SERVICE BRIEF

KUBERNETES SECURITY ASSESSMENT

EVALUATE THE SECURITY POSTURE OF YOUR KUBERNETES DEPLOYMENT

Organisations are rapidly adapting container technologies, devOps and transforming their IT services to microservice architectures. The common denominator in all of this is Kubernetes, the orchestration engine that enables organisations to automate deployments, scale, and manage containerised applications.

However, Kubernetes deployments are often complex, large and unfortunately insecure by default. This means that the engineers responsible for deploying the Kubernetes platform need full visibility into the potential attack vectors and weaknesses of the platform.

OUR APPROACH

mnemonic's Kubernetes security assessment helps identify technical risks associated with your Kubernetes deployment. Whether your organisation has just started containerising services, or is already a devOps team with a large scaled deployment, or somewhere in between, our penetration testers and container security consultants can help identify security issues in your deployment. We also help you understand the potential impact a compromised Kubernetes platform can have for the organisation.

Our assessments provide detection of known vulnerabilities, weak security configuration and policy drifts in combination with actionable advice. This empowers your organisation to **conduct quick**, **structured** and **prioritised remediation**. Additionally, deployments can always be tested and reviewed against common baselines such as Center of Internet Security's (CIS) Kubernetes Benchmark, ensuring a measurable security baseline for your deployments which can be continuously verified.

Our expert Kubernetes security consultants are equipped with the knowledge and resources to evaluate your deployment in any of the major public cloud providers, including **Microsoft Azure**, **Amazon Web Services**, and **Google Cloud Platform**. We can also evaluate deployments on bare metal, on-premise or private cloud platforms. We know that when it comes to Kubernetes security, one size definitely does not fit all, and consequently we always adapt our testing methods on a case-by-case basis.

SERVICE BENEFITS

Understand the attack model for Kubernetes
Understanding how attackers think of Kubernetes is key to understanding how to defend it. Our attack modelling ensures that testing is prioritised where security is most relevant to you, and that your organisation understands why and how our recommendation are relevant for your deployment.

Gain insight into effective hardening of Kubernetes clusters
Identify deviations from recommended security best practices for Kubernetes and map findings against industry baselines like Center of Internet Security Kubernetes Benchmark. We provide advice on how to harden the security configuration and make sure it not only becomes secure, but stays that way.

Identify high severity issues
Identify issues that are critical to cluster security. Find weak Pod Security Policies, poor network segregation and hardening, secret management issues, and a lot more

Maintain compliance
Stay compliant with security regulations, best practice and industry standards, while ensuring functional requirements of the environment are still maintained.

A TRUSTED ADVISOR IN CLOUD SECURITY

Our Kubernetes and container security experts understand that every organisation has different business drivers for their Kubernetes adoption, and can translate the implications of each driver into concrete technical recommendations that work for the business.

contact@mnemonic.io
+47 23 20 47 00
www.mnemonic.io

May 2022