Company: Türk Telekom
Company Description: Türk Telekomünikasyon A.Ş. (Türk Telekom) is Turkey's first and largest integrated telecommunications operator, headquartered in Ankara. With over 180 years of history, the company provides a comprehensive range of services including fixed-line and mobile telephony, broadband internet, digital television, and Wi-Fi under the unified "Türk Telekom" brand.
Nomination Category: Product & Service Categories - Business Technology Solutions
Nomination Sub Category: Cybersecurity Solution
Nomination Title: AI Assisted DDOS Support Platform

1. Which will you submit for your nomination in this category, a video of up to five (5) minutes in length about the the nominated new or new-version product or service, OR written answers to the questions for this category? (Choose one):

   Written answers to the questions

2. If you are submitting a video of up to five (5) minutes in length, provide the URL of the nominated video here, OR attach it to your entry via the "Add Attachments, Videos, or Links to This Entry" link above, through which you may also upload a copy of your video.

3. If you are providing written answers for your submission, you must provide an answer to this first question: If this is a brand-new product, state the date on which it was released. If this is a new version of an existing product, state the date on which the update was released:

   It is a new product which is released in Feb 2025 .

4. If you are providing written answers for your submission, you must provide an answer to this second question: Describe the features, functions, and benefits of the nominated product or service (up to 350 words):

   Total 344 words used.

   Since 2009, Türk Telekom has provided professional DDoS protection services for corporate and individual customers. When abnormal traffic exceeds thresholds, our mitigation infrastructure triggers alarms and generates forensic-quality PCAP (Packet Capture) files for analysis.

   Each alarm typically produces one or more PCAP records, which are archived by the Cyber Security Operations Center. Traditionally, analysts manually examine these files—reviewing headers, protocols, ports, and payloads—to determine the nature of the attack.

   Challenges in the Existing Process

   However, manual PCAP analysis has key limitations, especially during alarm spikes:

   • **Time-Consuming:** A single file may take minutes or hours to review, delaying response and causing service issues

   • **High False Positives:** Benign traffic often triggers alerts, wasting analyst effort

   • **Resource Constraints:** Limited staff slows incident prioritization and handling

   • **Inconsistent Analysis:** Similar attacks may be interpreted differently, affecting standardization and institutional learning

   The AI-Powered Solution: A Leap in Speed, Quality, and Efficiency

   To overcome operational challenges, Türk Telekom's Cyber Security Directorate integrated an AI-powered engine into its DDoS infrastructure. The system provides:

   • **Automated Analysis:** Rapid parsing of PCAP metadata, including IPs, ports, protocols, and traffic types

   • **Attack Detection:** AI classifies threats like SYN Floods, DNS Amplification, and Slowloris across all network layers

   • **False Positive Reduction:** ML filters benign traffic to minimize alert noise

   • **Mitigation Advice:** Suggests targeted actions like IP blocking or rate limiting

   • **Visual Insights:** PPS/BPS charts highlight abnormal traffic trends

   • **Continuous Learning:** Analyst feedback retrains the model for ongoing accuracy

   Project Impact and Strategic Value

   The AI-powered system has enhanced Türk Telekom's DDoS operations with the following key outcomes:

   • **Significantly reduced average analysis time**

   • **Lowered false positive rates, allowing focus on real threats**

   • **Increased customer satisfaction through faster, uninterrupted service**

   • **Created a centralized knowledge base for informed decision-making**

   • **Reduced operational workload, enabling focus on strategic tasks**

   This project goes beyond technical gains—it marks a strategic evolution. By treating AI as a cyber defense partner, Türk Telekom has shifted from reactive to adaptive security, uniting automation and human expertise to shape the future of cybersecurity.

5. If you are providing written answers for your submission, you must provide an answer to this third question: Outline the market performance, critical reception, and customer satisfaction with the product or service to date. State monetary or unit sales figures to date, if possible, and how they compare to expectations or past performance. Provide links to laudatory product or service reviews. Include some customer testimonials, if applicable (up to 350 words):

   Total 339 words used.

   Türk Telekom is Turkey's largest security ISP, serving over **5,000 DDoS-protected customers** nationwide. As such, our infrastructure faces a high volume of daily threats—averaging around **200 DDoS attacks per day** across various industries.

   Approximately 95% of incoming DDoS attacks are automatically mitigated using predefined rule sets. However, the remaining 5%—averaging 10 complex attacks per day—demand manual intervention by security analysts. While 10–15 minutes per incident may appear minimal in isolation, in the context of an ISP managing real-time traffic for thousands of customers, it is mission-critical.

   Each minute of delayed response increases the risk of service degradation, SLA violations, and reputational damage. What seems like a small operational fragment in percentage terms can cascade into large-scale impact. For an ISP operating in milliseconds, even a 15-minute delay is not just inefficiency—it's vulnerability.

   These complex cases often occur during attack surges, overwhelming resources and delaying response before customers are impacted.

   That's why even the "last 5%" is not an edge case—it's a **high-risk, high-impact** zone demanding intelligent, real-time support.

   With the deployment of our **AI-powered PCAP analysis system**, this manual workload has been drastically reduced. The AI model analyzes complex traffic data in **under one minute**, automatically flagging attack patterns and recommending mitigation actions directly to the analyst. This improvement represents a **10x reduction in analysis time**, enabling much faster response and reducing potential service disruption by the same factor.

   Thanks to this efficiency gain, attacks that previously required multiple analysts working in parallel can now be handled by **a single engineer**, freeing up personnel for more strategic tasks. This has directly contributed to a **significant increase in customer satisfaction**, particularly among high-priority clients such as banks, e-commerce platforms, and government services.

   Looking forward, we aim to extend the platform by automating not just detection and recommendation, but **full-scale mitigation**—allowing AI to respond in real time, eliminating human error and reducing response latency to near-zero levels.

   This system reflects not only technological progress but also streamlines our operations by uniting speed, precision, and scalability to boost national cyber resilience.

6. You have the option to answer this final question: Reference any attachments of supporting materials throughout this nomination and how they provide evidence of the claims you have made in this nomination (up to 250 words):

   Total 245 words used.

   To support the claims presented in this nomination, we have attached three key supporting materials that provide concrete evidence of the project's scope, implementation, and outcomes:

   1. AI-Assisted DdoS Analysis Platform Report (PPT)

   This presentation file outlines the **entire lifecycle** of the project—from initial problem statement and manual limitations to the design, development, deployment, and measurable impact of the AI-powered solution. It includes visual architecture diagrams, process flows, technical milestones, before/after comparisons, and quantified KPIs. The slide deck provides judges with a clear and structured understanding of the project's technical depth and strategic value.

   ---

   2. pcap_parsed_full_enriched.csv - PCAP Dataset Parsed Sample (CSV)

   This file presents an actual **sample output** generated from real PCAP traffic using a custom-built Python parser. It transforms raw, packet-level data into an AI-processable format. The CSV contains enriched metadata such as timestamps, source/destination IPs, ports, protocol types, packet lengths, and traffic flags. This demonstrates how the system automates a previously manual task—enabling fast, reliable AI-based analysis of traffic anomalies and DDoS patterns.

   ---

   3. AI-Assisted DDoS Analysis Platform Dashboard (PDF)

   This PDF captures the **end-user interface**—the dashboard cybersecurity analysts interact with during real-time operations. It showcases how AI results are visually presented, including attack detection summaries, protocol breakdowns, mitigation recommendations, traffic patterns, and alert prioritization. This interface exemplifies how AI insights are made actionable, helping analysts respond faster and more accurately during live attacks.

   Together, these attachments reinforce the platform's innovation, operational value, and technical excellence—helping judges evaluate its real-world impact.

Attachments/Videos/Links:

AI Assisted DDOS Support Platform

□ [REDACTED FOR PUBLICATION]