

Appendix 8. Glossary

APTs	Advanced Persistent Threats — Technically sophisticated and covert cyberattacks on targeted entities or people that can remain undetected for a significant period of time and aimed usually at collecting confidential information or causing significant damage.
BEC	Business Email Compromise — A type of fraudulent attack in which an attacker impersonates a company employee, manager, or contractor in business correspondence in order to cause funds to be transferred, obtain data, or cause other actions detrimental to the company.
DDoS	Distributed Denial of Service — An attack in which multiple devices simultaneously flood a server, service, or network with requests in order to overload it and make it unavailable to users.
DLL hijacking	Dynamic Link Library (DLL) Hijacking — An attack technique in which an attacker replaces or places a malicious DLL library so that a legitimate program loads it instead of the regular one and executes malicious code.
DPI	Deep Packet Inspection — A network traffic analysis technology that makes it possible to examine not only packet headers but also their contents to identify threats, filter data, and control the transfer of information.
EDR	Endpoint Detection and Response — A class of information security solutions designed to monitor endpoints, identify suspicious activity, investigate incidents, and respond to them.
IoT	Internet of Things — A network of interconnected physical devices equipped with sensors, software, and communications tools to exchange data with each other, with cloud systems, and with other digital platforms.
LLM	Large Language Model (LLM) — An artificial intelligence model trained on large amounts of text data and capable of understanding and generating natural language and performing text-related tasks.
MDR	Managed Detection and Response (MDR) — A service or class of services in which an external team of experts uses specialized technologies and analytics to identify threats, investigate incidents, and help customers respond to them.
OCR	Optical Character Recognition (OCR) — A technology for converting text from images, scans, or photographs into a machine-readable format for further processing, storage, and retrieval.
OT	Operational Technology — The set of systems, hardware, and software that control physical processes in industry, energy, transport, and other critical infrastructure facilities.
PoSA	Point-of-Sale Activation - thin cardboard cards for electronic product delivery.
SOC	Security Operations Center — A dedicated function or department that continuously monitors information security events, identifies threats, and coordinates incident response.
TIP	Threat Intelligence Platform — A platform for collecting, enriching, analyzing, and using cyberthreat data, including indicators of compromise, attacker information, and attacker tactics.

V2X	Vehicle-to-Everything — A technology for exchanging information in real time between a vehicle and other entities: cars, road infrastructure, pedestrians, networks, and cloud systems.
XDR	Extended Detection and Response — A class of information security solutions that combine data from multiple sources (endpoints, networks, servers, clouds, and other systems) to detect sophisticated attacks and provide a centralized response.
ICS	Industrial Control System — A set of software and hardware designed to automate, monitor, and control industrial processes in production and industrial infrastructure.
Wipers	Malicious software designed to destroy, damage, or permanently erase data and disrupt the operation of information systems.
Vendor	Vendor (supplier, manufacturer) — A company that develops, produces and/or supplies products, solutions or services under its own brand.
Viruses, worms, Trojans	Common types of malware: viruses embed themselves in files and spread when they are executed, worms spread on their own, and Trojans disguise themselves as legitimate software.
Cyberstalking	Systematic stalking, intimidation, or control of an individual using digital technology, including instant messaging, email, social media, spyware, and other online tools.
Clicker games	A genre of digital games based on repeated simple user actions or automatic accumulation of game resources; also known as idle games.
Endpoints, end devices	Physical devices connected to a corporate or other network and capable of exchanging data with other systems: computers, laptops, smartphones, servers, virtual machines, and embedded devices.
Mining	The process of using computing resources to confirm transactions on a blockchain network and receive rewards in the form of digital assets.
Generation Z	The generation of people born between the mid-1990s and early 2010s who grew up in an environment when digital technology and the internet were widely used.
Reverse engineering	The process of analyzing software, code, a device, or a technology to understand its operating principles, internal structure, algorithms, and potential vulnerabilities.
Stealer	Malware designed to covertly collect and extract sensitive information, including passwords, cookies, banking information, and account credentials.
Hackathons	Competitions or intensive team events in which participants create prototypes of digital solutions, products, or services in a limited time period.
Exploit	Software code, a script, or a technique that takes advantage of a vulnerability in a system, application, or device to perform unauthorized actions.