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

Detection Gap
Time between actual breach and discovery

Response Gap
Time between discovery to remediation to limit damage

Can we avoid this from happening again?

Have we been breached?

How bad is it?
Encrypted, resilient, and high-performance log collection and storage

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

Visualization & Analytics for forensics, reporting & incident response
When an Incident Occurs...

- 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

Very Chaotic!!!
Many Compromising Problems Are Difficult To Discover

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

10 failed logins
Intrusion Detection Systems
Vulnerability Assessment
Firewalls
Switches & Routers
Advanced Log Collector

Raw Log Data

Log Management

Event Management (SIEM)

Alert/Event Database

Automation And Integration
Security Controls Today

Prioritize, investigate, and remediate suspicious changes
Integrating Intelligence to Security Controls

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

Prioritize, investigate, and remediate suspicious changes