Cyber Security Terms and Definitions

AES – Advanced Encryption Standard

AET – Advanced Evasion Techniques

APT – Advanced Persistent Threat

CASB – Cloud Access Security Broker

CISA – Cybersecurity and Infrastructure Security Agency

CISO - Chief Information Security Officer

CMDB – Configuration Management Database

CnC or C2– Command and Control (server)

COTS – Commercial Off the Shelf (software)

CRLF – Carriage Return Line Feed

CSPM – Cloud Security Posture Management

CSRF – Cross Site Request Forgery

DAR – Data at Rest

DDoS – Distributed Denial of Service

DGA – Domain Generation Algorithm

DIT – Data In Transit

DLP – Data Loss Prevention

DMARC – Domain Based Message Authentication Reporting and Conformance

DNS - Domain Name System

DNSSEC – Domain Name System Security Extensions

EDR – Endpoint Detection and Response

GDPR – General Data Protection and Response

GPO – Group Policy Object

HMAC – Hash-based Message Authentication Code

HSM – Hardware Security Module

IaaS – Infrastructure as a Service

IAM - Identity and Access Management

IOC – Indicator of Compromise

IOT – Internet of Things

IPS – Intrusion Prevention System

JWT – JSON Web Tokens

Keylogger – Keystroke Logger

Kerberoasting – Kerberos-based attack

MAM – Mobile Application Management

MDM – Mobile Device Management

Metamorphic Malware - Malware that rewrites its own code

Polymorphic Malware - Malware that changes its code using encryption

MFA – Multi-Factor Authentication

MITM – Man in the Middle (attack)

NDR – Network Detection and Response

NGAV – Next-Generation Antivirus

NGFW – Next Generation Firewall

NIST – National Institute of Standards and Technology

NTLM – New Technology LAN Manager

NTPsec – Network Time Protocol – Secure

OTP – One Time Password

PaaS – Platform as a Service

PAM – Privileged Access Management

POLP – Principal of Least Privilege

RCE – Remote Code Execution

RDP – Remote Desktop Service

SaaS - Software as a Service

Salting - Technique to vary hashing results

SHA – Secure Hashing Algorithm

SIEM – Security Incident and Event Manager

SNMP – Simple Network Management Protocol

SOAR – Secure Orchestration, Automation and Response

SOC - Security Operations Center

SPAN – Switch Port Analyzer

SQL – Structured Query Language

STIX – Structured Threat Information Expression

TAP – Test Access Point

TAXII – Trusted Automated Exchange of Intelligence Information

TDE – Transport Data Encryption

Threat Vector - Method a threat uses to reach the target

TLS - Transport Layer Security

TPM – Trusted Platform Module

Trojan Horse - Malware that masquerades as legitimate software

UEBA – User and Entity Behavior Analytics

UEFI – Unified Extensible Firmware Interface

VOIP – Voice over Internet Protocol

VPC – Virtual Private Cloud

VPN – Virtual Private Network

WEB – Wired Equivalent Privacy

WPA – WiFi Protected Access

XSS – Cross Site Scripting

Zero Day - Vulnerability that is used by attackers before the vendor knows about it

Zero Trust - Security Architecture designed to Enforce Access Validation