SEAS-8414

Analytical Tools for Cyber Analytics

Survey of analytical tools for analyzing cyber security data with particular attention to the use of data analytics procedures in supporting appropriate cyber security policy decisions.

Dr. M

Welcome to SEAS Online at George Washington University

SEAS-8414 class will begin shortly

- **Audio:** To eliminate background noise, please be sure your audio is muted. To speak, please click the hand icon at the bottom of your screen (**Raise Hand**). When instructor calls on you, click microphone icon to unmute. When you've finished speaking, ***be sure to mute yourself again***.
- **Chat:** Please type your questions in Chat.
- **Recordings:** As part of the educational support for students, we provide downloadable recordings of each class session to be used exclusively by registered students in that particular class for their own private use. Releasing these recordings is strictly prohibited.

Agenda

Week-8: User security analyticstools

This lecture will shift the focus from digital assets to human beings. We will understand the role of motivation, indicators of compromise (IOC), and person of interest (POI) from the gwuscc.com user and employee perspective. We will cover the following tools:

- Identity and Access Management (**IAM**)
- User and Entity Behavior Analytics (**UEBA**)
- Insider Threat Detection Platform (**InTP**)

To understand the operation of tools, we will learn about conditional probability and the Bayes theorem.

What do these names have in common?

Jason Needham, Charles Eccleston, Kevin Patrick Mallory, Kun Chun, Jiaqiang Xu, Gregory Justice, Robert Mo, Walter Liew, Wen Chyu Liu, and Yuan Li.

What do these names have in common?

https://securityawareness.usalearning.gov/cdse/case-studies/cases.html

How to detect a malicious domain?

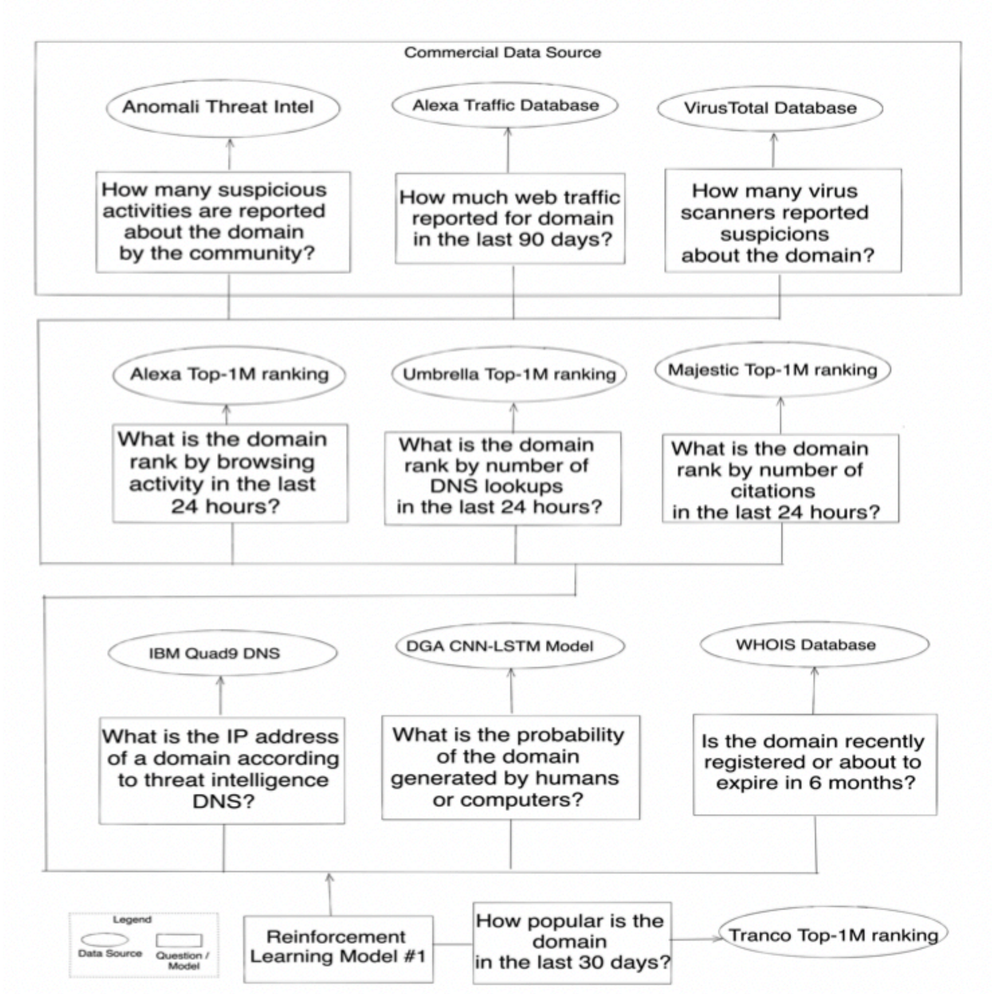
Practical - 1

https://cnn.com

Three Techniques

1. Domain Intelligence
2. Content Intelligence
3. Human Intelligence

1. Domain Intelligence



Threat Intel Websites

- https://www.virustotal.com/
- https://zulu.zscaler.com/
- https://www.talosintelligence.com/

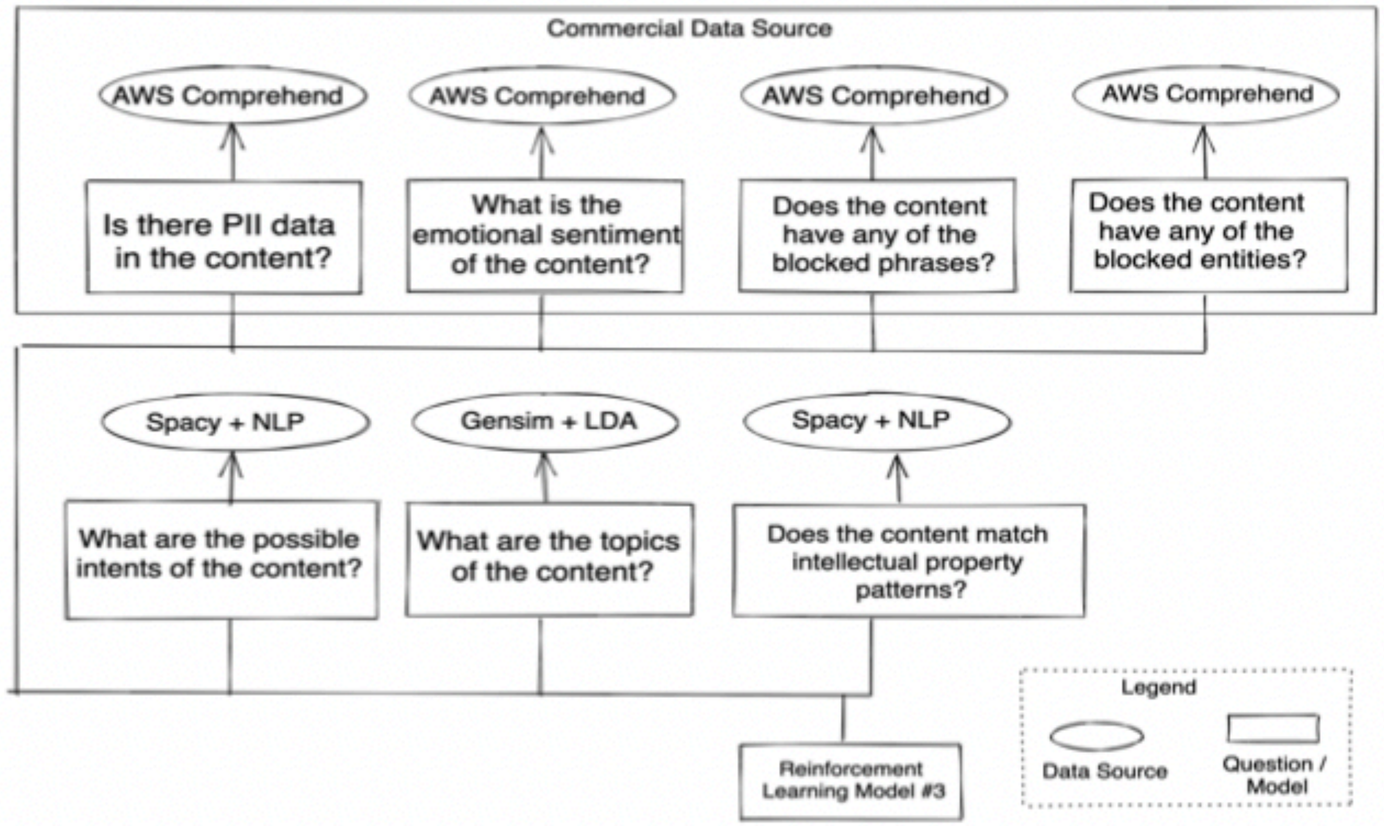
Can DNS solutions protect corporate assets offsite?

- Typo squatting domains
- Phishing domains
- Disposable domains
- Command and control (C2) domains
- Fast-flux domains
- Newly registered domains

2. Content Intelligence

- How do you differentiate a malicious vs. benign user?

Content Intelligence



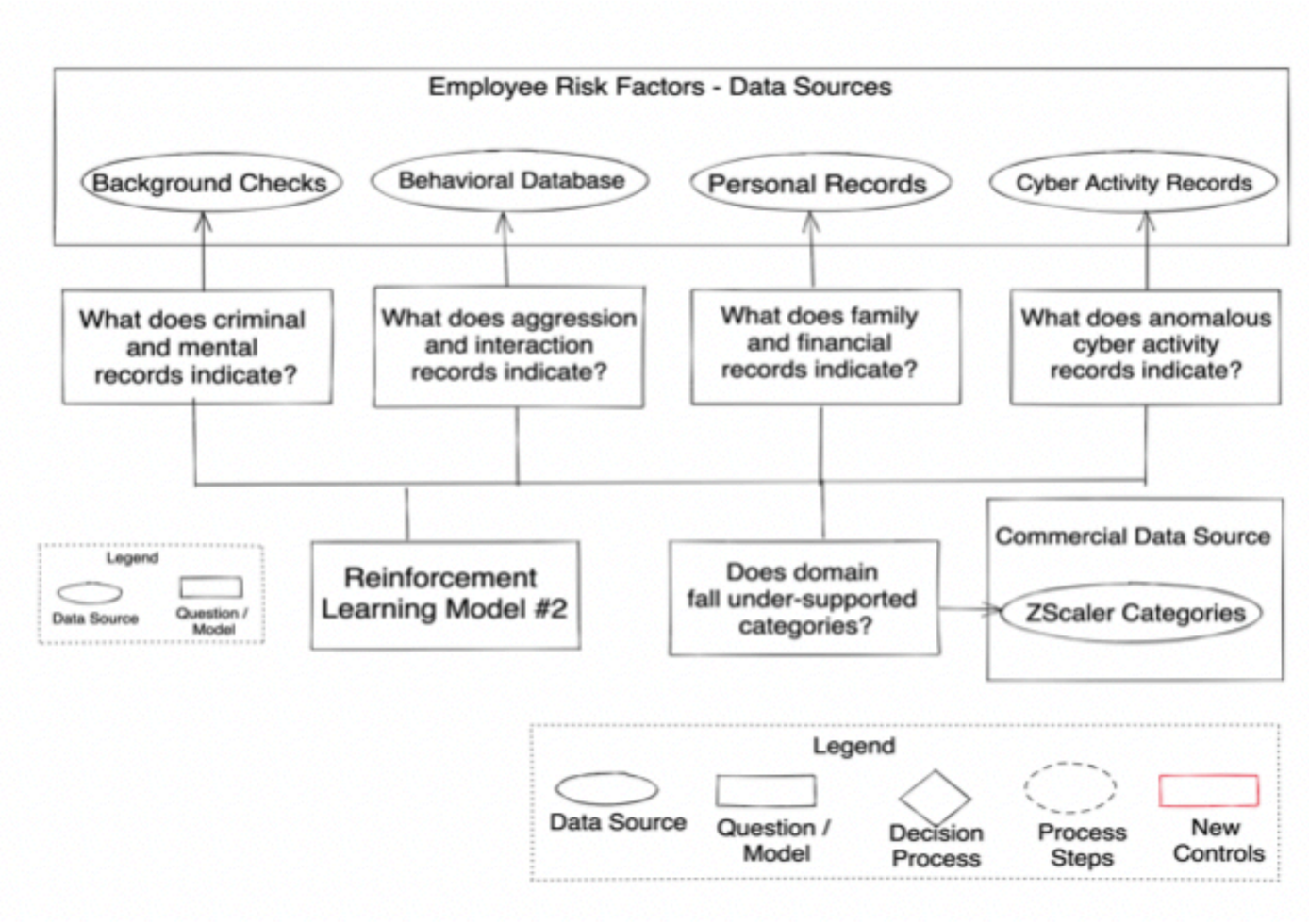
Can DLP solutions protect corporate assets offsite?

- Resource intensive to detect data leaks in motion
- Expensive to define access and classification (AIP is NOT DLP)
- DCA techniques are easy to fool
- Small and slow leaks are difficult to detect
- The myth of anomaly detection and machine learning techniques
- DLP is not compatible with revisions to graphics, printers, and kernel patches

3. Human Intelligence

- How do you differentiate a malicious vs. benign user?

Human Intelligence



Insider Threat

What is an insider threat platform?

An employee with authorized access exposing restricted company materials to an unauthorized outsider is called an insider threat. A program focused on deterring, detecting, and mitigating insider actions is called an insider threat platform (ITP).

Are all insiders the same?

Profile	IT Sabotage	Insider Theft of IP	Insider Fraud	Espionage
Who	Technical employees (e.g., System or Network Administrators, Developers, Programmers)	Most often Scientists, Engineers, Programmers, Sales personnel	Lower level employees (e.g., positions at help-desk, customer service, data entry)	Both technical and non-technical employees
	Employees with privileged access		Low/mid-level management	
When	Set up while employed	Usually within the period of 60 days before or after leaving the organisation	Happens over a long period of time	Happens over a long period of time
	Execute after termination			After the initial incident, a long period may pass before a following event
Motivation	Revenge	Start their own business	Financial need or greed	Financial need or greed
		New job position		Dissatisfaction with status
		Foreign government or organisation		
How	Access, ability, and motivation	Data exfiltration: E-mail, USB drives, physical documents, etc.	Corruption of organisational procedures	Methods span all profiles
			Inadequate auditing of critical and irregular processes	
What	Affects systems they worked on	Steal information they worked on	Personally identifiable information (PII)	Theft of information
			In some cases, fraud happens over a longer period of time and has great monetary impact.	Destruction of information to cover their tracks

Typical Insider Threat Implementation

1. Check the background of employees periodically
2. Make employees sign intellectual property agreement
3. Train employees regularly on security awareness
4. Monitor technical and behavioral actions
5. Increase monitoring of upcoming departures
6. Reconfirm employee agreement on departure
7. Process employee termination through identity and access management
8. Monitor suspicious actions of terminated accounts.

What is the problem with typical insider threat implementation?

Typical implementation has three thematic implementation-level issues that fail to catch the insiders.

1. **Lack of understanding about insider threat programs**: Many corporations misinterpret the bandwagon of User Entity and Behavior Analytics (UEBA), and compliance products with a stream of anomaly detection, language correlation, or cyber activity monitoring functionality as insider threat platforms (ITP).

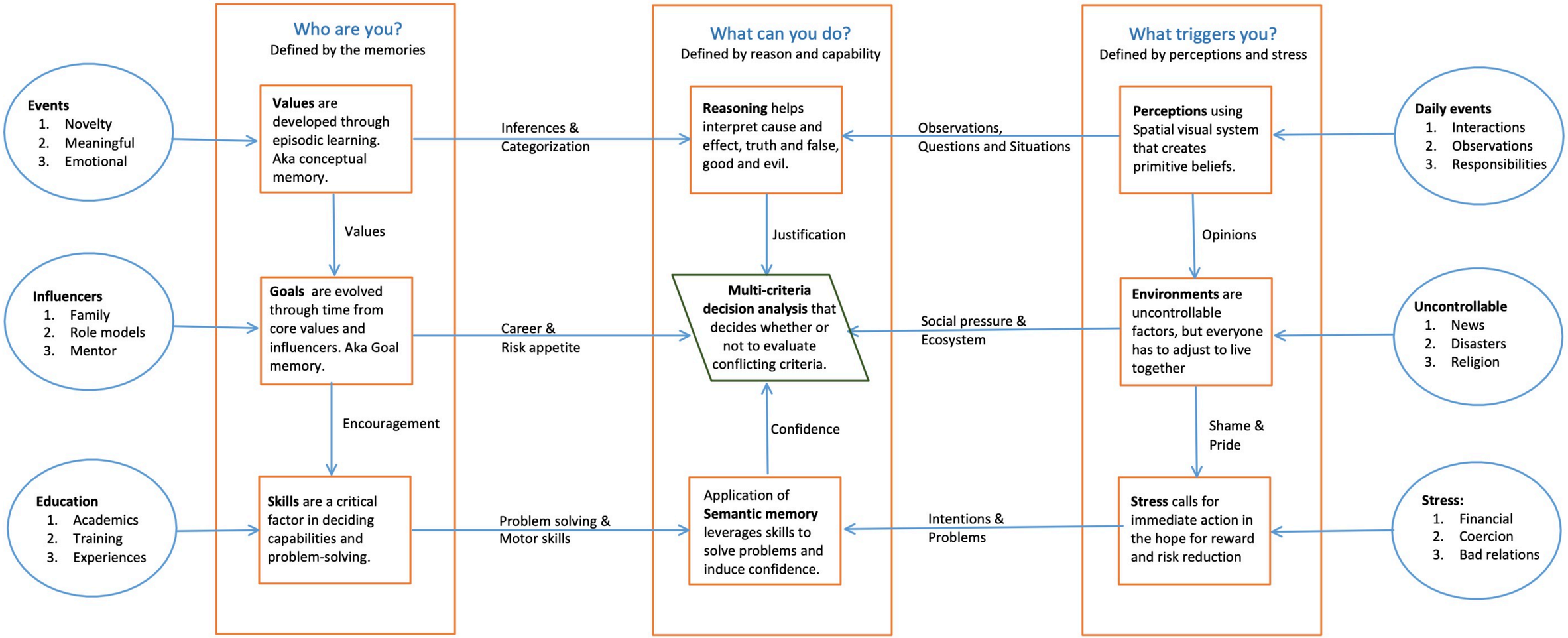
What is the problem with typical insider threat implementation?

2. **Lack of expertise**: Many operators of an ITP do not understand how to associate background checks, personal indicators, and behavioral indicators with historical cyber activity and potential fraud, espionage, sabotage, and unintentional disclosure.

What is the problem with typical insider threat implementation?

3. **Missing to learn from others**: Here is the summary of lessons (source: cdse.edu)
   - Lesson #1: Don't assume that serious insider problems are NIMO (Not In My Organization)
   - Lesson #2: Don't assume that background checks will solve the insider problem
   - Lesson #3: Don't assume that red flags will be read properly
   - Lesson #4: Don't assume that insider conspiracies are impossible
   - Lesson #5: Don't rely on single protection measures
   - Lesson #6: Don't assume that organizational culture and employee disgruntlement don't matter
   - Lesson #7: Don't forget that insiders may know about security measures and how to work around them
   - Lesson #8: Don't assume that security rules are followed
   - Lesson #9: Don't assume that only consciously malicious insider actions matter
   - Lesson #10: Don't focus only on prevention and miss opportunities for mitigation

Cognitive Neuroscience Architecture



Values

The values of a human being are developed based on episodic learning from our experiences of significant events in our lives. These core values are stored in conceptual memory. The conceptual memory molds an individual's character, which is reflected in core values. It is not possible for an employer to learn about an employee's core values just through an interview. The proposal suggests leveraging the following *background indicators*[6], which provide data sampling with reasonable variation and range to infer an employee's values.

- ○Compulsion
- ○Criminal records
- ○Indebtedness
- ○Sexual behavior
- ○Lack of judgment
- ○Conflict of interest activities Business dealing
- ○Remarks on social media
- ○Employment history
- ○History of emotional disorder Tax records assessment

Goals

Family members, bosses, co-workers, and role- models play a role in forming our life goals. The following *behavioral indicators* observed daily at work are an excellent source to learn about someone's intentions.

- Repeated transgression of procedures Regular rule breaker
- Poor social interaction
- Excessive volunteering
- Nonchalance
- Inappropriate jokes and bragging
- Impulsiveness
- Belligerence

Skills

Education, training, and job experiences are the primary source of expertise. They are part of the skills memory in cognitive theory and play a critical role in deciding capabilities and problem-solving. Resumes and regular *performance review indicators* by managers, peers, subordinates, and customers are the best sources of skills information.

Reasoning

Two individuals could come up with the same answer, but their rationality could differ. *Abductive reasoning* is the best source of data, which could be simplified for consumption *using automated reasoning tools*. From an ITP perspective, automated reasoning is also a source of prior for Bayesian statistics to derive weighted values in multi-criteria decision analysis.

Perceptions

Interactions, observations, and social connections are the source of developing opinions. Contacts from emails, phone calls, voluntary disclosure of family connections, political contributions, correlation of addresses, and phone numbers are the best sources of information to perform *link analysis*. The idea is to use the association to find the number of hops between the employee and the known conflict of interest. Perceptions also need *social interaction analysis* - please see Environment for more details.

Environment

It consists of uncontrollable aspects of life. Email, text, chat, social media, and blog posts are the best sources of investigative components for *social interaction analysis* to understand how an environment impacts an employee's reaction.

Stress

Compared to all the trigger points, stress is critical. When stress levels are high, the rest of the equations derived from other components hold low to no value in multi-criteria decision analysis. The following *stress indicators* are an excellent source to monitor.

Financial obligations
Moving to a new location
Loss of a family member or friend Depression
Feelings of inferiority
Break-up or divorce
Pandemic

Semantic activity

It may not be a familiar term for many non-cognitive scientists. The semantic activity is responsible for leveraging the skills developed through education and experiences to do the work, stored in semantic memory, to solve problems, and to induce confidence. In a professional organization, *UEBA* can observe most of the activities performed through semantic memory.

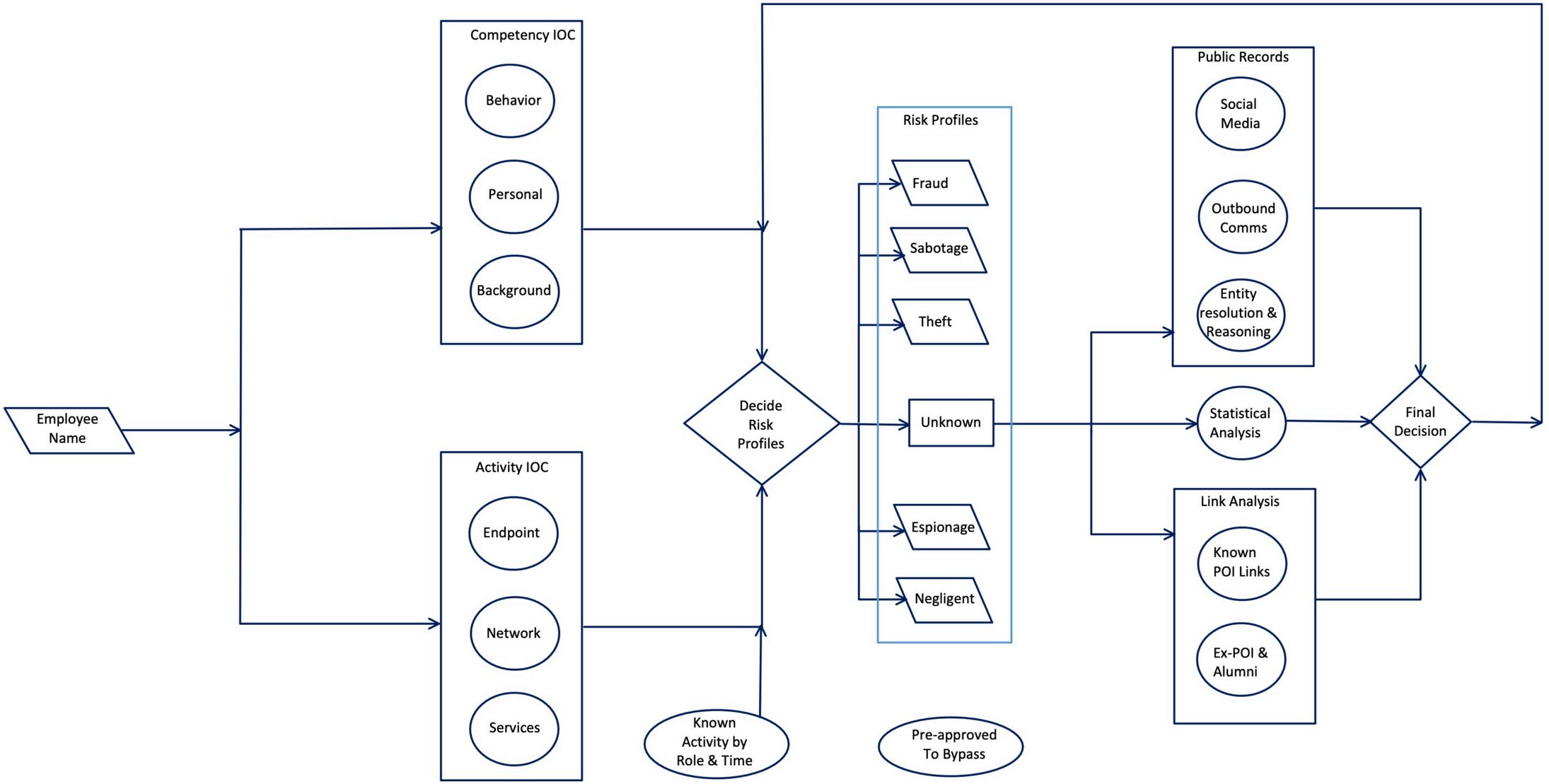
Multi-criteria decision analysis (MCDA)

The decision-maker part of our cognitive system. The input from every component goes through the Bayesian statistic, is weighted, and then MCDA is applied. *Picture of a Person* (PoP), representing all the attributes and their cause-and-effect relationship, is the best way to understand this component.

Scientific Connections

Area of Concentration	Proposed Solution
Values	Background indicators
Reasoning	Automated reasoning
Perceptions	Link analysis
Goals	Behavioral indicators
Multi-criteria decision	Picture of a person
Environments	Social interaction analysis
Skills	Performance review analysis
Semantic activity	UEBA, Compliance tools
Stress	Stress indicators

Practical Insider Threat Detection



What are personal indicators?

Indicator	Sabotage	Theft	Fraud	Espionage	Unintentional
Depression	High	Low	Low	Medium	High
Financial obligations	Low	High	High	Medium	Low
Address change (moving)	Low	High	High	Medium	Medium
Death among family or friends	Medium	Medium	Low	Medium	High
Feelings of inadequacy	High	Medium	Low	High	Medium
Break-up or divorce	Medium	Low	Low	Medium	High
Impending termination of contract	High	High	Low	Medium	Medium

What are behavioral indicators?

Indicator	Sabotage	Theft	Fraud	Espionage	Unintentional
Unwillingness to comply with established rules and procedures	High	Medium	Low	Medium	High
Repeated breach of procedures	Medium	High	High	High	High
Excessive or unexplained use of data copy equipment (fax, copy, camera)	Low	High	Low	High	High
Excessive volunteering which would elevate access to sensitive data	Low	High	High	High	Medium
Excessive overtime work	Low	High	High	High	Low
Bringing personal equipment to high-security areas	Low	High	Medium	High	High
Carelessness	Low	Low	Low	Low	High
Concerning statements, jokes, or bragging	Medium	Low	Low	Medium	High
Impulsiveness	Medium	Medium	Low	Low	High
Poor social interaction	High	Medium	Low	Low	Medium
Aggression	High	Medium	Low	Low	Medium

What are background indicators?

Indicator	Sabotage	Theft	Fraud	Espionage	Unintentional
Involvement with individuals or groups who oppose core beliefs of organisation	High	Medium	Medium	High	Medium
Criminal record	Medium	High	High	Medium	Low
Addiction (alcohol, drugs, gambling)	Medium	High	High	Medium	Medium
History of mental or emotional disorder	High	Medium	Low	Medium	Medium
Indebtedness	Low	High	High	Medium	Low
Sexual behaviour which indicates lack of judgement	Low	Medium	Medium	Medium	High
Engagement in activities which can cause a conflict of	Medium	High	High	High	Medium
Business dealings	Low	High	Medium	Medium	Low
Active presence in social media	Low	Low	Low	Low	High
Number of previous employers and average time of employment	High	High	Low	Low	High
Spending exceeds income	Low	High	High	High	Low

What are network indicators?

Indicator	Sabotage	Theft	Fraud	Espionage	Unintentional
Correspondence with competitors	Low	High	High	Medium	Low
E-mail messages with abnormally large amount of data	Low	High	High	High	Low
DNS queries which indicate involvement with internet underground	Medium	High	Low	Medium	Low
Use of suspicious protocols (e.g. IRC)	Low	High	Low	Low	High
Use of suspicious services (e.g. VPN, Tor)	Low	High	Low	Low	Low
Execution of offensive tools	Medium	High	Low	Medium	Low
Execution of malware	Medium	Low	Low	Low	High
Anomalous peaks in outgoing connection count	Medium	High	Low	High	Low
An unauthorised device is connected to the network	Medium	High	Low	High	Medium
Download of blacklisted software	High	Medium	Low	Medium	Medium
Connections initiated from a workstation outside working hours	Medium	High	Low	Medium	High

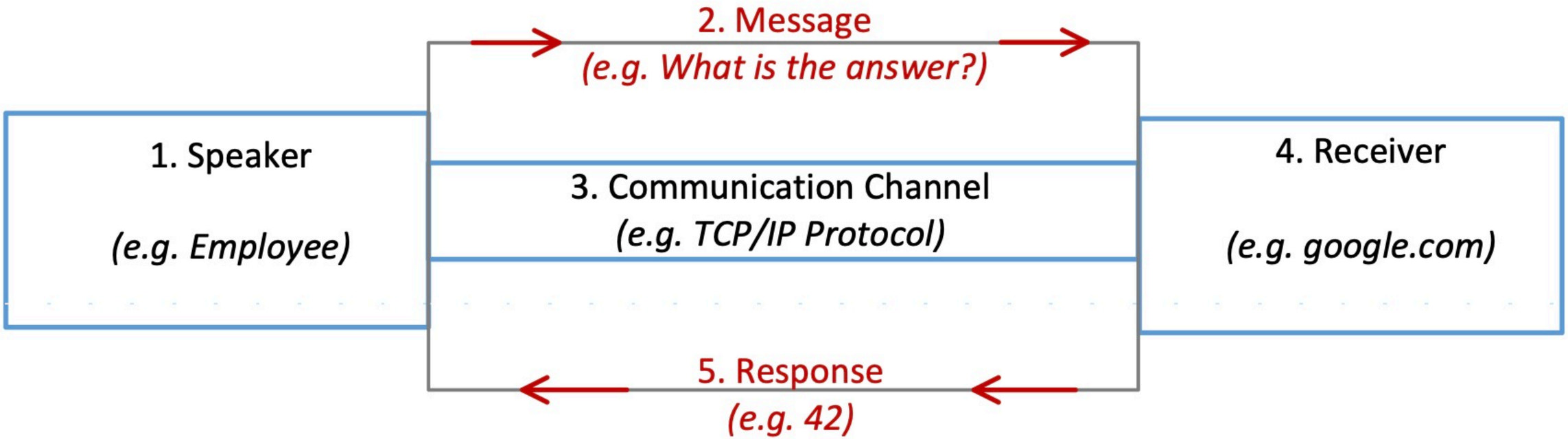
What are endpoint indicators?

Indicator	Sabotage	Theft	Fraud	Espionage	Unintentional
Anti-malware alerts	High	Medium	Low	Medium	High
Blacklisted files detected ('hacker tools')	High	High	Low	High	Low
(Attempt of) disabling anti-malware tools	High	High	Low	Medium	High
Attempted escalation of privileges	High	High	Low	Medium	Low
User attempts to print or copy confidential documents	Low	High	Low	High	Medium
Abnormally large number of software errors	High	Medium	Low	Medium	High
Unidentified device is attached (USB, CD-ROM)	Medium	High	Low	High	Medium
Failed login attempts	Medium	High	Low	Low	Low
Different users (attempting to) log in from the same workstation	Medium	High	Medium	Low	Low
User logs into a desktop workstation outside working hours	Medium	High	Medium	Low	Medium
Lack of log messages or monitoring data	High	High	Low	Medium	Medium

What are log-based indicators?

Indicator	Sabotage	Theft	Fraud	Espionage	Unintentional
Modification of centrally stored log files	High	High	Low	Medium	Low
User copies a large number of documents to a local disk	Low	High	Low	High	Low
Authentication failures	Medium	Medium	High	Medium	Low
Configuration file changes	High	Medium	Low	Medium	Medium
Permission changes	Medium	High	Medium	High	Medium
Database content changes	Medium	Low	High	Medium	Medium
Employee attempts to access resources not associated with his role	Low	High	High	High	Medium
User account is used from multiple devices	Medium	High	High	Medium	High
User account is set to expire in 30 days or less	High	High	Low	Medium	Low
Multiple accounts per user	High	High	Medium	Medium	Low

Back to Basics



What is due?

Homework & Discussions

Homework-5

- **Assignment:** Design a corporate infrastructure involving network, data, endpoint, code, web, and insider security controls.

- *How do you know what is vulnerable in your architecture?*

Threat Modeling

Practical Introduction using https://github.com/izar/pytm

Homework Expectations

- Architecture diagram
- Threat Modeling
- Three Mitigation controls
  - Domain
  - Content
  - Insider
- Without any PII content and publish it on GWU Blog
- Submit a link to GWU Blog post for grading

References

- https://www.cdse.edu/resources/case-studies/insider-threat.html
- https://resources.sei.cmu.edu/asset_files/TechnicalNote/2014_004_001_427430.pdf
- https://www.iarpa.gov/index.php/research-programs/icarus
- https://soar.eecs.umich.edu/workshop/39/files/Learning%20Taxonomy.pdf
- http://www.isle.org/~langley/papers/icarus.csr17.pdf
- https://ccdcoe.org/uploads/2018/10/Insider_Threat_Study_CCDCOE.pdf
- https://www.nationalinsiderthreatsig.org/pdfs/Insider%20Threats%20Incidents-Could%20They%20Happen%20To%20Your%20Organization.pdf
- https://resources.sei.cmu.edu/asset_files/TechnicalNote/2014_004_001_427430.pd