**Incident report analysis**

**Instructions**

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

| **Summary** | Multimedia Company that offers web design services, graphic design, and social media marketing solutions to small businesses experienced a DDoS attack, which compromised the internal network for two hours until it was resolved. During the attack, the organization's network services stopped responding due to the incoming flood of ICMP packets. 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 has investigated the security event and 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. | | |
| --- | --- | --- | --- |
| Identify | -Internal Network Compromised for 2 Hours until it was resolved.  -Multimedia Company - offers web design services, graphic design, and social media marketing solutions to small business.  -Normal Internal Network Traffic could not access any network resources | | |
| Protect | - Multimedia Company/Organization.  - Small Business Customers need access to the organization’s services  - Security Team Blocking ICMP Packets from compromising the internal network. | | |
| Detect | - SIEM tool would be ideal  - Internal network needs an enhanced Firewall  - Intrusion Detection System  - Intrusion Protection System  - Wireshark, TCPDUMP in order to understand network logs and when the ICMP attack occurred | | |
| Respond | * Contain IP Address from Malicious Actor * Monitor Firewall and Network Logs in order to block and allow verified IP Address to connect to network without having to be a spoofed or compromised IP Address. * Internal Network must be offline in order to isolate the problem * Address to Organization and Customers about the data breach in order to assure confidence in the organization’s business. * Implement new policies to the organization in order to discourage employees from being an internal threat. | | |
| Recover | * To prevent an organization from experience a Distributed Denial of Service Attack: * Network Monitoring Software needs to be implemented in order to detect abnormal traffic patterns. * The Organization’s Internal Network needs an IDS/IPS system embedded into the network to filter out some ICMP traffic based on suspicious characteristics * Security Information Event Management Tool (SIEM Tool) also needs to be implemented to help make clear network analysis and decision-making. | | |

| Reflections/Notes: |
| --- |

### **Step 1: Access the incident report analysis template**

To access template for this course item, click the following link and select *Use Template*.

Link to template:

* [Incident report analysis](https://docs.google.com/document/d/1EnieOKYJyKGsVff5Gg-3-dVwrHrZ2m8Hig6tVpfKqyg/template/preview?usp=sharing&resourcekey=0-eb5t-d69zTPLEGthIpVlXw)

Link to supporting materials:

* [Applying the NIST CSF](https://docs.google.com/document/d/15yCDbDCOAcJw-LTz2DeCA7UeLRfvsf176T6MA6ku6ok/template/preview?usp=sharing)
* [Example of an incident report analysis](https://docs.google.com/document/d/11eTIo1igTRFrY279DG9tHTO3tB3bugSGyknZxsvY5vI/template/preview?usp=sharing&resourcekey=0-97MA-eOwoGtqcfqky0vjmg)

OR

If you don’t have a Google account, you can download the template directly from the following attachment.

[Incident report analysis](https://d3c33hcgiwev3.cloudfront.net/zkcwf4m0TjKB_T9KR14uUw_8a94cc4dbd8d45bba088b72dbf6654f1_Incident-report-analysis.docx?Expires=1689120000&Signature=XgA35bozjvuUXhNXQONRTAuo5K6-re5U726kcGLCLZ0y49nZQYZlN6vA7gyxHVNaQJ2Dn6diHSaYlFyoBp0DfSDwQmGf4Ud7vMvfNiLiQhzXENv~yfNEp2CLFzwu0DjyOq~JNCtnzYsmLynDIApkxChw7uB3oZUe9ylorooII3Y_&Key-Pair-Id=APKAJLTNE6QMUY6HBC5A)

[DOCX File](https://d3c33hcgiwev3.cloudfront.net/zkcwf4m0TjKB_T9KR14uUw_8a94cc4dbd8d45bba088b72dbf6654f1_Incident-report-analysis.docx?Expires=1689120000&Signature=XgA35bozjvuUXhNXQONRTAuo5K6-re5U726kcGLCLZ0y49nZQYZlN6vA7gyxHVNaQJ2Dn6diHSaYlFyoBp0DfSDwQmGf4Ud7vMvfNiLiQhzXENv~yfNEp2CLFzwu0DjyOq~JNCtnzYsmLynDIApkxChw7uB3oZUe9ylorooII3Y_&Key-Pair-Id=APKAJLTNE6QMUY6HBC5A)

[Applying the NIST CSF](https://d3c33hcgiwev3.cloudfront.net/hlERrE3-Rae2Ey-tcNZVGw_42760fbf6522420faa3312f02184bcf1_Applying-the-NIST-CSF-.docx?Expires=1689120000&Signature=SU6zwkt85i~OVLNsf-K6eopArEVAqKuGbcXo7EFhtYtbcMEeHvC2zTqBVysXQ4jG3y3OVYNbtcKDNOgvh-Iyp4IazkZwthrpFnwXlqgwwkFnRRHVgZvsOR005UpzSFe5vw7T9ZUGiAWsYhCe4-dMuAcYSouftragrnUKcH-4TIY_&Key-Pair-Id=APKAJLTNE6QMUY6HBC5A)

[DOCX File](https://d3c33hcgiwev3.cloudfront.net/hlERrE3-Rae2Ey-tcNZVGw_42760fbf6522420faa3312f02184bcf1_Applying-the-NIST-CSF-.docx?Expires=1689120000&Signature=SU6zwkt85i~OVLNsf-K6eopArEVAqKuGbcXo7EFhtYtbcMEeHvC2zTqBVysXQ4jG3y3OVYNbtcKDNOgvh-Iyp4IazkZwthrpFnwXlqgwwkFnRRHVgZvsOR005UpzSFe5vw7T9ZUGiAWsYhCe4-dMuAcYSouftragrnUKcH-4TIY_&Key-Pair-Id=APKAJLTNE6QMUY6HBC5A)

[Completed Example of an Incident report analysis](https://d3c33hcgiwev3.cloudfront.net/bIq362jBTIayw5z_7aDnkQ_7561e226b9f04a5b96a817c47e6033f1_Completed-Example-of-an-Incident-report-analysis.docx?Expires=1689120000&Signature=RNItJaZj8jKwHe87RQemFc3GP0gelSDs6vph9767UaQ4RvC7xd3ovSO5wiLq-UquUwntD7oZPp2pp4qE4SG~qOgQoYU9sztvbEaOC6OcgeZfyY8b23sYGarP6yDoRzHmvE16pW-13s9Y68S0Is0vOdiZUamNTnYLv~HHJlMNWQ8_&Key-Pair-Id=APKAJLTNE6QMUY6HBC5A)

[DOCX File](https://d3c33hcgiwev3.cloudfront.net/bIq362jBTIayw5z_7aDnkQ_7561e226b9f04a5b96a817c47e6033f1_Completed-Example-of-an-Incident-report-analysis.docx?Expires=1689120000&Signature=RNItJaZj8jKwHe87RQemFc3GP0gelSDs6vph9767UaQ4RvC7xd3ovSO5wiLq-UquUwntD7oZPp2pp4qE4SG~qOgQoYU9sztvbEaOC6OcgeZfyY8b23sYGarP6yDoRzHmvE16pW-13s9Y68S0Is0vOdiZUamNTnYLv~HHJlMNWQ8_&Key-Pair-Id=APKAJLTNE6QMUY6HBC5A)

### **Step 2: Identify the type of attack and the systems affected**

Think about all of the concepts covered in the course so far and reflect on the scenario to determine what type of attack occurred and which systems were affected. List this information in the incident report analysis worksheet in the section titled “Identify.”

### **Step 3: Protect the assets in your organization from being compromised**

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.

### 

### **Step 4: Determine how to 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.

### **Step 5: Create a response plan for future cybersecurity 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.