PODER JUDICIÁRIO
JUSTIÇA DO TRABALHO
TRIBUNAL REGIONAL DO TRABALHO DA 14ª REGIÃO
SECRETARIA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO

DOCUMENTO DE OFICIALIZAÇÃO DE DEMANDA - DOD

1. IDENTIFICAÇÃO

Demanda		Treinamento: Offensive Security - PEN-300 - Evasion Techniques and Breaching Defenses - Advanced Pentesting Training
Data de proposição		Fevereiro de 2022
Demandante	Unidade administrativa	Núcleo de Infraestrutura e Comunicações - SETIC
	Responsável	Marcus Vinícius Alencar Terra
	E-mail	marcus.terra@trt14.jus.br

2. NECESSIDADE DA SOLICITAÇÃO E EXPLICITAÇÃO DA MOTIVAÇÃO

Em um ataque cibernético de grandes proporções, como os que ocorreram nos últimos anos ao judiciário brasileiro, os hackers geralmente usam técnicas de invasão avançadas e encadeadas, isto é, exploram vulnerabilidades que isoladamente podem não representar um alto risco para a administração pública, porém, agregadas permitem a obtenção de acesso permanente ao sistema, geralmente com a intenção de exfiltrar informações valiosas e/ou criptografar todos os ativos possíveis, possibilitando assim o “sequestro de dados” mediante a exigência de vultuosas quantias em dinheiro em troca da chave de descriptografia [caracterizando assim o ransomware].

E nesse processo de encadear vulnerabilidades, quase sempre é necessário burlar as defesas de perímetro, sistemas de antivírus e controles de acesso.

Portanto, imperativo se faz que a equipe de segurança da informação esteja capacitada a prever, identificar e monitorar possíveis portas de entrada através do domínio no que tange às técnicas de invasão e violação de defesas, através da qual será possível a criação de alertas e/ou armadilhas de defesa em nossa ferramenta de SIEM (Gerenciamento e Correlação de Eventos de Segurança) que serão baseados na análise do comportamento rotineiro do sistema.

Nesse contexto, faz-se portanto, oportuno, necessário e indispensável o desenvolvimento da equipe para entender essa cadeia de ataque para que possa atuar na implementação de controles rígidos de segurança cibernética, bem como tratar eventuais incidentes de segurança e trabalhar de forma preventiva na mitigação de riscos, evitando o vazamento de dados ou impactos negativos à Infraestrutura e Rede da Justiça do Trabalho.

Importante destacar a possibilidade de compartilhamento do conhecimento adquirido através da promoção de eventos e ações de treinamento/conscientização interna no âmbito da SETIC e demais unidades do TRT14, quais sejam necessários para a manutenção e solidificação das barreiras de segurança dentro da administração. Uma vez capacitado, a possibilidade de transmissão de conhecimento dentro do tribunal será uma realidade possível, aumentando ainda mais o nível de segurança do órgão através da disseminação entre todos os envolvidos no processo.

A solicitação do treinamento também é fundamentada em recente exigência do CNJ em sua resolução Nº 396 de 07/06/2021 em seu artigo 28, parágrafo III:

> **III - promover treinamento contínuo e certificação internacional dos profissionais diretamente envolvidos na área de segurança cibernética**

3. QUANTIDADE DE AQUISIÇÃO OU SERVIÇO A SER CONTRATADO

Treinamento oficial Offensive Security - **PEN-300 - Evasion Techniques and Breaching Defenses - Advanced Pentesting Training**, para o servidor WAINNER BRUM CAETANO.

4. MOTIVAÇÃO DA ESCOLHA DA EMPRESA / INSTRUTOR

A Acaditi é uma empresa especializada em capacitações e consultoria em TI, atualmente é composta pela AcadiTI, Acadi Security e Acadi Training.

A Acaditi é a **única representante da Offensive Security na América Latina**, conforme https://www.offensive-security.com/offsec-for-orgs/training-partners/, em tradução livre:

> "ACADI-TI (BRASIL)
>
> A ACADI-TI é uma empresa altamente especializada em treinamento e consultoria em Tecnologia e Segurança da Informação, voltada para empresas de diversos portes e mercados, bem como profissionais que buscam desenvolver suas competências técnicas. Sua principal missão é transformar vidas por meio da educação e ajudar seus clientes a se manterem seguros no mundo digital. ”

No aspecto administrativo e operacional, face às dificuldades de datas para realização do treinamento, decorrentes da especificidade do curso, vale ressaltar ainda que a empresa oferece **o curso em turma aberta e em data a ser escolhida pelo servidor dentro de 1 ano, além dos seguintes materiais de apoio**:

- Mais de 19 horas de vídeo
- Guia do curso em PDF de 700 páginas
- Fóruns de alunos ativos
- Acesso ao ambiente de laboratório virtual (60 dias)
- Acesso 24 horas a instrutores.

5. ALINHAMENTO ESTRATÉGICO

Plano	Objetivo estratégico
PDTIC 2021-2022	OEC8 - Aprimorar a Segurança da Informação e a Gestão de Dados
Resolução CNJ Nº 325/2020	Fortalecimento da Estratégia Nacional de TIC e Proteção de Dados.
Resolução Administrativa Nº 61/2021	Aprimorar a gestão, governança de TIC e a proteção de dados
Resolução CNJ nº 370/2021	Aprimorar a Segurança da Informação e a Gestão de Dados
Resolução CNJ Nº 396/2021	*III – promover treinamento contínuo e certificação internacional dos profissionais diretamente envolvidos na área de segurança cibernética*

6. RESULTADOS ESPERADOS

Tipo de Resultado	Sim	Não	Detalhamento
Melhora da prestação jurisdicional	X		Confidencialidade, Integridade e Disponibilidade das informações corporativas.
Ganho de produtividade	X		A experiência e o conhecimento técnico adquiridos no treinamento naturalmente tornará o trabalho técnico da seção de segurança da informação mais efetivo.
Redução de esforço	X		Conhecer a cadeia de ataque permite criar monitoramentos e armadilhas no SIEM para detectar possíveis ataques. Reduzindo o esforço de analisar os logs sem o conhecimento de como um ataque funciona e como os eventos são relacionados.
Redução de custo	X		Com as centenas de soluções de segurança no mercado, o conhecimento adquirido no curso certamente ajudará a escolher a melhor opção custo/benefício em uma eventual contratação de tais soluções.

Melhoria de controle	X		Contribuirá na implementação de controles internos fundamentados na gestão de riscos da segurança da informação.
Redução de riscos	X		Permite a aplicação de salvaguardas e contramedidas necessárias para mitigar o risco de uma invasão à rede do Tribunal
Determinação legal	X		Resolução CNJ Nº 396 de 07/06/2021 em seu artigo 28, parágrafo III
Determinação administrativa		X	

7. EQUIPE DE PLANEJAMENTO DA CONTRATAÇÃO

Nome		e-mail
Marcus Terra	Integrante demandante	marcus.terra@trt14.jus.br
Robson Alves Tiago	Integrante técnico	robson.tiago@trt14.jus.br
Wainner Brum Caetano	Integrante técnico	wainner.caetano@trt14.jus.br

8. FONTE DOS RECURSOS

Orçamento destinado aos cursos de TI.

6. ASSINATURAS

Demandantes	Data
Robert Armando Rosa	Datado e assinado eletronicamente