ENIGMA®

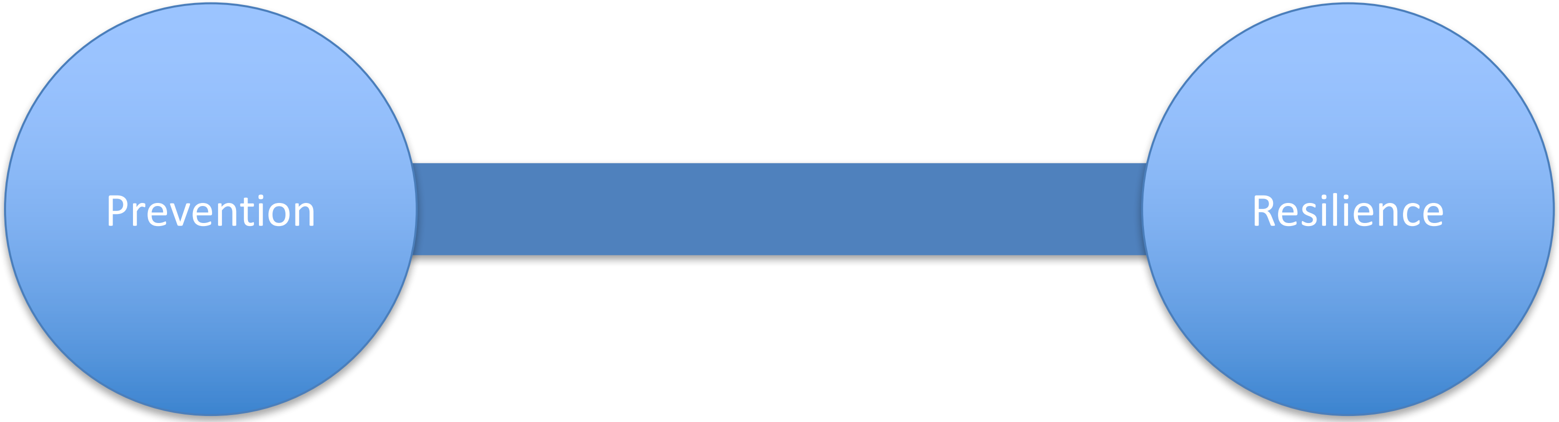
A USENIX CONFERENCE

What cybersecurity can learn from the Secret Service

Nathaniel Gleicher

Head of Cybersecurity Strategy, Illumio

POLICE


Prevention
Resilience

146

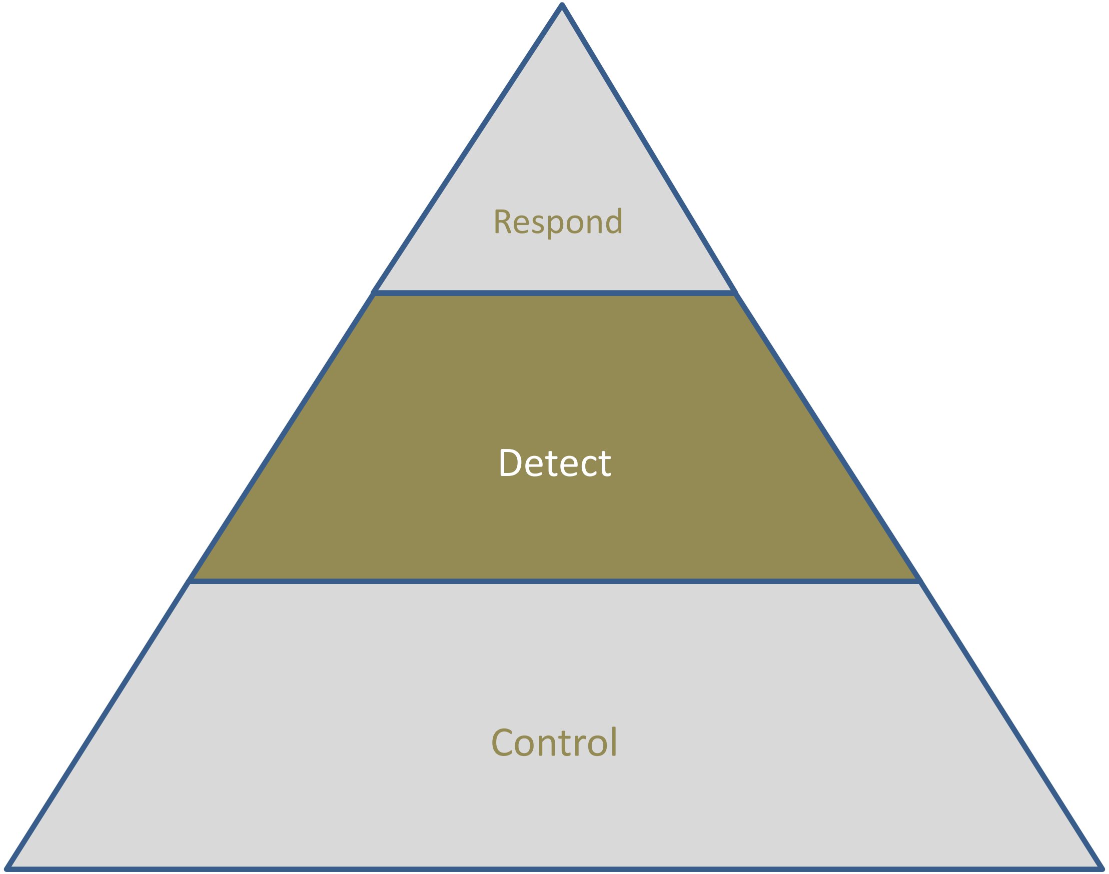
Dwell time (in days)

Why?

SECRET
US
SERVICE

Why the Secret Service?

POTUS Is a High-Value Asset



Respond

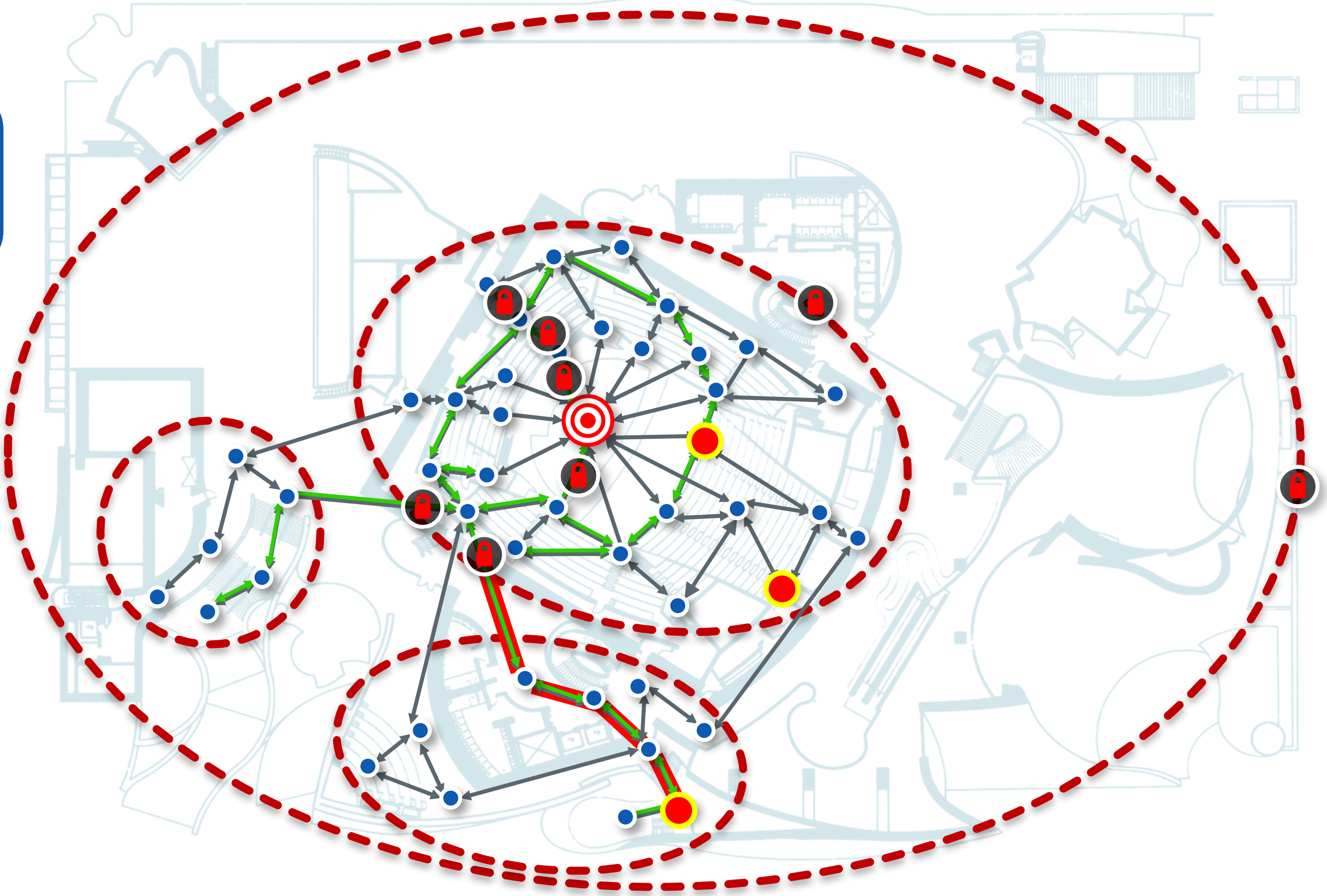
Detect

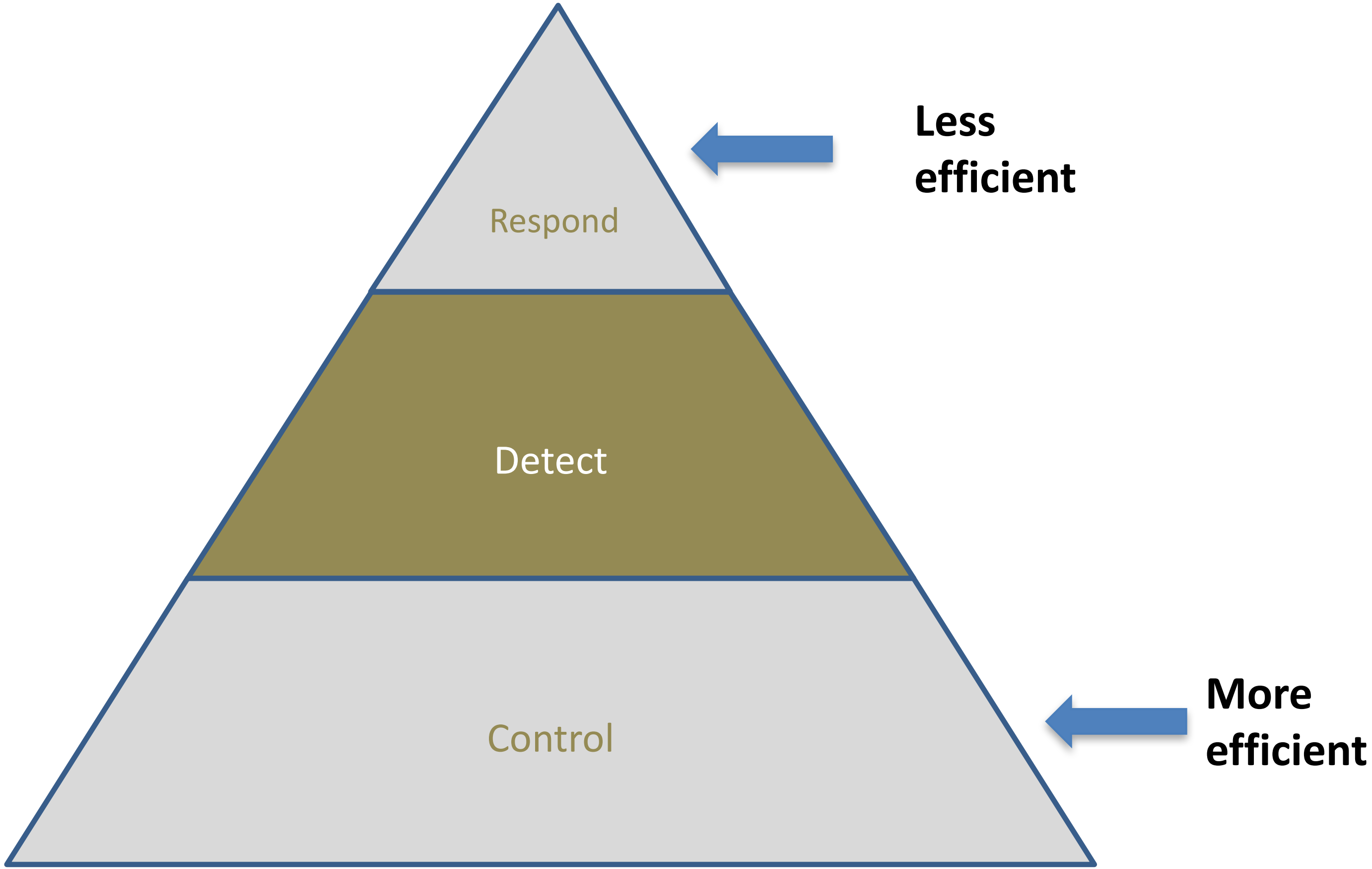
Control

Mapping the Relationship Graph

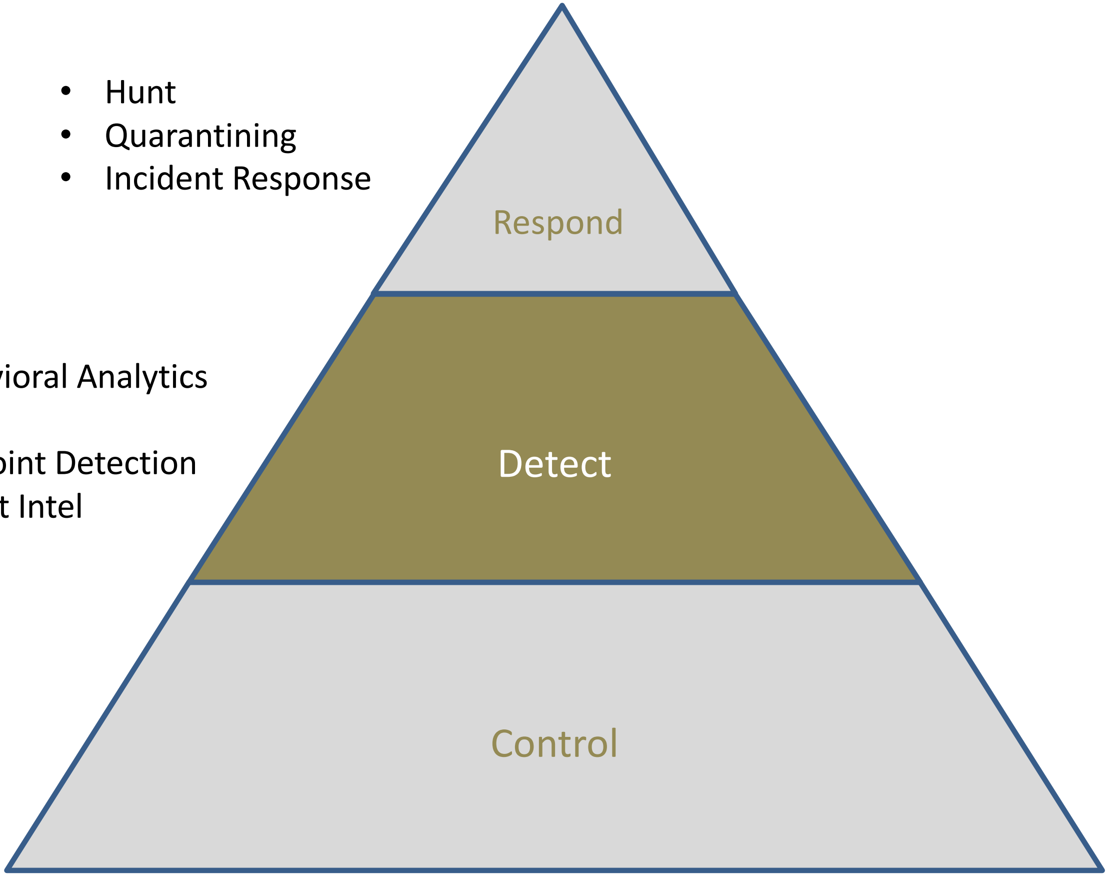
Control

- Metal detectors
- Video cameras
- ID checks




Respond
Detect
Control
Less efficient
More efficient

- Control is efficient
- Control helps prioritize
- Control speeds up detection and response

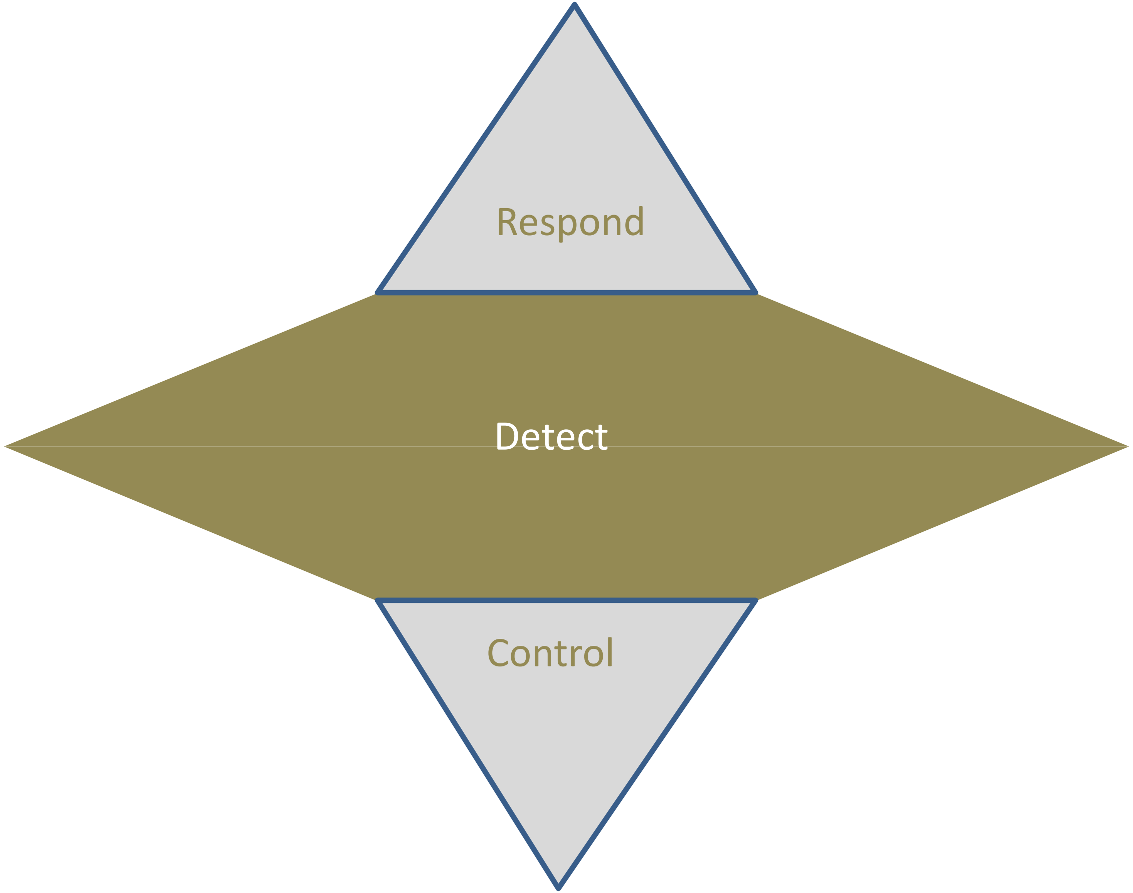


- Hunt
- Quarantining
- Incident Response

- Behavioral Analytics
- IDS
- Endpoint Detection
- Threat Intel

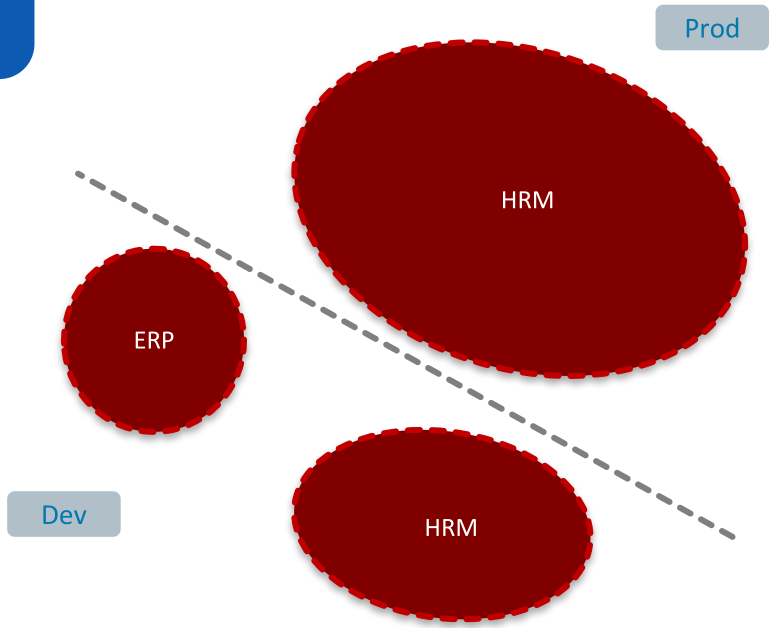
- Segmentation
- Patch Mgmt
- Identity/Access Mgmt
- Encryption

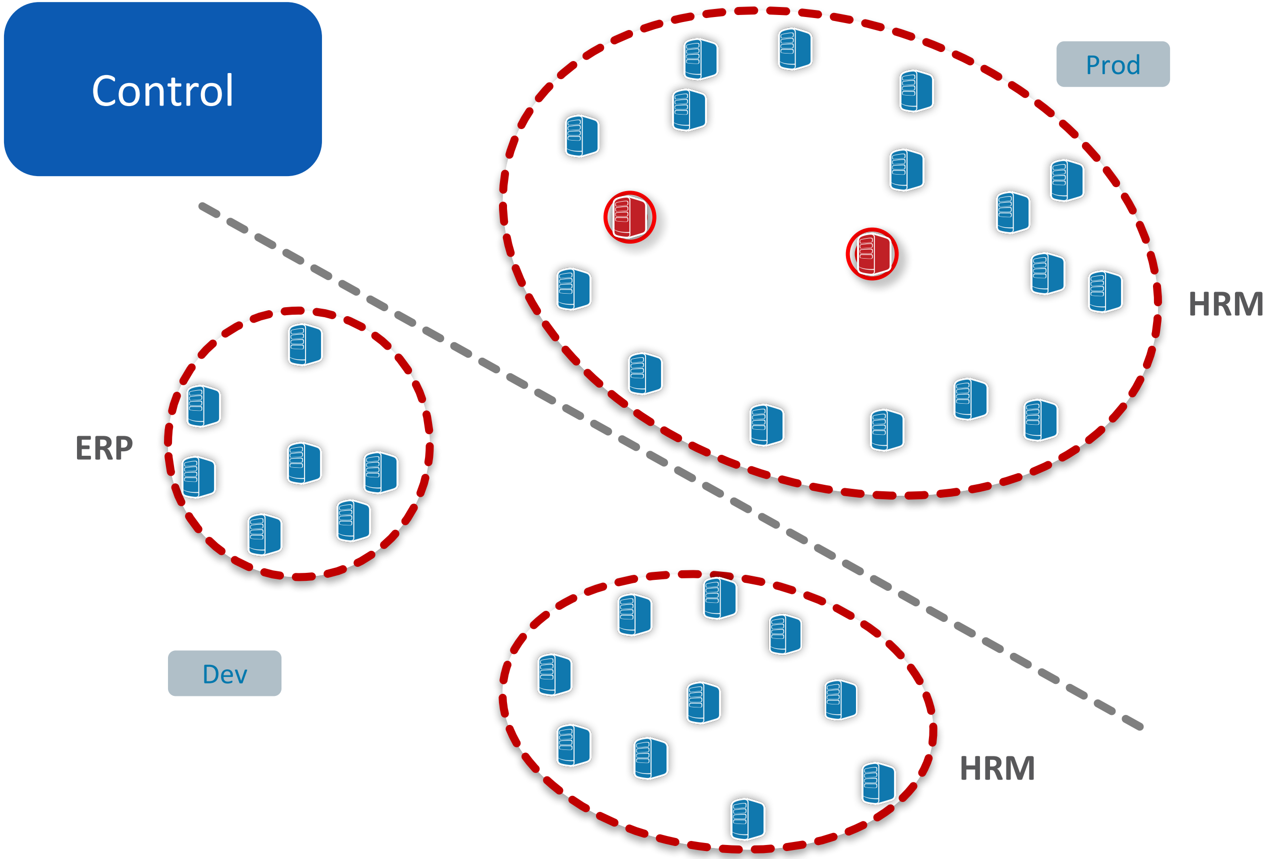
A dose of reality.


Respond
Detect
Control

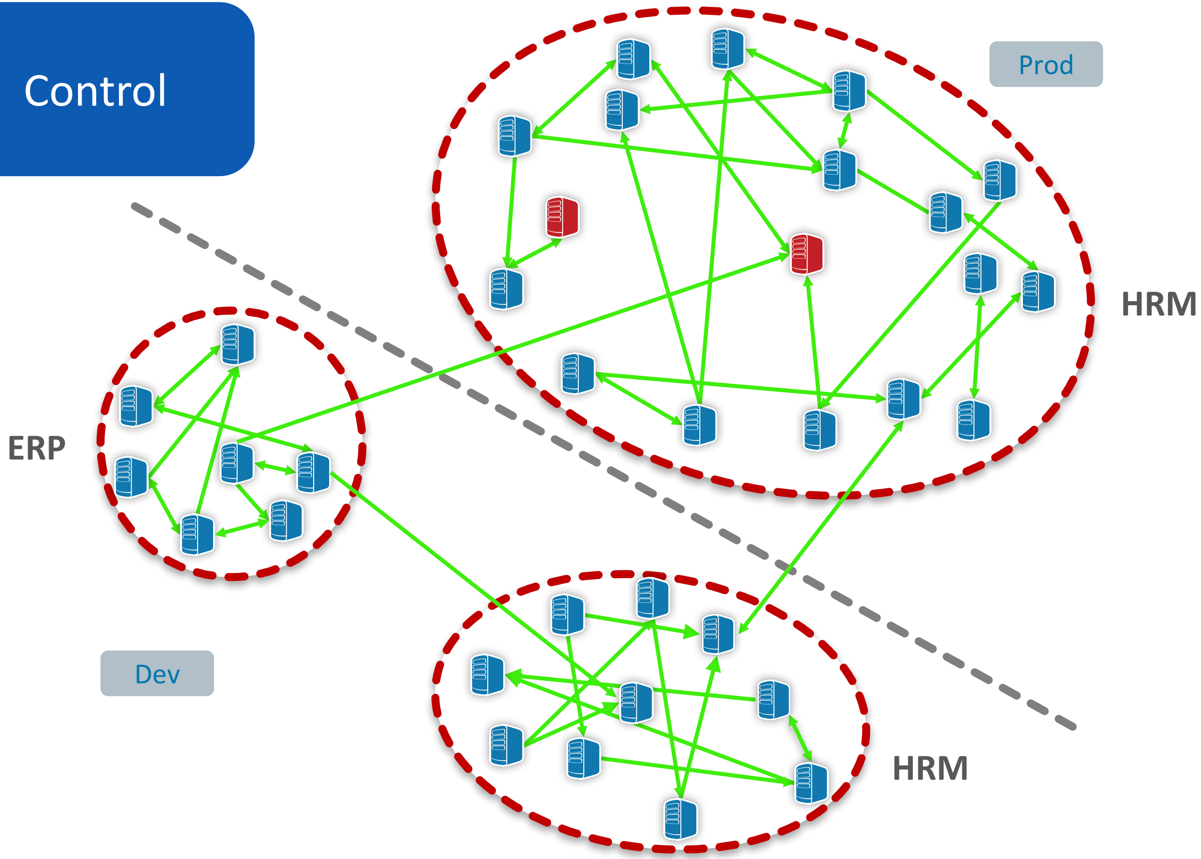
The Data Center Also Has a Relationship Graph

Control

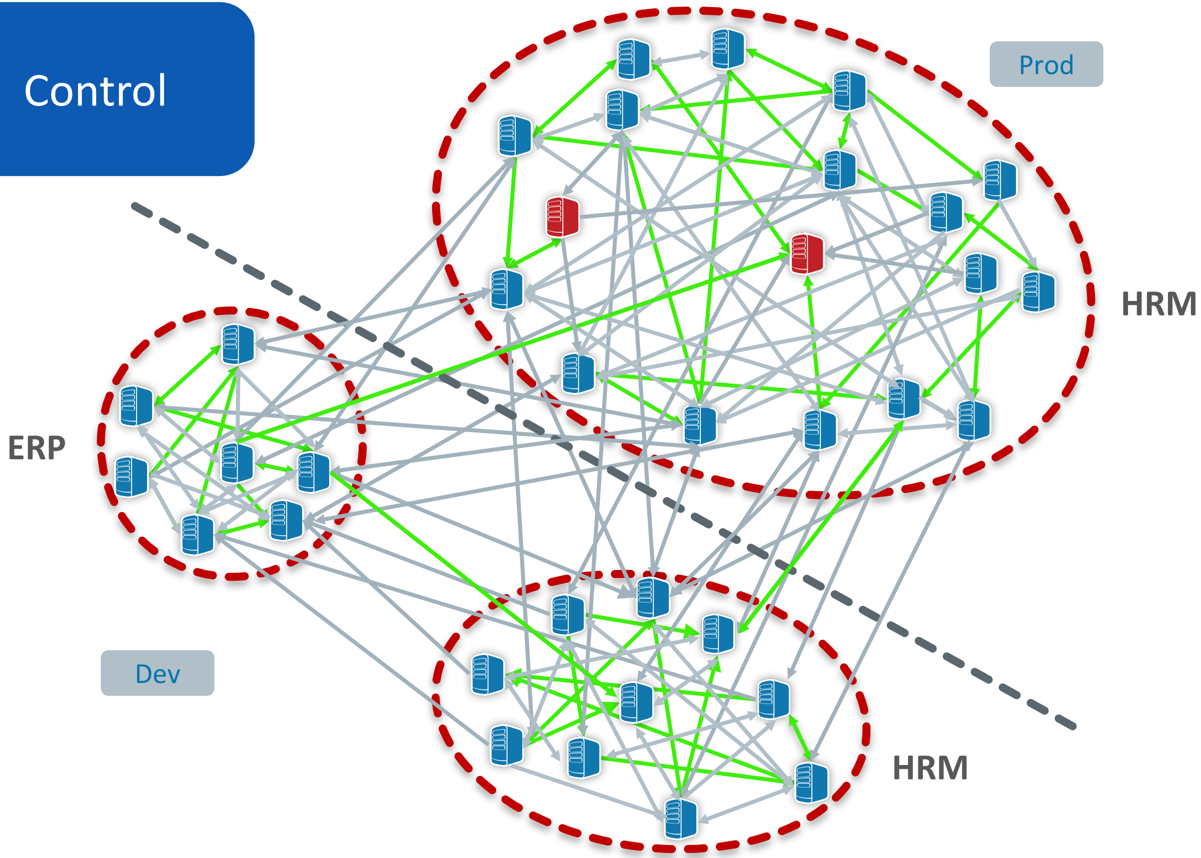



Control
Prod
HRM
ERP
Dev
HRM

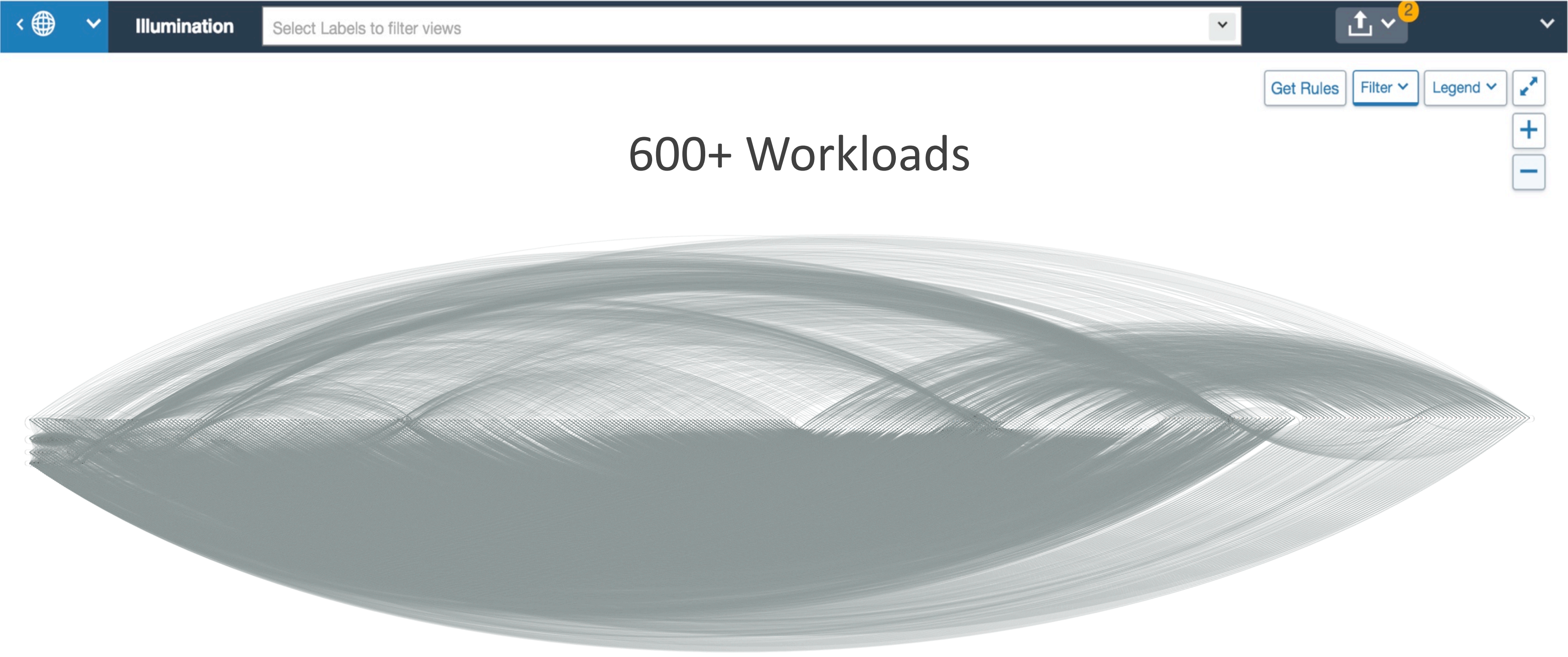
Control



Control



600+ Workloads

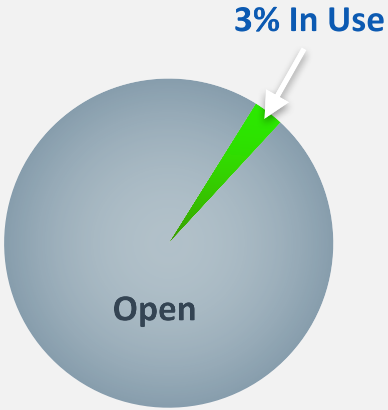


Data Center and Cloud Attack Surface

107 Workloads

244,050 Open Pathways

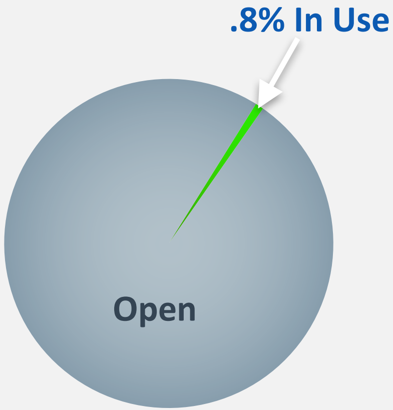
6,663 Paths In Use



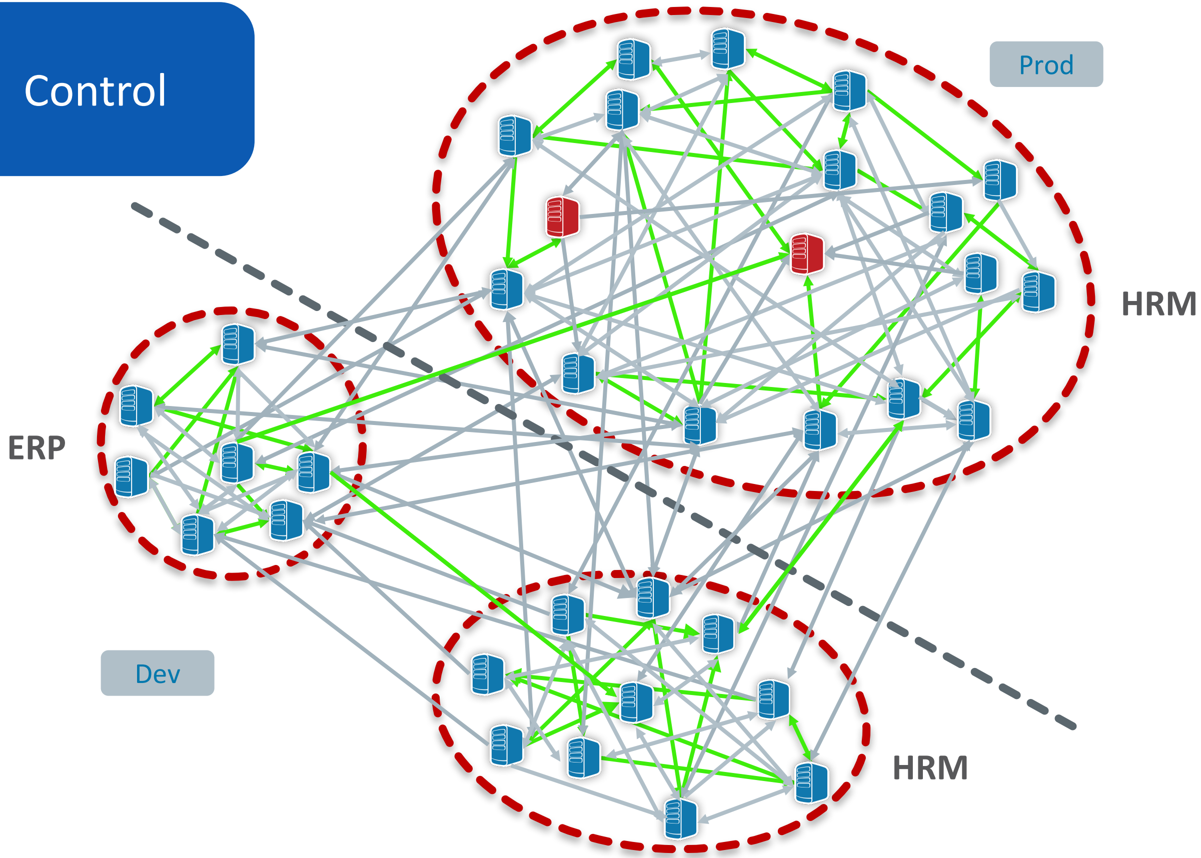
3,500 Workloads

37,012,842 Open Pathways

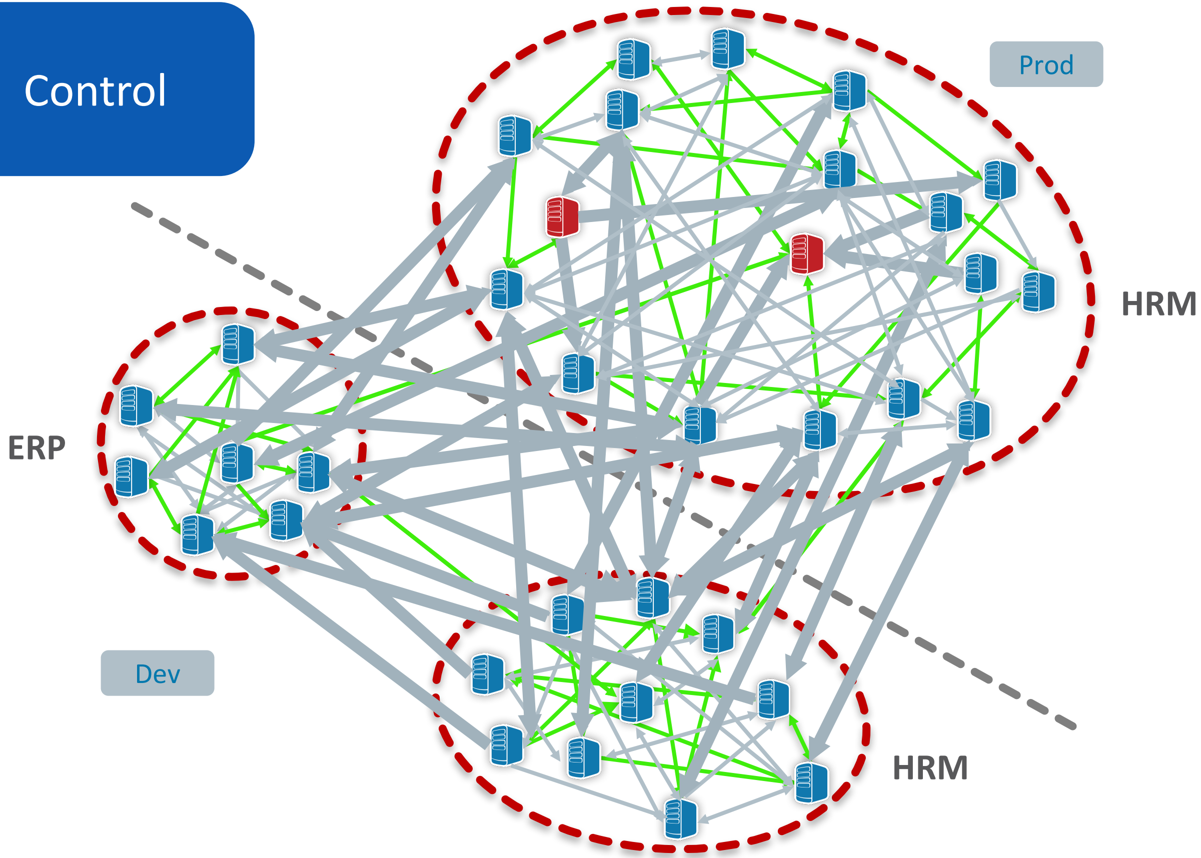
342,549 Paths In Use



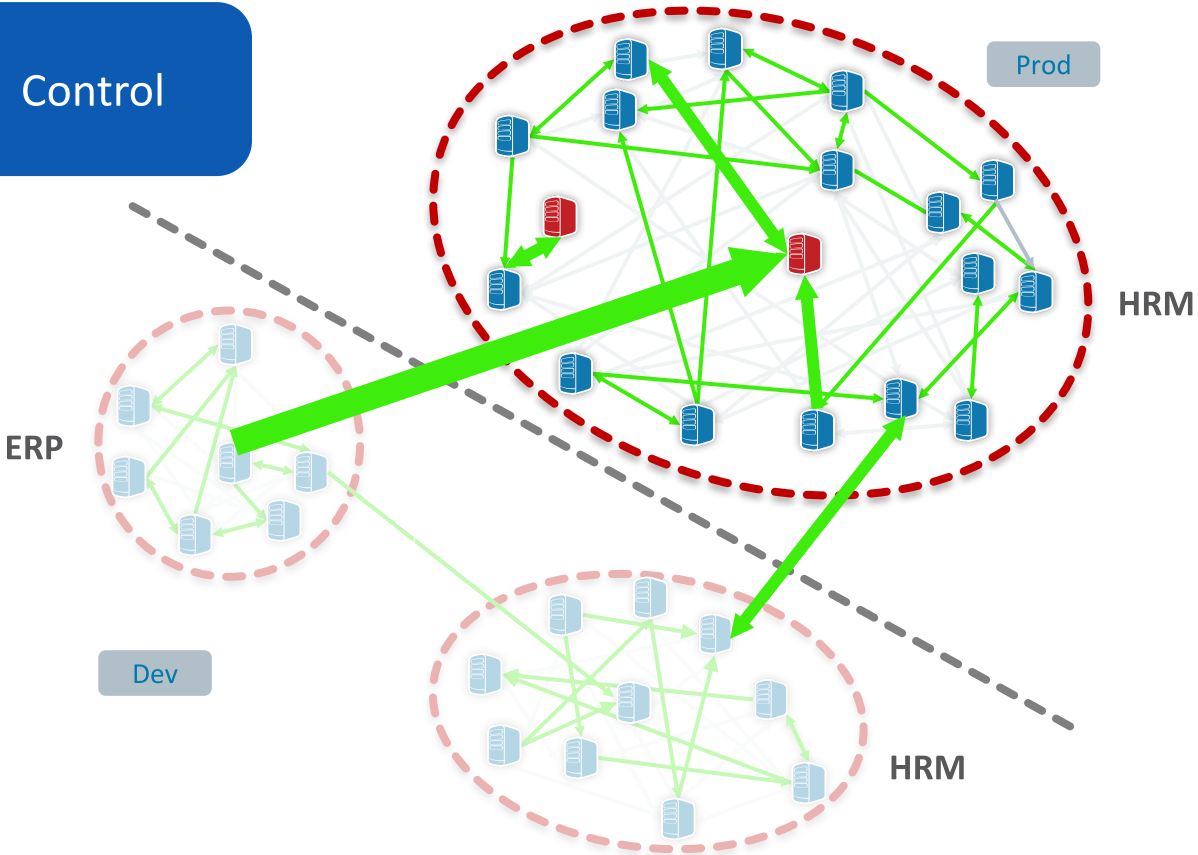
Control



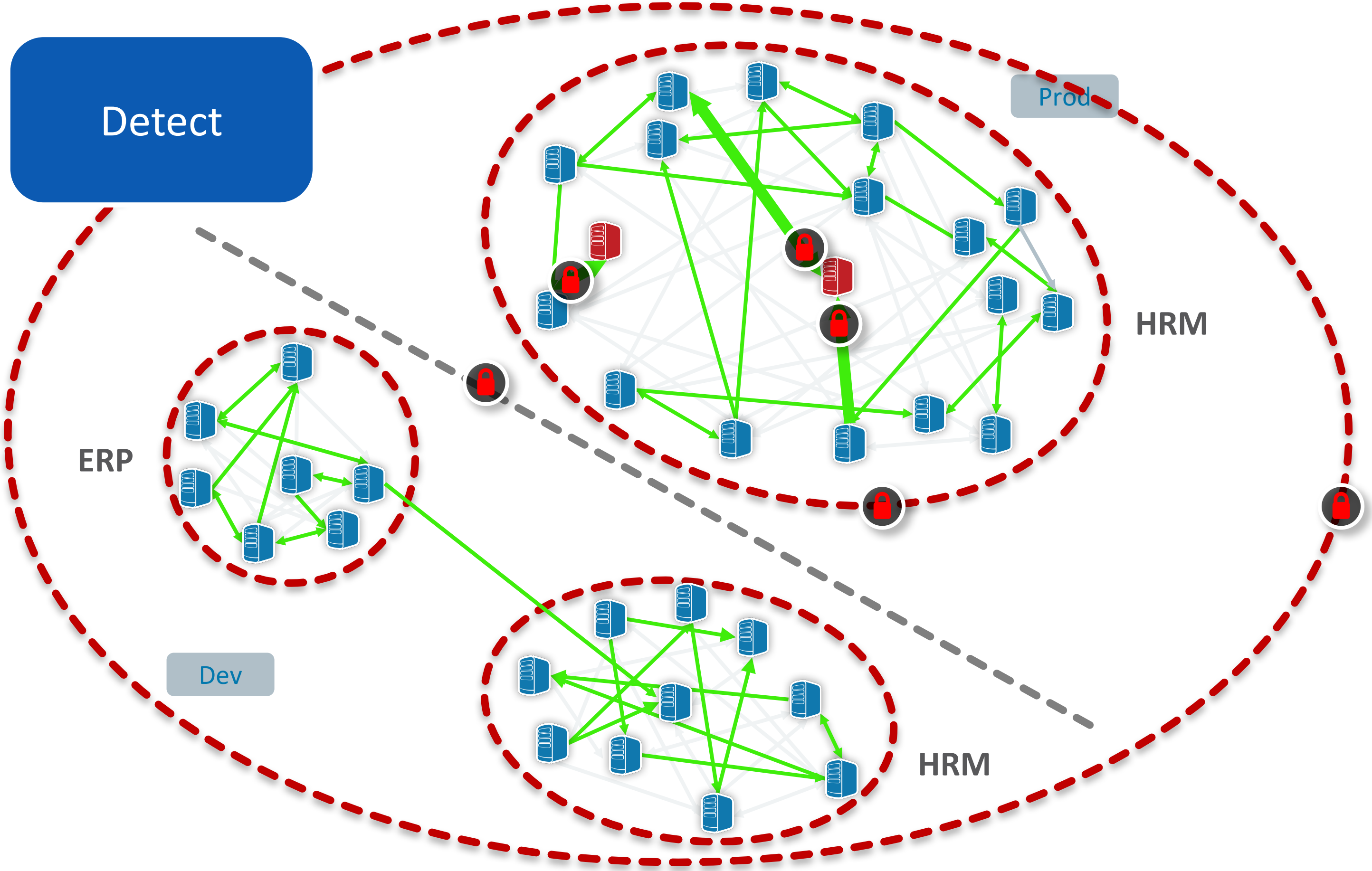
Control



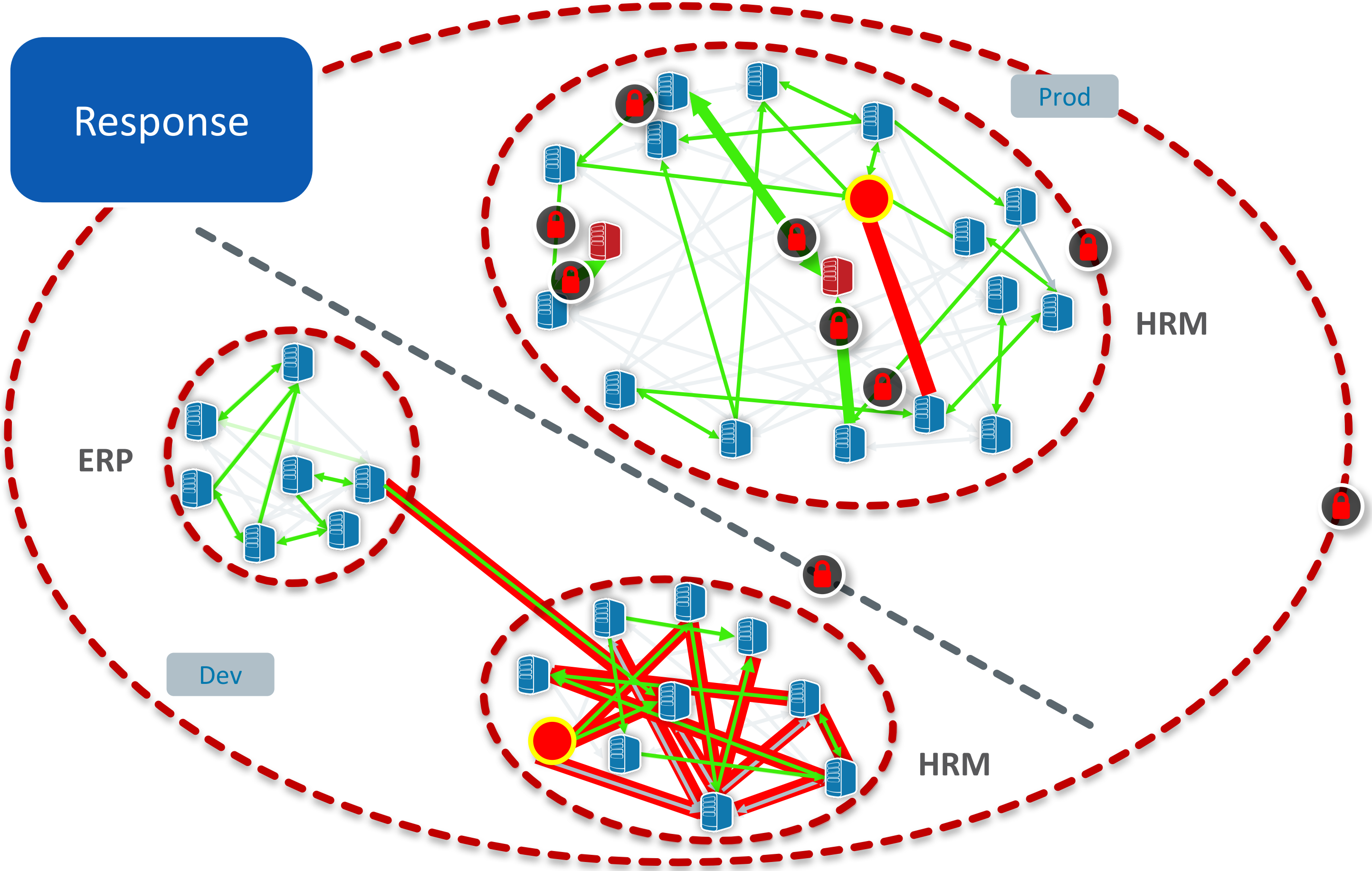
Control

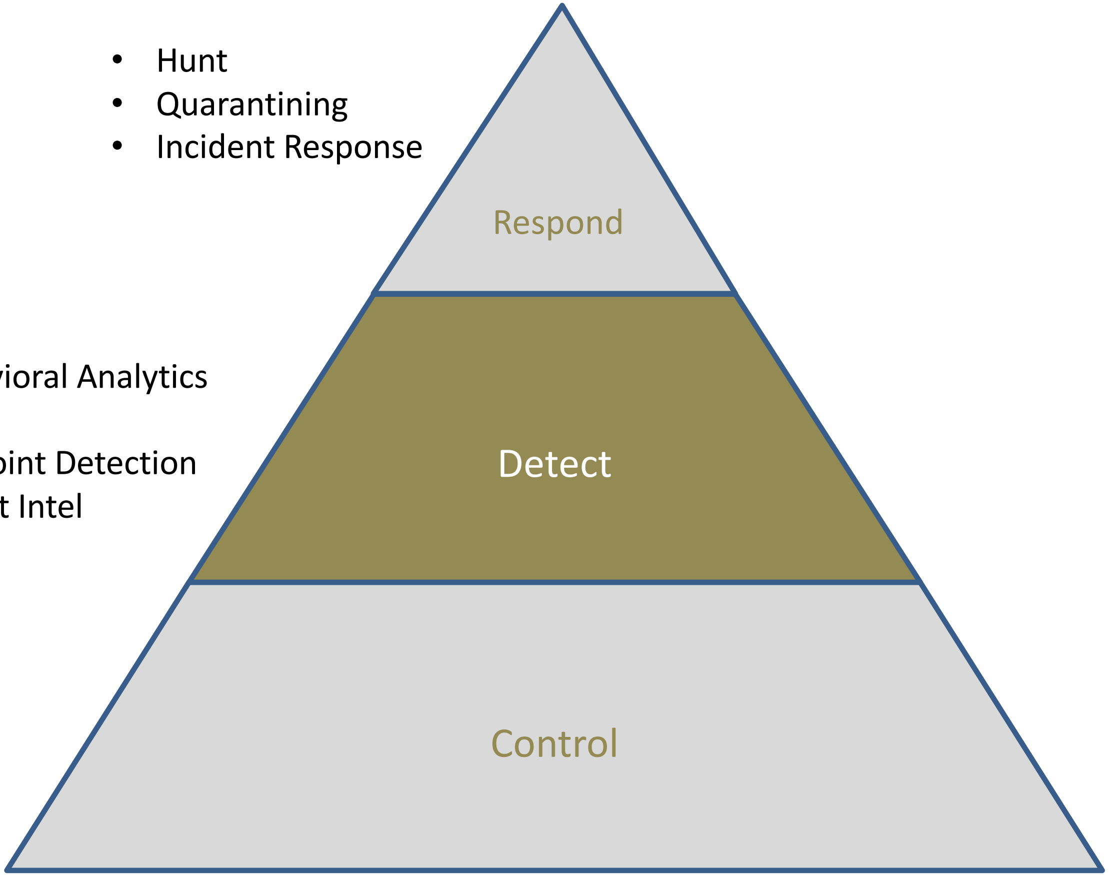


Detect



Response





- Hunt
- Quarantining
- Incident Response

Respond

- Behavioral Analytics
- IDS
- Endpoint Detection
- Threat Intel

Detect

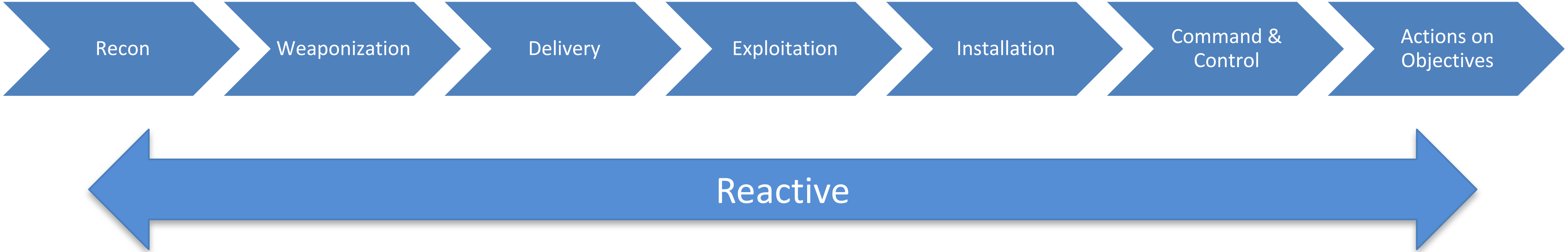
- Segmentation
- Patch Mgmt
- Identity/Access Mgmt
- Encryption

Control

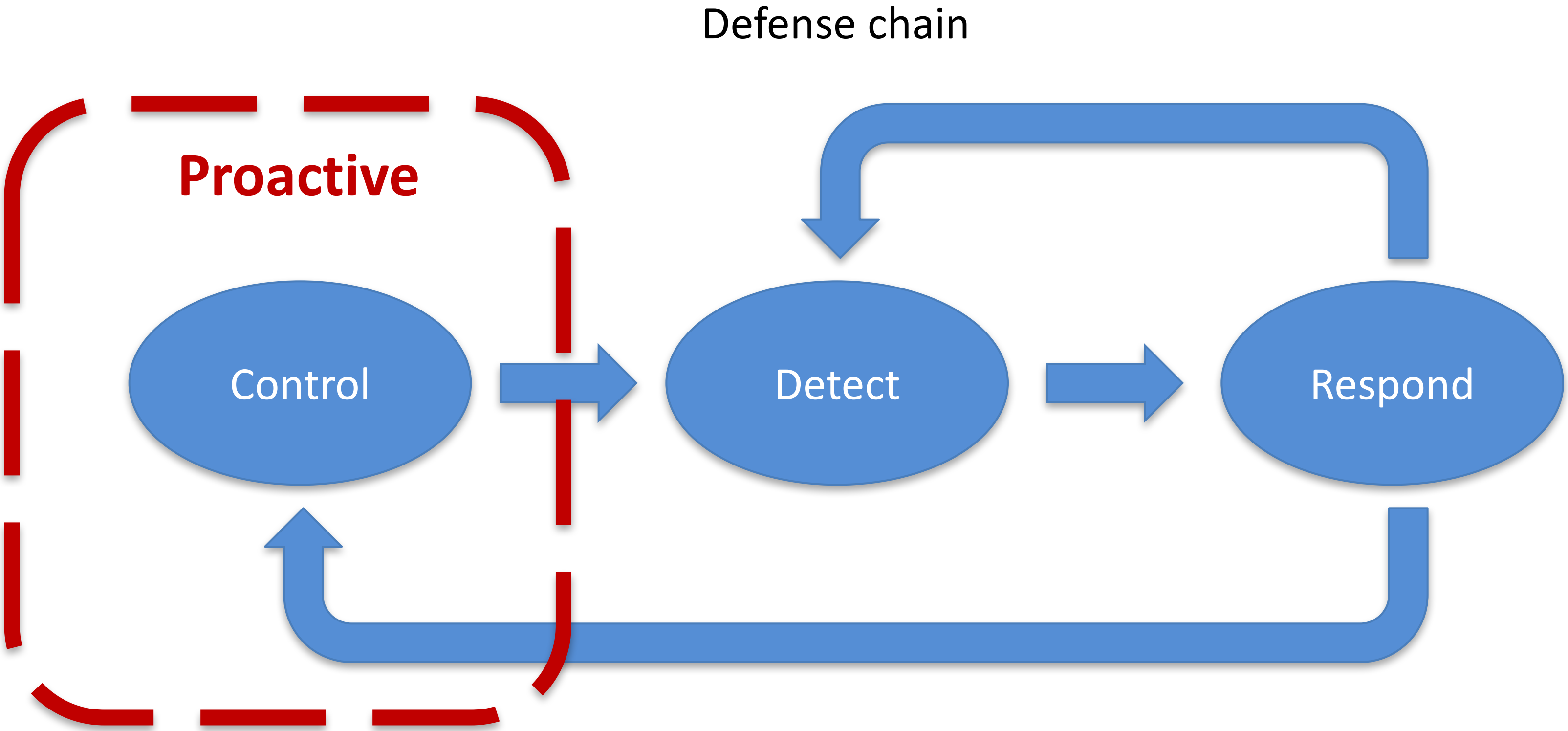
Proactive v. Reactive Security

Reactive security

Cyber Kill Chain



Proactive security



- Control is efficient
- Control helps prioritize
- Control speeds up detection and response
- Control focuses on proactive security

146

Dwell time (in days)

POLICE

Thank You

Nathaniel Gleicher

nathaniel.gleicher@illumio.com

🐦 @ngleicher