Preparation 1

Objective: Establish contacts, define procedures, and gather information to save time during the incident handling.

Contacts

- Make sure to also have contact points in your public relation team, human resources team and legal department
- Have a centralized logging facility
- Be sure to have a global authorization and clearance process. This process must specially take care of the removal of privileges on former jobs
- Provide strong authentication accordingly to the risk of the business application

Identification 2

Objective: Detect the incident, determine its scope, and involve the appropriate parties.

Insider abuses are hard to detect and there is no 100% success tips.

Technical identification

- **Alerts from a SIEM or correlation tools**

Malicious behaviour can have been detected with the correlation of several abnormal events

- **Alerts from an IDS/IPS detecting an intrusion**

In case the insider tried to hack the system, an Intrusion Detection System (or Intrusion Prevention System) can be able to trigger an alert.

Human identification

- **Management:**

The manager of the insider might be the first to notice the suspected behaviour.

- **Control, risk, compliance:**

These teams have their own systems to detect operational anomalies and they can also trigger alerts if something abnormal is detected.

- **Colleagues:**

Insider's colleagues are maybe the most valuable notification channel because they know perfectly the tasks, the process and the impacts on their duty jobs. They can guess easily what is happening.

- **External parties:**

External partners or structure can also have their own detection capabilities. If operations have been falsified internally, these external entities can bring a real enlightenment.

Containment 3

Objective: Mitigate the attack's effects on the targeted environment.

Don't do anything, without a written request from the concerned CISO/person in charge. Based on your legal team advisory, a written permission from the concerned user might also be handy.

- **Involve people:**

Different people should be informed about the abuse so that they can help to assist on it. This includes HR management, legal management, PR management and business management of the suspected insider.

- **Meeting:**

An HR manager should meet the suspected insider to explain him/her what has been found and what will happen. Support can be required from legal, technical and management people.

- **Privileges lowering:**

If the suspected insider is allowed to stay at work until the end of the investigation, provide him/her a computer with minimum authorizations.

- **Authorization freeze:**

Suspend access and authorizations of the suspected insider. This must include application clearance. This can also include system account, keys, building facility badge.

- **Remote access:**

Suspend remote access capabilities, i.e.: smartphones, VPN accounts, tokens...

- **Seizure:**

Seize all the professional computing device of the suspected insider.

Containment 3

Case 1: abnormal activity

If nothing malicious or fraudulent is confirmed yet, two investigations should start right now:

- forensics investigation on the computing devices of the suspected insider.
- log investigation on different audit trails components

Case 2: malicious / fraudulent activity

If malicious or fraudulent behaviour is already confirmed, think about file a complaint against the suspected insider.
In this case, do not take any further technical actions. Provide the legal team or law enforcement officer all requested evidences and be ready to assist on demand.

If collateral damages can result from the abuse, be sure to contain the incident impacts before making it public. Be sure to inform authorities if required.

Remediation 4

Objective: Take actions to remove the threat and avoid future incidents.

The remediation part is pretty limited in case of an insider abuse. Following actions can be considered depending on the case:

- Take disciplinary action against the malicious employee (or terminate the contract) and remove all his/her credentials.
- Delete all fictitious or fraudulent operations made by the insider
- Review all programs or scripts made by the insider and remove all unnecessary codes

Recovery 5

Objective: Restore the system to normal operations.

If the incident has not been made public yet, be sure to warn all the impacted stakeholders (customers, concerned partners …) and required authorities. This communication must be made by top management in case of huge impacts.

Eventually warn your employees or some local teams about the issue to raise awareness and increase security rules.

Aftermath 6

Objective: Document the incident's details, discuss lessons learned, and adjust plans and defences.

Report

An incident report should be written and made available to all of the actors of the incident.

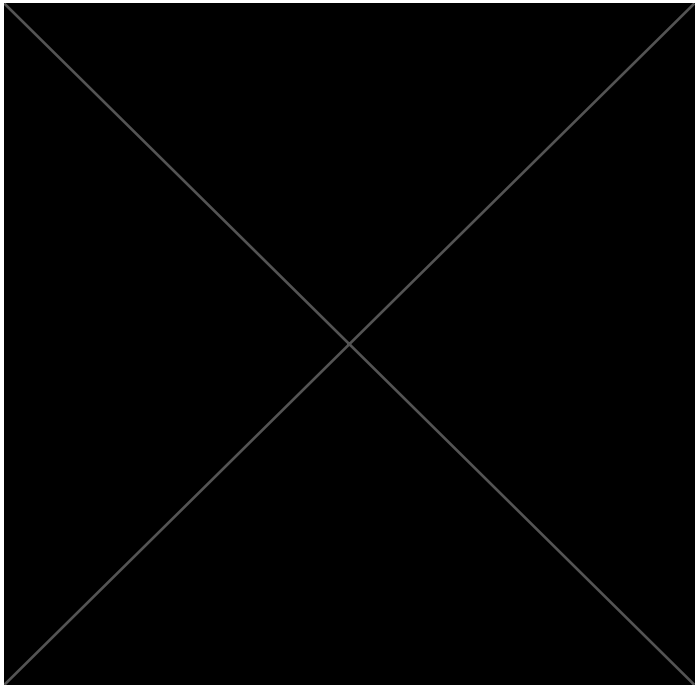
The following themes should be described:

- Initial detection
- Actions and timelines
- What went right
- What went wrong
- Incident impact

Capitalize

Some improvement might be especially valuable considering insider abuse:

- Authorization process improvements
- Controls improvements in the organisation
- Awareness on fraud and malicious activity



Abstract

This Incident Response Methodology is a cheat sheet dedicated to handlers investigating on a precise security issue.
Who should use IRM sheets?

- Administrators
- Security Operation Center
- CISOs and deputies
- CERT (Computer Emergency Response Team)

Remember: If you face an incident, follow IRM, take notes and do not panic. Contact your CERT immediately if needed:

Incident handling steps

6 steps are defined to handle security Incidents

- **Preparation: get ready to handle the incident**
- **Identification: detect the incident**
- **Containment: limit the impact of the incident**
- **Remediation: remove the threat**
- **Recovery: recover to a normal stage**
- **Aftermath: draw up and improve the process**

IRM provides detailed information for each step.