create a timeline highlighting the key event, technological advancement and pivotal moment in the history of cyber security. this timeline will showcase how threat and defenses have developed over time

A person sitting at a desk with an old typewriter

AI-generated content may be incorrect.**1940s–1950s: Early Concepts & Theoretical Foundations**

📌 **1943** – **First Theoretical Cybersecurity Idea**: British mathematician Alan Turing develops the concept of code-breaking, laying the foundation for cryptographic security.  
📌 **1949** – **First Concept of a Computer Virus**: John von Neumann theorizes self-replicating programs, foreshadowing modern malware.  
📌 **1950s** – **Cold War Intelligence & Encryption**: Governments develop early cryptographic methods for secure communications.

A group of people working in a computer room

AI-generated content may be incorrect.**🔹 1960s: Birth of Cybersecurity & Networking**

📌 **1965** – The first major vulnerability is recognized when MIT researchers identify time-sharing system flaws.  
📌 **1969** – **ARPANET Created**: The foundation of the internet is built, connecting four universities, but with no security measures in place.

**🔹 1970s: First Attacks & Security Measures**

📌 **1971** – **First Computer Virus ("Creeper")**: Bob Thomas creates "Creeper," a self-replicating program that spreads across ARPANET.  
📌 **1972** – **First Antivirus ("Reaper")**: Ray Tomlinson creates a program to remove the Creeper virus.  
📌 **1976** – **Public Key Cryptography Introduced**: Whitfield Diffie and Martin Hellman develop asymmetric encryption, revolutionizing secure communications.  
📌 **1979** – **First Major Network Hack ("Stanford Incident")**: Kevin Mitnick gains unauthorized access to a computer network.

A person sitting at a desk with computers

AI-generated content may be incorrect.**🔹 1980s: Rise of Malware & Cybercrime Awareness**

📌 **1983** – The term "computer virus" is coined by Fred Cohen.  
📌 **1986** – **First Anti-Hacking Law (CFAA, USA)**: The Computer Fraud and Abuse Act criminalizes unauthorized access to government and financial systems.  
📌 **1988** – **First Major Internet Worm (Morris Worm)**: Spreads across ARPANET, causing major slowdowns and raising security awareness.  
📌 **1989** – **First Ransomware Attack ("AIDS Trojan")**: Demands payment to unlock infected computers.

**🔹 1990s: The Internet Boom & Rise of Cybercrime**

📌 **1991** – **PGP Encryption Released**: Phil Zimmermann introduces "Pretty Good Privacy" for secure email communication.  
📌 **1995** – **First Large-Scale Phishing Attacks**: Fraudulent emails trick users into revealing passwords.  
📌 **1999** – **Melissa Virus Disrupts Email Systems**: One of the first widespread email-based malware outbreaks.



**🔹 2000s: The Age of Cyber Warfare & Advanced Threats**

📌 **2000** – **Denial of Service (DoS) Attacks Rise**: Hackers use botnets to overload major websites like Yahoo, CNN, and Amazon.  
📌 **2001** – **Code Red & Nimda Worms**: Attack Microsoft IIS web servers, causing widespread damage.  
📌 **2007** – **Cyber War Begins (Estonia Attack)**: Russia-linked cyberattacks take down Estonia’s digital infrastructure.  
📌 **2008** – **Conficker Worm Infects Millions**: Targets Windows computers and spreads rapidly.



**🔹 2010s: Nation-State Attacks & Cybersecurity Evolution**

📌 **2010** – **Stuxnet Worm Discovered**: First known cyberweapon targeting Iran’s nuclear program.  
📌 **2013** – **Massive Data Breaches (Yahoo, Target, Adobe)**: Millions of accounts compromised.  
📌 **2017** – **WannaCry & NotPetya Ransomware**: Causes global disruption, affecting hospitals, businesses, and governments.  
📌 **2018** – **Facebook–Cambridge Analytica Data Scandal**: Highlights data privacy concerns and the misuse of personal information.

**🔹 2020s: AI, Cloud Security, & Zero-Trust Architecture**

📌 **2020** – **Rise of AI-Driven Attacks & Deepfakes**: Attackers use AI for phishing, fraud, and misinformation.  
📌 **2021** – **Colonial Pipeline Ransomware Attack**: Major U.S. fuel pipeline shut down, leading to supply chain concerns.  
📌 **2023** – **Quantum Cryptography Developments**: Researchers advance quantum-safe encryption methods.  
📌 **2024+** – **The Future of Cybersecurity**: Growing focus on zero-trust security models, AI-driven defense, and regulations to combat cybercrime.

This timeline showcases how cybersecurity has evolved, highlighting major threats and the corresponding advancements in defense. Do you want any additions or adjustments? 🚀

make a one-page visual timeline that clearly outline the evolution of cybersecurity

https://github.com/Idahosadave/3mtt-Project/blob/10b28fbfb3a5d8fe431079aa9eeb054e4246a7a7/create%20a%20timeline%20highlighting%20the%20key%20event.docx