Cybersecurity Incident Report

Section 1: Identify the type of attack that may have caused this network interruption
One potential explanation for the website's connection timeout error message is due to a SYN flood attack on the web server. A SYN flood attack is one type of DOS attack that happens when a malicious attacker simulates a TCP connection by flooding the server with SYN Packets This analysis is consistent with the logs data which shows that an unusually large amount of illegitimate SYN packets were sent to the web server along with legitimate SYN requests originating from the company's employees. This overload caused the web server's available to consume available bandwidth faster than it can replenish leading to unavoidable exhaustion. This event could be classified as a Direct DoS SYN flood attack since it is coming from a single IP address.

Section 2: Explain how the attack is causing the website to malfunction
When website visitors try to establish a connection with the web server, a three-way handshake occurs using the TCP protocol. Explain the three steps of the handshake: 1. Visitors make a SYN request to the web server. This is the first part of the handshake requesting the web server to authorize the connection and request to open a communication channel. The SYN stands for "Synchronize" 2. Next, the web server sends a SYN ACK which stands for "Synchronize, Acknowledge". This is returned by the web server to the requesting client agreeing to the connection and asking the client to acknowledge the agreement. 3. The final step is the ACK packet sent to the web server from the client proving that they acknowledge the permission to connect. WHen this is completed, a successful TCP connection is established and data can flow between both nodes/ servers. Explain what happens when a malicious actor sends a large number of SYN packets all at once: When a threat actor sends a large number of SYN packets all at once, maybe a few hundreds in seconds, it overwhelms the server causing rapid depletion in the available bandwidth. This means that the server is using up the available bandwidth in an attempt to

meet up with the unusually high SYN requests. Eventually it uses up its available bandwidth causing it to crash. The server also struggles to fulfill additional requests coming from legitimate IP addresses adding to its load. In the travel agency's web server, legitimate requests were coming from the company's employees while a disproportionately large amount of the same requests were coming from a malicious attacker.

Explain what the logs indicate and how that affects the server: The log review indicates that an attacker initiates a connection with the web server which is handled normally. However, the malicious actor proceeds to persistently send large amounts of SYN requests to the web server. Although the web server was initially able to handle the requests, it soon began to struggle with the sheer amount of requests it received. This causes the web server to slow down in responding to legitimate requests from the agency's employees. This is indicated by the HTTP/1.1 504 and the [RST, ACK] error responses sent by the web server. Any of these error responses would indicate that the packet is dropped and would have to be re-initiated. The implication is that the company's employees cannot establish connection to the web server, and in turn, cannot sell their vacation packages to their customers. The agency's website will suffer some downtime while the attack is mitigated causing them to lose money and potentially customers.