Cybersecurity Incident Report

Section 1: Identify the type of attack that may have caused this network interruption
Our network protocol analyzer (Wirehark) alerted us to an unusual pattern of requests to IP address 192.0.2.1 that resulted in this specific IP address being unable to fulfill legitimate requests. Most of the requests during the alert period originate from the same IP address (198.51.100.23), and repeatedly request the same resource, indicating a Denial of Service (DoS) attack.

Section 2: Explain how the attack is causing the website to malfunction
As indicated, a large number of requests to the specified IP address, for the same resource, and originating from the same origin IP address indicate a Denial of Service (DoS) attack. By flooding the network with such a large number of requests, this affected the ability of this specific server to respond to legitimate traffic during the period of the attack. Potential consequences of this attack include lost revenue from legitimate traffic, and loss of trust in the parent organization due to lack of response and availability. A possible mitigation to prevent future attacks of this specific type may include identifying and automatically throttling traffic from specific IP addresses that exceed a pre-defined limit of requests within a specific timeframe.