Incident Response Playbook

Author: Sushmita Paul
Advisor: Jose Sierra
Course Number: CY 5010
Program Name: Master of Science in Cybersecurity
Course Name: Foundation of Information Assurance
November 27, 2019

Abstract

An incident response plan is an organized approach to address and manage the aftermath of a security breach or cyberattack called as security incident. The goal of the plan is to limit the damage and reduce the recovery time and costs. The incident response activities are performed by group of information security staff and C-suite level members of the organization called as computer security incident response team (CSIRT). This incident response team follows the organization's incident response playbook which consists of set of written instructions that outline the organization's response to network events and security incidents called as incident response plan. Incident response plan helps the team to respond to the incident quickly which will help an organization to minimize the losses; mitigate exploited vulnerabilities; restore services and processes; and reduce the risks that future incidents pose.

Introduction

Incident Response Playbook consists of set of rules and detailed procedures planned to deal with the security related incidents. Playbooks are designed to facilitate effective and appropriate action during an incident to minimize the impact of any cybersecurity incident. It mentions the incident response steps and procedures for investigations which need to be followed systematically to meet and comply with regulatory frameworks. This paper contains the instructions for identifying, notifying, analyzing, containing and recovering from some of the cyber security threats which help to mitigate the effect as below:

1. Identification - It is required to gather indicators of compromise (IoC) which are the forensic data like data found in system log entries that CSIRT team can use to track down threats on the system and network. By monitoring the indicators of compromise, organizations can detect attacks and act quickly to prevent breaches from occurring or limiting the damages by stopping attacks in earlier stages.
2. Notification – It is required to alert the CSIRT who is responsible to perform the incident handling activities. After getting the notification of the incident, the goal of the CSIRT is to minimize and control the damage resulting from incidents, provide effective response and recovery, and work to prevent future incidents from happening.
3. Analysis – The analyst is responsible to rapidly address the security incident to know the root cause and thus, help in improving incident handling procedures. Guidelines in this part will consists of instructions which will guide the analysts with steps to conduct forensic analysis of the incident.
4. Containment/Eradication - This include steps which will contain the threat, that is, doesn't cause any further damage and isolate the root cause of the attack. Measures need to be

taken to prevent the incident from recurring or escalating are described in this part of the plan.

5. Recovery – This phase of the plan ensure that affected systems are not in danger and can be restored to working condition. The purpose is to bring the affected systems back into production environment and ensure other incidents will not happen by continuously monitoring the network system.

The network and host controls present at Connected networks which will be used to mitigate the security incidents are as below:

1. Perimeter Firewall on the network egress points.
2. Intrusion Prevention Sensors and Intrusion Detection system on internal network
3. Email Gateway with Antimalware AntiSpam Protection
4. Security Information and Event Management (SIEM - Correlates logs from all security control systems)
5. Load balance before the servers
6. Multiple DNS servers
7. Anti-malware Endpoint Protection (includes Host based firewall and HIPS) on all devices
8. Full Disk Encryption on employee laptops only

Cybersecurity Incidents and Response Plan

Phishing email with malware in attachment

* Identification: Various factors need to be considered as indicators of compromise to identify phishing email with malware attachment as below:

1. Email Header:
    - The email address of the sender which includes the domain name of the email address.
    - Recipient Email Address
    - The subject line of the email.
    - Hostname and IP address of the sender's SMTP server
    - X-Originating IP Address
    - The X-Authenticated-User field
2. E-mail Message:
    - Email Attachment – If the original email has an attachment, a protocol needs to be followed to download it safely. The attachment needs to be collected and stored in a password protected zip file with password "malware". Also, check the kind of attachment.
    - MD5 hashes of the malware attachment
3. Review of DNS logs –
    - Massive spike in the request from a domain which is suspicious.
    - If any domain logs other than company's network present.
    - If the logs contain domains which are in the blacklist of the company.

- When a DNS server issues an NXDOMAIN response which means that the domain name server could not resolve the IP address of that domain. This can mean that someone made a typo when typing the domain, but it could also mean that the domain is malicious and no longer exists.
- If the top level domain is different from the ones which the company is using on daily basis.

4. Alert from the email gateways and perimeter firewall

* Notification: Incident Response Manager needs to be notified first regarding any security incident including this phishing email incident. Incident Response Manager will be responsible to delegate the task within its team of security analyst which also includes overseeing and prioritizing actions during the analysis and containment of the incident. Incident Response Manager needs to report to CISO of the incident so that CISO can monitor the situation. The CISO will be responsible to analyze the company's risk threshold and determine the way to protect the data while supporting the business' objectives.

* Analysis: The security analysts will be able to analyze the severity of the damage by determining the following:

1. Review email transaction logs received from Antimalware and Antispam Protection system in SIEM to know the Total number of impacted employees.
2. Review proxy logs in SIEM to identify total number of users clicked and accessed the phishing email attachment.
3. Integrity of the file needs to be checked by using hashing algorithm to detect if any important files are altered.

To further analyze the incident, following details of the recipients need to be collected:

- Username
- Employee ID
- Email Address
- Department
- Location
- Designation

If the user has opened the attachment, then following steps needs to be taken to further analyze the impact to patch vulnerability, if any and recover the effected computers:

1. Determine the Trojan present in the attachment.
2. Determine the vulnerability, if any, which has been exploited. If known vulnerability, check the CVE name.
3. Determine the way through which the attachment has exploited the vulnerability.
4. Determine the configuration abused.
5. Determine exploit command, or code that was run or injected.
6. Servers and domain names involved.
7. Network Monitoring and scanning to determine the connections sent to servers
8. Loss of sensitive data.
9. Determine the impact on servers, workstations, wireless devices, and the network infrastructure.

If the user has not opened the attachment, then following steps needs to be taken to analyze the impact and block the attack in future:

1. Once saved the file in a password protected zip file, the file should be downloaded and opened in a specific computer isolated from the company's network which is kept for working with the security incidents.
2. Check the contents of the zip before extracting it.
3. Open the file in the text editor to analyze the content of the file and check for the keywords to know the action which will be performed by the attachment.

* Containment/Eradication: The phishing attack needs to be contained before it spreads to other part of the company and therefore, this is the most critical phase of the plan. Following steps needs to be taken immediately based on the scenarios:

1. The username and passwords of the impacted employees need to be changed because once in a network, an adversary may delete or alter data with the aim of disrupting business operations.
2. Send an email to the messaging team to delete phishing email from all impacted users' mailboxes.
3. The login credentials of the people who has access to the resources in the impacted IT infrastructure needs to be changed.
4. If it is the employee laptop, remotely enable the Full Disk Encryption system.
5. Execute the "Remote Wipe" to delete any sensitive data or files from the smartphone or laptop so that it cannot be accessed. Have the employee return the effected smartphone or laptop and issue a new with new login credentials.
6. Continue monitoring all the systems within the IT infrastructure and all user account for any misuse or anomalies. If any of these are detected in any system, the system need to be shut down to conduct more detailed investigation.

7. The sender details need to be shared with the messaging team to block the sender in the email gateway by adding the sender ID in the block list of Antimalware and Antispam protection.
8. Based on the impact assessment, send an email to users not to open or click on email in the questions.
9. Network intrusion prevention systems and Antimalware Protection system are to be modified and designed to scan and remove malicious email attachments.
10. If any software vulnerability is exploited, it is vital to apply patches to the software targeted by the adversaries within 30 days of the incident reported. All types of infrastructure need to be patched, including laptops, mobile devices, desktops, servers, switches and routers so that if a compromised attachment opened, the malware will not be executed.
11. Determine what controls have failed to take the necessary steps to rectify them.

* Recovery: Recovery plans must be taken to ensure all systems are returned to the business operations and locked down all the backdoors that enabled the intrusion. Also, it includes steps needed to guide employees if similar incident happened in the future:

1. Routine testing of the perimeter firewall, network intrusion devices and routers must be done to make sure that the infrastructure is up to date.
2. Preserve affected system log files such as firewall, VPN, mail, network, client, web, server, and intrusion detection system logs
3. Keep monitoring the DNS logs to check if any host on the network looked up on the infected server.
4. Train employees to act on such kind of attacks.

5. Incident response manager will prepare an investigation report and will share it with the CISO and CIO to review to ensure everything was documented in the report.
6. CSIRT will prepare a lesson learned report which will contain the current security gaps and share it with leadership.
7. The technological or procedural changes in incident response plan must be updated if required and shared with the team.

Phishing email with credential harvesting web link

* Identification**:** Various factors need to be considered as indicators of compromise to identify the phishing email with malware in attachment:

1. Email Header:
    - The email address of the sender which includes the domain name of the email address.
    - Recipient Email Address
    - The subject line of the email.
    - Hostname and IP address of the sender's SMTP server
    - X-Originating IP Address
    - The X-Authenticated-User field
2. E-mail Message:
    - URL in the email body – A slight variation in the URL or a suspicious domain name will be an indicator. Also, check for the URL features and if the URL is present in the blacklist.
3. Review of DNS logs –
    - Massive spike in the request from a domain which is suspicious.
    - If any domain other than company's network is present.
    - If the logs contain domain names which are in the blacklist of the company.
    - When a DNS server issues an NXDOMAIN response which means that the domain name server could not resolve the IP address of that domain. This can mean that someone made a typo when typing the domain, but it could also mean that the domain is malicious and no longer exists.

- If the top level domain is different from the ones which the company is using on daily basis.

4. Alert from the email gateways and perimeter firewall

* Notification: Incident Response Manager needs to be notified first regarding any security incident including this phishing email incident. Incident Response Manager will be responsible to delegate the task within its team of security analyst along with overseeing and prioritizing actions during the analysis and containment of the incident. Incident Response Manager needs to report to CISO of the incident so that CISO can monitor the situation. The CISO will be responsible to analyze the company's risk threshold and determine the way to protect the data while supporting the business' objectives.

* Analysis: The security analysts will be able to analyze the severity of the damage by determining the following:

1. Review email transaction logs from Antimalware and Antispam Protection system in SIEM to know the Total number of impacted employees.
2. Review proxy logs in SIEM to identify total number of users clicked and accessed the URL.

To further analyze the incident, following details of the recipients need to be collected:

- Username
- Employee ID
- Email Address
- Department
- Location
- Designation

Following steps needs to be taken to analyze the root cause of the incident along with the impact on the company and its employees:

1. Analyze the URL based on the lexical features and host based features.
2. Use VM isolated from the organization's network and an isolated proxy server to investigate on the malicious URL which can lead to a spoofed website to determine the way the credentials are harvested and where the data on the website is posted by determining the TCP/IP address of the web server that hosts the spoofed website.
3. Query the URL with multiple user agents or querying the site with different source IP addresses using URL scanner.
4. Network Monitoring and scanning to determine the connections sent to servers while harvesting the credentials.
5. Loss of the sensitive data and files.
6. Determine the configuration abused.
7. Determine exploit command, or code that was run or injected.
8. Servers and domain names involved.

* Containment/Eradication: The phishing attack needs to be contained before it spreads to other part of the company and therefore, this is the most critical phase of the plan. Following steps needs to be taken immediately based on the scenarios:

1. The username and passwords of the impacted employees need to be changed immediately and confirm if the passwords are changed.
2. Block all the accesses of impacted employees in case the credentials are not allowed to change due to the activity by the malicious URL.
3. If it is the employee laptop, remotely enable the Full Disk Encryption system.

4. Since the files are backed up, execute the “Remote Wipe” to delete all the sensitive data or files from the laptop and computer.
5. If the impacted points are smartphones, execute the “Remote Wipe” to delete any sensitive data or files from the smartphone so that it cannot be accessed. Have the employee return the effected smartphone and issue a new with new login credentials.
6. Send an email to the messaging team to delete phishing email from all impacted users’ mailboxes and to block the sender in the email gateway by adding the sender ID in the block list of Antimalware and Antispam protection.
7. The login credentials of the people who has access to the resources in the impacted IT infrastructure needs to be changed.
8. Discover all the machines operated in the environment to register and vault shared, alternate-admin, service accounts, and secrets.
9. If the current URL is found to be malicious and not blocked, then initiate a block request.
10. If the IP address is blacklisted and not blocked, initiate an IP address block request.
11. Continue monitoring all the systems within the IT infrastructure and all user account for any misuse or anomalies. If any of these are detected in any system, the systems need to be shut down to conduct more detailed investigation.
12. Based on the impact assessment, send an email to users not to open or click on email in the questions.
13. Network intrusion prevention systems and Antimalware Protection systems are to be designed to scan and remove malicious emails.
14. If any software vulnerability is exploited, it is vital to apply patches to the software targeted by the adversaries. All types of infrastructure need to be patched, including laptops, mobile

devices, desktops, servers, switches and firewalls so that if a compromised attachment opened, the malware will not be executed.

15. Determine what controls have failed to take the necessary steps to rectify them.

* Recovery: Recovery plans must be taken to ensure all systems are returned to the business operations and locked down all the backdoors that enabled the intrusion. Also, it includes steps needed to guide employees if similar incident happened in the future:

1. Routine testing of the perimeter firewall, network intrusion devices and firewalls must be done to make sure that the infrastructure is up to date.
2. Preserve affected system log files such as firewall, VPN, mail, network, client, web, server, and intrusion detection system logs.
3. Keep monitoring the logs to search the DNS logs to check if any host on the network looked up on the infected server.
4. Educate employees about the risk of phishing and the characteristics of these attacks. Train them to determine if the link is malicious by hovering over the link if the domain on that matches with what is displayed.
5. Enforce session auditing and monitoring.
6. Although company has already enforced least access privilege, make sure to check the privileges for all the employees.
7. Incident response manager will prepare an investigation report and will share it with the CISO and CIO to review to ensure everything was documented in the report.
8. CSIRT will prepare a lesson learned report which will contain the current security gaps and share it with leadership.

9. The technological or procedural changes in incident response plan must be updated if required and shared with the team.

Lost laptop incident from an employee

* Identification**:** Stolen laptop reported by an employee is the first indicator of compromise in this situation. CSIRT need to look for the indicators of loss of company data through the stolen laptop. Following factors should be considered as Indicators of Compromise (IoS) for stolen data:

1. SIEM Logs of successful login in the stolen laptop.
2. Presence of IP addresses not associated with the company network in the SIEM logs along with the source and destination address.
3. Record of privilege escalation on the SIEM logs.
4. Detection of anomalies by the perimeter firewall while monitoring data packets between the outside network and inside network.
5. Detection of anomalies by the intrusion prevention sensors while monitoring data packets on internal networks.
6. Login attempts done on the stolen laptop from a foreign IP address.
7. Peak in the network traffic to the device in question.

* Notification**:** The employee should report the loss of laptop to their manager. The manager should involve human resource, and incident response manager. Incident Response Manager will delegate the work of monitoring and disabling access to the laptop to the security analysts. Human resource department will be responsible for disabling the employee's network access until it receives a clearance by incident response manager and provide new credentials to the employee after the clearance. Incident Response Manager needs to report to CISO of the incident so that CISO can monitor the situation. The CISO will be responsible to analyze the company's risk threshold and determine the way to protect the data while supporting the business' objectives.

* Analysis**:** It is important to monitor the data theft from the stolen laptop which will be performed by the security analysts. As soon as loss of laptop is reported, access to the laptop should be disabled remotely and steps need to be taken to track the laptop. Below given steps should be carried out in case of data theft to know the impact and root cause of suspicious activities, if any:

1. Determine the protective security measures present in the stolen laptop
2. Identify the specific intellectual property like source code, design documents on the stolen laptop and if these are encrypted or unencrypted to determine the level of actions required.
3. Identify types of data exposed to determine if any company regulations are violated.
4. Monitoring inbound and outbound network connections.

* Containment/Eradication: The impact of the stolen laptop can be minimized by following the below steps:

1. Execute the "Remote Wipe" to delete any sensitive data or files from the lost laptop so that it cannot be accessed.
2. Track the laptop using the tracking device mounted on the laptop.
3. Change the credentials of the employee.
4. Disable all the network access of the employee.
5. Remotely log out of the employee mailbox so that the attacker won't be able to access the sensitive information in the mailbox.
6. The attacker can access the shared folders, file and location if the password is compromised and the impact can be reduced by changing the password of all shared locations and files.
7. Send a mail to all the employees of the company to change their password so that even if the attacker gets the credentials of the administrator or any employee, it wouldn't be able to use that account to steal data.

8. If data is not encrypted and not able to delete the data as instructed in the step 1, remotely enable the Full Disk Encryption system of the employee laptop and change the encryption key.

Below given steps need to be taken to eradicate data theft due to stolen laptops:

1. Employee need to be trained to use single and very strong password.
2. Employ strong multifactor authentication on all the laptop of the company.
3. Train the employees to back up all the data in the password protected folder in shared network of the company on daily basis.
4. Adopt a least privilege policy on the outside network, that is employee should not be allowed to access a shared folder when on the network outside the company.
5. Employee awareness and education regarding the penalties for employee noncompliance and workforce training in basic security techniques.
6. Keep all the confidential data in the shared location of the company network instead of the laptop.
7. Conduct risk assessment in monthly basis.

* Recovery**:** Recovery plans must be taken to ensure all systems are returned to the business operations and locked down all the backdoors that enabled the intrusion. Also, it includes steps needed to guide employees if similar incident happened in the future:

1. Back up of all the data and source code need to be checked and protected by strong password if not done yet.
2. Preserve affected system log files such as firewall, VPN, mail, network, client, web, server, and intrusion detection system logs.

3. Routine testing of the perimeter firewall, network intrusion devices and routers must be done to make sure that the infrastructure is up to date.
4. Train employee regarding strong password ethics and multifactor authentication.
5. Enforce session auditing and monitoring.
6. Although company has already enforced least access privilege, make sure to check the privileges for all the employees.
7. Incident response manager will prepare an investigation report and will share it with the CISO and CIO to review to ensure everything was documented in the report.
8. CSIRT will prepare a lesson learned report which will contain the current security gaps and share it with leadership.
9. The technological or procedural changes in incident response plan must be updated if required and shared with the team.

System alert for USB inserted on employee machine

USB device can be inserted by a legitimate employee or by an attacker to harm the company's business. As per company's norm, popup is displayed on laptop/computer whenever any USB device is inserted to alert the legitimate employee and notification will be sent to the administrator of the specific department. If the legitimate employee will remove the USB device as instructed in the popup, the alert system will again notify the administrator regarding the removal of the USB device.

* Identification**:** The Antimalware Endpoint Protection system includes the host based firewall which will alert the administrator of the specific department whenever USB mass storage media is inserted or removed from any computer/laptop of the company. The alert from the HIDS is the indicator of compromise in this situation. The administrator should report the incident to the incident response manager to further track USB file writes to indicate possible data theft. CSIRT should monitor the SIEM logs for all the actions performed on the computer with the USB.

* Notification: The administrator of the respective department will receive the notification first which will be reported to the incident response manager. Incident response manager will delegate work to the security analyst to track and analyze the impact of the incident.

* Analysis: Inserting a USB device can lead to data theft which needs to be tracked and monitored for impact and further steps. Following actions should be monitored to get to root cause of any issues due to the insert of USB:

1. Monitor and save the SIEM logs generated by the endpoint protection system (as it contains the firewall and the intrusion prevention system) installed in the devices for the actions performed with the USB device.

2. Monitor the perimeter firewall for outgoing and incoming communications.
3. Scan the computer/laptop for trojans and viruses by using Antivirus packaged in Antimalware Protection system.
4. Monitor the DNS logs for IP addresses different from the computer network.
5. Check the hashes of the files and folders and compare it with the saved hashes of the original files and folders.

* Containment/Eradication: Steps followed in this process will be dependent on the actions performed by using the USB media device which is as below:

1. If the logs show copy of a sensitive data into the USB, execute "remote wipe" to delete all the sensitive data or files and revoke all the access of the employee.
2. If the logs show the outgoing and incoming communications with an IP address different from the computer's network, block all the outgoing and incoming communications to the device in question.
3. If the logs show execution of a code, execute "remote wipe" to delete all the sensitive data or files and revoke all the access of the employee.
4. Remotely change the credentials of the employee.
5. If the logs show any malicious activity performed, laptop should be submitted to the security analyst for further forensic of the laptop/computer by isolating it from the network of the computer.
6. If data is not encrypted and not able to delete the data as instructed in the step 1, remotely enable the Full Disk Encryption system of the employee laptop and change the encryption key

* Recovery**:** Recovery plans must be taken to ensure all systems are returned to the business operations and locked down all the backdoors that enabled the intrusion. Also, it includes steps needed to guide employees if similar incident happened in the future:

1. Preserve affected system log files such as firewall, VPN, mail, network, client, web, server, and intrusion detection system logs.
2. Routine testing of the perimeter firewall, network intrusion devices and routers must be done to make sure that the infrastructure is up to date.
3. Although company has already enforced least access privilege, make sure to check the privileges for all the employees.
4. Incident response manager will prepare an investigation report and will share it with the CISO and CIO to review to ensure everything was documented in the report.
5. CSIRT will prepare a lesson learned report which will contain the current security gaps and share it with leadership.
6. The technological or procedural changes in incident response plan must be updated if required and shared with the team.

Ransom note received in email with threat of DDOS attack on company

* Identification**:** In this situation, the compromise has not happened yet, but the note is the indicator of the upcoming threat. Since the team already know about the incoming threat, steps can be taken to prevent the attack. In case the DDoS attack, following would be the Indicators of Compromise:

1. Slow network traffic
2. Poor performance
3. Excessive processor usage
4. Failure of the service

* Notification**:** CISO has already been notified about the incident through the ransom note who will pass this information to the senior manager, CIO and incident response manager to analyze on the situations. Incident response manager will work with its team of security analyst and operations team lead to prevent the DDoS attack on the company network. The CISO will be responsible to analyze the company's risk threshold and determine the way to protect the data while supporting the business' objectives. Incident Response Manager needs to report to CISO of the incident so that CISO can monitor the situation.

* Analysis**:** Security analyst will analyze the company's infrastructure and network configuration which is listed below to prevent DDOS attack. In case of any missing configurations, the analyst should take appropriate steps to prevent or minimize the impact of DDOS attack.

1. The load balancing of the system of the company to distribute the traffic is good.
2. The perimeter firewall should be configured to drop incoming ICMP packets or block DNS responses from the network outside the network. This will prevent certain DNS and ping-based volumetric attacks.

3. Ensure that intrusion detection sensors, intrusion prevention sensors, and perimeter firewall is updated.
4. Ensure that the network architecture of the company is in place which includes the multiple DNS servers.
5. Use the bandwidth of the server available to the company when required.

In case the attack takes place, following steps should be taken to monitor the attack progression which will help to prevent the attack:

1. Type of DDoS attack
2. Characteristics of the attack
3. Check if the attack is coming from single IP source or multiple source.
4. Check for the attack pattern like if it is single sustained flood or burst attack.
5. Check if the attack includes the encrypted traffic or protocols.

* Containment/Eradication**:** If the DDoS attack happens, following steps needed to be taken to minimize the impact of the attack.

1. Ensure that the half-open connections are timed out more aggressively.
2. Ensure to drop spoofed or malformed packages.
3. Set the threshold of SYN, ICMP, and UDP flood drops.
4. The traffic to the network of the company should be rerouted to the mitigation center where it is scrubbed, and legitimate traffic is then forwarded to the organization.
5. If the DDoS attack happened after all the prevention, the DDoS defenses needs to be upgraded which includes the configuration of the firewall, intrusion detection system, and intrusion prevention devices.

* Recovery**:** Recovery plans must be taken to ensure all systems are returned to the business operations and locked down all the backdoors that enabled the attack. Also, it includes steps needed to guide employees if similar incident happened in the future:

1. Thorough inventory of all the system
2. Orderly restoration of the firewalls and all other appliances.
3. Reconnect the customer session in a strategic way.
4. Preserve affected system log files such as firewall, VPN, mail, network, client, web, server, and intrusion detection system logs.
5. Incident response manager will prepare an investigation report and will share it with the CISO and CIO to review to ensure everything was documented in the report.
6. CSIRT will prepare a lesson learned report which will contain the current security gaps and share it with leadership.
7. The technological or procedural changes in incident response plan must be updated if required and shared with the team.

References

1. NIST Computer Security Incident Handling Guide - https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf

2. Incident Response Playbook - https://www.scip.ch/en/?labs.20190103

3. Public Power Cyber Incident Response Playbook - https://www.publicpower.org/system/files/documents/Public-Power-Cyber-Incident-Response-Playbook.pdf

4. Phishing Email - https://www.cpni.gov.uk/system/files/documents/87/93/spear-phishing-understanding-the-threat.pdf

5. Phishing Email Defense - https://www.ciosummits.com/PhishMe-Phishing-Defense-Guide_2017.pdf

6. Denial of Service - https://fedvte.usalearning.gov/courses/RCA/course/videos/pdf/FIM_D03_S04_T02_STEP.pdf

7. Recover from Denial of Service - https://www.imperva.com/blog/recover-aftermath-ddos-attack/

8. Spotting Data Breach - https://www.itspmagazine.com/from-the-newsroom/spotting-the-breach-what-are-the-indicators-of-compromise

9. DDOS Countermeasures - https://blog.radware.com/security/ddosattacks/2019/10/what-to-do-when-you-are-under-ddos-attack/