Activity

The activities below will help prepare you for the end-of-path quiz. Complete the questions for each milestone as you make your way along your learning journey.

You use open source and third-party components in your development projects. Did you know that the average application consists of 106 open source components and contains 23 known vulnerabilities. What risks are in your projects?

Why is the Software Bill of Materials, the inventory of the open source and third party components you use to develop software, ***so*** *important?*

1. (resource 1.a) According to the article on vulnerabilities found in pacemakers, researchers looked at four different vendors and found over _____ vulnerabilities that hackers could exploit from their use of more than _____ third-party libraries.

2. (resource 1.b) In the blog “The Crucial Role of OSS License Compliance”, what are three things an OSS license grants others permission to do?

3. (resource 1.c) Are you aware of how many different libraries are included in your applications by way of dependencies? How might you validate this?
   _____
   _____
   _____

4. (resource 1.d) After completing the online course, *OSS-100 Open Source Software Licenses – What You Need To Know*, you will be able to:
    - Increase your awareness of OSS licensing.
    - Explain why licenses are important to you when using Open Source Software.
    - Identify some of the risks if you are unaware of OSS license requirements.
    - Explain how Sonatype's Nexus Lifecycle can help you

5. (resource 1.e) What is an SBOM? Who needs it most? Is it required by any governing bodies?

Outcome: *You're armed with more information about a Software Bill of Materials, and why an SBOM is **so** important.*

How can you generate a software bill of materials? Sonatype offers free, developer-friendly suite of tools to find and fix open source vulnerabilities. How can you use them today to start building security into your SDLC?

1. (resource 2.a) What is the purpose of Sonatype's free OSS Index?
   _____
   _____
   _____

2. (resource 2.a) Where does the vulnerability information come from that is reported in the OSS Index?
   _____
   _____
   _____

3. As you review resource 5, consider what is the longest amount of time you/your team has spent updating an application due to old dependencies before being able to move forward with new business requirements?

   _____
   _____
   _____

4. (resource 2.a) The free OSS Index has limitations. It is a manual process. Also, it does not:
   -
   -
   -

5. (resource 2.a) The blog post mentioned that If the OSS Index doesn't show vulnerabilities for a particular library, it doesn't mean it's free from **any** vulnerabilities. What **does** that mean?

   _____
   _____
   _____

6. (resource 2.b) Try out the OSS Index. This enables you to search millions of components to find any known, publicly disclosed vulnerabilities across a wide range of ecosystems.
   - In the Search for Components tab, key in *struts-core*, then click **Search**.
   - Click the component **pkg:maven/org.apache.struts/struts-core**.

   How many Critical Vulnerabilities were found?

   _____
   _____

   How many Severe Vulnerabilities were found?

   _____

What would you do next, regarding these issues?

7. (resource 2.b) Scan your projects for open source vulnerabilities, and build security into your development toolchain with native tools and integrations.
    - At the OSS Index page, click **Scan your dependencies** tab.
    - From the list provided, which scan tools do you use?

8. (resource 2.b) Identifying risk during development is critical, but what about the applications you've already built? Run the Nexus Vulnerability scanner on any existing or legacy applications to generate a complete Software Bill of Materials (SBOM)
    - Click **Try the Nexus Vulnerability Scanner for free.**
    - Scan the sample application provided, or your own application, by performing one of the following:
        - Download the scanner https://www.sonatype.com/appscan
        - Scan your application online via file upload. https://www.sonatype.com/appscan-upload

9. (resource 2.b) What does the scanner tell you about the scanned application?
    - What are some ways to overcome those issues?

Learn more about Vulnerability Scanner by reviewing the guide.
Read the Guide: http://cdn2.hubspot.net/hubfs/1958393/eBooks/AHC_Guide.pdf
(For further details, review the FAQs:
https://support.sonatype.com/hc/en-us/articles/213463928-Nexus-Vulnerability-Scanner-FAQ)

Outcome: *You've manually scanned your applications using the free tools available. That's a great start into building security into your SDLC. You've manually generated a software bill of materials, and you've identified some vulnerabilities. You're also aware of the limitations that come with using the free, manual tools. Move on to milestone 3 to learn how to automate and overcome those limitations.*

In this final trail of your learning path, explore the Nexus platform. When you're ready for precise data and remediation advice from the experts via an automated process, check out the Nexus Platform.

1. (resource 3.a) What is the Nexus Platform?

2. (resource 3.b) Select all that apply: Nexus Firewall:
   a. Ensures that developers are selecting only the highest quality open source components
   b. Lets you take in good components, and leave the bad, by quarantining non-compliant components at the door and enforcing open source policies during proxy.

c. Automated security policies prevent development teams from using non-compliant components, saving time and money across teams. This enables you to stop defective code at the start.

3. (resource 3.c) What are 3 types of policies (based on application type or organization) that are contextually enforced across every stage of the SDLC?

4. (resource 3.d) True or False: While Lifecycle indicates vulnerabilities found during the development process, Auditor indicates risk found in production applications.

5. (resource 3.e) Use the flowchart to determine whether your development team would benefit from Nexus Lifecycle or Nexus Auditor (or both).

6. (resource 3.f) Sonatype's Nexus Platform provides universal support for all of your favorite languages and packages. Which of those do you use most often?

7. (resource 3.g) Sonatype provides data with virtually no false-positives and no false-negatives. Check out our guide on Vulnerability Data to find out how.

    - From which sources does Sonatype gather vulnerability data?

    - How does Sonatype eliminate nearly all false positives and false negatives?

    - What data does Sonatype provide?

8. As you reflect on the importance of identifying the risk in the open source and third party software you use in development, consider how you might communicate this to your team by answering the following:
    - What are some things you have learned that might be easiest for your team to implement?
    - What might be most difficult, and why?
    - What are some ways to overcome those issues?
    - How will you celebrate success with your team?

9. ([resource 3.h]) After completing the online course, *IQ Server Foundations*, you'll be able to:
    - Identify risks and vulnerabilities in using open source software and ways to mitigate those risks
    - Articulate the benefits of using Nexus IQ
    - Describe where the developer fits into the Nexus IQ policy process
    - Define what is a policy
    - Recognize when remediation is required

10. (resource 3.i) Check out all of the free offerings available to support you at my.sonatype.com.
    - Collaborate with a community of users, and Sonatype experts.
    - Sign up to receive alerts each time Sonatype's Customer Education team publishes new content.

Outcomes: *You've had a chance to review the Nexus platform. You know how Sonatype provides very precise data and remediation advice from the experts, and automates this process along all stages of your SDLC. You're prepared to advance your stakes in building automated security into your projects.*