
TEMPEST
ACADEMY
Conference
TLP: Green

TEMPEST
ACADEMY
Conference

Objetivo do Evento:

O Tempest Academy Conference é mais um recurso ofertado dentro do programa **ACTION Talents**, visando:

- ✓ Contribuir com as Instituições de Ensino no processo de **formação profissional**, através da disseminação e compartilhamento de conhecimento técnico em cibersegurança;
- ✓ Realizar o **mapeamento e atração de Talentos** profissionais em cibersegurança;
- ✓ Apresentar o ***mindset***, a **realidade profissional** e o **ambiente dos eventos da comunidade de cibersegurança** à comunidade acadêmica.

Publico Alvo:

- Estudantes e Professores dos cursos de **Graduação** e **Técnicos** interessados em cibersegurança;
- Estudantes e Profs. cursos de **Pós-grad. Latu Senso** interessados em cibersegurança;

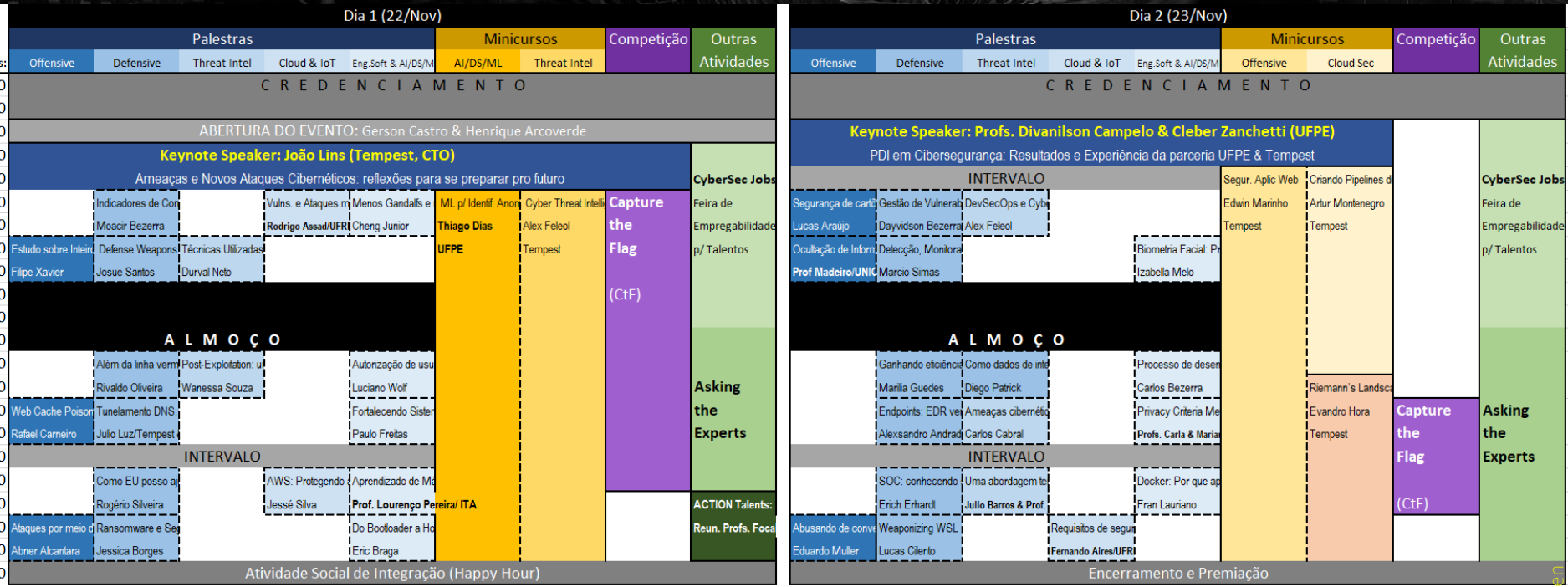
Atividades Previstas:

- Palestras Técnicas;
- Competição com Premiações (Capture the Flag);
- Ask the Experts;
- Coquetel e Atividade Social de Integração;
- Minicursos Técnicos;
- CyberSec Jobs: Feira de Empregabilidade para Talentos;
- Reunião Professores(as) do ACTION Talents;
- Sorteio de Brindes

TEMPEST ACADEMY Conference

Grade de Programação:

Overview



Programação sujeita a alterações sem aviso prévio.

Data: **22 e 23 Nov/2022** Local: **UFPE (Recife/PE)** Formato: **Híbrido**

TLP: Green

Palestras				
Keynotes				
Data	**Hora**	**Título Palestra**	**Palestrante**	**Descrição da Palestra**
22/Nov (Ter)	09:00	**Abertura do Evento**	**Henrique Arcoverde** Director of Operations **Gerson Castro** Head of Academy, Research & Publishing	Boas vindas, apresentação do objetivos & orientações gerais sobre a programação do evento;
	09:30	**KEYNOTE:** **Ameaças e novos ataques cibernéticos: reflexões para se preparar pro futuro**	**João Lins** CTO, Tempest	O objetivo dessa palestra é abordar algumas questões técnicas que envolvem o funcionamento, evoluções, aprendizados e reflexões dos ataques e das principais ameaças que tem ganho grande exposição na mídia desde o período pandêmico. E ainda serão feitas correlações entre tais aspectos e a necessidade crescente de formação especializada em cibersegurança, visando o alcance de resultados positivos nos seus respectivos campos de
23/Nov (Qua)	09:00	**KEYNOTE:** **IA aplicada a CyberSec: Overview e Resultados da parceria em PD&I entre Cin/UFPE & Tempest**	**Profs. Divanilson Campelo & Cleber Zanchettin** UFPE	Os Profs. Divanilson & Cleber deverão compartilhar uma visão geral das ações em Inteligência Artificial aplicada a Cibersegurança que o time do CIn/UFPE vem realizando através de ações de Pesquisa, Desenvolvimento & Inovação com seus alunos de Doutorado, Mestrado e Iniciação científica, visando responder aos desafios de empresas de mercado neste segmento, tal como, o que vem sendo feito em parceria com a Tempest.
	18:30	**Encerramento do Evento**	**Gerson Castro** Head of Academy, Research & Publishing	Divulgação & Premiação dos Vencedores do Capture the Flag (CTF); Sorteios e Agradecimentos finais.

Palestras				
Trilha: Segurança **Ofensiva**				
Data	**Hora**	**Título Palestra**	**Palestrante**	**Descrição da Palestra**
22/Nov (Ter)	11:30	**Estudo sobre Inteiros na linguagem C**	**Filipe Xavier** Tempest	Partiremos dos princípios básicos sobre inteiros, até chegarmos ao estudo de vulnerabilidades que envolvem o tema. Conhecer com mais profundidade o funcionamento dos inteiros em C, torna possível detectar falhas dessa natureza em aplicações reais. Sendo assim, para que se possa realizar uma análise sobre bugs na aritmética de inteiros, é preciso, sobretudo, estudarmos regras de conversão, wraparound e promoções de inteiros.
	15:00	**Web Cache Poisoning: uma demonstração prática**	**Rafael Carneiro** Tempest	Falaremos a respeito de caches e da vulnerabilidade web cache poisoning, como ela ocorre e quais cenários é possível explorá-la, através da realização de algumas demonstrações práticas.
	17:30	**Ataques por meio de misconfiguration em orquestradores Kubernetes**	**Abner Alcântara** Tempest	Na palestra sera explicado brevemente o que é Kubernetes, como funciona as features necessárias para os ataques, quais são os seus vetores e como se proteger.
23/Nov (Qua)	10:30	**Segurança de cartões RFID MIFARE CLASSIC 1KB**	**Lucas Araújo** Tempest	A apresentação busca abordar as vulnerabilidades presentes nos cartões de rádio frequência MIFARE CLASSIC de 1KB e suas técnicas de exploração. O MIFARE Classic foi introduzido em 1995 pela Philips, e rapidamente se tornou um produto com alta adesão no mercado por conta do seu baixo custo. O mesmo vem sendo utilizado principalmente em sistemas de transporte público, controle de acesso em instituições e até bases militares. Estima-se que até o final de 2008 foram produzidos 3.5 bilhões de cartões MIFARE Classic de 1KB e 4KB
	11:30	**Ocultação de Informações: Desafios e Aplicações**	**Prof.** Francisco **Madeiro** UNICAP	Nesta palestra, será apresentada uma visão geral do processo de ocultação da informação com foco em imagens digitais, através das técnicas de esteganografia e marca d'àgua, sendo apresentados desafios e aplicações.
	17:30	**Abusando de conversores html para pdf**	**Eduardo Müller** Tempest	Nesta palestra será demonstrado uma breve avaliação realizada em um conjunto de bibliotecas que permitem a conversão de código HTML para PDF, mostrando que tipo de vulnerabilidades podem ser inseridas num software através do uso dessas bibliotecas, além de como fazer para mitigar tais fragilidades.

TLP: Green

Palestras				
Trilha: Segurança **Defensiva**				
Data	Hora	Título Palestra	Palestrante	Descrição da Palestra
22/Nov (Ter)	10:30	**Indicadores de Comprometimento na engenharia de detecção de incidentes**	**Moacir Bezerra** Tempest	Nesta apresentação veremos como o avanço das tecnologias e das ameaças virtuais, tais como ataques de ransomwares que vêm crescendo nos últimos anos, tornou crucial analisar as ameaças de forma minuciosa e com inteligência.
	11:30	**Defense Weapons**	**Josué Santos** Tempest	Em tempos no qual o tema ataque cibernético está cada vez mais comum em fóruns públicos, muito se olha para metodologias de ataques, tentativas de exposições, desativações, roubos e obtenção acessos sem autorização, entre em outros. Mas ainda persiste alguns questionamentos: Como proteger? Como mitigar? Como olhar/analisar/tratar o ataque de forma holística? Com o intuito de contestar essas indagações, o Defense Weapons tem como proposta trazer a visão com foco em defesa para que as detecções aconteçam em tempo hábil e o potencial impacto , de quaisquer que sejam os eventos, sejam mitigados com sucesso. Neste papo abordaremos algumas metodologias de trabalho com base em frameworks, sendo eles : Mitre Att&ck, DeTT&ct e React. A ideia central é discutirmos desde as matrizes de táticas e técnicas de forma categorizada/ comportamento dos adversários à preparação, identificação, contenção, erradicação, recuperação até lições aprendidas.
	14:00	**Além da linha vermelha (Formação Avançada de Defesa)**	**Rivaldo Oliveira** Tempest	Palestra voltada para os times de defesa (SOC/CSIRT), efetuando um overview de modos de defesa avançada e o trabalho correlacionado do SOC com áreas como Threat Intelligence. Demonstração de formação inicial de modo de detecção baseado em comportamento (TTPs), seguindo como padrão Mitre Attack & Cyber Kill Chain.
	15:00	**Tunelamento DNS: Ataque e Detecção usando Machine Learning**	**Julio Luz** Tempest / UFPE	Nessa apresentação, mostraremos como o famoso protocolo DNS, criado com o intuito de converter nomes de domínios para endereços IP, pode ser (ab)usado por um atacante para exfiltrar dados de suas vítimas ou estabelecer um canal de comunicação discreto com o servidor do invasor, que poderá utilizar o mesmo para enviar comandos e então controlar a máquina comprometida. Vamos abordar o conceito dos ataques de tunelamento e exfiltração via DNS, para que servem, como funcionam e quando os atacantes utilizam essas técnicas, realizando uma prática com a ferramenta DnsCat2 popularmente utilizada para a técnica de tunelamento DNS, destacando também os dados anômalos gerados por esse ataque. Em seguida, falaremos sobre os desafios para a detecção e os mecanismos de proteção contra esses ataques. Por fim, será realizada uma prática de detecção utilizando a técnica de regressão logística e dados gerados pela simulação do ataque com a ferramenta DnsCat2.
	16:30	**Como EU posso ajudar na prevenção da fuga da informação?**	**Rogério Silveira** Tempest	O vazamento de dados é uma das principais preocupações das corporações, os investimentos para tentar mitigar esse problema não depende necessariamente apenas de ferramentas tecnológicas, mas os funcionários de uma empresa possuem grande responsabilidade para o êxito desse processo.Nessa apresentação vamos explorar o tema de vazamento de dados, que foi classificado em vazamento acidental, intencional, através de exploração de vulnerabilidades e engenharia social, bem como as boas práticas e processos para conscientização de todos.
	17:30	**Ransomware e Segurança Defensiva**	**Jéssica Borges** Tempest	Nesta palestra serão apresentados quais os principais impactos causados por ransomwares, bem como, as formas de proteção que podem ser utilizadas através de ferramentas de segurança, visando evitar a contaminação ou minimizar os danos.

Palestras				
Trilha: Segurança **Defensiva**				
Data	**Hora**	**Título Palestra**	**Palestrante**	**Descrição da Palestra**
23/Nov (Qua)	10:30	**Gestão de Vulnerabilidade e Estratégias de Priorização para Correção**	**Dayvidson Bezerra** Tempest	Com o aumento cada vez mais crescente de vulnerabilidades o desafio vai além das correções que devem ser feitas e se faz necessário trabalhar em uma estratégia de como priorizar as vulnerabilidades encontradas. Nessa talk vamos falar sobre gestão de vulnerabilidade, risco e algumas estratégias de priorização, com base nas experiencias e alguns cases vivenciados nos últimos anos.
	11:30	**Detecção, Monitoramento e Correlação de Eventos como estratégia e planejamento de resposta a incidentes num SOC através de SIEM e SOAR**	**Marcio Simas** Tempest	Nessa palestra será apresentada um overview sobre a aplicação dos conceitos de SIEM e SOAR no processo de resposta a incidentes de segurança, através da demonstração de casos de usos que permitam comparar como desafios encontrados no SOC podem ser superados com ou sem a utilização destas soluções.
	14:00	**Ganhando eficiência na detecção e visibilidade de tratamento de incidentes através do uso dos frameworks MITRE & Cyber Kill Chain**	**Marília Guedes** Tempest	Nessa palestra iremos abordar um pouco da experiência vivenciada no time de tratamento de incidentes, através do ganho de eficiência na aplicação dos frameworks Cyber Kill Chain (no processo de mitigação de ataques) e MITRE ATT&CK (com seu escopo mais profundo que inclui detalhes granulares no comportamento de ataques avançados, como Táticas, Técnicas e Procedimentos - TTPs).
	15:00	**Endpoints: EDR versus AntiVirus - entendendo a fronteira de utilização dessas soluções**	**Alexsandro Andrade** Tempest	Será apresentada um overview da aplicação dos conceitos de Antivírus e EDRs como soluções endpoints, visando esclarecer quais são os seus limite na cadeia de detecção, bem como, também responder a seguinte questão: como o posicionamento estratégico dessas 2 soluções auxiliam times de segurança a terem um melhor resultado na detecção, análise e contenção de anomalias no ambiente corporativo ?
	16:30	**SOC: Conhecendo sua estruturação e operação**	**Erich Erhardt** Tempest	Essa palestra tem como objetivo fazer um overview sobre o Security Operations Center (SOC), dando ênfase em sua estrutura básica, sua operação e no Defense Assessment.
	17:30	**Weaponizing WSL**	**Lucas Cilento** Tempest	O que é WSL? Pra que serve? E como ele pode ser utilizado para comprometer seu sistema Windows? Nessa palestra vamos abordar o Windows Subsystem for Linux e revisar como ele pode facilitar a sua vida, bem como os riscos que ele oferece e algumas formas de deixar esse sistema mais seguro.

TLP: Green

Palestras				
Trilha: **Threat Intelligence**				
Data	**Hora**	**Título Palestra**	**Palestrante**	**Descrição da Palestra**
22/Nov (Ter)	11:30	**Técnicas Utilizadas para Evitar Detecção e Takedown de Conteúdo Malicioso**	**Durval Neto** Tempest	Esta palestra apresentará técnicas utilizadas por fraudadores para evitar a detecção, e consequentemente o takedown, de URLs maliciosas. Durante o decorrer da palestra, serão demonstrados casos reais de campanhas utilizando os métodos apresentados.
	14:00	**Post-Exploitation: um panorama sobre as principais ferramentas de pós-exploração usadas por cibercriminosos**	**Wanessa Souza** Tempest	O que os adversários fazem depois de invadir e explorar um sistema? Nessa palestra vamos discutir sobre as principais ferramentas de pós-exploração usadas atualmente, abordando também as fases de um ataque com base em frameworks como Cyber Kill Chain e Mitre ATT&CK, o funcionamento de um servidor de comando e controle e as principais estratégias de defesa e detecção.
23/Nov (Qua)	10:30	**DevSecOps e Cyber Threat Intelligence juntos contra o Cibercrime**	**Alex Feleol** Tempest	O mercado global de DevSecOps está crescendo a uma velocidade muito alta e em sete anos (entre 2020 e 2027) terá alcançado um valor de US$ 15,9 bilhões. Isso acontece porque as empresas perceberam que investir no desenvolvimento seguro é muito mais eficiente do que ser surpreendido pelos cibercriminosos, pois no mercado
	14:00	**Como dados de inteligência podem ajudar na gestão de vulnerabilidades**	**Diego Patrick** Tempest	Com o crescente número de vulnerabilidades e a falta de profissionais especializados em cibersegurança, as organizações enfrentam um grande desafio ao encontrar inúmeras vulnerabilidades a serem corrigidas. Resolver esse desafio faz parte da gestão de vulnerabilidades, que tem como parte do processo decidir quais vulnerabilidades são as mais importantes. Nesta apresentação, que é baseada na minha pesquisa de estágio, iremos ver quais as fontes de dados de inteligência e como esses dados podem ajudar a ter um modelo efetivo de priorização de vulnerabilidades a serem corrigidas em um programa de gestão de vulnerabilidades.
	15:00	**Ameaças cibernéticas: cenário e desafios**	**Carlos Cabral** Tempest	Nesta apresentação, exploraremos os conceitos de vulnerabilidades e ameaças cibernéticas por meio de três casos reais: um ataque contra uma indústria petroquímica; a operação de uma quadrilha de ransomware e um zero-day encontrado em dispositivos da Apple que estava sendo usado como ponte para a instalação do spyware Pegasus.
	16:30	**Uma abordagem temporal para detecção de ataques de phishing**	**Prof. Carlo Revoredo & Julio Cesar Barros** UPE POLI	Ataques de phishing são conhecidos por apresentarem um curto tempo de atividade e combinados a uma alta disseminação, aumentando significativamente a propagação de páginas maliciosas, além de dificultar uma rastreabilidade sobre suas ações. Portanto, é sensato assumir que muitas mudanças de comportamento são de difícil observação no cenário de atuação do phishihng. Concomitantemente, considerando que muitos dos mecanismos de predição de phishing são sustentados por características presentes em uma página, este estudo defende a ideia de analisar com uma abordagem temporal as mudanças presentes no phishing com o passar dos anos. Com isso, o objetivo é analisar as características mais suscetíveis aos aspectos da volatilidade no ciclo de vida de um phishihg. Para tanto, técnicas de regressão logística e Análise de séries temporais são utilizadas para trazer luz sobre as mudanças de conceito apresentadas nos últimos 5 anos de ataques de phishing.

TLP: Green

Palestras				
Trilha: Cloud & IoT				
Data	**Hora**	**Título Palestra**	**Palestrante**	**Descrição da Palestra**
22/Nov (Ter)	10:30	**Vulnerabiliades & Ataques mais comuns em Cloud Computing**	**Rodrigo Assad** UFRPE	Neste encontro, o Prof. Rodrigo Assad irá apresentar as principais vulnerabilidades e as explorações realizadas por ataques mais comuns em ambientes de Cloud Computing, de acordo com o seu expertise desenvolvido em seus quase 15 anos de atuação profissional e ensino neste segmento específico da cibersergurança.
	16:30	**AWS: Protegendo aplicações Web com o WAF**	**Jesse Silva** Tempest	Nesta palestra demonstraremos algumas das vunerabilidades mais comuns de aplicações web e como podemos nos proteger contra elas dentro da Cloud. Também serão apresentados conceitos de aplicações web e suas vunerabilidades, OWASP e conceitos de rede como firewall, modelo OSI e protocolos utilizados na internet.
23/Nov (Qua)	17:30	**Requisitos de segurança para sistemas IoT: por onde começar?**	**Prof. Fernando Aires** UFRPE	O crescimento da IoT é visível e vem sendo acompanhado de preocupações razoáveis de segurança. Uma das formas de tornar sistemas IoT mais seguros é observar e implementar requisitos de segurança. Mas, como fazer isto quando existem centenas de requisitos propostos por diversas organizações relevantes? Nesta conversa, vamos conversar sobre como esta tarefa pode ser realizada.

Palestras				
Trilha: Engenharia de Sofware & Data Science(DS)/Artificial Intelligence(AI)/Machine Learning(ML)				
Data	Hora	Título Palestra	Palestrante	Descrição da Palestra
22/Nov (Ter)	10:30	**Menos Gandalfs e mais John Wicks (ou, - frameworks mágicos e + engenharia de software)**	**Cheng Júnior** Tempest	Você sabe quais problemas de segurança podemos ter em apenas utilizar um simples *framework* Web, ou de banco de dados? Será que seu sistema tem uma vulnerabilidade num código que não é seu? como identificar? como previnir? como vivem? como se alimentam? tudo isso e mais um pouco na TDC Recife 2019. Nesta palestra irei falar sobre os principais problemas de segurança e de engenharia de *software* que você pode ter ao adotar *frameworks* de alto acoplamento.
	14:00	**Autorização de usuários**	**Luciano Wolf** Tempest	A combinação "usuário e senha" nem sempre é o suficiente para decidir se alguém está autorizado a acessar uma parte do sistema. Uma forma natural é tentar atribuir perfis e este será o assunto a ser apresentado nessa palestra, visando ainda responder algumas dúvidas como: Devemos implementar todas as regras no backend? Devemos usar alguma ferramenta? Que tipo de políticas e regras?
	15:00	**Fortalecendo Sistemas de Detecção de Intrusão com Machine Learning"**	**Paulo Freitas** Tempest	Nesta apresentação, discutiremos o uso de machine learning (aprendizagem de máquina) em sistemas de detecção de intrusão (Intrusion Detection System – IDS). Destacaremos como machine learning pode fortalecer IDSs e permitir que eles detectem ataques cibernéticos mais complexos, explicando as principais técnicas de aprendizagem não supervisionada utilizadas por IDSs.
	16:30	**Aprendizado de Máquina em Segurança Cibernética**	**Prof Lourenço Pereira** ITA	Segurança Cibernética é um elemento essencial para a transformação digital em que vivemos. Percebemos que cada vez mais a complexidade e a integração de sistemas computacionais é alta e, com isso, temos o desafio de entender profundamente as tecnologias para saber lidar com a descoberta e mitigação de ameaças para previnir ações maliciosas que subvertem nossos sistemas. A situação de fragilidade em que estamos fica evidente quando observamos infraestruturas físicas onde sistemas computacionais provocam consequências cinéticas, causando baixas e danos nas mais variadas esferas de valor. Muito embora o avanço tecnológico tenha proporcionado melhora na comunicação entre as pessoas e também promovido melhores serviços em geral, percebe-se que ainda há muita fragilidade nos sistemas e nos recursos humanos que desenvolvem estes sistemas. Nesse contexto, é feita uma explanação sobre sistemas computacionais de modo que podemos estudá-las exaustivamente para caracterizar ataques conhecidos e detectar anomalias na carga de trabalho típica do sistema em análise. Assim, Aprendizado de Máquina é apresentado como ferramental capaz de auxiliar neste processo pois possibilita a avaliação em uma escala significativamente maior do que aquela praticada por um ser humano.
	17:30	**Android: do Bootloader a HomeScreen**	**Eric Braga** Tempest	Será que meu celular está lento? Demora muito para ele inicializar! A quantidade de informações, processos, serviços, daemons, criação e utilização de sockets é gigantesca para que o Android apresente a primeira tela ao usuário. O objetivo desta palestra é demonstrar para os ouvintes como o Sistema Operacional é inicializado do momento em que o botão de power é apertado até o momento em que o usuário pode interagir com as suas aplicações

TLP: Green

Palestras				
Trilha: Engenharia de Sofware & Data Science(DS)/Artificial Intelligence(AI)/Machine Learning(ML)				
Data	**Hora**	**Título Palestra**	**Palestrante**	**Descrição da Palestra**
23/Out (Qua)	11:30	**Biometria Facial: Principais Ataques e Mitigações**	**Izabella Melo** Tempest	Sistemas baseados em biometria facial se tornaram extremamente comuns durante a pandemia, período em que o distanciamento social se fez necessário e, o ato de ir presencialmente até determinados ambientes, como medida de segurança, tornou-se impraticável. E, como para toda grande novidade no mercado de segurança, essa explosão de sistemas baseados em biometria facial veio acompanhada de novas fraudes, cada vez mais sofisticadas. Nessa talk vamos entender um pouco mais sobre o funcionamento desses sistemas, os ataques que eles podem sofrer e as principais formas de mitigação
	14:00	**Processo de desenvolvimento SEGURO de software: aspectos relevantes & de implementação**	**Carlos Bezerra** Tempest	Incorporar requisitos de segurança no processo de desenvolvimento de software vem se tornando uma demanda cada vez mais evidente e exigida no mercado, mas ainda assim, muitos se perguntam: o que e como fazer para suprir esta necessidade? Mesmo sabendo que o uso adequado de processos, práticas e ferramentas de segurança, seja o meio mais coerente para se alcançar este objetivo, aplicar tudo isto no processo de desenvolvimento de software, apesar de essencial, pode ser bem desafiador para muita gente. Nessa palestra, serão discutidos e exibidos algumas das questões de segurança mais relevantes e também como tentar implementá-los da maneira mais fluida possível, em times de desenvolvimento de software.
	15:00	**Privacy Criteria Method: um método de especificação de requistos de privacidade utilizando linguagem natural**	**Profa. Carla Silva & Profa. Mariana Peixoto** UFPE	A privacidade é um requisito não funcional que se tornou uma preocupação devido as novas demandas de conformidade com as leis de proteção de dados. Contudo, as técnicas tradicionais de Engenharia de Requisitos não são suficientes para representar os requisitos de privacidade. Neste cenário, sugiu o Privacy Criteria Method (PCM), um método para auxiliar desenvolvedores ágeis na especificação de requisitos de privacidade. O PCM foi avaliado por meio de um estudo qualitativo com profissionais da indústria de diversos domínios de aplicação, os quais avaliaram a qualidade dos artefatos PCM produzidos, bem como a aplicabilidade, utilidade e escalabilidade do método. A apresentação explicará o PCM e discutirá a avaliação e seus resultados.
	16:30	**Docker: Por que aprender a falar baleiês?**	**Fran Lauriano** Tempest	Nessa apresentação abordarei as vantagens de uso da tecnologia Docker que for criada em 2013 e vem sendo uma das mais utilizadas para empacotamento de sistemas ou ambientes dentro de um container.

Minicursos					
Data	**Trilha**	**Hora**	**Título do Mini-Curso**	**Instrutor**	**Descrição do Mini-Curso**
22/Nov (Ter)	AI/DS/ML	08:00	**ML p/ Identificação de Anomalias em Tráfego de Rede** (Carga Horária: 8 horas)	**Thiago Dias Bispo** UFPE	A detecção de intrusão em redes de computadores é um problema diário crítico e desafiador na área da segurança cibernética. Abordagens tradicionais para detecção geralmente contam com metodologias baseadas em regras que nem sempre são eficazes, sobretudo na detecção de ataques cujo modo de operação não seja conhecido previamente. Na tentativa de contornar essas deficiências, metodologias recentes têm buscado enquadrar a detecção de intrusão em redes como um problema de identificação de anomalias usando métodos de aprendizagem de máquina (AM). Dada a relevância desse tópico, durante esse minicurso o participante aprenderá alguns conceitos fundamentais sobre o problema da detecção de anomalias usando AM, e sobre como isso vem sendo aplicado no problema da detecção de intrusão. Além disso, ao longo de uma sessão prática, o participante verá como aplicar algoritmos de AM na detecção de anomalias em dados de tráfego de rede.
	Threat Intel	08:00	**Cyber Threat Intelligence Fundamentals** (Carga Horária: 8 horas)	**Alex Feleol** Tempest	Neste mini-curso serão abordados os conceitos de Threat Intel com foco em Cyber Threat Intelligence, bem como, técnicas e dicas práticas e OSINT e OPSec para auxiliar sua organização na obtenção de informações sobre ameaças cibernéticas oriundas de diversas fontes do ciberespaço, incluindo a Deep Web e a Dark Net em redes anonimizadas pelo protocolo TOR (The Onion Router).
23/Nov (Qua)	Offensive	08:00	**Segurança de Aplicações Web** (Carga Horária: 8 horas)	**Edwin Marinho** Tempest	Promover a apresentação dos conceitos e aplicações práticas relacionadas a Segurança de Aplicações Web. Objetivos específicos: - Realizar nivelamento dos conceitos fundamentais sobre segurança de aplicações web; - Explicar como utilizar o BurpSuite, o software mais utilizado por um consultor de segurança web, tornando simples o dia a dia na identificação de vulnerabilidades; - Apresentar um conjunto de vulnerabilidades, trazendo descrição, formas de exploração e correção de tais problemas de segurança, dando ao aluno a capacidade de identificar e testar a existência de vulnerabilidades web.
	Cloud Sec	08:00	**Criando Pipelines de Dados com Airflow (Carga Horária: 4 horas)**	**Artur Montenegro & Henrique Menezes** Tempest	O Apache Airflow é uma ferramenta open-source para criar, monitorar e agendar fluxos de trabalho. Nesse contexto, um fluxo de trabalho é um conjunto de passos para se realizar uma tarefa de engenharia de dados, como por exemplo, escrever no banco de dados ou realizar transformações num conjunto de dados e salvar no AWS S3. Este será um workshop introdutório onde você aprenderá tudo que você precisa para iniciar a utilizar o Airflow. Primeiramente, faremos com que você fique confortável com os componentes do Apache Airflow tal como DAGs e por que elas são úteis. Então você aprenderá como implementar Airflow DAGs usando operators e como agendá-las e monitora-las. No final do workshop, você terá aprendido a como construir um pipeline de dados do início ao fim.
	Cloud Sec	14:30	**Riemann's Landscape** (Carga Horária: 3 horas)	**Evandro Hora** Tempest	Foi o atendimento a certos requisitos de segurança que tornou viável o comércio eletrônico e o internet banking, permitindo a Internet ser o que ela é hoje. Neste encontro com o Prof. Evandro Hora, sócio-fundador da Tempest, você vai ter a chance de curtir e entender a história dos bastidores da uma tecnologia fundamental para a segurança na Internet, o que somente se tornou possível por conta de um problema matemático, descoberto há 160 anos e ainda sem solução. Se você se interessa por Segurança da Informação, Privacidade, Criptografia e Matemática, então venha conhecer uma história incrível com uma abordagem lúdica e totalmente fora da curva.

TEMPEST ACADEMY Conference

Competição: Capture the Flag

O Evento promoverá uma competição no formato Capture the Flag (CtF), através de desafios estimulantes e divertidos, como mais uma oportunidade para o desenvolvimento de algumas habilidades técnicas que podem vir contribuir na formação da competência profissional em cibersegurança.

Os participantes poderão competir na modalidade presencial ou remota (online) e os vencedores receberão premiações anunciadas e entregues no final da competição.

Aos participantes presenciais, a Coordenação do Evento disponibilizará um ambiente bastante adequado, porém os competidores deverão trazer e utilizar os seus próprios notebooks. Todas as demais regras e regulamentos da competição, estão disponibilizadas no site do evento.

O CtF do Tempest Academy Conference contará com o suporte e operacionalização técnica da Hacking eSports.

TEMPEST ACADEMY Conference

Outras Atividades

CyberSec Jobs (Feira de Empregabilidade para Talentos):
Ao longo da realização do Evento, a Tempest e algumas de suas empresas parceiras, irão estar com seus times de Atração de Talentos organizando várias atividades junto aos participantes (presencias e remotos), tais como: sorteio de brindes, levantamento e análise de currículos, mapeamento de talentos profissionais, orientações sobre programas de estágios e possíveis entrevistas para ofertas de oportunidades e vagas profissionais.

Ask the Experts:
Durante todo o evento, em um ambiente exclusivo aos participantes inscritos apenas na modalidade presencial, Consultores Técnicos experientes da Tempest estarão disponíveis para uma interação 1:1 (***one on one***) com estudantes e professores(as) visando tirar dúvidas técnicas, trocar experiências profissionais ou prestar orientações técnicas sobre questões relacionadas às suas áreas de especialidades em cibersegurança.

Reunião Professores(as) do ACTION Talents:
Será realizado uma reunião especial somente aos Professores(as) participantes da Conferência (presenciais ou remotos) que vêm atuando na validação do piloto deste programa educacional da Tempest ao longo de 2022. O objetivo será que estes Profs. possam apresentar e compartilhar com os demais colegas as boas práticas e os seus bons resultados alcançados em todo o Brasil através do uso dos recursos do ACTION Talents.

Data: **22 e 23 Nov/2022**

Local: **UFPE (Recife/PE)**

Formato: **Híbrido**

TEMPEST ACADEMY Conference

Inscrições pelo Even3:

even3.com.br/tempestacademyconference

Participação Presencial:

- **R$30,00** (Público Geral)
- **R$20,00** (Estudantes e Profs. do CIn/UFPE)

Participação Remota (Online):

- **R$20,00** (Público Geral)

TLP: Green