

CompTIA Security+

Lecture 04

SY0-701

Vulnerabilities Management

By
Dr. Khaled ELMenshawy

Lecture

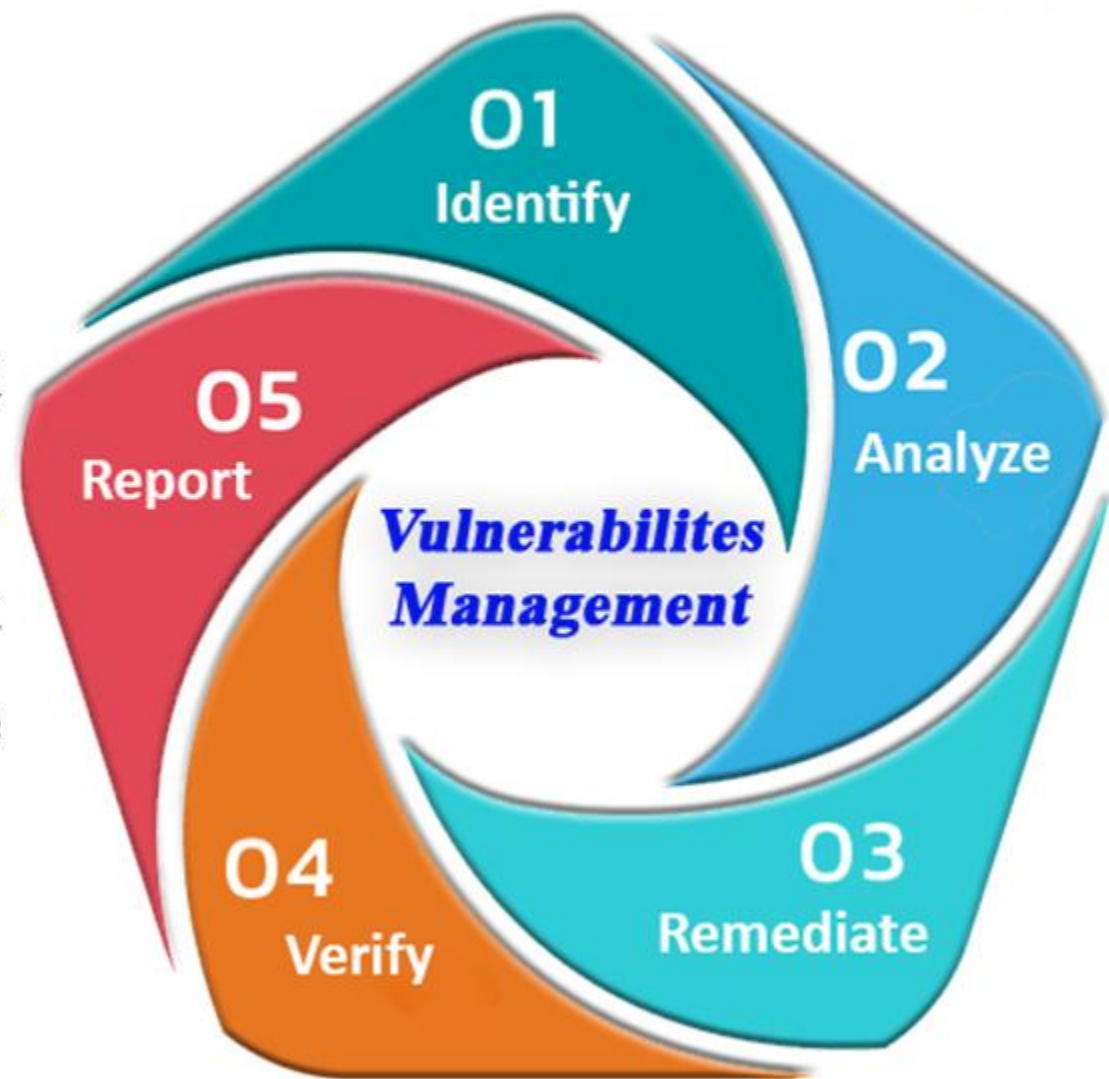
04

LEARNING OUTCOMES

- Understanding Vulnerability Management lifecycle.
- Understanding how to Identifying Vulnerability.
- Understanding Threat Intelligence Feed.
- Understanding Responsible Disclosure Programs.
- Understanding Vulnerability response and remediation.
- Understanding how to Verify Remediation.
- Understanding how to perform Vulnerability Reporting.

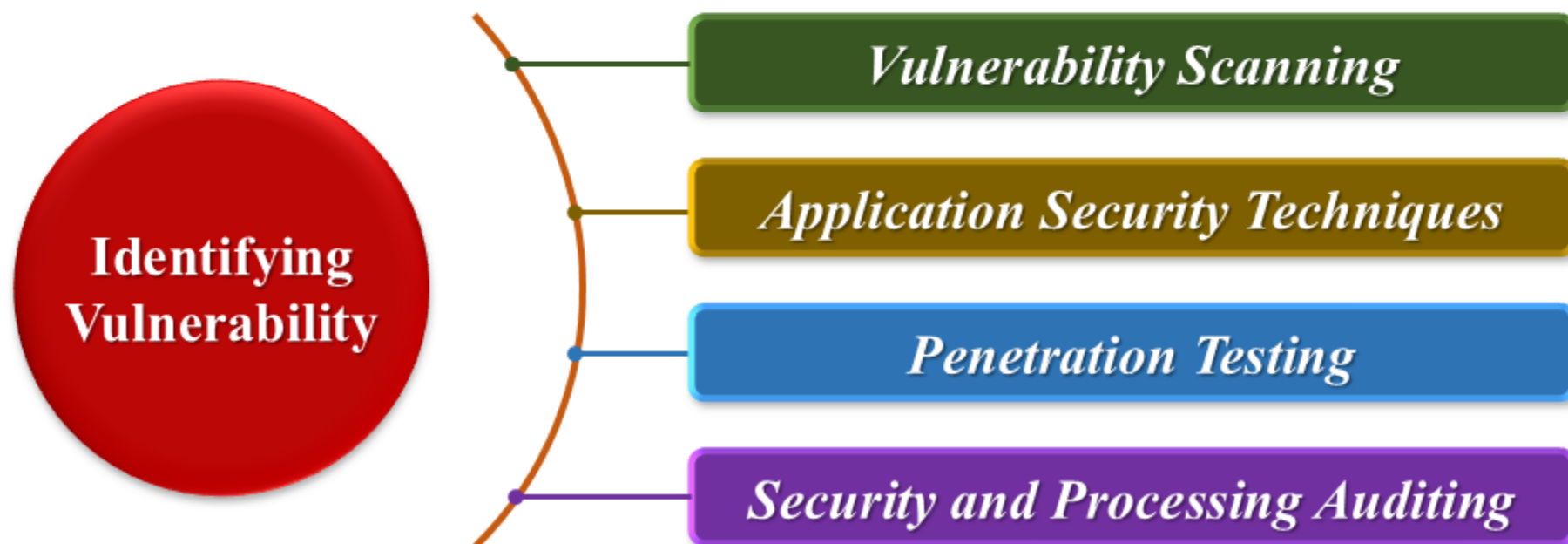
What is Vulnerability Management?

Vulnerability Management is a systematic and ongoing process of *identifying, evaluating, prioritizing, and mitigating vulnerabilities* in computer systems, networks, and software applications.



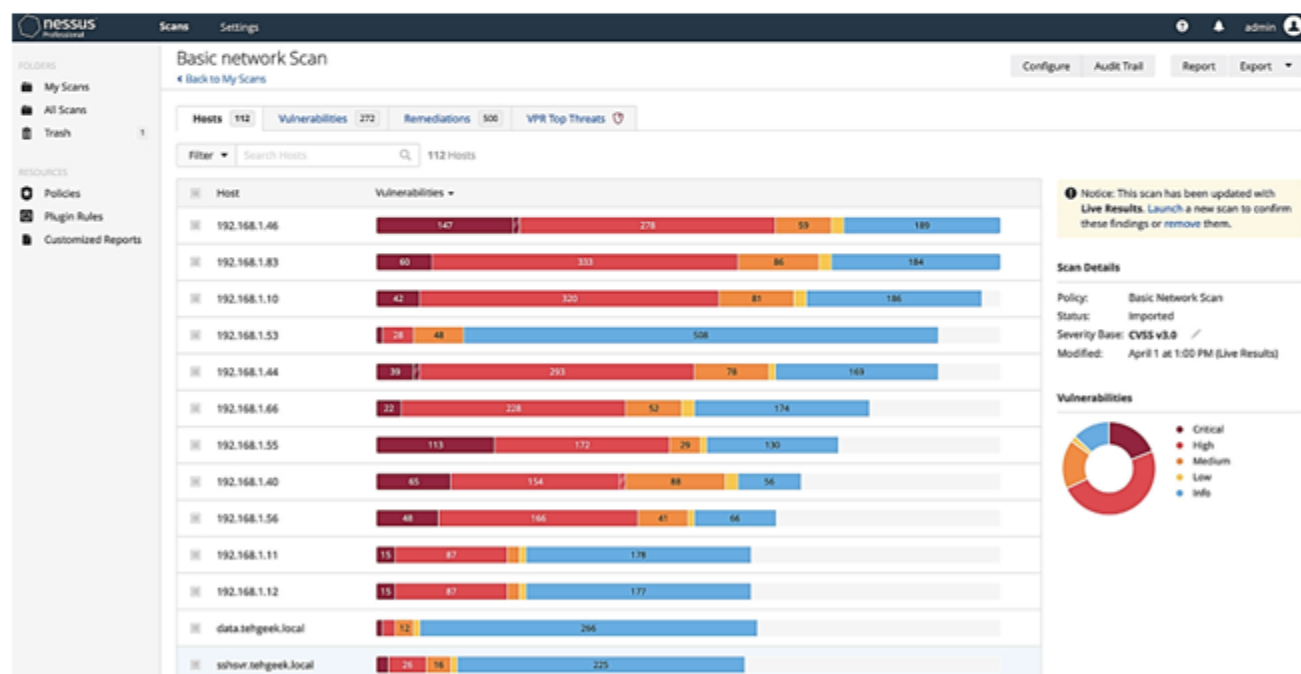
What is Identifying Vulnerability?

Identifying Vulnerability is a systematic practice of spotting and *categorizing weaknesses* in a system, network, or application *that could potentially be exploited*.



- **Vulnerability Scanning;** is an automated method of investigating networks, systems and applications to discover potential vulnerabilities.

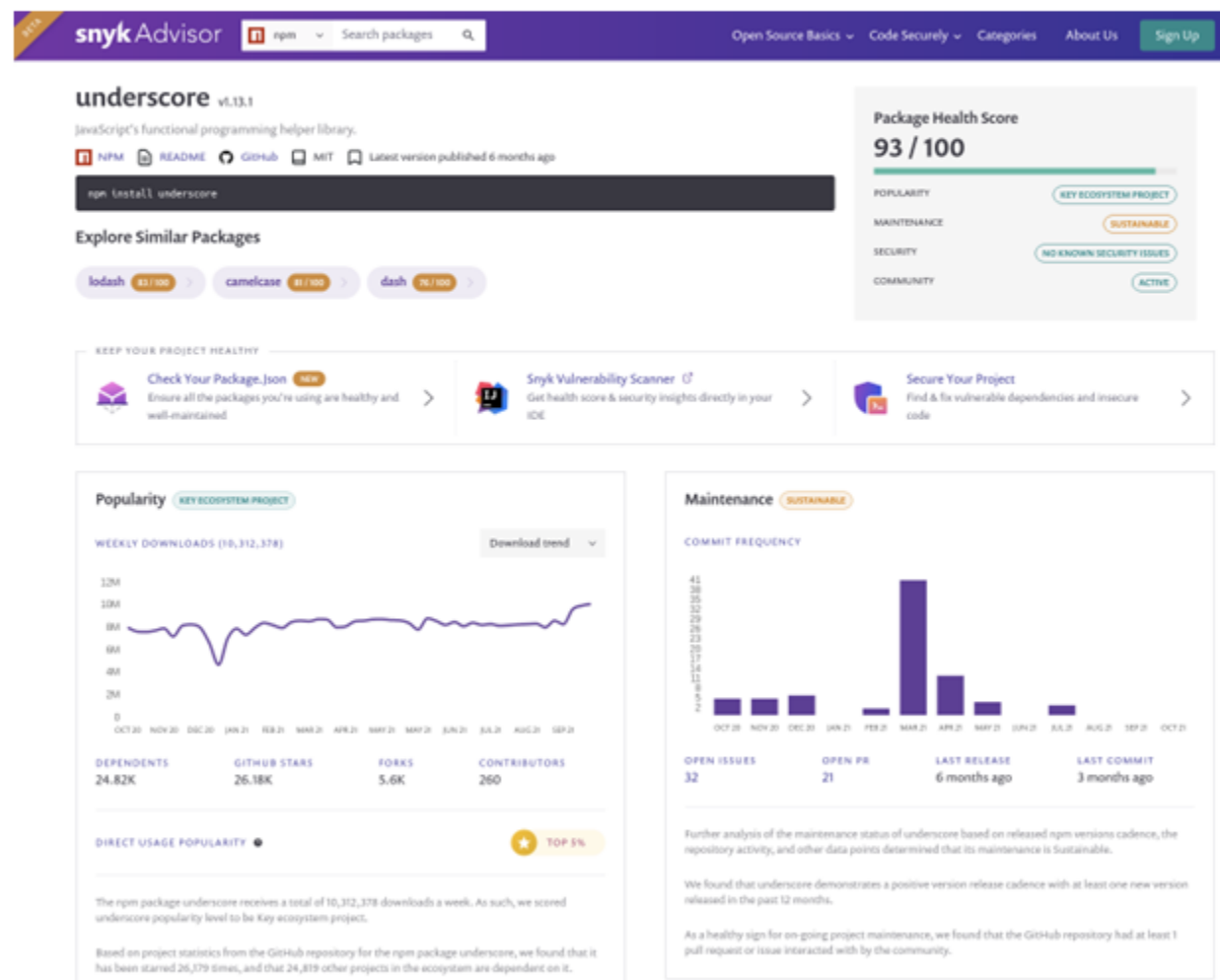
There are many different tools available to help you conduct a vulnerability scan, including things like *Nessus* and *OpenVAS*, analyze the system's current state and generate a detailed report listing out all the vulnerabilities and their criticality level.



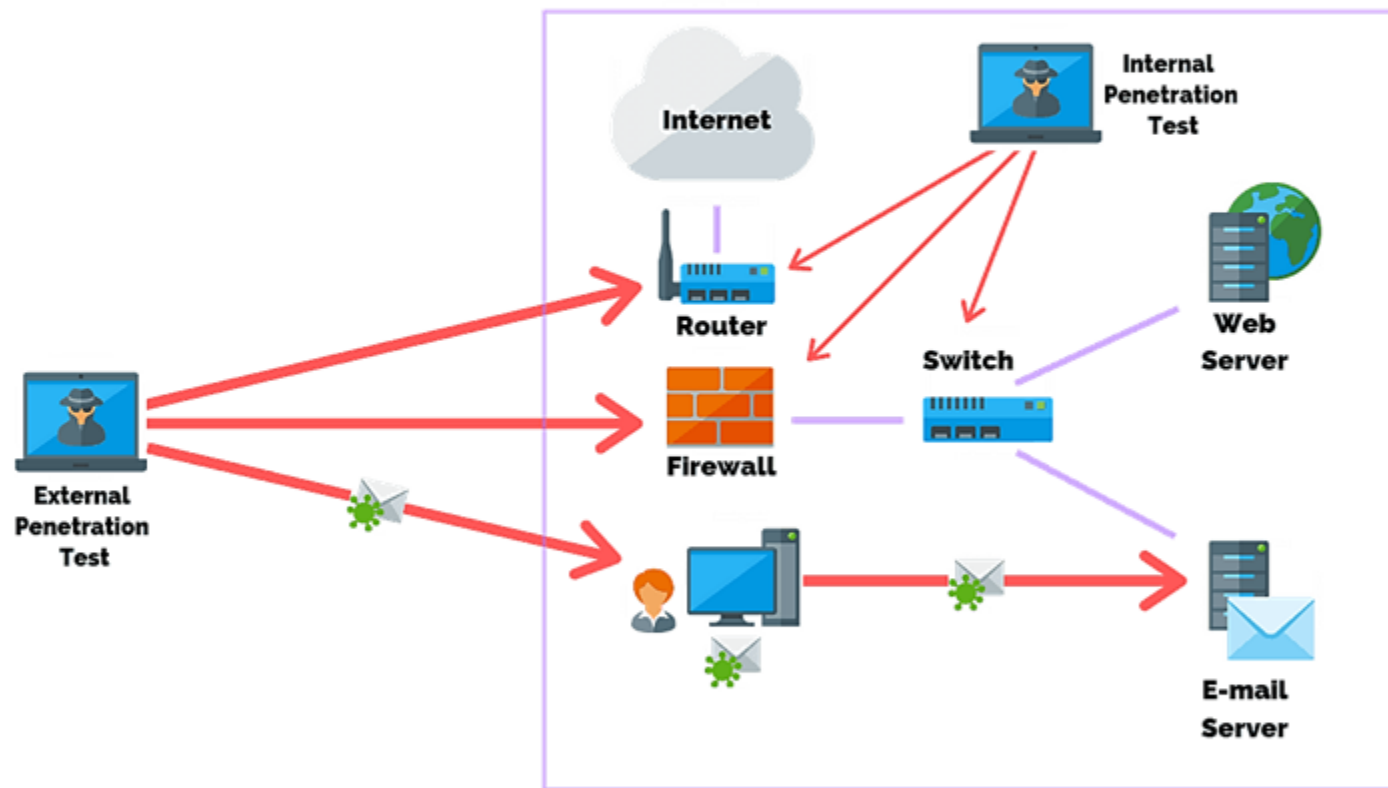
- ***Application Security Techniques;*** is used to safeguard our software from being manipulated during its lifecycle and ensure that any custom software that the organization develops is going to be free of vulnerabilities within its code base.
- ***Static Analysis;*** is going to be used to analyze an application source code *without running or executing that source code* (manual review or automated tool “*CodeScene*, *CodeQL*, etc.).
- ***Dynamic analysis;*** is going to *evaluate an application as it's being run* to determine if there are any vulnerabilities inside of that application (*Burp Suite* & *Peach Fuzzing tools*).

Identifying Vulnerabilities

- Package monitoring;** ensures that the libraries and components that your application depends on are secure and up to date. There are many tools available to conduct package monitoring, including things like *Snyk* and *Dependabot*, which are used to scan the application's dependencies and then alerting to any known vulnerabilities.



- **Penetration testing;** is used to simulate a real-world attack on a system to evaluate its security posture.
- **System and process audits;** are the processes that involves conducting a comprehensive review of the information systems, security policies and procedures.



What is Threat Intelligence?

Threat Intelligence; is a continual process used to *understand the threats faced by an organization*. Depending on the *organization's business and its missions*.

Threat intelligence is going to *combine data from a large number of sources* to keep cybersecurity professionals up to date on the latest attacks, vulnerabilities, threats, mitigations against zero-day attacks and much more.

Threat Intelligence can be received from various sources, including;

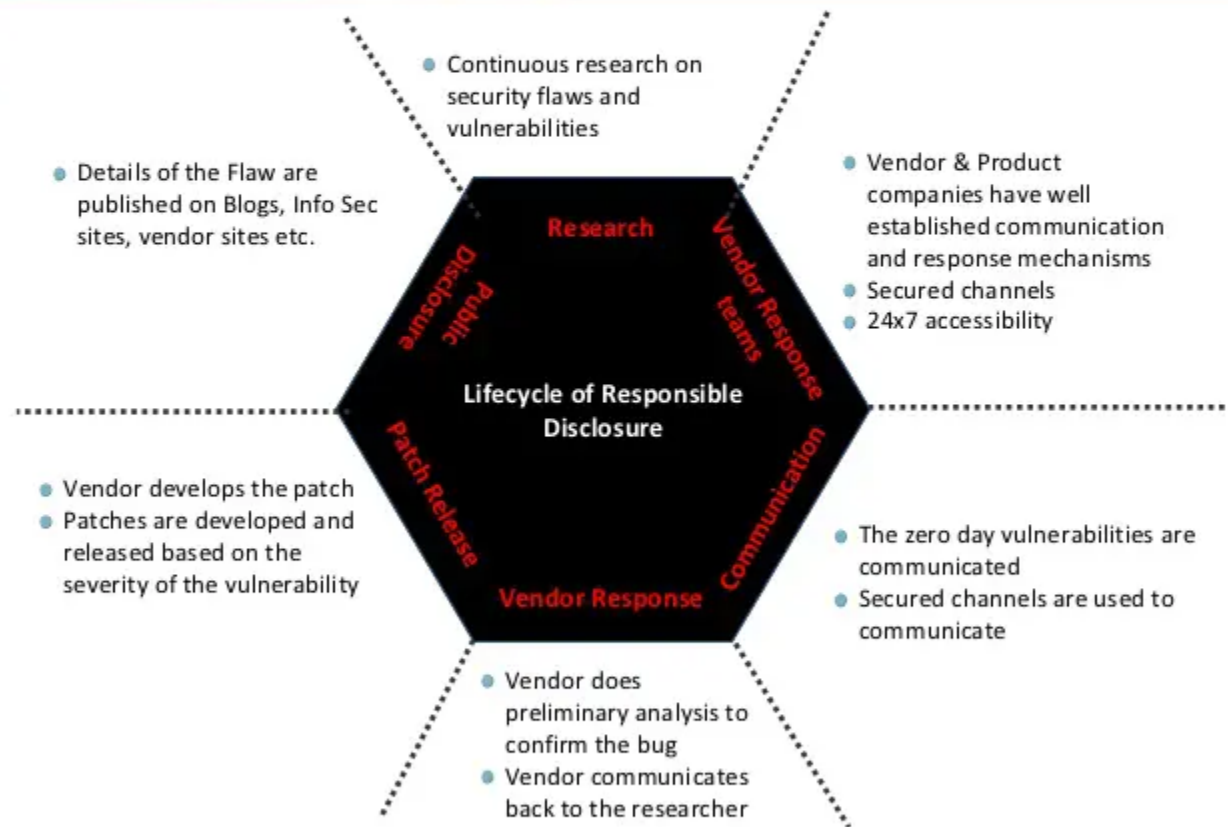
- ***Open-source Intelligence (OSINT)*** such as Live Cyberthreat map, Google hacking database, Common Vulnerabilities and Exposures (CVE), etc.
- ***Proprietary or Third-Party Feed;*** are Threat Intelligence feeds that are being provided by commercial vendors, usually under a subscription service such as FireEye, McAfee, Symantec, etc.
- ***Information sharing organizations;*** is a trusted community that actively collaborates to identify and disseminate information about cybersecurity threats.
- ***Dark web;*** is most often associated with illegal activities, it can also be a great source of Threat Intelligence for security researchers.

Responsible Disclosure Programs

What is Responsible Disclosure Program?

Responsible Disclosure Program; is a term used to describe the *ethical practice* where a security researcher is going to disclose information about a vulnerability in a software, hardware, or online service in a confidential manner to the relevant company who created the product or service.

Lifecycle of Responsible Disclosure



What is Bug Bounty Program?

Bug Bounty Program; is an open deal between the organizations and the *cybersecurity researcher to find bugs, security exploits, and other vulnerabilities* in the organization's system or product. In case, *if a researcher found bugs* in their system, he report it to the organization on behalf of which the *organization rewards the person*.



Responsible Disclosure Programs

Top Bug Bounty Programs:

- Google Vulnerability Reward Program.
- Facebook Bug Bounty Program.
- Microsoft Bug Bounty Program.
- Apple Bug Bounty Program.
- Intel Bug Bounty Program.
- Samsung Bug Bounty Program
- Uber Bug Bounty Program.



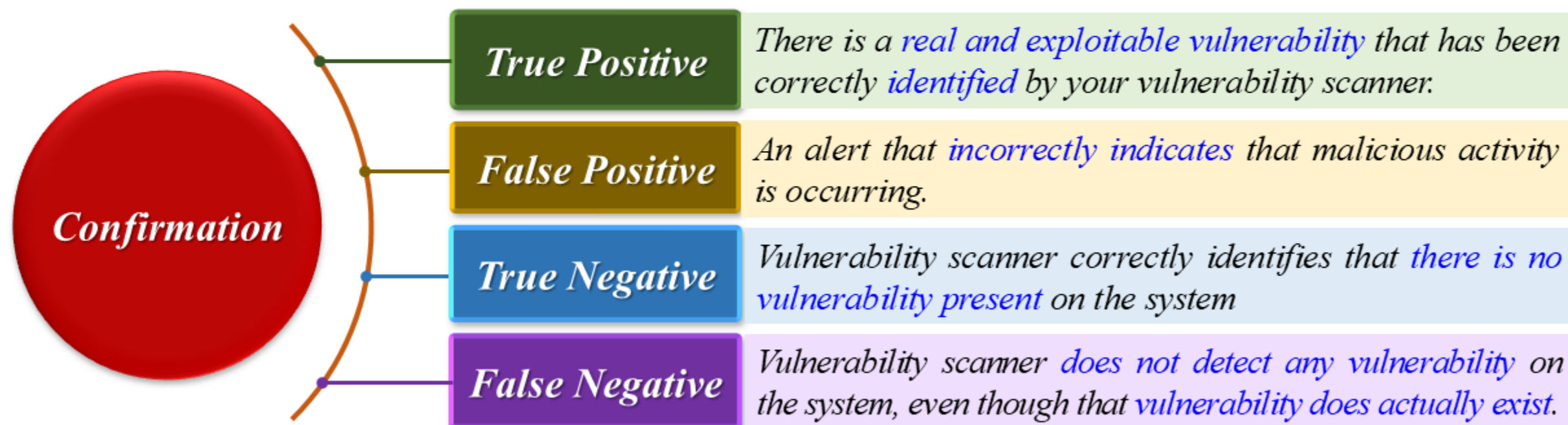

Highest reward
\$605,000


Paid researchers
703


Countries represented
68

Confirmation

Confirmation; is confirming the existence of vulnerabilities.



Prioritizing

Prioritizing; is *ranking the identified vulnerabilities* in the order of their severity and potential impact on the organization. Several factors are going to come into play during this process:

- The ease of exploitation.
- The magnitude of potential damage.
- The importance of the affected system to the organization's operations.

Prioritizing

Cybersecurity professionals often employ a scoring system like the *Common Vulnerability Scoring System (CVSS)*. *CVSS* is going to provide a standardized framework for assessing the severity of a vulnerability, and then *assign a numerical (0-10)* representation of the severity of an information security vulnerability.

Vulnerability scores and categories

SCORE RANGE	SEVERITY CATEGORY
0.0	None
0.1–3.9	Low
4.0–6.9	Medium
7.0–8.9	High
9.0–10.0	Critical

Classification

Classification; involves *categorizing the identified vulnerabilities* based on factors like the *type of threat, the potential impact* on the organization, and the systems or *data that may be affected*.

Using **Common Vulnerabilities and Exposures (CVE)** that contain a large database of every known vulnerability in the world. Each vulnerability will be assigned a specific **CVE** number, and this can be used to look up the relevant information about that vulnerability at the website cve.mitre.org.

Organizational Impact

Organizational impact of the vulnerabilities; The vulnerabilities *impact* of the different data and services that are going to be affected. can be assessed in terms of:

- Confidentiality
- Integrity
- Availability

Exposure Factor

Exposure factor; is an estimation of *the amount of loss that a vulnerability might cause* to the organization.

Risk tolerance

Risk tolerance; is the *level of risk that an organization is willing to accept* in the pursuit of its objectives before action is deemed necessary to mitigate that risk.

What is Vulnerability response and remediation?

Vulnerability response and remediation; is the process of *finding, addressing, and neutralizing security vulnerabilities* within an organization's IT environment. The process of vulnerability response and remediation is going to encompass a range of options:

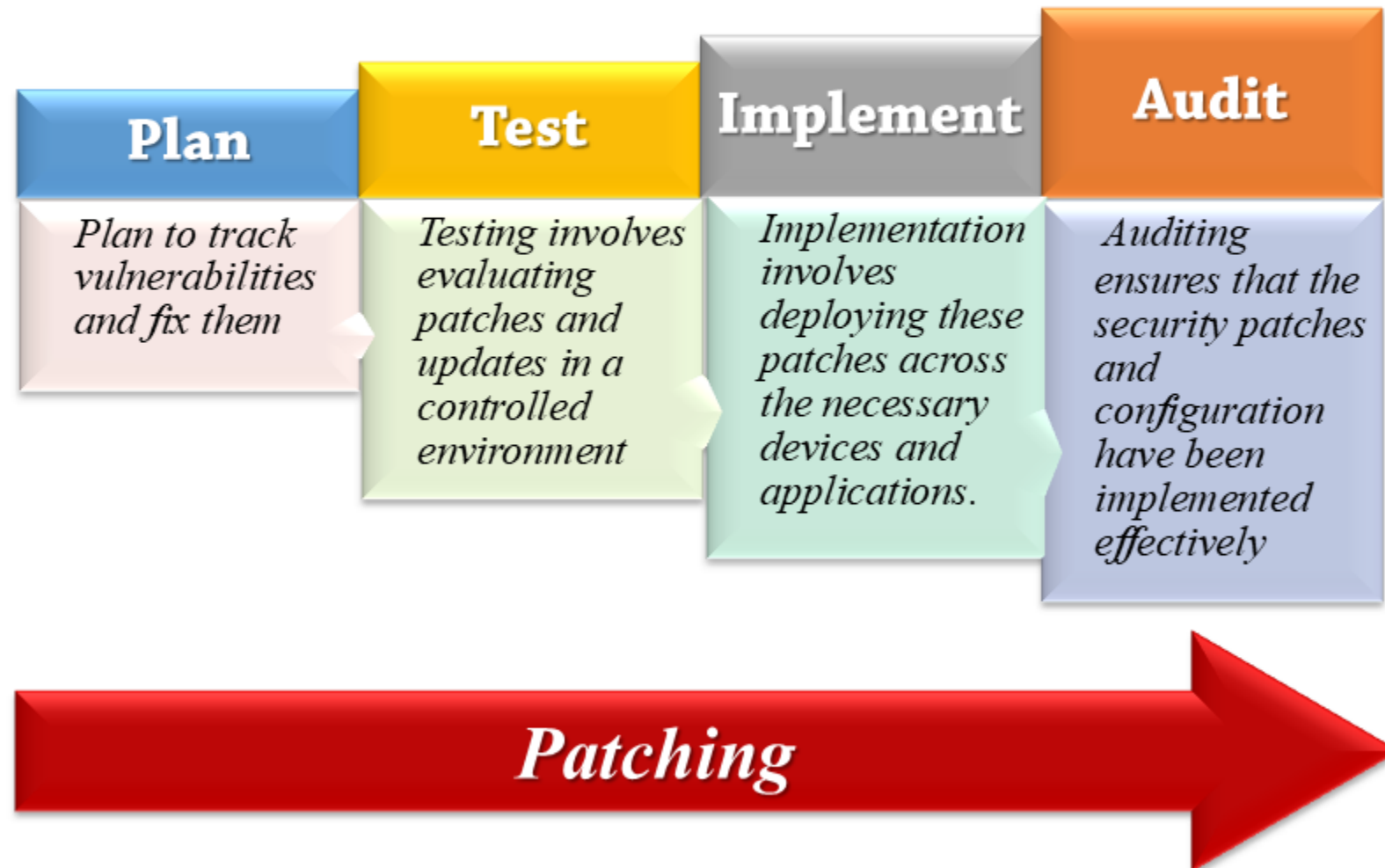
- Patching.
- Insurance.
- Network segmentation.
- Implementing compensating controls.
- Granting exceptions and exemptions.

- **Patching;** is the process of *applying updates to software, systems or applications* in order to fix security vulnerabilities or to improve performance.
- **Insurance;** is the process of *purchase an insurance policy* which is going to be a risk management strategy where an organization is going to procure an insurance policy that is designed to *mitigate any financial losses* that could result from a cyber incident like a data breach, network outage, or business interruption.
- **Network segmentation;** involves *dividing a computer network into smaller parts or segments* to improve performance and security by isolating different parts of the network from each other.

➤ **Implementing compensating controls;** are alternative security measures that can be implemented when a *standard security control cannot feasibly or effectively be implemented on a given system.*

➤ **Granting exceptions and exemptions;** An *exception* refers to a situation where a certain security control or policy is going to be temporarily bypassed because the operational business needs it to be.

An *exemption* is an instance where a security control or policy is permanently going to be waived for a specific reason.



What is verify remediation?

Verify Remediation; is the process of *verifying the remediation of certain vulnerability after mitigation.*

This is done by conducting the following:

- Rescan.
- Audit.
- Verification.

Rescan; is acting as double-checking and it *ensures the system is no longer vulnerable* to that specific vulnerability.

When performing the rescan, the following factors are taken into consideration:

- Schedule rescans to be conducted automatically.
- Using a comprehensive scan when conducting rescan.
- Rescan under the same conditions as your initial scan.

Audit; refers to the process of systematically *reviewing logs, configurations, and patches* to ensure that they're aligned with the established security standards and policies that the organization has.

Verification; is the final checkpoint in validating our vulnerability remediation process. Verification is going to involve *testing the system to confirm that the patches and configuration changes have the desired effect*. Penetration testing can be used during the verification process to simulate an attack vector to verify that the vulnerabilities have been properly addressed and remediated

What is Reporting?

Vulnerability Reporting; is the process of *documenting and communicating details about security weaknesses that were identified in systems or software* to the individuals or organizations that are responsible for addressing the issues to be able to ensure that these vulnerabilities are managed discreetly and effectively to prevent exploitation.

It's important that these reports use *clear, concise, and transparent language* to ensure that the vulnerabilities can be well understood by all the key stakeholders. Also need to ensure that *communications and the reports themselves remain confidential* because they contain an exhaustive list of every known vulnerability inside of our enterprise networks.

- **Internal reporting;** involves the *identification, documentation, and communication* of the organization's vulnerabilities *within the organizational structure*.
- **External reporting;** need to *discuss the vulnerabilities outside of the organization structure*. External reporting is usually going to involve discussions with the vendors, the partners, the customers, or the public at large. Ensure that *any sensitive details about the systems and the data they contain are not being disclosed*.

- **Responsible disclosures;** is the art of *disclosing vulnerabilities ethically to the affected stakeholders before making the announcement to the public* at large.
- **Confidentiality;** is *permitting the reports only to authorized stakeholder*. It is a non-negotiable matter because the details included in those reports are basically going to give the attacker everything they need.

