Catching malicious insiders through behavioral analytics

Jesse Hughes, Managing Principal
Agenda

Understanding bad guys

Recognizing what it takes to be a ‘good guy’
Heads up: This is going to get fluffy

How many times will this work?  

Thruway - Toll 10¢  
Exact change lane

Somebody’s gotta go back and get a ___load of dimes!

...maybe if we put a guard on it...
Scenario 1: the “new” employee

New employees may have old intentions

Person A
• Cleared government contractor working on-site
• Worked for multiple contractors
• US Citizen

Activities
• Expressed uneasiness with intelligence program
• Interviewed with separate company for position with increased access
• Stole hundreds (or more) classified documents
• Published some secrets, held the rest
Scenario 1: The “new” employee (cont’d)

Person B

• Research scientist
• Worked on proprietary programs for 2 U.S. chemical companies
• Foreign national (Permanent U.S. Resident)

Activities

• Stole research and proprietary information from first company
• Worked for a second company (a U.S. competitor of the first)
• Provided IP and research material to foreign government
Scenario 2: Recruited in place

If you don’t “social engineer” your people, someone else will

Person C

• Cleared government employee
• History of mental instability and performance issues

Activities

• Sought external advice on theft of documents; encouraged to do more
• Downloaded classified documents (in violation of protocols and policies)
• Leaked documents, ostensibly as a whistleblower
Scenario 2: Recruited in place (cont’d)

**Person D**
- Product developer for US company
- Access to sensitive programs
- US citizen

**Activities**
- Stole gift card codes for online purchases worth > $50,000
- Quit company
- Waited 2 years and then publicly released ~ $20,000 of gift card codes
- Claimed to be giving to the public (“Robin Hood” type)
“[Just because] you are ‘bad guy,’ doesn’t mean that you are ‘BAD’ guy.”

- Zangief

*Wreck It Ralph*
Who are the “bad guys?” They range from impulsive to professional

Different attackers have different characteristics; all may involve insiders

**Economic espionage (G2B)**
- Extensive training
- Long time horizon
- Unlimited resources
- Research, technology, IP, and trade secret focused

**Industrial espionage (B2B)**
- Limited training, if any
- Medium time horizon
- Sufficient resources for dedicated efforts
- Market motivations

**Criminal**
- Limited training, but experienced
- Medium time horizon
- Economies of effort across targets
- Financial motivation

**Lone wolf**
- No formal training
- Short time horizon
- Limited resources
- Wide range of motivation
Bad guys use a tried and true method: Attack life cycle

Works on ALL systems (including humans)

- Several published frameworks that cover basically the same thing
- This methodology was first implemented on the attacker side, before there was an internet
- It was used to stop hearts. Literally
Insiders may simply be someone else’s tool

Think of them like ones you’ve seen on police dramas

**Dupe / stooge**
- Unwitting
- Unwilling

**Source**
- Witting
- Unwilling

**Asset**
- Witting
- Willing
Good guys (?)
The most powerful correlation engine in the world is between human ears – enable people, remove obstacles

People

• Most valuable resource – provide them opportunities

• Enable them:
  • Training
  • Rotational Assignments
  • Avoid burnout

Empower them

• Take a chance on them
• Listen and action their suggestions
• Create an inclusive culture
Your defenses must map to attackers’ methodology

Use technology to empower people

1. Know what you have (people, processes, technology, infrastructure).

2. Know what you need to protect (what is of value).

3. Identify attack vectors

4. ID Indicators

5. Enable tools

6. Find analytic gaps
Cyberspace is only ONE component of insider detection

Most organizations separate technical and non-technical monitoring – this needs to be corrected

• Non-technical monitoring and response: a physical security function
• Technical monitoring done through SOC-like function
• Day to day operational priorities and sensitivity of information separate these functions causing a critical breakdown

Behavioral Analytics enable companies to discover anomalous behavior in a sea of data
Integrate technical and human indicators

**Human Indicators (e.g.):**
- Poor performance reviews
- Security violations
- Not accepting feedback
- Anger issues/disgruntled
- Financial issues

**Technical observables (e.g.):**
- Anomalous printing activity
- Erratic working hours
- Anomalous network behavior
- Network service usage
- Privileged access (role)
Behavioral-based threat monitoring

Approach
• Moves focus from objects on network to the user
• Adapts instantly to new critical objects introduced to network and requires no signature updates
• Requires 4-6 weeks of data to have a strong enough baseline

Needs to adapt and scale
• Individual behavior varies; broad based rules don’t all apply to each person
• Different organizations have different missions, therefore different risk factors and vulnerabilities
Baselines: All entities all observable

User oriented examples:
- Order and preference for use of applications
- Average number of daily interactions with objects on a network
- Average remote session length, concurrence of session
- Any activity during “off” or non-standard business hours
- Rate of password check out for secure file share access
- Account monitoring for new users plus those who have given notice

Machine oriented examples:
- Processes per server role (white list and black list); host, role, process name, user name, etc.
- Anomaly detection by server role
- Non-human services reaching in for access or keys
- Frequency of connections to other machines, time of day
- File changes (if user data is included in those logs)
Detecting anomalous behavior across a range of data

Alerting priority levels

$\sigma_1$, $\sigma_2$, $\sigma_3$
There is no easy, drop-in, out-of-the-box, fire-and-forget solution: You have to earn it

<table>
<thead>
<tr>
<th>Infrastructure</th>
<th>People</th>
<th>Process</th>
<th>Technology</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Make it scalable</td>
<td>• Hire for attitude and aptitude</td>
<td>• Establish early</td>
<td>• Don’t scrimp</td>
</tr>
<tr>
<td>• Anticipate growth</td>
<td>• Train for capability</td>
<td>• Stay flexible</td>
<td>• Enable your team</td>
</tr>
<tr>
<td>• Don’t scrimp</td>
<td>• Enable for cross-functional work</td>
<td>• Include non-traditional partners</td>
<td>• Push the limits and</td>
</tr>
<tr>
<td></td>
<td>• Empower to take risks</td>
<td>• Over communicate</td>
<td>demand more</td>
</tr>
<tr>
<td>• Deliberate data collection</td>
<td>• Recognize, reward, and promote</td>
<td>• Reach out beyond the org chart</td>
<td>• Be aggressive</td>
</tr>
</tbody>
</table>
Pop quiz

1. Describe the numbers in the upper right of the presentation. (What were the numbers? What order? Discernible sets? Any pattern?)

2. Name of the person to your left

3. Self-assessment:
   - Did you notice the numbers?
   - Did you get the name initially?
   - When did you identify the discrepancy in your own collection?
   - What actions did you take to correct it?
   - What assumptions did you make? Did you assume the numbers were an error? Was the neighbor’s name insignificant?
   - Did you discuss with anyone or just keep it to yourself?
Special thanks / worth mentioning

- Bruce Schneier does an excellent monthly blog: cryptogram.com – covers recent events from a balanced, holistic security perspective
- Mike Keleher w/ Comprehensive Solutions Group has a powerfully simple framework for entity analysis and for asking the right questions
- Rich Baich’s book “Winning as a CISO” provides a perspective on internal cultural awareness and creating momentum for information security
- Other books of interest (though not specifically about cyber security)
  - “Seven Pillars of Wisdom” by T. E. Lawrence
  - “Competitive Strategy” by Michael Porter
  - “From OSS to Green Berets” by Aaron Bank
For more information

Attend these sessions

• TT2977: Why you should care about insider threats (Pertinent)

• TB3111: Flight of the flightless bumblebee: Use cases created because no one said we couldn't (Perspective)

• TB3135: Using baselining to detect anomalies in HP ArcSight ESM (Technical)

Your feedback is important to us.
Please take a few minutes to complete the session survey.
Please give me your feedback

**Session** TB3262  **Speakers** Jesse Hughes and Tammy Torbert

Please fill out a survey.

Hand it to the door monitor on your way out.

Thank you for providing your feedback, which helps us enhance content for future events.
Thank you

Jesse Hughes

720.369.3986

Jesse.Hughes@hp.com