XRAY

Incident Handling Manual

Created for the Showcase scenario on the Inject Exercise Platform.

INJECT

Incident Handling Process

Communication during the incident handling process:

- Keep essential stakeholders, such as Public Relations (PR) and management, informed about the progress of the incident handling.
- Contact the Data Protection Officer (DPO) if a personal data breach is suspected.

Assessment and Triage:

- Upon an incident report, assess the severity and impact of the incident.
- Get as much information as possible about the incident.
- Decide if the incident requires an immediate response.

Containment:

- Isolate affected systems or networks.
- Preserve forensic evidence for possible law enforcement investigation.

Investigation and analysis:

- Investigate the incident to understand the root cause and scope.

Eradication and Recovery:

- Develop a plan to resolve the incident.
- Restore the functionality of affected systems, e.g. by using backups.

Lessons Learned:

- Share information about the incident with the relevant teams.
- Suggest ways to reduce the possibility of a similar incident in the future.

Available Tools

Contact list:

The contact list tool will help you retrieve available email contacts.

Crisis meeting initiation tool:

A crisis meeting is convened in a situation where a severe security incident has occurred, leading to a breach in the confidentiality, integrity, or availability of critical processes or services. Participants are informed by email when a crisis meeting is organized.

The participants of the crisis meeting are:

- Chief Executive Officer (CEO)
- DPO
- Head of Operations
- Head of Legal
- CSIRT

Internal warning tool:

Issuing an internal warning is appropriate for situations where the organization is under attack by an external actor or where such an attack can be anticipated with a high probability. Internal warnings are used to inform the employees, about such attacks, e.g. a phishing campaign or denial of service attack.

Created for the Showcase scenario on the Inject Exercise Platform.

INJECT