BITS Vulnerability Management Glossary

- **Vulnerability:** A weakness or flaw in a product, system's design or implementation that could be exploited by one or more threats to violate the system's security. Vulnerabilities include, but are not limited to, missing operating system and application patches, inappropriately installed or active applications and services, software flaws, software coding flaws, misconfigurations in systems
    - **Common Vulnerability and Exposures (CVE):** The Common Vulnerabilities and Exposures (CVE) system provides a reference method for publicly known information-security vulnerabilities and exposures maintained by MITRE. These CVEs can be identified and referenced within the National Vulnerability Database (NVD).
    - **National Vulnerability Database (NVD):** the US government repository of standard-based vulnerability management data. https://nvd.nist.gov/vuln/search
    - **CWE:** common software and hardware weaknesses. It serves as a common language, a measuring stick for security tools and as a baseline for weakness identification, mitigation and prevention efforts.
    - **CVSS:** Common Vulnerability Scoring System is owned and managed by FIRST.Org, Inc. (FIRST). CVSS is a scoring system designed to provide an open and standardized method of rating the potential impact and severity of IT vulnerabilities. CVSS is composed of three metric groups: Base, Temporal and Environmental.
        - **Base:** reflects the severity of a vulnerability according to its intrinsic characteristics which are constant over time and assumes worst-case impact across different deployed environments.
        - **Temporal:** adjust the Base severity of a vulnerability based on factors that change over time, such as the availability of exploit code.
        - **Environmental**: adjust the Base and Temporal severities to a specific computing environment considering factors such as mitigations.
        - **CVSS v2:** Started in 2005 to provide and standardized method for rating vulnerabilities' potential impact.
            - **CVSS v2 Calculator:** https://nvd.nist.gov/vuln-metrics/cvss/v2-calculator

Severity	Score
Low	**0.0 – 3.9**
Moderate	**4.0 – 6.9**
High	**7.0 – 10.0**

- **CVSS v3:** A newer version of CVSS that more accurately reflects vulnerabilities that fall under web application domain. Additional metrics were added such as scope and User Interaction and previous metrics such as Authentication were changed to Privileges Required. Additionally, the scale was modified to include critical.
  - **CVSS v3 Calculator:** https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator

Severity	Score
None	**0.0**
Low	**0.1 – 3.9**
Moderate	**4.0 – 6.9**
High	**7.0 – 8.9**
Critical	**9.0 – 10.0**

- **Zero-Day:** Also known as 0-day, is a newly discovered vulnerability or flaw which is identified before a patch has been released to mitigate the vulnerability or flaw. Once a patch is available the vulnerability or flaw is no longer called a zero-day.
- **Exploit:** An exploit is a piece of software, a chunk of data or a sequence of commands that takes advantage of a bug, glitch or vulnerability in order to cause unintended or unanticipated behavior to occur on computer software, hardware or something electronic.

- **Risk:** The potential for an unwanted or adverse outcome resulting from an incident, event or occurrence, as determined by the likelihood that a threat would exploit a vulnerability, with the associated consequences.
- **Impact:** The effect of an event, incident or occurrence of an exploited vulnerability.
- **Compliance Scan:** Scan to identify adherence to an organization's hardening standards on IT Systems.
  - **Hardening:** System hardening standards are used to set a baseline of requirements for securing a system. PCI-DSS requirement 2.2 requires baselines to be consistent with industry-accepted hardening standards. There are several industry standards that provide benchmarks for various operating systems and applications, such as CIS, NIST and ISO.
    - **Center Internet Security (CIS):** Provides Benchmarks for guidelines to securing 100's of distinct systems and platforms. https://www.cisecurity.org/cis-benchmarks/
    - **National Institute of Standards and Technology (NIST):** NIST maintains the National Checklist Repository, with information on a variety of security configuration checklists for specific IT products. https://nvd.nist.gov/ncp/repository
    - **International Organization for Standardization (ISO):** Independent non-government organization which develops relevant International standards. https://www.iso.org/standards.html
- **Vulnerability Scan:** Scan to identify vulnerabilities on IT Systems.
  - **Unauthenticated Scan:** A type of scan that does not require credentials to authenticate to a machine to determine the presence of vulnerability. This type of scan mimics a threat actor's view from the outside.

  - **Authenticated Scan:** A type of scan that requires administrative credentials to authenticate to a machine to determine the presence of vulnerability without having to attempt an intrusive scan. This type of scan results in fewer false positives and potential vulnerabilities which can lead to more findings as the scan is able to perform a deep scan of the system.
  - **Intrusive Scan:** A type of scan that attempts to determine the presence of vulnerability by actively executing a known exploit.
  - **External Scan:** Vulnerability scan conducted from outside the organization's perimeter firewall.
  - **Internal Scan:** Vulnerability scan conducted from within the organization's perimeter firewall.
  - **Port Scan:** a method of scanning for determining which ports on a network are open

- **Software Development Life Cycle (SDLC):** A software development methodology/process used to design, develop, test and secure high-quality software. Vulnerability Management scans can be performed at different stages of this life cycle.
  - **Static Application Security Testing (SAST):** Technologies designed to analyze application source code, byte code and binaries for coding and design conditions that are indicative of security vulnerabilities. These scans can be performed at multiple stages within the Software Development Life Cycle to lower the cost associated with security defect remediation.
  - **Dynamic Application Security Testing (DAST):** Technologies designed to detect conditions indicative of a security vulnerability in an application in its running state.
  - **Interactive Application Security Testing (IAST):** Technologies designed to detect software code vulnerabilities in running applications by utilizing software instrumentation
- **Integrated Development Environment (IDE):** A software that facilitates the development of applications. IDEs are designed to integrate programming tasks (code editor, compiler, debugger, build automation). Scanning technologies can sometimes include IDE plugins used for scanning for vulnerabilities during software development.
- **Vulnerability Management Disclosure Program:** offers a secure channel for researchers to report security issues and vulnerabilities, and typically includes a framework for intake, triage and workflows for remediation.
- **Bug Bounty:** a crowdsourcing initiative that rewards individuals for discovering and reporting vulnerabilities or bugs within software or applications.
- **Penetration Testing:** or ethical hacking, is the practice of testing a computer system, network or web application to find security vulnerabilities that an attacker could exploit.
- **Support Team:** The team responsible for implementing and maintaining the IT System

- **Vulnerability Remediation:** Corrective action to address a weakness or flaw in a product, system's design or implementation that could be exploited. Examples of remediation efforts could include installation of a software patch, adjustment of a configuration setting or removal of the affected software.
    - **First Detected:** This field denotes the first time a vulnerability was detected on a system.
    - **Last Detected:** This field denotes the last time a vulnerability was detected on a system.
    - **Resolved Within:** The time from scan completion to the implementation of the resolution
    - **Support Team:** The team responsible for implementing and maintaining the IT System
    - **Mitigating Controls:** Controls put in place to reduce either the probability or impact of a threat (i.e. vulnerability)
    - **Compensating Control:** Controls used by an organization instead of a recommended security control that provides equivalent or comparable protection for an information system
    - **Validated:** Analysis performed by the support teams to determine if the finding is a false positive or a legitimate finding.
    - **False Positive:** occurs when a scanner can access only a subset of the required information, which prevents it from accurately determining whether a vulnerability exists. To help reduce the number of false positives, you should configure your scanners with the appropriate credentials.
    - **End of Life (EOL):** means a vendor has decided that the product has reached the end of its "useful lifespan." EOL symbolizes the last stage of a product's life cycle, starting with design, development and eventual release and use.
    - **End of Support (EOS):** refers to where a company ceases support for a product or service. This is typically applied to hardware and software products when a company releases a new version and ends support for previous versions.
    - **Patch Management:** the process for identifying, acquiring, installing and verifying patches for applications, products and systems.
        - **Patch:** remediation or change applied to an asset to correct a security weakness or functionality problem in software and firmware.
    - **Update:** The process of applying new patches and or changes to the existing file or program on a system
    - **Upgrade:** The process of uninstalling the existing file or program and installing a new one in its place.