Insider Threat Indicators

The following list is not comprehensive and represents a matrix of insider threat indicator versus threat type as developed by the NATO Cooperative Cyber Defence Center of Excellence (CCDCOE) in 2014.

The complete document can be found here:
https://ccdcoe.org/sites/default/files/multimedia/pdf/Insider_Threat_Study_CCDCOE.pdf

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

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

Insider Threat Indicators

Soteritech
Insider Threat Training

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

Insider Threat Indicators

Soteritech
Insider Threat Training

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

Insider Threat Indicators

Soteritech
Insider Threat Training

Client-side 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

Insider Threat Indicators

Soteritech
Insider Threat Training

Service 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