Tech & InfoSec Acronym Cheat Sheet for Beginners

@ktgblogstech

Acronym	Meaning
2FA	Two Factor Authentication
AAA	Authentication, Authorization, Auditing
ACL	Access Control List
AD	Active Directory
ADFS	Active Directory Federation Services
AES	Advanced Encryption Standard
AP	Access Point
API	Application Programming Interface
APT	Advanced Persistent Threat
ARP	Address Resolution Protocol
ATP	Advanced Threat Protection
AUP	Acceptable Use Policy
AV	Antivirus
AWS	Amazon Web Services
BGP	Border Gateway Protocol
BIA	Business Impact Analysis
BIOS	Basic Input & Output System
BYOD	Bring Your Own Device
C&C/C2	Command & Control
CA	Certification Authority
CAPTCHA	Completely Automated Public Turing Test to Tell Computers & Humans Apart
CASB	Cloud Access Security Broker
CBK	Common Body of Knowledge
CCNA	Cisco Certified Network Associate
CCSP	Certified Cloud Security Professional
CERT	Computer Emergency Response Team
CEH	Certified Ethical Hacker
CIA	Confidentiality, Integrity, Availability
CIDR	Classless Inter-Domain Routing
CIRT	Computer Incident Response Team
CIS	Center for Internet Security
CISM	Certified Information Security Manager

CISO	Chief Information Security Officer
CISSP	Certified Information Systems Security Professional
CLI	Command-Line Interface
CMDB	Configuration Management Database
COB	Close of Business
CS	Computer Science
CS	Cybersecurity
CSPM	Cloud Security Posture Management
CVE	Common Vulnerabilities & Exposure
DAC	Discretionary Access Control
DAST	Dynamic Application Security Testing
DB	Database
DDoS	Distributed Denial of Service
DES	Digital Encryption Standard
DFIR	Digital Forensics Incident Response
DLP	Data Loss Prevention
DMARC	Domain-based Message Authentication, Reporting & Conformance
DMZ	Demilitarized Zone
DNS	Domain Name System
DoS	Denial of Service
DPA	Data Processing Agreement
DPIA	Data Privacy Impact Assessment
DR	Disaster Recovery
DRP	Disaster Recovery Plan
EAL	Evaluated Assurance Level
EDR	Endpoint Detection & Response
EOD/M/Y	End of Day/Month/Year
EOP	Escalation/Elevation of Privilege
FDE	Full Disk Encryption
FISMA	Federal Information Security Management Act
FQDN	Fully Qualified Domain Name
FTP	File Transfer Protocol
FTPS	File Transfer Protocol-Secure (SSL/TLS)
FW	Firewall

GCP	Google Cloud Platform
GDPR	General Data Protection Regulation
GLBA	Gramm-Leach-Bliley Act
GPO	Group Policy Object
GRC	Governance, Risk & Compliance
GRE	Generic Routing Encapsulation
HA	High Availability
HD	Hard Disk
HIPAA	Healthcare Insurance Portability & Accountability Act
HITECH	Health Information Technology for Economic & Clinical Health
HITRUST	Health Information Trust Alliance
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IaaS	Infrastructure-as-a-Service
IAM	Identity & Access Management
ICMP	Internet Control Message Protocol
ICS	Industrial Control System
IDS	Intrusion Detection System
IEEE	Institute for Electrical & Electronics Engineers
IKE	Internet Key Exchange
IOC	Indicator of Compromise
IP	Internet Protocol
IPS	Intrusion Prevention System
IPSec	Internet Protocol Security
IR	Incident Response
IRT	Incident Response Team
IS	Information Systems
IS	Information Security
ISAKMP	Internet Security Association Key Management Protocol
ISACA	Information Systems Audit & Control Association
ISC ²	International Information System Security Certification Consortium
ISO	International Organization for Standardization
IT	Information Technology
ITIL	Information Technology Infrastructure Library

JSON	JavaScript Object Notation
JWT	JSON Web Token
KB	Knowledge Base
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LFI	Local File Inclusion
MAC	Mandatory Access Control
MAC	Message Authentication Code
MD5	Message Digest 5
MDM	Mobile Device Management
MFA	Multi-factor Authentication
MIME	Multipurpose Internet Mail Extensions
MITM	Man-in-the-Middle
MTTR	Mean Time to Recover
MTTR	Meant Time to Remediate
NAC	Network Access Control
NAT	Network Address Translation
NCSC	National Cyber Security Center
NFS	Network File System
NGAV	Next Generation Antivirus
NGFW	Next Generation Firewall
NIC	Network Interface Card
NIDS	Network Intrusion Detection System
NIPS	Network Intrusion Prevention System
NIST	National Institute of Standards & Technology
NOC	Network Operations Center
OCI	Oracle Cloud Infrastructure
OOTB	Out of the Box
OPSEC	Operational Security
OS	Operating System
OSI	Open Systems Interconnection
OSINT	Open-Source Intelligence
OSPF	Open Shortest Path First
OT	Operational Technology

OTP	One-time Password
OWA	Outlook Web Access
OWASP	Open Web Application Security Project
P2P	Peer-to-Peer
PaaS	Platform-as-a-Service
PAM	Privilege Access Management
PAN	Personal Area Network
PAT	Port Address Translation
PCAP	Packet Capture
PCI	Payment Card Industry
PCI-DSS	Payment Card Industry Data Security Standard
PE	Portable Executable
PE	Privilege Escalation/Elevation
PGP	Pretty Good Privacy
PHI	Personal Health Information
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PLC	Programmable Logic Controller
PM	Project Manager
PO	Purchase Order
PPP	Point-to-Point Protocol
PPTP	Point-to-Point Tunneling Protocol
PS	PowerShell
RaaS	Ransomware-as-a-Service
RAT	Remote Access Tool
RAT	Remote Access Trojan
RAT	Remote Administration Tool
RBAC	Role-Based Access Control
RCA	Root Cause Analysis
RCE	Remote Code Execution
RDP	Remote Desktop Protocol
RFC	Request for Change

RFID	Radio Frequency Identification
RFP	Request for Proposal
RO	Read-Only
RPO	Recovery Point Objective
RTO	Recovery Time Objective
RW	Read-Write
SaaS	Software-as-a-Service
SAML	Security Assertion Markup Language
SAST	Static Application Security Testing
SCADA	Supervisory Control & Data Acquisition
SD-WAN	Software-Defined Wide Area Network
SDLC	Software Development Lifecycle
SDN	Software-Defined Networking
SECOPS	Security Operations
SFTP	Secure File Transfer Protocol (SSH)
SHA	Secure Hashing Algorithm
SID	Security Identifier
SIEM	Security Information & Event Management
SLA	Service Level Agreement
SMB	Server Message Block
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SOAP	Simple Object Access Protocol
SOAR	Security Orchestration, Automation & Response
SOC	Security Operations Center
SOP	Standard Operating Procedure
SOW	Statement of Work
SPF	Sender Policy Framework
SPN	Service Principal Name
SPOF	Single Point of Failure
SQL	Structured Query Language
SSE	Server-Side Encryption
SSH	Secure Shell
SSID	Service Set Identifier

SSL	Secure Sockets Layer
SSN	Social Security Number
SSO	Single Sign On
SSRF	Service-Side Request Forgery
TCP	Transmission Control Protocol
TLD	Top-Level Domain
TLDR	Too Long, Didn't Read
TLS	Transport Layer Security
ToE	Target of Evaluation
TPM	Trusted Platform Module
TTD	Time to Detection
TTL	Time to Live
TTP	Tactics, Techniques & Procedures
UAC	User Account Control
UAT	User Acceptance Testing
UDP	User Datagram Protocol
UPN	User Principal Name
UPS	Uninterruptible Power Supply
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
VA	Vulnerability Assessment
VHD	Virtual Hard Disk
VLAN	Virtual Local Area Network
VM	Vulnerability Management
VM	Virtual Machine
VoIP	Voice over Internet Protocol
VPC	Virtual Private Cloud
VPN	Virtual Private Network
VPR	Vulnerability Priority Rating
WAF	Web Application Firewall
WAN	Wide Area Network
WAP	Wireless Access Point
XDR	Extended Detection & Response
XSRF	Cross Site Request Forgery

XXS	Cross Site Scripting
YARA	Yet Another Recursive Acronym
ZT	Zero Trust