Vulnerability Response (VR) Implementation

Course Description:
This self-paced course provides in-depth knowledge and hands-on practice in configuring and implementing the ServiceNow Vulnerability Response application. Participants will learn the essentials of Vulnerability Response, including the reasons organizations need such solutions, the core concepts, and effective approaches for scalable and repeatable implementation. The course combines technical aspects, foundational processes, and tactical strategies to empower participants in managing the Vulnerability Response process efficiently.

Audience Profile:
This course is ideal for ServiceNow implementers, security operations professionals, IT security analysts, and anyone responsible for managing vulnerabilities or looking to deepen their expertise in ServiceNow's Vulnerability Response.

Prerequisite:
No specific prerequisites are listed, but familiarity with ServiceNow, IT security fundamentals, and security operations terminology is recommended for optimal learning.

Course Objective:
After completing this course, participants will be able to:

- Discuss the ServiceNow Vulnerability Response solution and its capabilities
- Explore vulnerabilities and vulnerable items
- Distinguish between Host, Application, and Container Vulnerability Response
- Discuss Software Bill of Materials (SBOM)
- Configure NVD integration
- Explore ServiceNow Store and Qualys Vulnerability Integration
- Understand the importance of CMDB in Vulnerability Response
- Configure assignment rules, remediation tasks, and target rules
- Manage solution management and exception handling
- Use Vulnerability Workspaces and response actions
- Discuss application penetration testing
- Explore Security Posture Control (SPC)

Table of Contents (TOC):