Initial Access Through Public-facing Applications

Threat actors are constantly devising means to infiltrate targeted networks through the exploitation of public-facing applications. Cyentia reported in 2021 that exploiting public-facing applications was 1 of 2 top Initial Access techniques. The study revealed that vulnerabilities in web applications led to 30 catastrophic cybersecurity incidents, causing a combined loss of $5.7 billion. Cyberattacks on public-facing applications extend beyond exploiting vulnerabilities and application-layer attacks. Threat actors also target cloud-based infrastructure by exploiting public-facing applications. Public-facing applications provide substantial advantages, but organizations must prioritize protecting these systems from vulnerabilities.

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.