



splunk>phantom

SEC2233

Deploying Splunk Enterprise Security and Phantom at Scale

Mayur Pipaliya, Ankit Bhagat
Forward Deployed Software Engineers | Splunk

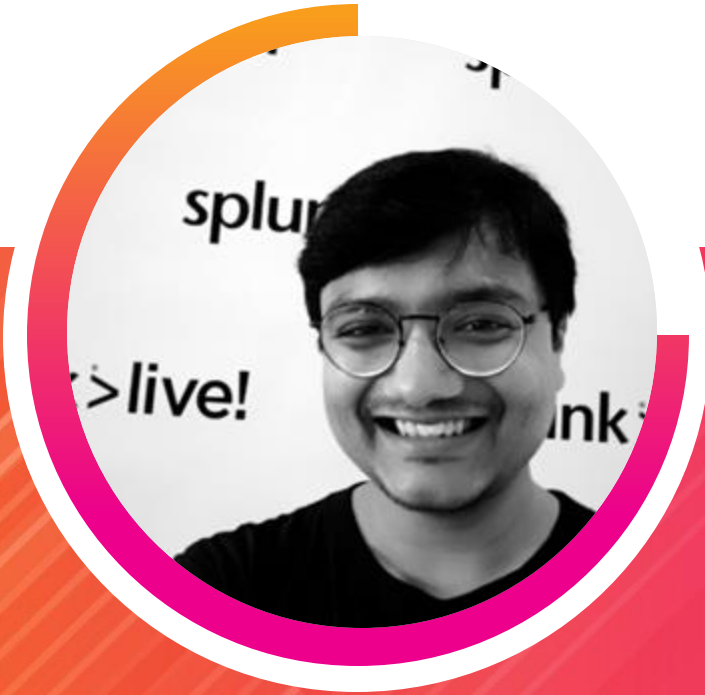
Forward-Looking Statements



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.



Mayur Pipaliya

Sr. Forward Deployed Software Engineer | Splunk



Ankit Bhagat

Forward Deployed Software Engineer | Splunk

Security Geek | /dev/urandom

r/homelab | building and breaking hardware

Photographer | help people see world
through my lens!

Hackathons | organize, ideate, evaluate!



@Zombie

~6000+ hours of gaming!

Street photographer | [@xynazog](#)

Live and breathe music

Hypebeast | Sneakers + denim nerd



[@xynazog](#)

Agenda

Let's see all of what are we going to cover in the next 40 minutes


1

Backstory 

2

Architecture
Discussion


3

Technical
Aspects and
Performance
Benchmarks


4

Demo 

5

Q&A! 

“Trust, but verify.”

Russian proverb



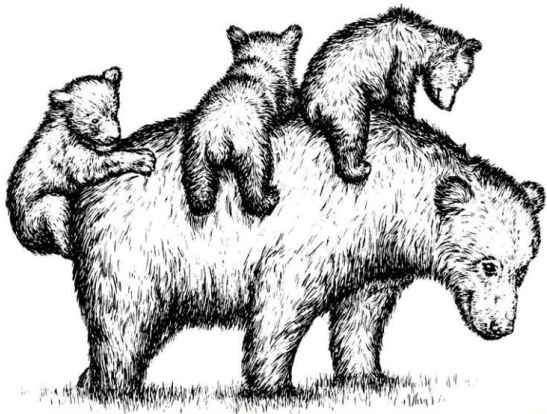
Backstory



Ninjas in the wild



Why ES + Phantom at Scale?



Solving Imaginary
Scaling Issues

At Scale

○ RLY?

@ThePracticalDev

1. Greater resiliency and availability
2. Automate complex ITOps & SecOps tasks
3. Speed, Productivity, performance
4. For fun and giggles

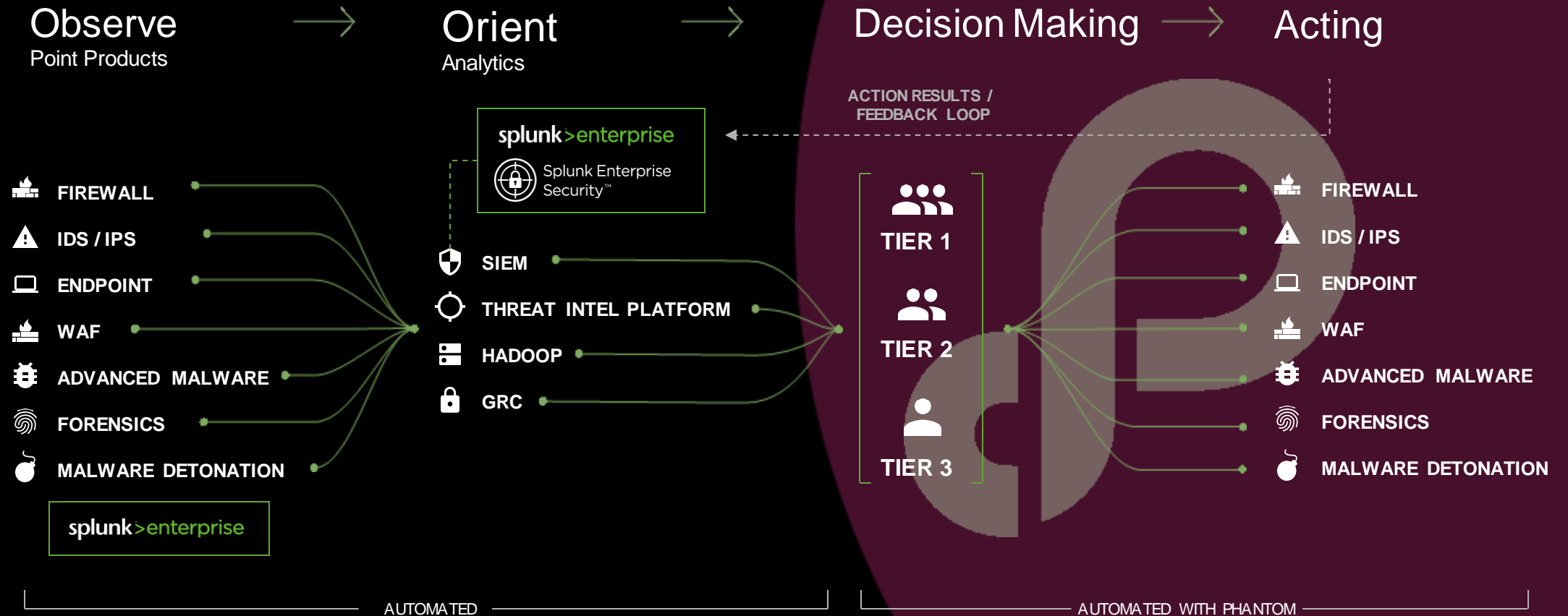


Architecture

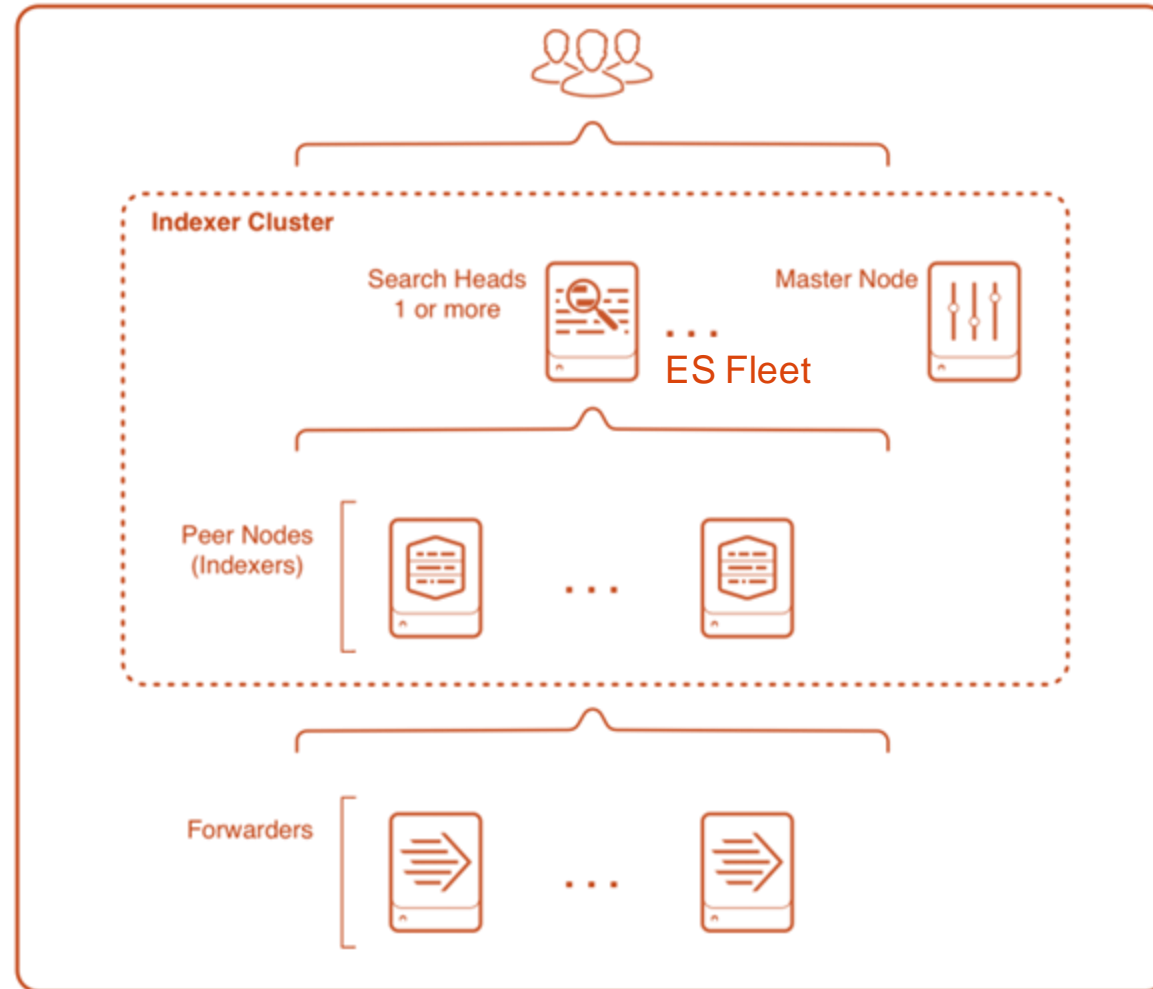
Discussing our favorite part of every project:
the backend

SOAR for Security Operations

Faster execution through the loop yields better security

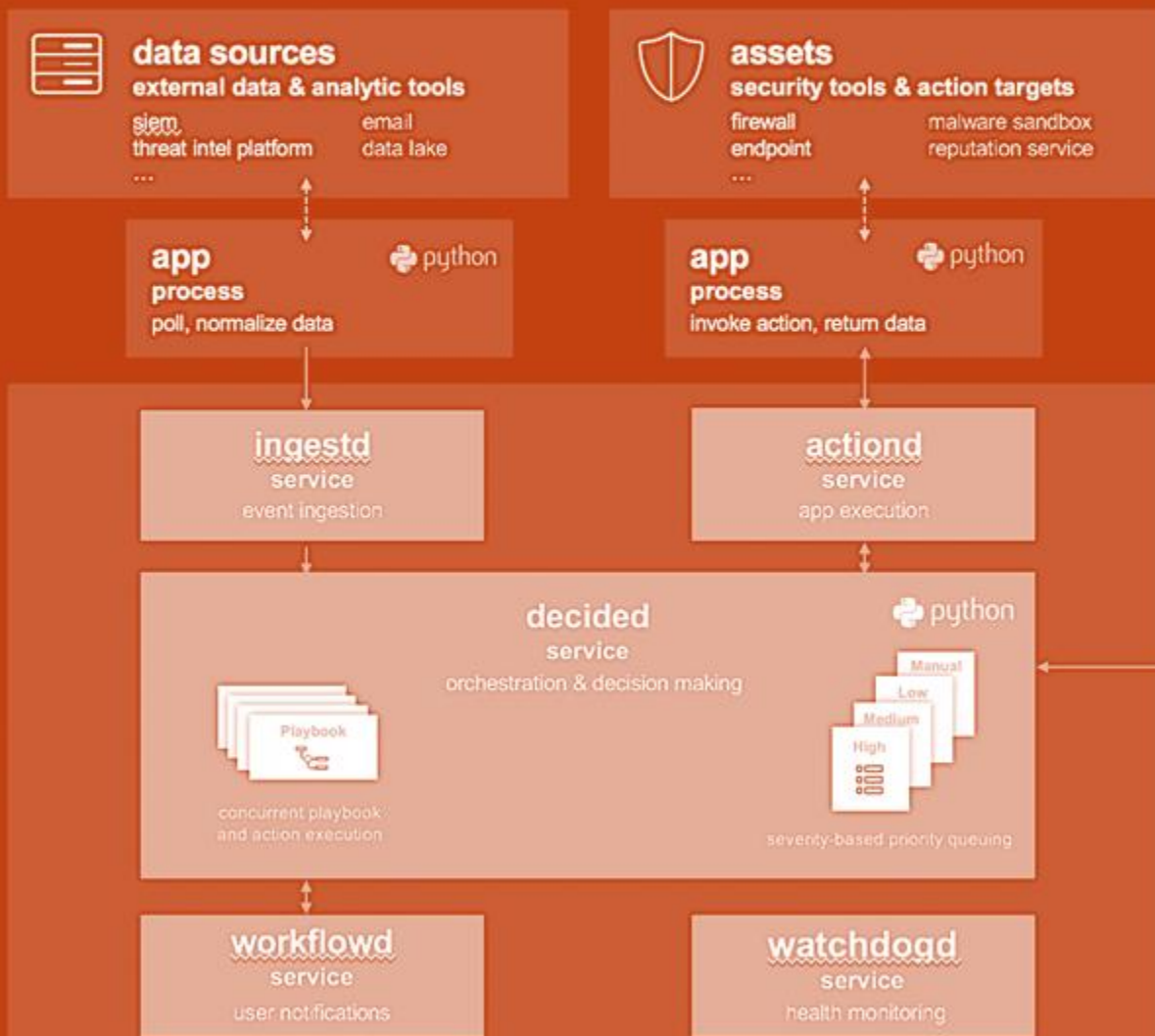


ES Search Head Clustering

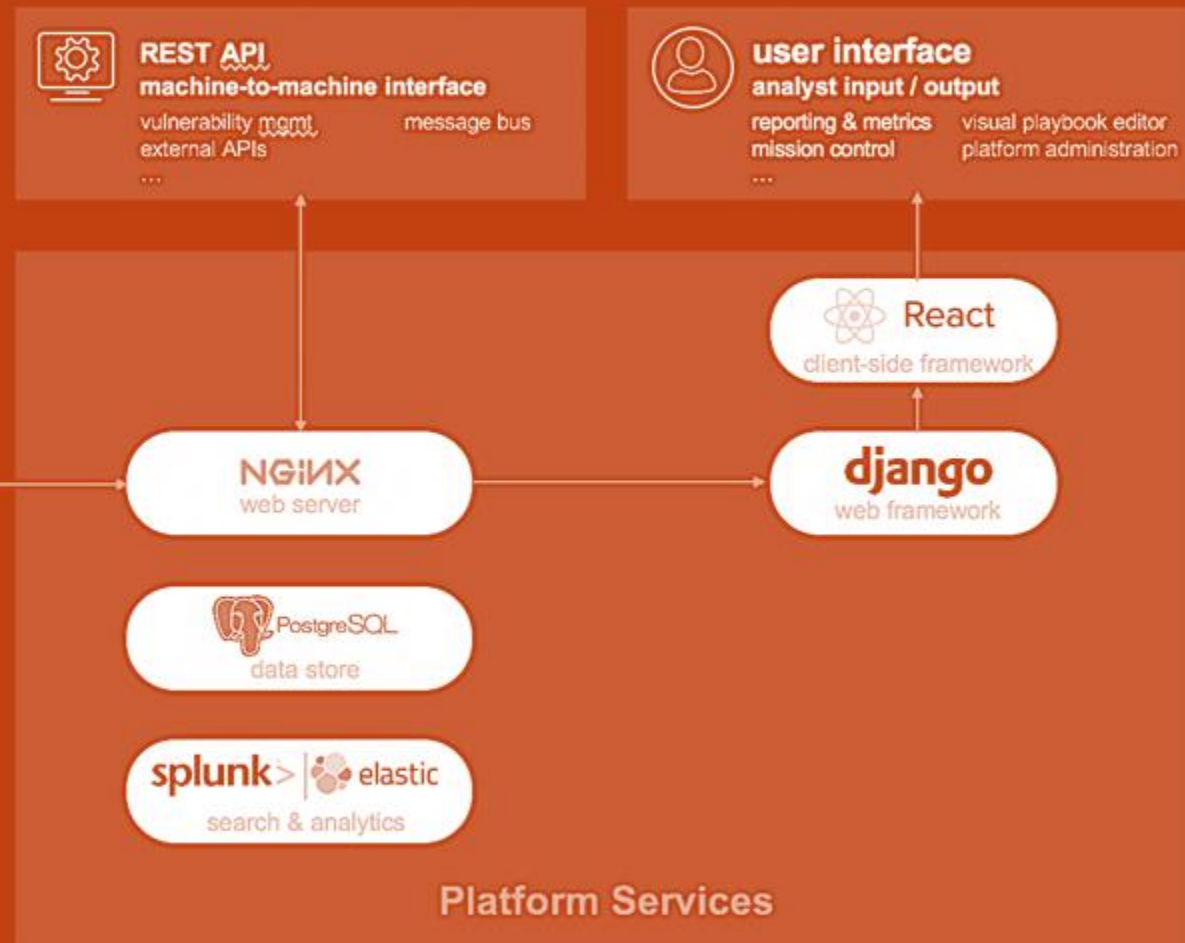


Phantom Platform Architecture

External Platforms & Services



Human-Machine Interfaces



Legend

↕ External Communication

↕ IPC

Phantom Microservices



Technical Aspects and Performance Benchmarks



“Believe in performance, not quotes.”

“Executed **45** playbooks and **950** actions against **2K** notable events to save **22.5** hours of analyst hours and money.”

Horizontal Scaling

Demo

Resources



Repositories,
cheatsheets, et al.

1. [Github Repository](#)
2. [Cheat Sheets](#)
3. [Troubleshooting Guide](#)
4. [Freebies - List of OSINT Integrations with Phantom](#)
5. [Sample Playbooks](#)



Q&A

Mayur Pipaliya | Speaker
Ankit Bhagat | Co-speaker



Thank You!

Go to the .conf19 mobile app to

RATE THIS SESSION

