Security, Compliance, and Operational Resilience

Glossary of Terms

vmware by Broadcom

Table of Contents

Access Control

The process of granting or denying users' access to specific resources based on their identity and permissions. It ensures that only authorized individuals can access sensitive data or perform certain actions within a system.

VMware Cloud Foundation and VMware vSphere implement a robust role-based access control permission model inside VMware vCenter Server, which permits administrators granular control over user permissions and capabilities.

Advanced Persistent Threat (APT)

A sophisticated, targeted, and prolonged cyberattack in which an intruder gains access to a network and remains undetected for an extended period. APTs are typically carried out by well-funded and organized groups, often with nation-state backing, and aim to steal sensitive data or disrupt critical systems. These attacks are known for their stealth, persistence, and adaptability.

Air Gap

A security measure that involves physically isolating a computer or network from unsecured networks, such as the public internet. This isolation helps prevent unauthorized access and potential threats from affecting the protected system or data.

VMware Cloud Foundation and VMware vSphere support air gapped environments through the limited use of online services and the availability of downloadable offline repositories for patching and updates.

Attacker

An individual or group that attempts to exploit vulnerabilities in systems, networks, or applications to gain unauthorized access, disrupt operations, or steal data. Attackers can be motivated by various factors, such as financial gain, political ideology, or personal reasons.

Authentication

The ability to prove that a person or application is genuine by verifying the identity of that person or application. Authentication often involves providing credentials, such as a username and password, to confirm that the user or application is who they claim to be. Also see “Multifactor Authentication.”

VMware Cloud Foundation and VMware vSphere components support several different ways to authenticate, using built-in username and password functionality, on-premises identity providers such as Microsoft Active Directory and Active Directory Federation Services, as well as cloud-based providers such as Okta, Microsoft Entra ID, and Ping.

Authorization

The act of determining whether a user or application has the right to conduct particular activities in a system, relying on authentication to prove the identification of the user or application. Authorization ensures that authenticated users or applications can only perform actions they are permitted to do.

VMware Cloud Foundation and VMware vSphere components support authorization of administrators and users through integrated role-based access control capabilities, as well as through connectivity to external sources such as Microsoft Active Directory and Active Directory Federation Services, Okta, Microsoft Entra ID, and Ping.

Availability

The assurance that a system or resource is accessible and functional when needed. Availability is one of the three core tenets of information security, alongside confidentiality and integrity.

VMware Cloud Foundation and VMware vSphere have numerous availability features to ensure workloads and data remain available, including vMotion and Cross-vCenter vMotion, Distributed Resource Scheduler, vSphere High Availability, Reliable Memory, network and storage I/O control, customizable vSAN storage policies, vSAN stretched clusters, proactive health checks, and more.

Backup

The process of creating copies of data to enable recovery in case of data loss or corruption. A proper backup strategy helps organizations restore data and maintain business continuity in the event of a disaster, cyberattack, or system failure. It should include regular, scheduled data copies to separate storage media or systems, version control to maintain multiple historical copies, and a retention policy to ensure that backups are kept for a sufficient period to meet recovery requirements. Additionally, backups should be tested regularly to verify their integrity and the ability to restore data successfully.

It's important to note that storing data on the same device or system as the original data does not qualify as a backup, as it does not protect against hardware failure, theft, or other localized risks. Similarly, using sync services or mirroring alone does not constitute a backup, as changes made to the original data, including deletions or corruptions, are immediately reflected in the synced or mirrored location. Proper backups should be independent of the original data location and protected against common risks.

VMware Cloud Foundation and VMware vSphere provide standard APIs and access methods to a large ecosystem of partners specializing in backup and restore software and solutions.

Business Continuity

The capability of an organization to maintain essential functions during and after a disruption, such as a natural disaster, cyberattack, or equipment failure. Business continuity planning involves identifying critical processes, developing strategies to minimize disruptions, and ensuring the organization can recover quickly.

VMware Cloud Foundation enables customers to proactively protect their environments and quickly recover from incidents and disasters through VMware Live Recovery, which includes integrated ransomware recovery as well as runbook-based recovery methods for failover and subsequent failback of entire enterprise data centers.

CIA Triad

An abbreviation for the core tenets of information security: confidentiality, integrity, and availability. Confidentiality ensures that data is protected from unauthorized access, integrity maintains the accuracy and consistency of data, and availability ensures that data and systems are accessible when needed.

Every feature in VMware Cloud Foundation and VMware vSphere fits into one or more of these three categories, making every feature a security feature.

Clone

An exact copy of a system, including its data, applications, and configuration settings. Cloning is often used for testing and deployment purposes, as it allows for the creation of identical systems or environments.

VMware Cloud Foundation and VMware vSphere allow cloning of virtual machines, both while running and while powered off. The clones are identical except for the unique identifiers each VM has, and the MAC addresses on the virtual network interfaces.

Cyber Resilience

An organization's ability to prepare for, respond to, and recover from cyber incidents, minimizing the impact on business operations, reputation, and financial stability. Cyber resilience involves a combination of technical controls, incident response planning, and business continuity and disaster recovery strategies.

Cybersecurity Maturity Model Certification (CMMC)

A unified standard for implementing cybersecurity across the Defense Industrial Base (DIB), which includes over 300,000 companies in the supply chain. CMMC is designed to protect controlled unclassified information (CUI) and federal contract information (FCI) within the DIB.

Compensating Control

Security and privacy controls implemented as an alternate solution to a requirement that is not workable for an organization to implement in its original form. The sum of the compensating controls must meet the intent and requirements of the original security control. Compensating controls provide flexibility in achieving security objectives when the prescribed controls are not feasible.

Confidentiality

Ensuring that data is protected from access by unauthorized parties. Confidentiality is one of the three core tenets of information security, alongside integrity and availability.

Cybersecurity

The practice of protecting systems, networks, and data from digital attacks, unauthorized access, and damage. Cybersecurity involves implementing various security measures, such as firewalls, encryption, and access controls, to prevent, detect, and respond to cyber threats.

Data Breach

An incident where data is accessed, copied, transmitted, viewed, or stolen by an unauthorized party. A data breach can occur due to various reasons, such as weak security controls, human error, or malicious attacks. The term does not necessarily indicate the intent behind the incident; other terms such as “data leak” and “information leakage” help convey whether a data breach was intentional or not.

Data Encryption

The process of converting data into a code to prevent unauthorized access. Encryption uses mathematical algorithms to transform readable data into an unreadable format, ensuring that only authorized parties with the decryption key can access the original data.

Data Exfiltration

The unauthorized transfer of data from a computer or network to another location, often for the purpose of theft or espionage. Exfiltration can occur through various methods, such as email, file transfer, or the use of malware. Detecting and preventing data exfiltration is a critical aspect of data security.

Data Leak

The unintentional exposure of sensitive information to an unauthorized party, often due to misconfiguration, human error, or security vulnerabilities. Data leaks can occur through various channels, such as unsecured databases, cloud storage, or emails sent to the wrong recipient.

Data Loss Protection (DLP)

Strategies and techniques used to ensure that sensitive data is not lost, misused, or accessed by unauthorized users. DLP solutions can identify, monitor, and protect sensitive data throughout its lifecycle, whether it's in use, in transit, or at rest.

Data-at-Rest Protections

Security measures applied to data stored on a device or system, such as encryption, access controls, and data backup. These protections help ensure the confidentiality and integrity of data when it is not being actively processed or transmitted.

Data-in-Transit Protections

Security measures applied to data as it travels between systems or devices, such as encryption and secure communication protocols. These protections help ensure the confidentiality and integrity of data while it is being transmitted over networks, preventing unauthorized interception or tampering.

Data-in-Use Protections

Security measures applied to data being processed or used by a system or application, such as memory encryption and access controls. These protections help ensure the confidentiality and integrity of data while it is being actively processed or accessed by authorized users or applications.

Defense-in-Depth

The application of multiple security controls in a layered manner to protect systems and data. Defense-in-depth assumes that no single security measure is perfect, and that by layering different controls, the overall security posture is strengthened. If one control fails, the other controls can still provide protection.

Digital Certificates

Electronic documents that use digital signatures to bind a public key with an identity, verifying that a particular public key belongs to a specific individual or entity. Digital certificates are used to establish secure connections, authenticate users and devices, and ensure the integrity of transmitted data.

Disaster Recovery

The process of restoring normal operations after a disruptive event, such as a natural disaster or cyberattack. Disaster recovery planning involves identifying critical systems and data, developing backup and restoration procedures, and testing the plan regularly to ensure its effectiveness.

Domain Name Service (DNS)

A system that translates human-readable domain names (e.g., www.example.com) into IP addresses, allowing devices to locate and communicate with each other on the internet. DNS acts as a phonebook for the internet, mapping domain names to their corresponding IP addresses.

Domain Name Service Security (DNSSEC)

A set of extensions to DNS that provide authentication of DNS data, ensuring that the data has not been tampered with and originates from the correct source. DNSSEC uses digital signatures to verify the authenticity and integrity of DNS responses, helping to prevent DNS spoofing and cache poisoning attacks.

Endpoint Detection and Response (EDR)

A security solution that monitors endpoint devices, such as computers and servers, to detect and respond to threats like malware and unauthorized access attempts. EDR solutions collect and analyze data from endpoints to identify suspicious activities and can take automated actions to contain and mitigate threats.

Firewall

A security system that monitors and controls network traffic based on predetermined security rules. Firewalls can be hardware devices or software applications, and they act as a barrier between trusted internal networks and untrusted external networks, such as the internet.

General Data Protection Regulation (GDPR)

A regulation in EU law on data protection and privacy for individuals within the European Union and the European Economic Area. GDPR sets strict requirements for how personal data must be collected, processed, and protected, and gives individuals more control over their personal data.

Health Insurance Portability and Accountability Act (HIPAA)

A U.S. federal law that establishes national standards for the protection of sensitive patient health information. HIPAA applies to covered entities (health plans, healthcare clearinghouses, and healthcare providers) and their business associates, requiring them to implement administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and availability of protected health information (PHI).

Identity Provider (IdP)

A system that creates, maintains, and manages identity information for users and provides authentication services to applications.

Identification

The process of uniquely recognizing and distinguishing an individual user of a system or application. Identification allows a system to associate specific access rights, permissions, and accountability to a user.

Immutable

Data or objects that cannot be modified after creation, ensuring data integrity and preventing tampering. Immutable storage is often used for critical data, such as audit logs or legal records, where any changes must be appended rather than overwriting the original data.

Incident

An event that results in the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations. Incidents can be caused by various factors, such as human error, natural phenomena, or malicious attacks.

Incident Response Plan

A documented plan that outlines the steps an organization will take to respond to a security incident. The plan typically includes procedures for detecting, analyzing, containing, and recovering from incidents, as well as roles and responsibilities for the incident response team.

Indicator of Compromise (IoC)

A piece of forensic evidence, such as data found in system log entries or files, that identifies potentially malicious activity on a system or network. IoCs help security teams detect, respond to, and prevent cyberattacks by providing a way to identify and track malicious actors and their methods.

Initial Access

The first stage of a cyberattack, in which an attacker gains access to a target system or network. Initial access can be achieved through various methods, such as exploiting vulnerabilities, stealing credentials, or using social engineering techniques. Once initial access is obtained, an attacker can move laterally within the network, escalate privileges, and execute their malicious objectives.

Information Assurance

The practice of protecting the confidentiality, integrity, and availability of information and information systems. Information assurance involves implementing various security controls and processes to manage risks and ensure the reliability and trustworthiness of information.

Information Security Management System (ISMS)

A framework of policies and procedures for systematically managing an organization's sensitive data and ensuring information security. An ISMS helps organizations identify, assess, and mitigate information security risks, and provides a structured approach to implementing and maintaining security controls.

Insider Threat

A security risk originating from within an organization, typically an employee, contractor, or business partner with authorized access to systems, data, or premises. Insider threats can be malicious (intentional) or unintentional and are often difficult to detect and prevent due to the individual's legitimate access and knowledge of security measures.

Integrity

The assurance that data has not been altered in an unauthorized manner. Integrity is one of the three core tenets of information security, alongside confidentiality and availability.

Intrusion Detection System (IDS)

A device or software that monitors a network for malicious activity or policy violations. An IDS analyzes network traffic and system logs to identify potential security breaches, and alerts administrators when suspicious activity is detected.

Intrusion Prevention System (IPS)

A device or software that monitors network traffic for malicious activity and takes action to prevent it. An IPS is similar to an IDS but can also automatically block or prevent detected threats in real-time.

IP Address Management (IPAM)

A method of planning, tracking, and managing the assignment of IP addresses within a network. IPAM helps ensure the efficient allocation of IP addresses, avoids conflicts, and maintains an accurate inventory of IP address assignments.

ISO/IEC 27001

An international standard that provides a framework for establishing, implementing, maintaining, and continually improving an information security management system (ISMS). ISO/IEC 27001 specifies requirements for assessing and managing information security risks, and helps organizations demonstrate their commitment to information security best practices.

Lateral Movement

A technique used by attackers, after gaining initial access to a system, to move laterally across a network and gain access to additional systems and resources. Lateral movement allows attackers to expand their foothold, escalate privileges, and locate and exfiltrate sensitive data.

Least Privilege

The principle of granting users only the minimum access rights necessary to perform their authorized tasks. Least privilege helps minimize the potential impact of a security breach by limiting the actions an attacker can take if they compromise a user account.

Malware

Software designed to damage, disrupt, or gain unauthorized access to a computer system. Malware can take many forms, such as viruses, worms, Trojans, ransomware, and spyware, and can be spread through various methods, such as email attachments, downloaded files, or infected websites.

Microsegmentation

A security technique that divides a network into smaller, isolated segments to control traffic between them and limit the impact of a security breach. Microsegmentation allows organizations to apply granular security policies to specific workloads or applications, reducing the attack surface and making it more difficult for attackers to move laterally within the network.

Multifactor Authentication

A security mechanism that requires users to provide two or more forms of identification to access a system or resource. Multi-factor authentication combines factors such as something the user knows (a password or PIN), something the user has (a security token, authenticator application, or smart card), and something the user is (a fingerprint or retina scan). This approach provides an additional layer of security beyond traditional username and password authentication.

National Institute of Standards and Technology (NIST) Cybersecurity Framework

A voluntary framework developed by NIST that provides a set of industry standards and best practices to help organizations manage cybersecurity risks. The framework is designed to be flexible and adaptable to various types of organizations, regardless of size, industry, or cybersecurity sophistication.

NIST 800-53 (Security and Privacy Controls for Federal Information Systems and Organizations)

A comprehensive set of security controls and guidelines developed by NIST for federal information systems and organizations. NIST 800-53 provides a flexible framework for selecting and implementing security controls based on an organization's risk assessment and the criticality of its systems and data.

NIST 800-171 (Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations)

A set of security requirements for protecting controlled unclassified information (CUI) when it is processed, stored, or transmitted by nonfederal systems and organizations. NIST 800-171 is designed to ensure the confidentiality, integrity, and availability of CUI in nonfederal systems, and is a requirement for many federal contracts and grants.

North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP)

A set of standards and requirements designed to secure the assets required for operating North America's bulk electric system. NERC CIP applies to all entities responsible for the reliability and security of the bulk electric system, including generators, transmission owners, and distribution providers.

Non-Repudiation

The assurance that an individual cannot deny having performed a particular action or transaction. Non-repudiation is achieved through the use of authentication mechanisms, digital signatures, and audit trails that provide proof of the origin, integrity, and receipt of data or actions.

OAuth

An open standard for access delegation, commonly used as a way for users to grant websites or applications access to their information on other websites without giving them the passwords. OAuth provides a secure way for applications to access user data without compromising the user's credentials.

Patch Management

The process of identifying, acquiring, installing, and verifying patches for software and systems. Patches are software updates that address security vulnerabilities, fix bugs, or improve performance. Effective patch management helps organizations maintain the security and stability of their systems by ensuring that known vulnerabilities are promptly addressed.

Payment Card Industry Data Security Standard (PCI DSS)

A set of security standards designed to ensure that all companies that accept, process, store, or transmit credit card information maintain a secure environment. PCI DSS applies to any organization that handles cardholder data, regardless of size or number of transactions, and requires them to implement a range of security controls to protect cardholder data

Penetration Testing

The practice of simulating attacks on a computer system, network, or web application to identify vulnerabilities that an attacker could exploit. Penetration testing helps organizations assess the effectiveness of their security controls and identify weaknesses that need to be addressed.

Phishing

A type of social engineering attack where the attacker attempts to trick the victim into revealing sensitive information or installing malware by sending fraudulent emails, messages, or websites that appear to be from legitimate sources. Phishing attacks often rely on psychological manipulation to create a sense of urgency or trust, leading victims to click on malicious links or provide confidential data.

Privacy

The right of an individual to control how their personal information is collected, used, and shared. Privacy involves implementing appropriate safeguards to protect personal data from unauthorized access, use, or disclosure, and respecting individuals' rights to access, correct, and delete their personal information.

Public Key Cryptography

A cryptographic system that uses a pair of keys, a public key and a private key, for secure communication and data protection. The public key is widely distributed and can be used by anyone to encrypt messages or verify digital signatures, while the private key is kept secret by the owner and is used to decrypt messages or create digital signatures. This asymmetric key system allows for secure communication without the need to share a secret key, as is the case in symmetric key cryptography. Public key cryptography is the foundation for security applications such as secure email, digital certificates, and key exchange protocols like Transport Layer Security (TLS).

Public Key Infrastructure (PKI)

A set of roles, policies, hardware, software, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates and manage public-key encryption. PKI is the foundation for secure communication and authentication in many network environments.

Ransomware

A type of malware that encrypts a victim's files and demands a ransom payment in exchange for the decryption key. Ransomware attacks can cause significant disruption to organizations by rendering critical data and systems inaccessible until the ransom is paid or the data is restored from backups.

Recovery Point Objective (RPO)

The maximum amount of data that an organization is willing to lose in the event of a disruption or disaster. RPO is typically expressed as a time period, such as one hour or one day, and determines how frequently data backups need to be taken to ensure that the maximum data loss threshold is not exceeded.

Recovery Time Objective (RTO)

The maximum amount of time that an organization can tolerate for a system or application to be unavailable after a disruption or disaster. RTO is typically expressed as a time period, such as four hours or one day, and determines how quickly systems need to be restored to minimize the impact on business operations.

Red Team/Blue Team

Red teams are offensive security professionals who are experts in attacking systems and breaking into defenses. Blue teams are the defenders who counter the red team's efforts and strengthen the organization's defenses.

Regulatory Compliance

The process of ensuring that an organization adheres to relevant laws, regulations, guidelines, and specifications relevant to its business processes. Regulatory compliance varies by industry and jurisdiction, and may include requirements related to data protection, privacy, financial reporting, environmental standards, and workplace safety, among others.

Replication

The process of creating and maintaining an exact copy of data or a system in real-time or near-real-time, often for disaster recovery or high availability purposes. Replication ensures that critical data and systems are continuously available, even in the event of a primary system failure or disruption.

Responsible Disclosure (Coordinated Disclosure)

A vulnerability disclosure model in which a security researcher or individual who discovers a vulnerability in a system or software reports it to the owner or vendor, allowing them time to investigate and remediate the issue before disclosing it to the public. Responsible disclosure aims to minimize the risk of the vulnerability being exploited by malicious actors while ensuring that the public is informed of the issue and its resolution.

Risk Assessment

The process of identifying, analyzing, and evaluating potential risks to an organization's assets, operations, and objectives. Risk assessment involves determining the likelihood and impact of various risk scenarios, and prioritizing risks based on their potential consequences and the organization's risk appetite.

Risk Management

The process of identifying, assessing, and prioritizing risks, and implementing strategies to mitigate, transfer, or accept those risks. Risk management helps organizations make informed decisions about allocating resources and implementing controls to minimize the impact of potential threats and vulnerabilities.

Role-Based Access Control (RBAC)

A method of restricting system access to authorized users based on their assigned roles within an organization. In RBAC, permissions are associated with roles, and users are assigned to these roles based on their responsibilities and qualifications. This approach simplifies access management by allowing administrators to assign permissions to roles rather than individual users, ensuring that users only have access to the resources they need to perform their job functions. RBAC helps maintain the principle of least privilege, reduces the risk of unauthorized access, and makes it easier to audit and manage user permissions across an organization.

Secure Boot

A security standard that ensures a device boots using only software trusted by the device manufacturer, protecting against malware and unauthorized modifications to the boot process. Secure Boot verifies the digital signatures of boot loaders and operating system components, preventing the execution of untrusted code during the boot process.

Secure Software Development Lifecycle (SSDLC)

A process that integrates security practices into the software development lifecycle, ensuring that security is considered and addressed at every stage of development, from design to deployment and maintenance.

Security Assertion Markup Language (SAML)

An open standard for exchanging authentication and authorization data between parties, particularly between an identity provider and a service provider. SAML enables Single Sign-On (SSO) by allowing users to authenticate with one system and access multiple applications without re-entering their credentials.

Security Audit

A systematic evaluation of an organization's information system's security to assess compliance with established policies, procedures, and industry standards. Security audits help identify weaknesses in security controls, prioritize remediation efforts, and provide evidence of due diligence to stakeholders and regulators.

Security Awareness Training

The process of educating employees about security policies, procedures, and best practices to reduce the risk of security incidents caused by human error or negligence. Security awareness training helps create a culture of security within an organization and empowers employees to recognize and respond appropriately to potential security threats.

Security Control

A safeguard or countermeasure designed to protect the confidentiality, integrity, and availability of data and systems. Security controls can be technical (e.g., firewalls, encryption), administrative (e.g., policies, procedures), or physical (e.g., access controls, surveillance).

Security Information and Event Management (SIEM)

A system that aggregates and analyzes log data from various sources across an organization's network to detect and respond to security incidents. SIEM solutions provide real-time monitoring, alerting, and reporting capabilities, helping security teams identify and investigate potential threats more efficiently.

Security Operations Center (SOC)

A centralized unit within an organization that is responsible for continuously monitoring, detecting, analyzing, and responding to cybersecurity incidents. The SOC team uses a combination of technology solutions and processes to prevent, detect, and respond to threats in real-time.

Security Policy

A document that defines an organization's approach to managing information security risks and protecting its assets. A security policy outlines the rules, procedures, and guidelines that employees, contractors, and third parties must follow to ensure the confidentiality, integrity, and availability of the organization's data and systems.

Segmentation

The practice of dividing a computer network into smaller, isolated segments or subnetworks to improve security, performance, and control. Segmentation helps contain the impact of security breaches, reduces the attack surface, and allows organizations to apply different security policies to different network segments based on their sensitivity and criticality.

Separation of Duties

The principle of dividing critical functions and responsibilities among multiple individuals to prevent any single person from having excessive control or the ability to commit fraud or errors without detection. Separation of duties helps maintain checks and balances, ensuring that no individual can compromise the integrity of a process or system.

Service Organization Control 2 (SOC 2)

A voluntary compliance standard developed by the American Institute of CPAs (AICPA) for service organizations, focusing on trust services criteria relevant to security, availability, processing integrity, confidentiality, and privacy. SOC 2 reports provide assurance to customers and stakeholders that a service organization has appropriate controls in place to protect sensitive data and ensure the reliability of its systems.

Single Sign-On

A session and user authentication service that allows a user to access multiple applications with one set of login credentials. Single Sign-On simplifies the user experience and reduces the risk of password fatigue by eliminating the need for users to remember and manage multiple sets of credentials for different applications.

Snapshot

A point-in-time copy of a system or data, snapshots provide a quick and space-efficient way to capture the state of a system or dataset at a particular moment, allowing for easy rollback or restoration if needed.

VMware Cloud Foundation and VMware vSphere support snapshots of virtual machines, which capture the entire state of the virtual machine, including virtual hardware configuration and virtual disks.

Social Engineering

The use of psychological manipulation to trick individuals into revealing sensitive information or taking actions that compromise security. Social engineering attacks exploit human vulnerabilities, such as trust, fear, or curiosity, to bypass technical security controls and gain unauthorized access to systems or data.

Software Bill of Materials (SBOM)

A formal record containing the details and supply chain relationships of the various components used in building a software product. An SBOM helps organizations understand the composition of their software, including any open source or third-party components, which can be useful for managing security risks, complying with regulations, and responding to vulnerabilities.

Supply Chain

The sequence of processes involved in the production and distribution of a commodity or service, from the procurement of raw materials to the delivery of the final product to the end user. In the context of cybersecurity, supply chain risk management involves identifying, assessing, and mitigating risks associated with the hardware, software, and services used by an organization, as well as the third-party vendors and suppliers involved in the supply chain.

System Hardening

The process of securing a system by reducing its attack surface and minimizing its vulnerabilities. System hardening involves configuring the system securely, removing unnecessary software and services, applying security patches, and implementing access controls and other security measures to make the system more resistant to attacks.

Tactics, Techniques, and Procedures (TTPs)

The patterns of activities, methods, and tools used by threat actors to carry out attacks and achieve their objectives. TTPs provide a framework for understanding and describing the behavior of threat actors, and can be used to develop targeted defense strategies and detect potential threats.

Threat

A potential cause of harm to a system, network, or organization, which may result in unauthorized access, damage, or disruption. Threats can be external (e.g., hackers, malware) or internal (e.g., malicious insiders, human error), and can exploit vulnerabilities in technology, processes, or people.

Threat Actor

An individual or group that is responsible for a threat event, either through malicious intent or accidental actions. Threat actors can include cybercriminals, nation-state hackers, hacktivists, insiders, or even unwitting employees who may cause security incidents through negligence or error.

Threat Intelligence

Information about current and emerging threats that can be used to inform an organization's security decisions and actions. Threat intelligence includes data on threat actors, their tactics, techniques, and procedures (TTPs), and indicators of compromise (IoCs) that can help organizations detect, prevent, and respond to potential security incidents.

Transport Layer Security (TLS)

A cryptographic protocol that provides secure communication over a computer network. TLS encrypts data transmitted between two parties, ensuring confidentiality and integrity of the information exchanged. It is widely used to secure web browsing, email, and other internet-based services.

Trusted Platform Module (TPM)

A secure cryptoprocessor that is embedded in a device to provide hardware-based security functions, such as secure storage of cryptographic keys, device authentication, and attestation of system integrity. TPMs help protect against software-based attacks and ensure that a device boots into a trusted state.

Two-Factor Authentication (2FA)

A type of multi-factor authentication that requires users to provide two forms of identification to access a system or resource. Typically, 2FA combines something the user knows (e.g., a password) with something the user has (e.g., a security token or mobile app) to provide an additional layer of security beyond single-factor authentication.

Virtual Private Network (VPN)

A secure, encrypted connection between two or more devices over a public network, such as the internet. VPNs allow remote users to securely access an organization's network resources and protect the confidentiality and integrity of data transmitted over untrusted networks.

VLAN

A Virtual Local Area Network, which is a logical subdivision of a physical network that allows devices to communicate as if they were connected to the same physical network, even if they are on different physical segments. VLANs help improve network security and performance by isolating traffic and applying different security policies to different network segments.

Vulnerability

A weakness in a system, application, or process that could be exploited by a threat actor to gain unauthorized access, disrupt operations, or compromise data. Vulnerabilities can result from software bugs, misconfigurations, design flaws, or human errors, and can be mitigated through patching, system hardening, and other security measures.

Vulnerability Assessment

The process of identifying, classifying, and prioritizing vulnerabilities in systems, applications, and networks. Vulnerability assessments involve using automated scanning tools and manual testing techniques to discover potential security weaknesses and provide recommendations for remediation.

Vulnerability Disclosure

The process of identifying, reporting, and communicating information about vulnerabilities in systems, software, or hardware to the appropriate parties, such as vendors, developers, and the public. Vulnerability disclosure policies and programs provide guidelines for how vulnerabilities should be reported, assessed, and remediated, and help ensure that potential risks are addressed in a timely and responsible manner.

Vulnerability Management

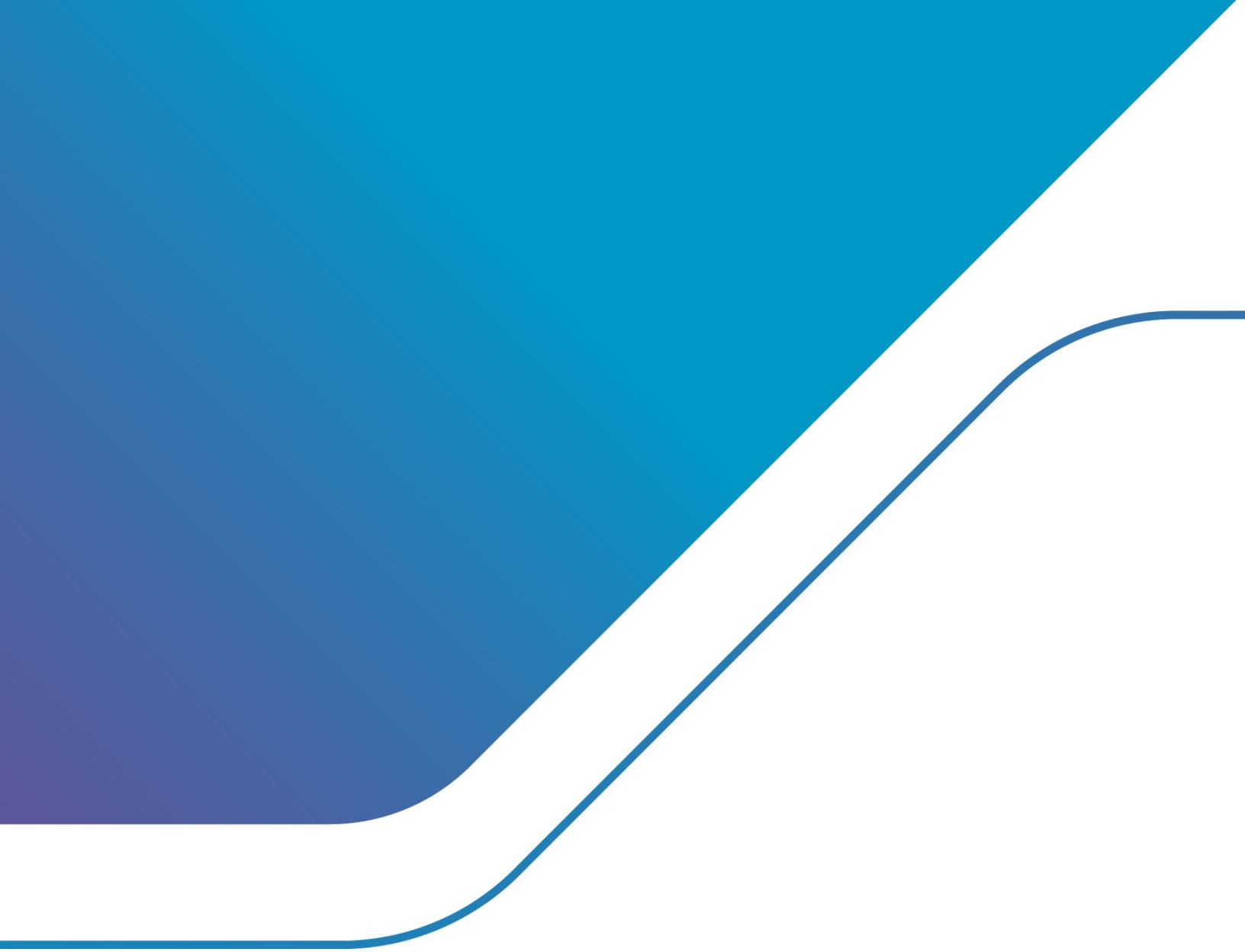
The ongoing process of identifying, evaluating, prioritizing, and remediating vulnerabilities in an organization's systems and networks. Vulnerability management involves establishing policies and procedures for regularly assessing and mitigating vulnerabilities, as well as tracking and reporting on the effectiveness of remediation efforts.

Zero-Day Vulnerability

A software vulnerability that is unknown to those who should be interested in mitigating the vulnerability (including the vendor of the target software). Until the vulnerability is mitigated, hackers can exploit it to adversely affect computer programs, data, additional computers, or a network.

Zero Trust

A security model that assumes no implicit trust for any entity, whether inside or outside the network perimeter, and requires continuous verification and authorization for every access request. Zero Trust relies on strict identity verification, device authentication, and least-privilege access controls to minimize the risk of unauthorized access and lateral movement within a network.



vmware® by Broadcom