

# Prepare



Connect with trusted communities  
to share information

# Prepare



Implement a central log management system

# Prepare



Implement event and alert management system for effective first triage

# Prepare



Implement case management system for effective incident handling

# Prepare



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

# Prepare



Implement detection use cases to cover the required scope

# Prepare



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

# Prepare



Establish visibility into all critical assets and platform

# Prepare



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

# Prepare



Deploy remote forensics software

# Prepare



Deploy tools and capabilities for containment

# Prepare



Prepare decision tree and establish processes for GDPR readiness

# Prepare



Attend or organize internal and  
external exercises

# Prepare



Prepare and build coordination and escalation team for major incidents

# Prepare



Prepare and implement playbooks  
for assisting analysts

# Prepare



Prepare a list of critical assets for prioritisation

# Prepare



Ensure knowledge of all used operating systems in the team

# Prepare



Establish different kinds of communication channel for various stakeholders

# Prepare



Make a list of contact details for relevant peers

# Prepare



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

# Prepare



Build backup infrastructure in case  
of emergency

# Prepare



Search for threats through regular threat hunting

# Prepare



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

# Prepare



Joker - invent a new preparation step

# Prepare



Joker - invent a new preparation step

# Prepare



Joker - invent a new preparation step

# Detect



Search for email attributes inside all  
of your mailboxes

# Detect



Search for cron jobs on Linux server

# Detect



Search for configuration settings on  
remote system

# Detect



Search for malicious configuration  
changes on remote system

# Detect



Search for processes on a remote host

# Detect



Search for files on a remote host

# Detect



Search for file hash on a remote host

# Detect



Search for destination IPs in  
network logs

# Detect



Search for source IPs in your  
network logs

# Detect



Search for domains in your network logs

# Detect



Search for referrer in your network logs

# Detect



Search for user agent in your  
network logs

# Detect



Search for URL in your network logs

# Detect



Search for leaked data in public  
search engines and paste sites

# Detect



Detect credential abuse by looking  
at login anomalies

# Detect



Detect credential leakage through monitoring external paste sites

# Detect



Detect leaked sensitive information  
on public source code repository

# Detect



Detect lateral movement with pipes

# Detect



Detect lateral movement with local admin

# Detect



**Detect lateral movement with  
credential abuse**

# Detect



Detect malicious process injection

Defensomania

# Detect



Detect leaked information through active cybercrime forum monitoring

# Detect



Detect unauthorized access on  
remote system

# Detect



Detect unknown domain  
administrator in your user  
management

# Detect



Detect unknown local administrator account on compromised system

# Detect



Detect in-memory malware on  
remote host

# Detect



Check GDPR relevance

# Detect



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

# Detect



Joker - invent a new detection  
method

# Detect



Joker - invent a new detection  
method

# Detect



Joker - invent a new detection  
method

# Respond



Remove persistence mechanisms  
on compromised system

# Respond



Remove malicious config settings  
on a compromised system

# Respond



Remove malware on compromised system

# Respond



Stop malicious process on  
compromised system

# Respond



Stop data leakage on compromised system

# Respond



Remove sensitive data on public  
accessible website

# Respond



Start first response to gather volatile  
data

# Respond



Collect and analyse logs from  
compromised system

# Respond



Collect evidence from compromised system

# Respond



Collect files from compromised  
system

# Respond



Collect the list of local accounts  
from compromised system

# Respond



Create and collect disk image for a compromised system

# Respond



Create file system timeline for a disk image

# Respond



Extract C2 IPs from a malware sample

# Respond



Search for found C2 servers

# Respond



Search for other affected systems  
after initial compromise

# Respond



Block domain names

Defensomania

# Respond



Block IPs

Defensomania

# Respond



Block URLs

Defensomania

# Respond



Block access to API

Defensomania

# Respond



Block employee account

# Respond



Isolate system

Defensomania

# Respond



Take remote system offline

# Respond



Disable network connectivity on  
remote system

# Respond



Delete malicious emails in  
employees mailboxes

# Respond



Sinkhole C2 server

Defensomania

# Respond



Capture traffic to C2 server

# Respond



Force password reset

Defensomania

# Respond



Add evidence to long time storage

# Respond



Mitigate a DDoS attack

# Respond



Initiate hot patching or immediate fix  
of exploited vulnerability

# Respond



Create a GDPR notification

# Respond



Document indicators of attack and indicators of compromise centrally.

# Respond



Share indicators of attack and of compromise with the community

# Respond



Joker - invent a new respond action

# Respond



Joker - invent a new respond action

# Respond



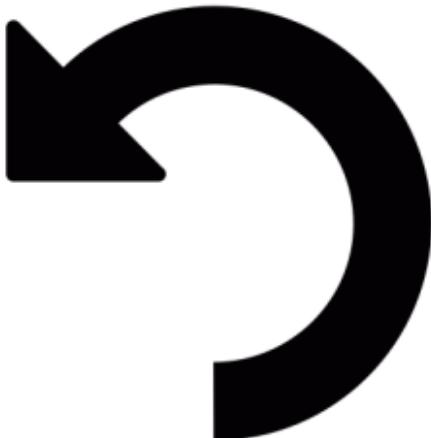
Joker - invent a new respond action

# Respond



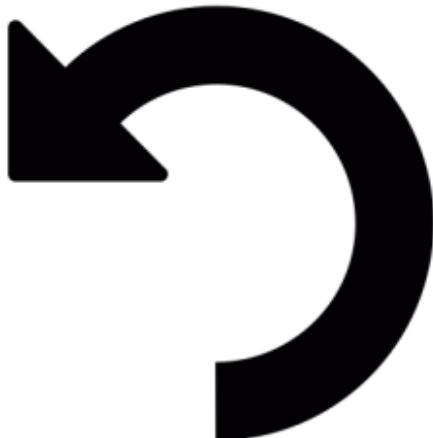
Joker - invent a new respond action

# Recover



Initiate fresh installation of  
compromised system from trusted  
install sources

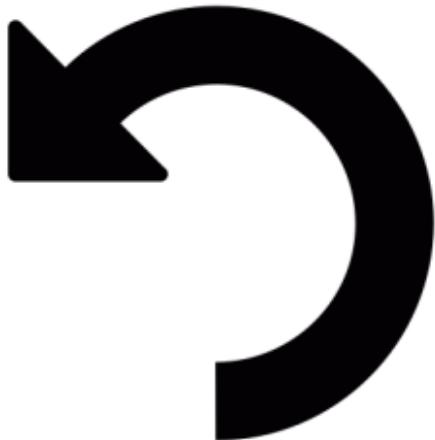
# Recover



**Initiate the patching of a critical  
vulnerability**

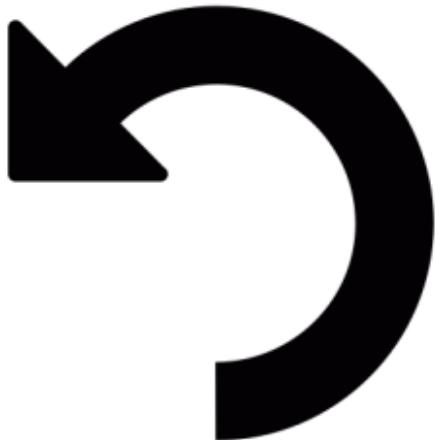
Defensomania

# Recover



Initiate an audit on a platform

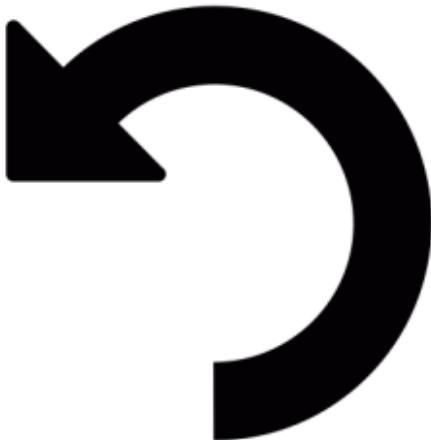
# Recover



Restore backup

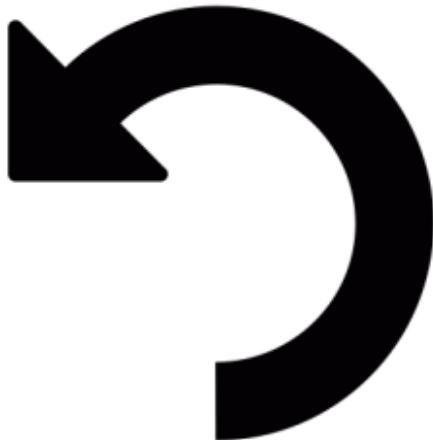
Defensomania

# Recover



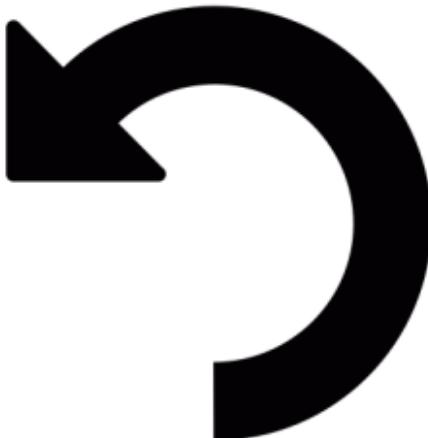
**Bring the service online which you took offline during the incident**

# Recover



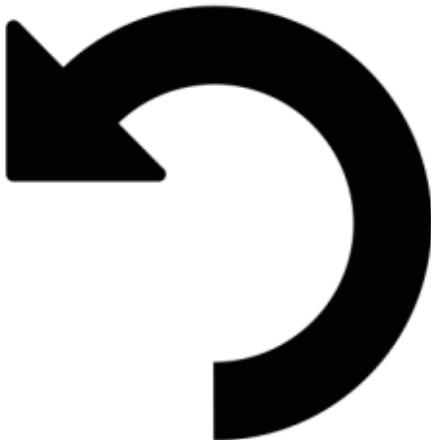
Rotate API keys for a compromised account

# Recover



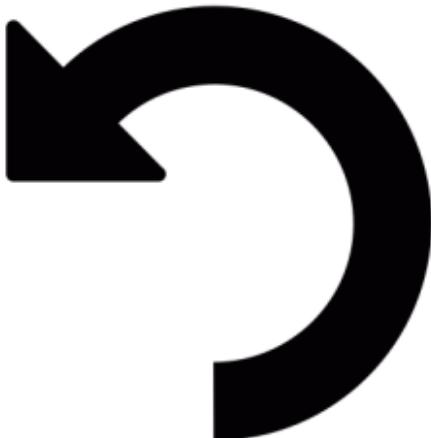
Change credentials for a compromised service account which was disabled during the incident

# Recover



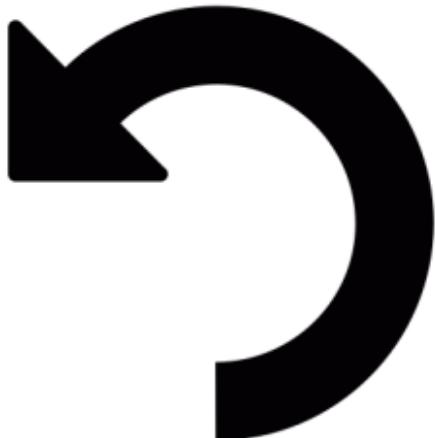
Implement long term monitoring  
through new security monitoring use  
cases and incident response  
processes

# Recover



Add a security deficit to the policy framework

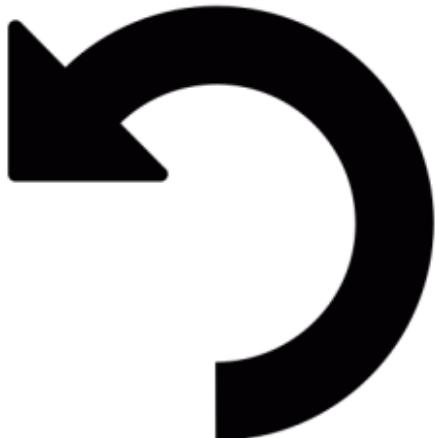
# Recover



Joker - invent a new recover action

Defensomania

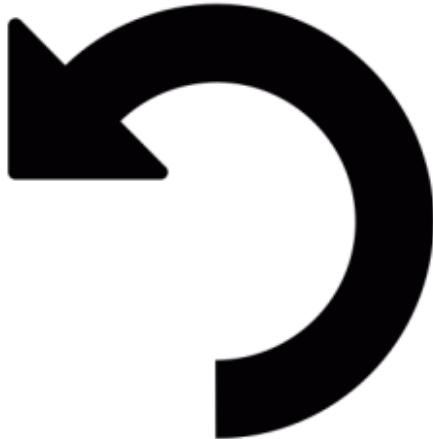
# Recover



Joker - invent a new recover action

Defensomania

# Recover



Joker - invent a new recover action

Defensomania

# Lessons Learned



Organize and perform lessons learned meeting

# Lessons Learned



Define technical debts and report them accordingly

# Lessons Learned



Document results and new knowledge for the team and company

# Lessons Learned



Improve incident response  
processes

# Lessons Learned



Improve incident detection  
capabilities

# Lessons Learned



Add new detection rule to internal  
and external repositories

# Lessons Learned



Joker - invent a new lessons learned step

# Lessons Learned



Joker - invent a new lessons learned step

# Lessons Learned



Joker - invent a new lessons learned step

# Lessons Learned



Joker - invent a new lessons learned step

# Communication



Publish external news article

# Communication



Inform public relations department  
about possible questions from  
outside

# Communication



Communicate findings to  
management

# Communication



Create an incident report

# Communication



Write answer to request made on  
external platform

# Communication



Joker - invent a new communication way

# Communication



Joker - invent a new communication way

# Communication



Joker - invent a new communication way