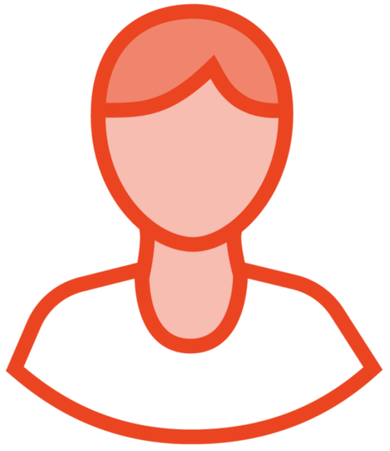
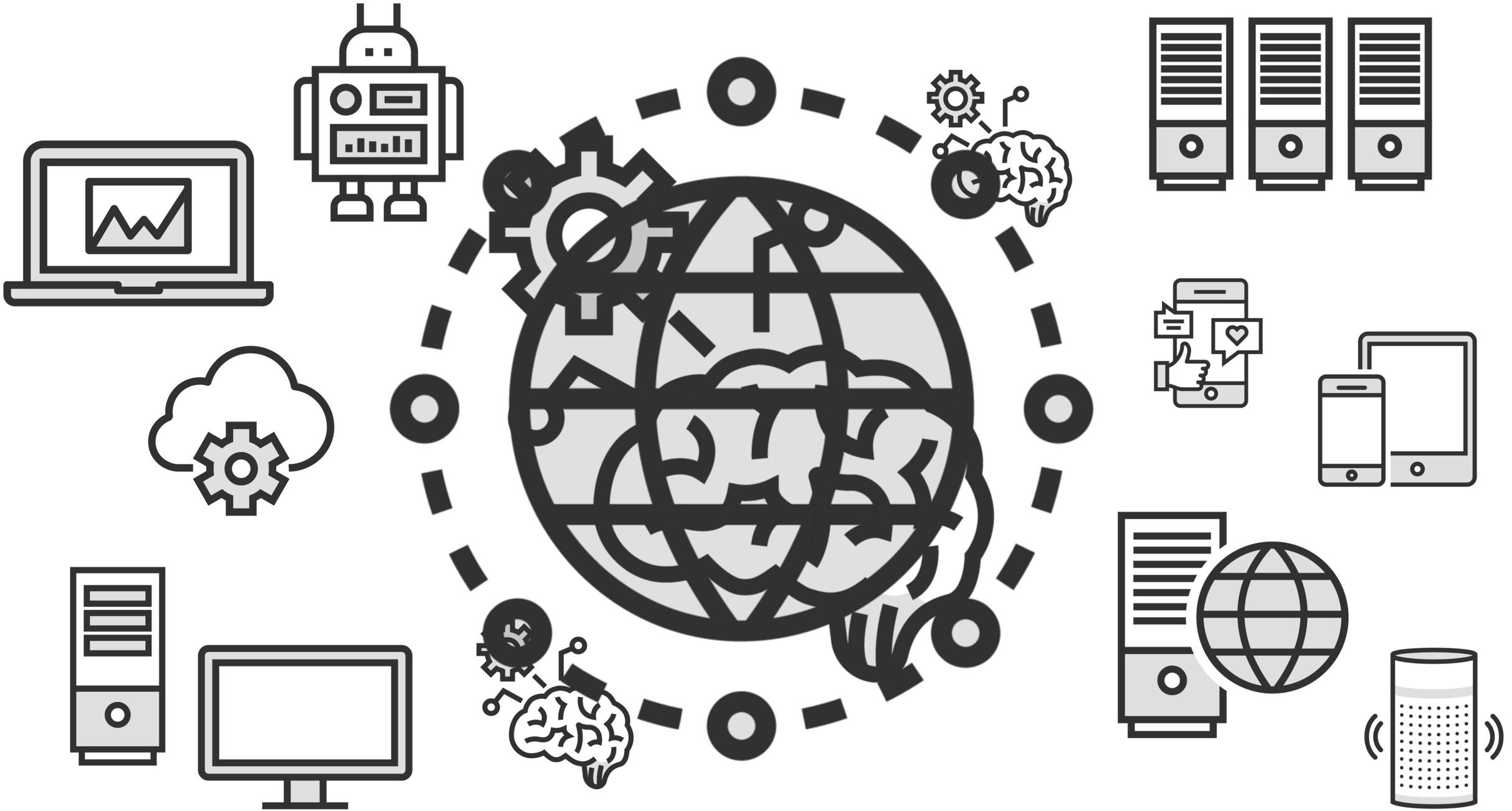
Ethical Hacking: Vulnerability Analysis

Identifying Vulnerability Assessment Concepts

Dale Meredith
MCT | CEI | CEH | MCSA | MCSE
Cyber Security Expert

dalemeredith.com | Twitter: @dalemeredith | Linkedin: dalemeredith





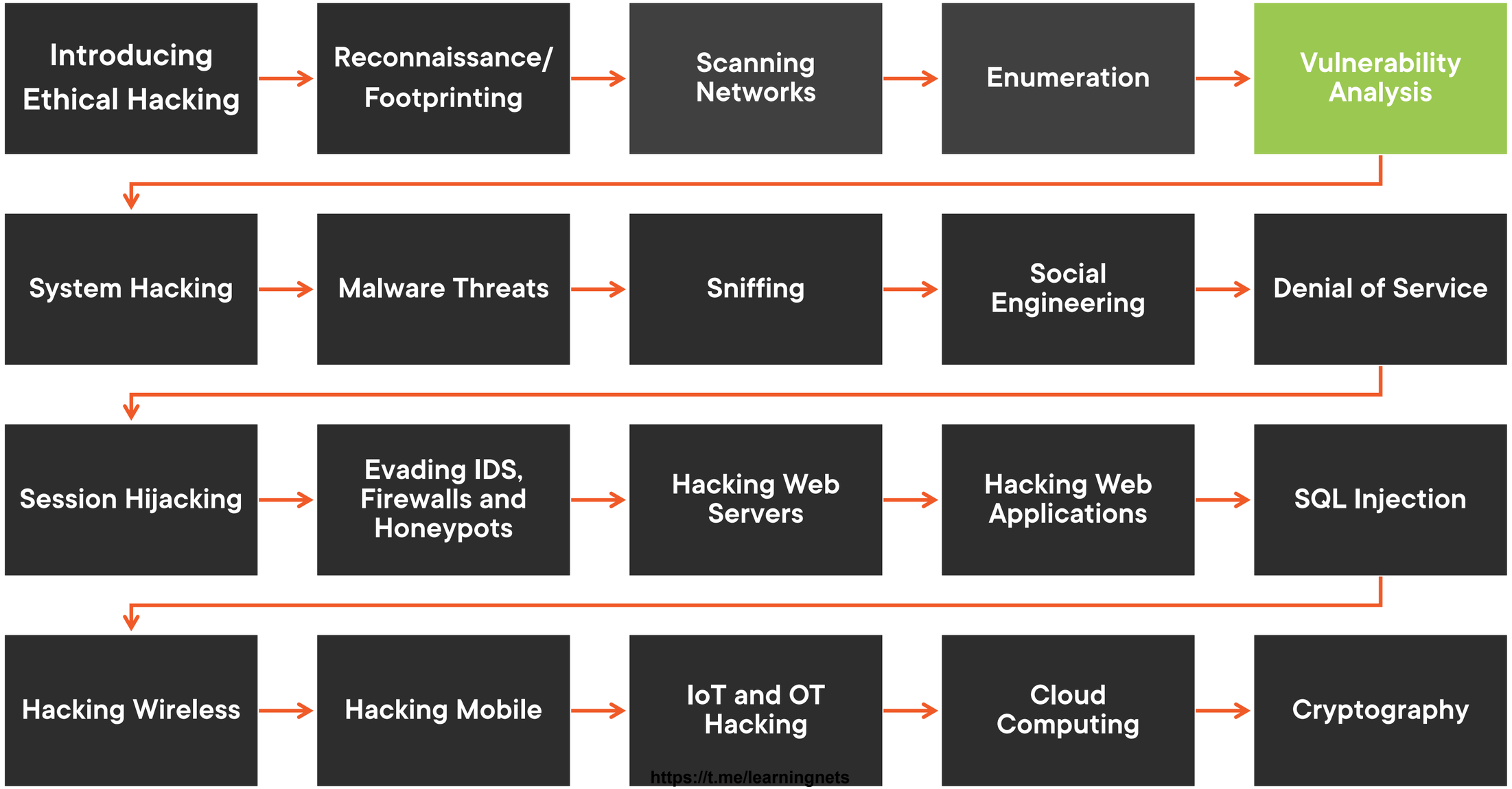
Ethical Hacking: Vulnerability Analysis

Identifying Vulnerability Assessment Concepts

Dale Meredith
MCT | CEI | CEH | MCSA | MCSE
Cyber Security Expert

dalemeredith.com | Twitter: @dalemeredith | Linkedin: dalemeredith

Ethical Hacking Series

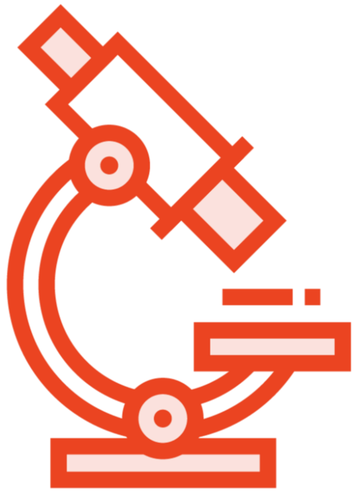


What is Vulnerability Assessment?

Vulnerability Assessments

Assesses

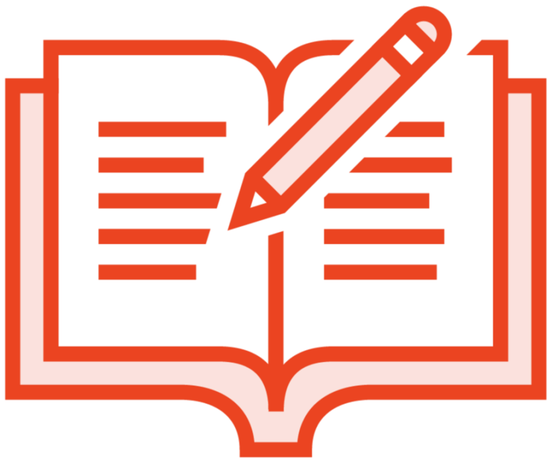
Examines



Detects

Quantifies

Vulnerability Research



Study

Identify

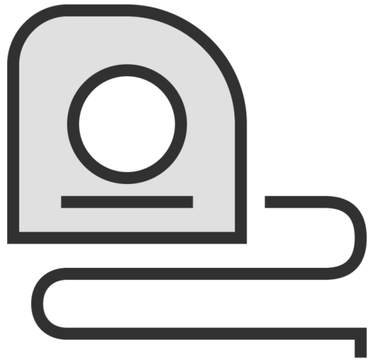
Read

Vulnerability Scoring Systems and Databases

Common Vulnerability Scoring System (CVSS)

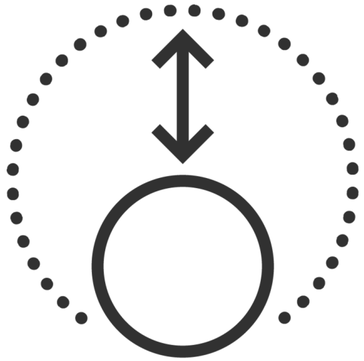
Calculates a base score between one and ten, with ten being the most severe

Score is determined and generated by a vector string that represents the numerical score for each group as a block of text



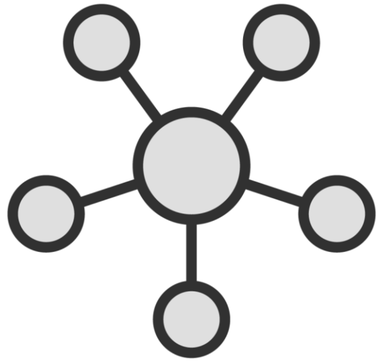
Base Metric

Inherent qualities of a vulnerability



Temporal Metric

Changing features during the lifetime



Environmental Metric

Particular environment or implementation

Common Vulnerabilities and Exposures (CVE)

CVE is a list of publicly known cybersecurity vulnerabilities. Each entry contains an identification number, a description, and at least one public reference.

CVE identifiers enable data exchange between security products and provide a common language for describing data

CVE IDs

Provide a baseline for evaluating which tools are most effective and appropriate for identified needs

Better coverage

Easier interoperability

Enhanced security

National Vulnerability Database (NVD)

- **Security checklist refrences**
- **Software vulnerabilities**
- **Misconfiguration findings**
- **Product names**
- **Impact metrics**

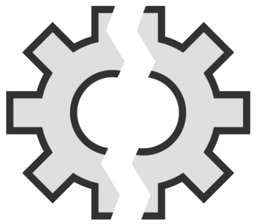
NVD does not conduct active vulnerability testing

NVD performs an analysis on CVEs that have been published in the CVE dictionary

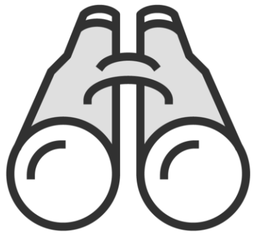
Analysis is done by aggregating data points from information publicly available

Common Weakness Enumeration (CWE)

A category system for software flaws and inadequacies

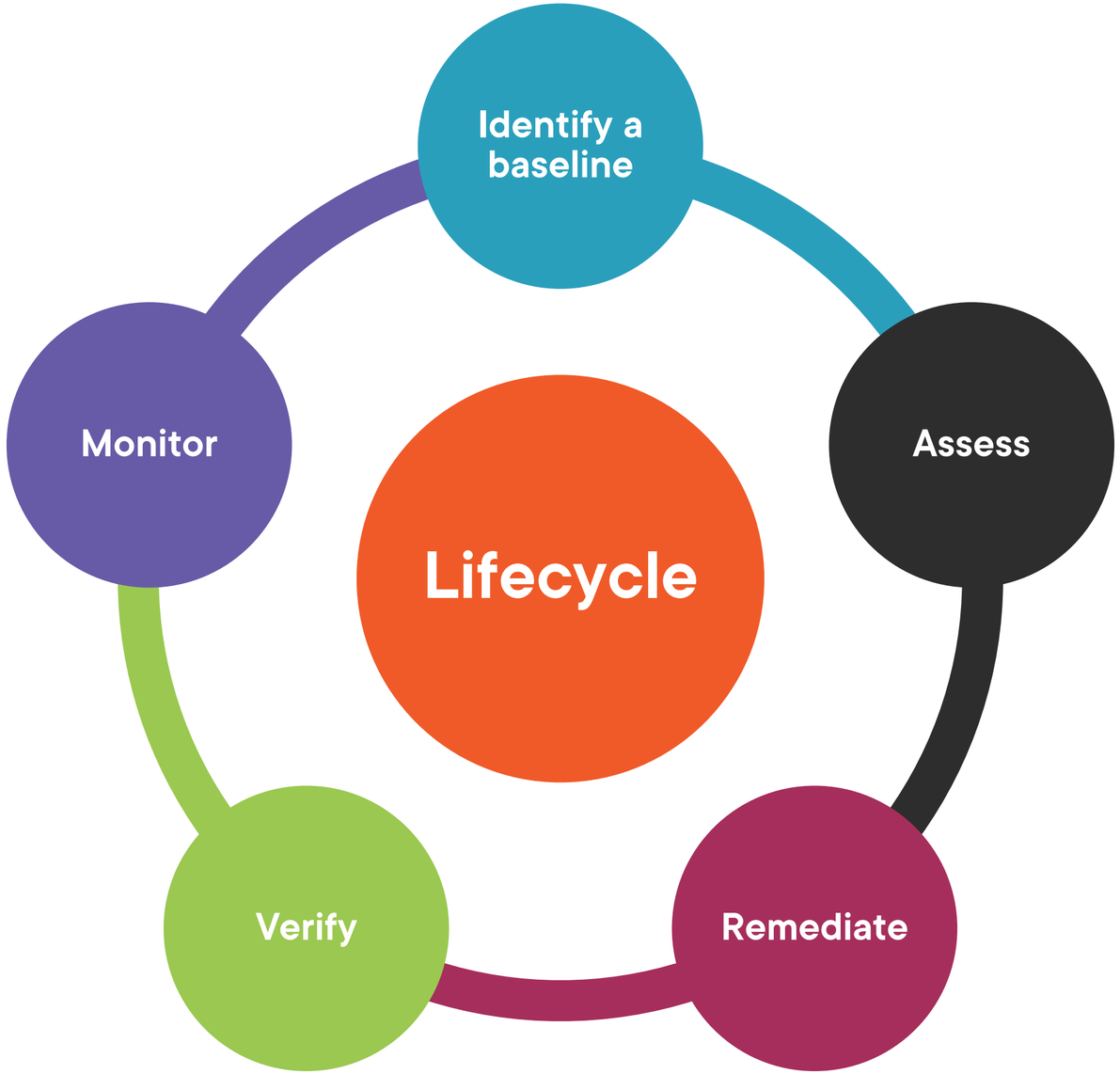


Used as a baseline for weakness detection, mitigation, and prevention

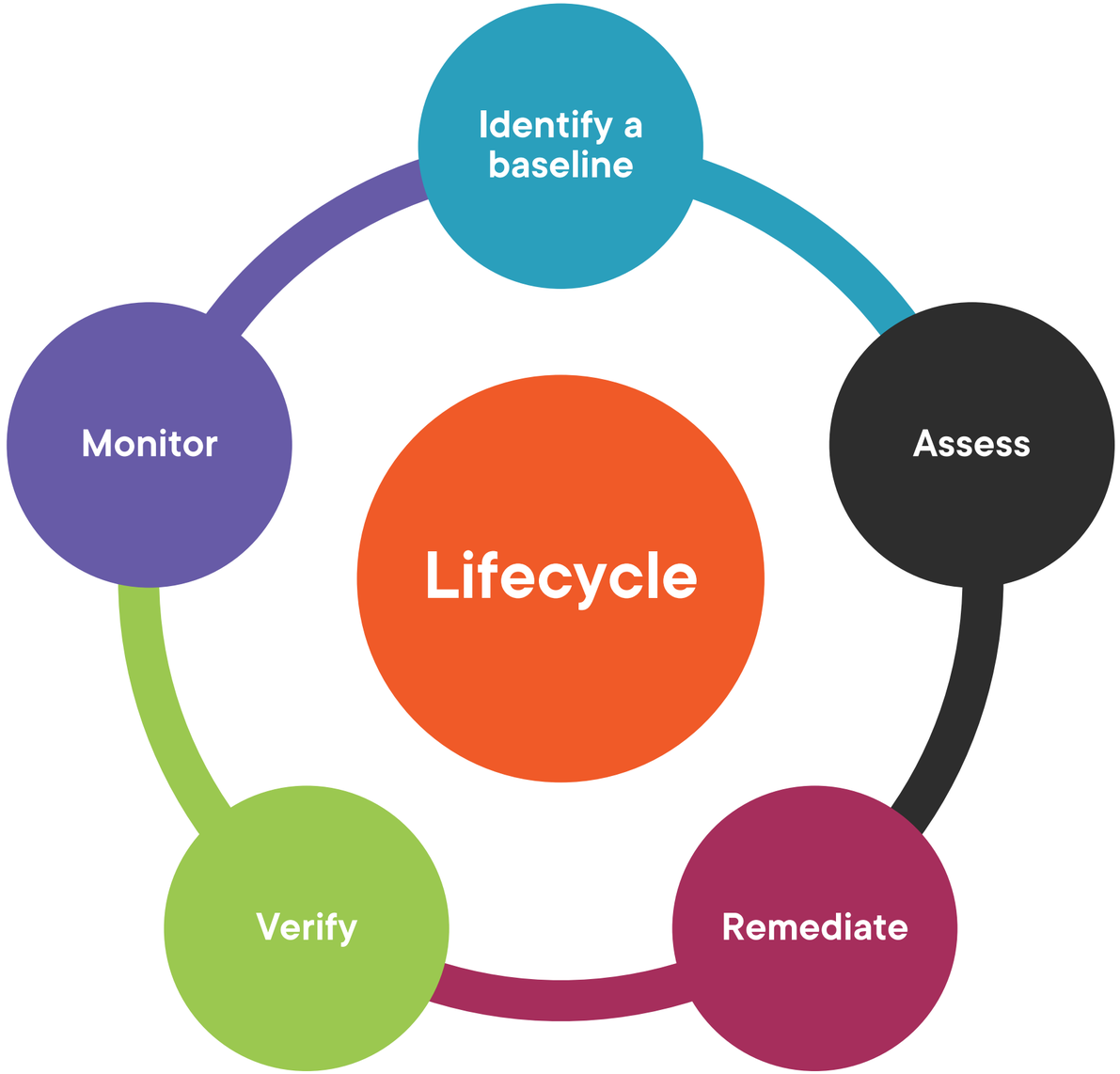


Offers an advanced search option that allows attackers to view vulnerabilities based on research ideas, development ideas, and architectural concepts

The Lifecycle



- Identify a baseline
- Assess and summarize the risk level
- Remediate the weaknesses
- Verify issues have been fixed
- Monitor to maintain



Pre-assessment Phase

Three Phases

Pre-assessment Phase

Vulnerability Assessment Phase

Post-assessment Phase

Pre-assessment Phase

Preparation stage

Defines standards and scope

Devises information protection procedures

Pre-assessment Phase

Identify the business process

Examine the apps, data, and services that back up company procedures

Locate the authorized software, drivers, and basic configurations

Create an inventory and prioritize critical assets

Understand and map the network infrastructure

Identify controls

Understand and practice policy implementation

Clarify the scope of the assessment

Design appropriate information protection procedures

Vulnerability Asessment Phase

Vulnerability Assessment Phase

Examine the network architecture

Evaluate threats to the environment

Perform penetration testing to identify vulnerabilities

Consider and evaluate physical security

Analyze physical assets

Assess operational security

Examine policies and procedures to identify security gaps

Assess infrastructure interdependencies

The goal of the vulnerability assessment is to identify weaknesses that could be exploited by attackers.

Post-assessment Phase

Three Phases

Pre-assessment Phase

Vulnerability Assessment Phase

Post-assessment Phase

Post-assessment Phase

Analyze the findings of the assessment and develop a risk assessment report

Develop a remediation plan to address short-term and long-term solutions

Verify the effectiveness of the remediation plan

Learning Check

Learning Check

- CVSS
- CVE
- Vulnerability Assessment Phase
- Post-assessment Phase

Up Next: Optimizing Your Vulnerability Scans