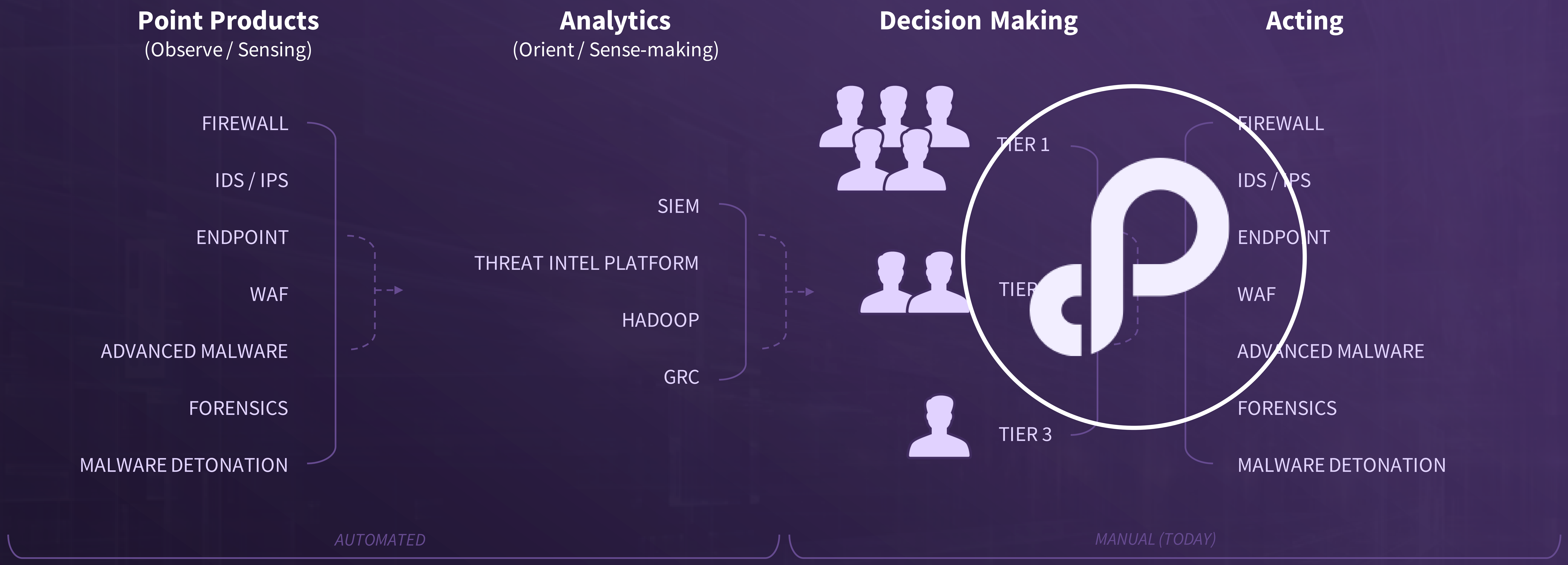
Phantom™

Purpose and Use of Message Fabric

Sourabh Satish
Co-Founder and CTO

sourabh@phantom.us

Automating Security Operations



Point Products
(Observe / Sensing)

FIREWALL
IDS / IPS
ENDPOINT
WAF
ADVANCED MALWARE
FORENSICS
MALWARE DETONATION

Analytics
(Orient / Sense-making)

SIEM
THREAT INTEL PLATFORM
HADOOP
GRC

Decision Making

TIER 1
TIER
TIER 3

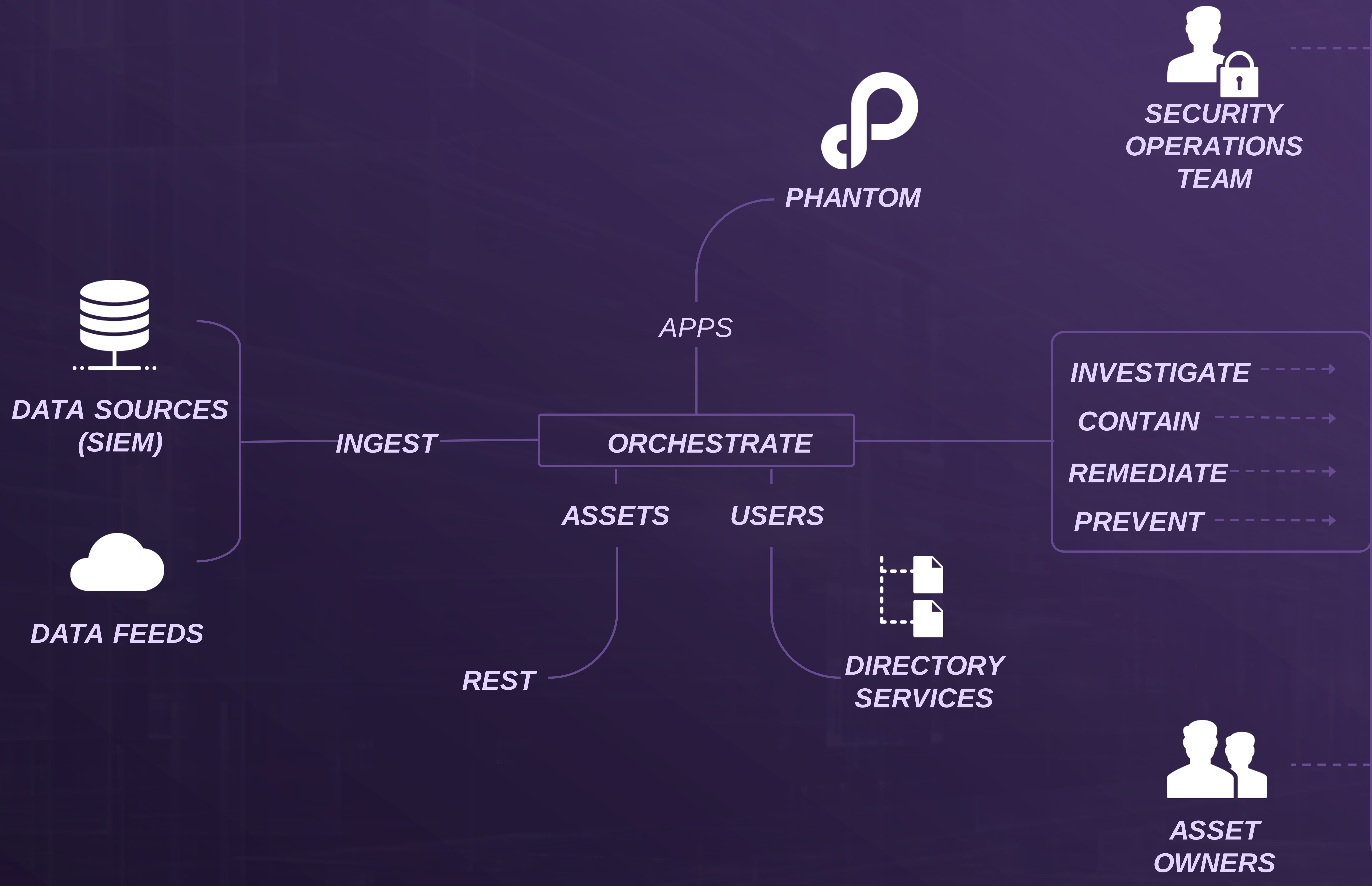
Acting

FIREWALL
IDS / IPS
ENDPOINT
WAF
ADVANCED MALWARE
FORENSICS
MALWARE DETONATION

AUTOMATED

MANUAL (TODAY)

Phantom Key Concepts



PHANTOM

APPS

DATA SOURCES (SIEM)

DATA FEEDS

INGEST

ORCHESTRATE

ASSETS

USERS

REST

DIRECTORY SERVICES

SECURITY OPERATIONS TEAM

INVESTIGATE

CONTAIN

REMEDIATE

PREVENT

ASSET OWNERS

ENDPOINT TECH
CrowdStrike, Tanium, CarbonBlack, etc.

FIREWALLS
Cisco, PAN, etc.

SIEM
Splunk, Qradar, etc.

VIRTUALIZATION
VMWare

SANDBOX
Anubis, LastLine, ThreatGrid, Cuckoo, etc.

IT TICKETING
JIRA, Remedy, ServiceNow, etc.

REPUTATION SERVICES
VirusTotal, ReversingLabs, OpenDNS, etc.

IDENTY MANAGEMENT
AD

FORENSICS
Volatility

PUBLIC INFRASTRUCTURE
Whois

Data Movement in Security Automation

Reasons and ways in which data moves in Security Automation and Orchestration platforms

1. **Ingestion**
   - Data is either pulled from data sources
   - Data is posted to the platform

2. **Response Actions**
   - Investigate, Contain, Remediate, Other
     - Authorizations and Approvals

3. **Action Results and Resolution**

Role of Message Bus and Services

1. **Scalability**
2. **Resiliency**

- Large scale deployments and performance/reliability demands require **componentized** and **hierarchical** deployments.

- In most enterprises there are hundreds of control points, security products and complex overlay networks that must be connected to orchestrate a comprehensive response.

Message Bus Architectures present a very unique opportunity for orchestration platforms to overcome these challenges

e.g. – mutual authentication, scalability, et.

Message Bus for Security Automation

Attributes of a Message Bus Solution for Security Automation:

- **SECURITY / TRUST**
  - Authenticated Publisher and Subscribers
    - Who can publish and who can subscribe what kinds of messages?
  - Integrity and Verification of messages
    - signed messages
- **SENSITIVITY / CONFIDENTIALITY**
  - Full support for Traffic Light Protocol (TLP)
    - Not all subscribers should be able to see all levels of messages

Message Bus – other ‘desired’ attributes

- **Severity for prioritization of Messages**
  - Security events are often very time sensitive and response needs can vary in urgency (depending on phase of an attack aka. ‘Kill chain’
- **Message TTL (life span)**
  - Certain Messages (especially response actions) need to have ‘life span’ specified since they are only valid for a limited time span

Challenges

- Security vendors/products are sensitive (and hence passive-aggressive) to features that lead them down the path of commoditization!

- Enterprises will not upgrade to latest and best version overnight and hence a heterogeneous environment will exist and will need protection meanwhile

- Message Format (IOCs, COA, etc.) standardization will take a while to materialize from standards to implementations.

Connect with Phantom

RSAC Innovation Sandbox 2016 FINALIST

blog.phantom.us

@TryPhantom

announce+subscribe@phantom.us

Thank you!

Sourabh Satish

sourabh@phantom.us