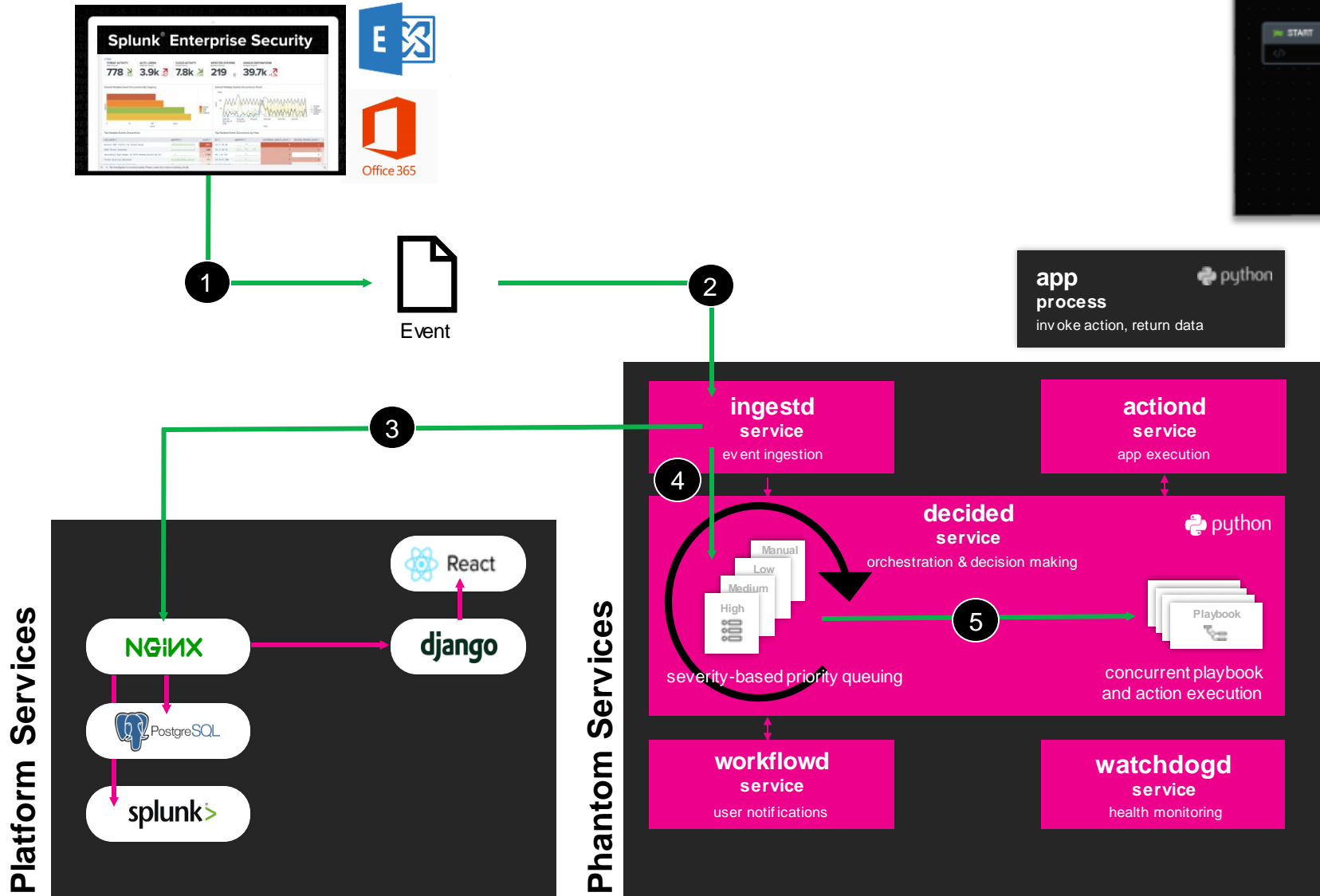
Playbook Execution



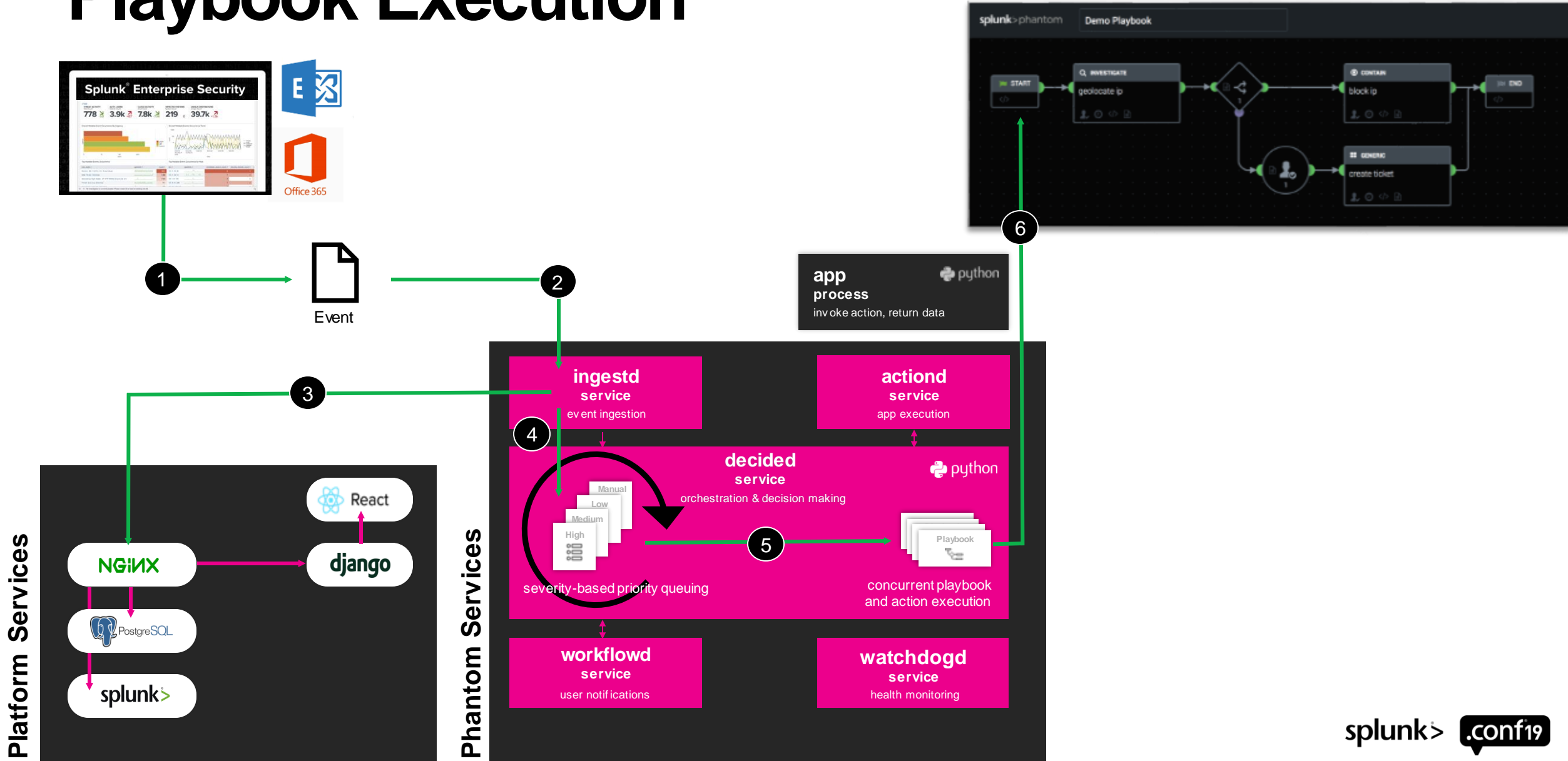
Playbook Execution



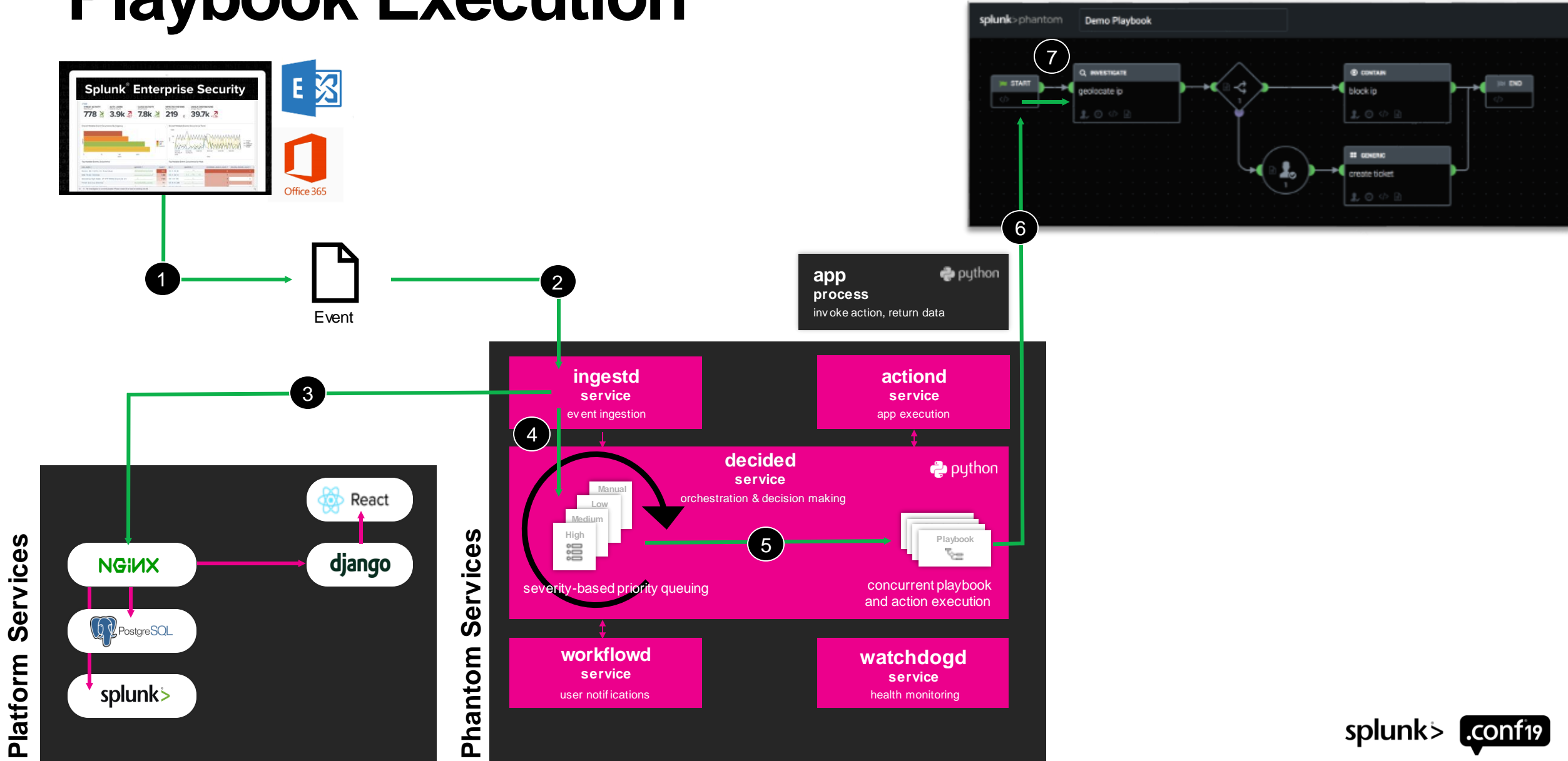
Playbook Execution



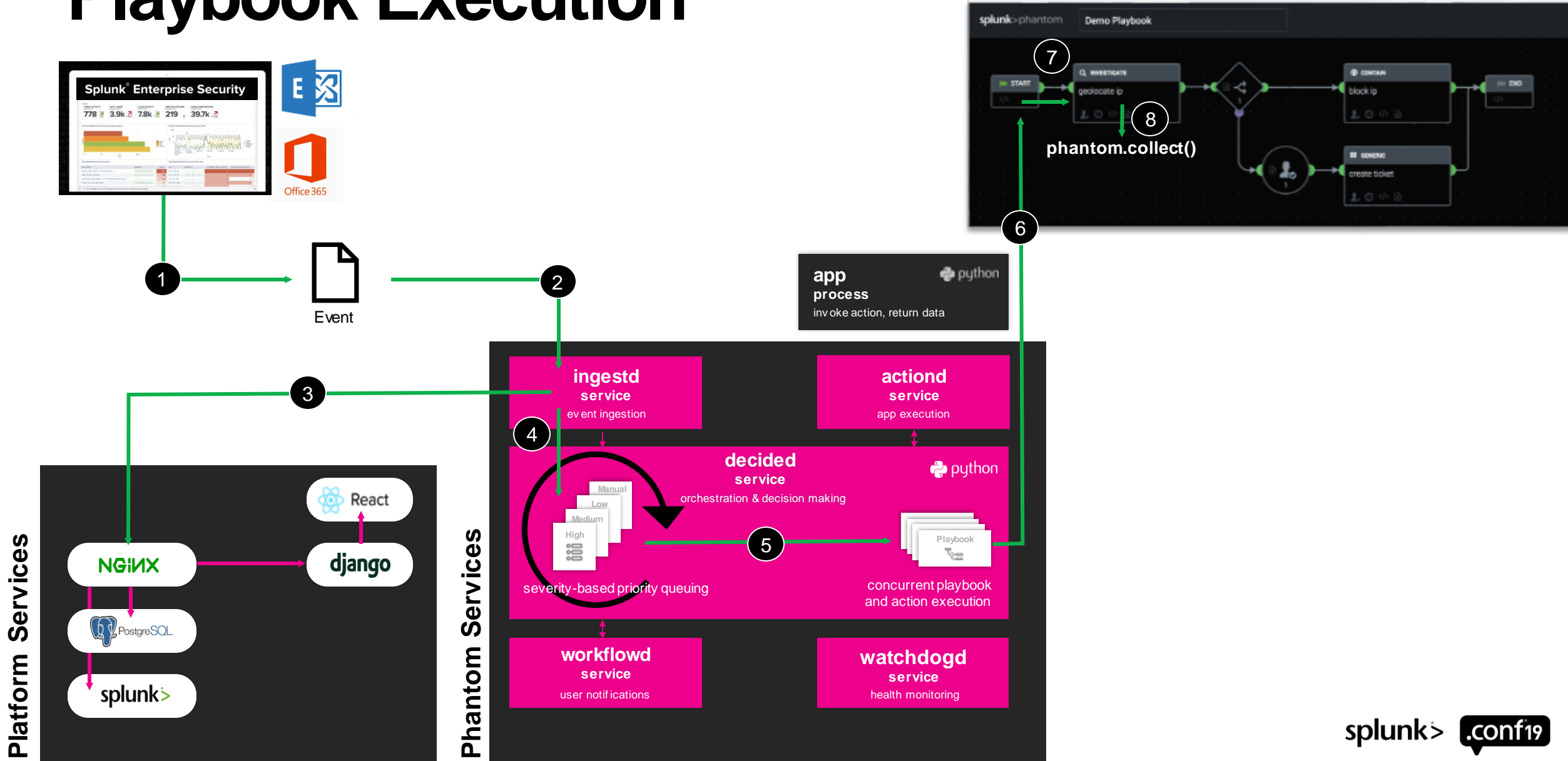
Playbook Execution



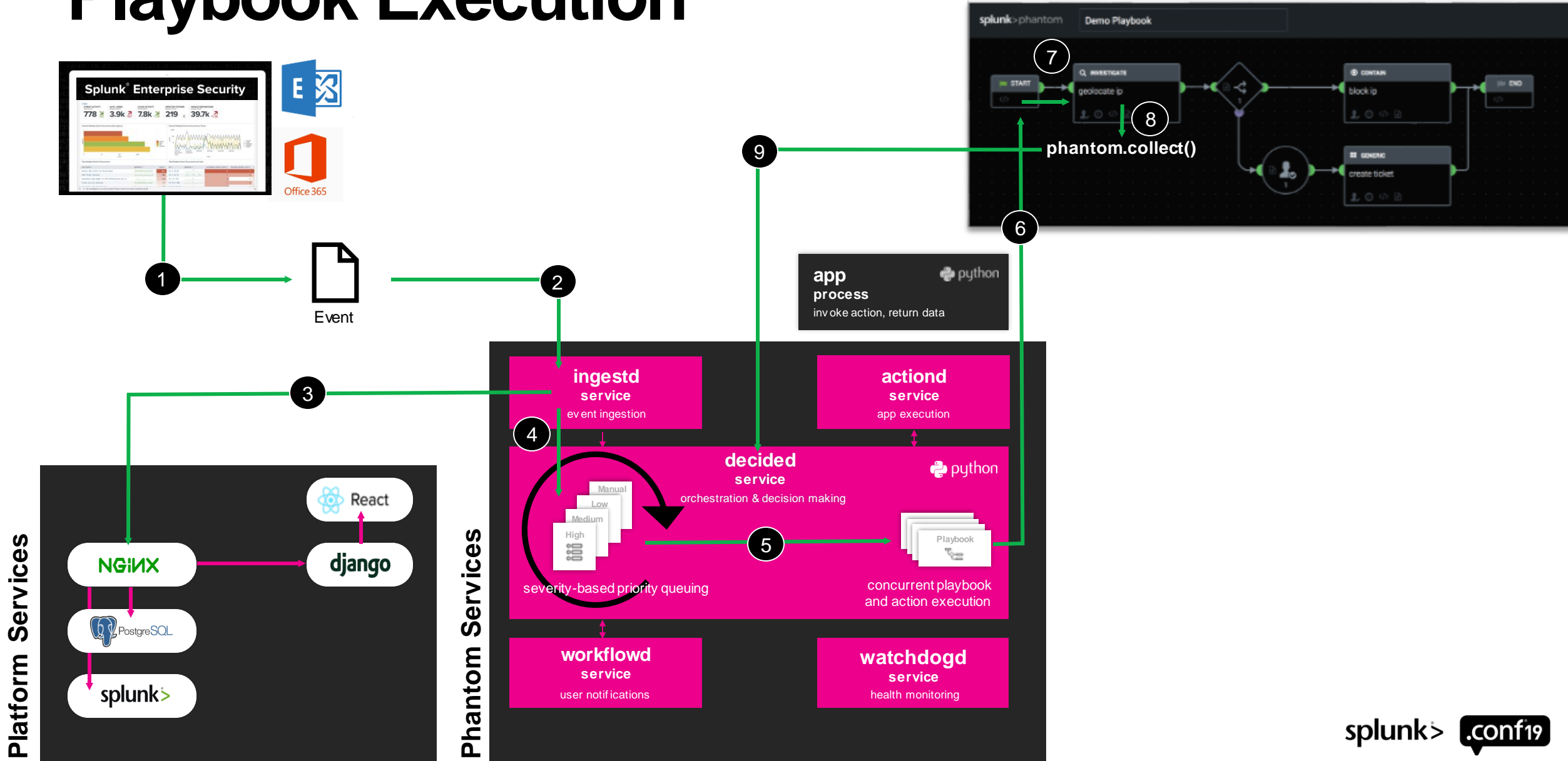
Playbook Execution



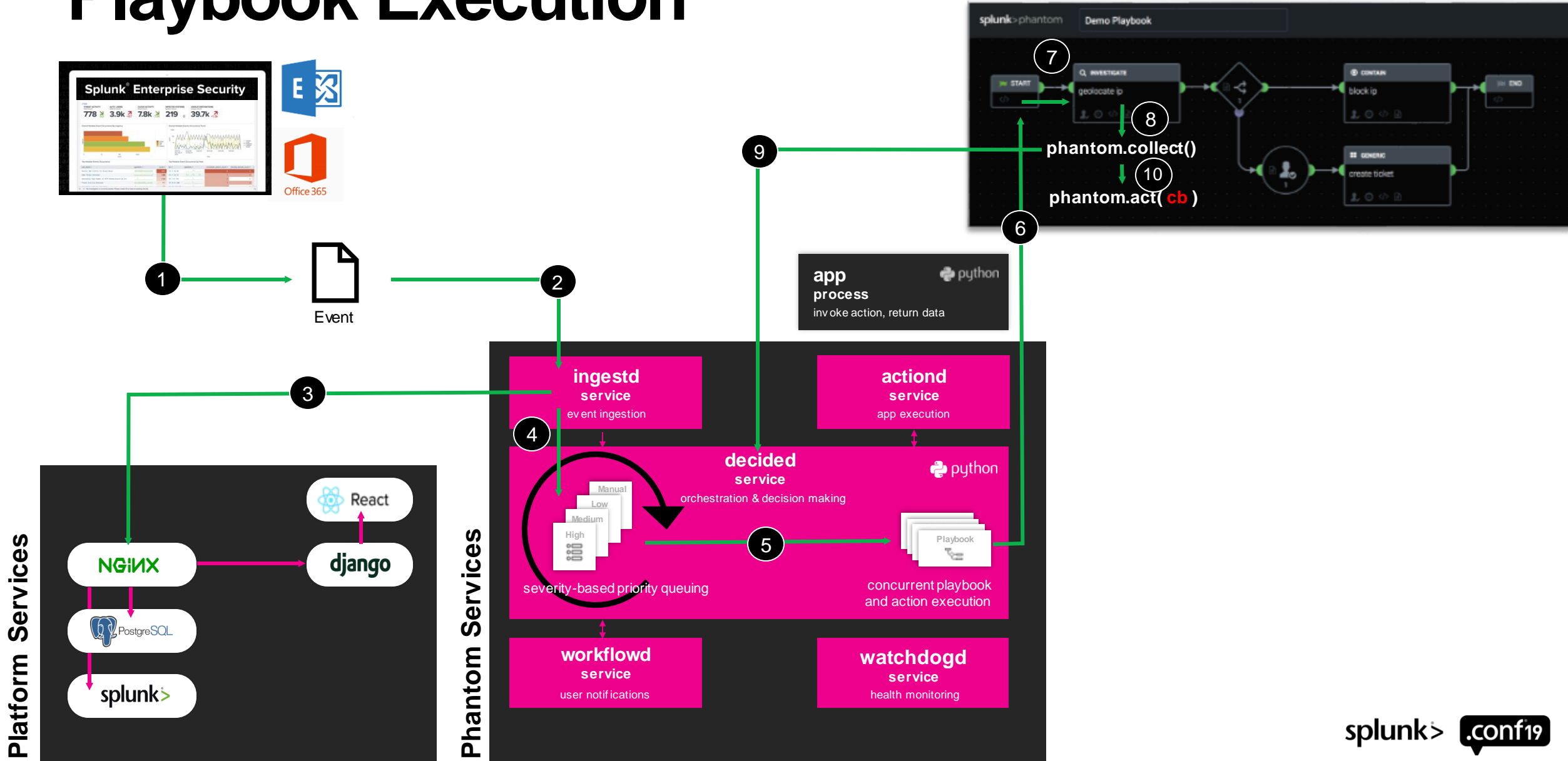
Playbook Execution



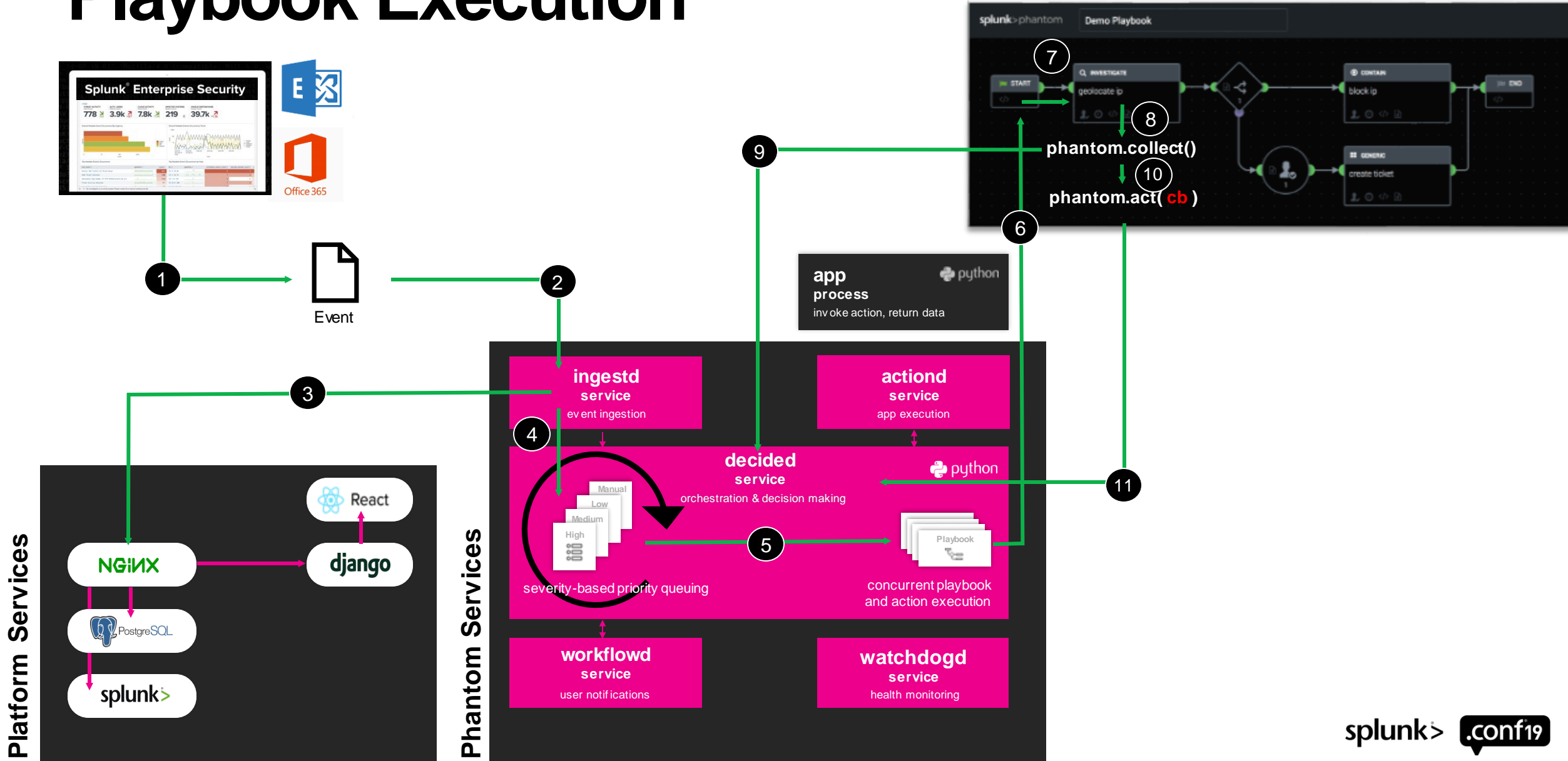
Playbook Execution



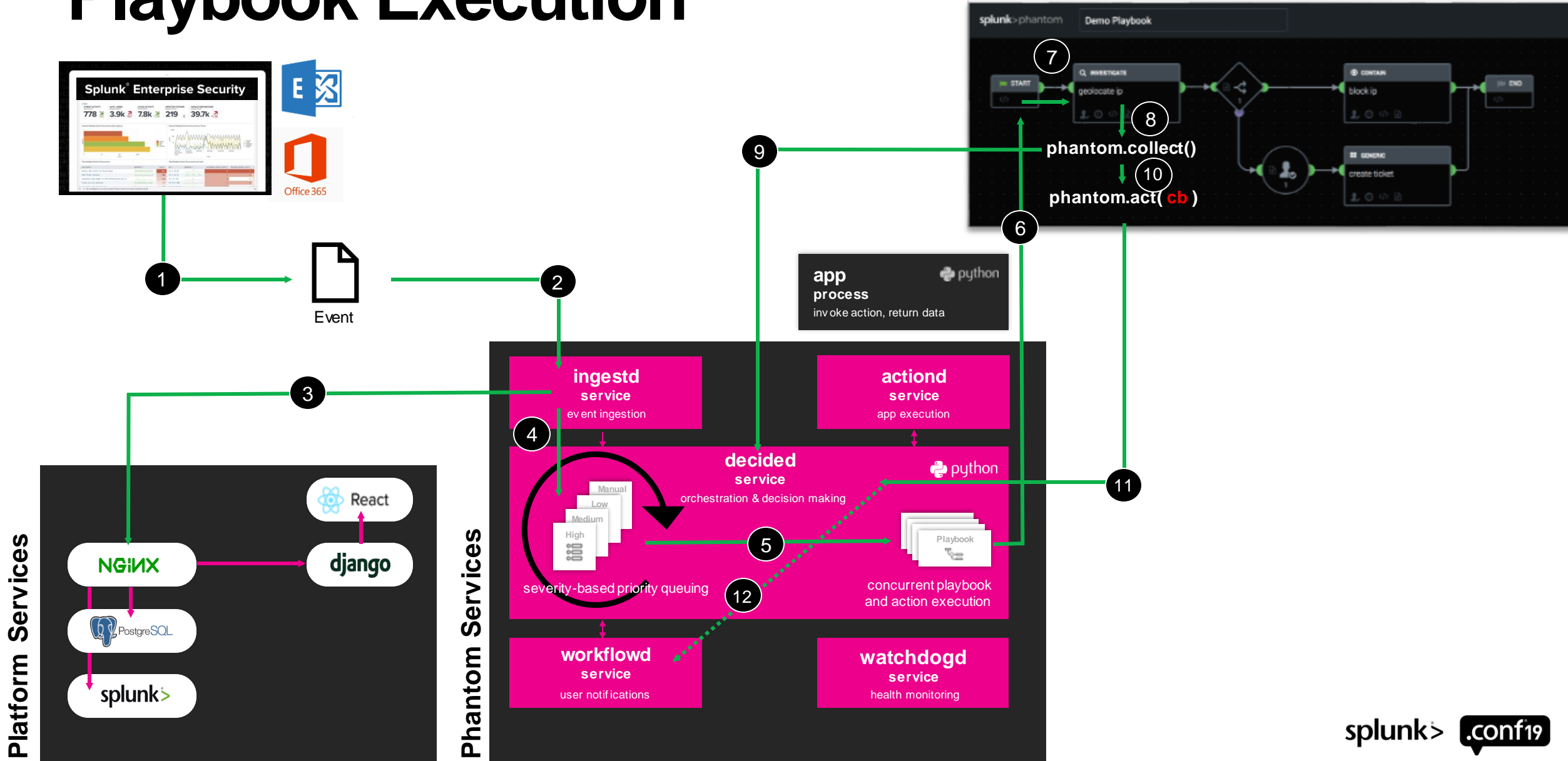
Playbook Execution



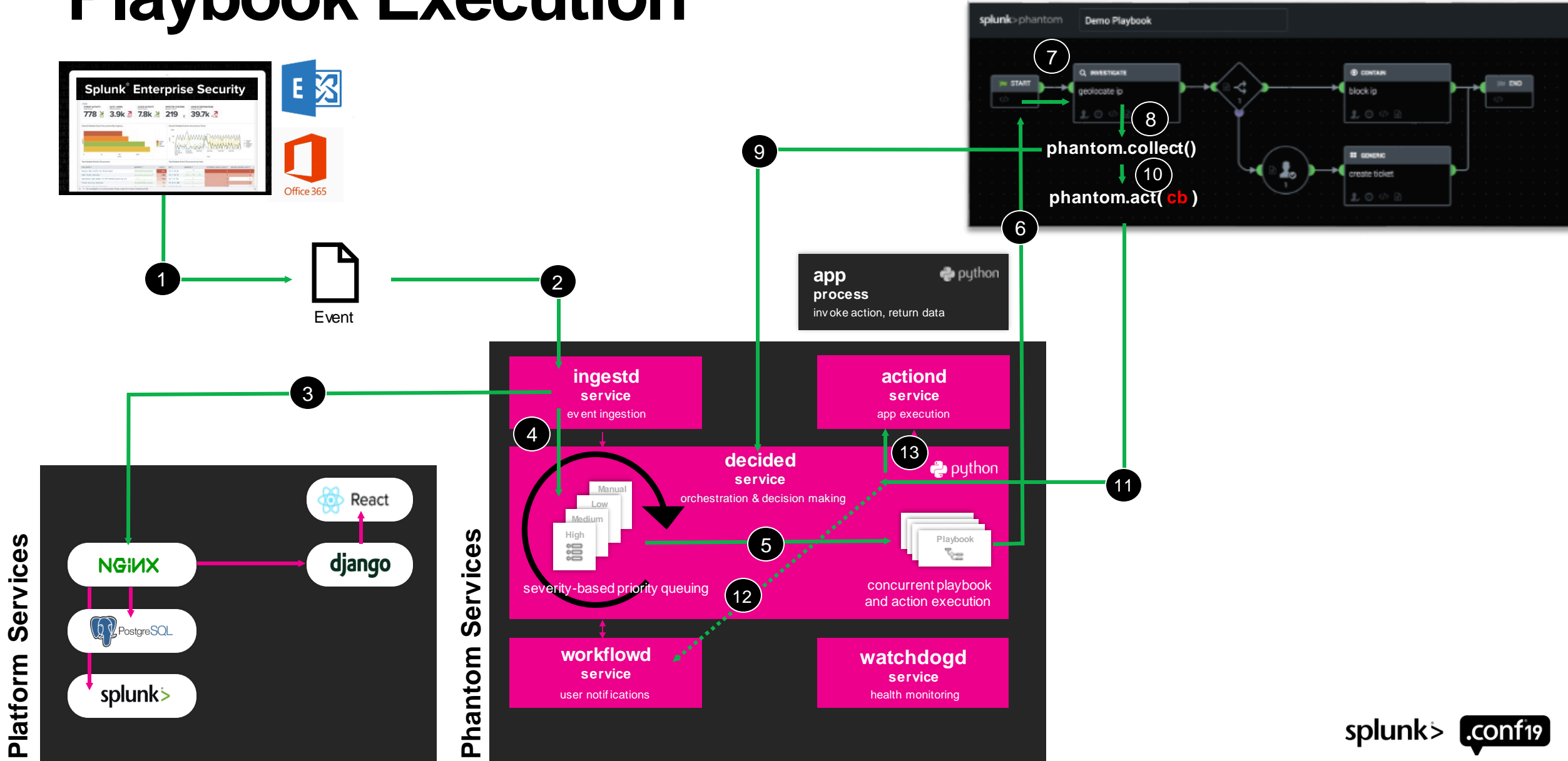
Playbook Execution



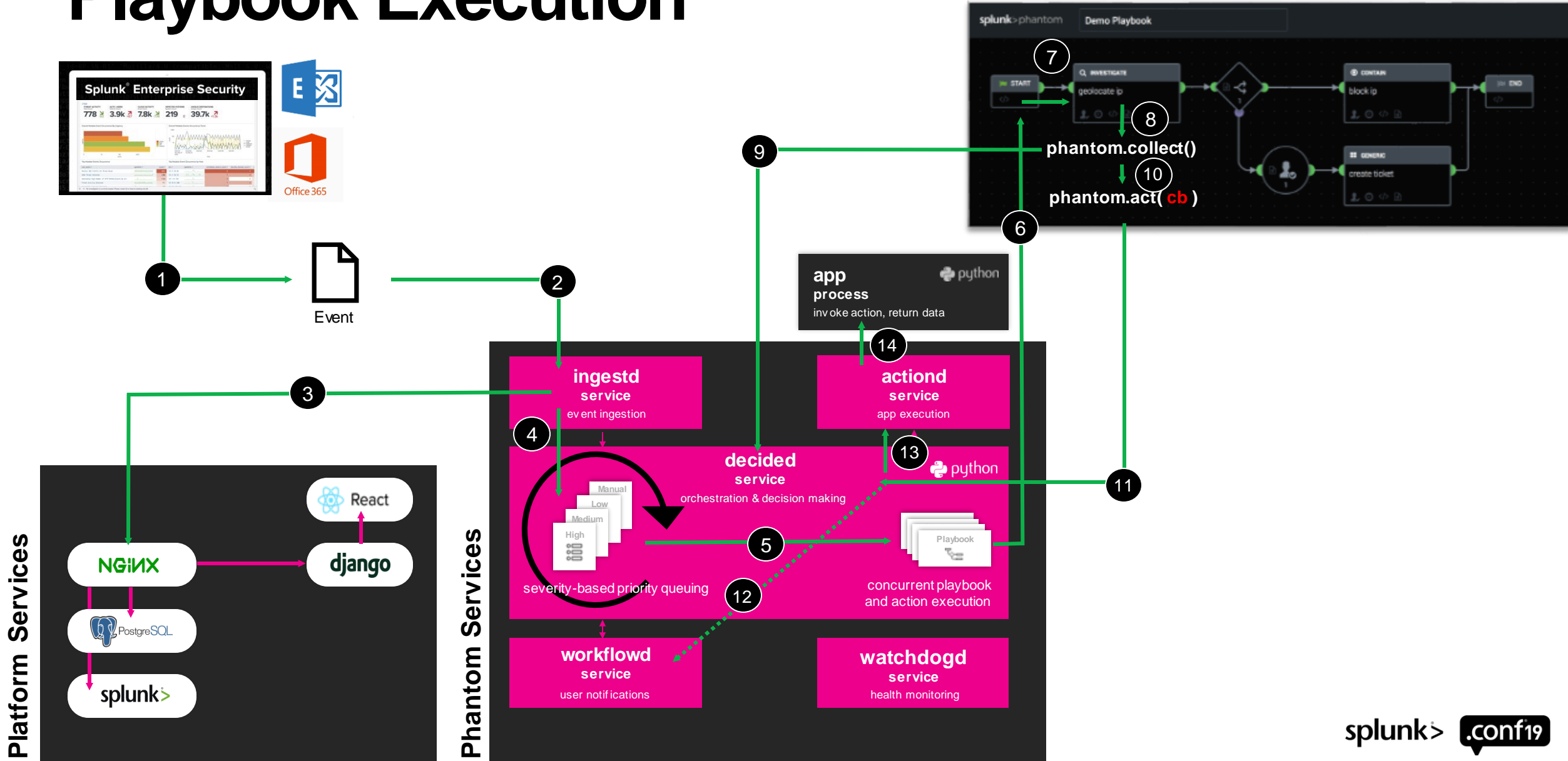
Playbook Execution



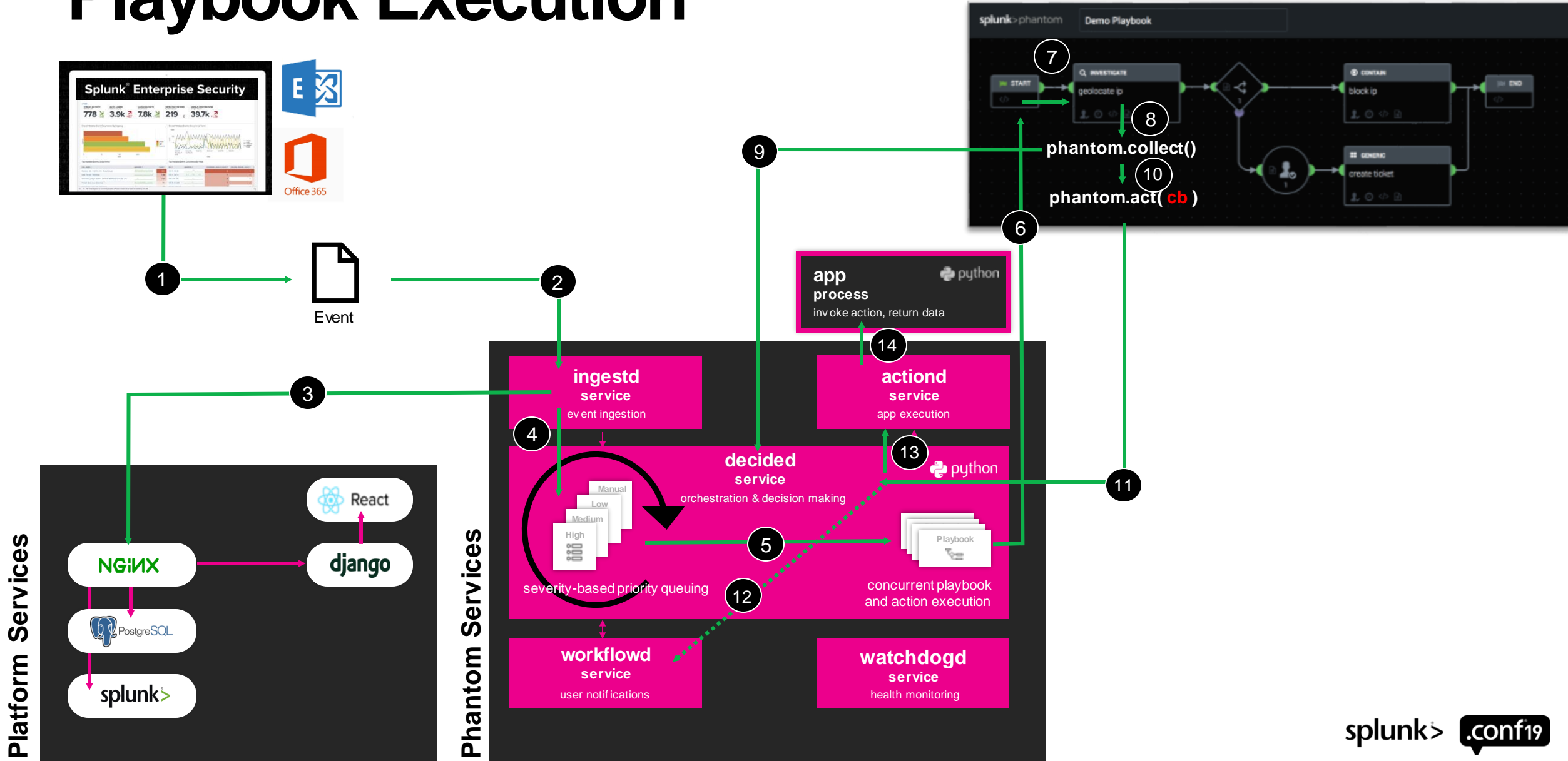
Playbook Execution



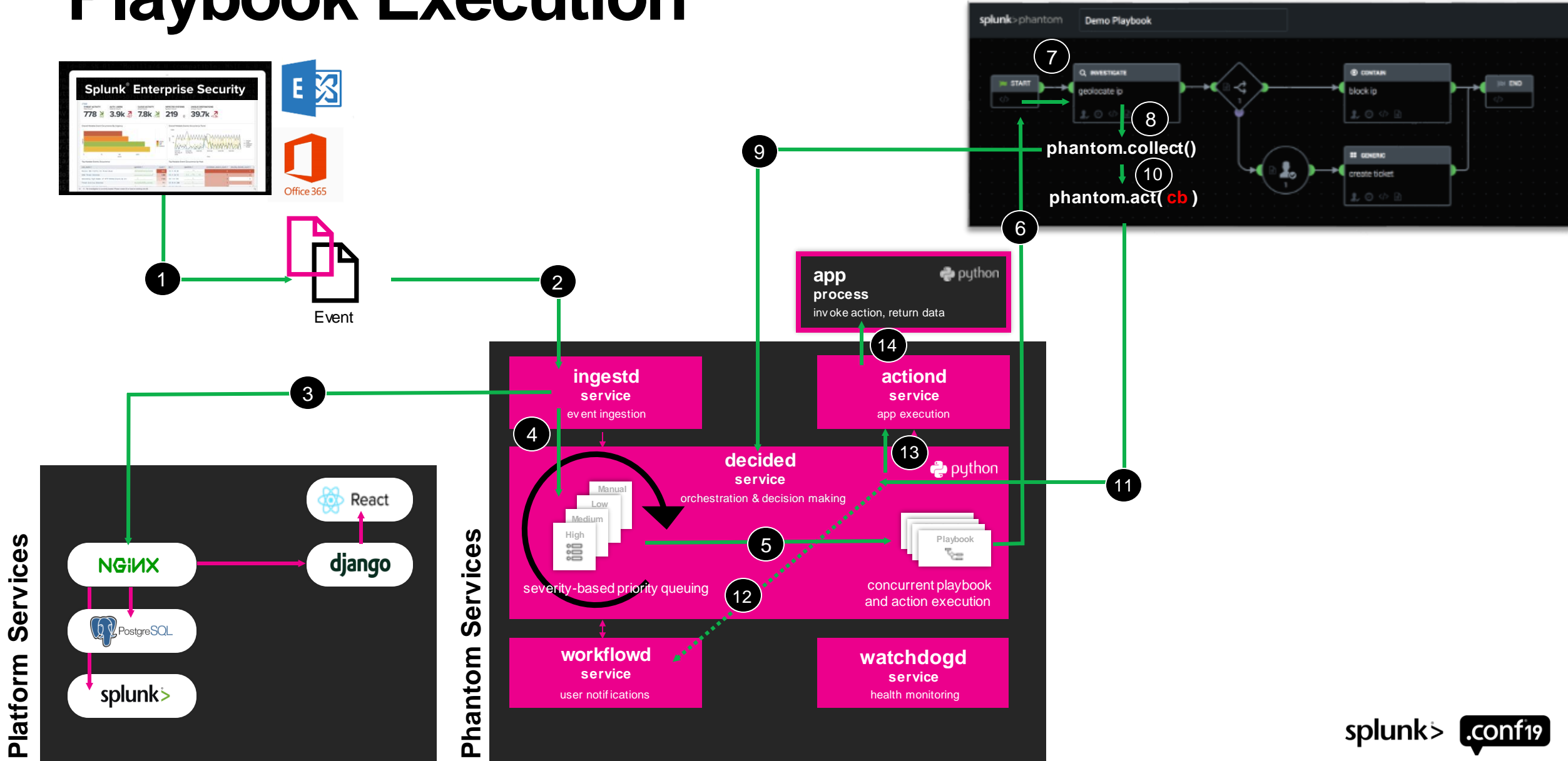
Playbook Execution



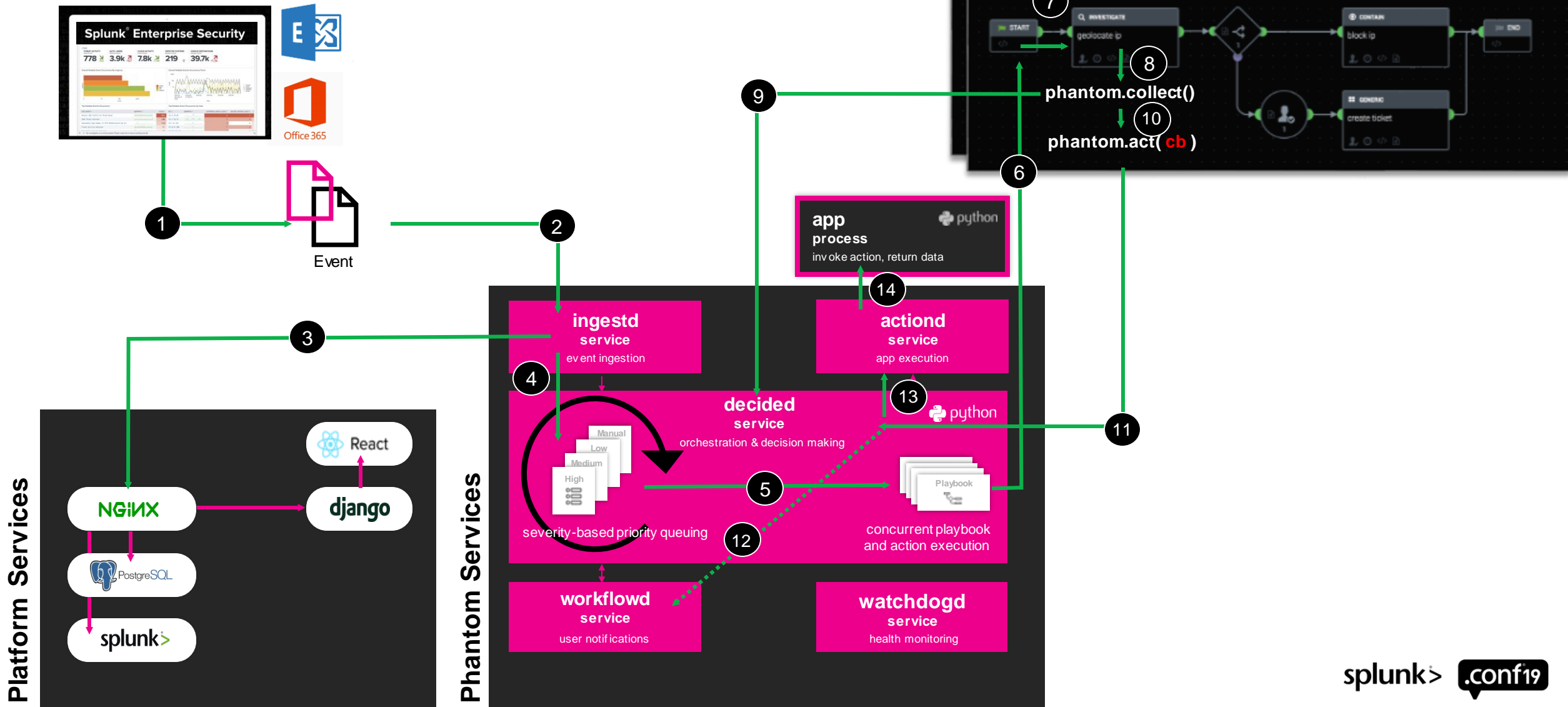
Playbook Execution



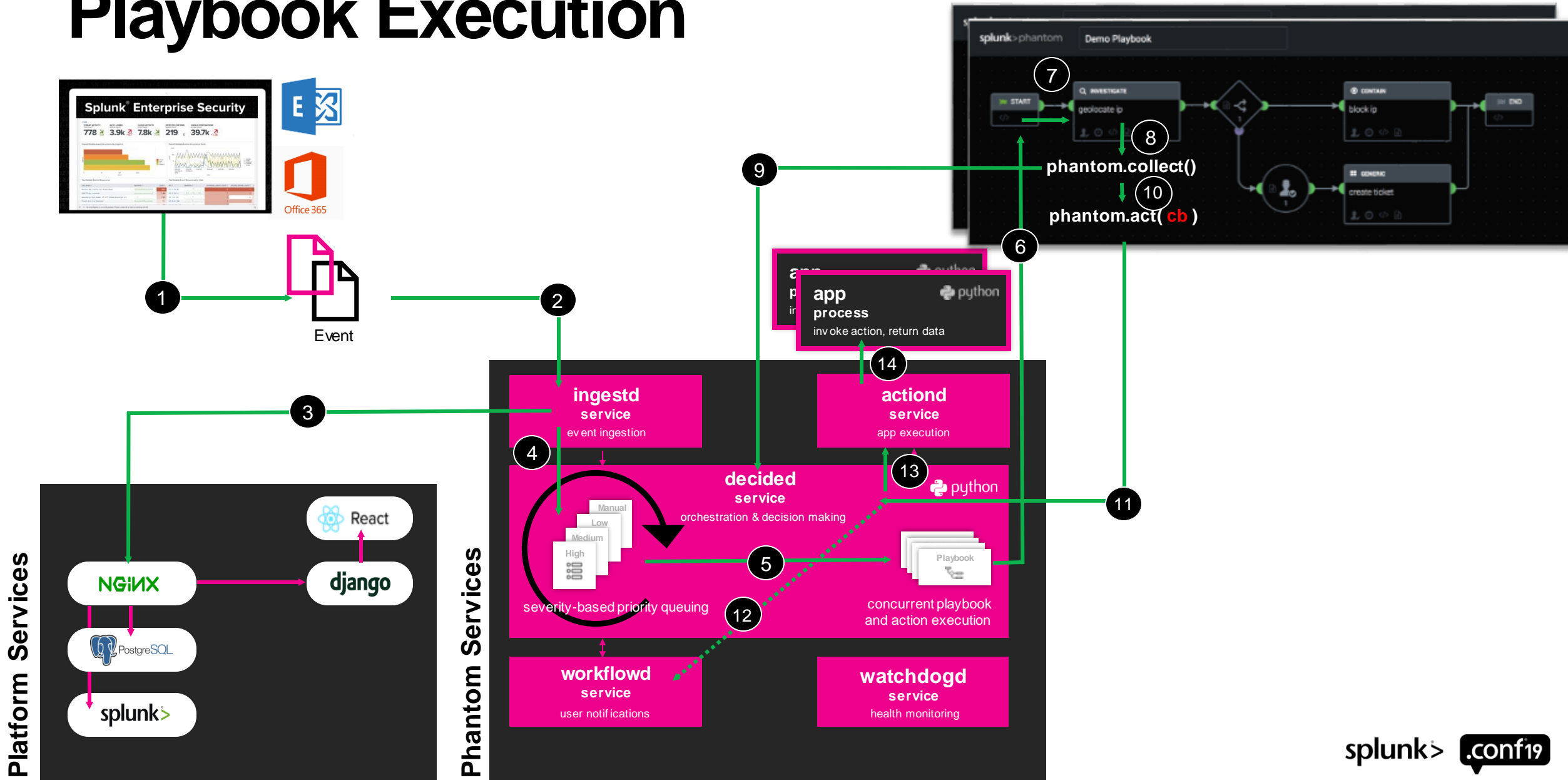
Playbook Execution



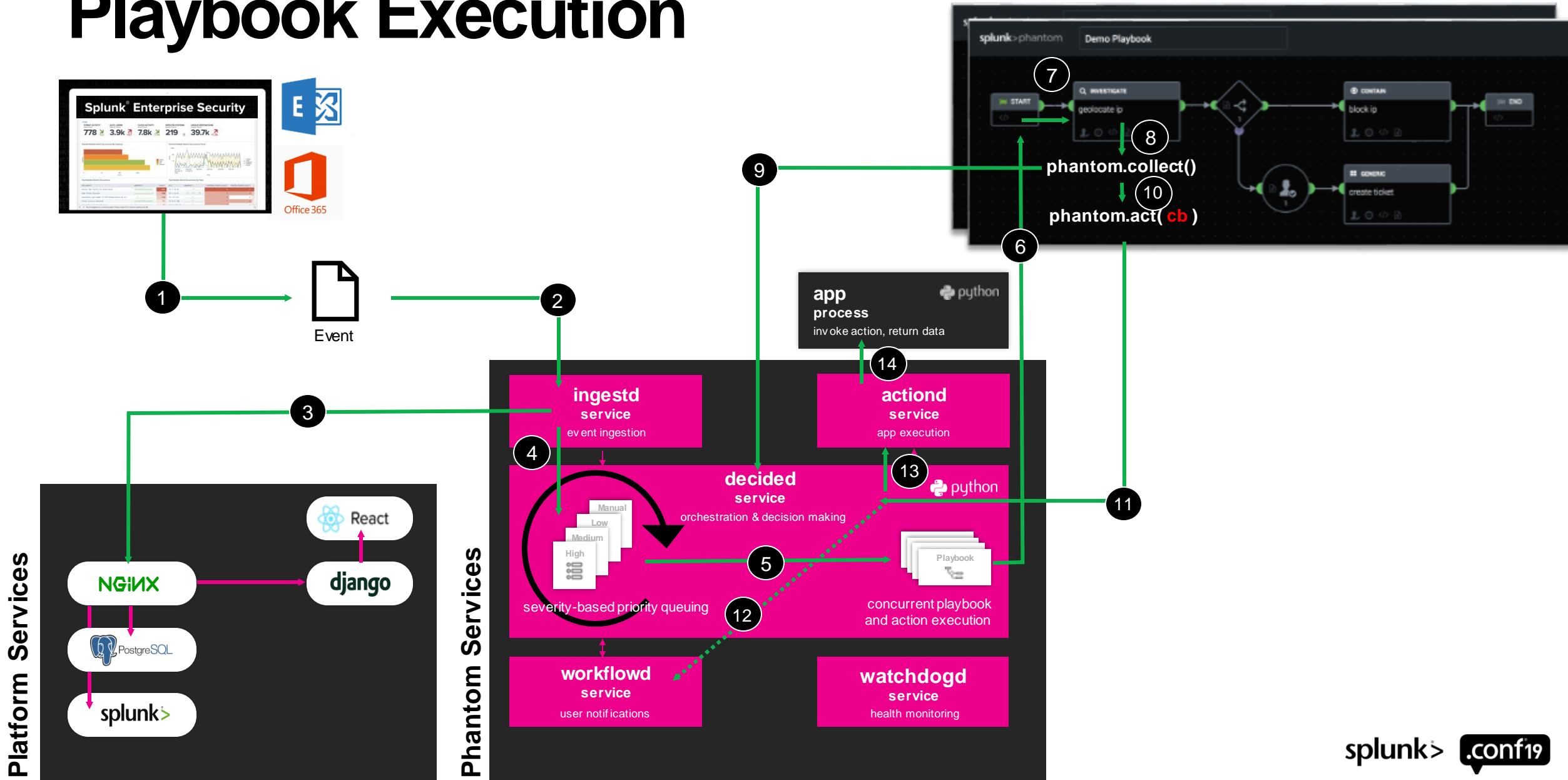
Playbook Execution



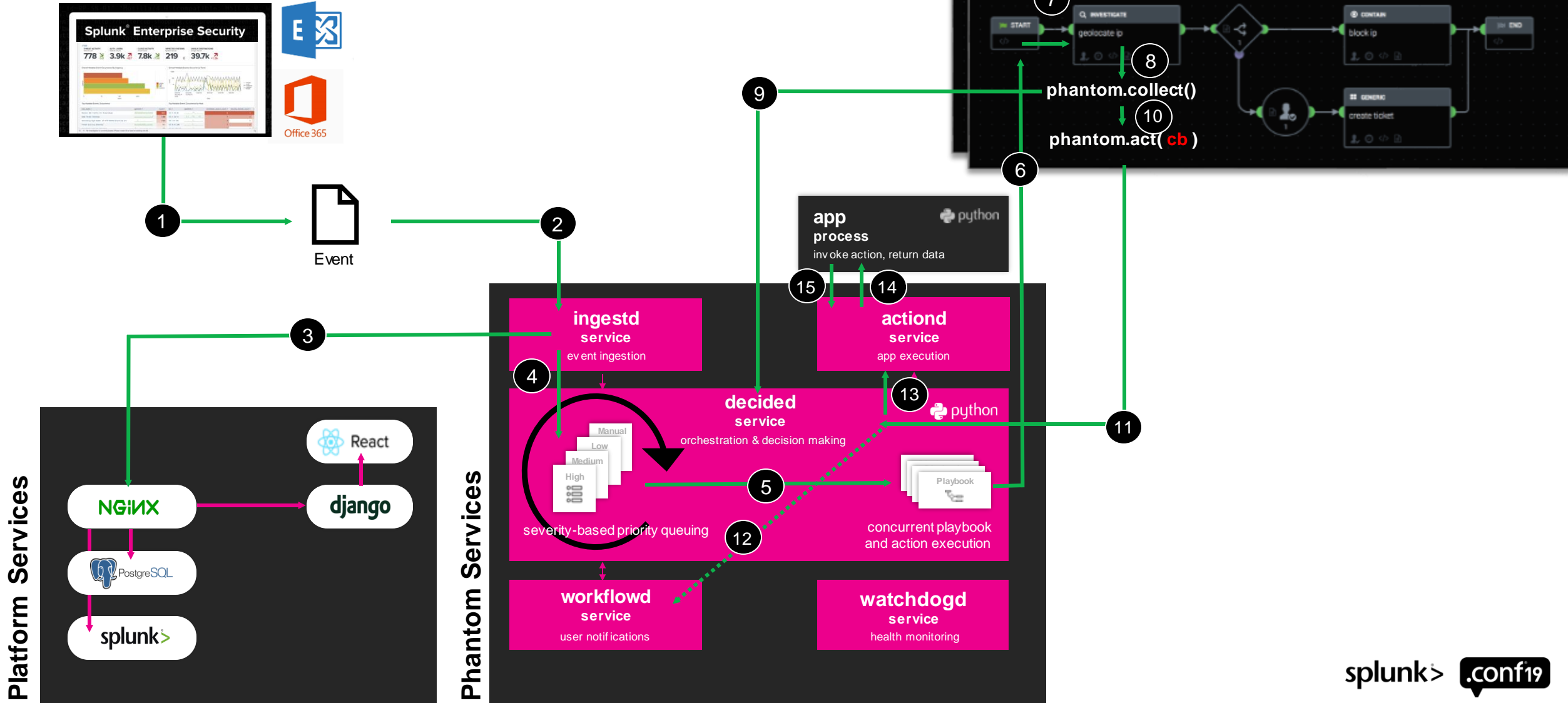
Playbook Execution



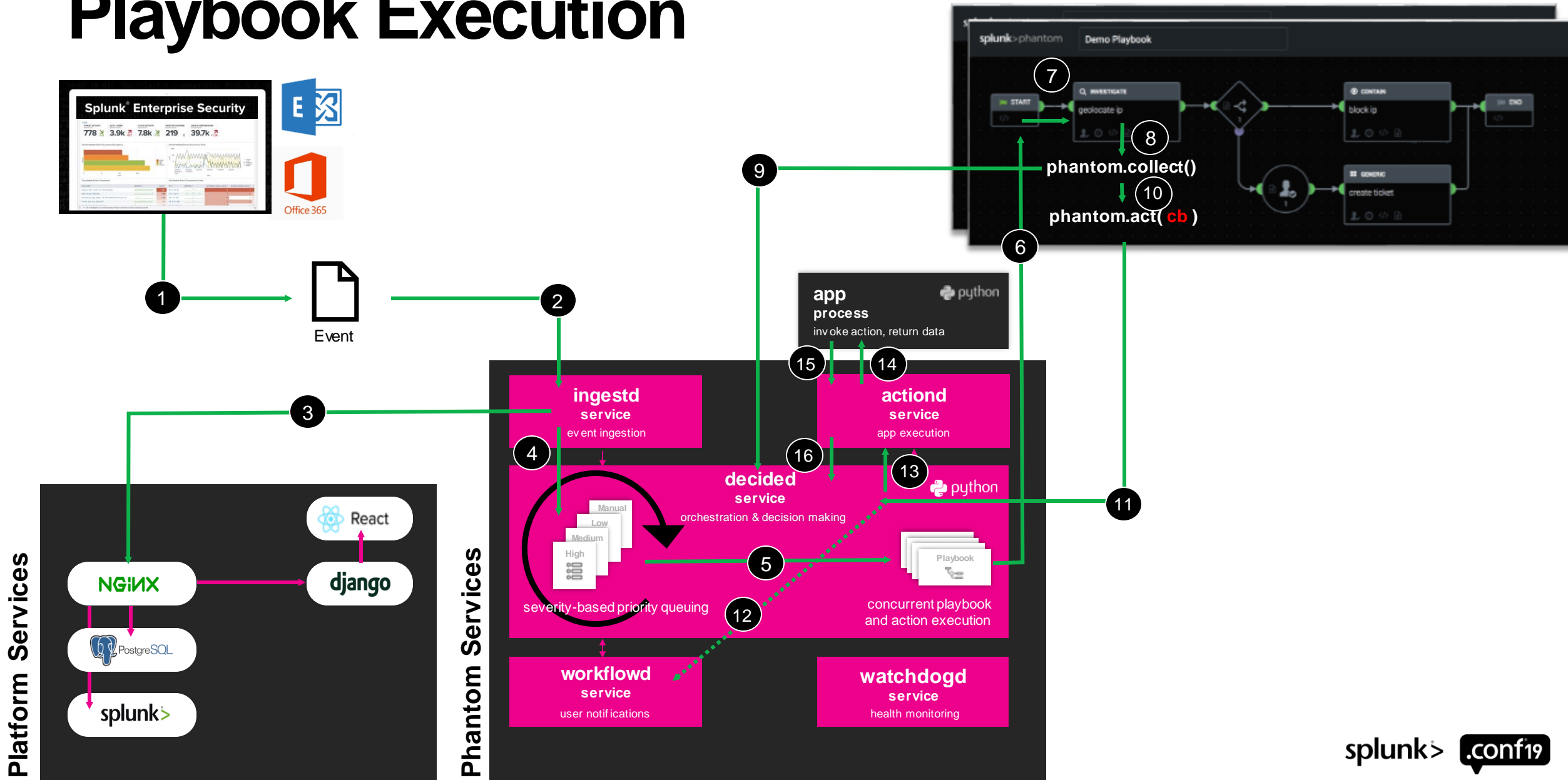
Playbook Execution



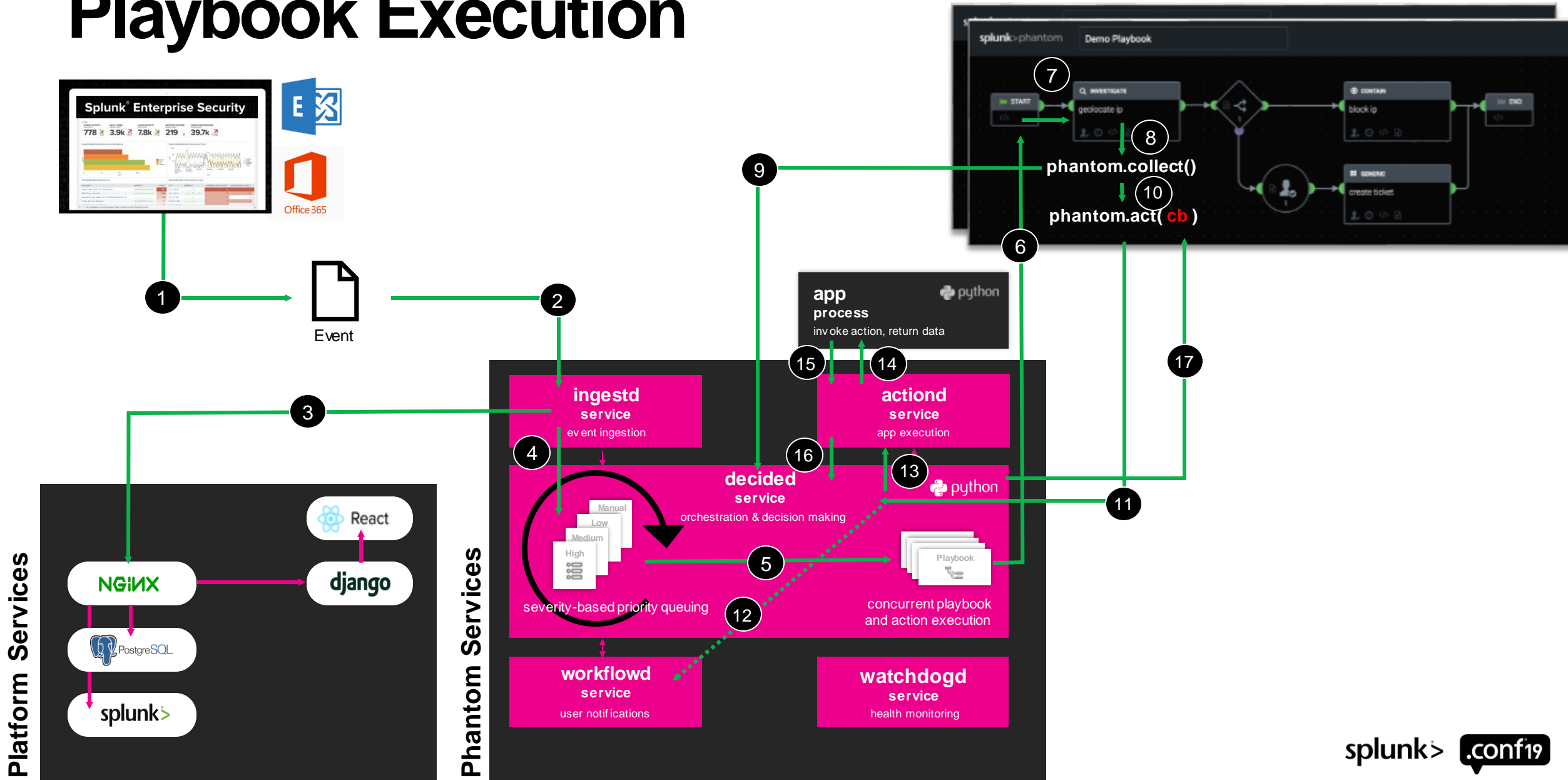
Playbook Execution



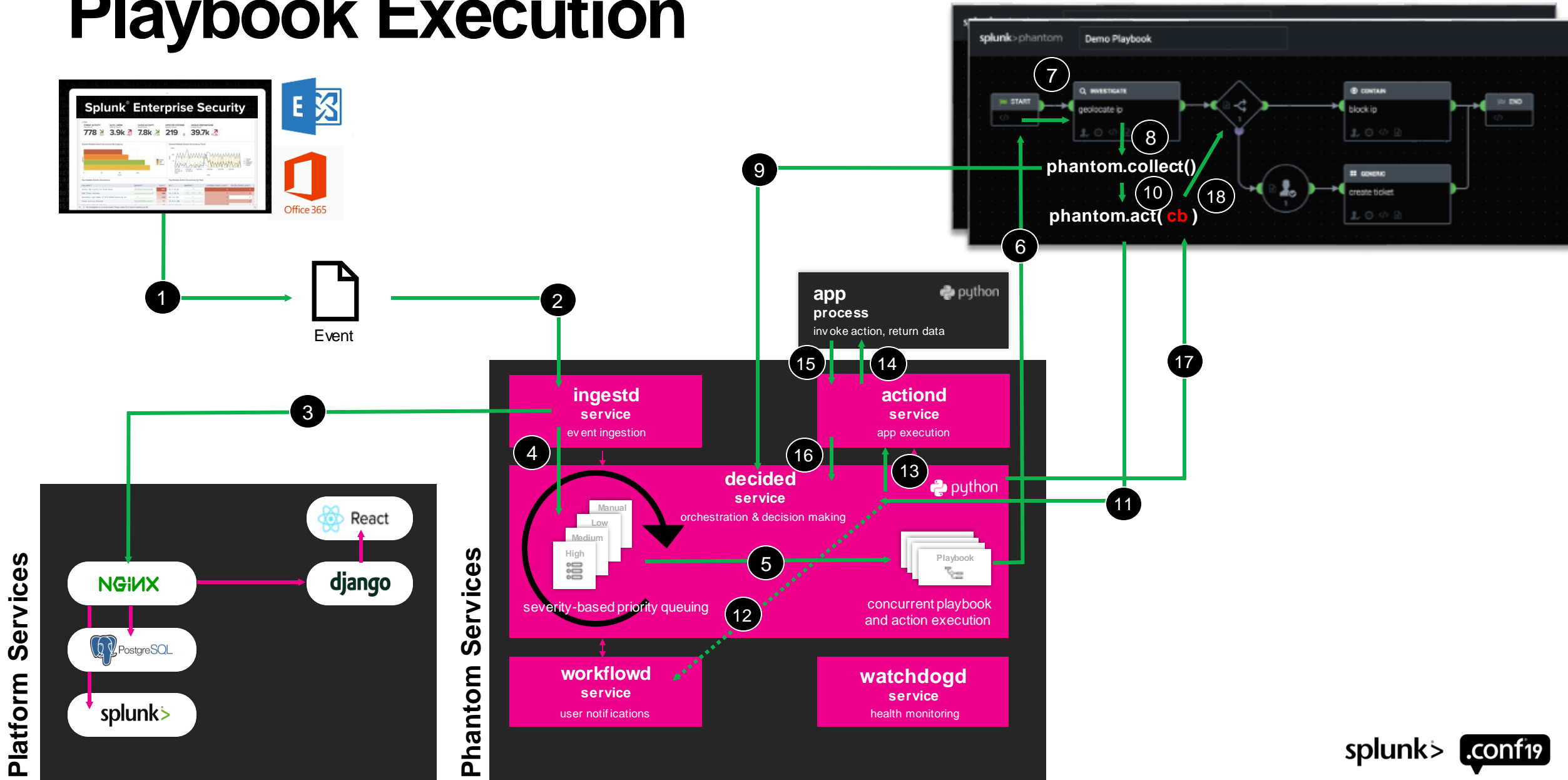
Playbook Execution



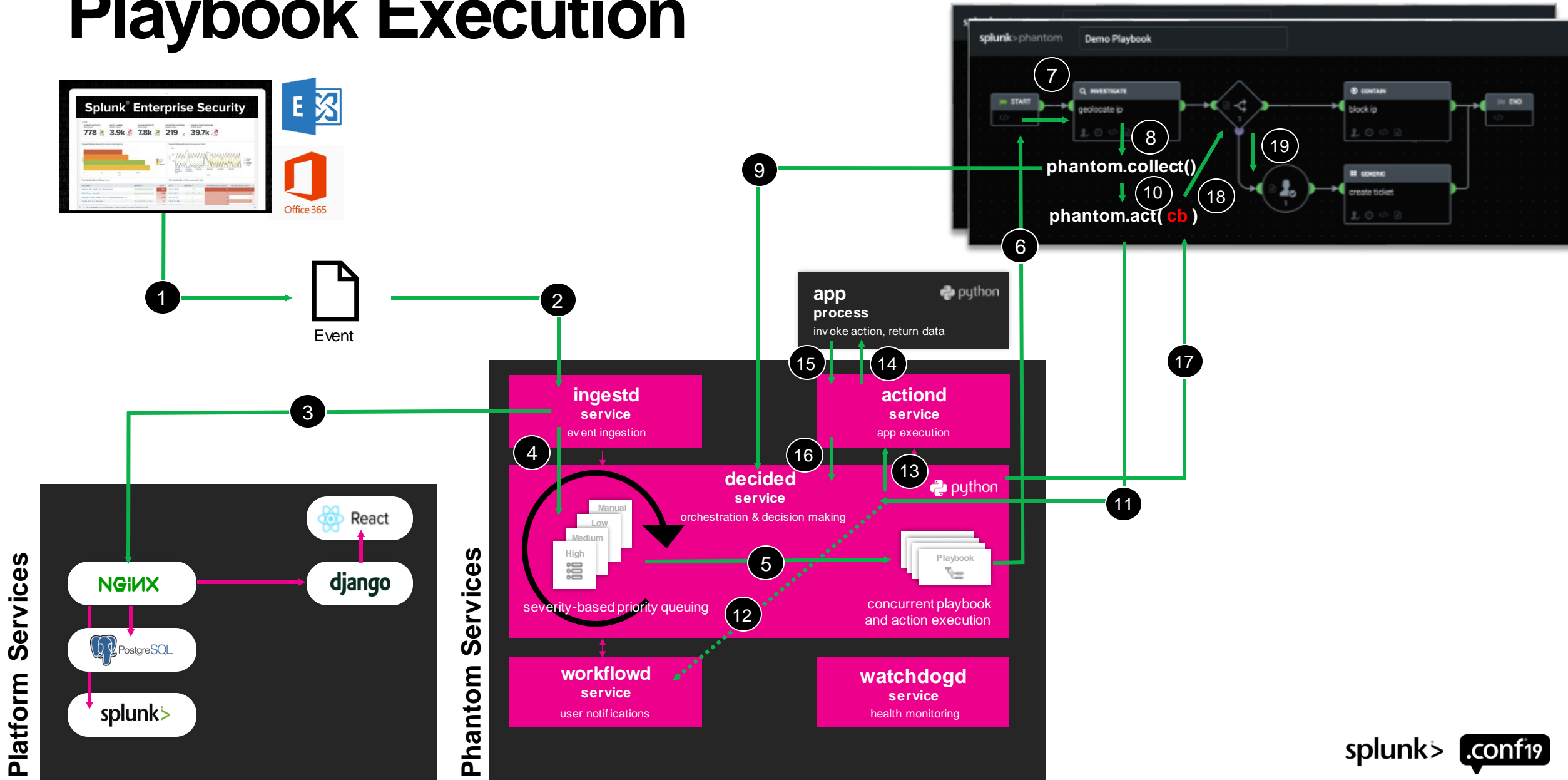
Playbook Execution



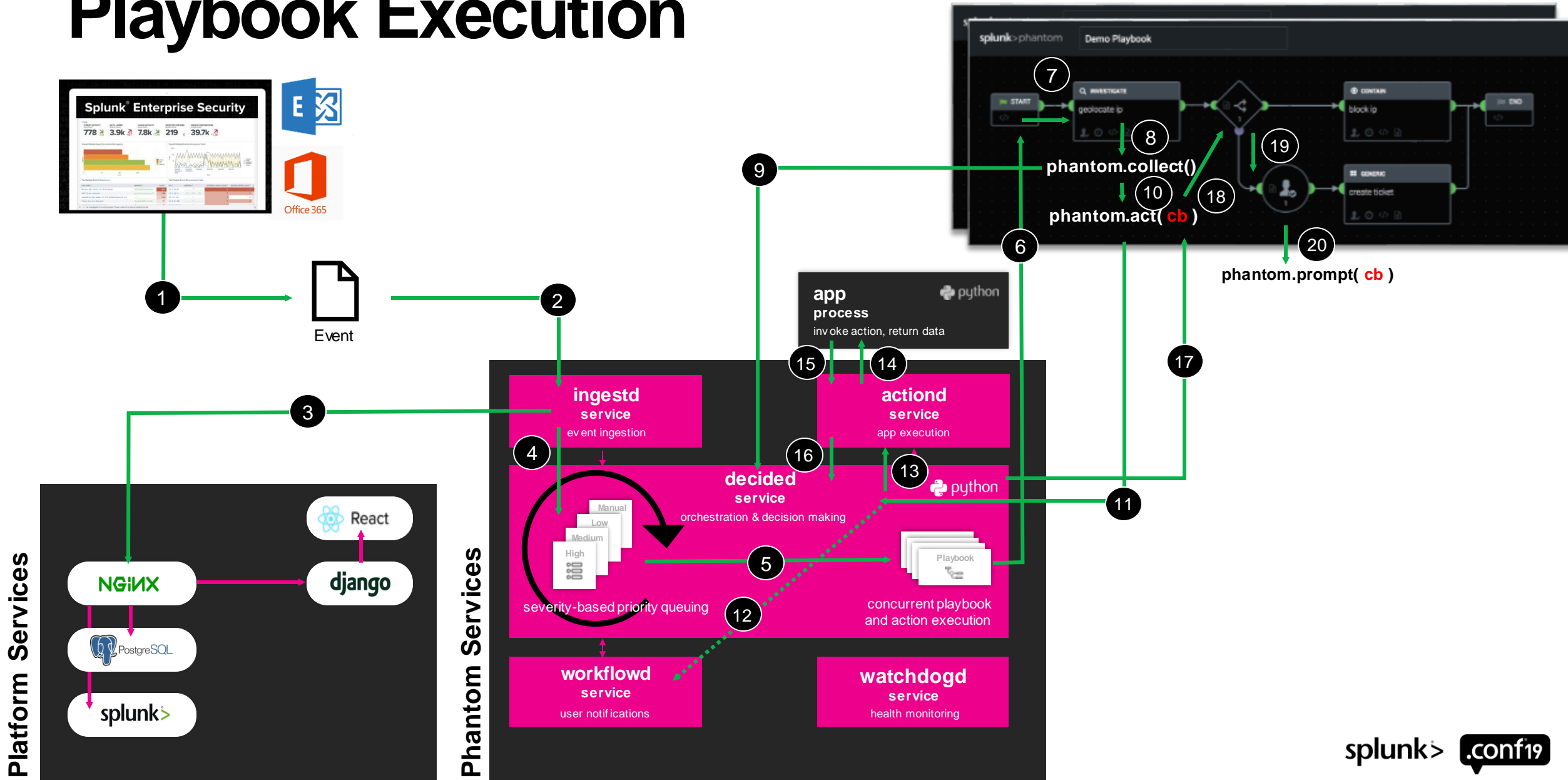
Playbook Execution



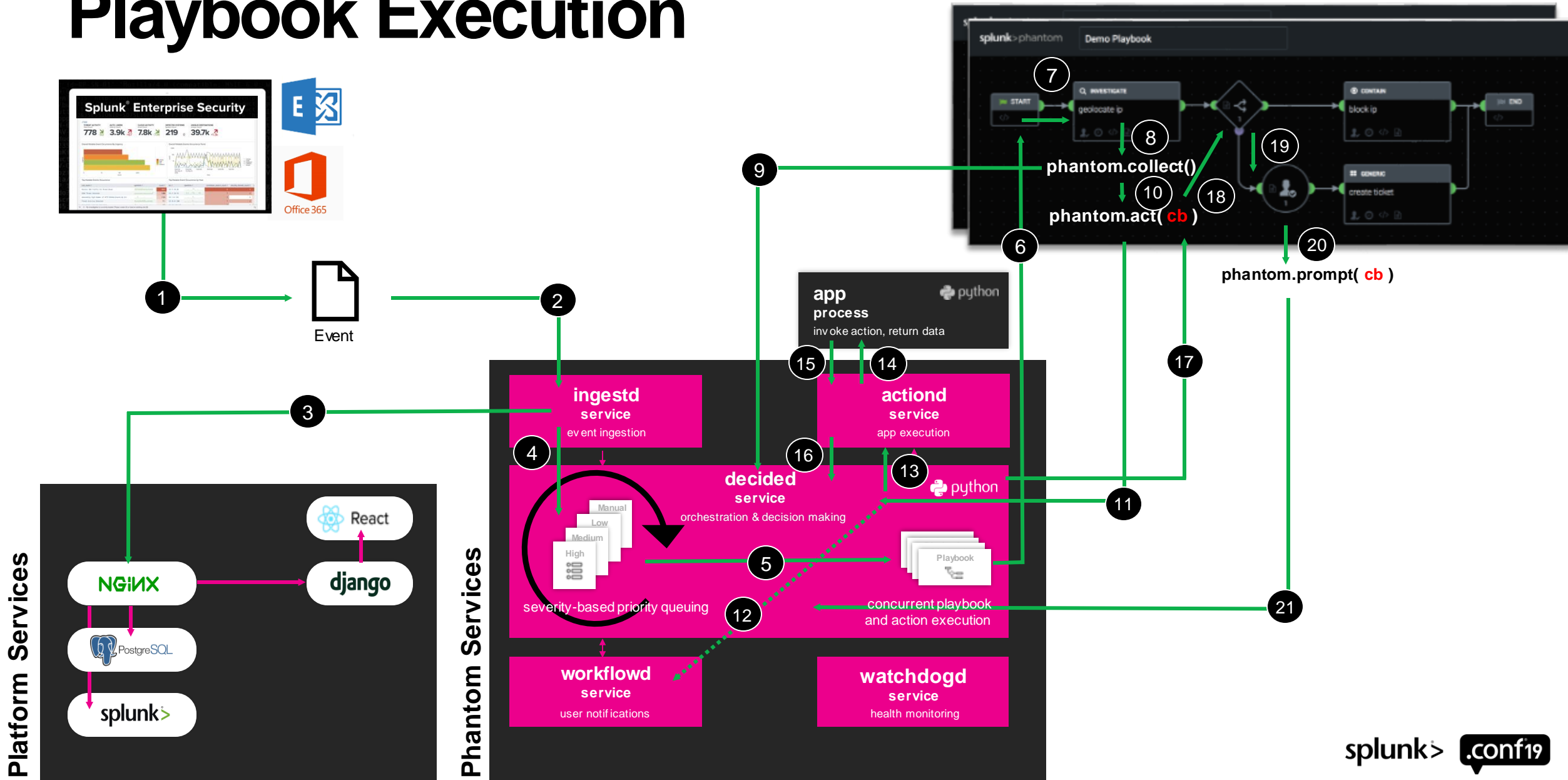
Playbook Execution



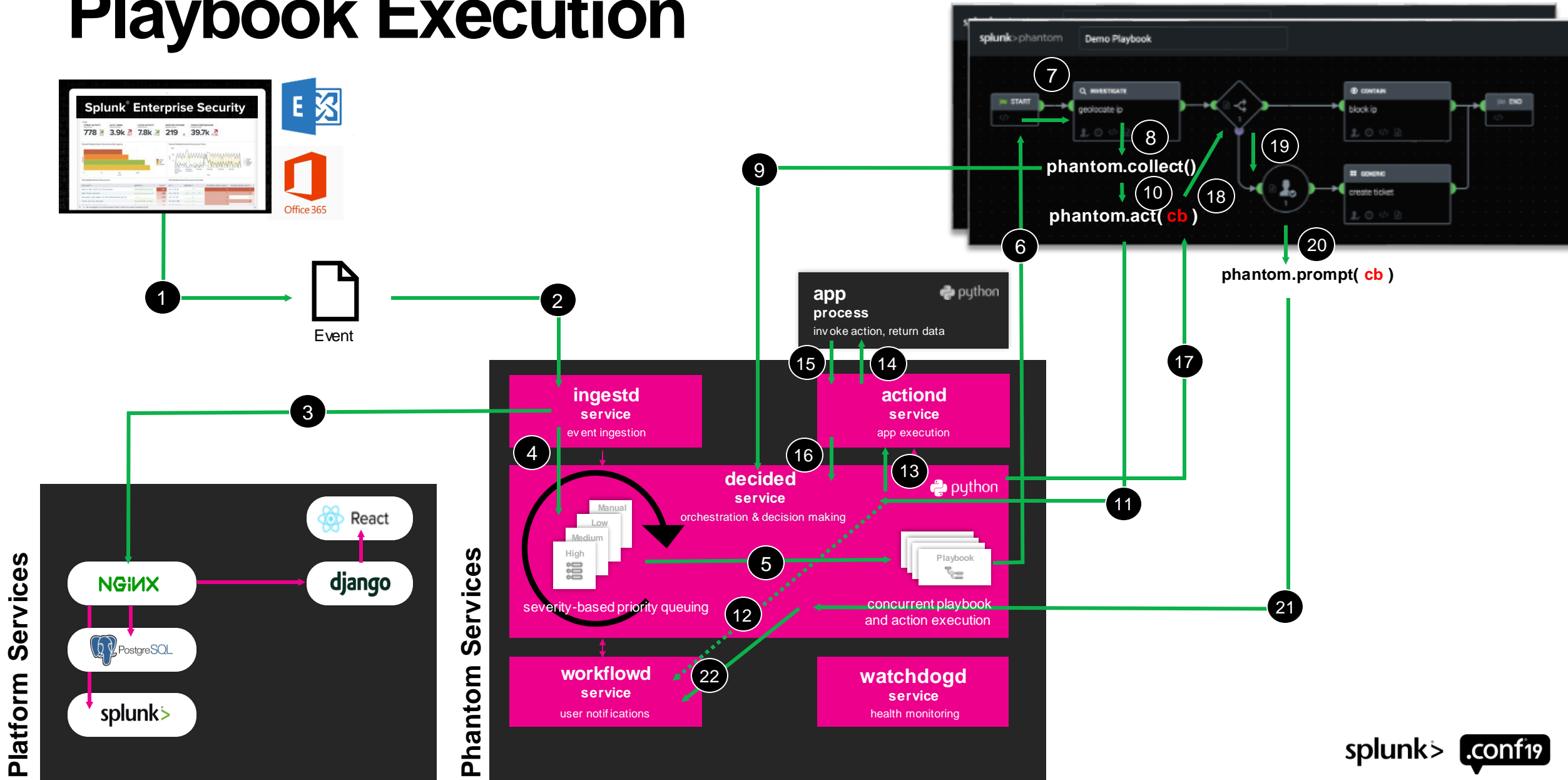
Playbook Execution



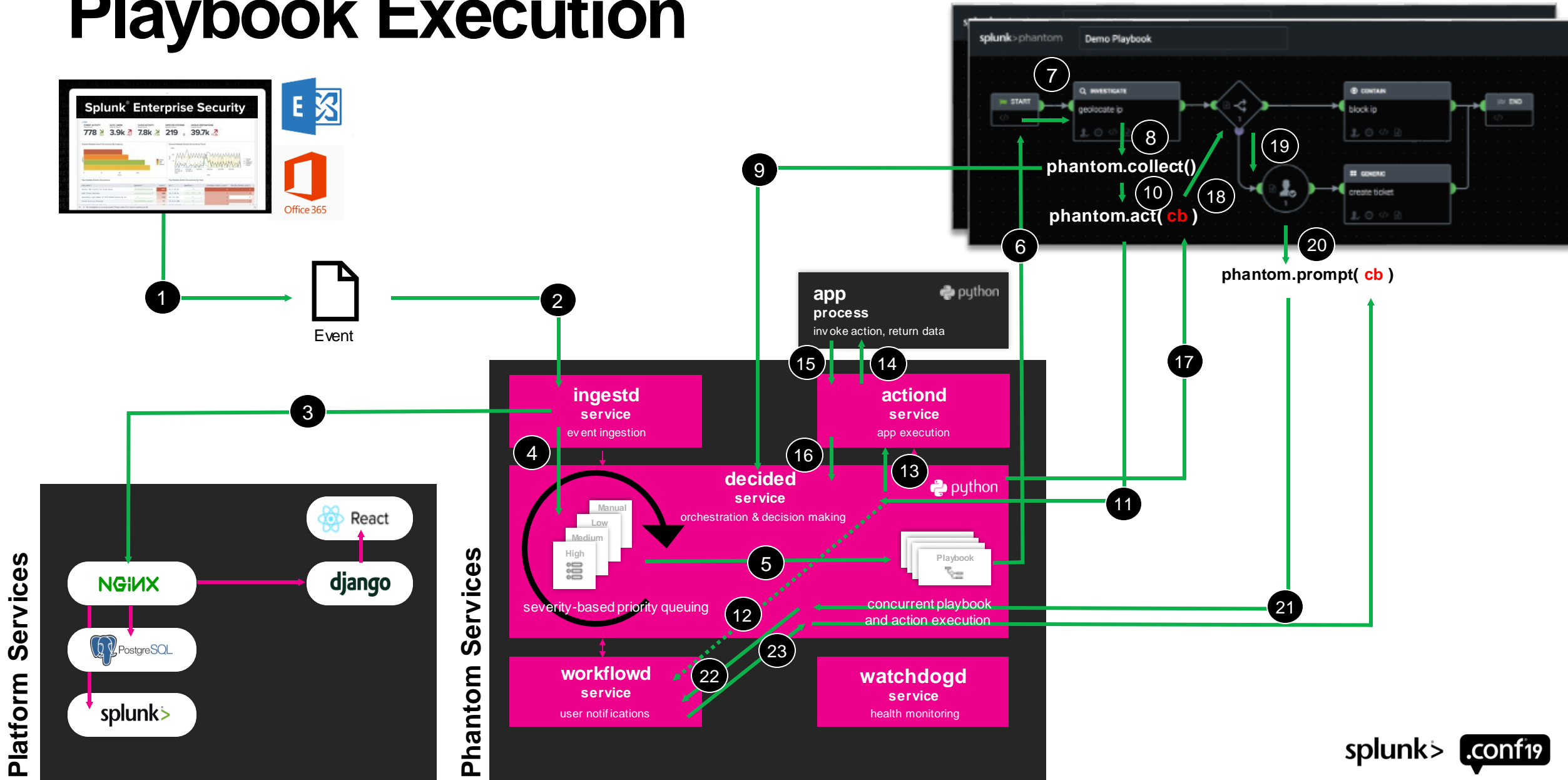
Playbook Execution



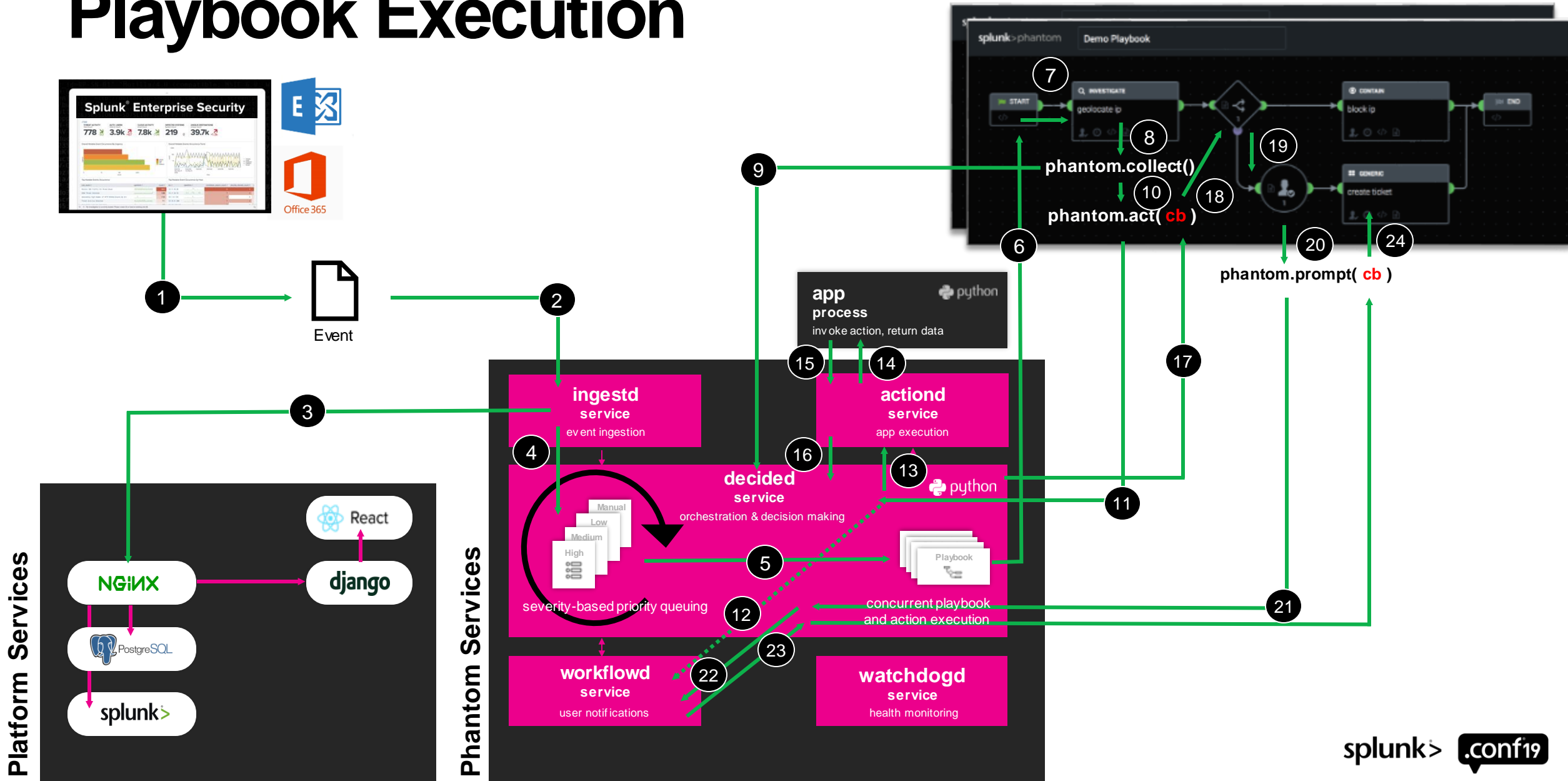
Playbook Execution



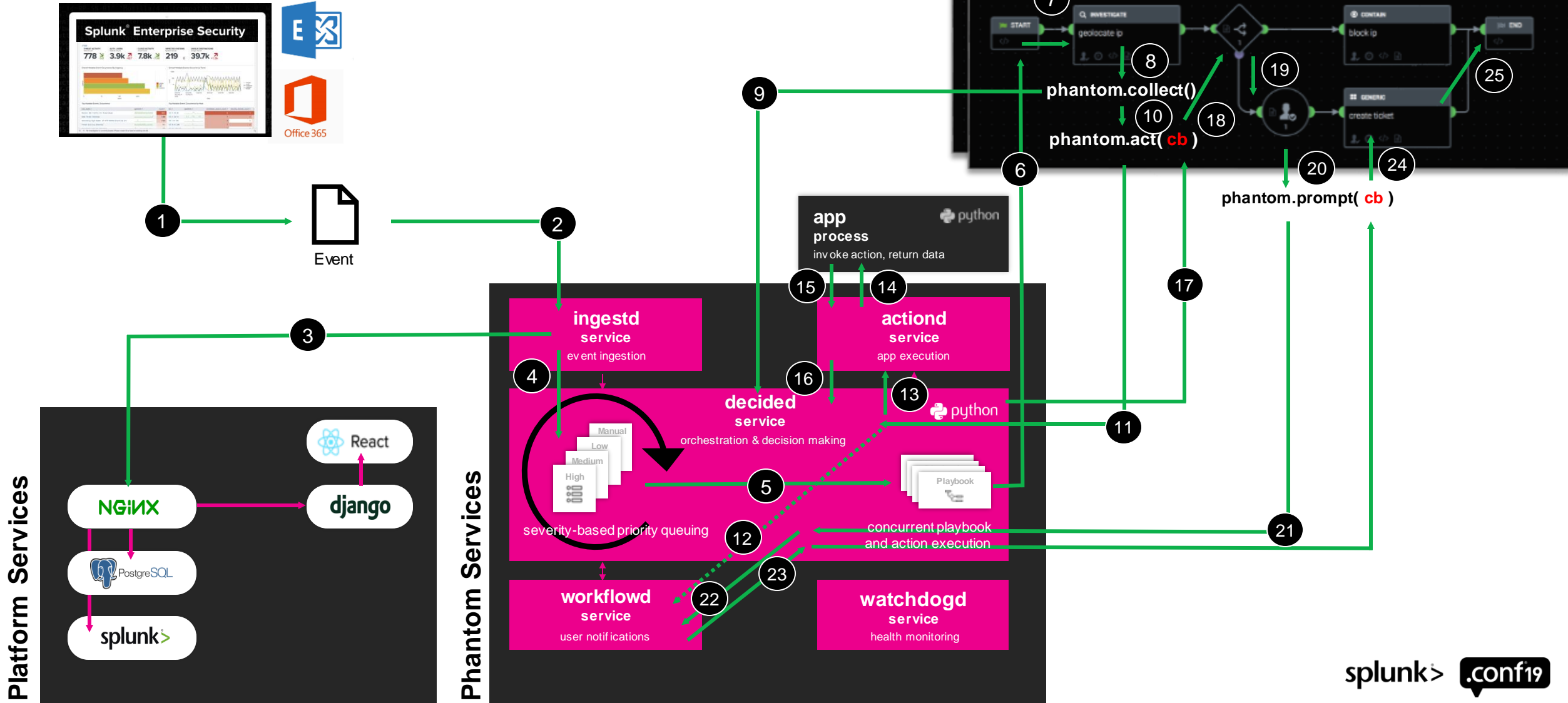
Playbook Execution



Playbook Execution



Playbook Execution

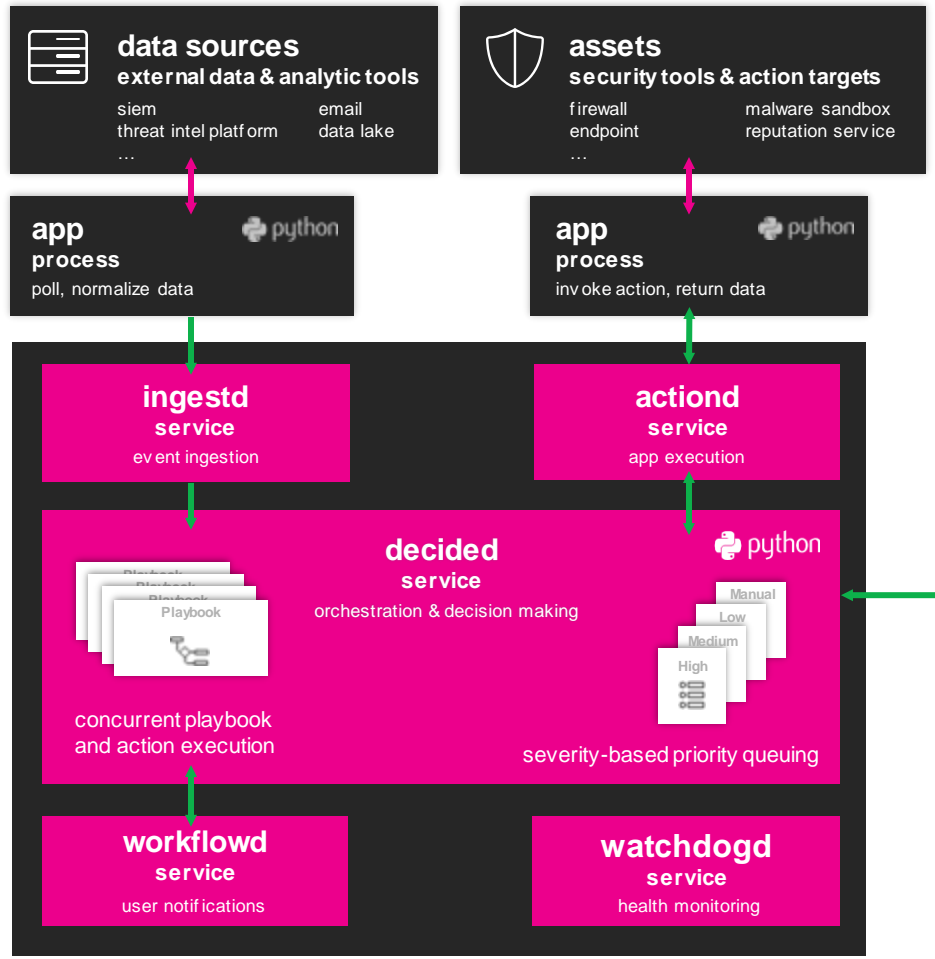




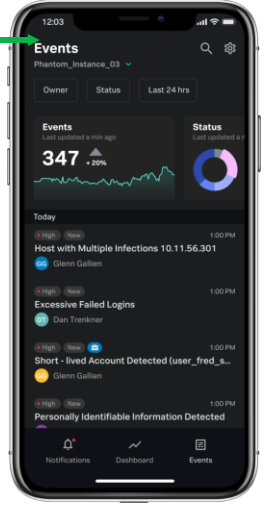
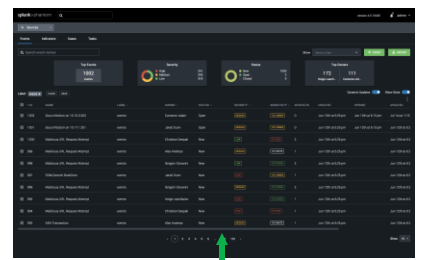
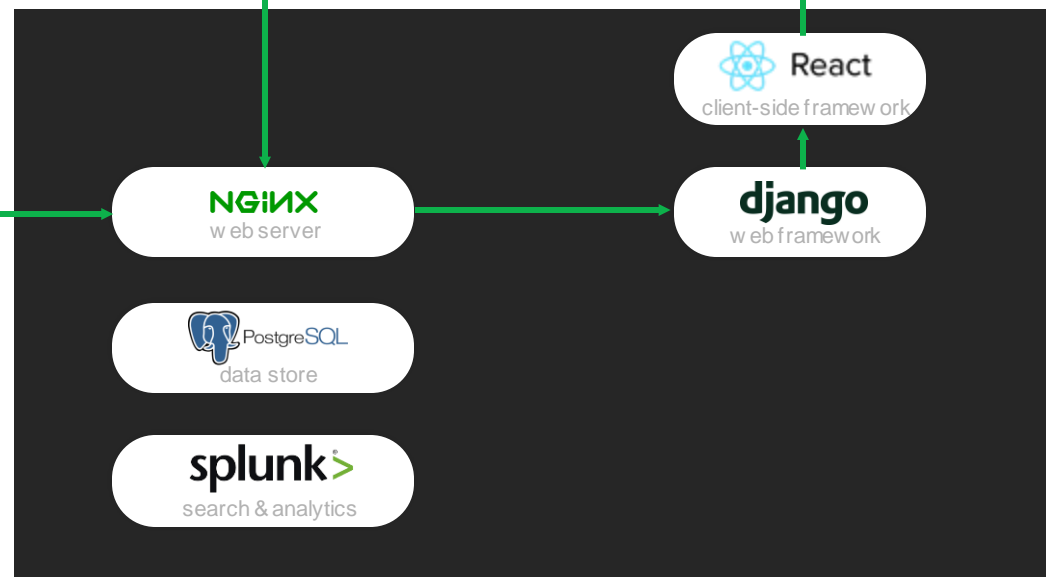
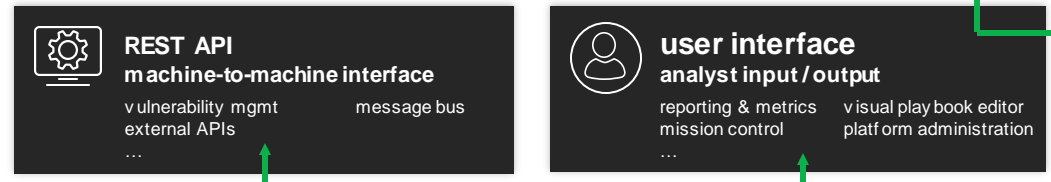
Clustered Architecture

Phantom Platform Architecture

External Platforms & Services



Human-Machine Interfaces

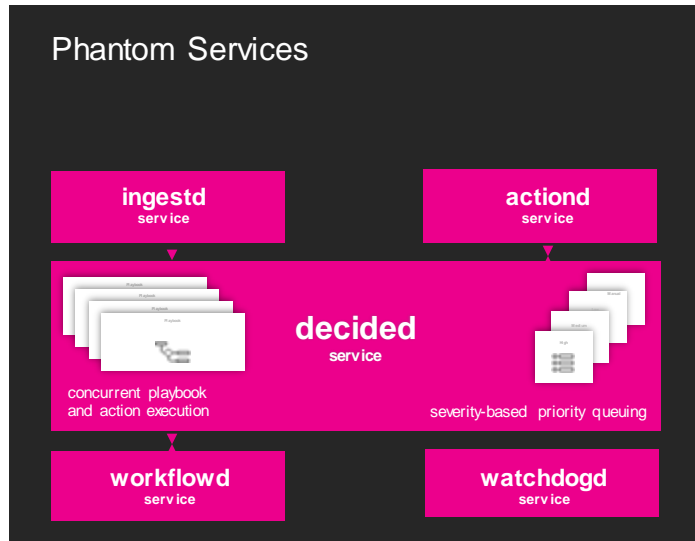


LEGEND

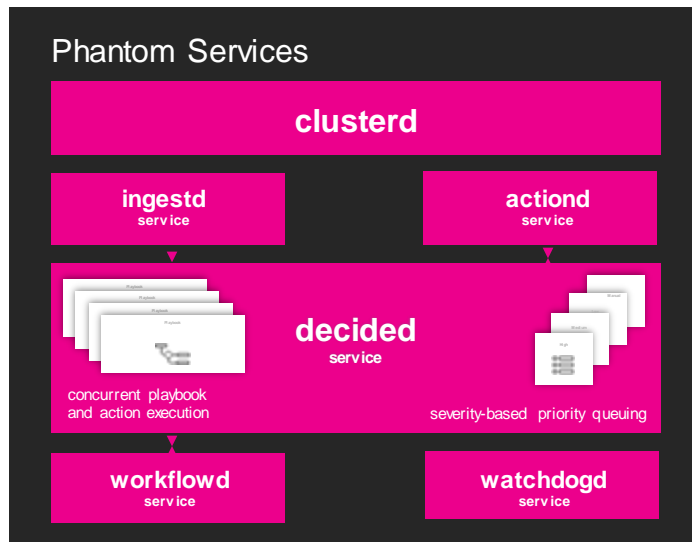
- ↕ = External Communication
- ↕ = IPC

Phantom Services

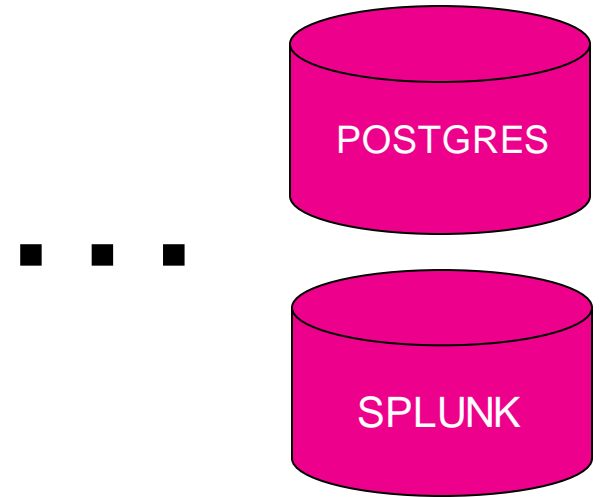
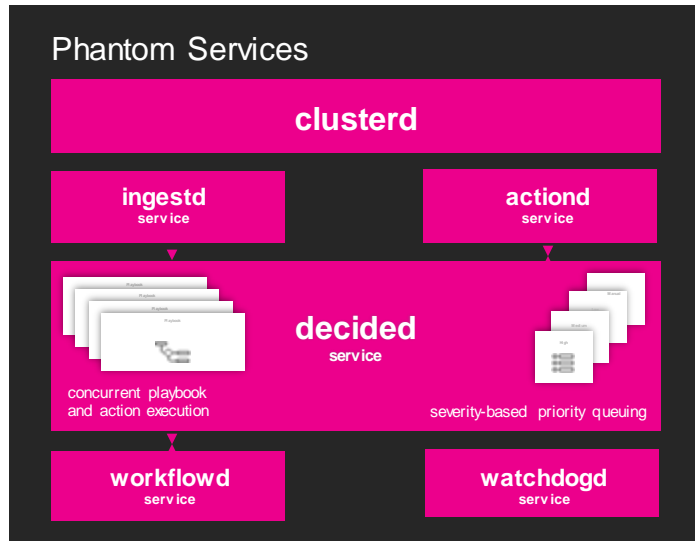
Phantom Platform Architecture



Phantom Platform Architecture

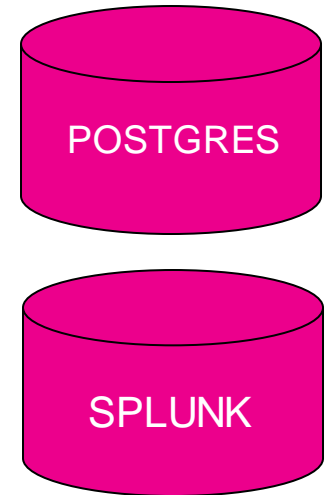
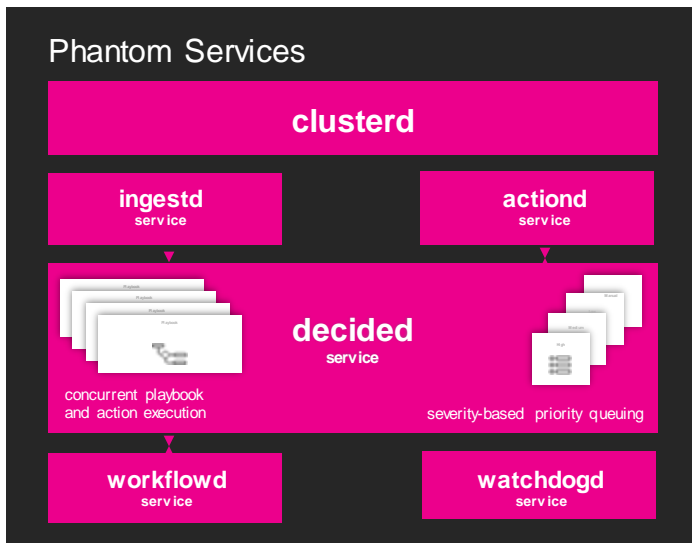


Phantom Platform Architecture



Phantom Platform Architecture

RabbitMQ



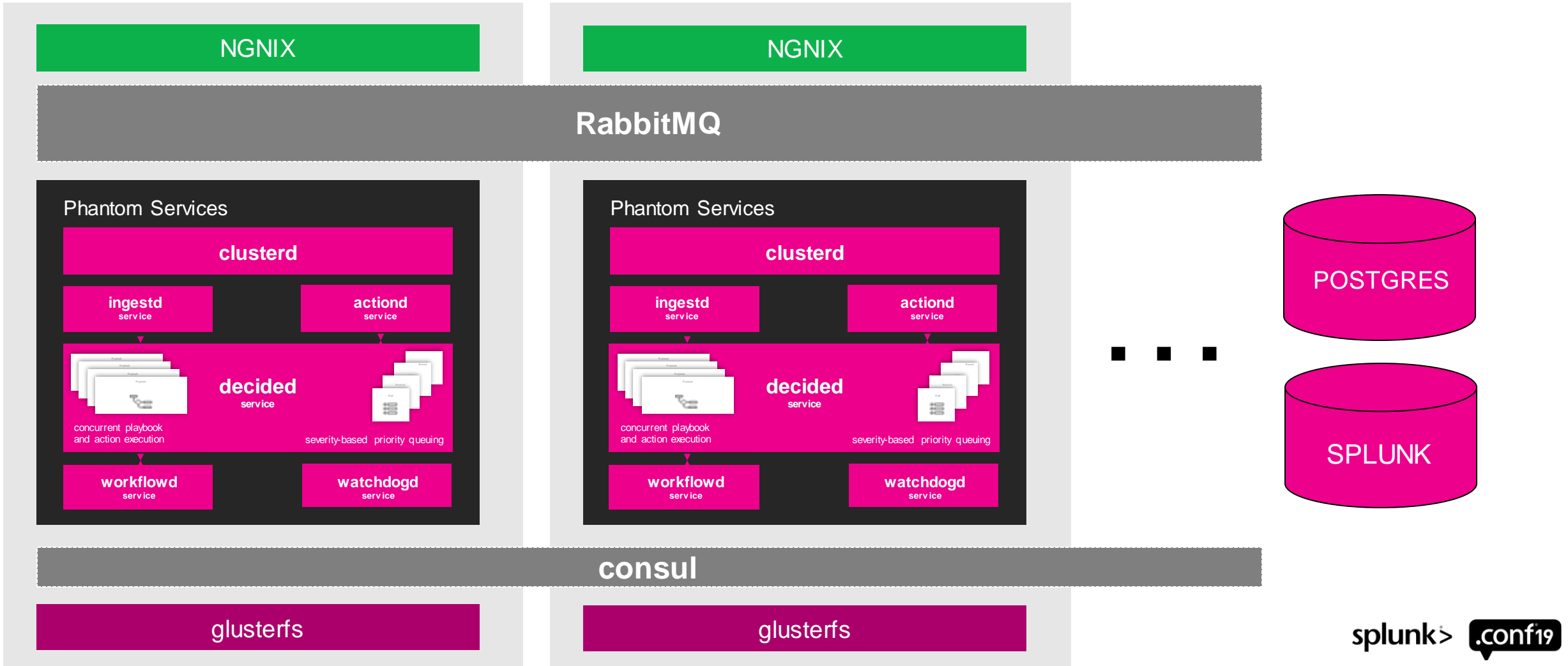
Phantom Platform Architecture



Phantom Platform Architecture



Phantom Platform Architecture



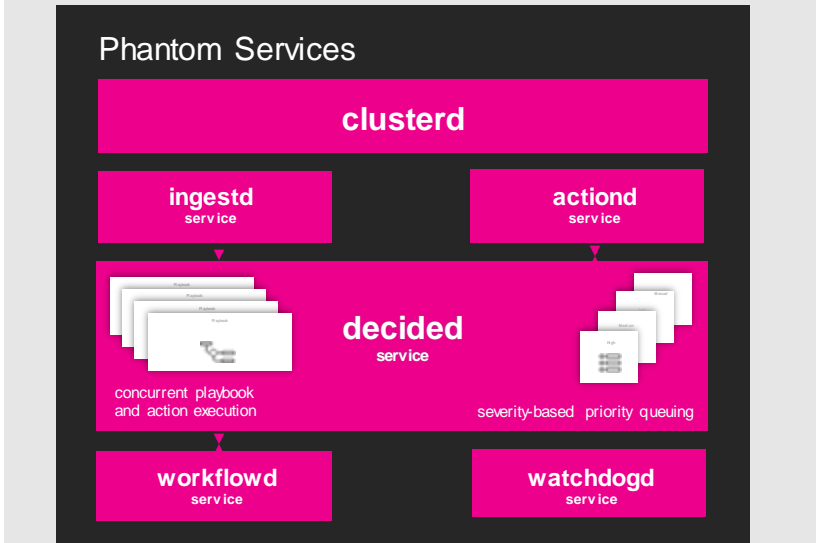
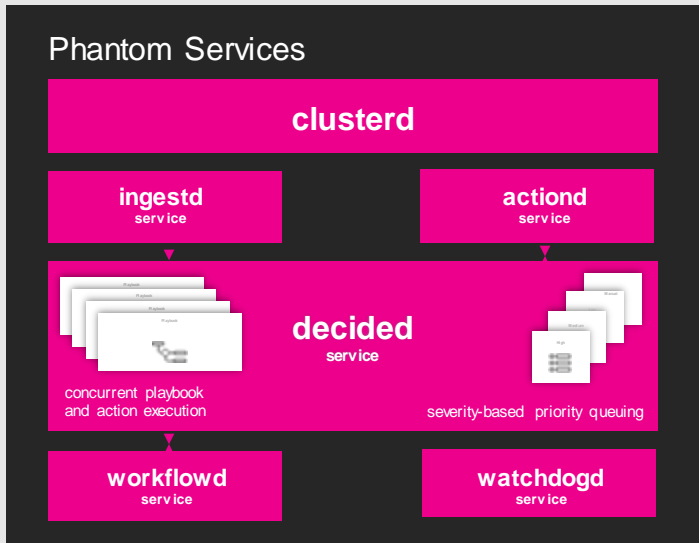
Phantom Platform Architecture

Load Balancer (HA PROXY)

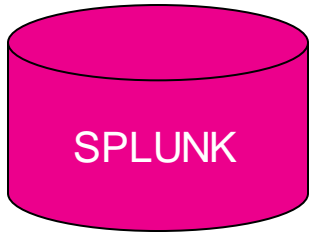
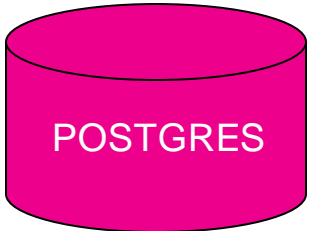
NGNIX

NGNIX

RabbitMQ



...



consul

glusterfs

glusterfs

Summary

Closing remarks

Please ask questions

Reach out to us on the Slack (***phantom-community***) with any questions

Reach us via: <https://support.splunk.com>

Lot of exciting sessions to attend. Here are a few other sessions I recommend:

- **SEC1705 - Diving into Splunk Phantom's Overlooked Features**
 - Tuesday, October 22, 03:00 PM - 03:45 PM
- **SEC1671 - Use Splunk SIEMulator to Generate Data for Automated Detection, Investigation, and Response**
 - Thursday, October 24, 11:45 AM - 12:30 PM



splunk>

Thank

You!

Go to the .conf19 mobile app to

RATE THIS SESSION

