# INCIDENT RESPONSE MODULE CHALLENGE

*If you have any questions, please ask them in the "phishing-analysis-module" channel, under the "Operation Chimera" category on the SBT Discord server.*

If you feel you're familiar with what Incident Response is, and how to deal with a security incident, then you may be ready for the Challenge! We suggest you still do some of your own research using the 'Useful Links' in the training material before attempting the Challenge.

### Challenge Brief:

There has been a system compromise on a server that holds Personal Identifiable Information on customers. You will complete a fictional scenario and attempt to get the best possible result, by following NIST SP 800-61r2. Remember that the stages are:

1. **Preparation**
2. **Detection and Analysis**
3. **Containment, Eradication, Recovery**
4. **Lessons Learned**

**Read to submit your Challenge?** Head over to the website and click on the 'Challenge Submission' button under the Vulnerability Management module.

| Part One) Incident Response Quiz | |
|---|---|
| [Preparation] What is the main purpose of this stage? | 1) Manually searching for threat actors inside the network<br>2) Responding to a cyber attack<br>3) Teaching analysts how the SIEM platform works<br>4) Implementing defences to prevent security incidents |
| [Preparation] What is a CSIRT Jump Kit? | |
| [Preparation] What is a Retainer Team? | |
| [Preparation] What is a Standard Operating Procedure? (SOP) | |

| | |
|---|---|
| [Preparation] What security control can be tuned to allow or deny specific network traffic both inbound and outbound? | 1) IDPS<br>2) Web Proxy<br>3) Firewall<br>4) VPN |
| [Preparation] What is the general name for a Policy that tells employees what they can and can't do at work? | |
| [Detection and Analysis] Name THREE attack vectors, as listed within NIST SP 800 61r2 | |
| [Detection and Analysis] What is a common issue with IDPS systems, that can cause issues when trying to identify an incident? | |
| [Detection and Analysis] Which statement is an example of a Precursor? | 1) A standard user account suddenly having administrator privileges<br>2) Web server logs showing it has been scanned for vulnerabilities |
| [Detection and Analysis] Which statement is an example of an Indicator? | 1) An unusual file on a server's desktop<br>2) An underground forum has discussion about targeting a company |
| [Analysing] What is Profiling, and how does it help detect security incidents? | |
| [Prioritisation] Should incidents be prioritised? Why? | |
| [Containment] Name two measures that can be used to contain a threat | |
| [Recovery] Name two measures that are usually taken to repair affected systems | |
| [Lessons Learned] Why is this stage so important? | |

| Part Two) Incident Response Scenario Questions | |
|---|---|
| After a phishing email was opened by a Dickson United employee, malware was downloaded to the system, and harvested credentials (account details) from both live memory, and stored on the hard drive in files and browsers. Name and explain two security controls that could have stopped this attack at the delivery stage, or the exploitation stage. | |
| Analysts were slow to identify this incident, as IDPS didn't take any action against the malware, or generate an alert. What is this issue known as? | 1) False Negative<br>2) False Positive<br>3) False Response |
| The malware also initiated a reverse connection, allowing the attacker to execute commands on the employees' system. From here, the actor used the credentials to log in to database that contains customer data (PII). At this point the security team is aware of the activity, and need to contain the threat. The attacker has already begun exfiltrating the data via a DNS tunnel. What would be the most appropriate measure to contain the attacker, and why? | |
| Now the threat is contained, and unable to spread to any other systems, analysts have discovered that some Personally Identifiable Information has been successful exfiltrated. Which TWO business Departments would be the most appropriate to notify both the authorities and affected customers? | 1) Human Resources<br>2) Legal<br>3) Communications<br>4) Finance |
| Before deleting the malware, analysts collected a number of indicators such as the file name, the file hash value, its' hard-coded command and control server IP, and a text string which appears to be a signature "Bl4de//". Should this information be shared with other organisations? Why? | |
| During the Lessons Learned stage, it was discovered that the employee who was compromised didn't need access to the database for his work. It was suggested that all accounts for the database should be reviewed to see if they actually need access. Is this a good idea? Why? | |