Cybersecurity Incident Report

Section 1: Identify the type of attack that may have caused this network interruption
The interruption appears to be a result of a potential SYN flood attack. This conclusion is based on an unusually high number of requests observed. The fact that these requests originate from the same IP address suggests that a direct DoS SYN flood attack was the method used by the threat actor.

Section 2: Explain how the attack is causing the website to malfunction
The attack commenced with a request sent from the IP address 203.0.113.0, to which the website responded normally. Consequently, the website continued to function without any issues. However, the problem emerged when the same IP address persistently generated numerous SYN requests, overwhelming the website. These types of attacks lead to service disruption, they can also impact the company's reputation, and customer trust. Prevention: In order to prevent these types of attacks the team recommends installing an IPS to detect abnormal traffic.