Estágio em Segurança da Informação

Tempest Security Intelligence
Remoto

Prazo

16/08/2024

Salário

A combinar

Local

nan

Descrição

DESCRIÇÃO DA VAGA

Essa vaga permite você concorrer a vagas no Programa de Estágio da Tempest para as áreas de Consultoria Técnica, Intel SaaS (Plataformas, Cyber Threat Intelligence e Situacional de Cyber Threat Intelligence) e Resposta a Incidentes. Para saber mais, confira a descrição das áreas no nosso site (https://www.tempest.com.br/programa-de-estagio/). Verifique a modalidade de contratação de cada área (híbrido, remoto ou presencial) e inscreva-se!

RESPONSABILIDADES E ATRIBUIÇÕES

CONSULTORIA TÉCNICA (HÍBRIDO para Recife ou São Paulo e REMOTO para o restante do Brasil)

Atividades:

- Adquirir conhecimentos sobre segurança da informação em geral;

- Adquirir conhecimentos teóricos e práticos sobre segurança de aplicações web e mobile;

- Realizar prática supervisionada junto com analistas da Tempest, atuando na execução de projetos reais de pentest web e mobile;

- Atuar em um projeto de pesquisa e desenvolvimento.

INTEL SAAS - PLATAFORMAS (HÍBRIDO para Recife ou São Paulo)

Atividades:

- Desenvolver e manter sistemas de coleta (web scrapers);

- Aprender sobre como funcionam requisições HTTP e bloqueios comuns contra acessos automatizados, modelagem de dados e soluções nuvem para armazenamento de big data;

- Desenvolver e manter plataformas de acesso aos dados coletados, podendo ser APIs REST, integrações automatizadas e uso de ferramentas de orquestração de eventos;

- Atender pedidos de outras equipes na área para fornecer suporte nas tarefas do dia a dia, levantar dados/estatísticas, automatizar tarefas repetitivas;

- Participar de reuniões cadenciais da equipe.

INTEL SAAS - CYBER THREAT INTELLIGENCE (HÍBRIDO para Recife ou São Paulo e REMOTO para o restante do Brasil)

Atividades:

- Aprender sobre o processo de engenharia de detecção desde de nosso planejamento, concepção até a etapa de entrega;

- Adquirir conhecimentos teóricos associado a ataques cibernéticos e técnicas de detecção de ameaças;

- Entender o processo de desenvolvimento de detecções seguindo práticas de mercado;

- Aprender a utilizar tecnologias e frameworks de mercado bem como: Magma, Sigma, MITRE ATTC&K, YAML, NIST, 4eyes, KANBAN, etc.;

INTEL SAAS - SITUACIONAL DE CYBER THREAT INTELLIGENCE (HÍBRIDO para Recife ou São Paulo e REMOTO para o restante do Brasil)

Atividades:

- Aprender sobre análise de múltiplos documentos, indicadores e técnicas sobre ameaças cibernéticas e realizar prática supervisionada junto com analistas da Tempest;

- Realizar prática supervisionada junto com analistas da Tempest na condução de pesquisas de inteligência em fontes abertas (OSINT);

- Realizar prática supervisionada junto com analistas da Tempest na produção de relatórios de inteligência contendo a descrição de ameaças e recomendações de mitigação.

RESPOSTA A INCIDENTES (HÍBRIDO para São Paulo)

Atividades:

- Aprender sobre projetos de resposta a incidentes e realizar prática supervisionada junto com analistas da Tempest;

- Adquirir conhecimentos sobre preservação de dados, processamento e análises em sistemas Windows, Linux , Mac OS X e logs, utilizando soluções forenses como Magnet Axiom;

- Realizar diagnósticos referentes às vulnerabilidades, fraudes e cibercrimes;

- Recuperação de dados e elaborar relatórios.

REQUISITOS E QUALIFICAÇÕES

Estar cursando Análise e Desenvolvimento de Sistemas, Ciência da Computação, Engenharia da Computação, Redes de computadores, Segurança da informação, Sistema de informação e Sistemas para Internet, ou cursos similares.

INFORMAÇÕES ADICIONAIS

Para as vagas de estágio nas áreas de Consultoria Técnica, Intel SaaS - Cyber Threat lintelligence e Intel SaaS - Situacional de Cyber Threat lintelligence, o regime de estágio será HÍBRIDO para a pessoa que for das Regiões Metropolitanas de Recife ou São Paulo, caso a pessoa seja de qualquer outro local do Brasil, o regime será REMOTO.

Para as vagas de estágio na área de Intel SaaS - Plataformas, o regime de estágio será HÍBRIDO para Recife ou São Paulo (NÃO tem modalidade remota).

Para as vagas de estágio na área de Resposta a Incidentes, o regime de estágio será HÍBRIDO para São Paulo (NÃO tem modalidade remota).

ETAPAS DO PROCESSO

Etapa 1: Cadastro

1

Cadastro

Etapa 2: Triagem + Mapeamento comportamental

2

Triagem + Mapeamento comportamental

Etapa 3: Teste Específico

3

Teste Específico

Etapa 4: Dinâmica de Grupo + Vídeo

4

Dinâmica de Grupo + Vídeo

Etapa 5: Entrevista Individual + Teste de Fit Cultural

5

Entrevista Individual + Teste de Fit Cultural

Etapa 6: Devolutiva do processo

6

Devolutiva do processo

Etapa 7: Contratação

7

Contratação

JÁ PENSOU EM FAZER PARTE DO TIME DA MAIOR EMPRESA ESPECIALIZADA EM CIBERSEGURANÇA DO BRASIL?

Estagiar na Tempest é ter a oportunidade de aprender com profissionais qualificados e preparados para lidar com os maiores problemas de cibersegurança. Com mais de 20 anos de experiência, nós trabalhamos como aliados de nossos clientes. Somos um grupo batalhador, inquieto, que privilegia o profundo conhecimento técnico, mas não deixa de valorizar as sólidas relações pessoais que são um terreno fértil para o desenvolvimento de novas ideias, inovações em produtos e serviços e amizades para toda a vida.

Participe do nosso processo e venha fazer parte do nosso coletivo de protagonistas!

Processo de Seleção

Inscrições e Mapeamento Comportamental - De 01/07 a 19/07/2024

Teste Específico - De 24/07 a 28/07/2024

Dinâmica de Grupo e Vídeo - Até 12/08/2024

Entrevista Individual - Até 22/08/2024

Devolutiva - Até 23/08/2024

Início do Estágio - A partir de 09/10/2024

Respeito à Diversidade. Conhecimento não se mede pela cor da pele, pela orientação sexual, pela deficiência, pela religião que se pratica ou pela roupa que se veste. Portanto, a Tempest não considera que características como essas são critérios para avaliação de pessoas que se candidatam para as nossas vagas. Para nós é importante o quanto você conhece das variadas competências com as quais lidamos por aqui, como aplicar esse repertório de conhecimentos ao longo de sua trajetória profissional e como poderá colaborar conosco.