EVALUATION CRITERIA CHECKLIST

Considering the large volume of information you need to gather and digest, we have come up with a practical checklist that you can use to evaluate a potential security tool with a step-by-step approach. Use this checklist to compare each vendor and technology to make an optimal selection that meets your requirements.

Ease of Deployment and Use:

1) How easy is it to deploy the tool on a scale of 1 to 10?

2) Is it user-friendly and intuitive, or does it require extensive training to use effectively?

- [x] Yes
- [ ] No

3) How quickly can a user master the tool in total hours?

test

Compatibility:

1) Does the tool work with the technologies, frameworks, and libraries that you use in your applications?

- [ ] Yes
- [ ] No

2) Does the tool integrate with your development and testing workflows?

- [ ] Yes
- [ ] No

3) How easy is it to deploy the tool on a scale of 1 to 10?

- Source code managers
- Development software
- CI/CD
- DevOps tools

Effectiveness:

1) How effective is the tool in detecting vulnerabilities and threats in your applications on a scale of 1 to 10?

2) Is the detection rate high and can the tool identify a range of vulnerabilities, including hidden and unlinked files?

- [x] Yes
- [x] No

False Positives:

1) What is the rate of false positives identified?

test

2) Does the number of false positives significantly slow down remediation?

- [x] Yes
- [ ] No

3) Is there a way to set up rules to minimize the incidence of false positives?

- [ ] Yes
- [ ] No

Reporting:

1) How easy is it to understand and act on the reports generated by the tool on a scale of 1 to 10?

2) Does the tool provide clear and actionable reports and analytics that can help identify trends and prioritize vulnerabilities?

- [ ] Yes
- [ ] No

3) Do the reports have a user-friendly UI?

- [ ] Yes
- [ ] No

4) How much customization can be done with reporting on a scale of 1 to 10?

Support and Training

1) Does the vendor provide adequate support and training resources to help your team get up to speed and use the tool effectively?

- [ ] Yes
- [ ] No

1) Does the number of false positives significantly slow down remediation?

- [ ] Knowledge base/documentation
- [x] Email support
- [x] Phone
- [ ] Chat
- [ ] Custom training workshops
- [ ] Certification program

Team Empowerment:

1) Does the tool support modern development methodologies such as DevSecOps?

- [ ] Yes
- [ ] No

2) Does it encourage collaboration between developers and security teams?

- [ ] Yes
- [ ] No

3) Does it provide detailed and actionable vulnerability reports that can help developers improve code quality?

- [ ] Yes
- [ ] No

Cost:

1) What is the cost of the tool?

1) How does the cost compare to other vendors?

- [ ] Hight
- [ ] Average
- [ ] Low

3) Does the tool fit within your budget and provide good value for money compared to other tools on the market?

- [ ] Yes
- [ ] No

3) Is the above true when you consider the total cost of ownership, including licensing, training, and support costs?

- [ ] Yes
- [ ] No