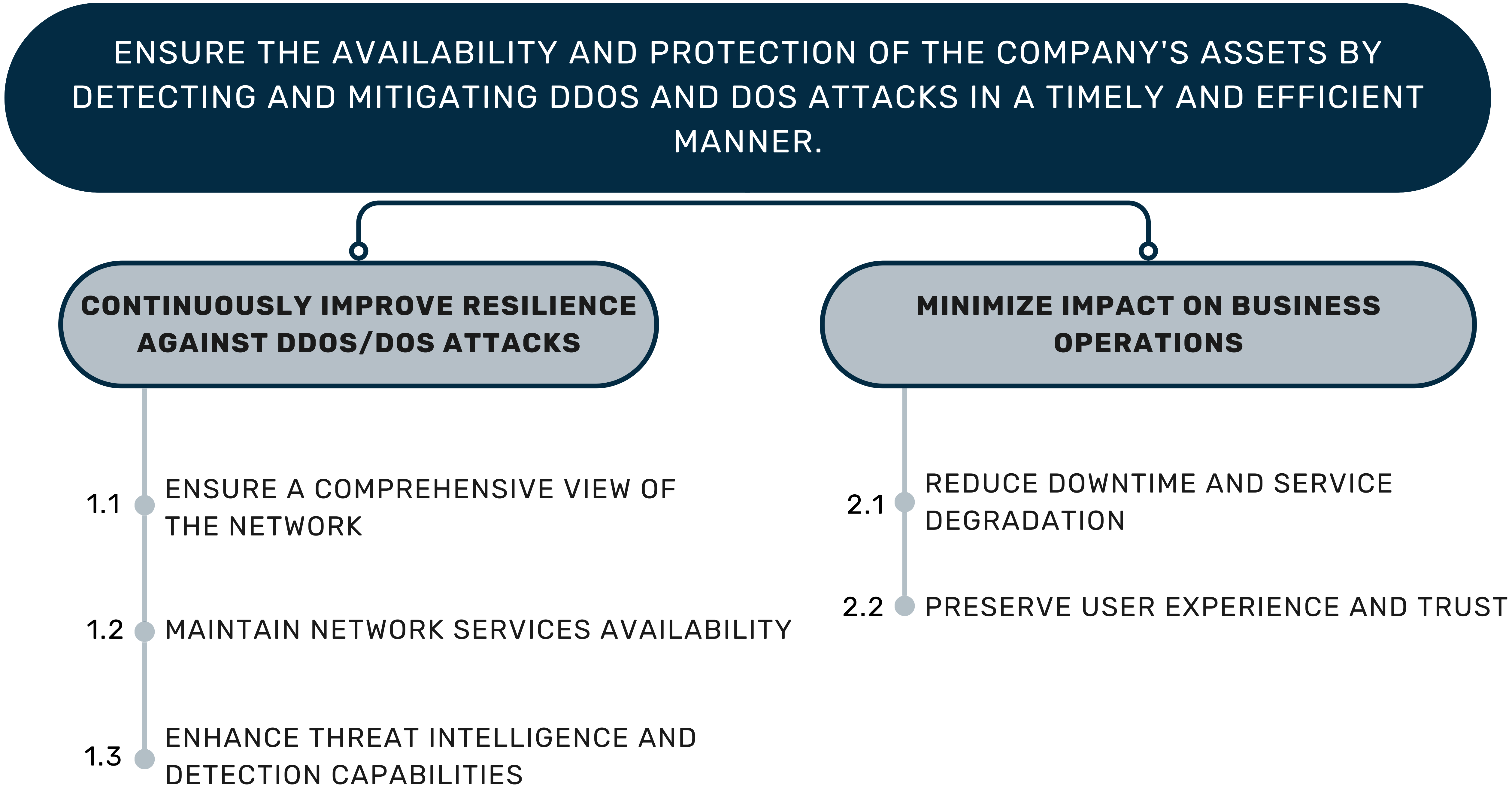
MONITOR THE COMPANY'S NETWORK TO DETECT AND MITIGATE DISTRIBUTED DENIAL-OF-SERVICE (DDOS) AND DENIAL-OF-SERVICE (DOS) ATTACKS, ENSURING THE AVAILABILITY AND INTEGRITY OF CRITICAL SERVICES. THE USER MUST HAVE A REAL-TIME OVERVIEW OF THE ENTIRE NETWORK INFRASTRUCTURE TO PROMPTLY IDENTIFY ABNORMAL TRAFFIC PATTERNS AND INTERVENE BEFORE THE ATTACK SIGNIFICANTLY IMPACTS BUSINESS OPERATIONS.

THIS MAY INVOLVE DYNAMICALLY BLOCKING MALICIOUS IP ADDRESSES, RATE-LIMITING SUSPICIOUS TRAFFIC, AND REROUTING LEGITIMATE REQUESTS TO MITIGATE SERVICE DISRUPTIONS. ADDITIONALLY, THE SYSTEM SHOULD FACILITATE THE RAPID DEPLOYMENT OF COUNTERMEASURES, SUCH AS ACTIVATING CLOUD-BASED DDOS PROTECTION SERVICES OR ADJUSTING FIREWALL AND INTRUSION PREVENTION SYSTEM (IPS) RULES.



ENSURE THE AVAILABILITY AND PROTECTION OF THE COMPANY'S ASSETS BY DETECTING AND MITIGATING DDOS AND DOS ATTACKS IN A TIMELY AND EFFICIENT MANNER.

CONTINUOUSLY IMPROVE RESILIENCE AGAINST DDOS/DOS ATTACKS

1.1 ENSURE A COMPREHENSIVE VIEW OF THE NETWORK

1.2 MAINTAIN NETWORK SERVICES AVAILABILITY

1.3 ENHANCE THREAT INTELLIGENCE AND DETECTION CAPABILITIES

MINIMIZE IMPACT ON BUSINESS OPERATIONS

2.1 REDUCE DOWNTIME AND SERVICE DEGRADATION

2.2 PRESERVE USER EXPERIENCE AND TRUST