INFOSOFT IT SOLUTIONS

Training | Projects | Placements

Revathi Apartments, Ameerpet, 1st Floor, Opposite Annapurna Block, Info

soft it solutions Software Training& Development 905968394,918254087

KUBERNETES SECURITY TRAINING

1. Introduction to Kubernetes Security

- Overview of Kubernetes architecture
- Understanding security challenges in Kubernetes environments
- Threat models and attack surfaces

2. Authentication and Authorization

- Kubernetes authentication methods (X.509 certificates, service accounts, etc.)
- Role-Based Access Control (RBAC)
  - Roles and Cluster Roles
  - Role Bindings and Cluster Role Bindings
- OpenID Connect (OIDC) and external authentication providers

3. Network Security

- Network policies
  - Understanding Kubernetes network policies
  - Implementing network policies using tools like Calico, Weave, or Cilium
- Service mesh for secure communication (Istio, Linkerd)
- Securing ingress and egress traffic
- DNS security in Kubernetes

4. Pod Security

- Pod Security Policies (PSPs) and their alternatives (Pod Security Admission)
- Securing containers
  - Best practices for container image security
  - Using security context to enforce security controls
  - Seccomp, App Armor, and SELinux profiles
- Running non-root containers
- Limiting resource usage and setting resource quotas

5. Supply Chain Security

- Image scanning (tools like Trivy, Clair)
- Using trusted registries
- Image signing and verification (Cosign, Notary)
- Securing the CI/CD pipeline

6. Data Security

- Secrets management
  - Kubernetes secrets vs. external secret management tools (HashiCorp Vault, AWS Secrets Manager, etc.)
  - Encrypting secrets at rest
- Persistent volume security
  - Encrypting data at rest
  - Access controls for persistent volumes

7. Security Monitoring and Logging

- Audit logging
  - Kubernetes audit logging
  - Centralized logging solutions (ELK/EFK stack, Fluentd, Fluent Bit)
- Monitoring and alerting
  - Prometheus and Grafana
  - Security monitoring tools (Falco, Sysdig, Aqua Security)
- Intrusion detection systems (IDS) for Kubernetes

8. Compliance and Governance

- Ensuring compliance with regulations (GDPR, HIPAA, PCI-DSS)
- Policy enforcement
  - Open Policy Agent (OPA) and Gatekeeper
  - Kyverno for policy enforcement
- Managing cluster security posture

9. Incident Response and Forensics

- Incident response planning
- Tools for incident response (Kube ctl, K9s, etc.)
- Forensic analysis in Kubernetes
- Backup and disaster recovery strategies

<u>ADVANCE TOPICS;-</u>

1. Advanced Authentication and Authorization

- Deep dive into Kubernetes authentication mechanisms
- Advanced RBAC configurations and best practices
- Integrating external authentication providers (LDAP, SAML, OAuth)
- Implementing OIDC for federated authentication

2. Advanced Network Security

- Comprehensive network policy management
  - Advanced network policy use cases and patterns
- Implementing and managing a service mesh for security (Istio, Linkerd)
- Securing multi-cluster communication
- Advanced DNS security techniques
-

3. Advanced Pod Security

- Detailed configuration of Pod Security Admission
- Advanced container runtime security
    - Seccomp, AppArmor, and SELinux deep dive
    - Custom security profiles and policies
- Best practices for hardening container images
- Advanced use of init containers for security

4. Advanced Supply Chain Security

- Implementing secure CI/CD pipelines
- Advanced image scanning and vulnerability management
- Image signing with Cosign, Notary, and verifying image signatures
- Managing and mitigating supply chain attacks

5. Data Security and Encryption

- Advanced secrets management
    - Integrating external secret management solutions (Hashi Corp Vault, AWS Secrets Manager, etc.)
- Implementing encryption at rest and in transit
- Advanced persistent volume security
    - Custom encryption configurations
    - Access control mechanisms for storage
-

6. Monitoring, Logging, and Incident Response

- Advanced audit logging configurations and use cases
- Comprehensive monitoring strategies
    - Custom metrics and alerts with Prometheus and Grafana
    - Using Falco, Sysdig, and other security monitoring tools
- Building an incident response playbook
- Advanced forensics techniques in Kubernetes

7. Policy Enforcement and Governance

- Advanced policy enforcement with OPA and Gatekeeper
- Deep dive into Kyverno for policy automation
- Implementing and managing compliance (GDPR, HIPAA, PCI-DSS) at scale
- Governance models for large-scale Kubernetes deployments

8. Multi-Tenancy and Cluster Hardening

- Advanced multi-tenancy strategies
    - Namespaces, network segmentation, and RBAC configurations
- Securing Kubernetes operators and custom controllers
- Hardening Kubernetes components (API server, etcd, kubelet)
- Securing managed Kubernetes services (GKE, EKS, AKS) with custom configurations

9. Zero-Trust Security Model

- Implementing zero-trust principles in Kubernetes
- Advanced identity and access management
- Network segmentation and micro-segmentation strategies
- Continuous monitoring and compliance enforcement

10. Emerging Threats and Advanced Defense Mechanisms

- Identifying and mitigating emerging threats
- Advanced techniques for defense in depth
- Machine learning and AI-driven security approaches
- Future trends in Kubernetes security