Cybersecurity Incident Report

Section 1: Identify the type of attack that may have caused this network interruption
We started experiencing a SYN flood attack at approx T3.39 from IP address 203.0.113.0

Section 2: Explain how the attack is causing the website to malfunction
SYN flood attack works by opening a “handshake” between sender and server, but not following up. In geek terms, sender sends “SYN”, and server replies “SYN,ACK”, which means “okay, ready”. A normal sender would send “ACK”, then the actual traffic. However, a malicious sender can send NOTHING, forcing server to wait for traffic until it finally times out and send a “RST,ACK” which roughly translates to “are you still there?” and if malicious sender send a LOT of of SYN, the server can be overwhelmed as it waits for a lot of traffic that never comes, which would mean it can’t listen to any other traffic. In our case, the attack started at T3.39. Originally the server was able to keep up with legitimate traffic, but it started to fail at T6.23 when it asked 198.51.100.16 to send again. From there on, only one legit request got through at T14.88. The rest of traffic only contains SYN flood attacks as the server kept waiting for a reply that never came. The malicious sender sent 4-8 requests per second, overwhelming the server. The server became completely unresponsive to normal traffic. To the rest of the world, it is as if our server disappeared or timed out. If we have a SOAR system in place, we can immediately block the malicious traffic from getting through our firewall. However, this will likely not work for a DDOS attack. A long term solution is to use a CDN (content delivery network) such as Cloudflare to get our website out there so it remains available.