TRIBUNAL DE CONTAS DO ESTADO DE SÃO PAULO

DTI – Departamento de Tecnologia da Informação

DTEC – Divisão de Tecnologia

ESTUDO TÉCNICO PRELIMINAR

SEI 0014392/2024-70

CAPACITAÇÃO DA EQUIPE DE SEGURANÇA

1. DESCRIÇÃO DA NECESSIDADE

A realização de treinamentos técnicos pela equipe de segurança da informação é necessária para aprimorar a proteção dos dados e para garantir a integridade das operações de TI do Tribunal de Contas do Estado de São Paulo. Por ser uma área em constante evolução, os profissionais responsáveis pela proteção desses recursos devem estar atualizados, bem como devem conhecer as ameaças cibernéticas atuais e as técnicas utilizadas pelos atacantes. Treinamentos regulares poderão capacitar a equipe a identificar, prevenir e responder de maneira eficaz a incidentes de segurança, para minimizar riscos e evitar potenciais danos à infraestrutura digital e à reputação da instituição.

Além disso, a crescente complexidade das novas ameaças e ataques exige que os profissionais de segurança possuam um conhecimento profundo e especializado, muitas vezes adquirido por meio de capacitação direcionada. No cenário atual, não basta conhecer os princípios, melhores práticas e principais controles de segurança. Deve-se entender as ameaças e conhecer as táticas, técnicas e procedimentos utilizados pelos atacantes, além de ter a capacidade de realizar testes vulnerabilidades e penetração, que são fundamentais para avaliar os controles de segurança aplicados e identificar as fraquezas existentes nos recursos de tecnologia da informação.

Devido à falta de especialização da equipe de segurança na área de testes de penetração (pentest), o TCESP contratou uma consultoria para mapear e corrigir eventuais falhas na detecção de ataques cibernéticos à infraestrutura computacional do Tribunal. No entanto, os erros recorrentes da contratada na execução do serviço resultaram na suspensão do contrato 102/22 (SEI 0001464/2022-57), impedindo que o objetivo pretendido fosse alcançado. Porém, dado que as ameaças cibernéticas são constantes e não aguardam a resolução de problemas internos, as atividades previstas naquela contratação deverão ser realizadas. Nesse sentido, entende-se que, com um treinamento complementar ao contratado no processo 0014801/2022-76, focado na

realização de testes de penetração, a equipe de segurança estará apta a dar continuidade nos serviços iniciados pela consultoria, além de realizar de forma mais eficiente os testes de aplicações definidos na instrução de serviço GDTEC 1/2024 (SEI 0013966/2024-92).

Outro fator que reforça a necessidade de aprimoramento técnico da seção são as atribuições definidas na Resolução nº 08/2019 (processo SEI nº 0014287/2019-73), que alterou a redação de dispositivos da Resolução nº 07/2012:

> *1. gerenciar as redes de dados do Tribunal;*
> *2. gerenciar o ambiente de segurança da informação do Tribunal;*
> *3. monitorar os ativos de rede de dados e serviços de comunicação;*
> *(...)*
> *7. apoiar a elaboração políticas, normas e procedimentos de segurança da informação, orientando e fiscalizando a sua aplicação;*
> *8. realizar análises de risco e de segurança do ambiente de Tecnologia da Informação do Tribunal, tomando ações para eliminar e/ou diminuir eventuais causas e impactos;*
> *9. tratar os incidentes de segurança da informação, em conjunto com as demais unidades administrativas, respondendo pela sua gestão e pelo intercâmbio de informações com os responsáveis por redes externas;*
> *10. realizar avaliações e inspeções periódicas de segurança da informação.*

Por conta disso, é fundamental que os servidores da área de segurança da informação recebam treinamento regular que possibilite seu aprimoramento técnico, de forma que possam realizar avaliações de segurança com maior abrangência, eficiência e qualidade.

O objetivo da aquisição dos treinamentos é capacitar os servidores da área de redes e segurança da informação do TCESP, para que possam melhor atuar na defesa da infraestrutura tecnológica do tribunal, aperfeiçoando sua proteção contra as ameaças externas, que crescem e se tornam mais complexas a cada dia.

Sendo um órgão público governamental, o tribunal está em um dos setores econômicos mais visados por organizações criminosas digitais, que buscam ativamente por falhas e brechas de segurança na rede da corte de contas paulista, de forma a explorá-las e obter vantagens financeiras. Numa das técnicas mais utilizadas na atualidade, criminosos tentam inserir *ransomware* em computadores de uma rede institucional, que são programas maliciosos de computador que criptografam (codificam) os dados, que só podem ser recuperados com uma chave de acesso, que os bandidos exigem vultosas somas de dinheiro para entregar.

Mesmo que não se pague o resgate, que começa em centenas de milhares de dólares, o vazamento de uma imensa gama de informações sigilosas de funcionários, agentes públicos e órgãos jurisdicionados, bem como do dano à imagem e reputação da instituição, além da paralização das atividades até a recuperação da normalidade após a paralização dos serviços, possuem custo imensurável, que faz com a contratação dos cursos seja de valor irrisório.

2. ÁREA REQUISITANTE

Identificação da Área requisitante	Nome do responsável
DTEC-2 - Seção Técnica de Redes e Segurança da Informação do DTI – Departamento de Tecnologia da Informação do TCESP	Ricardo Abbade

Tabela 1 - Requisitante

3. DEMONSTRAÇÃO DA PREVISÃO DA CONTRATAÇÃO NO PLANO DE CONTRATAÇÕES ANUAL

Esta contratação não está prevista no plano de contratações anual. Entretanto, está prevista no Plano de Atividades do DTI de 2024.

4. NECESSIDADES DE NEGÓCIO

4.1. Capacitar a equipe técnica para a realização de Testes de Penetração (“Penetration Testing”, conhecido coloquialmente como pentest);
4.2. Nivelar o conhecimento dos servidores da seção;

5. ESTIMATIVA DA QUANTIDADE

Quantidade	Descrição
2	Capacitação em pentest - nível intermediário
5	Capacitação em pentest - nível avançado

Tabela 2: Quantitativo de vagas

6. LEVANTAMENTO DE MERCADO

Foi realizada uma pesquisa sobre as principais empresas e fornecedores que oferecem soluções de segurança cibernética, com foco na formação e certificação de profissionais em testes de penetração. O mercado dispõe de diversas certificações relevantes, cada uma com abordagens e ênfases ligeiramente diferentes. As certificações mais destacadas são:

6.1. Nível intermediário:

6.1.1. Certified Ethical Hacker da EC-Council: O CEH é uma das certificações mais conhecidas na área de segurança da informação, focada em testes de penetração e *hacking* ético;

6.1.2. CompTIA PenTest+: A PenTest+ é uma certificação focada em testes de penetração que cobre metodologias de pentesting, planejamento, escaneamento de redes, identificação de vulnerabilidades e exploração. Trata-se de um treinamento voltado para iniciantes e intermediários;

6.1.3. GIAC Certified Incident Handler (GCIH): O GCIH é uma certificação voltada para a identificação, resposta e mitigação de ataques cibernéticos. Embora não inclua a parte de testes ofensivos de segurança como o CEH, ela cobre uma ampla gama de técnicas de hacking usadas por atacantes e como responder a essas ameaças;

6.1.4. CREST Practitioner Security Analyst (CPSA): O CPSA é uma certificação que avalia as habilidades de segurança ofensiva e defensiva. É semelhante ao CEH no sentido de focar em habilidades práticas, porém, é mais popular no Reino Unido e em partes da Europa.

6.2. Nível avançado:

6.2.1. O Certified Penetration Testing Professional da EC-Council: O CPENT um curso avançado em testes de penetração, voltado para profissionais que já possuem conhecimento prévio em segurança e querem aprimorar suas habilidades.

6.2.2. Offensive Security Certified Professional (OSCP): O OSCP é uma certificação bastante respeitada na área de testes de penetração. O foco está em testar as habilidades práticas de invasão, com um exame prático de 24 horas;

6.2.3. GIAC Penetration Tester (GPEN): GPEN é uma certificação orientada a profissionais de segurança que querem validar suas

habilidades em testes de penetração. É um exame teórico, mas cobre uma ampla gama de técnicas e ferramentas usadas no pentesting.

7. ANÁLISE COMPARATIVA DAS SOLUÇÕES

A tabela 3 faz um comparativo das áreas específicas nos cursos de nível intermediário em que há um maior interesse e necessidade da equipe de segurança da informação do TCESP, de acordo com o levantamento de mercado:

Ponto de Comparação	CEH (EC-Council)	CompTIA PenTest+	GCIH (GIAC)	CPSA (CREST)
Engenharia Social e Técnicas de Phishing	Abrange técnicas de engenharia social e phishing	Não coberto de forma extensa	Cobertura limitada, mais voltado para resposta a incidentes	Não coberto de forma significativa
Criptografia e Ataques Criptográficos	Cobertura abrangente de algoritmos de criptografia e ataques relacionados	Foco limitado em criptografia	Não é foco principal, já que é voltado para resposta a incidentes	Pouca ou nenhuma cobertura de criptografia
Hacking de Dispositivos Móveis e IoT	Cobre técnicas de hacking em dispositivos móveis e IoT	Foco em redes e sistemas tradicionais, não em IoT/móveis	Não coberto	Foco principal em segurança de redes tradicionais
Segurança de Aplicações Web	Abrange vulnerabilidades em aplicações web, como SQL Injection, XSS, CSRF	Foco em segurança de rede e infraestrutura, menos detalhado em aplicações web	Não é o foco principal	Cobertura básica de ataques a aplicações web

Ponto de Comparação	CEH (EC-Council)	CompTIA PenTest+	GCIH (GIAC)	CPSA (CREST)
Reconhecimento de Redes (Footprinting e Scanning)	Enfoca técnicas detalhadas de footprinting e escaneamento de redes	Cobre reconhecimento, mas com menos profundidade	Foco limitado ao contexto de resposta a incidentes	Cobre parcialmente, mas com foco em infraestrutura
Evasão de Perímetro (IDS/IPS, Firewalls)	Inclui técnicas para evasão de sistemas de segurança	Coberto, mas com menos profundidade	Foco na resposta a incidentes, não em evasão	Cobertura básica de evasão de perímetro
Engenharia Reversa de Malware	Introduz conceitos básicos de engenharia reversa de malware	Não coberto	Mais focado em identificar e mitigar malware, sem foco em engenharia reversa	Não abordado

Tabela 3: Comparação entre os treinamentos CEH, Pentest+, GCIH e CPSA

A tabela 4, por sua vez, faz a mesma comparação entre aspectos específicos cobertos pelos treinamentos de nível avançado:

Ponto de Comparação	CPENT	OSCP	GPEN
Testes de Penetração em Ambientes Nuvem	Inclui práticas de pentesting em ambientes de nuvem	Mínimo foco	Não coberto
Segmentação e Pivoting em Redes Isoladas	Testes em redes segmentadas, exigindo pivoting	Pivoting básico em redes menores	Foco teórico e mais generalista
Ataques Avançados de Buffer Overflow	Exploração de buffer overflow em diferentes arquiteturas	Coberto, mas em menor profundidade	Coberto de forma teórica e sem profundidade prática
Evasão de IDS/IPS/Firewalls	Cobertura extensa de técnicas de evasão avançadas	Evasão de perímetro limitada	Cobertura mais teórica
Pentesting de Sistemas Web Corporativos	Foco em sistemas web empresariais	Pentesting em sistemas web básicos	Cobertura mais geral

Ponto de Comparação	CPENT	OSCP	GPEN
Ataques Contra Redes Wireless Corporativas	Inclui ataques avançados em redes wireless	Coberto de forma básica	Não coberto
Técnicas de Defesa e Contra-ataque	Envolve simulações de resposta e mitigação de incidentes	Foco em ataque, pouca ênfase em defesa	Não coberto

Tabela 4: Comparação entre os treinamentos CPENT, OSCP e GPEN

Com base na comparação dos aspectos técnicos abordados na tabela 3, o treinamento CEH oferece uma formação mais completa e profunda em áreas fundamentais do hacking ético, como engenharia social, criptografia, hacking de dispositivos móveis/IoT, segurança de aplicações web e técnicas avançadas de evasão. Isso faz do CEH uma escolha superior para quem busca uma certificação que cubra tanto as vulnerabilidades mais comuns quanto as ameaças emergentes, preparando os profissionais para enfrentar uma variedade de desafios na área de segurança cibernética.

Já na comparação entre os treinamentos avançados, o CPENT da EC-Council destaca-se pela sua abordagem prática robusta em redes tradicionais e modernas, sua cobertura ampla de criptografia e engenharia reversa de malware, além do foco em evasão de perímetro e segurança de IoT. Desta forma, o CPENT se apresenta uma escolha mais indicada para a equipe técnica do TCESP, que possui profissionais que já possuem experiência e desejam se especializar em técnicas avançadas de testes de penetração, enfrentando cenários mais complexos e realistas, o que vai além do foco oferecido pelo OSCP e GPEN.

8. REGISTRO DE SOLUÇÕES CONSIDERADAS INVIÁVEIS

Não há soluções inviáveis.

9. ANÁLISE COMPARATIVA DE CUSTOS (TCO)

Descrição	Qtde	PROCURADORIA GERAL DA REPÚBLICA - Pregão 54/2022	TRIBUNAL REGIONAL ELEITORAL DE MATO GROSSO DO SUL - Número do Contrato 288/2024	TRIBUNAL SUPERIOR ELEITORAL RJ - Contratação Direta nº 8/2024	Valor médio
Treinamento Certified Ethical Hacker da EC-Council	2	20.000,00	33.060,00	22.660,00	25.240,00

Tabela 5: TCO do treinamento intermediário

Descrição	Qtde	TRIBUNAL DE JUSTICA DO DISTRITO FEDERAL - Pregão 03/2022	ACADI-TI https://loja.acaditi.com.br/certificacoes-ec-council/cpent-certified-penetration-tester-live-online	TRIBUNAL REGIONAL ELEITORAL DO RIO DE JANEIRO - PROCESSO Nº 2022.0.000043002-2	Valor médio
Treinamento Certified Penetration Testing Professional da EC-Council	5	32.291,65	79.650,00	55.650,00	55.863,88

Tabela 6: TCO do treinamento avançado

O valor total estimado da contratação é de R$ 81,103,88.

10. DESCRIÇÃO DA SOLUÇÃO

O Certified Ethical Hacker (CEH) é um treinamento de certificação oferecido pela EC-Council, amplamente reconhecido como um dos principais cursos de hacking ético e segurança ofensiva no setor de segurança cibernética. Seu objetivo é capacitar os profissionais a pensarem como um adversário, permitindo-lhes identificar, analisar e explorar vulnerabilidades em sistemas e redes, mas com a intenção de proteger e fortalecer essas infraestruturas.

Enquanto o Certified Penetration Testing Professional (CPENT), por sua vez, é um treinamento avançado de pentesting que capacita profissionais a realizar testes de penetração em ambientes corporativos complexos. O curso foca em habilidades práticas para atacar e defender redes segmentadas, sistemas operacionais, infraestrutura de nuvem e dispositivos IoT. Os alunos

aprendem técnicas de evasão de perímetro, exploração de vulnerabilidades, pivoting em redes isoladas e ataques a aplicações web corporativas. O treinamento é intensivo, com laboratórios práticos, simulando cenários realistas de ataques cibernéticos, preparando os profissionais para enfrentar desafios sofisticados em segurança cibernética.

11. JUSTIFICATIVAS PARA O PARCELAMENTO OU NÃO DA CONTRATAÇÃO

Como os dois tipos de treinamento são independentes, considera-se que podem ser divididos em lotes distintos.

12. DEMONSTRATIVO DOS RESULTADOS PRETENDIDOS EM TERMOS DE ECONOMICIDADE E DE MELHOR APROVEITAMENTO DOS RECURSOS HUMANOS, MATERIAIS E FINANCEIROS DISPONÍVEIS

A qualificação técnica do corpo de servidores da DTEC-2 proporcionará diversos benefícios, tanto em termos de economicidade quanto de otimização dos recursos disponíveis. A capacitação visa aumentar a eficiência dos profissionais, melhorando a segurança da informação no TCESP e entre seus jurisdicionados, com impacto direto na redução de custos operacionais e diminuição de riscos de incidentes de segurança cibernética.

Além disso, ao investir no desenvolvimento de competências internas, o aproveitamento dos recursos humanos será maximizado, reduzindo a dependência de terceiros e fornecedores externos para a resolução de problemas técnicos, especialmente em áreas críticas como a proteção de dados e a segurança de sistemas. A iniciativa também promove a valorização do

serviço público, ao fortalecer a qualificação dos servidores e proporcionar um ambiente de trabalho mais seguro e eficiente.

Do ponto de vista financeiro, essa medida tende a gerar economias a médio e longo prazo, ao evitar custos com correção de falhas, incidentes de segurança e a contratação de serviços emergenciais. No que diz respeito aos recursos materiais, a gestão mais qualificada proporcionará uma melhor utilização das ferramentas e tecnologias disponíveis, maximizando seu potencial e aumentando o ciclo de vida útil dos equipamentos e sistemas.

Em síntese, a qualificação técnica dos servidores trará uma melhoria contínua da eficiência operacional, promovendo maior segurança e economia de recursos em todos os níveis, além de fomentar uma cultura de inovação e excelência dentro do TCESP.

13. CONTRATAÇÕES CORRELATAS E/OU INTERDEPENDENTES

Nenhuma.

14. DESCRIÇÃO DE POSSÍVEIS IMPACTOS AMBIENTAIS E RESPECTIVAS MEDIDAS MITIGADORAS

Trata-se de treinamento tecnológico por meio de computadores comuns conectados em rede, envolvendo apenas o uso de energia elétrica de baixa tensão, não havendo previsão de impactos ambientais.

15. POSICIONAMENTO CONCLUSIVO SOBRE A ADEQUAÇÃO DA CONTRATAÇÃO PARA O ATENDIMENTO DA NECESSIDADE A QUE SE DESTINA

Ante o exposto, entende-se que a contratação dos dois treinamentos é conveniente e necessária. Uma vez que a equipe DTEC-2 estará amparada tecnicamente por treinamentos internacionalmente reconhecidos na área de segurança da informação e com grande aceitação de mercado. Tornando-se apta a atender de forma eficiente a demanda definida na instrução de serviço GDTEC 1/2024 (SEI 0013966/2024-92) e dar continuidade aos trabalhos não concluídos do contrato de consultoria firmado via SEI 0014801/2022-7.

16. RESPONSÁVEIS PELA ELABORAÇÃO DO ESTUDO TÉCNICO PRELIMINAR E TERMO DE REFERÊNCIA

Flávio de Souza Oliveira (DTEC-2), Irineu Yukio Akaji (DTEC-2), Márcio Yudi Sato (DTEC-2), Nêilor Felipe Bastos (DTEC-2), Ricardo Abbade (DTEC-2) e Rodrigo Silva Mendonça (DTEC-2).