Cybersecurity Glossary 101

Trustwave®
Government Solutions

For over 20 years, Trustwave and Trustwave Government Solutions have worked to provide the tools, technology and the insight to combat malicious cyber threats and protect our customers in both the public and private sectors.

In today's world, cyber threats continue to evolve, and so does the terminology. It can be challenging to keep up with the various acronyms, new defense methods and emerging technology. That's why Trustwave decided to put together this cyber security glossary. I hope this pocket guide will put the latest cyber security terminology at your fingertips.

Sincerely,

Bill Rucker

President, Trustwave Government Solutions

2FA -2 Factor Authentication

2FA requires both knowledge (like a password) and something tangible (such as a hardware or software authentication system) to gain access to a protected computer system.

Adaptive Authentication

Adaptive Authentication is a method for selecting the right authentication factors depending on a user's risk profile and tendencies - it adapts the authentication type to each situation.

AI - Artificial Intelligence

AI is technology that appears to emulate human behavior in that it can continually learn and draw its own conclusions (even based on novel or abstract concepts), engage in natural dialog with people, and / or replace people in the execution of more complex (non-routine) tasks.

AV - Antivirus

Antivirus software is a computer program or set of programs that seek, detect, prevent and/ or remove software viruses and malware (like worms, trojans and adware).

API – Application Programming Interface

API is a software intermediary that allows two applications to talk to each other. An example of this would be using an app on your mobile phone, as the app needs to connect to the internet and sends data to a server. Then the server retries that date, interprets it, performs the necessary actions and sends it back to your mobile phone.

APT - Advanced Persistent Threats

APTs are highly sophisticated and prolonged computer hacking processes that often target a specific entity for business or political motives.

ASV - Approved Scanning Vendor for PCI

An ASV is an organization deploying security services and tools (sometimes called an ASV scan solution) to conduct external vulnerability scanning services to validate adherence with the external scanning requirements of PCI DSS Requirement 11.2.2.

BAS - Breach and Attack Simulation Tools

BAS tools automate the simulation of advanced adversarial activities to help expose gaps to be remediated before a real attacker can exploit the same gaps to cause damage.

Big Data

Big Data describes new structures and techniques being applied to harness - and distill insight from - massive quantities of data.

Blockchain

A growing list of records, called blocks, linked using cryptography. It is a decentralized, distributed and public digital ledger that is used to record transactions across many computers in a way that the record can't be altered retroactively without additionally changing all successive blocks and the consent of the network.

Bot/Botnet

A botnet (combination of 'robot' and 'network') is a collection of internet-connected devices, such as PCs, servers, mobile devices and IoT devices that are controlled as a group.

Browser Isolation

Browser isolation removes the browsing process from the end user's desktop and moves it to a dedicated browser server (or cloud-based browser service) to confine related security threats.

Brute Force Attack

A brute force attack is a trial-and-error method for attempting to crack a password, username or data encryption key. The term comes from the fact that the approach relies on intensive effort ("brute force") rather than employing more sophisticated techniques.

BEC - Business Email Compromise

Business email compromise (BEC) is a form of phishing where a criminal attempts to get a worker, customer or vendor to send money or disclose private information by sending a phony email that appears to be coming from a trusted company figure.

Blended Threats

Blended threats are security threats to a network delivered using multiple vectors. For instance, a malicious URL delivered by email, with a text that encourages the recipient to click the link, is a Blended Threat attack.

C2 - Command and Control

C2 is often used by attackers to retain communications with compromised systems within a target network.

CARTA - Continuous Adaptive Risk and Trust Assessment

According to Gartner, a CARTA mindset allows enterprises to make decisions based on risk and trust. Decisions must continuously adapt, security responses must continuously adapt, and thus Risk and Trust must continuously adapt.

CASB - Cloud Access Security Broker

CASB describes technology platforms that help organizations better secure the use of cloud delivered applications (SaaS) and infrastructure. It helps encrypt or handle data to make it more secure in a cloud environment.

CCPA - California Consumer Privacy Act

The California Consumer Privacy Act (CCPA) is a law aimed at enhancing online privacy and consumer protection for California residents. Signed into law in 2018, CCPA is effective as of January 1, 2020. The CCPA seeks to assure Californians the right to know what personally identifiable information (PII) is being collected, to know whether the data is sold or disclosed and to whom, to control/prevent sale or disclosure of the PII and to request deletion of PII by a business.

CIA – Confidentiality, Integrity and Availability

Confidentiality assures information is accessible only by authorized parties; integrity makes sure information is reliable; and availability ensures data is readily accessible to the organization as it works to address its business requirements.

CIO - Chief Information Officer

The Chief Information Officer is a senior executive responsible for a company's Information Technology (IT) strategy and infrastructure, including security.

CIS - Center for Internet Security Critical Security Controls

CIS is a non-profit organization that develops Configuration Policy Benchmarks that allow businesses to improve security and compliance programs and postures.

CISO - Chief Information Security Officer

The Chief Information Security Officer (CISO) is a senior executive responsible for an organization's information and data security. In this evolving role CISOs develop and run enterprise-wide processes aimed at reducing IT and business risk as well as assuring regulatory compliance.

CISSP - Certified Information Systems Security Professional

CISSP is an information security certification for security analysts. It was created by an independent information security certification - International Information System Security Certification Consortium, known as ISC.

CSPM - Cloud Security Posture Management

Cloud Security Posture Management concentrates on security assessment and compliance monitoring for workloads in public cloud environments. It can be used to provide a unified view across disparate cloud environments.

Cloud-Delivered Security

Cloud-Delivered Security is security technologies designed to protect critical infrastructure, applications, and data delivered as-a-service from the cloud as opposed to being installed and maintained on-prem.

CMDB - Configuration Management Database

CMDB provides the ability to log devices that move in and out of an environment, which facilitates easier targeting and patching of any potential security vulnerabilities.

CoBiT - Control Objectives for Information and Related Technologies

CoBiT is an IT management framework first developed in 1996 published by the IT Governance Institute and the Information Systems Audit and Control Association (ISACA) to help businesses develop, organize and implement strategies around information management and governance.

Container

A container is a software unit that packages code so applications can run quickly across multiple environments. Containerization allows applications to be developed once and easily deployed across virtually any environment regardless of operating system, virtual machine or bare metal, on-prem data centers or public cloud.

COPPA - Children's Online Privacy Protection Act

COPPA requires that the operators of websites or online services directed to children under a certain age must provide notice on the site and obtain verifiable parental consent before collecting data.

COSO - Committee of Sponsoring Organizations of the Treadway Commission

COSO is dedicated to providing thought leadership through the development of frameworks and guidance on enterprise risk management, internal control and fraud deterrence.

Cryptocurrency

Cryptocurrency is a digital asset / virtual currency designed to work as a medium of exchange that uses strong cryptography to secure financial transactions, control the creation of additional units, and verify the transfer of assets.

Cryptomining / Cryptojacking

Cryptomining is a system by which “miners” contribute computer processing power and get paid in cryptocurrency to validate blockchain transactions. In its malicious form, Cryptojacking is where hackers take control of a victim’s computing resources to secretly mine cryptocurrency for their own benefit.

CSPM - Cloud Security Posture Management

Cloud Security Posture Management concentrates on security assessment and compliance monitoring for workloads in public cloud environments. It can be used to provide a unified view across disparate cloud environments.

CTI - Cyber Threat Intelligence

CTI is based on a collection of intelligence using Open Source Intelligence (OSINT), Social Media Intelligence (SCOMINT), Human Intelligence (HUMINT), technical intelligence or intelligence from the deep and dark web.

CVE - Common Vulnerabilities and Exposures

CVE is a program launched by MITRE, a nonprofit that operates federal government-sponsored research and development centers, to identify and catalog vulnerabilities in software or firmware into a free “dictionary” for organizations to use as a resource to improve their security.

CWPP - Cloud Workload Protection Platform

CWPP is a term developed by Gartner to describe an emerging category of technology solutions primarily used to secure server workloads in public cloud Infrastructure as a Service (IaaS) environments.

Cyber Insurance

Cyber insurance offers protection in the event an organization is victimized by a cyber attack.

Cybersecurity Ratings

Cybersecurity Ratings describe the strength of an organization's cybersecurity posture based on a calculated rating and/or score.

DAG - Data Access Governance

DAG is a data security technology that allows enterprises to gain visibility to sensitive unstructured data that exists across the organization and enforce policies to control access to that data.

Dark Web

The Dark Web is the part of the World Wide Web that is only accessible by means of special software, allowing users and website operators to remain somewhat more anonymous.

DAST - Dynamic Application Security Testing

DAST is a security solution used to uncover vulnerabilities in software during its running

Data Breach

A data breach occurs when sensitive, protected, private or confidential information is stolen, copied, viewed or conveyed to an unauthorized/ untrusted party or environment. Motivations for such attacks vary and include financial gain (personal or organizational), socio-political goals (hacktivism) and state-sponsored espionage.

Data Lake

Data Lakes are centralized repositories for storing large amounts of raw data, including system data and data for reporting and advanced analytics. They may contain structured, semi-structured and unstructured data as well as images, audio and video.

Data Protection

Data protection is the process of preserving valuable information against theft, loss or errors occurring in the storage and transmission process.

DDI - DNS, DHCP, IPAM

DDI solutions (Domain Name System/Service, Dynamic Host Configuration Protocol and IP address management) provide organizations with tools to efficiently manage IP address management (IPAM), as well as DNS and DHCP services management across the network. Many enterprises still manage IPAM manually, a process that's time-consuming, error-prone and difficult to update.

DDoS - Distributed Denial of Service

DDoS is a form of cyber-attack in which multiple compromised systems work together to disrupt an online service, server, or network by overwhelming the target with malicious traffic.

Deception Platforms

Deception Platforms are designed to lure in bad actors in order to collect intelligence about their tactics and intentions to improve other preventative security controls in real time.

DevOps – Development and Operations

DevOps is a software development methodology that combines software development with information technology operations.

DevSecOps – Development, Security and Operations

DevSecOps has emerged as an enterprise application development best practice that embraces the inherent agility benefits of DevOps, but recognizes that the security organization needs to be integrated as an early participant in the DevOps process.

DFIR – Digital Forensics and Incident Response

DFIR is a field within cybersecurity that focuses on the identification, investigation and remediation of cyberattacks.

DLP - Data Loss Prevention

DLP is a technology and business process designed to detect and prevent violations to corporate policies regarding the use, storage, and transmission of sensitive data.

Dwell Time

Dwell Time represents the length of time a cyber attacker has free reign in an environment from the time they get in until they are eradicated.

Edge Computing

Edge computing is an open IT architecture model which distributes computation and data storage toward the “edge” of the network. Data is processed by the device itself or by a local computer or server, rather than being transmitted to a centralized data-processing warehouse. Since the edge is where data is generated, the practice improves network response and saves bandwidth.

EDR - Endpoint Detection and Response

EDR solutions record key activity of endpoints and provide security analysts with necessary information to conduct both reactive and proactive threat investigations.

Encryption

Encryption is a method in which plaintext or other data is converted from readable form to an encoded version that can only be decrypted with a decryption key.

Endpoint Security

Endpoint security applies threat prevention, detection and response capabilities to the multitude of devices that interact with corporate networks. Endpoints can include computers, tablets, mobile devices, point-of-sale (POS) systems, and IoT devices.

FEDRamp - The Federal Risk and Authorization Management Program

In 2012, FEDRamp began providing guidance to US government and corporate organizations offering a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.

Fileless Attacks

Fileless Attacks inject malicious code into RAM memory and exploit approved applications on targeted devices to achieve their objectives and thwart detection.

Firewall

Firewalls are network security devices or systems that monitor and regulate network traffic (incoming and outgoing) based on defined security rules.

FISMA - Federal Information Security Management Act of 2002

FISMA provides a framework to ensure comprehensive measures are taken to secure US federal information and assets.

FDA - Forensic Data Analysis

Forensic Data Analysis, also known as Data Forensics, refers to the study of digital data and the investigation of cybercrime. FDA may focus on mobile devices, computers, servers and other storage devices, and it typically involves the tracking and analysis of data passing through a network.

FWaaS - Firewall as-a-Service

FWaaS is an emerging method to deliver select firewall functionality as a cloud service as opposed to the more traditional hardware-based firewall platforms.

GDPR - General Data Protection Regulation

GDPR sets strict rules regarding the collection and processing for Personally Identifiable Information for citizens of the EU.

GLBA - Gramm-Leach-Bliley

GBLA, more commonly known for its authors (Gramm-Leach-Bliley Act) includes provisions to protect consumers' personal financial information held by financial institutions.

Hacker

A hacker is someone who uses technical expertise to solve computing challenges. T he term may refer to any skilled programmer – including "ethical hackers" – but in common contemporary usage it typically signifies a cyber criminal.

Hardware Authentication

Hardware authentication is an approach to user authentication that relies on a dedicated physical device (such as a token) held by an authorized user, in addition to a basic password, to grant access to computer resources.

HIPAA - Health Insurance Portability and Accountability Act

The goal of HIPAA is to enable the movement of health information among health-related organizations in a protected manner.

HITRUST - The Health Information Trust Alliance

HITRUST is a United States non-profit that has established a Common Security Framework (CSF) (in collaboration with healthcare, technology and information security leaders) that can be used by any organization that creates, accesses, stores or exchanges sensitive and/or regulated data.

Honeypot

Honeypots are computers or computer systems that mimic potential cyberattack targets for the purpose of detecting intrusions and building threat intelligence by analyzing the tactics, techniques and procedures of the malicious actors.

IAM - Identity and Access Management

IAM is the processes, technology, and people used to create, manage, authenticate, control, and remove the permissions a user (internal, external, and customer) has to corporate technology resources.

IAST - Interactive Application Security Testing

IAST is an emerging application security testing approach which combines elements of both of its more established siblings in SAST (Static Application Security Testing) and DAST (Dynamic Application Security Testing).

IDS - Intrusion Detection Systems and IPS - Intrusion Prevention Systems

The key difference between IDS and IPS lies in "detection" vs. "prevention." Intrusion Detection Systems (IDS) monitor and scrutinize network traffic for known cyberattack signatures. Intrusion Prevention Systems (IPS), which reside between the internal network and external networks (like the Internet), reject incoming traffic when it indicates a recognized security threat profile.

IGA - Identity Governance and Admin

IGA is a component of an Identity Access Management (IAM) program that ensures only the right users are getting access to the right applications at the right time.

Incident Management

Cybersecurity incident management is the real-time process of identifying, managing, monitoring and analyzing computer and network security threats or incidents (which may include anything from attempted intrusions to successful compromises/data breaches) and responding appropriately.

Insider Threat

Insider Threat represents a threat to the systems and protected data of an organization that emanates from the people within the organization or trusted third parties.

IOC - Indicator of Compromise

IOCs are clues to compromise or pieces of forensic data, system log entries or files, that can be considered unusual and may identify potentially malicious activity on a system or network.

IoT - Internet of Things

IoT represents a rapidly growing class of non-traditional computing devices that are connected to the internet to drive some sort of intelligent operation.

IR - Incident Response

IR reflects actions a company takes to manage the aftermath of a security breach or cyberattack.

IRM - Integrated Risk Management

IRM is an approach to risk management that integrates risk activities from across an organization to enable better and more sustainable strategic decision making.

ISO 27000

ISO 27000 is an internationally-recognized standard of good practice for information security, ISO/IEC 27001 specifies an Information Security Management System (ISMS) a suite of activities concerning the management of information risks into an overarching management framework through which the organization identifies, analyzes and addresses its information risks.

ITSM – Information Technology Service Management

The activities that are performed by an organization to design, build, deliver, operate and control information technology (IT) services offered to customers.

KRI - Key Risk Indicator

Key risk indicator metrics articulate an organization's level of risk and allow security and business leaders to track how the risk profile is evolving. For instance, cybersecurity operations can use metrics that analyze the threats and vulnerabilities reported by various tools.

Lateral Movement

Lateral Movement describes a common cyberattack technique where intruders, having gained initial access to a network, move through the system "sideways" (or "east-west"), looking to escalate their privileges to access high-value targets.

Least Privilege

The principle of least privilege restricts users or processes from being granted access rights in excess of those specifically required for the performance of their defined tasks.

Malware

Malware (short for “malicious software”) describes any software developed for the purpose of infiltrating, damaging, disabling or seizing control of computers, computer systems, mobile devices and networks.

MDR - Managed Detection and Response

MDR is an outsourced service that leverages external experts to make the security benefits of tools such as EDR and proactive threat hunting accessible to customers of all maturity levels.

Medjacking

Medjacking – or medical device hijacking – refers to the hacking a critical medical device. Many devices currently in use – anything that’s linked to a wireless network – is potentially susceptible, and the hundreds of at-risk technologies include MRI systems and implantables like pacemakers and insulin pumps.

MFA - Multi-Factor Authentication

Similar to 2FA as it requires both knowledge (like a password) and something tangible (such as a hardware or software authentication system) to gain access to a protected computer system.

Microsegmentation

Microsegmentation is an emerging IT security best practice of implementing granular isolation (segmentation) policies between data center workloads.

MITRE ATT&CK - Adversarial Tactics, Techniques & Common Knowledge

MITRE's National Cybersecurity Federally Funded Research and Development Centers (FFRDC's) Adversarial Tactic, Techniques, and Common Knowledge (ATT&CK) repository of collected cybersecurity data.

ML - Machine Learning

Machine Learning is considered to be a subset of artificial intelligence (AI), and is currently the most common application of AI.

MSS - Managed Security Services

MSS are security service functions that have been outsourced to an external service provider (such as management of security tools, threat management, incident response, and forensics).

MSSP - Managed Security Service Provider

An MSSP is an IT service provider that performs any number of cybersecurity related activities for its clients on an outsourced basis.

MTTD - Mean Time to Detect

MTTD is the average length of time it takes a cybersecurity team to discover incidents in their environment.

MTTR - Mean Time to Respond/Remediate

MTTR is the amount of time it takes an organization to neutralize an identified threat or failure within their network environment.

NAC - Network Access Control

NAC is a security technology that provides visibility and control of devices accessing a corporate network.

Network Security

Network security comprises the technologies, policies and practices dedicated to monitoring, preventing and responding to illegal, malicious and unauthorized attempts to penetrate and compromise computer networks.

NIST CSF - National Institute of Standards and Technology Cybersecurity Framework

NIST CSF is a non-regulatory agency and a physical sciences laboratory of the United States Department of Commerce. The organization states its 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.”

NTA - Network Traffic Analysis and NBA - Network Behavior Analysis

NTA and NBA are fairly similar terms that describe technologies that use advanced analytics, machine learning, and rule-based techniques to detect suspicious activity on enterprise networks.

NYDFS Cybersecurity Regulation - New York Department of Financial Services

The NYDFS Cybersecurity Regulation (23 NYCRR 500) comprises a new set of New York Department of Financial Services rules imposing strict digital security requirements on financial institutions, such as banks, mortgage companies and insurance firms. Additionally, NYCRR applies to unregulated third parties working with regulated companies. Under NYCRR affected organizations must implement a detailed cybersecurity plan, articulate wide-ranging policies and establish/operate a cybersecurity incident reporting system.

OT/ICS/SCADA - Operational Technology, Industrial Control Systems and Supervisory Control and Data Acquisition Systems

OT represents systems that are used to monitor and manage the manufacturing equipment or industrial process assets of an organization.

OWASP - Open Web Application Security Project

OWASP is an open-source community project turned non-profit organization that provides unbiased and practical, cost-effective information about computer and Internet applications.

PAM - Privileged Access Management

PAM polices privileged accounts (how administrators login to critical IT resources they must manage). Since access rights associated with admin privileges are high level, they are often the target of cyber attacks and must be uniquely secured.

Patch Management

The patch management process keeps computer systems and applications up to date by routinely obtaining, testing, and deploying appropriate code changes (patches) to address vulnerabilities. A good patch management process also coordinates workflow between IT and Security teams and tracks deployment status.

Patching

Patching is a modification to software, or the underlying computer system, designed to fix a security vulnerability or a performance issue (bug), or add new features.

PCI and PCI DSS -The Payment Card Industry Data Security Standard

PCI compliance, usually refers to the PCI Data Security Standard (DSS) which is an information security standard for organizations that handle branded credit cards from the major card companies.

Penetration Testing

Penetration Testing, sometimes called ethical hacking or shortened to pen test, is an authorized attack performed to evaluate a system or application in order to find exploitable vulnerabilities so they can be proactively remediated.

PFI - PCI Forensic Investigator

PCI Forensic Investigators (PFIs) help uncover cardholder data compromise and when and how it may have occurred.

Phishing

Phishing is a fraudulent attempt to trick individuals into divulging sensitive information (usernames, passwords and banking details) by pretending to be a trusted source, often through an email communication.

PII - Personally Identifiable Information

PII represents information about a person that can identify them such as date of birth, social security number, credit card numbers and street address.

PIPEDA - Personal Information Protection and Electronic Documents Act

IRM is an approach to risk management that integrates risk activities from across an organization to enable better and more sustainable strategic decision making.

PKI - Public Key Infrastructure

PKI consists of a set of roles, hardware, software, policies, processes, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates and manage public-key encryption.

QSA - Qualified Security Assessor for PCI

QSA is a PCI Security Standards Council designation applied to individuals who meet specific information security education requirements, have taken the appropriate training from the PCI Security Standards Council, are employees of a Qualified Security Assessor (QSA) company approved PCI security and auditing firm, and will be performing PCI compliance assessments as they relate to the protection of credit card data.

Ransomware

Ransomware is a type of malicious software, or malware, that is designed to deny access to, or "lock," a computer system until a sum of money (ransom) is paid.

RASP - Runtime Application Self-Protection

RASP is a term popularized by Gartner to describe an emerging application security technology.

Red Team

Red Team is an independent group that challenges an organization to improve its security effectiveness by assuming an adversarial role or point of view.

ROC - Report on Compliance for PCI

The ROC form must be completed by all Level 1 Visa merchants undergoing a PCI DSS (Payment Card Industry Data Security Standard) audit.

SAML - Security Assertion Markup Language

Security Assertion Markup Language is an open-standard that makes possible the exchange of authentication and authorization data between parties (such as between service and identity providers).

SASE - Secure Access Service Edge

SASE (pronounced sassy) is a new term coined by Gartner to describe the convergence of the WAN edge and network security.

SAST - Static Application Security Testing

SAST is a security solution used to uncover vulnerabilities in software during its static (not-running) state by analyzing such things as its source code, byte code or binary code.

SD-WAN - Software-Defined WAN

SD-WAN has found application within enterprises that have a significant branch office footprint to simplify the deployment and management of network services across its many locations.

SDLC - Software Development Lifecycle

SDLC is a framework used to detail commonly accepted discrete phases -- and associated requirements -- that comprise the full software development process.

SDN - Software Defined Networking

SDN is an approach to computer networking in the LAN or data center of an enterprise that uses software to abstract the underlying network elements and to logically centralize network intelligence and control.

SDP/ZTNA - Software Defined Perimeter/ Zero Trust Network Access

A Software Defined Perimeter is a scalable, cloud-native security framework designed to narrowly segment access to networks and systems by establishing one-to-one connections between users and required resources. SDPs are built on user identities, not IP addresses, and employ Zero Trust principles to limit network access and reduce the attack surface.

Security Orchestration

This is a method of integrating and streamlining workflows across disparate tools to improve both security analyst efficiency and threat detection and response.

Serverless

Serverless is an emerging cloud computing paradigm in which the provider runs the server and manages allocation of machine resources.

Shadow IT

Shadow IT, also called Stealth IT or Client IT, is hardware or software used within organizations without explicit organizational approval.

Shift Left

In the world of software application development, “shift-left” is a concept that promotes the value of integrating security into the software development lifecycle as early as possible.

SIEM - Security Information and Event Management

SIEM is a software tool that allows security operations teams to identify potential incidents by consolidating and correlating log data from many other tools in the environment.

SOAR - Security Orchestration, Automation and Response

SOAR is a term developed by Gartner to describe technology platforms that aggregate security intelligence and context from disparate systems, and apply machine intelligence to streamline (or even completely automate) the incident detection and response process.

SOC - Security Operation Center

A SOC is a formalized function in a company that is staffed with domain experts (either in-house or outsourced) and focuses on preventing, detecting, analyzing, and responding to cybersecurity incidents.

SOC 2

Developed by the American Institute of Certified Public Accountants (AICPA), SOC 2 requires establishment and adherence to policies and procedures surrounding the security, availability, processing, integrity and confidentiality of customer data. More specifically, SOC 2 ensures that cybersecurity measures reflect up-to-date cloud requirements.

Social Engineering

Within the cybersecurity context, social engineering describes an attempt to manipulate people into divulging confidential information or performing actions inimical to the interests of them or their organizations.

Software Composition Analysis

Software Composition Analysis (SCA) tools help reduce vulnerabilities created by software development teams utilizing open source software (OSS) elements.

SOX - Sarbanes Oxley

SOX is a federal law that established sweeping auditing and financial regulations for public companies.

Spyware

A type of malware that functions by spying on user activity without their knowledge. The capabilities include activity monitoring, collecting keystrokes, data harvesting (account information, logins, financial data), and more.

SQLi - SQL Injection

SQLi is a type of application exploit called a code injection technique, in which an attacker adds malicious Structured Query Language (SQL) code to a web form input box to get access to resources.

SSL/TLS - Secure Sockets Layer/ Transport Layer Security

Secure Sockets Layer (SSL), the most widely used cryptography protocol in Internet history, was designed to provide communications security over a computer network.

SSO - Single Sign On

SSO is a user access and session authentication service that allows users to use a single set of login credentials (e.g., name and password) to access multiple applications.

SWIFT - Society for Worldwide Interbank Financial Telecommunication

SWIFT is a global member-owned cooperative and the world's leading provider of secure financial messaging services, it enables secure, seamless and automated financial communication between users.

Threat Hunting

Threat Hunting is the process of proactively and continuously searching networks to detect and isolate advanced threats that have evaded existing security solutions.

Tokenization

Tokenization is a process that secures important data by replacing it with unique identifiers containing essential information (but in a form that doesn't threaten its security).

TPRM - Third Party Risk Management

TPRM is the process of analyzing and controlling risks presented to an organization, its data, operations and finances by parties OTHER than the organization itself.

Trojan Horse

A piece of malware that often allows a hacker to gain remote access to a computer through a "back door".

TTPs - Tactics, Techniques, and Procedures

TTPs define how hackers orchestrate and manage attacks.

UEBA - User and Entity Behavior Analytics and UBA- User Behavior Analytics

These are systems that apply advanced analytics including machine learning to establish a baseline for the behavior of various users and/or entities (in this case, technology elements such as servers, applications, network traffic, databases, etc.) interacting with a corporate network.

URL – Uniform or Universal Resource Locator

A URL is the address of a resource on the Internet and the protocol used to access it. It indicates the location of a web resource, like a street address indicates where a person lives. It is often referred to as a "web address".

Vulnerability Management

Vulnerability management refers to the process of discovering, classifying, prioritizing, remediating, reporting and responding to software and network security vulnerabilities.

Watering Hole Attack

Watering hole attacks happen when an attacker targets a specific group of users by infecting websites they frequent with malware.

Worm

A piece of malware that can replicate itself in-order-to spread the infection to other connected computers.

XDR – Extended Detection and Response

XDR is a platform that provides comprehensive protection from a wide range of threats to your endpoints, network, users, and cloud workloads through continuous and automated monitoring, analysis, detection, and remediation.

XSS - Cross Site Scripting

XSS is a computer security vulnerability normally found in web applications that allows attackers to inject client-side scripts into benign and trusted websites.

Zero Day

Zero Day refers to a vulnerability in a system or software that was not previously known until after it was successfully hacked (either by a nefarious or ethical hacker).

Zero Trust

Zero Trust is an information security model based on the principle of maintaining strict access controls by not trusting anyone or any action by default, even those already inside the network perimeter. Each transaction is evaluated for need and risk.

Trustwave®

Government Solutions

www.trustwavegovt.com