iterasec

Container Security Audit for Government IT Center

Client:
Government IT Center (EU Country)

Industry:
Government / Public Sector

Company Size:
Large-scale National Infrastructure Provider

Services Used:
On-site Container Infrastructure Audit (OpenShift)

Client

The client is a prominent Government IT Center responsible for various critical IT developments supporting national infrastructure across multiple governmental departments. Handling highly sensitive information and providing essential IT services, the center ensures the efficient and secure operation of national government infrastructure.

Background

In an engagement with a Government IT Center (EU Country), Iterasec conducted an onsite, comprehensive security audit of their OpenShift container platform, which underpins critical national infrastructure operations. Given the sensitivity and scale of the systems, identifying and mitigating potential vulnerabilities was paramount to ensuring operational resilience, regulatory compliance, and protection against advanced threat actors.

The Challenge

The Government IT Center needed an in-depth and complete security audit of their OpenShift container infrastructure. Key requirements included:

- **Specialized Expertise:**
  They sought cybersecurity specialists with proven experience and in-depth knowledge of OpenShift environments.
- **On-site Audit Requirement:**
  Due to the sensitivity of the information, the security assessment had to be performed strictly onsite, using the client's secured workstations.
- **Detailed Assessment:**
  They required an exhaustive evaluation to uncover potential vulnerabilities and configuration weaknesses that could compromise national security.
- **Lack of Segregation of Duties (High Risk):**
  Administrative privileges were overly concentrated among few accounts, combining operational, deployment, and security roles without separation.
- **Absence of Multi-Factor Authentication (High Risk):**
  Administrator access relied solely on passwords, exposing the environment to phishing and credential theft risks.
- **Vulnerable ArgoCD Version Deployed (Medium Risk):**
  An outdated ArgoCD version with known vulnerabilities was in use, risking remote code execution and token leaks.
- **Privileged Containers Permitted (Medium Risk):**
  Pods were allowed to run with privileged container status without restrictions, increasing host-level compromise risks.
- **Excessive Authorization Privileges (Medium Risk):**
  User and service accounts had permissions beyond necessity, often with cluster-admin rights, amplifying post-compromise impact.

The Solution

Iterasec assigned one of its lead penetration testers — a recognized expert in container security and OpenShift — to conduct the comprehensive onsite audit. The approach included:

- **Conducted on-site security testing**
  strictly from the client's secured workstations to comply with internal protocols.
- **Reviewed OpenShift infrastructure**
  including access controls, workload configurations, network policies, API server settings, and GitOps practices (ArgoCD).
- **Identified critical vulnerabilities**
  such as lack of segregation of duties, absence of MFA, outdated ArgoCD deployment, and permissive container settings.
- **Detected additional technical risks**
  including default-permitted privileged containers, unsecured volume mounts exposing sensitive data, excessively privileged service account tokens, unnecessary cluster-admin roles, and insufficient logging configurations.
- **Developed an actionable remediation plan**
  based on CIS Kubernetes Benchmarks and OpenShift best practices to address identified vulnerabilities and strengthen the environment.

The Outcome

Following Iterasec recommendations, the Government IT Center achieved major improvements:

- **Role-Based Access Controls Enforced:**
  Administrative and service accounts were restructured based on strict segregation of duties and least privilege principles.
- **Multi-Factor Authentication Implemented:**
  MFA was made mandatory for all administrative operations, significantly strengthening access security.
- **ArgoCD Instances Upgraded:**
  Vulnerable versions were replaced with secured releases, eliminating critical exploitation pathways.
- **Privileged Containers Restricted:**
  Container deployment policies were hardened, reducing the risks of host-level compromises.
- **Logging and Monitoring Enhanced:**
  New solutions were deployed to improve visibility into system activities and support forensic investigations.
- **Enhanced Operational Confidence:**
  Provided the client with actionable insights and guidelines, reinforcing their confidence in the security of their containerized environments.
- **Compliance and Best Practices Alignment:**
  Enabled the Government IT Center to align their OpenShift environment with industry best practices and compliance requirements, crucial for national security operations.

Conclusion

This audit demonstrated that even highly secured environments managing national infrastructure must proactively identify and mitigate evolving container security threats. Each technical finding highlighted the interconnected risks across identity management, runtime security, and infrastructure configuration. Through targeted remediation, the Government IT Center substantially elevated its security posture, ensuring greater resilience against sophisticated adversaries while maintaining compliance with national cybersecurity mandates.