Incident Report: Bytebistro.com Website Outage Oct31

Role: Cybersecurity Analyst, Byte Bistro Ltd
Date: October 31, 2025
Incident: Website (bytebistro.com)
Severity: Critical
Detection Source: Splunk SIEM Alert & Customer Ticket Reports

1. Incident Summary

At **09:46 a.m.**, the Intrusion Detection System (IDS) and integrated ticketing system automatically generated an **alert flagging a SYN flood attack** against the organizations web server. The IDS reported approximately **24,600 SYN packet per second** originating from **1500 distinct source IPs**. The alert was initially routed to the Networks Operations (NetOps) team for review before being escalated to the Cybersecurity team once the impact on web services became evident.

At **9:48 a.m.**, shortly after the IDS alert, I initiated a network traffic capture using **Wireshark** on the mirrored network span connected to the company web server. The captured was saved as a short .pcap file to record live traffic directed towards the web server during the suspected attack. The file was then uploaded to the SIEM and analysed using **Suricata** to verify the presence and characteristics of the SYN flood activity.

At **09:49 a.m**. our support team received multiple customer reports that the company website (Bytebistro.com) was unavailable, with customers/users reporting HTTP 503 – Service Unavailable errors, indicating the server was unable to handle incoming requests, and HTTP 502 – Bad Gateway erorrs, suggesting communication issues between the web server and its upstream service. Visitors attempting to access the website experienced failed page loads and timeouts.

Initial investigation confirmed that the web server was still powered on and reachable via the internal network but was not processing new HTTP connections. This suggested the issue was **not a server crash or shutdown**, but rather a service degradation likely caused by excessive inbound traffic.

At this early stage, the suspected cause was identified as a potential **SYN flood denial-of-service (DoS) attack**, where numerous incomplete TCP connections attempts consume server resources and prevent legitimate users from connections. However, a detailed log analysis is required to confirm the nature of this attack and to produce an **urgent mitigation report.**