DECODING CYBERESPIONAGE FROM INSIDER MISTAKES
INTRODUCTIONS

KEN BELL
Deputy CISO, Forcepoint
AGENDA

- How is Insider Threat Different Than Cybersecurity
- How an Insider Threat Program Works
- Real World Examples
THE CYBER CONTINUUM OF INTENT

ACCIDENTAL INSIDER
Inadvertent Actors
Convenience Seekers

COMPROMISED INSIDER
Malware Victims
Impersonated Users

MALICIOUS INSIDER
Rogue Employees
Criminal Actor Employees
USER BEHAVIOR PERSONAS THAT POSE RISK TO AN ORGANIZATION

MALICIOUS INSIDER: 22%
ACCIDENTAL INSIDER: 68%
COMPROMISED INSIDER: 10%

Source: Ponemon 2016

Protecting the human point.
COST OF AN INSIDER BREACH

Average Cost Per Incident

Accidental Insider: $207
Malicious User: $347
Compromised Insider: $493

Average Annualised Cost

Accidental User: $0
Malicious User: $1,228
Compromised User: $776

Source Ponemon 2016
KEY ELEMENTS OF USER BEHAVIORAL ANALYSIS

Activity Monitoring

Intent

HUMAN BEHAVIOR

Statistical Baseline

Forensic Evidence
How an Insider Threat Program Works
KEY DIFFERENCES BETWEEN CYBER AND INSIDER

PEOPLE ARE NOT COMPUTERS

- People don’t follow strict patterns
- People have *emotions* (of course)

PEOPLE WORK IN HUMAN TIME

- People operate in **minutes, hours, days, weeks**
- Computers operate in **milliseconds (and less)**
REQUIREMENTS FOR BUILDING AN INSIDER THREAT PROGRAM

DETECT which individuals are interacting with information systems which pose the greatest potential risk

RAPIDLY and thoroughly understand that user’s potentially risky behavior and the context around it
INSIDER THREAT PROGRAM STAKEHOLDERS

- Security
- Legal/HR
- IT
- Other Stakeholders

Most malware investigations end with patching, reimaging or upgrades.

Human investigations typically end with: policy violations, employment terminations or legal proceedings/arrests.
A DAY IN THE LIFE

- Real insider threat is done with old investigative processes that are amplified by technology.
- Artificial intelligence and machine learning can help point you in a direction but can’t provide “detection -> conviction”.

**Human Intelligence Triage**
- HR
- Legal
- Employee Reporting

**POI Monitoring**
- Terminated Employees
- Suspected Malicious
- Sad / Angry / Stressed

**Tech Alert Triage**
- DLP Alerts
- Insider Threat Triggers
- Analytics Alerts

**Investigations**
The goal of human behavior analysis is to start with the assumption that your theory is wrong.

Establish alternative theories and attempt to prove them wrong.

If you are able to disprove the alternatives then the original theory is likely to be true.
BUSINESS OUTCOMES OF AN INSIDER THREAT PROGRAM

OUTCOMES
- Auditing
  - Compliance
  - Change Control
  - ...
- Insider Threat Protection
  - Data Exfiltration
  - Financial fraud
  - Malware compromise
  - Broken Business Process...

VISIBILITY
- Application
  - Instant Messaging
  - General
- Webmail
- Web URL
- Email
- File
- Printer
  - Clipboard
  - Keyboard
  - Logon
  - Video
- System Info
  - Process
  - Registry
  - Event Log
  - Network
- Fingerprint
  - Pattern Recognition
  - Inventory
  - Monitor

ANALYTICS
- Pattern recognition
- Outlier detection
- Semantic analysis
- ...

CONTROL
- Allow
- Block
- Monitor / Audit / log
- Quarantine
- Tag
- Encrypt
- Apply DRM
- Delete
- Notify
  - Send email
  - Send to SIEM
- Record Video
- Collect deeper forensics

DATA
- Fingerprint
- Pattern Recognition
- Inventory
- Monitor

MACHINE
- System Info
- Process
- Registry
- Event Log
- Network

USER
- Application
- Printer
- System Info
- Fingerprint
- Pattern recognition
- Outlier detection
- Semantic analysis
- ...

WEB
- Webmail
- Web URL
HOW TO GET STARTED

VISIBILITY

• Can you see the people?
• Can you see the data?

CONTROL

• Can you stop the bad?
• Can you free the good?

ANALYTICS

• Do you see the patterns?
• Can you predict the actions?
Real World Examples
THE CASE OF THE JEALOUS INTERN

• The investigation:
  • IT Security at military base sees PII flowing into its network
  • PII is coming from a nearby State University
  • NCIS and local authorities called in to investigate
The Investigation:

- User reports to help desk that they can not log in
- This inquiry reveals that the user is already logged in from an internal IP address
- Further investigation reveals that several user accounts were logged in a short amount of time from the same internal IP address
Forcepoint Insider Threat
PROTECTING THE HUMAN POINT.

KEN BELL
kbell@forcepoint.com
www.forcepoint.com