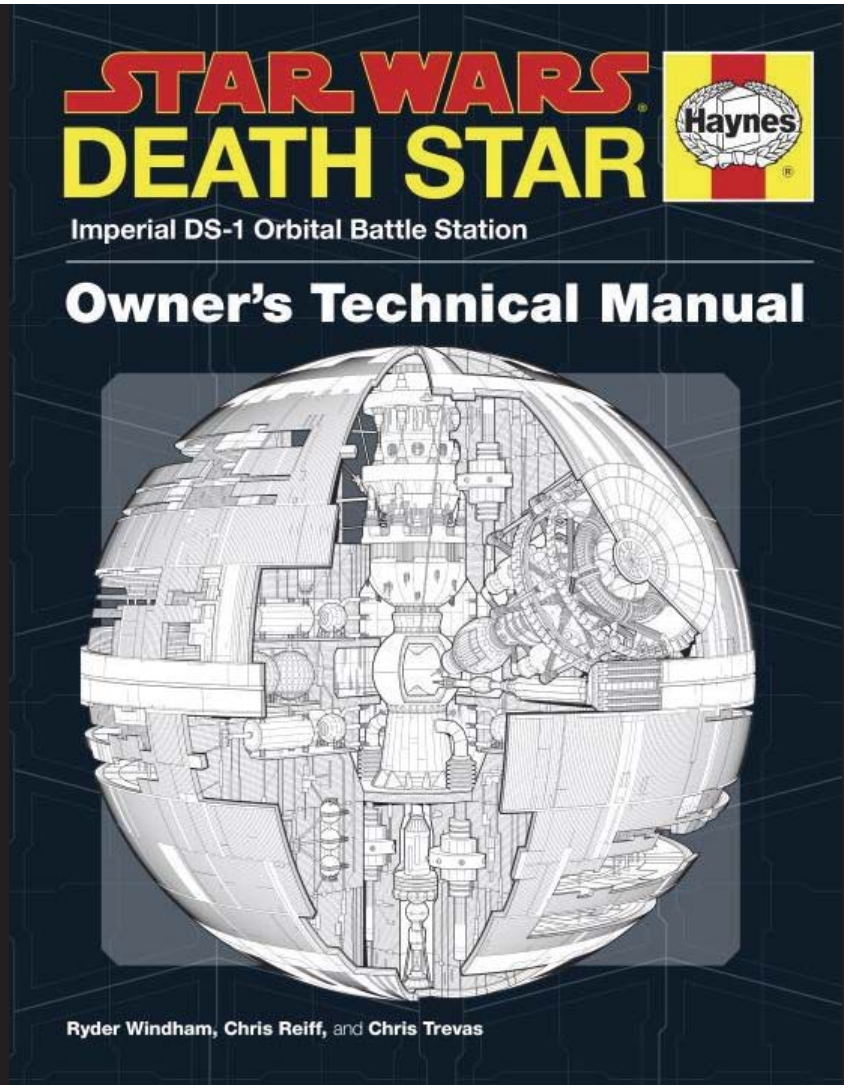
HOW WE SAVED THE DEATH STAR AND IMPRESSED LORD VADOR

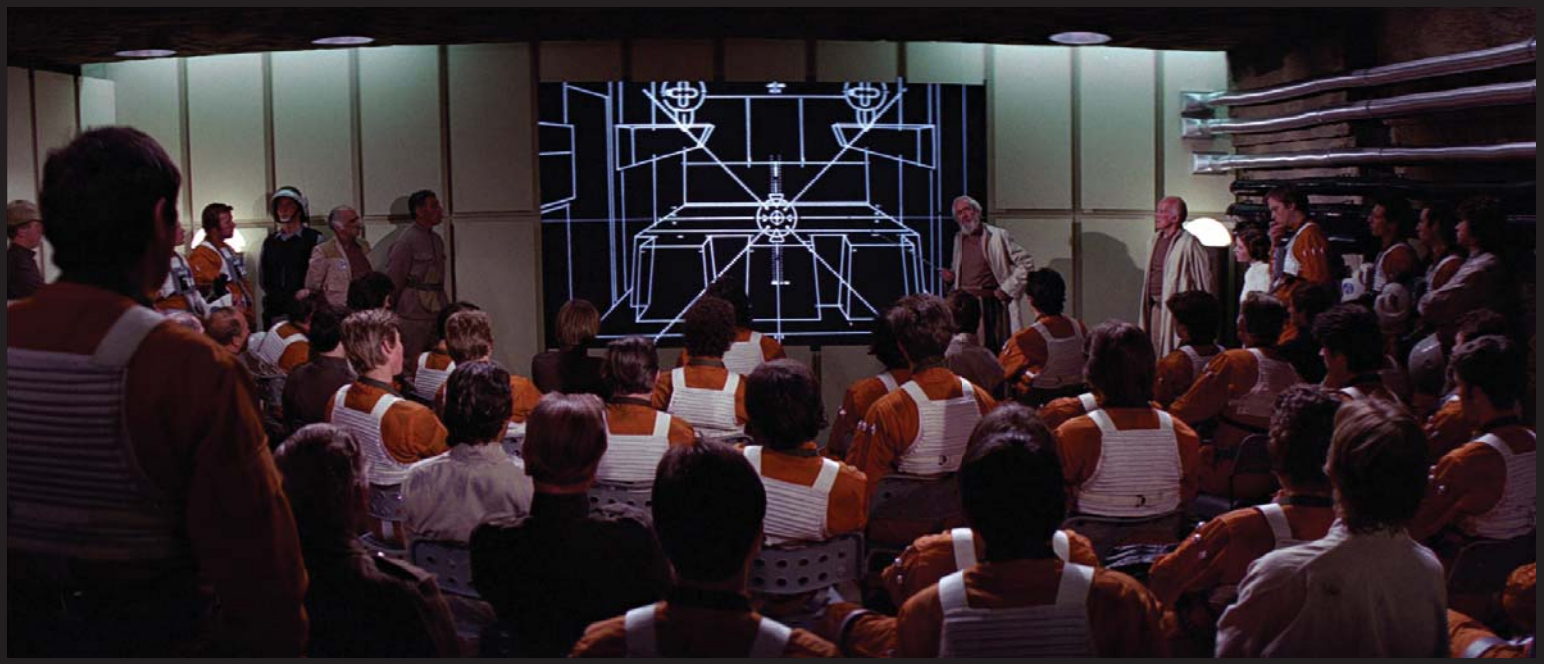
ADMIRAL MATTHEW VALITES
ADMIRAL JEFF BOLLINGER

THINGS ARE NOT GOING WELL FOR THE IMPERIAL ARMY...

PRINCESS LEIA EXFILTRATES DEATH STAR PLANS

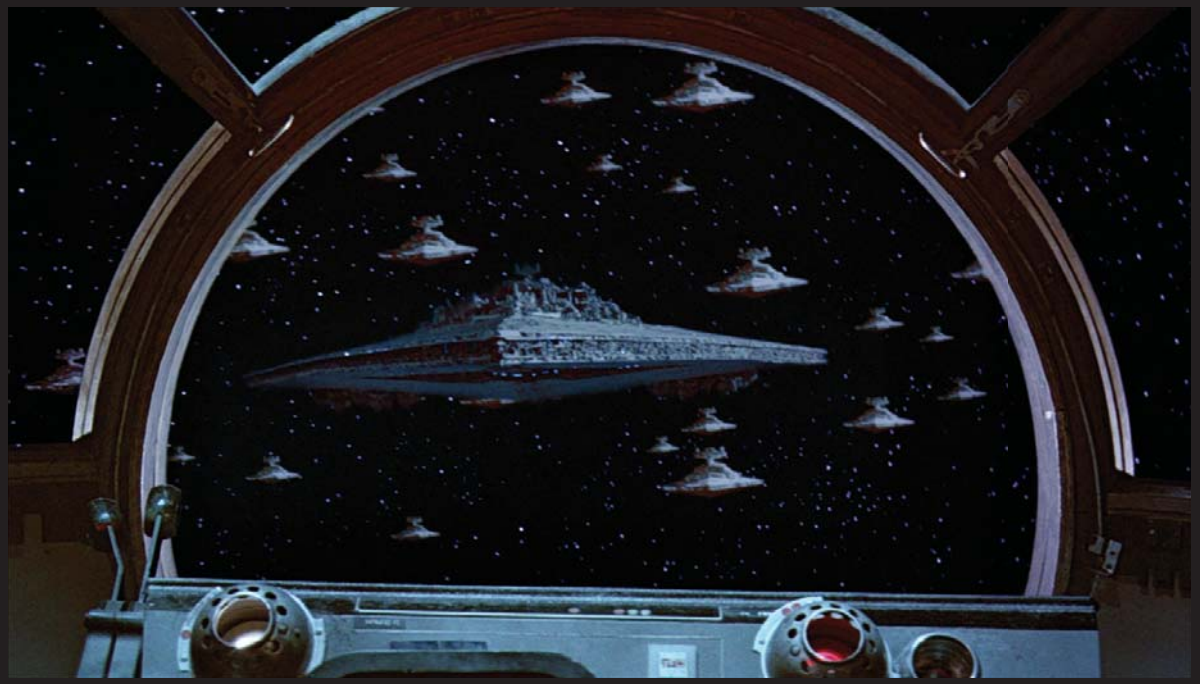


HAN AND LUKE RESCUE THE PRINCESS AND ESCAPE CAPTURE ON THE DEATH STAR



USING EXFILTRATED DATA, REBELS ATTACK
AN UNPATCHED VULNERABILITY,
DESTROYING THE FIRST DEATH STAR

LORD VADOR FIRES CISO AND RE-ORGS THE IMPERIAL ARMY SECURITY MONITORING CAPABILITIES



LORD VADOR AND THE EMPEROR USE A HONEYPOT TO TRAP LUKE

ADMIRAL MATTHEW VALITES

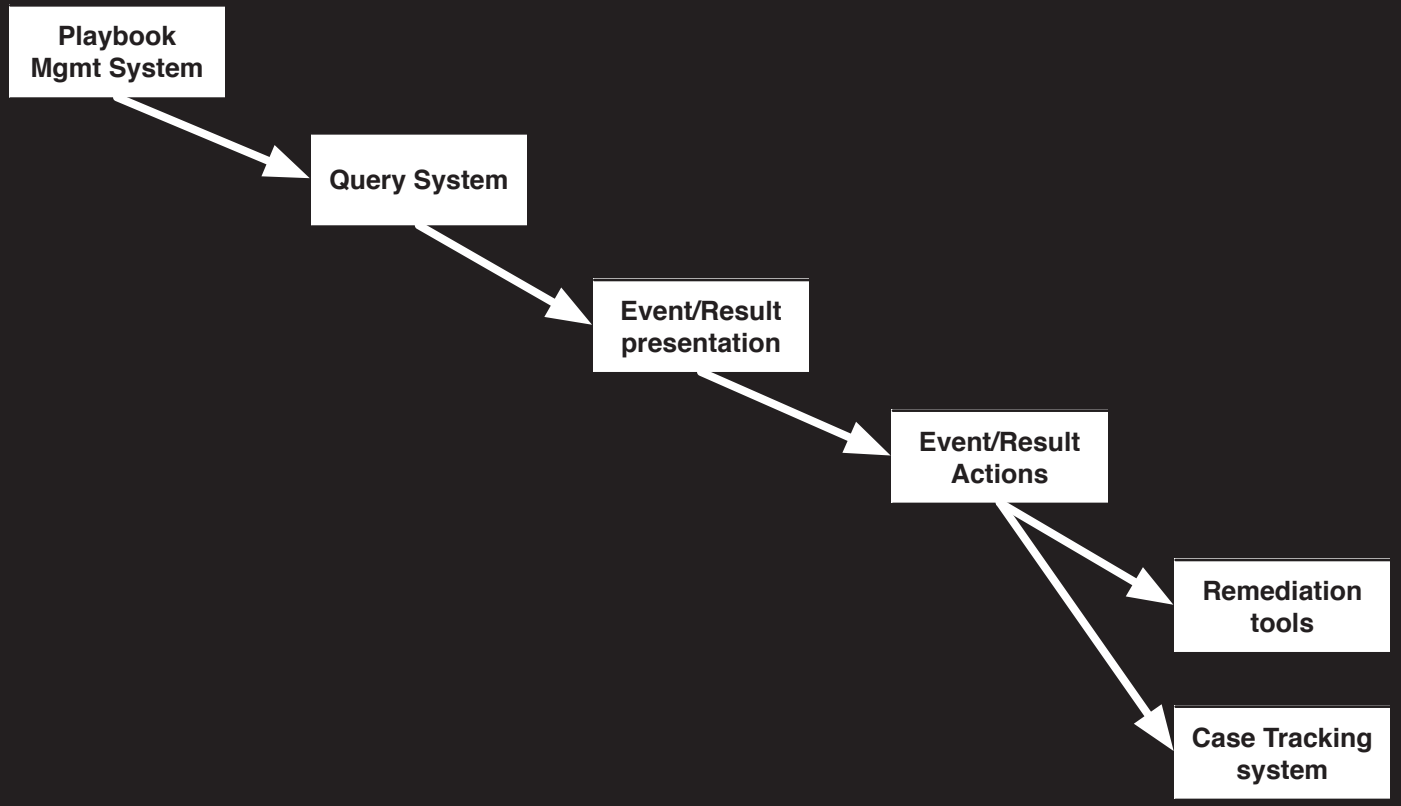
BIO BLAH BLAH BLAH

ADMIRAL JEFF BOLLINGER

BIO BLAH BLAH BLAH

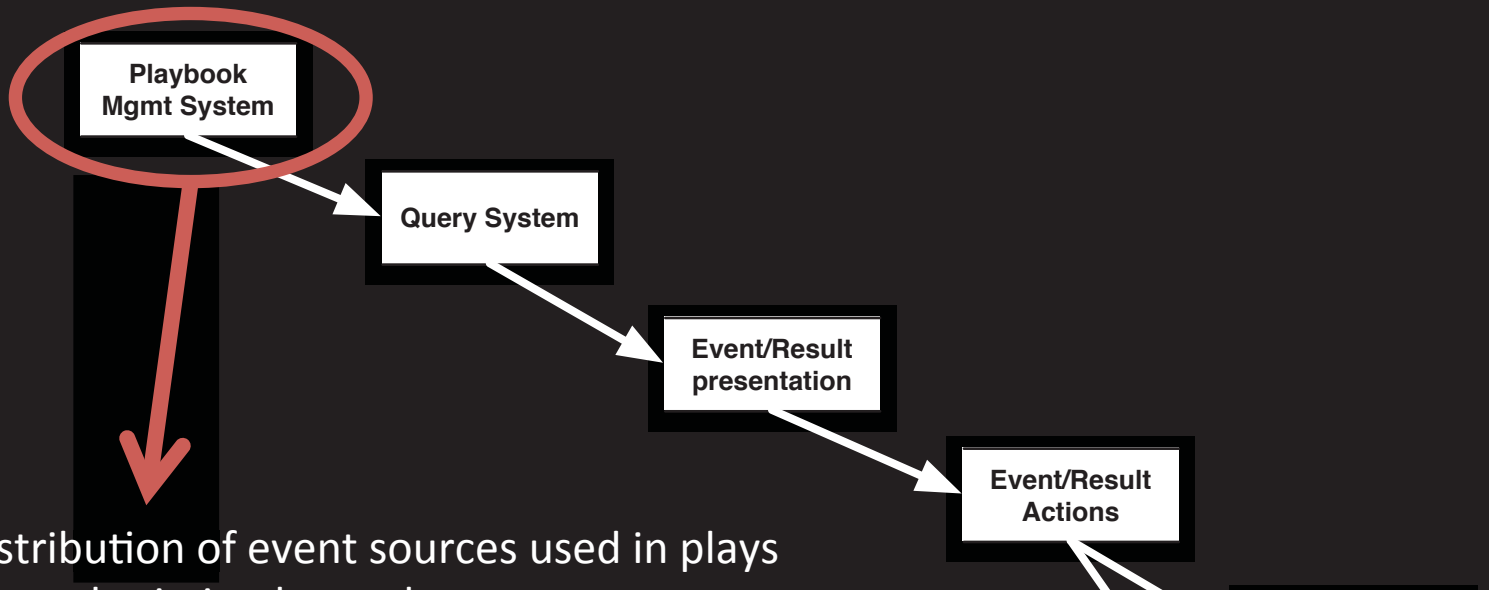
GETTING THE RIGHT METRICS

SECURITY MONITORING PROCESS



GETTING THE RIGHT METRICS

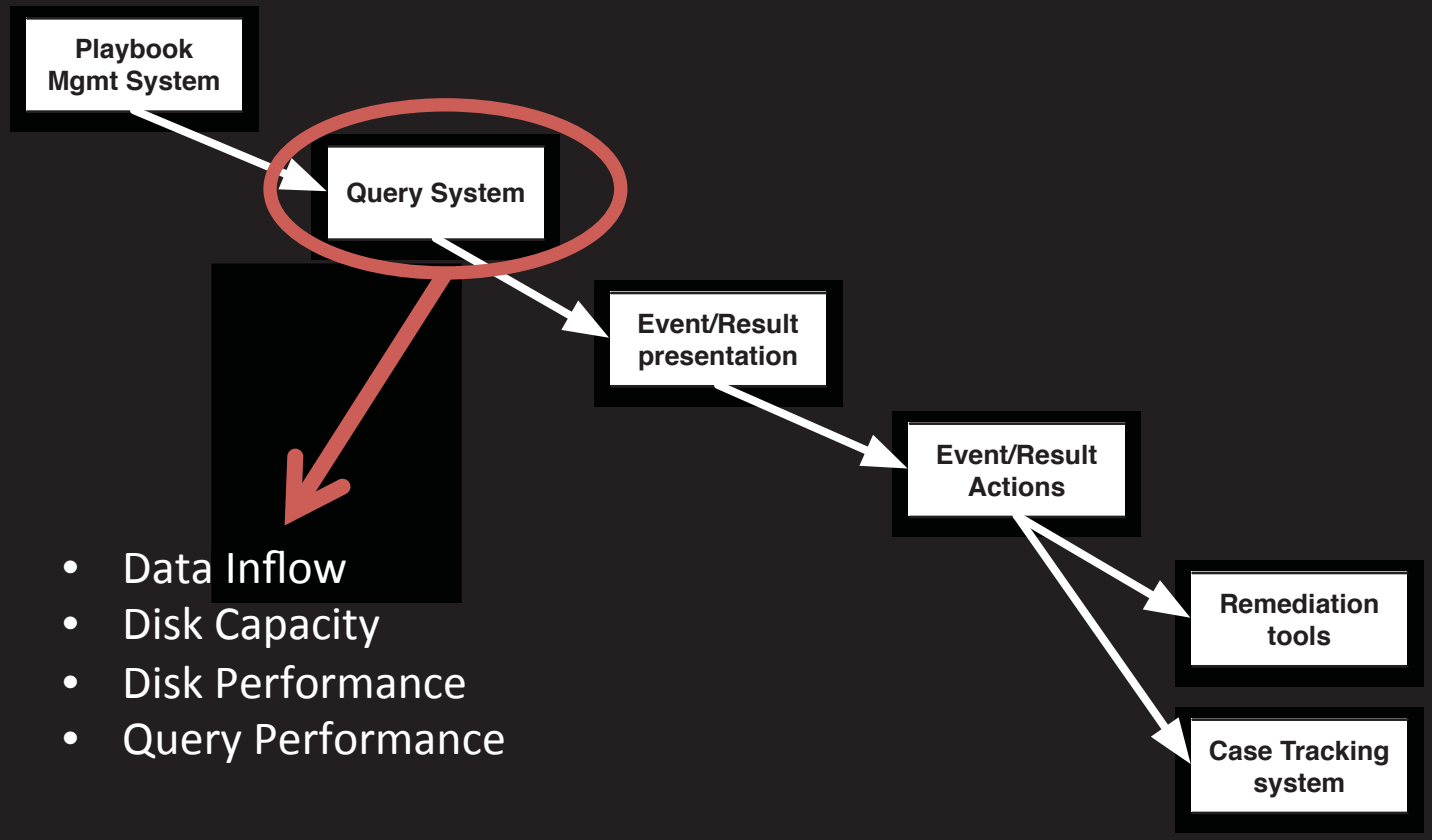
SECURITY MONITORING PROCESS



- Distribution of event sources used in plays
- Play submission by analyst
- Frequency of play submission/update
- Play status (New, QA, Deployed, Retired, etc)
- Time to transition play status

GETTING THE RIGHT METRICS

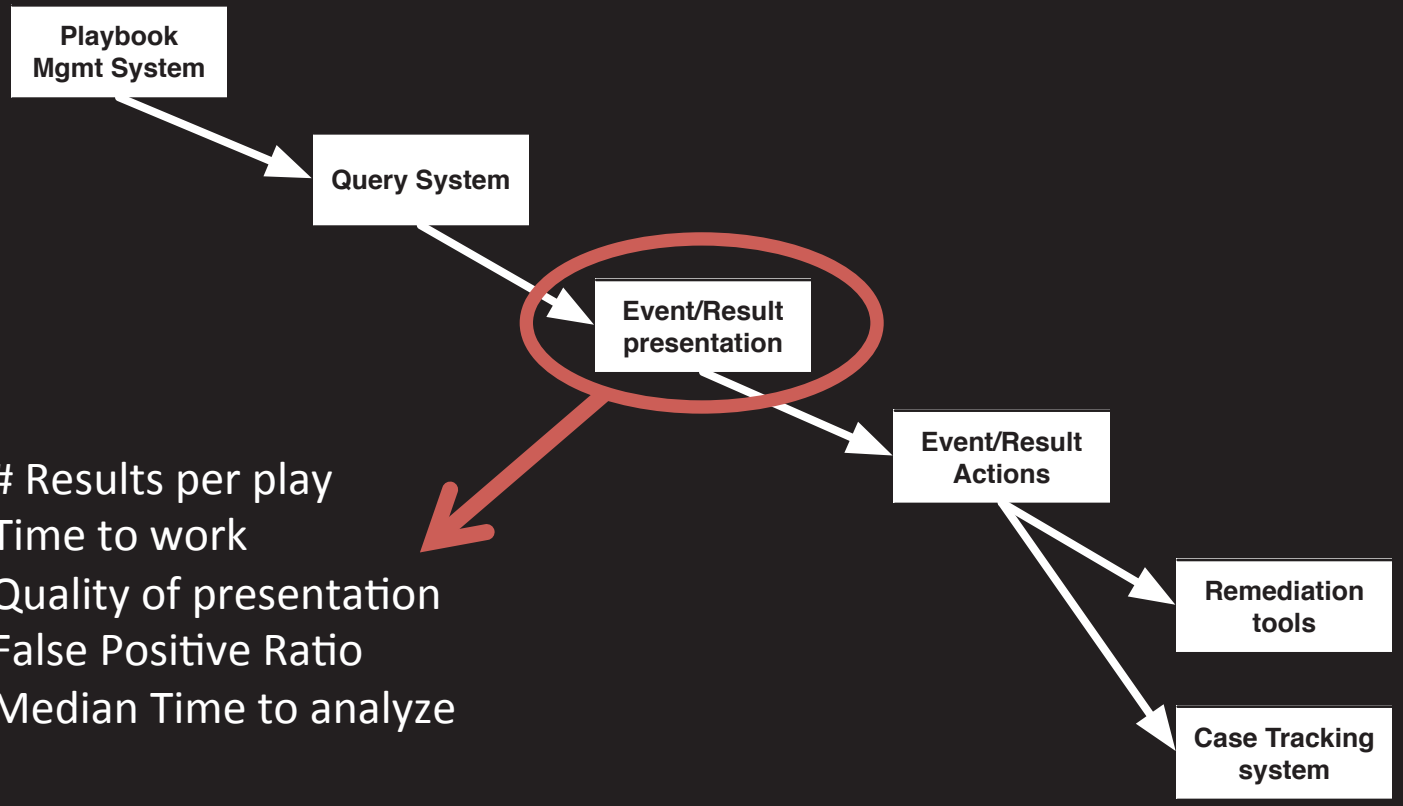
SECURITY MONITORING PROCESS



- Data Inflow
- Disk Capacity
- Disk Performance
- Query Performance

GETTING THE RIGHT METRICS

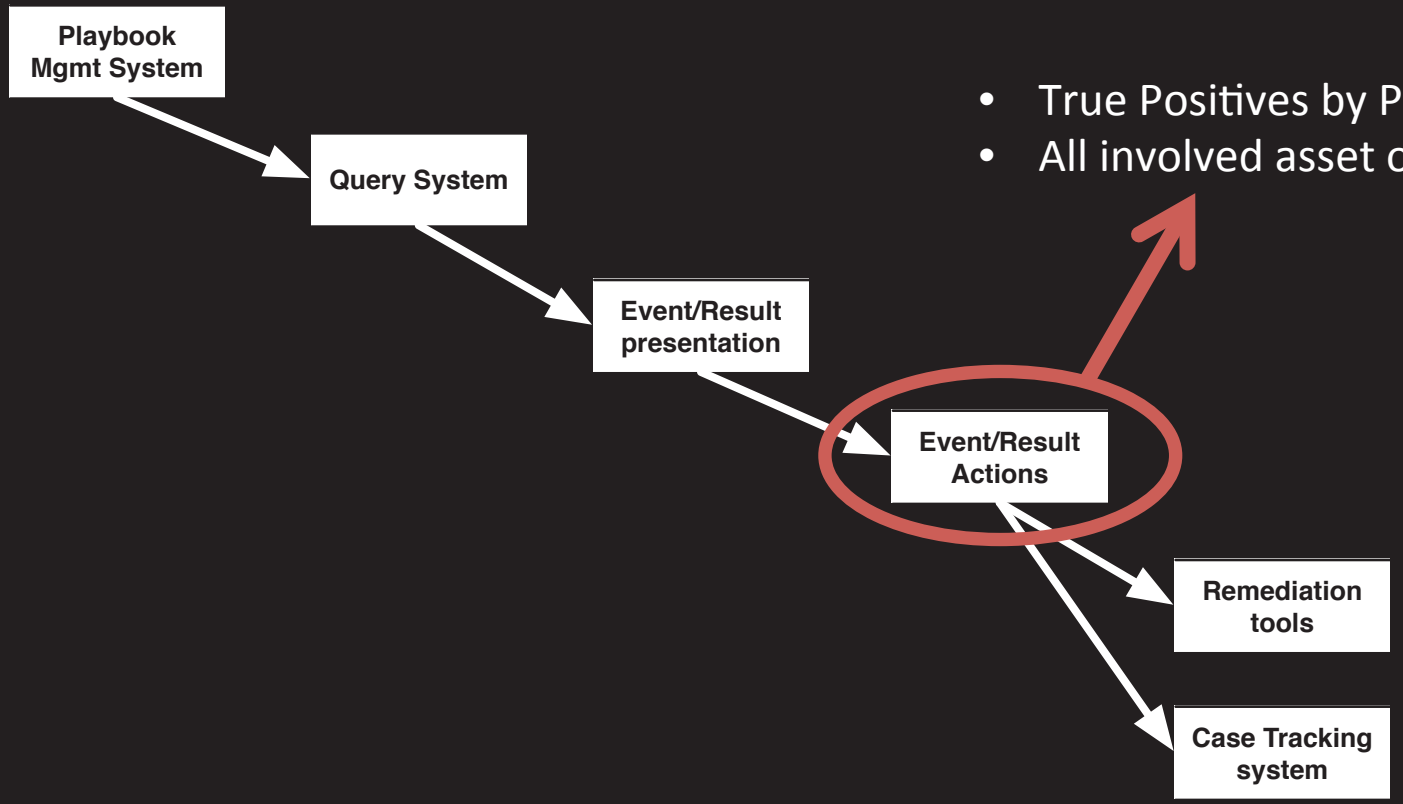
SECURITY MONITORING PROCESS



- # Results per play
- Time to work
- Quality of presentation
- False Positive Ratio
- Median Time to analyze

GETTING THE RIGHT METRICS

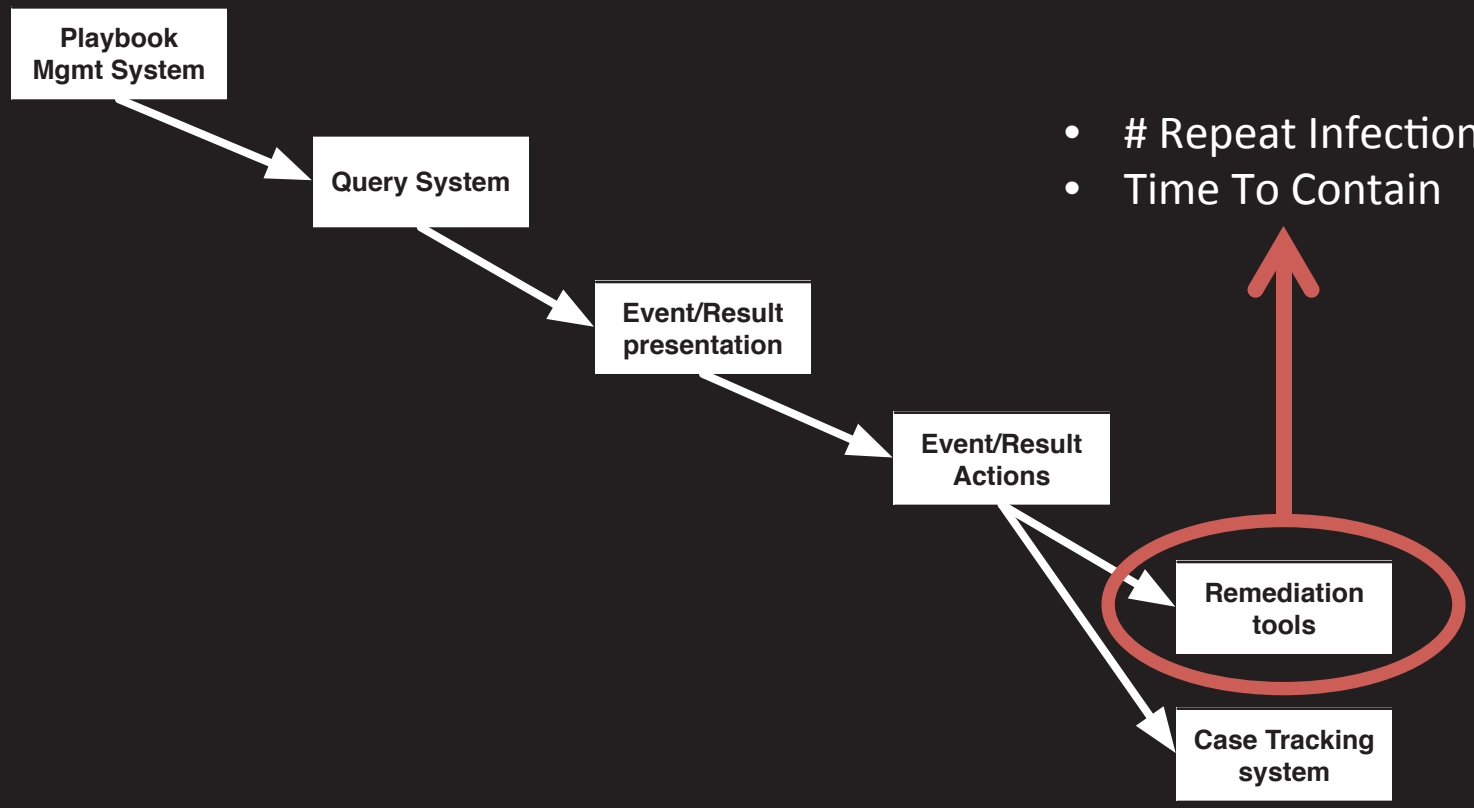
SECURITY MONITORING PROCESS



- True Positives by Playbook ID
- All involved asset owners

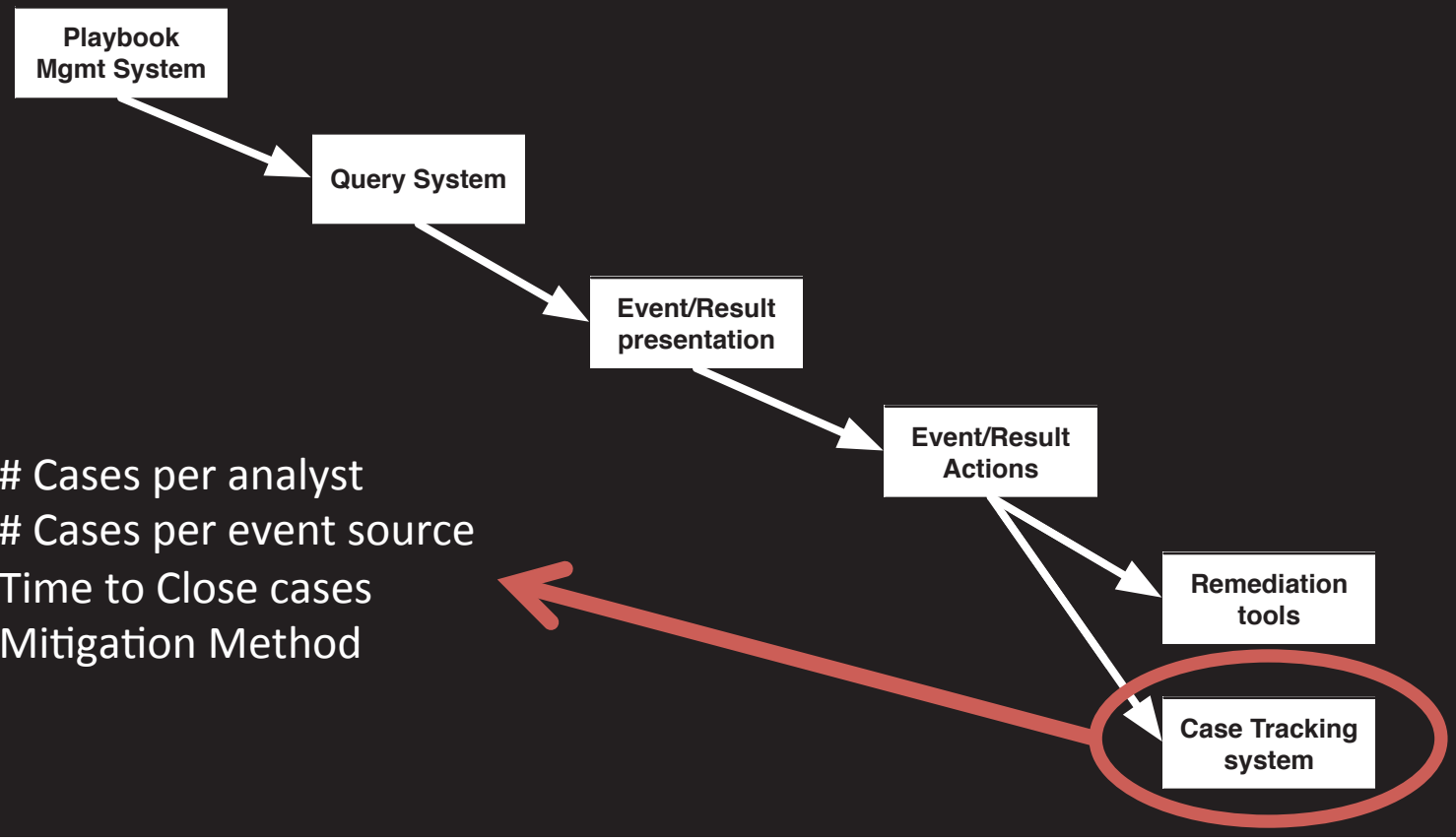
GETTING THE RIGHT METRICS

SECURITY MONITORING PROCESS



GETTING THE RIGHT METRICS

SECURITY MONITORING PROCESS



- # Cases per analyst
- # Cases per event source
- Time to Close cases
- Mitigation Method

USING A COMMON LANGUAGE

'INCIDENT'

- Asset compromise?
- Involves one host or multiple hosts?
- Synonymous with a case?

'TIME TO CONTAIN / WORK / MITIGATE'

- When does the clock start?
- When is an incident contained?
- How does mitigate differ from remediation?

'PLAY EFFICACY'

- Why classify plays as benign?
- What is the base rate fallacy?

USING A COMMON LANGUAGE

TTD/TTC/TTM

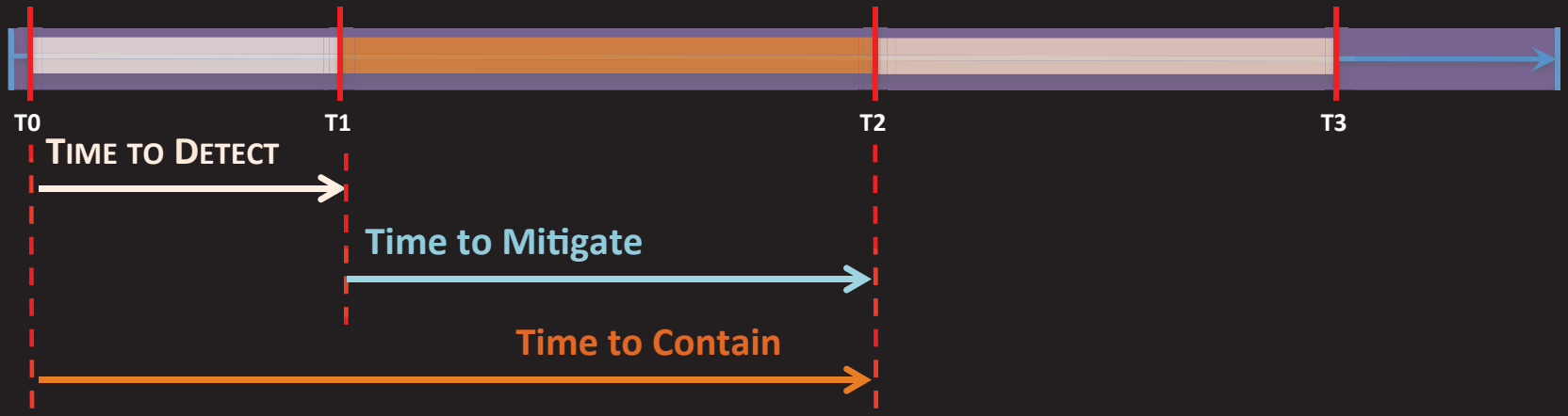
INCIDENT TIMELINE

T0: First Activity
Beginning of incident; e.g. host infected

T1: Detection
Awareness of breach, via detection technology or other notification

T2: Containment
Breach is no longer able to do damage or spread

T3: Remediation
Asset is cleaned, threat is removed



USING A COMMON LANGUAGE

PLAY EFFICACY

4 RESULT TYPES:

- **True Positive**
- **False Positive**
- **Benign**
- **Indeterminable**

FALSE POSITIVE PARADOX:

Given:

- 90% TP rate
- 0.015% FP rate

Assuming 1 in 1,000,000 events are malicious:

- 0.59% probability of TP