Incident Report Using NIST CSF

Introduction

This presentation covers three key aspects of the project: the scenario, the notes used, and the final result. The scenario outlines the project goals, the notes provide guidance, and the final project demonstrates how these elements were applied.

Scenario:

Scenario

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 incident and integrate your analysis into a general security strategy:

- **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.

Step-By-Step Instructions

Follow the instructions and fill in the sections to complete the activity. Then, go to the next course item to compare your work to a completed exemplar.

Notes:

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/AssetManagement:Whichhardwaredevices, operating systems, and software were affected? Trace the flow of the attack through the internal network. ● Process/Businessenvironment:Whichbusinessprocesseswere affected in the attack? ● People:Whoneedsaccesstotheaffectedsystems?
Protect	Develop and implement safeguards to protect the identified items and ensure delivery of services: ● Accesscontrol:Whoneedsaccesstotheaffecteditems?Howare non-trusted sources blocked from having access? ● Awareness/Training:Whoneedstobemadeawareofthisattack and how to prevent it from happening again? ● Datasecurity:Isthereanyaffecteddatathatneedstobemade more secure? ● Informationprotectionandprocedures:Doanyproceduresneed to be updated or added to protect data assets? ● Maintenance:Doanyoftheaffectedhardware,operating systems, or software need to be updated? ● Protectivetechnology:Arethereanyprotectivetechnologies,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: ● Anomaliesandevents:Whattoolscouldbeusedtodetectand alert IT security staff of anomalies and security events, such as a security information and event management system (SIEM) tool? ● Securitycontinuousmonitoring:WhattoolsorITprocessesare needed to monitor the network for security events? ● Detectionprocess:Whattoolsareneededtodetectsecurity events, such as an IDS?

Respond	Design action plans for responding to threats and attacks: ● Responseplanning:Whatactionplansneedtobeimplemented to respond to similar attacks in the future? ● Communications:Howwillsecurityeventresponseprocedures be communicated within the organization and with those directly affected by the attack, including end users and IT staff? ● Analysis:Whatanalysisstepsshouldbefollowedinresponsetoa similar attack? ● Mitigation:Whatrespondingstepscouldbeusedtomitigatethe impact of an attack, such as offlining or isolating affected resources? ● Improvements:Whatimprovementsareneededtoimprove response procedures in the future?
Recover	Construct a plan and implement the framework for recovering and restoring affected systems and/or data: ● Recoveryplanning:Howwillresourcesberestoredfollowingan attack? ● Improvements:Doanyimprovementsneedtobemadetothe current recovery systems or processes? ● Communications:Howwillrestorationproceduresbe 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.

Final Project:

- Incident Report

Incident report analysis

Instructions

As you continue through this course, you may use this template to record your ndings a er completing an activity or to take notes on what you've learned about a speci c tool or concept. You can also use this chart as a way to practice applying the NIST framework to di erent situations you encounter.

Summary	The organization faced a security incident when the internal network abruptly ceased functioning due to a distributed denial of service (DDoS) a ack. The cybersecurity team identi ed the disruption, a ributing it to an in ux of ICMP packets overwhelming the network. To counteract the a ack, immediate measures were taken to block the malicious activity and temporarily halt non-critical network services, allowing for the restoration of essential network functions.
Identify	The recent cybersecurity incident at our multimedia company, characterized by a DDoS a ack utilizing a ood of ICMP ping packets, necessitates a comprehensive understanding of the a ected systems, processes, assets, data, people, and capabilities. By addressing the following key questions, we aim to create a detailed inventory to guide our response and mitigation e orts. The DDoS a ack targeted our internal network, impacting hardware devices, and the so ware they were running on. The a ack a ected the company. Potentially resulting in nancial implications for the company during the 2-hour network downtime. Access to the a ected systems is crucial for the cybersecurity team, enabling them to promptly respond to and mitigate the a ack. The team has the

	necessary permissions and access levels to take immediate action in response to security incidents.
Protect	In response to the recent cyber a ack that disrupted our internal network, we're taking steps to protect our systems, data, and team. We're limiting access to important systems to only essential cybersecurity and response folks. Firewalls will block unwanted tra c, and we'll regularly check and adjust them to stay safe. Everyone in the company will get training to recognize and report any suspicious activities. We'll also encrypt sensitive data to make it more secure. Our response plan will get an update to be er deal with these kinds of a acks. Regular checkups and xes will happen to keep everything up to date. We're adding extra tools, like intrusion prevention systems, to stop bad tra c. This all aims to make our defenses stronger, prevent similar issues, and keep our overall security in good shape. Ongoing monitoring and adjustments will be crucial for adapting protective measures to evolving cyber threats.
Detect	We will leverage a SIEM tool to detect and alert our IT security sta of anomalies and security events. This tool will analyze log data. Implementing network monitoring tools like Wireshark, tcpdump, or Splunk will allow us to continuously monitor the network for security events. These tools will provide visibility into network activities, helping us identify unusual pa erns or behaviors. Deploying an Intrusion Detection System (IDS) will be essential for detecting security events. Or even be er, an IPS that can detect any network a ack and take action right away.
Respond	To make sure we can handle problems well, we're creating plans for how to respond to a acks or threats. These plans will have clear steps, roles, and responsibilities, so we can act quickly if similar issues happen again. We'll share these plans within the company and with the people directly a ected, like end users and IT sta . We'll also learn from each incident by looking at what happened, re ning our plans based on these lessons. If there's an a ack, we'll take speci c steps to lessen its impact, like isolating or turning o a ected

	parts. And, we're commi ed to ge ing be er over time by regularly looking at what worked and what didn't, making our plans, communication, and overall ability to handle future issues even stronger.
Recover	In cra ing our recovery plan for xing systems and data a ected by an a ack, we're prioritizing a clear and organized process. The plan outlines steps and priorities for bringing back a ected resources e ciently and in a timely manner. We'll regularly check and improve our recovery systems and processes to learn from each incident and make them be er over time. Communication channels will be set up to share the restoration procedures within the organization, and clear strategies will be in place to keep those directly impacted, including end users and IT sta , informed about the progress. By doing this, we aim to ensure a smooth and transparent recovery process, aligning with the NIST CSF's idea of a resilient recovery with clear plans

---

Re ections/Notes: