JOSE NOGUEIRA DA COSTA NETO
11/04/2024 09:01

ROBERT ARMANDO ROSA
13/05/2024 11:06

ETP - ESTUDO TÉCNICO PRELIMINAR

Processo Administrativo n.º XX/2024

Contratação do Curso de Segurança Kubernetes

Porto Velho, 05 de abril de 2024

INTRODUÇÃO

Nos últimos anos, a computação em contêineres tem revolucionado a forma como as aplicações são desenvolvidas, implantadas e gerenciadas. Nesse cenário, o Kubernetes emergiu como a principal plataforma de orquestração, oferecendo recursos avançados para gerenciar aplicativos baseados em contêineres em ambientes de produção em larga escala.

Com o aumento da adoção do Kubernetes para orquestração de contêineres em ambientes de produção, a segurança dos clusters Kubernetes tornou-se uma preocupação central para empresas e desenvolvedores. Embora o Kubernetes ofereça uma série de recursos de segurança, a configuração incorreta e as práticas inadequadas podem expor os clusters a uma série de vulnerabilidades. Tais vulnerabilidades, se não tratadas, podem ser exploradas por um atacante e prejudicar a disponibilidade e/ou consistência dos dados, sendo foco central de mitigações realizadas pelas pessoas que atuam em prol da segurança.

1. DEFINIÇÃO E ESPECIFICAÇÃO DAS NECESSIDADES E REQUISITOS

1.1. Da necessidade em sentido amplo

A necessidade de contratação de treinamento/curso em Segurança em Cluster Kubernetes para os profissionais da área de tecnologia do TRT14 surge pelos desafios existentes em segurança de clusters kubernetes e também da necessidade de implementação das melhores práticas:

Desafios:

Gestão de Identidade e Acesso: O controle de acesso granular é fundamental para garantir que apenas usuários autorizados possam interagir com os recursos do cluster. Gerenciar identidades e permissões de forma eficaz pode ser complexo, especialmente em ambientes com várias equipes e aplicativos.

Configuração Incorreta: Configurações inadequadas, como credenciais expostas, serviços não seguros e permissões excessivas, podem levar a violações de segurança. A

falta de auditoria e monitoramento adequados pode tornar ainda mais difícil detectar e remediar essas vulnerabilidades.

Exploração de Vulnerabilidades de Contêineres: Contêineres mal configurados ou com software desatualizado podem ser explorados por invasores para obter acesso não autorizado ao cluster ou para executar código malicioso.

Ataques de Rede: Clusters Kubernetes são frequentemente expostos à Internet, tornando-os alvos potenciais para ataques de rede, como ataques DDoS, sniffing de pacotes e interceptação de comunicação não criptografada.

Exemplos de Melhores Práticas:

Princípio do Menor Privilégio: Configure permissões e acessos de forma mínima e específica. Use roles e role bindings do Kubernetes para conceder acesso apenas aos recursos necessários para cada usuário ou serviço.

Segurança de Imagem de Contêiner: Utilize imagens de contêineres confiáveis e mantenha-as atualizadas. Escaneie regularmente as imagens em busca de vulnerabilidades conhecidas e aplique patches ou atualizações conforme necessário.

Rede Segura: Utilize Network Policies para controlar o tráfego de rede entre os pods e implante medidas de segurança de rede, como firewalls e gateways de API, para proteger o tráfego de entrada e saída do cluster.

Monitoramento e Auditoria: Implemente ferramentas de monitoramento e auditoria para rastrear atividades suspeitas e identificar anomalias de segurança. Isso inclui monitoramento de logs, métricas de desempenho e alertas de segurança em tempo real.

Gerenciamento de Chaves e Credenciais: Armazene e gerencie chaves de criptografia e credenciais de forma segura, utilizando soluções como Kubernetes Secrets e serviços de gestão de chaves externas.

Atualizações e Patches: Mantenha o software do Kubernetes e dos componentes do cluster atualizados com as últimas correções de segurança. Implemente um processo de

gerenciamento de patches regular para garantir que as vulnerabilidades conhecidas sejam corrigidas rapidamente.

Em resumo, a segurança de clusters Kubernetes é um aspecto crítico da operação de ambientes de contêineres em escala. Adotar práticas de segurança robustas desde o início do ciclo de vida do cluster é essencial para proteger os aplicativos e os dados dos usuários contra ameaças cibernéticas. Ao seguir as melhores práticas de segurança e manter-se atualizado sobre as últimas ameaças e soluções de segurança, as organizações podem mitigar os riscos e garantir a integridade e disponibilidade de seus clusters Kubernetes. Então, o treinamento em Segurança de Cluster Kubernetes é necessário para ser ter uma equipe capacitada/qualificada para atuar com expertise diante dos desafios existentes, aplicando as melhores práticas, buscando de forma contínua pela eficiência e inovação, e pelo compromisso do TRT14 em fornecer o melhor serviço possível ao público e em investir no desenvolvimento de seus profissionais.

1.2. Identificação das necessidades (requisitos) de negócio

Ao considerar a importância da Segurança de Clusters Kubernetes para os profissionais da área de tecnologia do TRT14, é crucial identificar claramente as necessidades de negócio que essa capacitação deve atender. Abaixo estão as expectativas e os resultados desejados que o treinamento em Segurança de Clusters Kubernetes deve proporcionar:

Capacitação Avançada em Segurança Kubernetes: O treinamento deve oferecer uma compreensão profunda e prática dos conceitos, técnicas e ferramentas de segurança específicas para ambientes Kubernetes. Os participantes devem ser capazes de implementar e gerenciar medidas de segurança avançadas em clusters Kubernetes em cenários reais de negócios.

Tomada de Decisão Aprimorada em Segurança de Clusters: Com a capacitação, espera-se que os profissionais possam analisar ameaças de segurança, identificar vulnerabilidades e tomar decisões mais informadas para proteger os clusters Kubernetes contra ataques e violações de segurança.

Otimização da Segurança dos Processos Internos: O treinamento deve capacitar os profissionais a identificar e implementar práticas e políticas de segurança que otimizem a proteção dos clusters Kubernetes e dos aplicativos neles hospedados, garantindo a integridade e a disponibilidade dos serviços.

I**novação em Segurança Kubernetes:** Os participantes devem ser incentivados a pensar de forma inovadora e a desenvolver novas soluções e abordagens para proteger clusters Kubernetes contra ameaças emergentes e evasivas.

Integração de Práticas de Segurança com Sistemas Existentes: O treinamento deve abordar como as práticas de segurança em clusters Kubernetes podem ser integradas aos sistemas e infraestruturas existentes no TRT14, garantindo uma segurança holística e uma transição suave para ambientes Kubernetes.

Ética e Conformidade em Segurança Kubernetes: Dada a natureza sensível dos dados e das operações do TRT14, é essencial que o treinamento aborde aspectos éticos, de conformidade e legais relacionados à implementação e operação seguras de clusters Kubernetes.

Colaboração e Trabalho em Equipe em Segurança Kubernetes: O treinamento deve promover a colaboração entre os participantes, incentivando a troca de conhecimentos, boas práticas e experiências em segurança de clusters Kubernetes. Isso fortalecerá a coesão da equipe e promoverá uma cultura de segurança cibernética colaborativa.

Alinhamento com Objetivos Estratégicos de Segurança: O curso/treinamento em Segurança de Clusters Kubernetes deve estar alinhado com os objetivos estratégicos de segurança do TRT14, garantindo que as competências adquiridas contribuam diretamente para a proteção dos ativos e a mitigação de riscos de segurança cibernética.

Avaliação e Feedback Contínuos: O treinamento deve incluir mecanismos de avaliação e feedback, permitindo que os participantes avaliem seu progresso em termos de implementação e gestão de segurança em clusters Kubernetes e recebam orientação contínua para melhorar.

Flexibilidade e Personalização: Reconhecendo que cada profissional pode ter um nível diferente de familiaridade e experiência em segurança cibernética, o treinamento deve ser flexível e personalizável, atendendo às necessidades individuais dos participantes e oferecendo abordagens adaptáveis para diferentes contextos de segurança.

O Treinamento em Segurança de Clusters Kubernetes deve ser uma experiência completa e prática que capacite os profissionais do TRT14 a protegerem os ambientes Kubernetes de maneira eficaz, ética e alinhada com os objetivos estratégicos de segurança da instituição. Ao abordar essas necessidades e requisitos de negócio, o treinamento proporcionará uma base sólida para a proteção dos ativos e a continuidade dos serviços do TRT14 em um ambiente cada vez mais digital e interconectado.

1.3. Identificação das necessidades (requisitos) tecnológicas

Para garantir que o treinamento em Segurança de Clusters Kubernetes atenda às necessidades do TRT14 e esteja alinhado com os padrões e práticas atuais de Tecnologia da Informação e Comunicação (TIC), é essencial identificar os requisitos tecnológicos associados. Abaixo estão os componentes, capacidades e considerações tecnológicas que o treinamento deve abordar:

Padrões de TIC: O treinamento deve estar alinhado com os padrões de TIC adotados pelo TRT14, garantindo que as práticas e técnicas de segurança em clusters Kubernetes estejam de acordo com as diretrizes e regulamentações da instituição.

Capacidades em Segurança Kubernetes: O curso deve abordar as principais capacidades de segurança em clusters Kubernetes, incluindo autenticação, autorização, controle de acesso, criptografia, monitoramento e detecção de ameaças.

Metodologias e Processos: O treinamento deve incorporar metodologias e processos específicos para segurança em clusters Kubernetes, como a implementação de políticas de segurança, práticas de hardening, e procedimentos de resposta a incidentes.

Ferramentas e Plataformas: O curso deve apresentar e oferecer prática em ferramentas e plataformas específicas para segurança em clusters Kubernetes, como Kubernetes

Security Policies, Network Policies, RBAC (Role-Based Access Control), e ferramentas de monitoramento.

Treinamento em Práticas de Resposta a Incidentes: Os participantes devem ser capacitados com técnicas e procedimentos para identificar, investigar e responder a incidentes de segurança em clusters Kubernetes, garantindo uma resposta eficaz a ameaças em tempo real.

Atualização Contínua e Aprendizado: Dada a natureza em constante evolução das ameaças de segurança, o treinamento deve enfatizar a importância da atualização contínua e fornecer recursos para os profissionais se manterem atualizados sobre as últimas tendências e técnicas em segurança de clusters Kubernetes.

Colaboração e Compartilhamento de Conhecimento: O curso deve promover a colaboração entre os participantes, incentivando o compartilhamento de conhecimento e experiências em segurança de clusters Kubernetes, fortalecendo a capacidade da equipe para enfrentar desafios de segurança de forma colaborativa.

O Treinamento em Segurança de Clusters Kubernetes deve ser uma experiência prática e abrangente, capacitando os profissionais do TRT14 a protegerem efetivamente os ambientes Kubernetes contra ameaças e vulnerabilidades, e garantindo a conformidade com os padrões de segurança e regulamentações relevantes. Ao abordar esses requisitos tecnológicos, o treinamento preparará os profissionais para enfrentar os desafios de segurança cibernética em ambientes de contêineres Kubernetes de maneira eficaz e proativa.

2. PREVISÃO NO PLANO ANUAL DE CONTRATAÇÕES

O curso está previsto na página 42, item Necessidades levantadas para o Plano de Capacitação de TIC 2024, do [PDTIC - Plano Diretor de Tecnologia da Informação e Comunicação 2023-2024 - Ed. 2023-1]

		database and manage performance.			
17	**SEGURANÇA EM CLUSTER KUBERNETES – CKS**	O curso ensina configurar autenticação e autorização no Cluster Kubernetes, revisar configurações de segurança com CIS Benchmark, gerenciar políticas de segurança de rede, gerenciar políticas e restrições o cluster através do Open Policy Agent, melhorar segurança de imagens de Container, detectar ameaças, implementar a imutabilidade de containers e realizar auditoria em tempo de execução no Cluster, restringir o acesso de um contêiner a recursos no cluster, através do AppArmor e Seccom.	Segurança da Informação e Proteção de Dados	Seção de Infraestrutura Computacional	A realizar (2024)

3. ESTIMATIVA DA DEMANDA - QUANTIDADE DE BENS E SERVIÇOS

A contratação de 10 (dez) vagas para o Curso/Treinamento em SEGURANÇA EM CLUSTER KUBERNETES – CKS, uma decisão estratégica baseada em uma análise cuidadosa das necessidades e capacidades do TRT14. A seguir, apresentamos as justificativas para essa quantidade: A escolha de 10 vagas diz respeito além das pessoas vinculadas à SEÇÃO DE INFRAESTRUTURA COMPUTACIONAL, quais sejam: 1 - José Nogueira da Costa Neto (Chefe da Seção de Infraestrutura Computacional), 2 - Roosevelt de Almeida Justo (Assistente 4), 3 - Marcelo Rodrigues de Oliveira (Assistente 4), 4 - José Manoel Júnior (Assistente 4), e 5 - Márcio Ribeiro de Oliveira, também as pessoas que tratam da segurança dos ambientes de containers ou operam sobre estes adicionando novos recursos, como: 6 - Rômulo Valente Ferreira (Coordenador de Infraestrutura e Serviços), 7 - Wainner Brum Caetano (Chefe da Divisão de Segurança da Informação), 8 - Rafael Genovez Idalgo (Assistente 5) , 9 - Josimar Roberto da Silva (Chefe da Seção de Banco de Dados), 10 - Andrus da Silva Sandres (Chefe da Seção de Gerência de Redes de Comunicação).

Em conclusão, a estimativa de demanda para 10 vagas do Curso/Treinamento em SEGURANÇA EM CLUSTER KUBERNETES – CKS é baseada em uma combinação de necessidades estratégicas, históricas e operacionais do TRT14. Esta quantidade garante que o treinamento tenha um impacto significativo na Secretaria de Tecnologia e Informação, promovendo inovação, eficiência e desenvolvimento contínuo.

4. Justificativa da inexigibilidade de licitação

A empresa contratada, Empresa 4Linux Software e Programas Ltda, inscrita sob o CNPJ nº 04.491.152/0001-9, já prestou serviços de treinamento para este Tribunal e para outros órgãos da administração pública direta e indireta, com inexigibilidade de licitação, devido a alta especialização do curso, conforme o documento nº x deste processo. A seguir lista-se alguns casos de estudos/contração de contratação da empresa:

Órgão	Data

MP PA	23/06/2022
PM PA	05/06/2023
TRT5	06/06/2023

5. Descrição do curso

O curso "**SEGURANÇA EM CLUSTER KUBERNETES – CKS",** tem duração de 20 horas**,** que devem ser administradas de 06/05/2024 até 10/05/2024.

Objetivo do curso:

Ensinar aos alunos técnicas para aumentar a segurança em cluster Kubernetes através das melhores práticas.

O curso ensina configurar autenticação e autorização no Cluster Kubernetes, revisar configurações de segurança com CIS Benchmark, gerenciar políticas de segurança de rede, gerenciar políticas e restrições o cluster através do Open Policy Agent, melhorar segurança de imagens de Container, detectar ameaças, implementar a imutabilidade de containers e realizar auditoria em tempo de execução no Cluster, restringir o acesso de um contêiner a recursos no cluster, através do AppArmor e Seccom. Além de conteúdos alinhados com o mercado de trabalho e que são cobrados na certificação Kubernetes Security Specialist (CKS).

Após o curso você estará apto a:

Gerenciar:

- contas de serviço e usuário Role, RoleBinding e ClusterRoleBinding (RBAC) certificados no Cluster
- autorização de clientes externos
- Ingress com certificado TLS
- contextos de segurança
- ConstraintTemplate e Constraint
- políticas Egress e Ingress para bloquear acesso
- políticas a partir de Labels, portas TCP/UDP, Namespaces e de endereço IP
- segurança do Kubernetes Dashboard
- Criar Secret para armazenar chave e certificado
- Revisar configurações de segurança com CIS Benchmark
- Atualizar Cluster Kubernetes
- Verificar binários da plataforma
- Instalar o Open Policy Agent
- Testar regras através do Rego Playground
- Melhorar segurança de imagens
- Realizar varredura de vulnerabilidade de imagem
- Fazer análise estática com Kubesec/OPA Conftest
- Imutabilidade de containers em tempo de execução
- Detectar ameaças no Cluster Kubernetes
- Auditoria no Cluster Kubernetes

Restringir:

- o acesso de um contêiner a recursos com AppArmor o acesso de Pods com AppArmor
- Syscalls de um Contêiner com Seccom
- Syscalls de Pods com Seccom
- Utilizar e proteger secrets no kubernetes
- Instalar e configurar Containerd
- Sandbox em container Runtime
- Instalar e configurar Gvisor e Kata Containers
- Executar Pods através de RuntimeClass

Conteúdo Programático:

- Configurar Autenticação e Autorização no Cluster Kubernetes
- Gerenciar contas de serviço e usuário
- Gerenciar Role, RoleBinding e ClusterRoleBinding
- RBAC - Role-Based Access Control
- Gerenciar certificados no Cluster
- Gerenciar autorização de clientes externos
- Criar Secret para armazenar chave e certificado
- Gerenciar Ingress com certificado TLS
- Network Policies
- Gerenciar políticas Egress e Ingress para bloquear acesso
- Gerenciar políticas a partir de Labels
- Gerenciar políticas a partir de portas TCP/UDP
- Gerenciar políticas a partir de Namespaces
- Gerenciar políticas a partir de endereço IP
- Restringindo o acesso à API de metadados em nuvem
- Cluster Setup
- Gerenciar segurança do Kubernetes Dashboard
- Revisar configurações de segurança com CIS Benchmark
- Atualizar Cluster Kubernetes
- Verificar binários da plataforma
- Contextos de segurança e Open Policy Agent
- Gerenciar contextos de segurança
- Introdução e instalação do Open Policy Agent
- Gerenciar ConstraintTemplate e Constraint
- Testar regras através do Rego Playground
- Segurança da cadeia de suprimentos
- Melhorar segurança de imagens
- Varredura de vulnerabilidade de imagem

6. Estimativa do Valor da Contratação

Descrição	Quantidade	Valor Unitário (R$)	Valor Total (R$)
SEGURANÇA EM CLUSTER KUBERNETES –	10	1.742,40	17.424,00

CKS			

7. Justificativa para o parcelamento ou não da solução

Trata-se de contratação de uma única prestação do serviço, não se aplicando o parcelamento da solução, conforme descrito na proposta comercial, página 4:

> "***A partir desse entendimento o nosso pagamento deve ser realizado em até 30 (trinta) dias, contados do aceite da presente proposta e envio da nota de empenho/pedido, por meio de depósito em conta ou boleto bancário e após apresentação de Nota Fiscal."***

8. Contratações Correlatas e/ou Interdependentes

Não se aplica.

9. Área requisitante/responsáveis

Área Requisitante	Responsável
Seção de Infraestrutura Computacional	JOSÉ NOGUEIRA DA COSTA NETO