Review the scenario below. Then complete the step-by-step instructions.

You are a cybersecurity analyst working for a multimedia company that offers web design services, graphic design, and social media marketing solutions to small businesses. Your organization recently experienced a DDoS attack, which compromised the internal network for two hours until it was resolved.

During the attack, your organization's network services suddenly stopped responding due to an incoming flood of ICMP packets. Normal internal network traffic could not access any network resources. The incident management team responded by blocking incoming ICMP packets, stopping all non-critical network services offline, and restoring critical network services.

The company's cybersecurity team then investigated the security event. They found that a malicious actor had sent a flood of ICMP pings into the company's network through an unconfigured firewall. This vulnerability allowed the malicious attacker to overwhelm the company's network through a distributed denial of service (DDoS) attack.

- **To address this security event, the network security team implemented:**
- **A new firewall rule to limit the rate of incoming ICMP packets**
- **Source IP address verification on the firewall to check for spoofed IP addresses on incoming ICMP packets**
- **Network monitoring software to detect abnormal traffic patterns**
- **An IDS/IPS system to filter out some ICMP traffic based on suspicious characteristics**

As a cybersecurity analyst, you are tasked with using this security event to create a plan to improve your company's network security, following the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF). You will use the CSF to help you navigate through the different steps of analyzing this cybersecurity event and integrate your analysis into a general security strategy. We have broken the analysis into different parts in the template below. You can explore them here:

- **Identify security risks through regular audits of internal networks, systems, devices, and access privileges to identify potential gaps in security.**
- **Protect internal assets through the implementation of policies, procedures, training and tools that help mitigate cybersecurity threats.**
- **Detect potential security incidents and improve monitoring capabilities to increase the speed and efficiency of detections.**
- **Respond to contain, neutralize, and analyze security incidents; implement improvements to the security process.**
- **Recover affected systems to normal operation and restore systems data and/or assets that have been affected by an incident.**

section 1 : summerise the security event:
provide a summary of the security event that occurred. Include information about the security event, its cause, the impact, and the response. You can also include information about targeted systems, the attack source, and the estimated impact.

section 2 :identify the type of attacks and the systems effected:
Think about all of the concepts covered in the course so far and reflect on the scenario and define what

type of attack occurred and which systems were affected. List this information in the incident report analysis worksheet in the section titled “Identify.”

section 3:protect the assets in your organization being compramised.
Next, you will assess where the organization can improve to further protect its assets. In this step, you will focus on creating an immediate action plan to respond to the cybersecurity incident. When creating this plan, reflect on the following question:

What systems or procedures need to be updated or changed to further secure the organization’s assets?

Write your response in the incident report analysis template in the “Protect” section.

section 4: detect similar incidents in the future:
It is important to continuously monitor network traffic on network devices to check for suspicious activity, such as incoming external ICMP packets from non-trusted IP addresses attempting to pass through the organization’s network firewall.

For this step, consider ways you and your team can monitor and analyze network traffic, software applications, track authorized versus unauthorized users, and detect any unusual activity on user accounts. Write your response in the incident response analysis worksheet in the “Detect” section.

section 5: response to future cyber security incidents:
After identifying the tools and methods you and your organization have in place for detecting potential vulnerabilities and threats, create a response plan in the event of a future incident. This typically happens after the incident occurred and has been resolved by you and your team. In this case, you will create a response plan for future cybersecurity incidents. Some items to consider when creating a response plan to any cybersecurity incident:

- How can you and your team contain cybersecurity incidents and affected devices?
- What procedures are in place to help you and your team neutralize cybersecurity incidents?
- What data or information can be used to analyze this incident?
- How can your organization’s recovery process be improved to better handle future cybersecurity incidents?

Write your response in the incident report analysis template under the “respond” section.

section 6: Recover from the incident :
Consider what steps need to be taken to help the organization recover from the cybersecurity incident. Reflect on all the information you gathered about the incident in the previous steps to consider which devices, systems, and processes need to be restored and recovered.

Consider the following questions:

- **What information do you need to be able to recover immediately?**
- **What processes are in place to help the organization recover from the incident?**
- **Write your response in the “recover” portion of the worksheet.**

Be sure to address the following in your completed activity.

Course 3 incident report analysis

- Summarize the security event
- Identifies the type of attack and the systems impacted by the incident
- Offers a protection plan against future cybersecurity incidents
- Describes detection methods that can be used to identify potential cybersecurity incidents
- Includes a response plan for the cybersecurity incident and outline for future cybersecurity incidents
- Outlines recovery plans you and the organization can implement in future cybersecurity incidents.

Applying the NIST CSF

Earlier in this program you learned about the uses and benefits of the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF). There are five core functions of the NIST CSF framework: identify, protect, detect, respond, and recover.

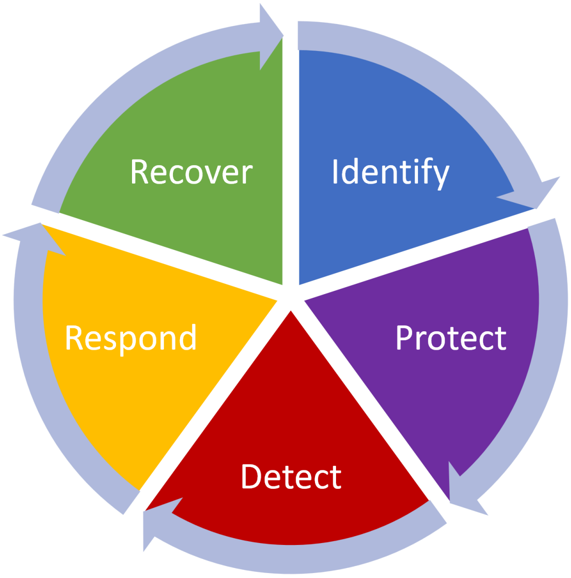

Image: 5 core functions of the NIST CSF

These core functions help organizations manage cybersecurity risks, implement risk management strategies, and learn from previous mistakes. Plans based on this framework should be continuously updated to stay ahead of the latest security threats. The core functions help ensure organizations are protected against potential threats, risks, and vulnerabilities. Each function can be used to improve an organization's security:

- **Identify:** Manage security risks through regular audits of internal networks, systems, devices, and access privileges to identify potential gaps in security.

- **Protect**: Develop a strategy to protect internal assets through the implementation of policies, procedures, training and tools that help mitigate cybersecurity threats.

- **Detect**: Scan for potential security incidents and improve monitoring capabilities to increase the speed and efficiency of detections.
- **Respond**: Ensure that the proper procedures are used to contain, neutralize and analyze security incidents and implement improvements to the security process.
- **Recover**: Return affected systems back to normal operation and restore systems data and assets that have been affected by an incident.

Some questions to ask for each of the five core functions, include:

Identify	Create an inventory of organizational systems, processes, assets, data, people, and capabilities that need to be secured: ● Technology/Asset Management: Which hardware devices, operating systems, and software were affected? Trace the flow of the attack through the internal network. ● Process/Business environment: Which business processes were affected in the attack? ● People: Who needs access to the affected systems?
Protect	Develop and implement safeguards to protect the identified items and ensure delivery of services: ● Access control: Who needs access to the affected items? How are non-trusted sources blocked from having access? ● Awareness/Training: Who needs to be made aware of this attack and how to prevent it from happening again? ● Data security: Is there any affected data that needs to be made more secure? ● Information protection and procedures: Do any procedures need to be updated or added to protect data assets? ● Maintenance: Do any of the affected hardware, operating systems, or software need to be updated? ● Protective technology: Are there any protective technologies, like a firewall or an intrusion prevention system (IPS), that should be implemented to protect against future attacks?
Detect	Design and implement a system with tools needed for detecting threats and attacks: ● Anomalies and events: What tools could be used to detect and

	alert IT security staff of anomalies and security events, such as a security information and event management system (SIEM) tool? ● Security continuous monitoring: What tools or IT processes are needed to monitor the network for security events? ● Detection process: What tools are needed to detect security events, such as an IDS?
Respond	Design action plans for responding to threats and attacks: ● Response planning: What action plans need to be implemented to respond to similar attacks in the future? ● Communications: How will security event response procedures be communicated within the organization and with those directly affected by the attack, including end users and IT staff? ● Analysis: What analysis steps should be followed in response to a similar attack? ● Mitigation: What responding steps could be used to mitigate the impact of an attack, such as offlining or isolating affected resources? ● Improvements: What improvements are needed to improve response procedures in the future?
Recover	Construct a plan and implement the framework for recovering and restoring affected systems and/or data: ● Recovery planning: How will resources be restored following an attack? ● Improvements: Do any improvements need to be made to the current recovery systems or processes? ● Communications: How will restoration procedures be communicated within the organization and with those directly affected by the attack, including end users and IT staff?

The NIST CSF and its five core functions provide a framework of planning proactive to applying reactive measures to cybersecurity threats. These functions are essential for ensuring that an organization has effective security strategies in place. An organization must have the ability to quickly recover from any damage caused by an incident to minimize their level of risk.

Incident report analysis - Example

Summary	This morning, an intern reported to the IT department that she was unable to log in to her internal network account. Access logs indicate that her account has been actively accessing records in the customer database, even though she is locked out of that account. The intern indicated that she received an email this morning asking her to go to an external website to log in with her internal network credentials to retrieve a message. We believe this is the method used by a malicious actor to gain access to our network and customer database. A couple of other employees have noticed that several customer records are either missing or contain incorrect data. It appears that not only was customer data exposed to a malicious actor, but that some data was deleted or manipulated as well.
Identify	The incident management team audited the systems, devices, and access policies involved in the attack to identify the gaps in security. The team found that an intern's login and password were obtained by a malicious attacker and used to access data from our customer database. Upon initial review, it appears that some customer data was deleted from the database.
Protect	The team has implemented new authentication policies to prevent future attacks: multi-factor authentication (MFA), login attempts limited to three tries, and training for all employees on how to protect login credentials. Additionally, we will implement a new protective firewall configuration and invest in an intrusion prevention system (IPS).
Detect	To detect new unauthorized access attacks in the future, the team will use a firewall logging tool and an intrusion detection system (IDS) to monitor all incoming traffic from the internet.

Respond	The team disabled the intern’s network account. We provided training to interns and employees on how to protect login credentials in the future. We informed upper management of this event and they will contact our customers by mail to inform them about the data breach. Management will also need to inform law enforcement and other organizations as required by local laws.
Recover	The team will recover the deleted data by restoring the database from last night’s full backup. We have informed staff that any customer information entered or changed this morning would not be recorded on the backup. So, they will need to re-enter that information into the database once it has been restored from last night’s backup.

FINAL : Incident report analysis (NIFT-CSF)

Summary	The organization experienced a **Distributed Denial of Service (DDoS)** attack targeting its internal network. The attacker used a flood of **ICMP packets** (commonly known as a ping flood) to overwhelm the network infrastructure. This attack exploited an **unconfigured firewall**, which allowed the malicious traffic to pass through unchecked. The result was a **complete outage of network services for two hours**, halting access to internal resources. The **incident response team** reacted by blocking all incoming ICMP packets, shutting down non-critical services, and restoring critical operations. Subsequent investigations revealed that a **malicious actor used spoofed IP addresses** to launch the attack, making it more difficult to trace the origin.
Identify	The attack was clearly a **Distributed Denial of Service (DDoS)** attack,

	specifically using an **ICMP flood** technique, which is a common method for overwhelming networks by sending an excessive number of ping requests. The attacker also employed **IP spoofing** to hide the true source of the traffic. The systems affected during this incident included the organization's **firewall**, which was not properly configured, and the **internal network infrastructure**, including servers and services required for web design, graphic design, and social media marketing operations. These systems were rendered inaccessible during the attack, significantly impacting the business's ability to serve its clients.
Protect	To prevent similar incidents in the future, several protections need to be put in place. First, the organization must properly configure all firewalls with strict rules that filter unnecessary or suspicious traffic, especially limiting or rate-limiting ICMP requests. Network segmentation should be implemented to isolate critical services from public-facing systems, reducing the potential blast radius of such attacks. Additionally, updating internal security policies to include specific procedures for preventing and responding to DDoS attacks is essential. All IT staff should also undergo training to understand DDoS prevention strategies and firewall management, ensuring that such vulnerabilities are proactively addressed and not overlooked.
Detect	Detecting similar attacks in the future will rely on continuous **network traffic monitoring** and the deployment of intelligent detection systems. Implementing advanced **Intrusion Detection and Prevention Systems (IDS/IPS)** can help identify unusual traffic patterns and immediately flag large volumes of ICMP packets from unknown or non-trusted IP addresses. Establishing **baseline behavior patterns** for normal network activity will also assist in quickly spotting anomalies. Tools like **Security Information and Event Management (SIEM)** systems can collect and correlate data from various sources, allowing for real-time alerts when suspicious activity is detected. Monitoring user behavior

	and authentication attempts will also help identify compromised accounts or unauthorized access attempts.
Respond	In preparing for future cybersecurity incidents, a clear **incident response plan** must be in place. This includes having predefined steps for **containing threats**, such as isolating affected devices or blocking certain types of traffic at the firewall. Once a threat is contained, the organization must work to **neutralize** the attack by identifying and shutting down the source or method of intrusion. All incidents should be logged and **analyzed** using data from IDS, firewalls, and network monitoring tools to understand the method, impact, and possible prevention strategies. To improve resilience, regular incident response drills should be held, and lessons learned from past incidents should be integrated into updated security procedures.
Recover	Recovering from a cybersecurity incident like a DDoS attack involves several key steps. First, the organization must **restore critical services and systems** to full functionality, ensuring they are free of any lingering malicious activity. All **backups** should be reviewed and verified for integrity before being used in the recovery process. Additionally, the organization should conduct a full **system health check** to ensure performance is stable. Moving forward, the recovery plan should include investments in **redundancy**, such as using cloud-based DDoS mitigation services and high-availability architecture. Documenting the incident and the recovery efforts will also help in refining future response and recovery processes, ensuring that the organization is better prepared for similar threats.

Reflections/Notes: This incident revealed the critical importance of properly configured firewalls and proactive network monitoring. It showed how a single oversight, like an unconfigured firewall, can lead to major disruptions. The response efforts were effective, but highlighted the need for a stronger, well-documented incident response plan and ongoing staff training. Moving forward, regular audits, automated threat detection, and improved team preparedness will be key to strengthening our cybersecurity posture and preventing future attacks.