

Cloud Vulnerability Management

4.1 Explain Vulnerability Management Concepts

Description

- In this episode, we will take a look at vulnerability management concepts, tools, and strategies for your cloud environment.

Resources

- <https://www.microsoft.com/en-us/videoplayer/embed/RE4Y1FX?postJsMsg=true>
- <https://aws.amazon.com/inspector/>
- <https://orca.security/platform/vulnerability-management/>
- <https://github.com/zegl/kube-score>
- <https://cve.mitre.org/>

Learning Objectives

- Define Vulnerability Management
- List and describe types of vulnerability management common to cloud environments
- List and describe the steps taken during vulnerability management
- Define CVE and its function in vulnerability management

Notes

- Define Vulnerability Management
 - Discovery, Verification, and Remediation of security vulnerabilities
 - Usually done with a software application
- Vulnerability Management Types
 - Cloud-specific
 - [Defender Vulnerability Management \(https://www.microsoft.com/en-us/videoplayer/embed/RE4Y1FX?postJsMsg=true\)](https://www.microsoft.com/en-us/videoplayer/embed/RE4Y1FX?postJsMsg=true)
 - [Amazon Inspector \(https://aws.amazon.com/inspector/\)](https://aws.amazon.com/inspector/)
 - [Orca Security Vulnerability Management \(https://orca.security/platform/vulnerability-management/\)](https://orca.security/platform/vulnerability-management/)
 - [Kube-Score \(https://github.com/zegl/kube-score\)](https://github.com/zegl/kube-score)
 - Web App Specific
 - Burp Suite Scanner
 - Arachni
 - Nikto
 - Nuclei
 - SQLMap
 - WPScan
 - Do it all
 - Tenable.io
 - Nessus
 - Qualys
 - OpenVAS/Greenbone
- Steps
 - Scanning Scope
 - Identification
 - Assessment
 - Remediation
- Common Vulnerabilities and Exposures(CVE)
 - Developed by [Mitre \(https://cve.mitre.org/\)](https://cve.mitre.org/)