Kubernetes Penetration Testing

What Is Kubernetes?

Kubernetes is an open-source container orchestration software that enables you to automate many manual processes in the SDLC. Often hosted in a cloud environment, Kubernetes helps with scaling and management of containerized applications. Kubernetes is used for:

- Deploying Clustered Applications
- Pushing Changes to Applications
- Scaling Applications Up or Down
- Monitoring Applications

Kubernetes Penetration Testing in Simple Words

Kubernetes penetration testing is the process of avoding misconfigurations and implementing safeguarding measures and mitigations when deploying Kubernetes. Evaluating the security of Kubernetes pods, nodes, containers, and clusters by simulating attacks empowers you to learn about the configuration settings, network architecture, and security policies of your Kubernetes architecture.

What Nordic Defender Kubernetes Test Offers

At Nordic Defender, we offer Kubernetes penetration testing services to help you identify potential vulnerabilities in your infrastructure and take proactive measures to address them. Using the best Kubernetes testing frameworks and tools, our team of experienced security professionals simulate sophisticated attacks that can find the weaknesses in your Kubernetes environment.

1. Assessment of Your Kubernetes Infrastructure
2. Identification of Security Risks
3. Security Testing
4. Reporting and Remediation

Contact us today to learn more about our Kubernetes penetration testing services and how we can help you safeguard your infrastructure against potential threats.

Contact us to get started!

✉ **sales@nordicdefender.com**

✆ **(+46) 031-108810**

Check our website here
www.NordicDefender.com

NORDIC DEFENDER
Modern Security Solutions Provider

What Nordic Defender Kubernetes Penetration Testing Includes

- Checking the API Gateway Security
- Checking the Kubernetes Clusters for Potential Vulnerabilities
- Checking Security Policies for Implementation Issues
- Checking User Access, Ensuring That Sensitive
- Information Is Not Pushed to Git Repositories
- Checking Policy Enforcer, Ensuring That Docker Files Are Fully Secure
- Ensuring That the Security Best Practices and Benchmarks Are Met