September 12 2023

Must-Know Facts & Stats on Cybersecurity Threat Intelligence

Cyber threat intelligence plays a critical part in helping organisations defend against potential security breaches, cyber-attacks, and other vulnerabilities. Here are some crucial points with compelling stats and facts that every New Zealand organisation should be aware of

Rising Cyber Threats in NZ

According to CERT NZ, New Zealand's cyber incident reporting agency, the number of incidents reported in 2020 increased by 65% compared to 2019.

Local threats mean local consequences. Focusing solely on global threat intelligence might leave you exposed to risks specific to the New Zealand digital landscape.

The Global Financial Impact is rising

Cybercrime is expected to cost the global economy $10.5 trillion annually by 2025, up from $3 trillion in 2015, according to Cybersecurity Ventures.

The economic implications of cyber threats are monumental and growing. A global perspective on threat intelligence helps in understanding the financial risk your organisation could potentially face.

Industry-Specific Threats

Healthcare and financial services are among the most targeted sectors globally. In New Zealand, the public sector also reports a high number of incidents.

Your industry may have unique vulnerabilities. Customising threat intelligence to cater to your specific industry can significantly enhance your cybersecurity measures.

Human Element & Insider Threats

According to the Ponemon Institute, 34% of all cybersecurity incidents in 2020 involved internal actors.

Threat intelligence isn't just about warding off external attackers. It should also help you identify potential risks within your organisation, from unintentional data leaks to malicious insider activities.