Incident Detection and Response with SIEM

Cameron Naghdi

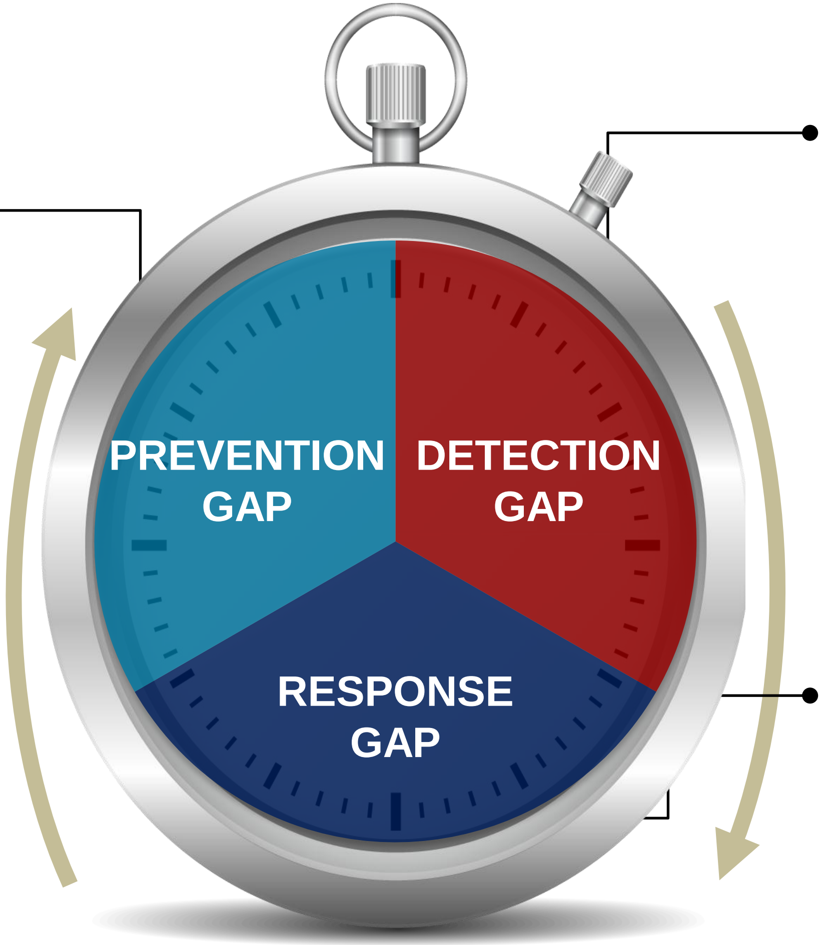
Systems Engineer

Challenge: Enterprise Cyberthreat Gap

Prevention Gap

Time to put preventative measures in place to avoid future attacks

Can we avoid this from happening again?



Detection Gap

Time between actual breach and discovery

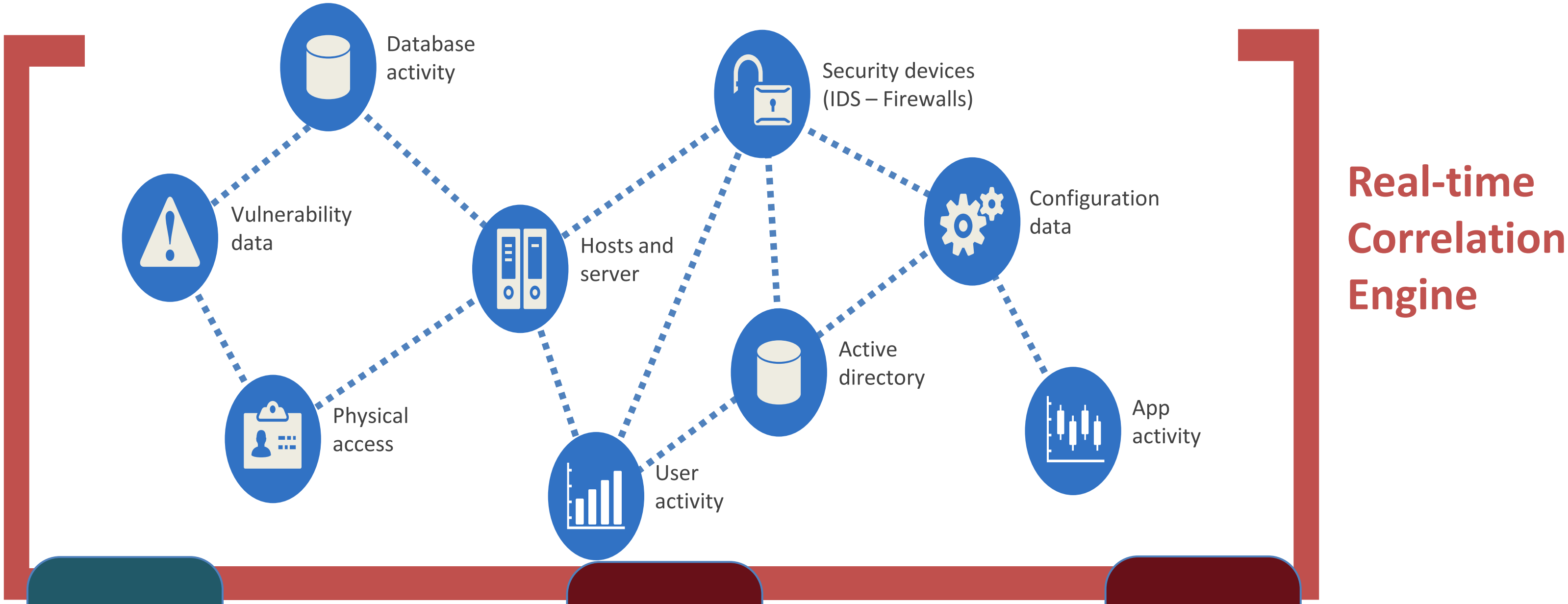
Have we been breached?

Response Gap

Time between discovery to remediation to limit damage

How bad is it?

Log Intelligence



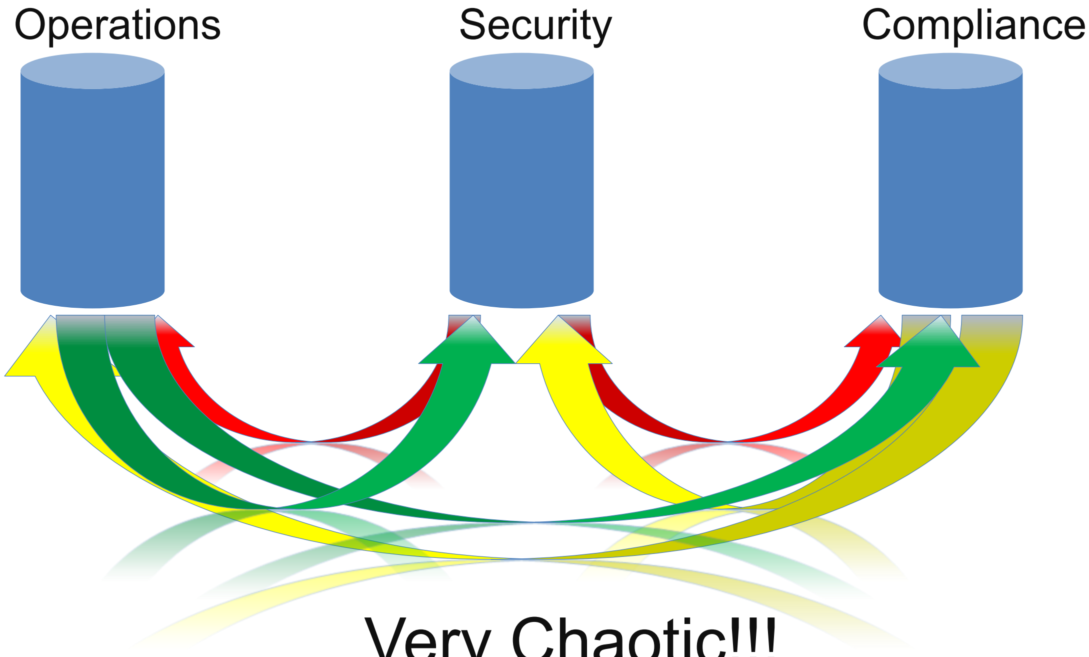
Real-time correlation of a SIEM with a powerful security analytics engine

Encrypted, resilient, and high- performance log collection and storage

Visualization & Analytics for forensics, reporting & incident response

I.N.T.E.L.L.I.G.E.N.C.E.

When an Incident Occurs…



Very Chaotic!!!

- This creates confusion today and increases time to response
- The enterprise loses visibility without business focused context
- The incident continues to affect critical systems and cost money

Many Compromising Problems Are Difficult To Discover

- Logging turned off
- FTP event to foreign IP
- New user added
- Login successful
- FTP enabled
- 10 failed logins
- DLL modified by new user

Just Detecting Change Is Not Enough… **Multiple Intelligence** sources Are Required

- ⚠ Logging turned off
- ⚠ New user added
- ⚠ FTP enabled
- ⚠ DLL modified by new user

Typical FIM **cannot** provide these types of alerts. **Change intelligence is required**.

Just Detecting Log Events Is Not Enough…

Multiple Intelligence Feeds Are Required

⚠ FTP event to foreign IP

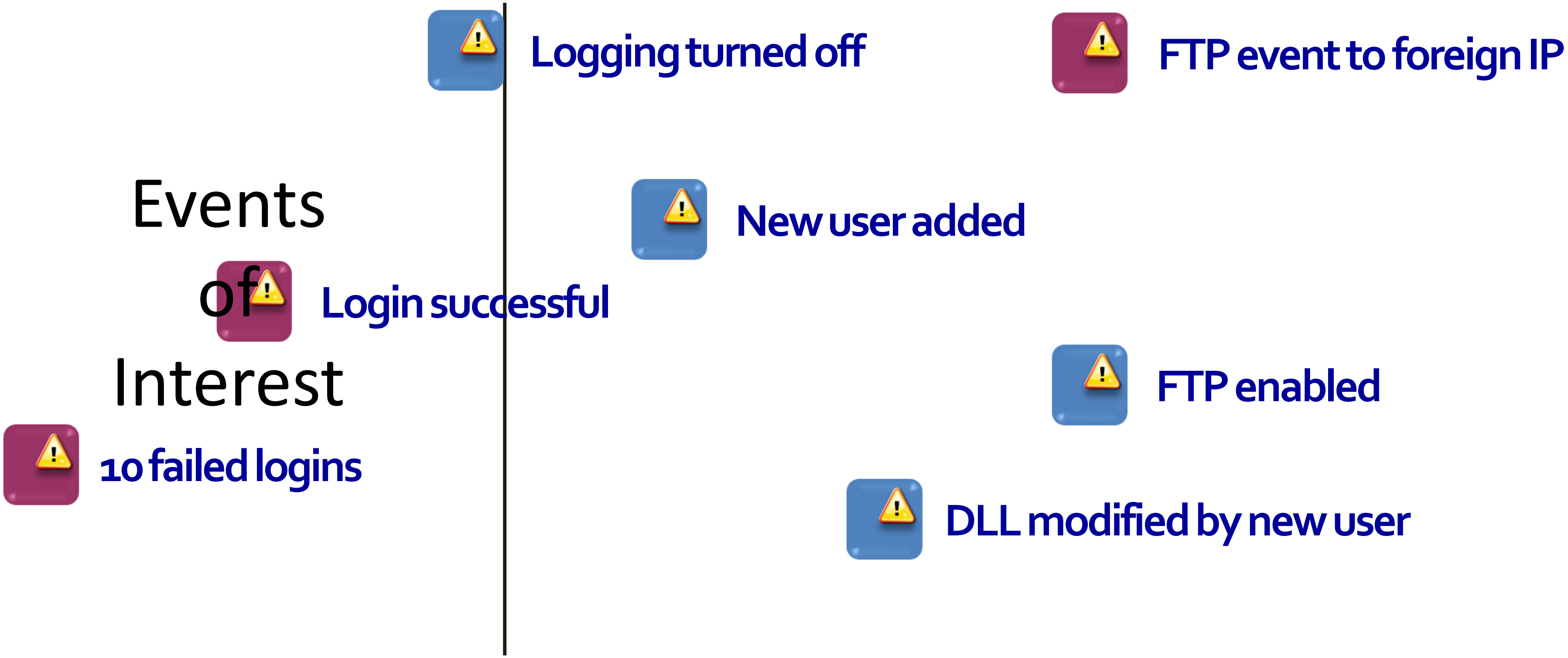
⚠ Login successful

⚠ 10 failed logins

Log management alone **cannot** alert on these events—**SIEM is required**.

Relating **Change Events** to **Log Events**…

Best Chance To Discover Compromises



Events of Interest

Logging turned off

FTP event to foreign IP

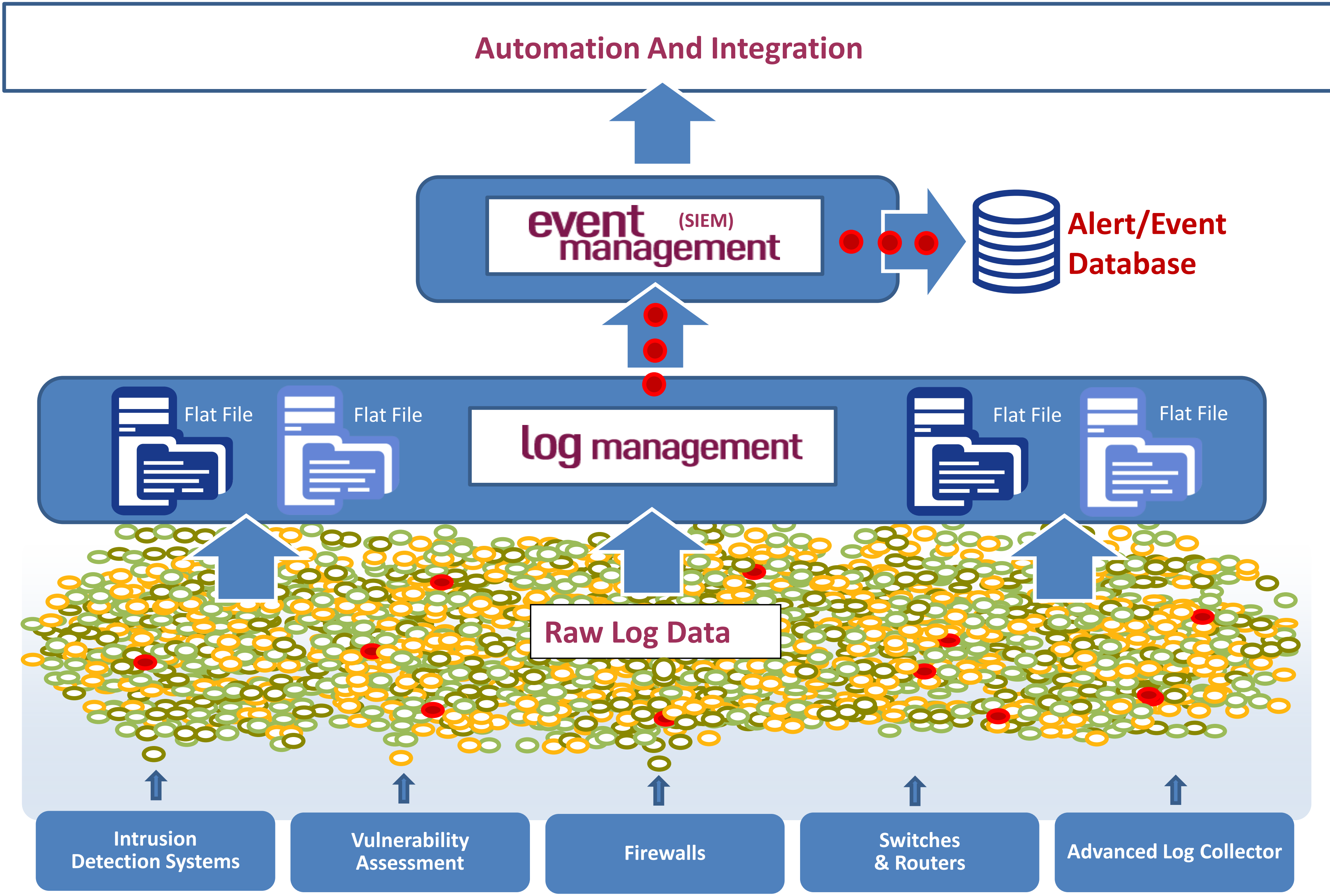
New user added

Login successful

FTP enabled

10 failed logins

DLL modified by new user



Automation And Integration

event management (SIEM)

Alert/Event Database

Flat File

Flat File

log management

Flat File

Flat File

Raw Log Data

Intrusion Detection Systems

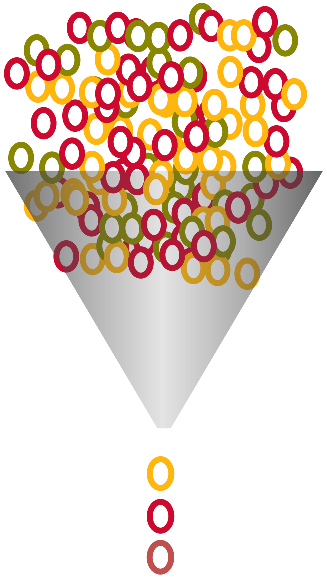
Vulnerability Assessment

Firewalls

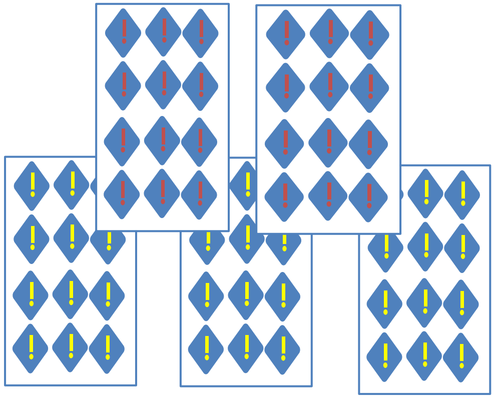
Switches & Routers

Advanced Log Collector

Security Controls Today

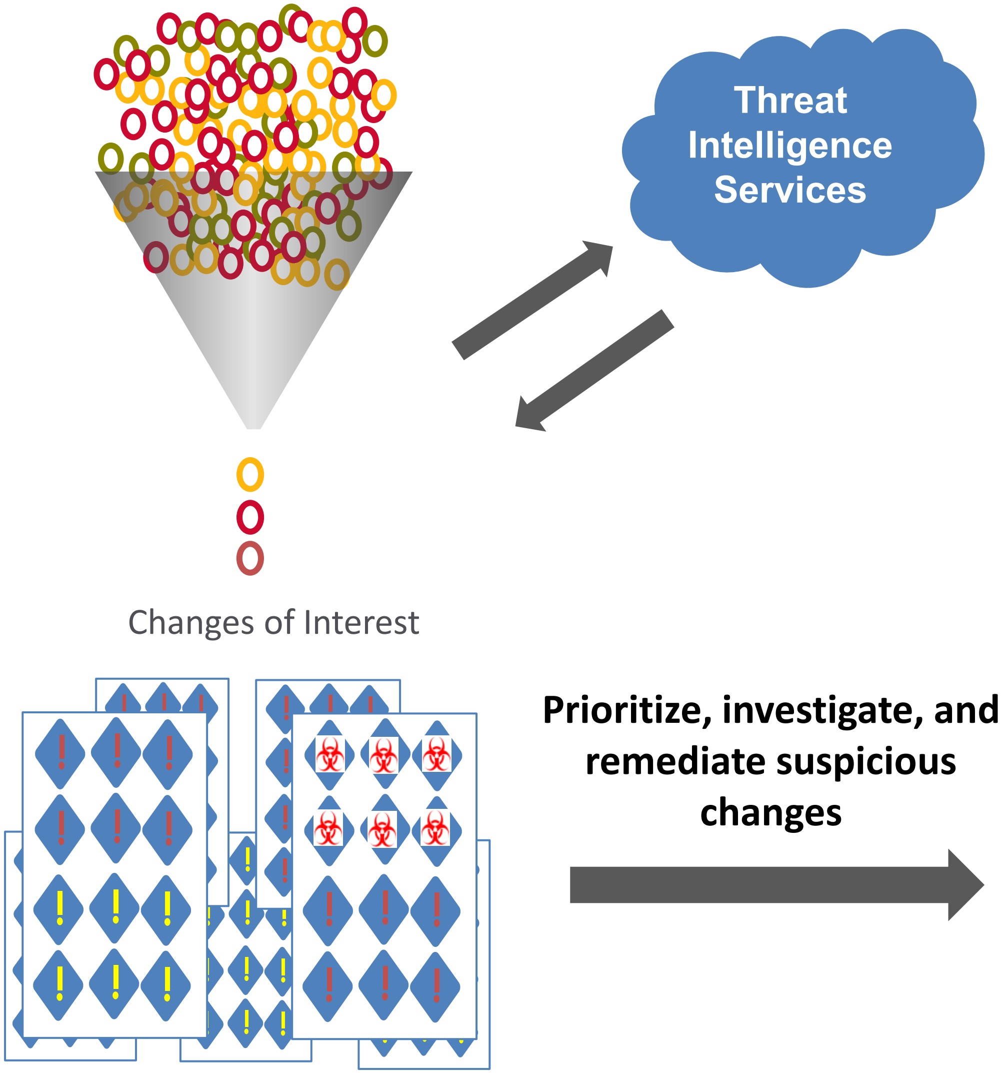


Changes of Interest



Prioritize, investigate, and remediate suspicious changes

Integrating Intelligence to Security Controls



Threat Intelligence Services

Changes of Interest

Prioritize, investigate, and remediate suspicious changes

- Identify indicators of compromise
- Detect & eliminate zero-day threats
- Shorten time to detection & remediation
- Protect against repeat threats

Q&A

THANK YOU