

ENGINEERING PRINCIPLES

for Developing Advanced
Cybersecurity Automations

.....
Matt Rodriguez and Tom Goetz
Phoenix Cybersecurity



Agenda



1
Introduction


2
Automation
Use Cases

3
Scoping
Automation

4
Designing
Automation

5
Implementing
Automation

Our Clients



“Phoenix Cybersecurity had extensive experience implementing our solution in the real world and it showed. Our initiative has been fantastically successful, due in major part to their skills.”

**Chief Privacy Officer
U.S. Department of Defense**

- U.S. Federal Government
 - Department of Homeland Security
 - Department of Defense
 - Department of Justice
 - Department of Veterans Affairs
 - U.S. Navy
 - U.S. Air Force
- Financial Services
- Healthcare

Implemented Use Cases

Event Triage

Phishing

Malware

Rogue
Device

Web
Access

Classified
Data Spill

Endpoint
Compliance

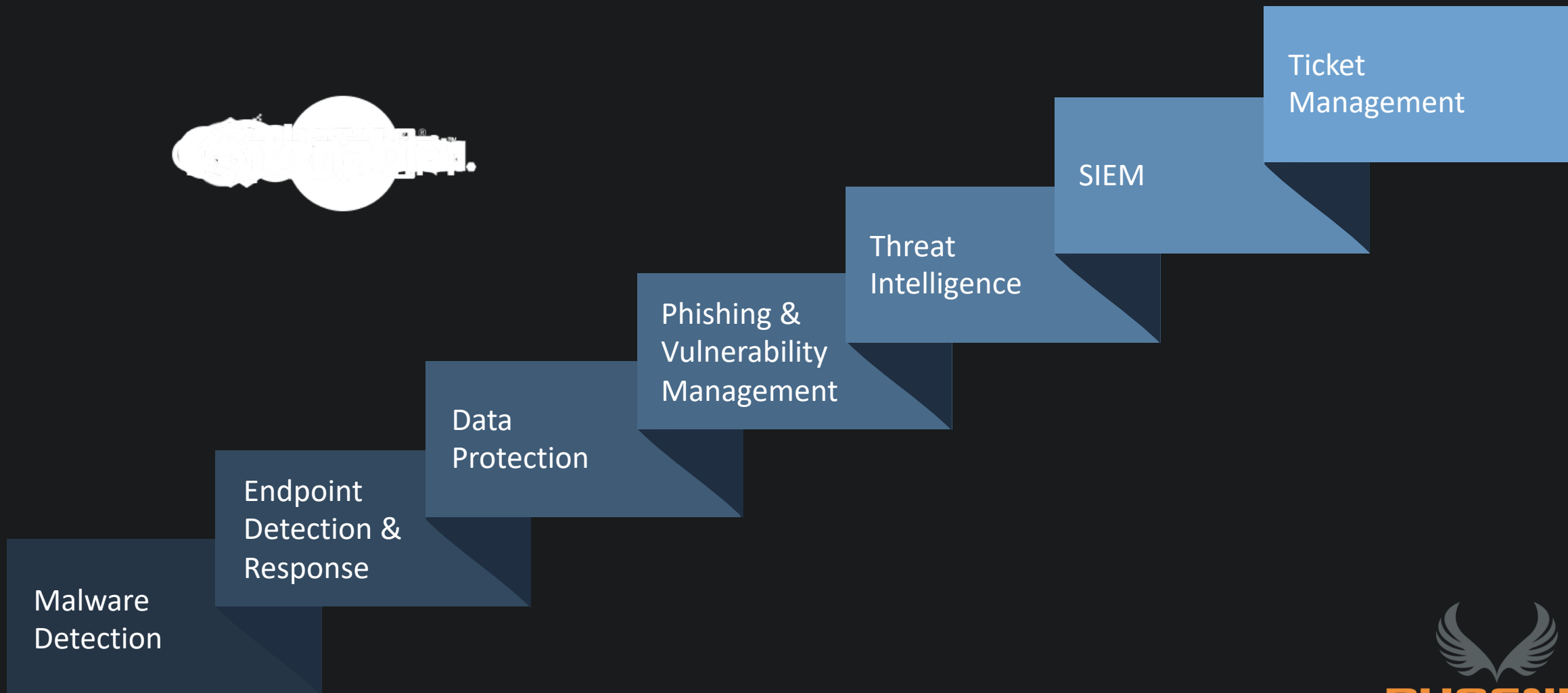
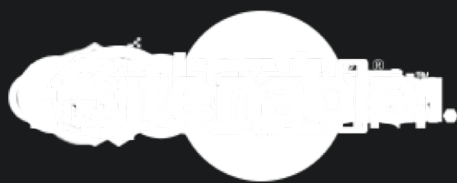
Unauthorized
Software

Privilege
Escalation

Forensic
Investigation

Reporting /
Dashboards

What do you want to Automate?



Choosing What to Automate



Analyst



Manager

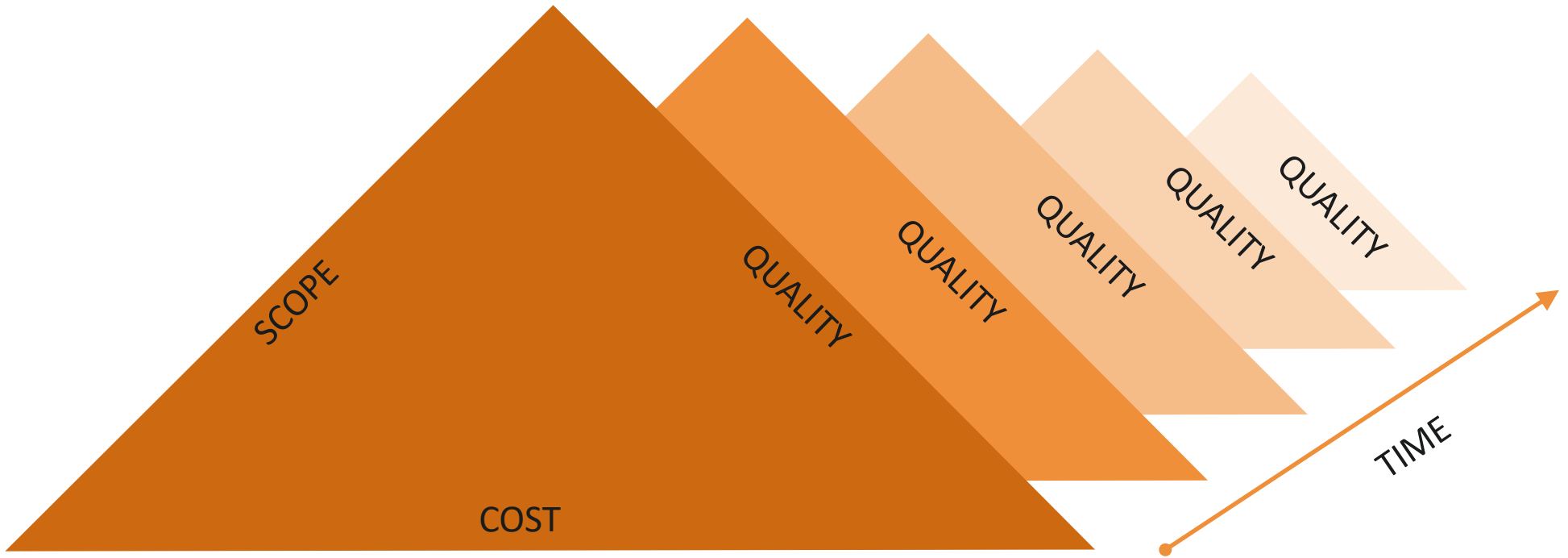
Applied

Practical

Theoretical



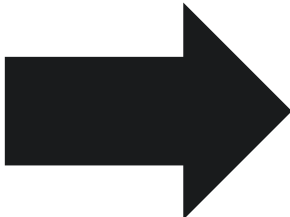
Time-to-Value Pressure



Understand Integrations and Data



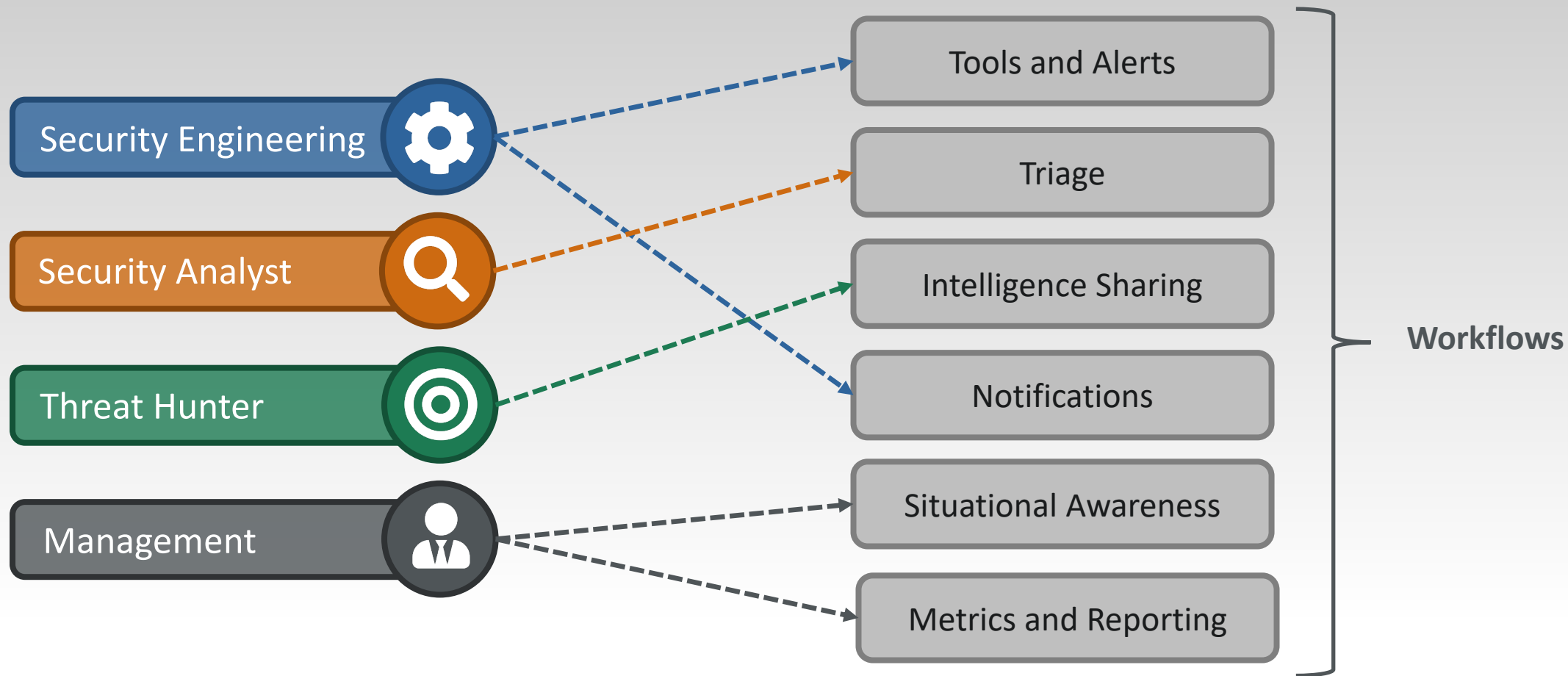
Inconsistent Data



JSON	JSON	JSON
JSON	JSON	JSON
JSON	JSON	JSON
JSON	JSON	JSON
JSON	JSON	JSON
JSON	JSON	JSON
JSON	JSON	JSON
JSON	JSON	JSON

Standardized Data

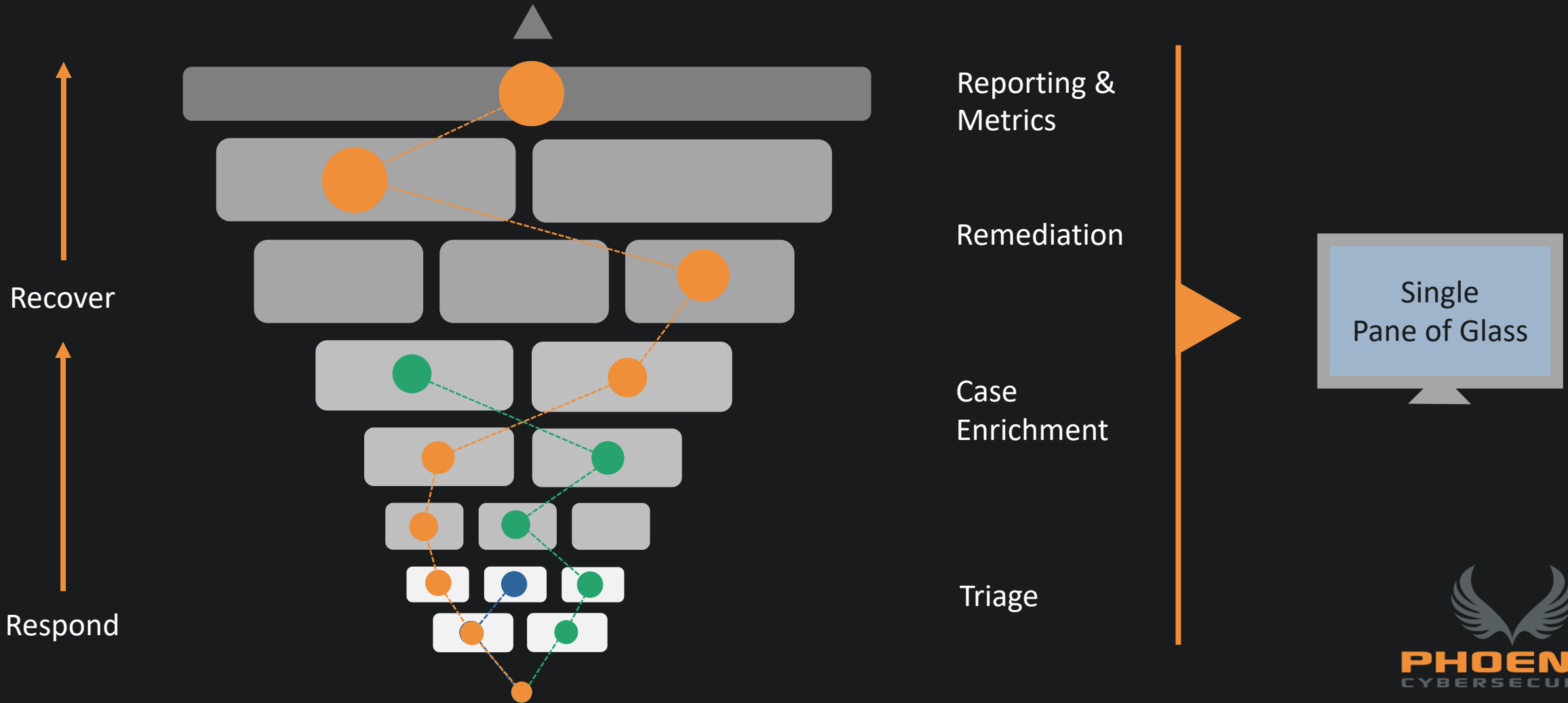
Workflow Ownership



Priority-based, Modular App Framework



Detailed Case for System of Record



Recover

Respond

Reporting & Metrics

Remediation

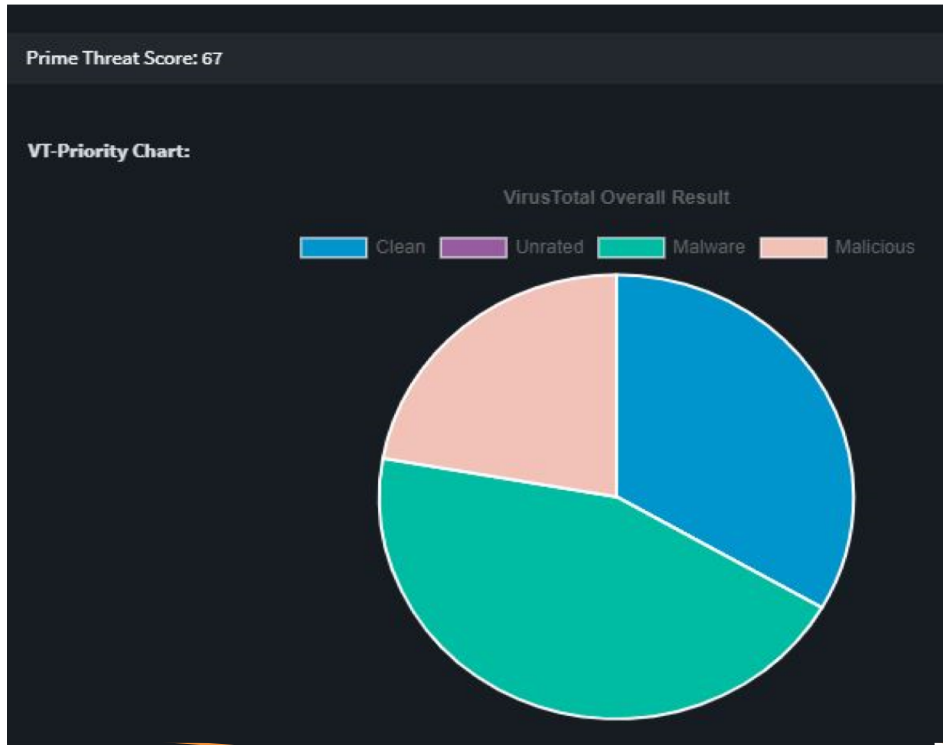
Case Enrichment

Triage

Single Pane of Glass



Single-Pane-of-Glass Curation



1

VIRUSTOTAL DATA

Search:

TOOL	CLASSIFICATION	PRIME TOOL
Baidu-International	Clean	No
BitDefender	Malware	Yes
Blueliv	Clean	No
C-SIRT	Clean	No
Certly	Clean	No
CLEAN MX	Clean	No
Comodo Site Inspector	Clean	Yes
CyberCrime	Clean	No
CyRadar	Clean	No

VirusTotal Treat Score: 15

Prime Threat Score: 67

VF-Full Chart:

VirusTotal Overall Result

Legend: Clean (blue), Unrated (purple), Malware (green), Malicious (orange)

VF-Priority Chart:

VirusTotal Overall Result

Legend: Clean (blue), Unrated (purple), Malware (green), Malicious (orange)



Engineering Principles Review



1

Establish Practical Operating Procedures (SOP)

2

Standardize Data Collection and Process Outputs

3

Assign Process Workflows to Most-Qualified Owner

4

Create a Modular, Templated App Framework

5


Implement Single-Pane-of-Glass Curation

6

Automate and Document the Deployment Lifecycle


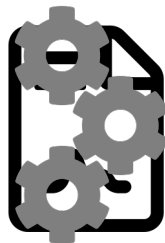


Deployment of Automation




Development Environment

010101010101010101010101
010101010101010101010101
010101010101010101010101
010101010101010101010101



Staging Environment

010101010101010101010101
010101010101010101010101
010101010101010101010101
010101010101010101010101



Production Environment

Q&A



Thank You!

Matt Rodriguez

Cybersecurity Solutions Architect

matt@phxcyber.com

Tom Goetz

Senior Cybersecurity Engineer

tom@phxcyber.com



1-888-416-9919 | info@phxcyber.com | www.phxcyber.com