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

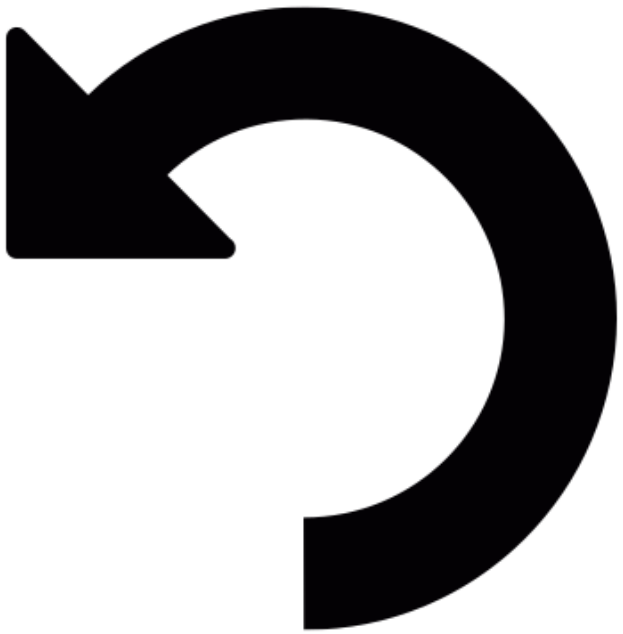
Defensomania

Respond

Joker - invent a new respond action

Defensomania

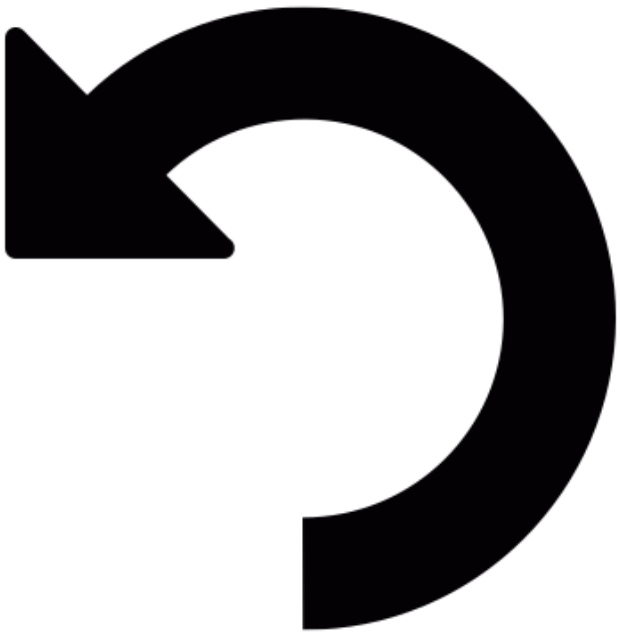
Recover



Initiate fresh installation of compromised system from trusted install sources

Defensomania

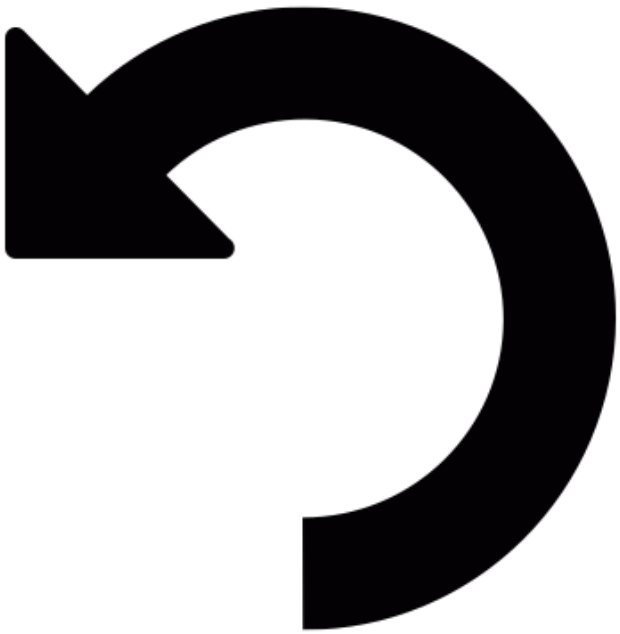
Recover



Initiate the patching of a critical vulnerability

Defensomania

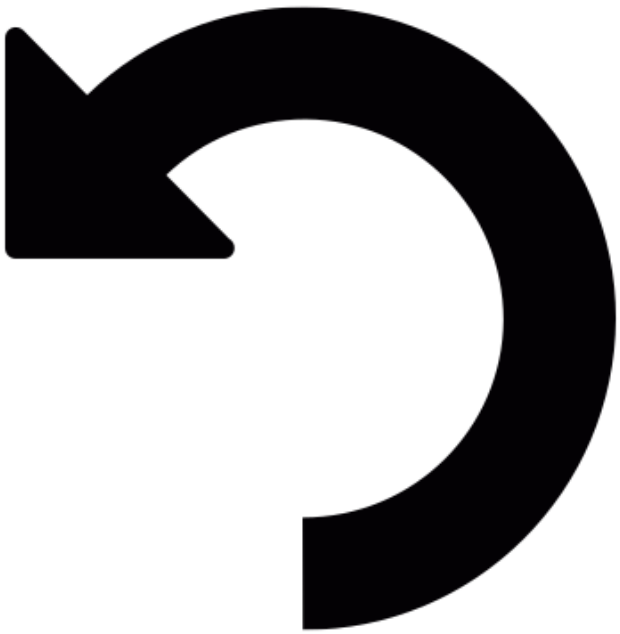
Recover



Initiate an audit on a platform

Defensomania

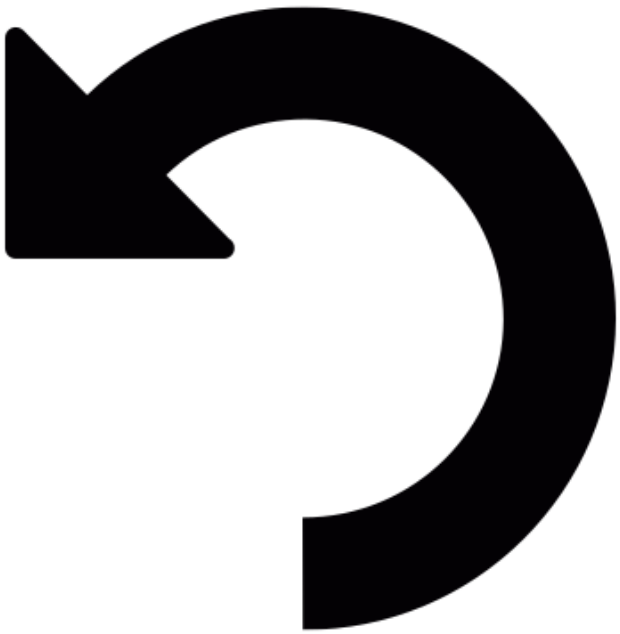
Recover



Restore backup

Defensomania

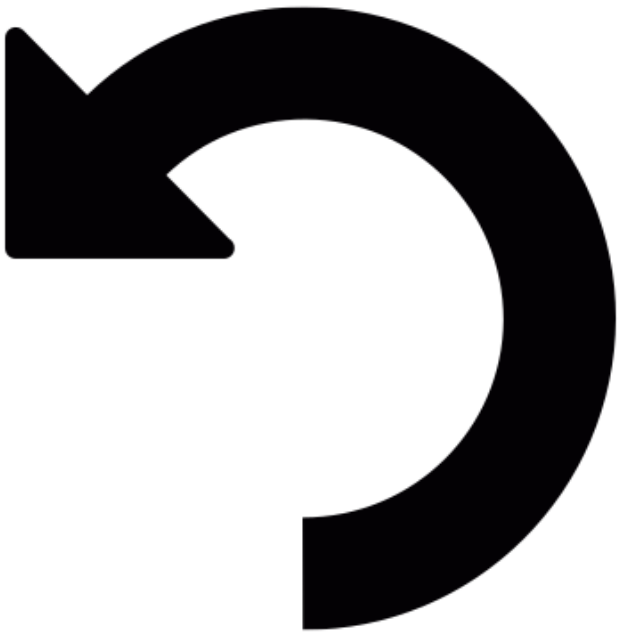
Recover



Bring the service online which you took offline during the incident

Defensomania

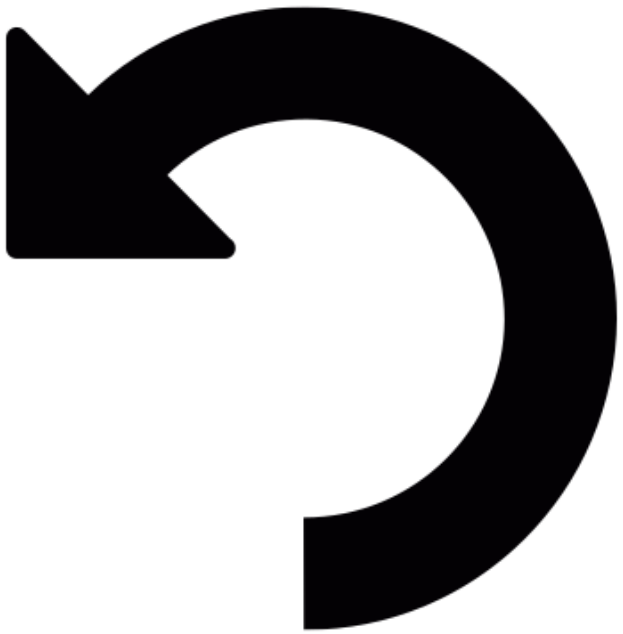
Recover



Rotate API keys for a compromised account

Defensomania

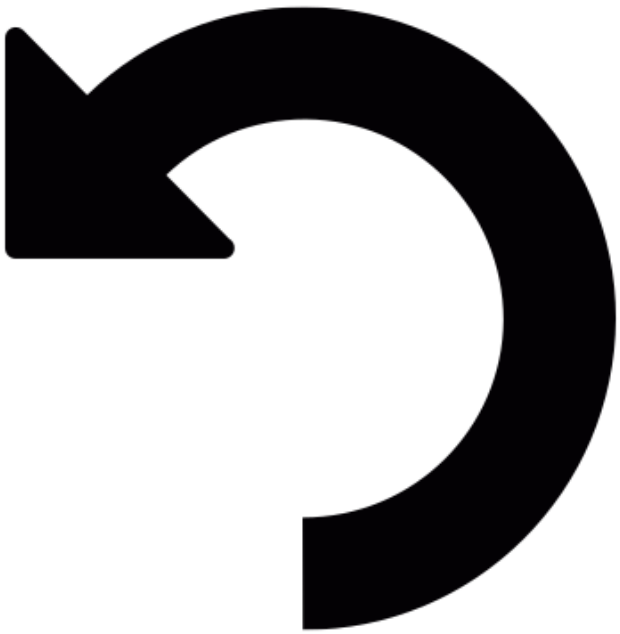
Recover



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

Defensomania

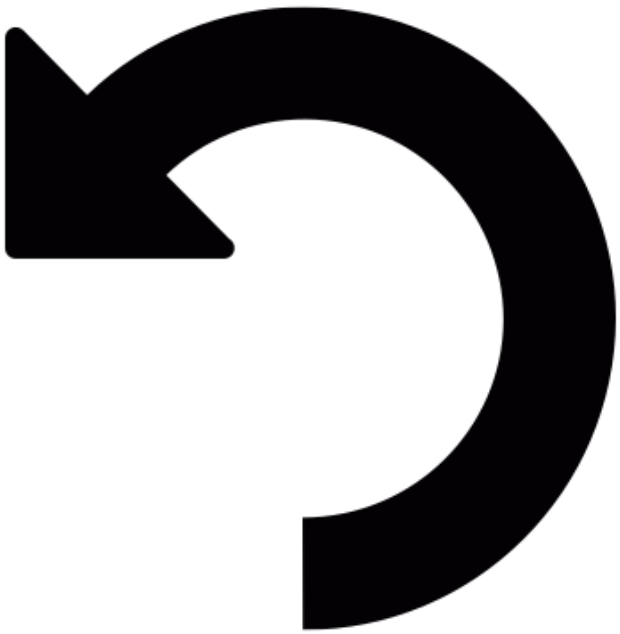
Recover



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

Defensomania

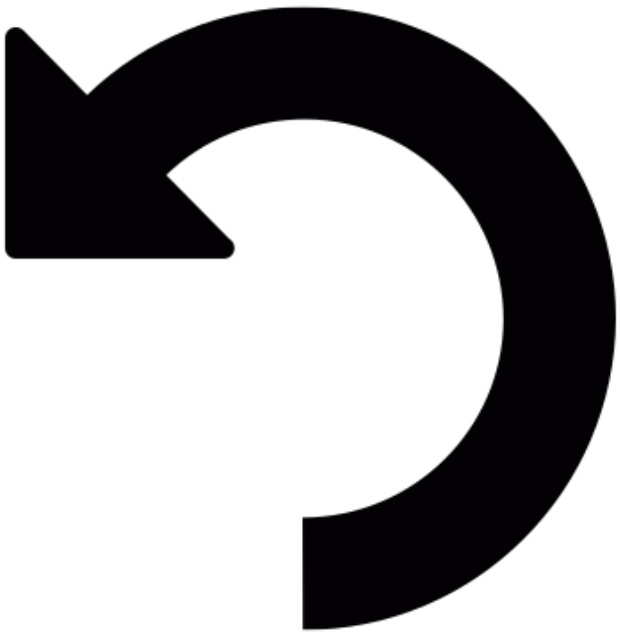
Recover



Add a security deficit to the policy framework

Defensomania

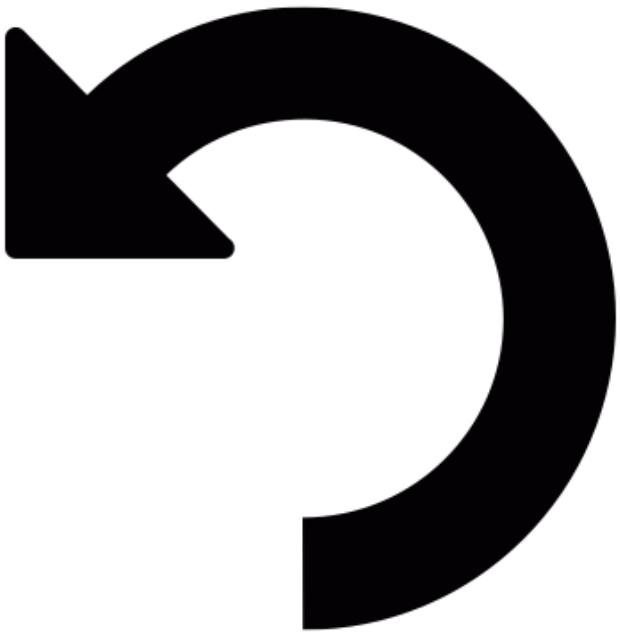
Recover



Joker - invent a new recover action

Defensomania

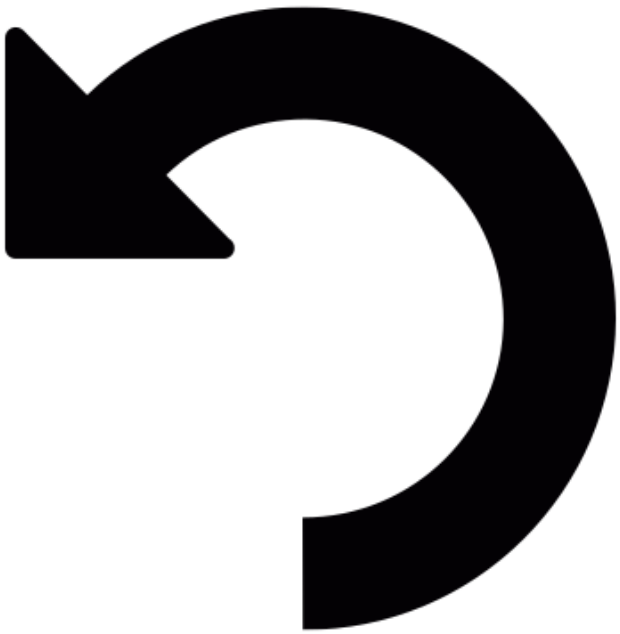
Recover



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

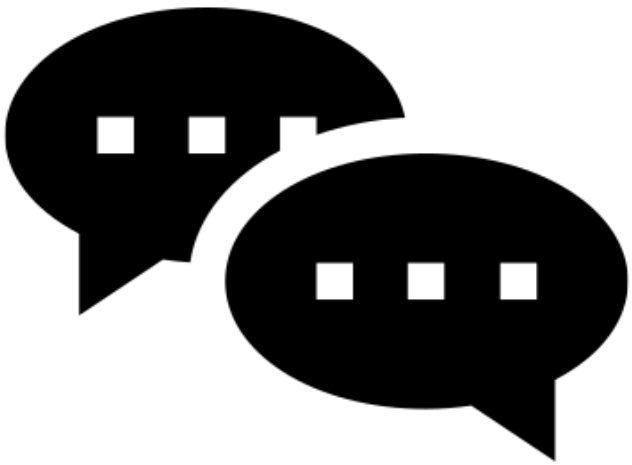
Defensomania

Lessons Learned

Joker - invent a new lessons learned step

Defensomania

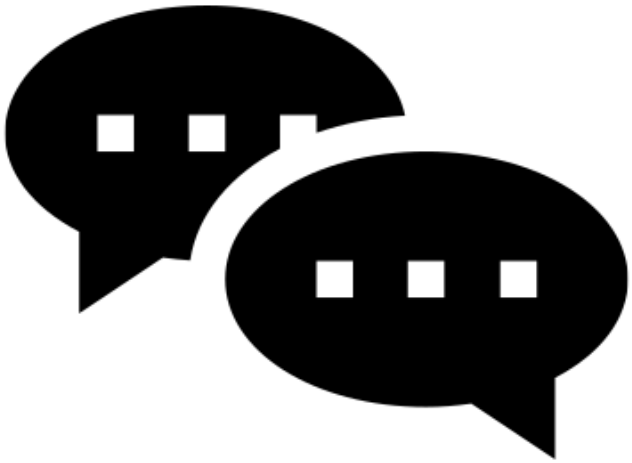
Communication



Publish external news article

Defensomania

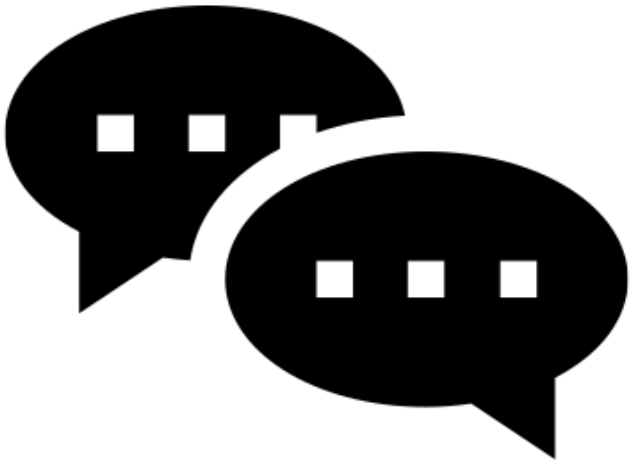
Communication



Inform public relations department about possible questions from outside

Defensomania

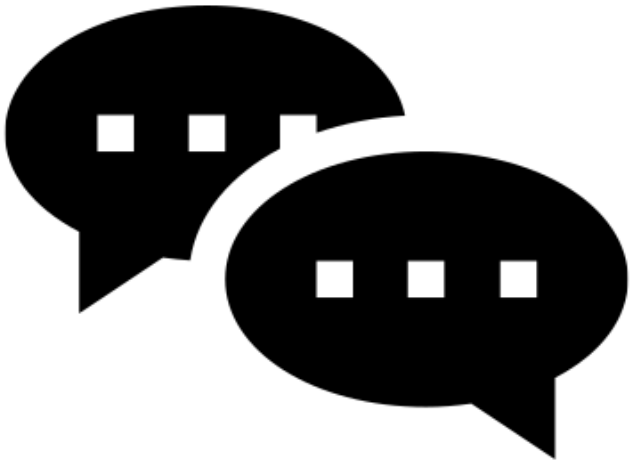
Communication



Communicate findings to management

Defensomania

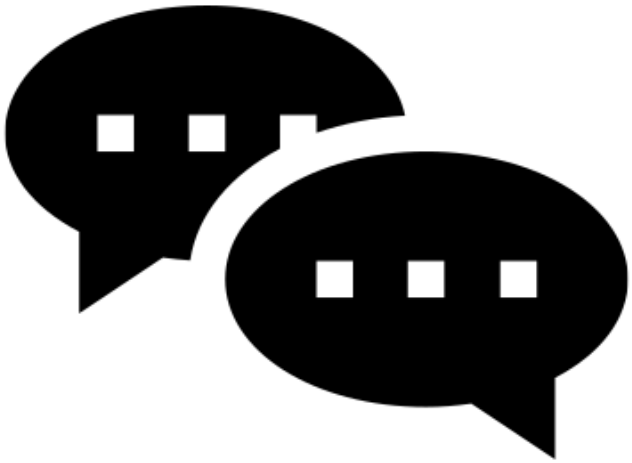
Communication



Create an incident report

Defensomania

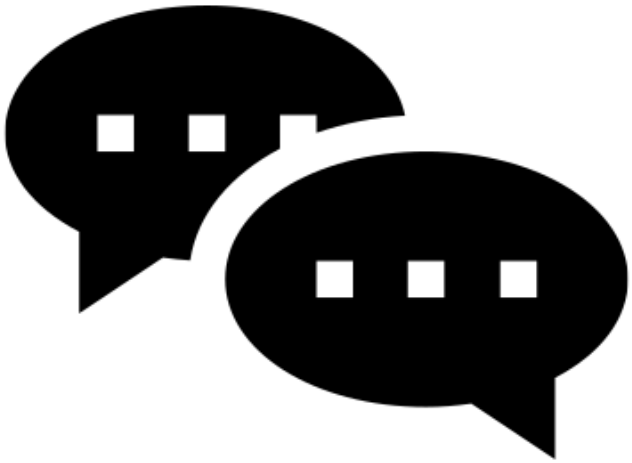
Communication



Write answer to request made on external platform

Defensomania

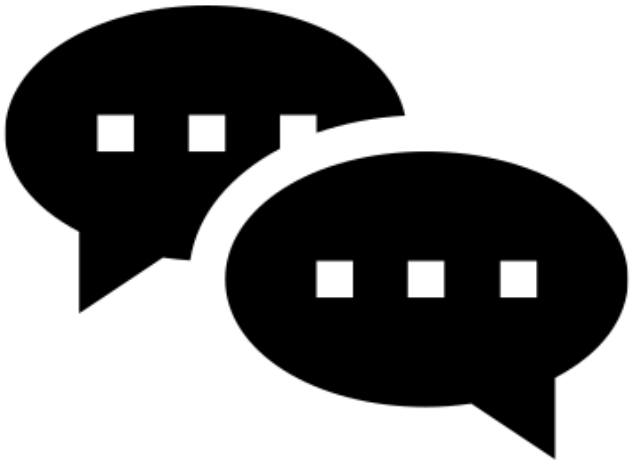
Communication



Joker - invent a new communication way

Defensomania

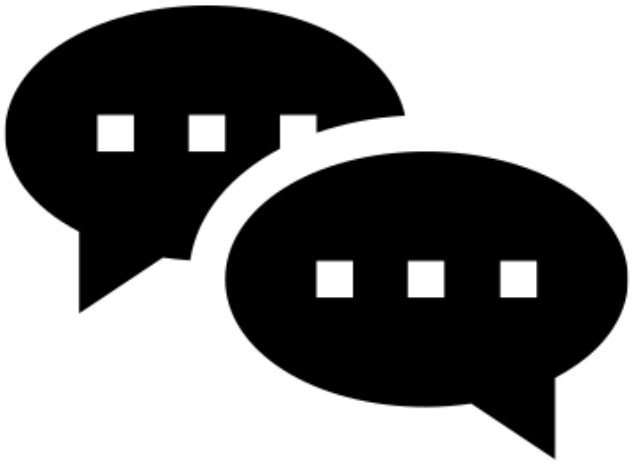
Communication



Joker - invent a new communication way

Defensomania

Communication



Joker - invent a new communication way

Defensomania

Scenario

A supplier of your HRM software was targeted and a backdoored version was distributed. You may already upgraded. Indicators of compromise were published.

Defensomania

Scenario

Your national CERT has published some indicators of compromise for your country and specifically for your industrial sector. Report back if you found hits.

Defensomania

Scenario

Different employee accounts were abused for further attacks against your customers. During initial analysis, you found that all of them visited a typo domain of your corporate portal.

Defensomania

Scenario

An employee's workstation was infected with a banking Trojan which not only changed network settings but also installed email monitoring software. It is related to a recent malvertising campaign.

Defensomania

Scenario

You are notified that one of your ticketing systems is compromised and malware was placed on that server. It connects to other systems reachable from the ticketing server.

Defensomania

Scenario

Spear phishing attack against an employee and employee reports login in into a similar looking company portal.

Defensomania

Scenario

Spear phishing attack against an employee using a malicious document which after it was opened executed code on the computer.

Defensomania

Scenario

Employee downloads a malware through a fake software package which connects back to command and control servers using DNS.

Defensomania

Scenario

Vulnerability was exploited on one of your servers and an attacker had access to the database with customer data. A increased bandwidth was registered on the network device.

Defensomania

Scenario

A database with customer data was exposed to the Internet through a misconfigured firewall and someone on Twitter is leaking data from that database.

Defensomania

Scenario

A public git repository leaked internal credentials and it's unclear whether the credentials were already abused.

Defensomania

Scenario

Servers from your main online service were targeted by a DDoS and are unavailable.

Defensomania

Scenario

Malicious code was distributed to your endpoints during the routine update of a signed application.

Defensomania

Scenario

A domain admin has run a malicious attachment after loudly proclaiming how dumb their users are for doing the same.

Defensomania

Scenario

Security company has released an APT group PDF at BH USA. The list of IOCs includes a host in your ASN.

Defensomania

Scenario

Every night new corporate accounts are abused for sending spam.

Defensomania

Scenario

Email infrastructure got compromised. Attackers have full access to your mailboxes.

Defensomania

Scenario

Attackers got domain admin in your environment. Backdoor accounts were created and disk encryption software was activated?

Defensomania

Scenario

An adversary has access to your Jenkins server.

Scenario

An adversary has access to your vulnerable Jenkins server. Jenkins jobs with credentials are visible to everyone.

Defensomania

Scenario

Someone is impersonating you to customer support at one of your service provider.

Defensomania

Scenario

Your DNS was modified to respond with an attacker's DKIM key.

Defensomania

Scenario

Due to a botched CI/CD script, complete source code exposure on production.

Defensomania

Scenario

A bug in your webapp has allowed every record to be accessed via URL enumeration and IDOR.

Defensomania

Scenario

Your subscription database is hacked. Thousands of new accounts are added and hard to distinguish from old.

Defensomania

Scenario

New paste on a public paste site was found with password hashes and emails from your customer DB from 3 years ago. More recent hashes are missing.

Defensomania

Scenario

Your reception software has leaked all of your visitor logs. They are available via torrent.

Defensomania

Scenario

A script has been logging exported variables containing full user registration objects. This logging method is full of plaintext passwords.

Defensomania

Scenario

Joker - be evil and invent a new nightmare and worst case scenario. What scenario will get your team struggling? (If you want to get crazy then contribute your scary scenario for the sake of humanity.)

Defensomania

Scenario

Joker - be evil and invent a new nightmare and worst case scenario. What scenario will get your team struggling? (If you want to get crazy then contribute your scary scenario for the sake of humanity.)

Defensomania

Scenario

Joker - be evil and invent a new nightmare and worst case scenario. What scenario will get your team struggling? (If you want to get crazy then contribute your scary scenario for the sake of humanity.)

Defensomania

Scenario

A developer has just typo'd an upstream package installation to their laptop. There was a malicious package waiting for that typo and post-installation code is exfiltrating data.

Defensomania

Scenario

An engineer has typo'd a package they are adding to a product repository. It is malicious. The CI/CD and prod environment variables are exfiltrated to a C&C

Defensomania

Scenario

A malicious browser extension was installed on different corporate computers. It injects keyloggers into websites.

Defensomania

Scenario

Your software build imports from an employee's personal NPM package. The employee quits and vandalizes the package, causing a public incident.

Defensomania

Scenario

An adversary takes control of your MDM service account. Your MDM support team cannot be reached for account recovery.

Defensomania

Scenario

Your DNS was modified to respond with an attacker's DKIM key. Spearphishes will be signed by your domain in 30 minutes.

Defensomania

Scenario

The certificates involved with your primary code signing process have been compromised and used to sign malicious apps.

Defensomania

Scenario

An employee has left a firewall rule wide open after several hours of troubleshooting a network issue.

Defensomania

Scenario

An employee has left a firewall rule wide open after a faulty change request was implemented. Bruteforcing attempts were registred on previously protected servers.

Defensomania

Scenario

You allow customers to upload sensitive information to your platform to share them with others. However, the data was left unprotected and anyone could access and download the content.

Defensomania

Scenario

You were informed that one of your website directories used to share files with external parties were accessible and writable by any anonymous user. Suspicious files were found.

Defensomania

Scenario

You were informed that your MDM solution was compromised and over 75% of your employee's mobile devices are infected with malware.

Defensomania

Scenario

You were informed that your firewalls were compromised and malware was executed on these devices to steal information.

Defensomania