GLOSSARY OF TECHNICAL TERMS

This glossary of technical terms contains explanations of certain technical terms used in this document in connection with our Company and our business. Such terminology and meanings may not correspond to standard industry meanings or usages of those terms.

"adversarial sample-mutation engines"	Systems that automatically generate and modify attack inputs (adversarial samples) using controlled mutation techniques to test, evade, or harden detection models.
"AI"	Artificial intelligence.
"AIoT"	AI of things.
"API"	Application programming interface, a software intermediary that enables communication, function invocation, and data exchange between different applications or systems.
"behavior modeling"	The process of analyzing and learning patterns of normal and anomalous activity across users, systems, or networks to detect deviations that may indicate malicious behavior.
"container"	A lightweight, isolated runtime environment that packages an application and its dependencies while sharing the host operating system kernel.
"data exfiltration"	The intentional or accidental leakage, transmission, access, or disclosure of data to unauthorized individuals, organizations, or systems, including intentional theft and maloperation, and accidental leakage caused by system vulnerabilities.
"data inventory"	The organized record of an organization's data assets, including their location, type, ownership, and sensitivity.
"data lineage"	The tracking of data from its origin through all transformations and movements across systems.
"data residency"	The geographic location and jurisdiction where data is stored and processed.
"desensitization"	The process of converting, masking, or replacing sensitive data through technical means to prevent unauthorized access and leakage, while maintaining data availability in specific scenarios.
"homomorphic encryption"	A cryptographic technique that allows computations to be performed on encrypted data without decrypting it.
"information silos"	Isolated data systems or repositories within an organization that are mutually independent, difficult to interconnect, share, or integrate.
"IoT"	Internet of Things

GLOSSARY OF TECHNICAL TERMS

"log"	A record of events or activities generated by systems, applications, or devices.
"machine learning"	A method of enabling systems to learn patterns from data and improve performance without explicit programming.
"masking"	One of the common techniques for data desensitization, achieved by partially hiding the content of the data.
"metadata"	Data used to describe, annotate, or explain the attributes, sources, structures, usage patterns, and contextual information of other data.
"penetration testing"	The process in which authorized security professionals simulate the techniques and methods of real-world attackers to conduct offensive testing on target systems, networks, or applications, in order to proactively discover security vulnerabilities, assess security risks, and verify the effectiveness of existing protective measures.
"petabyte"	A unit of measurement for data, where 1 petabyte (PB) equals 1,024 terabytes (TB) and 1 terabyte equals 1,024 gigabytes (GB).
"privilege escalation"	The exploitation of a system to gain higher access rights than those originally granted.
"red-blue confrontation"	A cybersecurity exercise in which an attacking team (red team) and a defending team (blue team) simulate real-world threats to test and improve security capabilities.
"retention rules"	Rules define how long data is stored and when it should be archived or deleted.
"Security Data Center"	A centralized facility or system for storing, managing, and protecting data with integrated physical and data security controls.
"SOAR"	Security Orchestration, Automation and Response, a cybersecurity approach that integrates tools and automates workflows to detect, analyze, and respond to security threats efficiently.
"SQL"	Structured Query Language, a programming language used to manage and query data stored in relational databases.
"stress-testing"	The process of evaluating a system's performance and resilience under extreme or high-load conditions.
"threat intelligence"	The information and analysis about potential or existing cyber threats used to inform and improve security decisions.
"virtualization"	The technology that enables multiple isolated computing environments to run on a single physical system by abstracting hardware resources.