Insider Threats: Detection and Prevention

Tim Medin, IANS Faculty

Contributor: Mike Saurbaugh, IANS Faculty

Agenda

- Session overview
- Defining the challenge
- Early warning indicators
- Security controls to put in place to detect and prevent insider threats
- Insider threat monitoring solutions to consider
- Detection tool essentials
- 10 steps to success

Why Is This a Problem?

- Errors, mistakes – really just trying to do their job
- This is *MINE,* and I'm taking it with me*!*
- Two can play at this game
- Intentional harm
- Violence in the workplace
- Critical assets may or may not all be accounted for
- Rules may not apply to all
- A lot of small leaks of information
- Employees are *stressed* and watching other companies with unrest and social challenges

IANS

What Gets Monitored?

- Personally identifiable information (PII)
- Database activity
- Intellectual property (IP), source code
- Device activity
- Network communications (email, chat, file shares)
- Local storage
- Remote logins, including off-hours
- Unauthorized changes to code and network
- Learn from past incidents (can you detect where others failed?)

IANS

Who Is Monitored and Who Decides?

- Business units – good networking and relationships are important
- Conscious about employee privacy
- Legal and HR may be involved
- Third parties require monitoring
- Contractors
- There should be a committee working with information security (legal, HR, corporate security)
- Privacy laws come into play

Key Data Questions

- What value does the data have?
  - Will vary by business unit
- Who can access the data?
- Where is the data?
- Who is protecting the data?
- How well is the data protected and will you know if it is misused?

Limiting Exposure

- Start by evaluating the hiring process (background checks, interview behavior)
- Enforce least privilege and remove admin rights wherever possible
- Ensure recertification of privileged accounts
- Apply network segmentation
- Implement a strong data destruction and system decommissioning process

Early Warning Indicators

Be on the lookout

Suspicious Activity

- Volumetric network traffic (src/dst)
- Peripherals
- Failed logins
- Unauthorized devices
- Unauthorized changes

IANS

When Times Are Tough

- During company layoffs
- Change in leadership
- Weakening culture
- Social issues
- Record negative comments by personnel

Security Controls to Put in Place

Detect and prevent threats

Human Resources

- Partner with HR
  - Employees on probation
  - Financial difficulties
  - Other life issues that may lead to irrational decisions
  - Part of enterprise resource planning (ERP) system
- Mandatory vacations
- Two-person (dual-control) rule
- Oversight group to watch those with access

Additional Components to Include

- Clear and concise policies
  - Enforced and validated through technical controls
- Training and education
- Strong change management
- Strong password management and recovery process

Employee Awareness and Training

- Train employees about data protection and privacy from the beginning of employment
- This includes contractors and those in third-party agreements
- Include social media
- Communicate “examples” of what to do and not to do as an employee
  - It helps for people to understand what is and is not acceptable
  - Few want to risk repercussions

Balancing Privacy and Monitoring

- Be transparent about what is being monitored
  - Monitoring software to avoid associating personal versus work-related data (depending on locations and privacy law)
- Masking identities may be required based on European laws
  - Data minimization to mask identity into systems and data sources

Insider Threat Monitoring Solutions

Solutions to evaluate

Fundamentals to Get Started

- Skilled people
  - Analysts with the ability (and time) to investigate
- Determining what is monitored
- Process with analysis
  - Outline the process and business unit flow
- Tools will require good visibility for analysis
  - SSL inspection is one area that provides good insight (privacy considerations)

IANS

Quick-Hitters

- Email monitoring
  - File size, encryption (or lack thereof), file type
- Network traffic
  - Cloud storage, among others
- Administrative rights
- Data based on compliance
  - Payment Card Industry (PCI)
  - Health Information Portability and Accountability Act (HIPAA)
  - Others

Reporting Phishing

- There's a lot of value in having users report suspected phish
- Allows you to learn "who else" received the phish or may have received it
- End result is the ability to respond, triage and remediate more quickly

Detection Tool Essentials

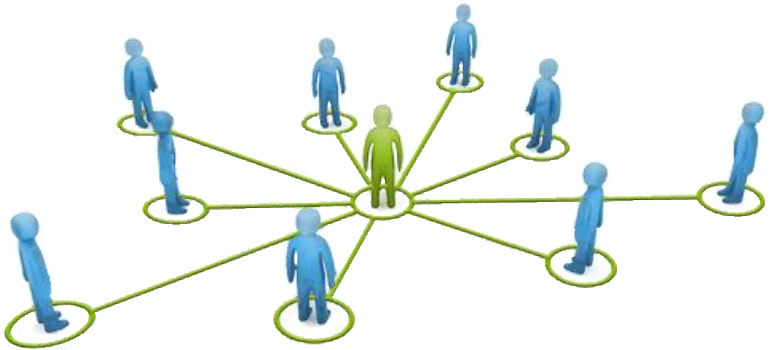
Tools to Consider

- User and entity behavior analytics (UEBA)
- Security information and event management (SIEM)
- Endpoint detection and response (EDR)
- Data loss prevention (DLP)
- Cloud access security broker (CASB)
- Breach and attack simulation (identify changes)
- Identity and access management (IAM)
- Deception technologies

IANS

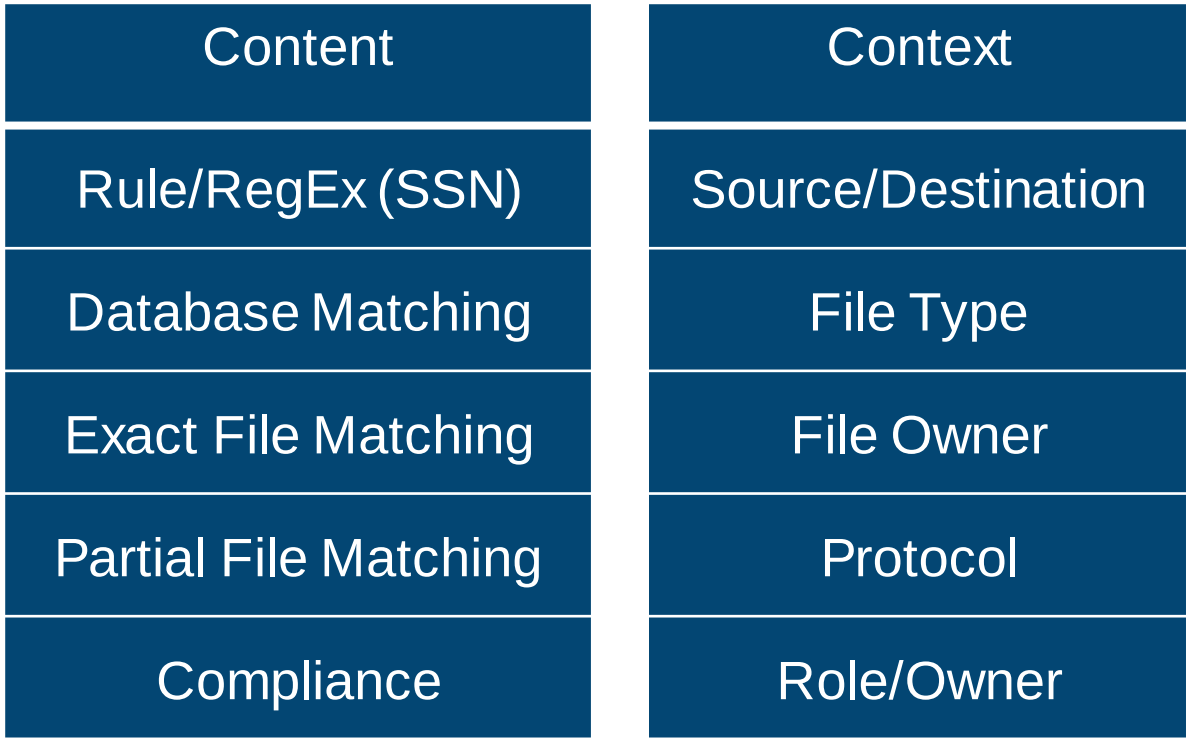
Tools and Resources to Consider

- Exabeam
- Securonix
- ObserveIT
- AttackIQ
- Verodin
- SafeBreach
- Splunk
- DLP vendors (Forcepoint, Symantec, Digital Guardian)
- CrowdStrike, Carbon Black, SentinelOne
- National Insider Threat Task Force (NITTF)
- CERT Insider Threat Center (sei.cmu.edu)



DLP Examples

- File size
- Frequency of access
- Outbound connections (SSH, for example)
- Encrypted files
- Source/destination



10 Steps to Success

1. Know your data and assets
2. Protect
3. Ensure documentation and policy transparency
4. Work with HR (hiring and termination)
5. Focus on employee training (e.g., phishing, passwords)
6. Leverage technology (e.g., SIEM, UEBA)
7. Baseline normal vs. abnormal
8. Enforce least privilege
9. Implement change management
10. Have a disaster recovery/business continuity plan (DR/BCP) in place to recover

IANS

Thank you!

ask@iansresearch.com