A behavioral risk model for the early detection of insider risks

Signals

Incoming data is processed to create observations

- Access type
- Email activity
- Facility access logs
- File downloads
- File renaming
- Geographical location
- Internet traffic
- Phone records
- System access logs
- Time of day
- Travel records
- Web access

Observations

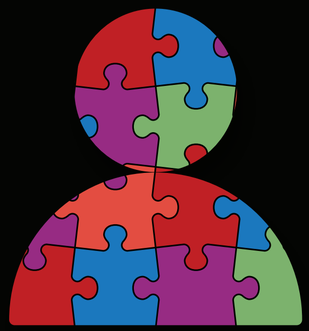
Observations processed to create indicators

- Authorization attempts
- File combinations
- File size
- Frequency of access
- Frequency of communication
- HR/performance information
- Install scripts
- Usage patterns
- Websites

Indicators

Indicators assessed to evaluate insider risks

- Attempts to access privileged data
- Access attempts outside of the pattern
- Disgruntled employee
- Harvesting data
- Policy violations
- Suspicious communications



Behavioral risks

Early detection of behaviors that match insider risk types

Reference: Greitzer & Frincke (2010)[1]

[1] *Greitzer, FL, and DA Frincke. (2010). "Combining Traditional Cyber Security Audit Data with Psychosocial Data: Towards Predictive Modeling for Insider Threat Mitigation." In: CW Probst, J Hunter, D Gollmann & M Bishop (Eds.),* Insider Threats in Cyber Security, *New York: Springer, pp. 85-113.*