Definition

Insider threats are security risks that arise from people within an organization who have authorized access to its assets and networks. These individuals, such as employees, contractors, or partners can use their access to harm the organization intentionally or unintentionally. Insider threats can be difficult to detect and can cause significant damage to an organization's data systems and security.

Insider Threat Examples

Some examples of insider threats include:

Negligent insiders

Employees who don't follow proper IT procedures, such as leaving their computer logged in or not changing default passwords

Malicious insiders

Employees who have malicious intent to harm the organization, such as stockpiling data to use in a new job

Signs of an Insider Threat

Some signs of an insider threat include:

Unusual data movement, such as large data downloads or sending large amount of data outside the company
Use of unsanctioned software or hardware, such as tools to bypass security control
Increased requests for access to sensitive information

Homeland Security defines insider threat as the threat that an employee or a contractor will use his or her authorized access, wittingly or unwittingly, to do harm to the security of the United states.

Unintentional threat:

Negligence:

- Allowing someone to “piggyback” through a secure entrance point
- Misplacing or losing a portable storage device containing sensitive information
- Ignoring messages to install new updates and security patches

Accidental:

- An insider of this type mistakenly causes an unintended risk to an organization. Examples include mistyping an email address and accidentally sending a sensitive business document to a competitor, unknowingly or inadvertently clicking on a hyperlink, opening an attachment in a phishing email that contains a virus, or improperly disposing of sensitive documents.

Intentional Threats

The intentional insider is often synonymously referenced as a “malicious insider.” Intentional threats are actions taken to harm an organization for personal benefit or to act on a personal grievance. For example, many insiders are motivated to “get even” due to a perceived lack of recognition (e.g., promotion, bonuses, desirable travel) or termination. Their actions can include leaking sensitive information, harassing associates, sabotaging equipment, perpetrating violence, or stealing proprietary data or intellectual property in the false hope of advancing their careers.

DTEX Systems

As the global leader for inside risk management, DTEX empowers organizations to prevent data loss and support a trusted workforce by stopping insider risks from becoming insider threats. Its InTERCEPT platform consolidates the essential elements of data loss prevention, user behavior analytics, and user activity monitoring in a single light-weight platform to detect and mitigate insider risks well before data loss occurs.

Data Loss Prevention
User Behavior Analytics
User Activity Monitoring

Detect

Mitigate

What are some criteria you would use to evaluate DTEX software on its ability to detect employees who pose an insider risk?

Breadth of insider threats

- File download from external sources/to local computer, disk etc
- Data copy - network
- Deleting code - Repo
- Deleting files/data
- Malicious code/software install/injection
- Bypassing security controls to perform actions
- Clicking phishing email links
- Sending emails with viruses
- Sabotaging network/data/servers/employee accounts/company accounts
- Gaining access to company confidential data/services
- Requesting higher permissions/clearance/access

Data Formats

- Various data source types

Visibility

- Metrics/Graphs
- Drill-down capabilities

Context-aware Detection to avoid false positives and true negatives

Sources

Google
Homeland Security
CISA