The Rise of DDoS Attacks: Why They Should Concern Every Organization

Distributed Denial-of-Service (DDoS) attacks have emerged as a potent weapon, capable of crippling even the most robust online infrastructure. These malicious assaults involve flooding a website or server with a deluge of traffic, overwhelming its resources, and rendering it inaccessible to legitimate users. The consequences can be devastating, ranging from reputational damage and financial losses to operational disruptions and compromised data.

In the first half of 2023 alone, a staggering 7.9 million DDoS attacks – roughly 44,000 per day – flooded servers across the globe, marking a 31% increase compared to the same period in 2022. This alarming surge highlights the growing threat of cybercrime and underlines the urgent need for robust cybersecurity measures for businesses and individuals alike. The surge in the digital deluge stems from a multifaceted convergence of factors that collectively create a perfect storm in the realm of cybersecurity.

This report contains valuable insights for navigating the evolving cyber landscape. To unlock the full content, reach out to your customer success manager or email info@criticalstart.com.

CRITICALSTART® offers a pioneering solution to modern organizational challenges in aligning cyber protection with risk appetite through its Cyber Operations Risk & Response™ platform, award-winning Managed Detection and Response (MDR) services, and a dedicated human-led risk and security team. By providing continuous monitoring, mitigation, maturity assessments, and comprehensive threat intelligence research, they enable businesses to proactively protect critical assets with measurable ROI. Critical Start's comprehensive approach allows organizations to achieve the highest level of cyber risk reduction for every dollar invested, aligning with their desired levels of risk tolerance.