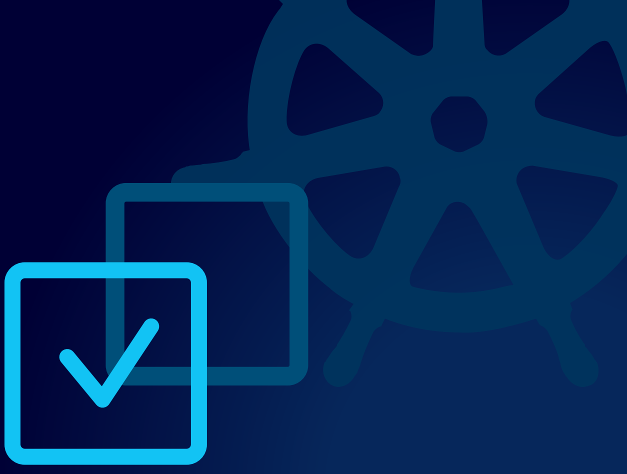
XM Cyber

Kubernetes Best Practices

Security Checklist



In recent years, Kubernetes use by development teams has grown significantly, given the ease and flexibility it provides for managing and deploying applications. But as critical as it is for the management of applications, it opens many new security issues that can be exploited by attackers. And misconfigurations are an even greater challenge; Since Kubernetes is highly customizable, tweaks to various configuration options can affect application security unintentionally.

To help reduce risks, we present this succinct Kubernetes Security Best Practices Checklist. Use it to keep your clusters safer and efficiently reduce risk.

□ Implement Role-Based Access Control (RBAC):

- Define roles and associated permissions for users and service accounts within your Kubernetes cluster.
- Regularly review and update RBAC policies to ensure least privilege access.
- Conduct regular audits to ensure RBAC policies are being followed.

□ Use Third-Party Authentication for API Server:

- Integrate your Kubernetes API server with a third-party authentication provider.
- Implement multi-factor authentication for increased security.
- Regularly update authentication configurations and maintain secure communication between the API server and authentication provider.

□ Isolate Kubernetes Nodes:

- Make sure K8 nodes are isolated.
- Deploy network segmentation to isolate nodes from each other.
- Regularly monitor and review node isolation configurations.

□ **Monitor Network Traffic to Limit Communications:**

- Utilize Kubernetes Network Policies to control inbound and outbound network traffic between pods.
- Implement network monitoring tools to identify and block abnormal network behavior.
- Regularly review and update network policies based on monitoring results.

□ **Use Process Whitelisting:**

- Implement process whitelisting solutions to allow only approved processes to run within pods.
- Regularly review and update process whitelisting configurations to prevent unauthorized processes.

□ **Turn on Audit Logging:**

- Enable audit logging for Kubernetes API server and system components.
- Regularly review audit logs for suspicious activities and security incidents.
- Implement automated alerts for critical audit log events.

□ **Keep Kubernetes Version Up to Date:**

- Regularly check for and apply security patches and updates for Kubernetes components.
- Follow Kubernetes release notes and security advisories for updates.
- Establish a process for testing updates in a staging environment before applying them to production.

□ **Restrict Access to Kubelets:**

- Secure access to Kubelets by enabling TLS authentication and encryption.
- Implement role-based access control for Kubelet API access.
- Regularly review and update Kubelet access controls.

□ **Keep up with Latest Developments:**

- Stay informed about the latest Kubernetes security best practices and trends.
- Join Kubernetes security community forums and mailing lists for updates.
- Regularly attend security training sessions and webinars.

□ **Consider Not Mounting Service Tokens Unless They Are Needed:**

- Limit the use of service account tokens only to pods that require them.
- Implement secrets management solutions to securely manage and distribute sensitive tokens.
- Regularly review and rotate service account tokens

□ **Understand Attack Paths in Kubernetes:**

- Identify potential attack vectors and entry points to your Kubernetes cluster.
- Conduct threat modeling exercises to assess security risks and vulnerabilities.
- Regularly review and update security controls to mitigate identified attack paths.
- Implement security measures such as network segmentation, isolation, and least privilege access to prevent unauthorized access.
- Stay informed about common attack techniques and tactics used against Kubernetes clusters to proactively defend against potential threats.

Why XM Cyber for Kubernetes

Now security teams can get access to a multitude of techniques to protect Kubernetes clusters. Kubernetes Exposure Management helps security teams protect critical assets running in Kubernetes clusters across public cloud, private cloud, and on-premises infrastructure.By mapping all possible attack paths onto an attack graph, teams can gain context of risk towards critical assets in Kubernetes clusters. And by understanding this context, issues can be accurately prioritized, to focus on remediating the exposures where attack paths converge at choke points. This allows for productive remediation that reduces risk in the most efficient way.

Kubernetes Exposure Management delivers continuous visibility into exposures, risky permissions, and misconfigurations that could allow attackers to breach Kubernetes environments and access valuable data and applications. By extending XM Cyber's industry-leading XM Attack Graph Analysis™ to Kubernetes, organizations can now see risks and intelligently prioritize remediation based on potential impact to critical assets.

XM Cyber