Cybersecurity Buzzwords

Ntirety

Cybersecurity Buzzwords

Cybersecurity threats can feel even more daunting when they are described and identified by acronyms and industry buzzwords not used in everyday conversation. But when it comes to protecting business IT and sensitive data, knowledge is power. Build a better defense vocabulary using the definitions and meanings of critical cybersecurity terminology below.

Schedule a consultation to see how compliant security will protect and optimize your business by visiting **ntirety.com/get-started** today.

A

AD DS (Active Directory Domain Services) A server function within the Active Directory Microsoft developed service that lets administrators store and manage information about resources from a network and application data in a distributed database

AI (Artificial Intelligence) Any computer or machine using computing power to solve problems that might typically involve a human

Alarm An observable event that could cause harm or potential compliance violation detected through threat sensors or log collection appliances deployed within a computer system's environment

Amazon S3 "Simple Storage Service" from Amazon Web Services that offers data storage

Analytics The ability to utilize data to make informed decisions on potential security threats or vulnerabilities

Anomaly Detection The ability to monitor for unusual events or trends in network traffic

Antivirus Software designed to detect, prevent and eliminate malware

API (Application Programming Interface) Programming code that allows communication between computers or computer programs

APTs (Advanced Persistent Threats) A prolonged and targeted cyberattack in which an intruder gains access to a network to steal data and remains undetected for an extended period of time

Automation The use of applications to automatically carry out processes based on certain events or triggers

Click on the terms below to take you to the page where the term is.

Types of Cyberattacks and Threats

AWS (Amazon Web Services) A cloud computing platform that offers compute power, database storage, content delivery, and more

Azure A cloud-based service designed by Microsoft that provides tools needed for a business to run any virtual operations such as data storage or analytics

B

Blockchain A database that holds encrypted blocks of data and chains them together making it difficult for hackers to make changes in the system

Botnet A network of private computers infected with malicious software and controlled as a group without the owners' knowledge

Breach Any incident that results in unauthorized access to computer data, applications, networks or devices

BYOD (Bring Your Own Device) When a customer wants to use our service, but has existing firewalls that they would like to use instead of getting them as part of the service

C

Case (or Incident) A correlation of alarms that imply harm to an information system, violate acceptable use policies, or circumvent standard security practices

Castle Mentality This is an outdated approach to cybersecurity based on the idea that securing the perimeter of an IT environment (i.e. building castle walls and digging a moat) is enough. It is outdated because it ignores activity within the environment that may be malicious and it is becoming more and more difficult to secure the perimeter of more advanced cloud and hybrid environments.

CCPA (California Consumer Privacy Act) Law that grants consumers greater jurisdiction over personal information collected from them by businesses

CHD (Card Holder Data) Personal details from a person with a debit or credit card

CIS (Center for Internet Security) Nonprofit organization whose mission is to "identify, develop, validate, promote, and sustain best practice solutions for cyber defense and build and lead communities to enable an environment of trust in cyberspace"

Cloud-based Services available through the internet

Colocation Method of how IT equipment is installed and stored

Compliance Actions that provide proof of abidance to internal policies and external laws

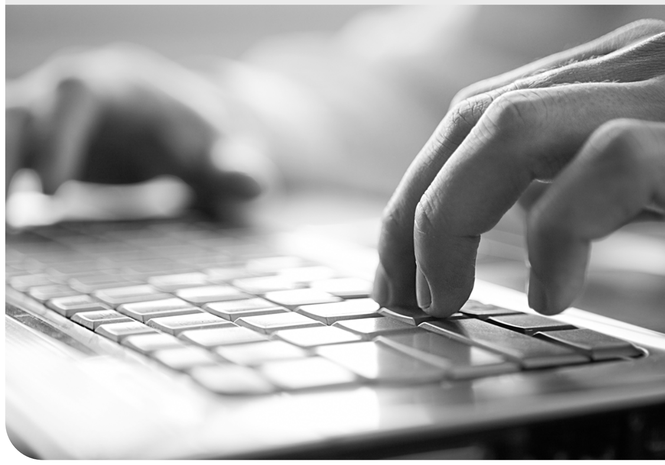
Compliance Management Solution that leverages automation and built-in compliance frameworks to ensure compliance at any time and generates audit-ready reports on demand

Compromise Disclosure of information to unauthorized persons, or a violation of the security policy of a system in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object may have occurred

Configuration The way in which parts are organized in a computer system

BYOD
(Bring Your Own Device)

When a customer wants to use our service, but has existing firewalls that they would like to use instead of getting them as part of the service



Configuration Management Engineering process in which a product's performance consistency is maintained

Container Software package that "contains" an application's code that holds files and libraries needed to run

CPQ (Configure, Price, Quote) Tool in Salesforce for businesses to use to create quotes for orders

CSP (Cloud Service Provider) Company that offers a cloud-based platform or storage services

D

DaaS (Desktop as a Service) Cloud-based resource that manages back-end responsibilities that would otherwise be provided by application software

Data Cleansing Process of identifying and eliminating inaccurate data from a database

Database Collection of data that is organized, stored, and accessed through a computer system

DDoS (Distributed denial-of-service) attack A malicious attempt to disrupt normal traffic of a targeted server, service or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic

Development Process of establishing a group of hardware and software components and their interfaces to create the layout for the buildout of a computer system

Disaster Recovery How an organization manages an event that negatively affects an IT infrastructure's usual operations

Distributed Database Database that consists of multiple databases across different physical locations

DNS (Domain Name System) Tracks names used for websites and translates domain names into their personal IP addresses

DOS (Denial of service attack) Attack where machine or network sources are inaccessible to their intended users because a cyber-criminal has shut down the system

DRaaS (Disaster Recovery as a Service) Cloud-based offering that lets an organization to store its data in a third-party cloud computer infrastructure

DW (Data Warehouse) System used for reporting and analyzing information from different sources into a single data storage unit

E

EDR (Endpoint Detection and Response) A set of cybersecurity tools which are designed to detect and remove any malware from devices- endpoints- or any other form of malicious activity on a network

Encryption The process of converting information or data into a code, especially to prevent unauthorized access

Engagement User interactions over an interface such as number of times a webpage is viewed or time spent on a site

EPP (End Point Protection) Software deployed at endpoints or entry points of end-user devices such as desktops, laptops, and mobile devices to prevent those devices from being exploited by malicious actors or campaigns

Click on the terms below to take you to the page where the term is.

Compliance Laws, Rules, and Regulations

EPTM (Endpoint Threat Management) The authentication and supervision of the access rights of endpoints devices to a network

Escalation This is a notification to a client that there is increased activity that warrants closer monitoring and/or response. In more serious cases, the SOC will email or call the client to follow up directly.

Exploit A code that takes advantage of a software vulnerability or security flaw

F

FERPA (Family Educational Rights and Privacy Act) Federal law that secures the privacy of student education information

Full stack Software development that is composed of code connecting front (UI) to back end (API, etc.) computer interfaces

G

GCP (Google Cloud Platform) cloud services offered by Google that provide data storage and analytics

GDPR (Geometric Data Protection Regulation) European Union (EU) law that gives individuals control of their personal data

Geoblocking Service that provides the ability to restrict or allow access based upon the user's source IPs geographical location

GitHub Web-based service that lets software developers to collaborate and track project progress

GLA (Guidance Level Agreement) A commitment between a service provider and a client that focuses on availability, performance, security and cost in regards to a service provided

H

Hacker A person that utilizes computers to gain unauthorized access to data

Half stack A partial software development that works on either the front end or back end of a computer interface

HIPAA (Health Insurance Portability and Accountability Act) Law that governs the use and release of an individual's health records

HITRUST (Health Information Trust Alliance) Organization made up of representatives from the healthcare industry that helps healthcare groups and their providers with security and compliance matters

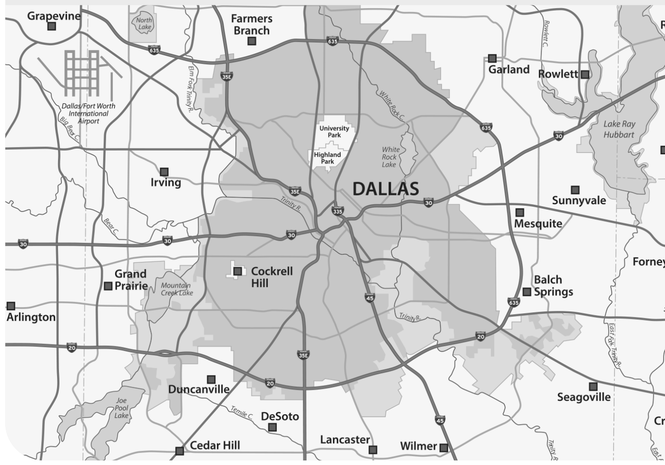
I

IaaS (Infrastructure-as-a-service) A form of cloud computing that delivers fundamental compute, network, and storage resources on-demand, over the internet, and on a pay-as-you-go basis

ICB (Individual Case Basis) A change is made to a set of rules based on specific circumstances

Geoblocking

Service that provides the ability to restrict or allow access based upon the user's source IPs geographical location



Identity and Access Management Framework an organization uses to manage and protect its users and their identities

IDS (Intrusion Detection System) A device or software application that monitors a network or systems for malicious activity or policy violations and sends an alarm to an administrator

Indicator of Attack A focus on finding what an attacker's specific goal is to better prepare for future attacks

Indicator of Compromise Evidence of potential attacks on a network

Interface An interaction between a computer and another object or individual such as a printer, another computer, or a human

Internet Protocol Security A set of rules to establish secure communication over the IP networks

IOT (Internet of Things) A system of interrelated computing devices, mechanical and digital machines provided with unique identifiers and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction

IP (Internet Protocol address) Numerical name for a computer network

IPS (Intrusion Prevention System) A network security/ threat prevention technology that examines network traffic flows to detect and prevent vulnerability exploits

IT Risk Management Organized approach for identifying and proactively eliminating potential issues within computer systems

K

Kill chain Framework to understand process of cyber attacks

L

LAN (Local Area Network) Collection of computers in a small area such as an office or school

Logs A record of the events occurring within an organization's systems and networks

M

Machine Learning Utilizing computer algorithms that learn through experience and analysis of large datasets to make predictions or decisions

Malicious Insider This is an internal threat to an organization that comes from a person within the organization, such as an employee, former employee, contractor, or business associate taking advantage of their security access to inflict harm on the organization. The threat may involve fraud, the theft of confidential or commercially valuable information, the theft of intellectual property, or the sabotage of computer systems.

Malware Any software intentionally designed to cause damage to a computer, server, client, or computer network, also known as malicious software

Click on the terms below to take you to the page where the term is.

Organizations and Approaches

Castle Mentality

CIS (Center for Internet Security)

HITRUST (Health Information Trust Alliance)

NIST (National Institute of Standards and Technology)

MDM (Mobile Device Management) Security software that allows organizations to enforce company policy through monitoring of employee mobile devices

MDR (Managed Detection and Response) Cybersecurity service that provides organizations with threat detection and prevention active monitoring

MPS (Messages per Second) A measurement of throughput used to understand the volume of logs that an environment generates that will need to be collected by the SIEM tool for analysis and storage

Multi-Factor Authentication Electronic confirmation method that requires a user to give two or more pieces of information in order to have access to a resource

N

Next-Generation A term often used in conjunction with firewall to describe firewalls that have advanced features for enhanced security

NFT (Non-Fungible Token) Data that is stored on a blockchain that is unique and cannot be replaced

NIDS (Network Intrusion Detection System) Device that manages a network for suspicious activity

NPS (Net Promoter Score) A measure of customer loyalty focusing on word-of-mouth promotion, passiveness, or detraction

NPS (Network Policy Server) Service that helps a user to manage network access authentication and authorization

NIST (National Institute of Standards and Technology) United States agency whose mission is to "promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life"

NoSQL (Not only Structured Query Language) A database that stores and retrieves data using unique key values such as numbers or characters rather than rows and columns

NTA (Network Traffic Analysis) The process of intercepting, recording and analyzing network traffic communication patterns in order to detect and respond to security threats

O

OSI (Open Systems Interconnection) Guidelines on how different computer systems should communicate with each other

P

PaaS (Platform-as-a-service) A cloud computing offering that provides users with a cloud environment in which they can develop, manage and deliver applications

PCI (Payment Card Industry) Standards for electronic payment usage such as credit or debit cards

Penetration Test An authorized simulated cyberattack on a computer system, performed to evaluate the security of the system

Multi-Factor Authentication

Electronic confirmation method that requires a user to give two or more pieces of information in order to have access to a resource

PHI (Protected Health Information) Information in medical records that can be traced back to an individual

Phish An attacker tricks a user into revealing confidential information using false pretenses

PII (Personally Identifiable Information) Information that can be traced to an individual's identity

POC (Proof of Concept) Evidence from an experiment that shows the feasibility of a concept

R

Ransomware A form of malware that encrypts a victim's files and an attacker demands ransom from the victim in order to regain access to their data

RAT (Remote Access Tool/Trojan) RAT is a type of malware that creates a backdoor for administrative control and unauthorized remote access to a victim's machine. Attackers can use the exploited machines to perform various malicious activities such as installing and removing programs, manipulating files, reading data from the keyboard, harvesting login credentials, etc.

RBL (Real-Time Blacklist) A list of IP addresses that are known for sending spam messages or emails

Real-Time This term means near instantaneous, and in security is often used to describe intrusion prevention measures that can identify threats and stop them with little or no reaction time needed

S

SaaS (Software-as-a-service) A cloud computing offering that provides users with access to a vendor's cloud-based software that can be accessed through web or API

Secure Remote Access Service that allows client IT staff to establish secure connections with a remote, non-public computer network

Security Posture Management Service that continuously monitors cloud resources for security threats. Our security experts will provide recommendations on improving security posture within the cloud

Security Reporting Service that provides metrics-based reporting of monthly or weekly events, granting visibility of trends and patterns, as well as common events and alarms in your infrastructure

Serverless Function A task written by a software developer to perform one action

Service Level Agreement A commitment between a client and a service provider to ensure customers are receiving the services that they are entitled to

SIEM (Security information and Event Management) Platform that combines information management with event management to provide real-time analysis of security alerts generated by applications and network hardware. It is also used to log security data and generate compliance reports.

SmartResponse Actions that are automated defensive or operational responses to triggered alarm rules

SOAR Security Automation & Orchestration

Click on the terms below to take you to the page where the term is.

as-a-Services

DaaS (Desktop as a Service)

DRaaS (Disaster Recovery as a Service)

IaaS (Infrastructure-as-a-service)

NPS (Network Policy Server)

PaaS (Platform-as-a-service)

SaaS (Software-as-a-service)

UCaaS (Unified Communications as a Service)

SOC A Security Operations Center is a centralized unit staffed by expert security personnel that deals with security issues on an organizational and technical level

SQL (Structured Query Language) Domain specific language used in programming

SSL (Secure Socket Layer) A protocol for transmitting private information via the Internet using a cryptographic system that uses two keys to encrypt data – a public key known to everyone and a private or secret key known only to the recipient of the message

T

Triage and Incident Management When the SOC examines incoming alarms to determine false positives from threats and create cases to notify the client of any identified threats

Tuning The process of configuring rules for alerts and notifications in a SIEM to remove false positives in order to make alerts more meaningful and reduce noise

U

UBA (User Behavior Analytics) UBA is a cybersecurity process involving detection of insider threats, targeted attacks, and financial fraud. UBA solutions look at patterns of human behavior, and then apply algorithms and statistical analysis to detect meaningful anomalies from those patterns—anomalies that indicate potential threats.

UCaaS (Unified Communications as a Service) Cloud-based offering that offers a variety of communication functions such as instant messaging or video conferencing

URL Filtering Allows monitoring and controlling of how users access the web over HTTP and HTTPS with the use of deep packet inspection

User Acceptance Testing Software is tested by its intended audience to determine if it is completing its functions correctly

V

VDI (Virtual Desktop Infrastructure) A desktop environment that is hosted on a central server

VMware A computer software company that provides cloud-based services allowing businesses to use multiple applications on one server

VPN (Virtual Private Network) A network that lets users send and receive data from public networks while hiding a user's identity making it more difficult for third parties to track online activity

Vulnerability A weakness which can be exploited by a cyberattack to gain unauthorized access to or perform unauthorized actions on a computer system

Vulnerability Management Service that utilizes machine learning to quickly identify and manage potential vulnerabilities in a public cloud environment

Vulnerability Scan An automated system that looks for weaknesses within network devices or software applications

URL Filtering

Allows monitoring and controlling of how users access the web over HTTP and HTTPS with the use of deep packet inspection

W

WAF (Web Application Firewall) Protects web applications from potential attacks through filtering, monitoring, and blocking

WAN (Wide Area Network) A form of telecommunication that extends over a large geographical location

X

XDR (Cross-layered detection and response) Gathers data from a variety of security endpoints, servers and other protective layers

Z

Zero Day This refers to a newly discovered software vulnerability. Because the developer has just learned of the flaw, it also means an official patch or update to fix the issue has not been released, so hackers manage to exploit the security hole before the vendor can release a patch.

Zero Trust A way of thinking that instills the notion that one should not automatically assume entities within a network are trustworthy.