3DES
Triple Digital Encryption Algorithm

AAA
Authentication, Authorization, and Accounting

ABAC
Attribute-based Access Control

ACL
Access Control List

AD
Active Directory

AES
Advanced Encryption Standard

AES256
Advanced Encryption Standards 256bit

AH
Authentication Header

AI
Artificial Intelligence

AIS
Automated Indicator Sharing

ALE
Annualized Loss Expectancy

AP
Access Point

API
Application Programming Interface

APT
Advanced Persistent Threat

ARO
Annualized Rate of Occurrence

ARP
Address Resolution Protocol

ASLR
Address Space Layout Randomization

ASP
Active Server Pages

ATT&CK
Adversarial Tactics, Techniques,

AUP
Acceptable Use Policy

AV
Antivirus

BASH
Bourne Again Shell

BCP
Business Continuity Planning

BGP
Border Gateway Protocol

BIA
Business Impact Analysis

BIOS
Basic Input/Output System

BPA
Business Partnership Agreement

BPDU
Bridge Protocol Data Unit

BSSID
Basic Service Set Identifier

BYOD
Bring Your Own Device

CA
Certificate Authority

CAR
Corrective Action Report

CASB
Cloud Access Security Broker

CBC
Cipher Block Chaining

CBT
Computer-based Training

CCMP
Counter-Mode/CBC-MAC Protocol

CCTV
Closed-Circuit Television

CERT
Computer Emergency Response Team

CFB
Cipher Feedback

CHAP
Challenge-Handshake Authentication Protocol

CIO
Chief Information Officer

CIRT
Computer Incident Response Team

CIS
Center for Internet Security

CMS
Content Management System

CN
Common Name

COOP
Continuity of Operations Planning

COPE
Corporate-owned Personally Enabled

CP
Contingency Planning

CRC
Cyclic Redundancy Check

CRL
Certificate Revocation List

CSIRT
Computer Security Incident Response Team

CSO
Chief Security Officer

CSP
Cloud Service Provider

CSR
Certificate Signing Request

CSRF
Cross-Site Request Forgery

CSU
Channel Service Unit

CTM
Counter-Mode

CTO
Chief Technology Officer

CVE
Common Vulnerabilities and Exposures

CVSS
Common Vulnerability Scoring System

CYOD
Choose Your Own Device

DAC
Discretionary Access Control

DBA
Database Administrator

DDoS
Distributed Denial-of-Service

DEP
Data Execution Prevention

ECB
Electronic Code Book

ECC
Elliptic-curve Cryptography

ECDHE
Elliptic-curve Diffie-Hellman Ephemeral ECDSA

EFS
Encrypted File System

EIP
Extended Instruction Pointer

EOL
End of Life

EOS
End of Service

ERP
Enterprise Resource Planning

ESN
Electronic Serial Number

ESP
Encapsulating Security Payload ESSID

FDE
Full Disk Encryption

FIM
File Integrity Monitoring

FPGA
Field Programmable Gate Array

FRR
False Rejection Rate

FTP
File Transfer Protocol

FTPS
Secured File Transfer Protocol

GCM
Galois/Counter Mode

GDPR
General Data Protection Regulation GPG

GPO
Group Policy Object

GPS
Global Positioning System

GPU
Graphics Processing Unit

GRE
Generic Routing Encapsulation

HA
High Availability

HDD
Hard Disk Drive

HIDS
Host-based Intrusion Detection System

HIPS
Host-based Intrusion Prevention System

HMAC
Hash-based Message Authentication Code

HOTP
HMAC-based One-time Password

HSM
Hardware Security Module

HSMaaS
Hardware Security Module as a Service HTML

HTTP
Hypertext Transfer Protocol

HTTPS
Hypertext Transfer Protocol Secure HVAC

IAM
Identity and Access Management ICMP

IDEA
International Data Encryption Algorithm IDF

IdP
Identity Provider

IDS
Intrusion Detection System

IEEE
Institute of Electrical and Electronics Engineers IKE

IM
Instant Messaging

IMAP4
Internet Message Access Protocol v4 IoC

IoT
Internet of Things

IP
Internet Protocol

IPS
Intrusion Prevention System

IPSec
Internet Protocol Security

IR
Incident Response

IRC
Internet Relay Chat

IRP
Incident Response Plan

ISA
Interconnection Security Agreement

ISFW
Internal Segmentation Firewall

ISO
International Organization for Standardization ISP

ISSO
Information Systems Security Officer ITCP

IV
Initialization Vector

KDC
Key Distribution Center

KEK
Key Encryption Key

L2TP
Layer 2 Tunneling Protocol

LAN
Local Area Network

LDAP
Lightweight Directory Access Protocol

LEAP
Lightweight Extensible Authentication Protocol MaaS

MAC
Media Access Control

MAM
Mobile Application Management

MAN
Metropolitan Area Network

MBR
Master Boot Record

MD5
Message Digest 5

MDF
Main Distribution Frame

MDM
Mobile Device Management

MFA
Multifactor Authentication

MFD
Multifunction Device

MFP
Multifunction Printer

ML
Machine Learning

MMS
Multimedia Message Service

MOA
Memorandum of Agreement

MOU
Memorandum of Understanding

MS-CHAP
Microsoft Challenge Handshake

MSP
Managed Service Provider

MSSP
Managed Security Service Provider

MTBF
Mean Time Between Failures

MTTF
Mean Time to Failure

MTTR
Mean Time to Repair

MTU
Maximum Transmission Unit

NAC
Network Access Control

NAS
Network-attached Storage

NAT
Network Address Translation

NDA
Non-disclosure Agreement

NFC
Near-field Communication

NFV
Network Function Virtualization

NGFW
Next-generation Firewall

NG-SWG
Next-generation Secure Web Gateway

NIC
Network Interface Card

NIDS
Network-based Intrusion Detection System

NIPS
Network-based Intrusion Prevention System

NIST
National Institute of Standards & Technology

NOC
Network Operations Center

NTFS
New Technology File System

NTLM
New Technology LAN Manager

NTP
Network Time Protocol

OAUTH
Open Authentication

OCSP
Online Certificate Status Protocol

OID
Object Identifier

OS
Operating System

OSI
Open Systems Interconnection

OSINT
Open-source Intelligence

OSPF
Open Shortest Path First

OT
Operational Technology

OTA
Over-The-Air

OTG
On-The-Go

OVAL
Open Vulnerability and Assessment Language

OWASP
Open Web Application Security Project

P12
PKCS #12

P2P
Peer-to-Peer

PaaS
Platform as a Service

PAC
Proxy Auto Configuration

PAM
Pluggable Authentication Modules

PAP
Password Authentication Protocol

PAT
Port Address Translation

PBKDF2
Password-based Key Derivation Function 2

PBX
Private Branch Exchange

PCAP
Packet Capture

PCI DSS
Payment Card Industry Data Security Standard

PDU

Power Distribution Unit

PE

Portable Executable

PEAP

Protected Extensible Authentication Protocol

PED

Portable Electronic Device

PEM

Privacy Enhanced Mail

PFS

Perfect Forward Secrecy

PGP

Pretty Good Privacy

PHI

Personal Health Information

PII

Personally Identifiable Information

PIN

Personal Identification Number

PIV

Personal Identity Verification

PKCS

Public Key Cryptography Standards

PKI

Public Key Infrastructure

PoC
Proof of Concept

POP
Post Office Protocol

POTS
Plain Old Telephone Service

PPP
Point-to-Point Protocol

PPTP
Point-to-Point Tunneling Protocol

PSK
Preshared Key

PTZ
Pan-Tilt-Zoom

PUP
Potentially Unwanted Program

QA
Quality Assurance

QoS
Quality of Service

RA
Registration Authority

RAD
Rapid Application Development

RADIUS
Remote Authentication Dial-in User Service

RAID
Redundant Array of Inexpensive Disks

RAM
Random Access Memory

RAS
Remote Access Server

RAT
Remote Access Trojan

RC4
Rivest Cipher version 4

RCS
Rich Communication Services

RFC
Request for Comments

RFID
Radio Frequency Identifier

ROI
Return on Investment

RPO
Recovery Point Objective

RSA
Rivest, Shamir, & Adleman

RTBH
Remotely Triggered Black Hole

RTO
Recovery Time Objective

RTOS
Real-time Operating System

RTP
Real-time Transport Protocol

S/MIME
Secure/Multipurpose Internet Mail Extensions

SaaS
Software as a Service

SAE
Simultaneous Authentication of Equals

SAML
Security Assertions Markup Language

SCADA
Supervisory Control and Data Acquisition

SCAP
Security Content Automation Protocol

SCEP
Simple Certificate Enrollment Protocol

SDK
Software Development Kit

SDLC
Software Development Life Cycle

SDLM
Software Development Life-cycle Methodology

SDN
Software-defined Networking

SDP
Service Delivery Platform

SDV
Software-defined Visibility

SED
Self-Encrypting Drives

SEH
Structured Exception Handling

SFTP
SSH File Transfer Protocol

SHA
Secure Hashing Algorithm

SIEM
Security Information and Event Management

SIM
Subscriber Identity Module

SIP
Session Initiation Protocol

SLA
Service-level Agreement

SLE
Single Loss Expectancy

SMB
Server Message Block

SMS
Short Message Service

SMTP
Simple Mail Transfer Protocol

SMTPS
Simple Mail Transfer Protocol Secure

SNMP
Simple Network Management Protocol

SOAP
Simple Object Access Protocol

SOAR
Security Orchestration, Automation, Response

SoC
System on Chip

SOC
Security Operations Center

SPF
Sender Policy Framework

SPIM
Spam over Internet Messaging

SQL
Structured Query Language

SQLi
SQL Injection

SRTP
Secure Real-time Transport Protocol

SSD
Solid State Drive

SSH
Secure Shell

SSID
Service Set Identifier

SSL
Secure Sockets Layer

SSO
Single Sign-on

STIX
Structured Threat Information eXpression

STP
Shielded Twisted Pair

SWG
Secure Web Gateway

TACACS+
Terminal Access Controller Access Control System

TAXII
Trusted Automated eXchange of Indicator Information

TCP/IP
Transmission Control Protocol/Internet Protocol

TGT
Ticket Granting Ticket

TKIP
Temporal Key Integrity Protocol

TLS
Transport Layer Security

TOTP

Time-based One Time Password

TPM
Trusted Platform Module

TSIG
Transaction Signature

TTP
Tactics, Techniques, and Procedures

UAT
User Acceptance Testing

UDP
User Datagram Protocol

UEBA
User and Entity Behavior Analytics

UEFI
Unified Extensible Firmware Interface

UEM
Unified Endpoint Management

UPS
Uninterruptible Power Supply

URI
Uniform Resource Identifier

URL
Universal Resource Locator

USB
Universal Serial Bus

USB OTG

USB On-The-Go

UTM
Unified Threat Management

UTP
Unshielded Twisted Pair

VBA
Visual Basic for Applications

VDE
Virtual Desktop Environment

VDI
Virtual Desktop Infrastructure

VLAN
Virtual Local Area Network

VLSM
Variable-length Subnet Masking

VM
Virtual Machine

VoIP
Voice over IP

VPC
Virtual Private Cloud

VPN
Virtual Private Network

VTC
Video Teleconferencing

WAF

Web Application Firewall

WAP
Wireless Access Point

WEP
Wired Equivalent Privacy

WIDS
Wireless Intrusion Detection System

WIPS
Wireless Intrusion Prevention System

WORM
Write Once Read Many

WPA
WiFi Protected Access

WPS
WiFi Protected Setup

XaaS
Anything as a Service

XML
Extensible Markup Language

XOR
Exclusive Or

XSRF
Cross-site Request Forgery

XSS
Cross-site Scripting