Table 52. Frequency of Cyberattacks in Telkom

Description	Years		
	2025	2024	2023
Brute Force Attack on network elements (frequency)	994	879	366,732
Longest Distributed Denial of Service Attack (minutes)	4,320	4,407	1,818
Attacks with the largest volume in gigabits per second (Gbps)	1,160	537.1	199.1

Throughout 2025, 994 Brute Force Attack attempts against network elements were recorded. The longest Distributed Denial of Service (DDoS) attacks occurred in February, November, and December 2025, each lasting 4,320 minutes, while the largest volume of attacks reached 1,160 Gbps in October 2025. The higher frequency of attacks identified in 2025 was primarily due to the deployment of additional sensors that enabled earlier incident detection. Although indicators such as attack frequency and duration increased compared to 2024, the resilience of Telkom's cybersecurity system ensured that the company's operations remained undisrupted.

TelkomGroup remains committed to maintaining vigilance and safeguarding the information system through a strengthened monitoring and prevention strategy. These efforts enable the rapid identification and response to potential server threats, ensuring the integrity and security of the system are well protected.

AI Governance and Security at TelkomGroup

Telkom is committed to adopting and developing artificial intelligence (AI) in a responsible, safe, and customer- and stakeholder-oriented manner. In 2025, Telkom developed personal data protection procedures for AI system implementation by emphasizing the ethical principles of AI use and development within TelkomGroup. Every AI project at Telkom is subjected to impact identification from the initial stage through privacy threshold analysis (PTA) to consistently apply the principle of privacy by design.

Telkom explicitly designates the roles and responsibilities of all key actors in the AI cycle (providers/developers, deployers, and end-users or operators) at each stage of deliverables. Telkom formally documents the mapping of these roles through a cooperation agreement or service level agreement (SLA), which includes indemnity clauses as the basis for liability in the event of potential losses.

Telkom also requires an impact analysis of personal data protection and considers the rights of personal data subjects at all stages of AI development. All of these obligations are consolidated within the AI lifecycle as the foundational framework for personal data protection, with the application tailored to Telkom's role in each AI project.

Figure 101. AI Lifecycle and Personal Data Protection Responsibility