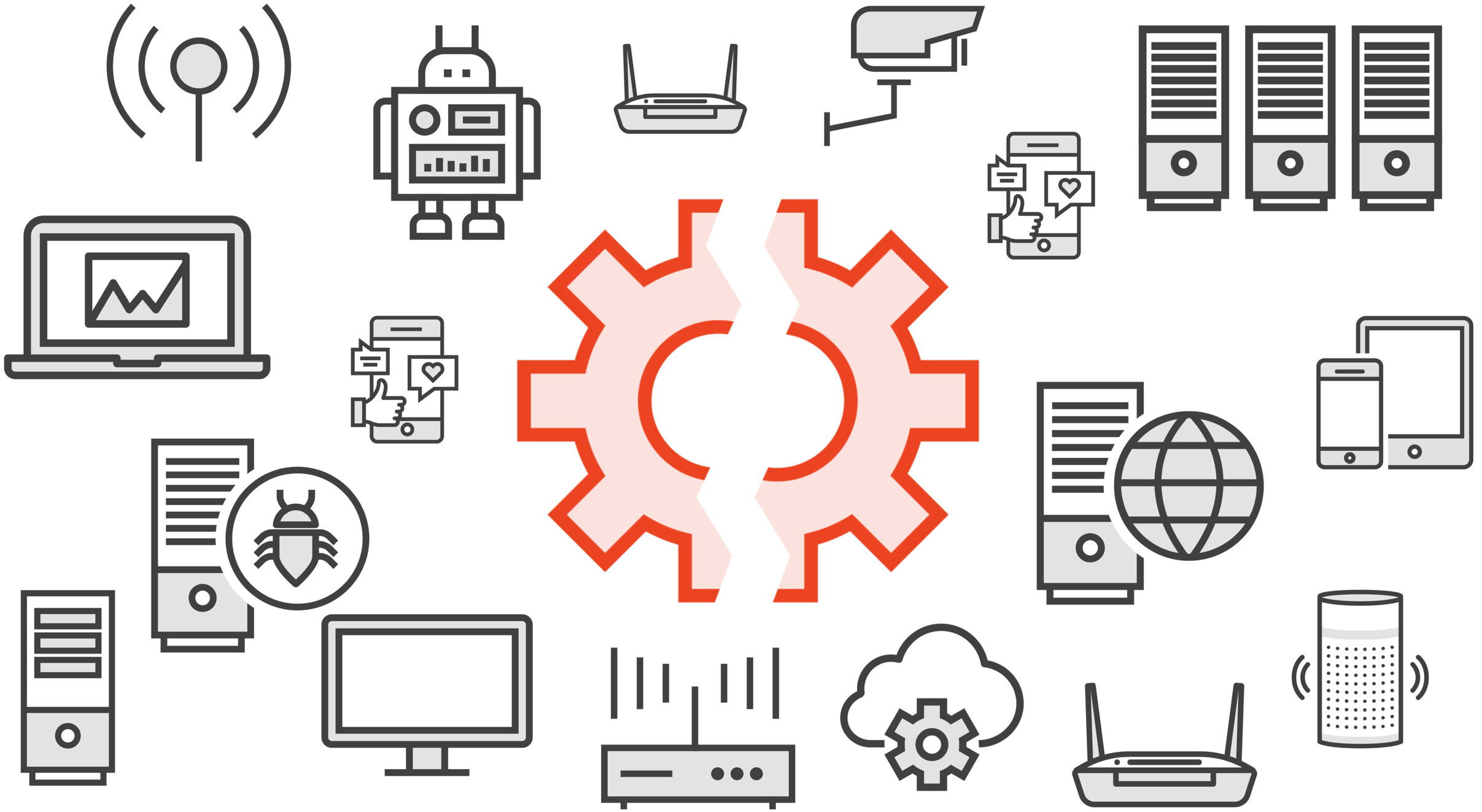
Optimizing Your Vulnerability Scans

Dale Meredith

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

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

Classifications



Vulnerability Categories

Misconfiguration

Defaults

Buffer overflows

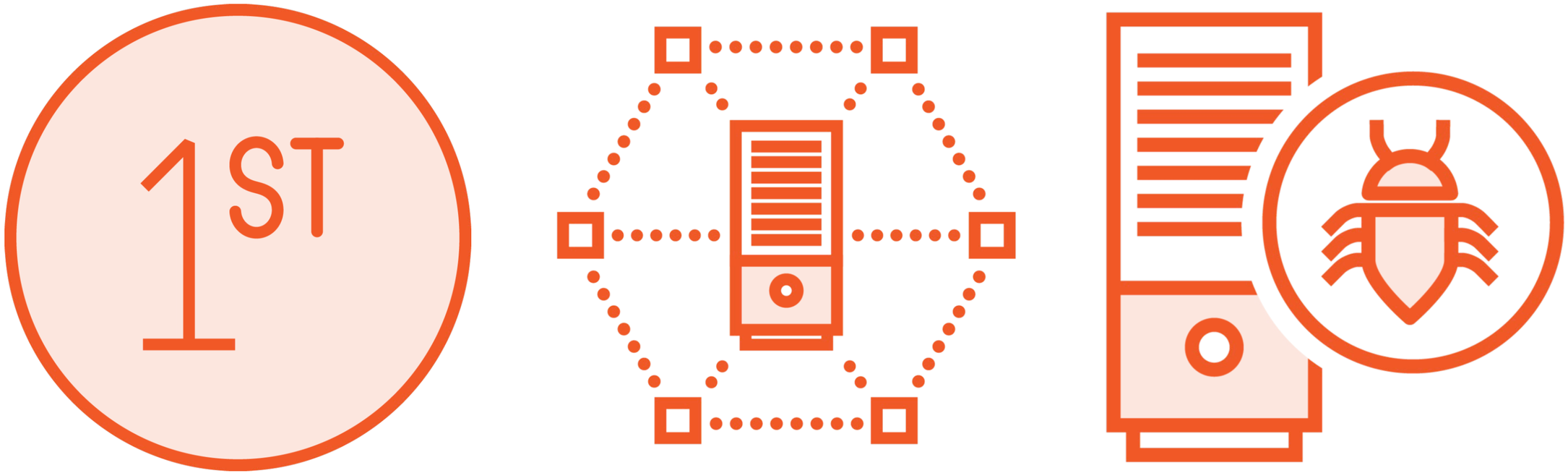
Design flaws

Unpatched systems

Misconfiguration

		Incorrect folder permissions	Enabled configuration pages
Default accounts or passwords	Improper authentications	Disabled security settings	Misconfigured SSL certificates
Weak password	Unpatched software	Insecure file permissions	Debug's enabled
Open admin ports	Outdated software	Unnecessary services	Outbound connections

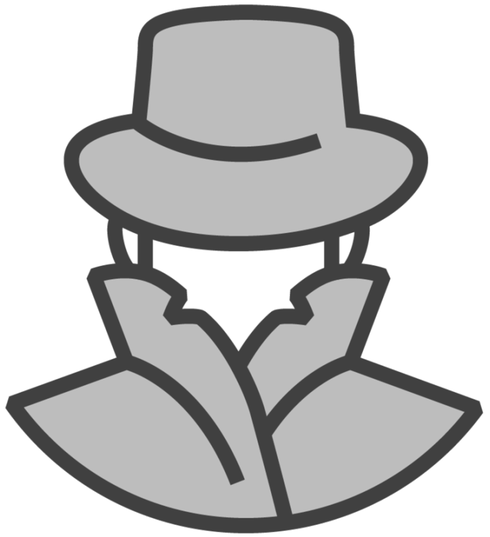
Defaults



Failing to alter default settings can allow entry to outside attacks

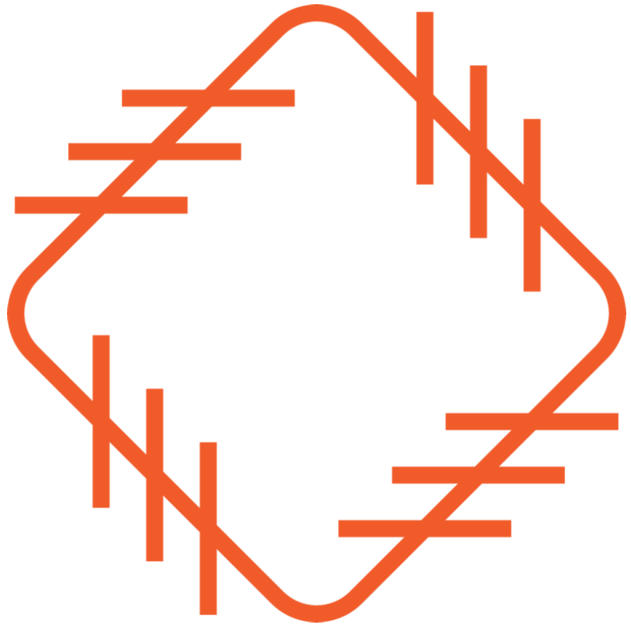
Buffer Overflows

A software vulnerability that occurs as a result of programming mistakes



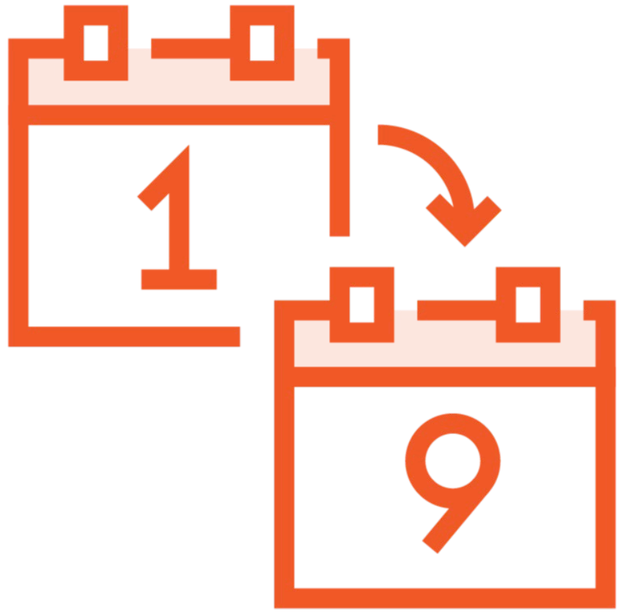
Attackers attempt to take over the system by overwriting content beyond the allotted size of the buffer

Unpatched Systems



Unpatched servers jeopardize data integrity

Exposes data and can result in financial loss



Update software, patch, and fix bugs regularly

Design Flaws

Found in all operating systems

Created by faulty encryption or faulty data validation

Allows attackers access to a system

Vulnerabilities in Operating Systems

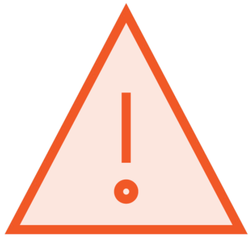
Keep the OS updated

Minimize software program installs

Use applications that have firewall capabilities

Application Vulnerabilities

Concerns about vulnerabilities in applications should be balanced against the importance of secure application architecture



Application flaws are exploited by attackers

Developers must have a thorough knowledge of the anatomy of typical security flaws and create secure apps that validate and authorize users correctly

Active, Passive, Internal and External

Active Assessment

Exploits vulnerabilities to see if they are real

Facilitated by ethical hackers or penetration testers

Passive Assessment

Data collection

Utilizes automated tools that scan for known vulnerabilities

Advantages and Disadvantage

Active assessment

Passive assessment

Internal and External Assessments

Internal

External

Host, Network, and Wireless

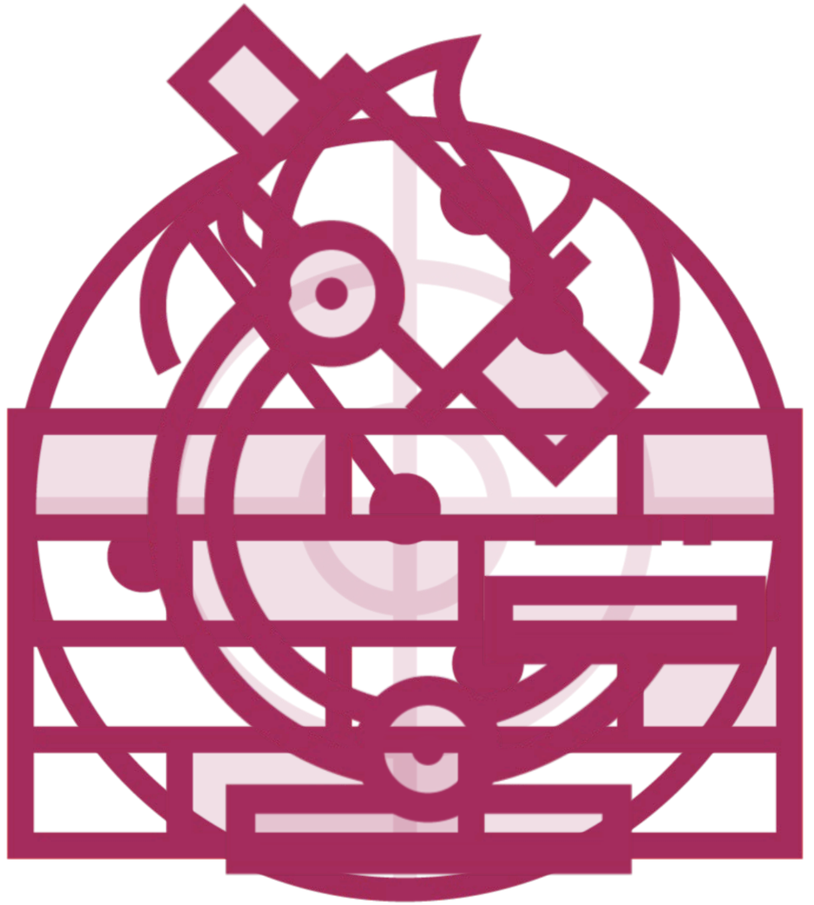
Host-based Assessment

Performed on individual systems

Identifies vulnerabilities that may not be detectable from a network-based perspective

Network-based Assessment

- **Studies the network for choke points**
- **Searches for systems with known vulnerabilities**
- **Analyzes systems for backdoors or Trojans**
- **Attempts to access the system**



Wireless Assessment

The process of detecting and analyzing security flaws

Organizational test verifies wireless networks and uncovers rogue networks

Sniffing wireless traffic and deciphering encryption keys

Identifies flaws that would otherwise go undetected

Application and Databases

Application Assessments

Identifies vulnerabilities in web applications

Utilizes both manual and automated tools

Application Assessments

- SQL injection
- Cross-Site Scripting (XSS)
- Cross-Site Request Forgery (CSRF)
- Session hijacking
- Parameter tampering

Database Assessments

Identifies vulnerabilities in database systems

Utilizes database technologies to identify data exposure or infection-type vulnerabilities

Employs both manual and automated tools

Database Assessments

SQL injection

Privilege escalation

Data leakage

Credentialed and Non-credentialed Assessments

Credentialed Assessment

Known as authenticated assessment

Identifies flaws more easily than non-credential evaluations

Accessing credentials is more challenging

Recognized as the most effective method for detecting security flaws

Non-credentialed Assessment

- **Conducted without root-level access**
- **Does not require credentials from the assets**
- **Information gathered is less reliable**
- **Determines if the target has weak or missing security controls**
- **Fails to detect vulnerabilities covered by firewalls**
- **False-positive outcomes are possible**

Manual and Automated Assessmets

Manual and Automated Assessments

Manual Assessment

Labor-intensive and time-consuming

Identifies vulnerabilities that automated tools are unable to find

Considers the target's specific business environment

Determines if the vulnerability is a true risk to the organization

Automated Assessment

Faster and easier to conduct

Utilizes automated tools that obtain CVE/CWE information

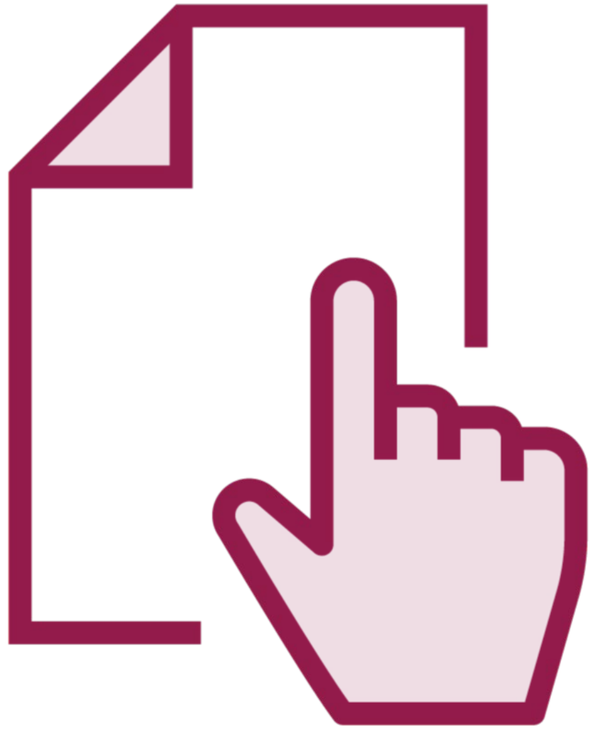
Only as good as the signatures they use to identify vulnerabilities

May generate false-positives

Learning Check

Learning Check

- Application assessment
- Host-based
- External-based
- Active assessment



Up Next:
Types of Vulnerability Assessment Tools