# Prepare

Connect with trusted communities to share information

Defensomania

# Prepare

## Implement a central log management system

Defensomania

# Prepare

## Implement event and alert management system for effective first triage

Defensomania

# Prepare

## Implement case management system for effective incident handling

Defensomania

# Prepare

## Implement automation and orchestration to support analysts during first triage and incident investigations

Defensomania

# Prepare

Implement detection use cases to cover the required scope

Defensomania

# Prepare

Build know-how for new threats and provide trainings to analysts

Defensomania

# Prepare

Establish visibility into all critical assets and platform

Defensomania

# Prepare

Ensure central log collection for relevant logs on systems in monitoring and incident response scope

Defensomania

# Prepare

Deploy remote forensics software

Defensomania

# Prepare

Deploy tools and capabilities for containment

Defensomania

# Prepare

## Prepare decision tree and establish processes for GDPR readiness

Defensomania

# Prepare

Attend or organize internal and external exercises

Defensomania

# Prepare

Prepare and build coordination and escalation team for major incidents

Defensomania

# Prepare

Prepare and implement playbooks
for assisting analysts

Defensomania

# Prepare

Prepare a list of critical assets for prioritisation

Defensomania

# Prepare

Ensure knowledge of all used operating systems in the team

Defensomania

# Prepare

Establish different kinds of communication channel for various stakeholders

Defensomania

# Prepare

Make a list of contact details for relevant peers

Defensomania

# Prepare

Ensure and implement collaboration between SOC and CSIRT and clarify responsibilities during an incident

Defensomania

# Prepare

## Build backup infrastructure in case of emergency

Defensomania

# Prepare

Search for threats through regular threat hunting

Defensomania

# Prepare

Implement detection to find sensitive data which was indexed in a public search engine

Defensomania

# Prepare

Joker - invent a new preparation step

Defensomania

# Prepare

Joker - invent a new preparation step

Defensomania

# Prepare

Joker - invent a new preparation step

Defensomania

# Detect

Search for email attributes inside all of your mailboxes

Defensomania

# Detect

Search for cron jobs on Linux server

Defensomania

# Detect

Search for configuration settings on remote system

Defensomania

# Detect

Search for malicious configuration changes on remote system

Defensomania

# Detect

Search for processes on a remote host

Defensomania

# Detect

Search for files on a remote host

Defensomania

# Detect

Search for file hash on a remote host

Defensomania

# Detect

Search for destination IPs in network logs

Defensomania

# Detect

Search for source IPs in your network logs

Defensomania

# Detect

Search for domains in your network logs

Defensomania

# Detect

Search for referrer in your network logs

Defensomania

# Detect

Search for user agent in your network logs

Defensomania

# Detect

Search for URL in your network logs

Defensomania

# Detect

Search for leaked data in public search engines and paste sites

Defensomania

# Detect

Detect credential abuse by looking at login anomalies

Defensomania

# Detect

Detect credential leakage through monitoring external paste sites

Defensomania

# Detect

Detect leaked sensitive information on public source code repository

Defensomania

# Detect

Detect lateral movement with pipes

Defensomania

# Detect

## Detect lateral movement with local admin

Defensomania

# Detect

## Detect lateral movement with credential abuse

Defensomania

# Detect

Detect malicious process injection

Defensomania

# Detect

Detect leaked information through active cybercrime forum monitoring

Defensomania

# Detect

Detect unauthorized access on remote system

Defensomania

# Detect

Detect unknown domain administrator in your user management

Defensomania

# Detect

Detect unknown local administrator account on compromised system

Defensomania

# Detect

## Detect in-memory malware on remote host

Defensomania

# Detect

Check GDPR relevance

Defensomania

# Detect

Find attacker through attacker's real IP which leaked because of bad op-sec

Defensomania

# Detect

Joker - invent a new detection method

Defensomania

# Detect

Joker - invent a new detection method

Defensomania

# Detect

Joker - invent a new detection method

Defensomania

# Respond

Remove persistence mechanisms
on compromised system

Defensomania

# Respond

Remove malicious config settings
on a compromised system

Defensomania

# Respond

## Remove malware on compromised system

Defensomania

# Respond

Stop malicious process on compromised system

Defensomania

# Respond

Stop data leakage on compromised system

Defensomania

# Respond

Remove sensitive data on public accessible website

Defensomania

# Respond

Start first response to gather volatile data

Defensomania

# Respond

Collect and analyse logs from compromised system

Defensomania

# Respond

Collect evidence from compromised system

Defensomania

# Respond

Collect files from compromised system

Defensomania

# Respond

Collect the list of local accounts
from compromised system

Defensomania

# Respond

Create and collect disk image for a compromised system

Defensomania

# Respond

Create file system timeline for a disk image

Defensomania

# Respond

## Extract C2 IPs from a malware sample

Defensomania

# Respond

Search for found C2 servers

Defensomania

# Respond

Search for other affected systems after initial compromise

Defensomania

# Respond

## Block domain names

Defensomania

# Respond

## Block IPs

Defensomania

# Respond

## Block URLs

Defensomania

# Respond

Block access to API

Defensomania

# Respond

Block employee account

Defensomania

# Respond

Isolate system

Defensomania

# Respond

Take remote system offline

Defensomania

# Respond

## Disable network connectivity on remote system

Defensomania

# Respond

Delete malicious emails in employees mailboxes

Defensomania

# Respond

Sinkhole C2 server

Defensomania

# Respond

Capture traffic to C2 server

Defensomania

# Respond

Force password reset

Defensomania

# Respond

Add evidence to long time storage

Defensomania

# Respond

## Mitigate a DDoS attack

Defensomania

# Respond

Initiate hot patching or immediate fix of exploited vulnerability

Defensomania

# Respond

## Create a GDPR notification

Defensomania

# Respond

Document indicators of attack and indicators of compromise centrally.

Defensomania

# Respond

Share indicators of attack and of compromise with the community

Defensomania

# Respond

Joker - invent a new respond action

Defensomania

# Respond

Joker - invent a new respond action

Defensomania

# Respond

Joker - invent a new respond action

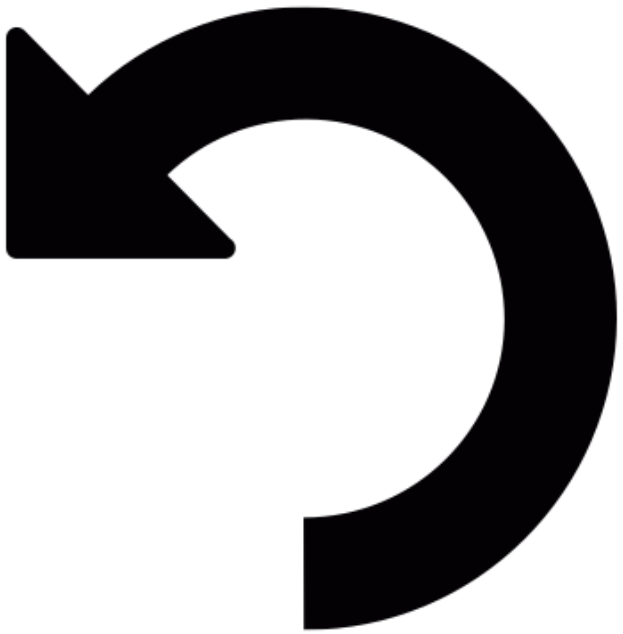
Defensomania

# Respond

Joker - invent a new respond action

Defensomania

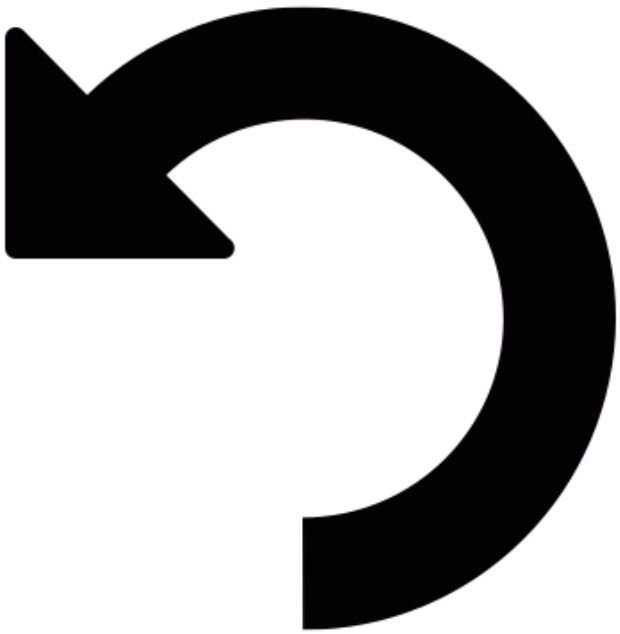
# Recover



Initiate fresh installation of compromised system from trusted install sources

Defensomania

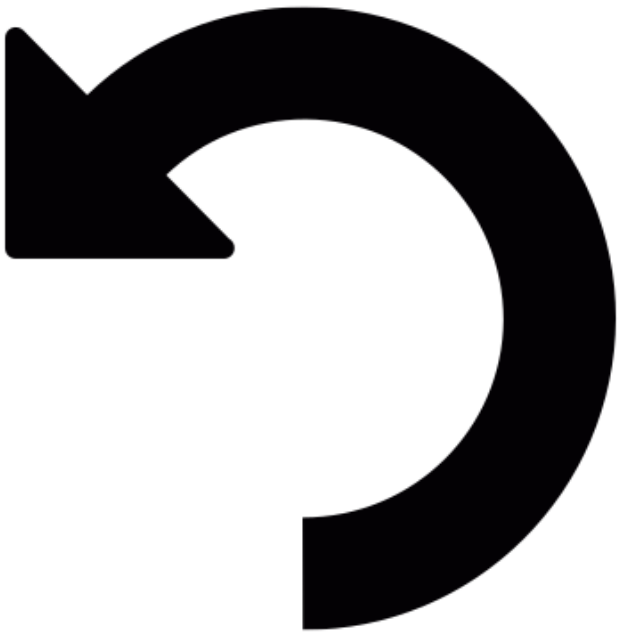
# Recover



Initiate the patching of a critical vulnerability

Defensomania

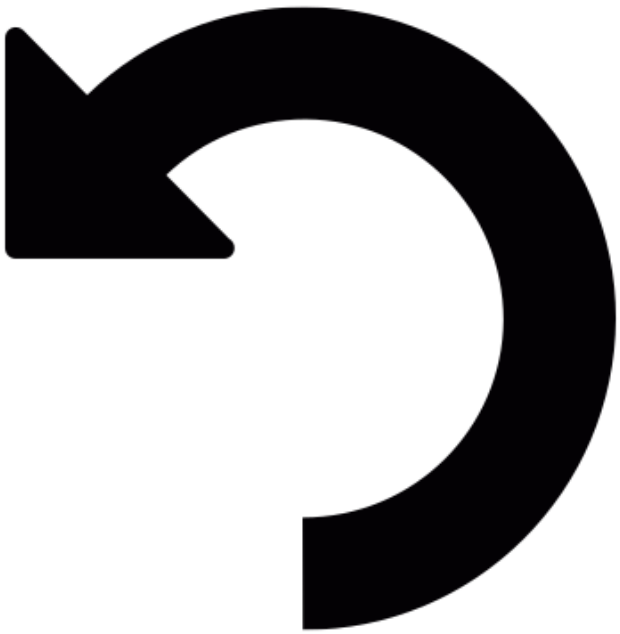
# Recover



Initiate an audit on a platform

Defensomania

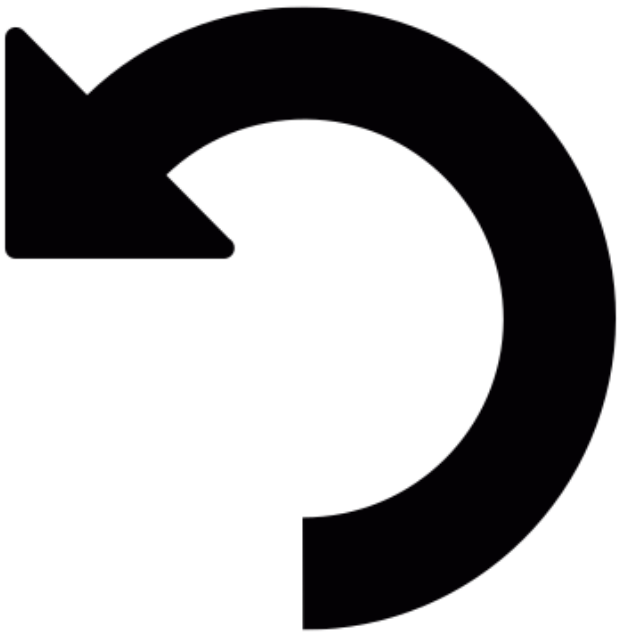
# Recover



Restore backup

Defensomania

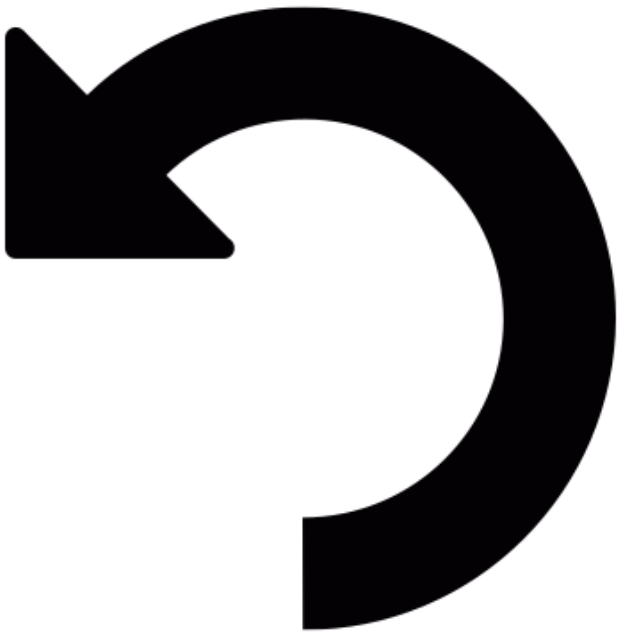
# Recover



Bring the service online which you took offline during the incident

Defensomania

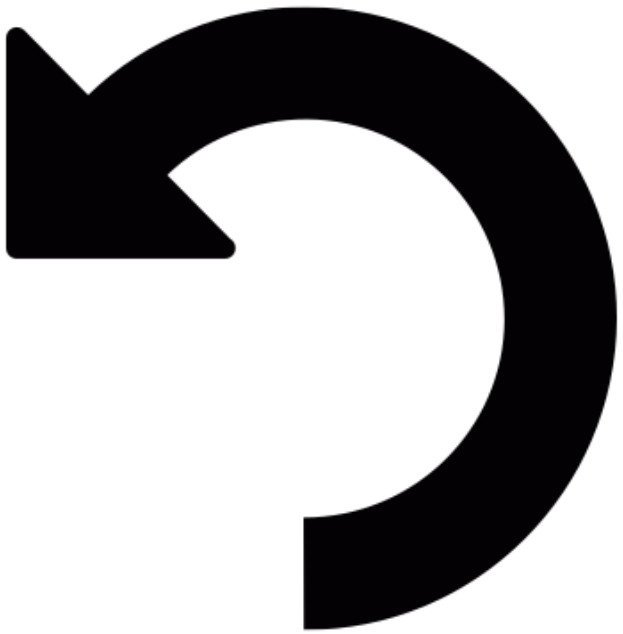
# Recover



Rotate API keys for a compromised account

Defensomania

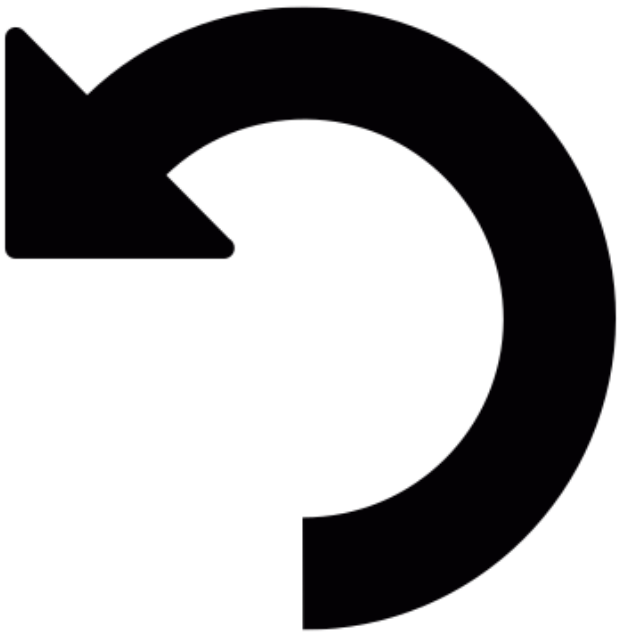
# Recover



Change credentials for a compromised service account which was disabled during the incident

Defensomania

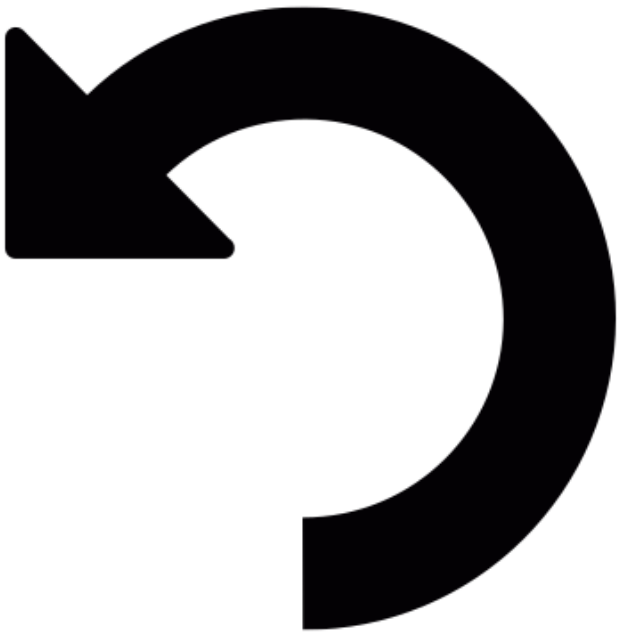
# Recover



Implement long term monitoring through new security monitoring use cases and incident response processes

Defensomania

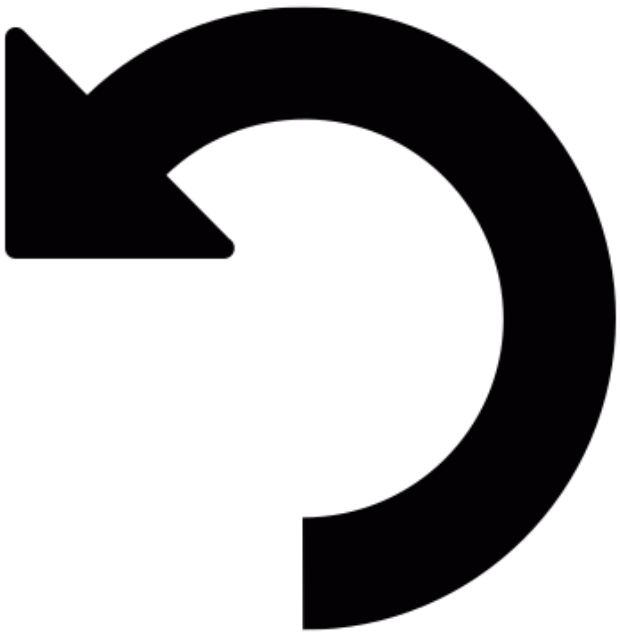
# Recover



Add a security deficit to the policy framework

Defensomania

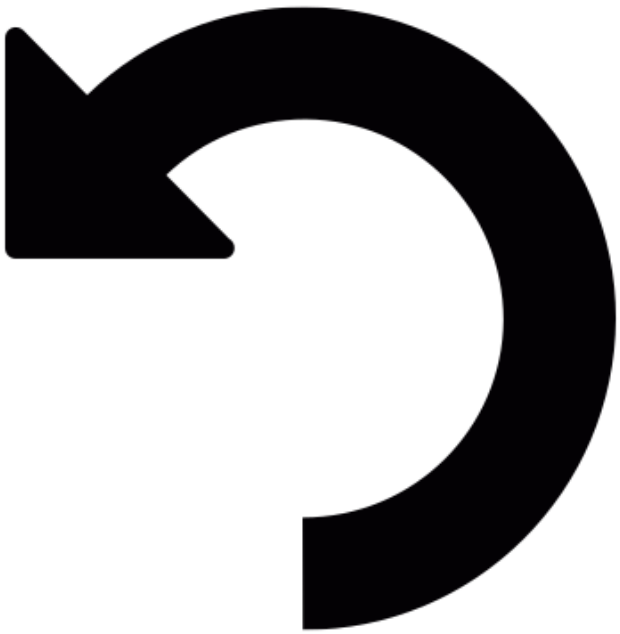
# Recover



Joker - invent a new recover action

Defensomania

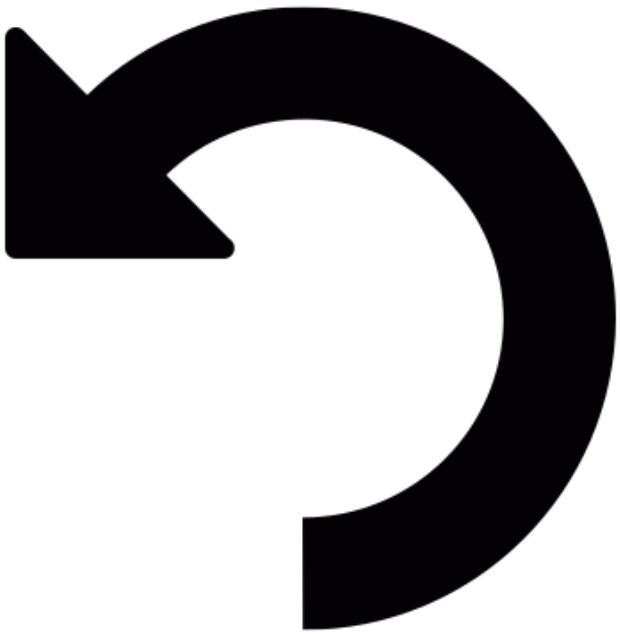
# Recover



Joker - invent a new recover action

Defensomania

# Recover



Joker - invent a new recover action

Defensomania

# Lessons Learned

Organize and perform lessons learned meeting

Defensomania

# Lessons Learned

## Define technical debts and report them accordingly

Defensomania

# Lessons Learned

Document results and new knowledge for the team and company

Defensomania

# Lessons Learned

## Improve incident response processes

Defensomania

# Lessons Learned

## Improve incident detection capabilities

Defensomania

# Lessons Learned

## Add new detection rule to internal and external repositories

Defensomania

# Lessons Learned

Joker - invent a new lessons learned step

Defensomania

# Lessons Learned

Joker - invent a new lessons learned step

Defensomania

# Lessons Learned

Joker - invent a new lessons learned step

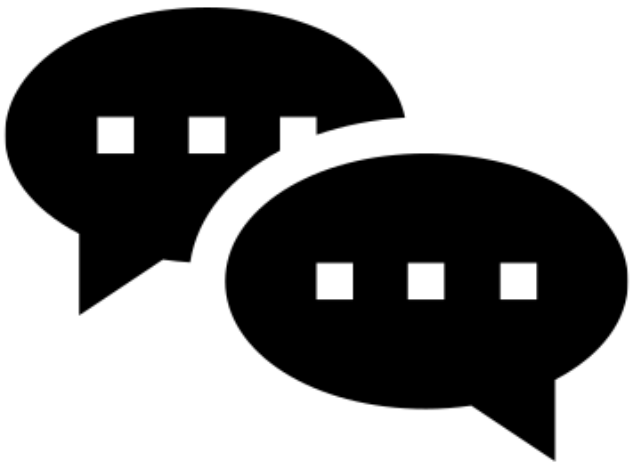
Defensomania

# Lessons Learned

Joker - invent a new lessons learned step

Defensomania

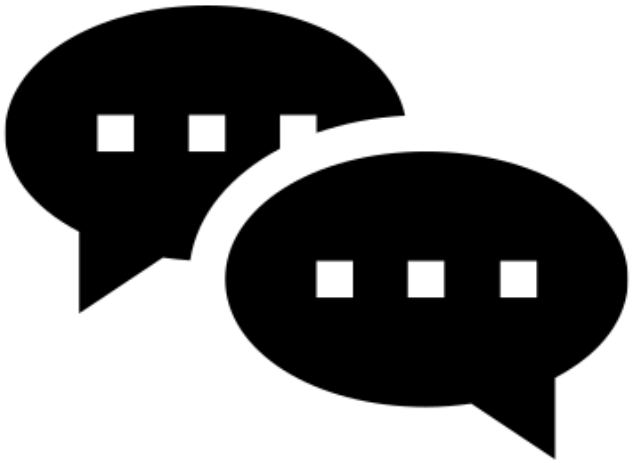
# Communication



## Publish external news article

Defensomania

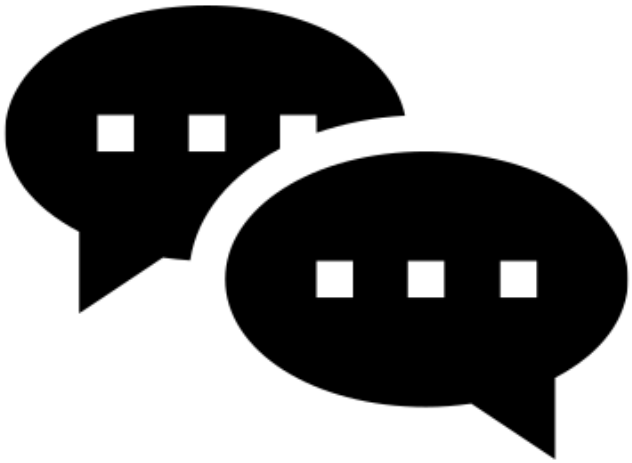
# Communication



Inform public relations department about possible questions from outside

Defensomania

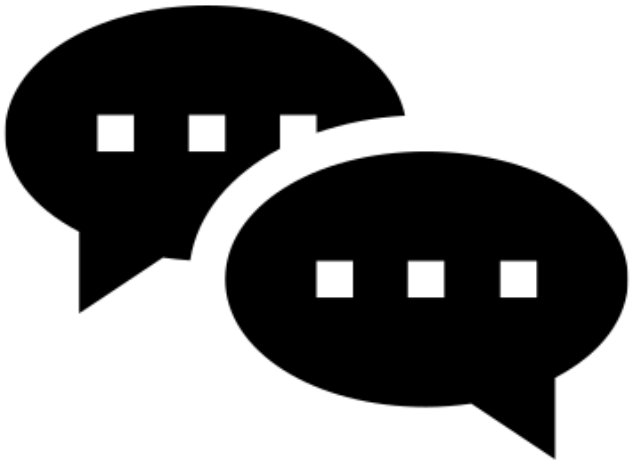
# Communication



## Communicate findings to management

Defensomania

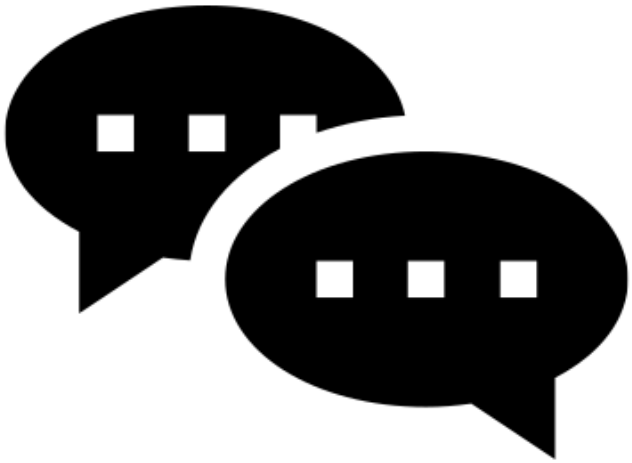
# Communication



## Create an incident report

Defensomania

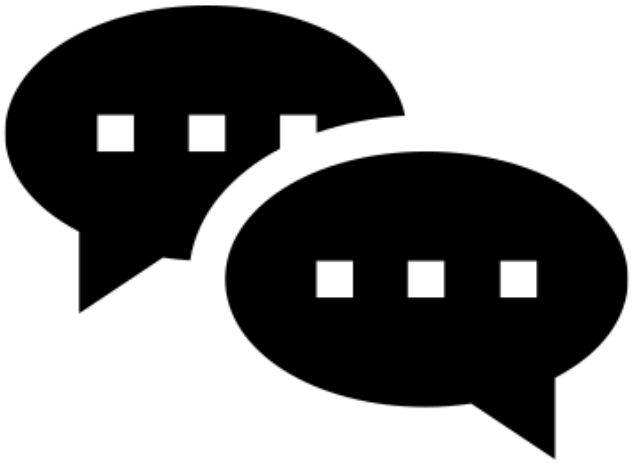
# Communication



Write answer to request made on external platform

Defensomania

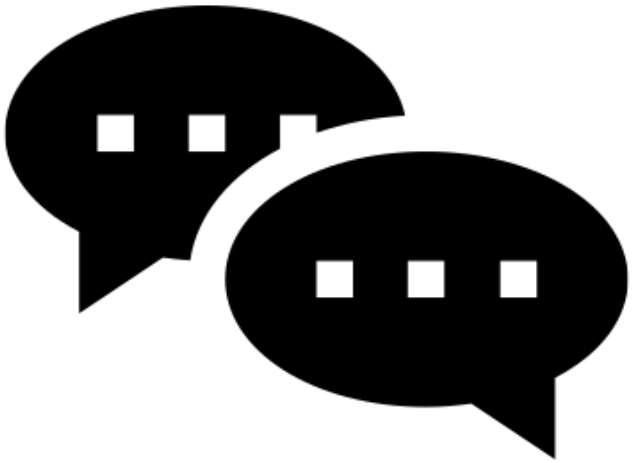
# Communication



Joker - invent a new communication way

Defensomania

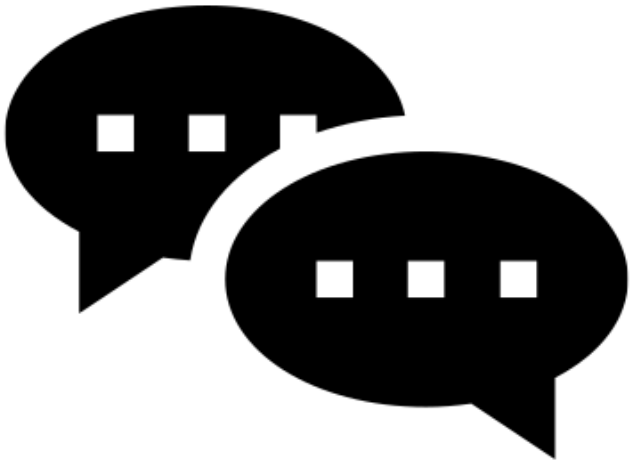
# Communication



Joker - invent a new communication way

Defensomania

# Communication



Joker - invent a new communication way

Defensomania