+--------------------------------------------------------------------------------+

| CYBERSECURITY EVOLUTION

+--------------------------------------------------------------------------------+

| 1971 | Creeper Virus

| | • The first self-replicating program on ARPANET sparks

| | the idea that code can “travel” across networks.

+--------------------------------------------------------------------------------+

| 1982 | Elk Cloner

| | • An early virus for personal computers, illustrating the

| | vulnerability of emerging PC systems.

+--------------------------------------------------------------------------------+

| 1988 | Morris Worm

| | • One of the first significant Internet worms that exposed

| | large-scale network vulnerabilities.

+--------------------------------------------------------------------------------+

| 1990s | Rise of Firewalls & Antivirus Software

| | • A period when dedicated security software and hardware

| | defenses (intrusion detection systems, firewalls, etc.)

| | began to mature alongside the growth of the Internet. |+--------------------------------------------------------------------------------+

|2000-03 | Era of High-Profile Worms & Attacks

| | • Attacks such as Code Red, Nimda, and SQL Slammer showcased

| | the peril of unpatched systems and spurred rigorous security

| | measures in businesses and governments.

+--------------------------------------------------------------------------------+

| 2010 | Stuxnet

| | • A sophisticated malware targeting industrial control systems heralded the age of state-sponsored cyber warfare.

+--------------------------------------------------------------------------------+

| 2013 | Snowden Revelations

| | • Exposed mass surveillance and cyber espionage at a global

| | scale, shifting public and political discourse on

| | cybersecurity and privacy.

+--------------------------------------------------------------------------------+

| 2017 | WannaCry & NotPetya

| | • Global ransomware attacks that stressed the vulnerabilities

| | of legacy systems and the interconnected nature of modern

| | critical infrastructure.

+--------------------------------------------------------------------------------+

| 2020s | AI-Driven Defense, Cloud Security & IoT Vulnerabilities

| | • With the accelerated shift to remote work and smart devices,

| | integrated security frameworks (including AI-enhanced threat

| | detection and cloud security measures) are now at the forefront.

+------------------------------------------------------------------------------