Tempest

ACADEMY

Conference

2023

Integrando Cibersegurança e Proteção de Dados nas Metodologias de Desenvolvimento de Software Orientado a Dados

Desenvolvendo Software Seguro em uma Era Data-Driven

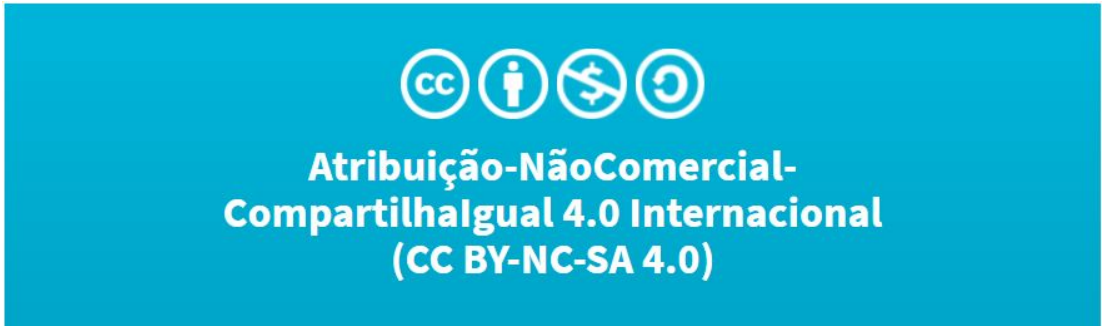
por Vinicius Cardoso Garcia, PhD

Professor Associado, Cin @ UFPE

Classificação da Informação: PÚBLICA
Autor da apresentação: <Nome do autor da apresentação>

Licença do material

Este Trabalho foi licenciado com uma Licença



Mais informações visite

https://creativecommons.org/licenses/by-nc-sa/4.0/deed.pt_BR

Tempest

ACADEMY

Conference

01 Fundamentos e Contexto

02 Metodologias e Práticas de Desenvolvimento

03 Implementação e Tecnologias

04 Preparação para o Futuro

Classificação da Informação: PÚBLICA Autor da apresentação: <Nome do autor da apresentação>

Quem sou eu

- D.Sc. em Engenharia de Software, CIn-UFPE + Universität Mannheim , 2010
- Professor Associado III @ Cin-UFPE [Ago-2010]
    - 60 BSc; 1/46 MSc; 4/7 (+co) DSc :: http://viniciusgarcia.me
    - ES (bit.ly/vcg-es); Microsserviços (bit.ly/vcg-microservices); DevOps (bit.ly/vcg-devops)
    - Coordenador de Extensão e Cultura [Jun-2021]
- Pesquisador Associado @ INES [Instituto Nacional para Ciência e Tecnologia em Engenharia de Software] :: http://www.ines.org
- Cientista Associado @ TDS.company

Warm up

Tempest
[ACADEMY]
Conference

Dados são o novo urânio e por isso precisa ter os seus cuidados

O desenvolvimento de software não é apenas sobre criar soluções funcionais, mas também sobre garantir que essas soluções sejam seguras e confiáveis.

O uso crescente de Inteligência Artificial para melhorar a detecção de ameaças em tempo real

Melhores práticas, desafios e estratégias futuras para integrar a cibersegurança de maneira eficaz no ciclo de desenvolvimento de software

Por que Cibersegurança e Proteção de Dados Importam?

Tempest
[ACADEMY]
Conference

Tudo é software ~> tudo é digital ~> tudo em rede

Com o aumento da quantidade e valor dos dados,

crescem também os riscos associados

Crescente complexidade regulatória

Segurança e a proteção de dados não são mais

RNFs

Introdução

Tempest
[ACADEMY]
Conference

Quantidade de dados que criamos, processamos e armazenamos tem crescido exponencialmente e isso nos leva a novos desafios [segurança dos dados e sistemas]

Conceitos fundamentais de cibersegurança e proteção de dados

~> ESDD

Melhores práticas, metodologias e ferramentas que podem ser integradas ao longo do ciclo de vida do desenvolvimento

Não é apenas uma questão de segurança, mas também um imperativo ético e legal

Panorama Atual

Tempest
[ACADEMY]
Conference

Situação Atual da Cibersegurança e Proteção de Dados...

... aumento dramático tanto no volume quanto na sofisticação dos ataques cibernéticos

Alguém lembra de algum incidente de segurança recente?

Impacto das Violações de Dados: não são apenas um risco financeiro

A Necessidade de Conscientização e Preparação

Panorama Atual

Tempest
[ACADEMY]
Conference

Em um mundo onde os dados são tão valiosos quanto o ouro, como podemos garantir que estão seguros?

Fundamentos de Cibersegurança

Tempest
[ACADEMY]
Conference

Cibersegurança não é apenas sobre ferramentas e tecnologias...

... é fundamentada em princípios básicos que orientam como protegemos nossos sistemas e dados

Triângulo da CIA

- Confidencialidade: garantir que as informações são acessíveis apenas para aqueles autorizados a vê-las
- Integridade: refere-se à precisão e consistência dos dados
- Disponibilidade: as informações e recursos devem estar acessíveis para usuários autorizados quando necessários

Fundamentos de Cibersegurança

Tempest
[ACADEMY]
Conference

Esses princípios são constantemente desafiados por ameaças como malware, phishing, ataques de negação de serviço, entre outros

A cibersegurança começa com a conscientização

Como você pode garantir a confidencialidade, integridade e disponibilidade em seu código e arquitetura de sistema?

Proteção de Dados - Legislações e Normas

Tempest
[ACADEMY]
Conference

À medida que a quantidade de dados que geramos e armazenamos cresce, também cresce a preocupação com a forma como esses dados são tratados.

GDPR - Regulamento Geral sobre a Proteção de Dados ['consentimento explícito' e 'direito ao esquecimento']

LGPD - Lei Geral de Proteção de Dados Pessoais [visa proteger a liberdade e a privacidade dos dados pessoais]

Exemplos de Impacto das Legislações?

Proteção de Dados - Legislações e Normas

Tempest
[ACADEMY]
Conference

Qual o impacto dessas leis na vida dos desenvolvedores?

Princípios de Privacidade por Design: significa considerar a privacidade e a proteção de dados em cada etapa do desenvolvimento

Isso inclui minimizar a coleta de dados, proteger os dados armazenados e garantir transparência na utilização dos dados.

Desenvolvimento Orientado a Dados

Tempest
[ACADEMY]
Conference

... refere-se à prática de usar dados como o principal fator orientador no processo de design, desenvolvimento e otimização de software

Desafios Associados?

É essencial pensar criticamente sobre como você coleta, armazena e utiliza os dados. Questões como 'Que dados são realmente necessários?', 'Como podemos protegê-los?' e 'Estamos em conformidade com as leis de proteção de dados?'

Riscos e Desafios na Segurança de Sistemas Orientados a Dados

Tempest
[ACADEMY]
Conference

Quando falamos de sistemas orientados a dados, enfrentamos uma gama única de desafios de segurança.

Esses desafios são amplificados pela escala, velocidade e variedade dos dados que estamos processando e armazenando

- Volume de Dados e Complexidade
- Desafios na Análise de Dados
- Conformidade Legal e Privacidade de Dados

Metodologias de Desenvolvimento de Software

Tempest
[ACADEMY]
Conference

O desenvolvimento de software era uma arte dominada por especialistas, com decisões muitas vezes baseadas em intuição e experiência passada

1960, nascimento da ES, começamos a ver uma abordagem mais sistemática e disciplinada, mas a coleta e análise de dados ainda eram limitadas pelas tecnologias disponíveis na época.

Internet e Big Data, Google e Amazon mostraram como insights baseados em dados poderiam ser usados para melhorar produtos e serviços

Hoje em dia podemos não apenas coletar uma grande quantidade de dados, mas também analisá-los em tempo real para informar decisões durante todo o ciclo de vida do software

Integração de Cibersegurança nas Metodologias Ágeis

Tempest
[ACADEMY]
Conference

- Como é a Cibersegurança em um Contexto Ágil?
- Práticas Ágeis e Segurança
  - Scrum e Kanban enfatizam a entrega contínua e a adaptabilidade
  - Avaliação contínua de riscos e a implementação de medidas de segurança
- DevSecOps, integra segurança no processo de desenvolvimento e operações.
  - Automação de testes de segurança, integração contínua e entrega contínua (CI/CD) com um enfoque em segurança

Integração de Cibersegurança nas Metodologias Ágeis

Tempest
[ACADEMY]
Conference

- Ferramentas e Tecnologias
  - scanners de segurança estática e dinâmica, sistemas de gerenciamento de vulnerabilidades e soluções de monitoramento de segurança contínua
- Cultura de Segurança
  - promover a conscientização sobre segurança e encorajar uma mentalidade proativa em relação à identificação e mitigação de riscos

DevSecOps - Segurança em DevOps

Tempest
[ACADEMY]
Conference

- Integração da segurança como um componente fundamental no processo de DevOps
  - significa incorporar práticas de segurança em cada fase do ciclo de vida de DevOps
  - Exemplo: ao integrar um scanner de segurança estática no pipeline de CI, cada commit de código é automaticamente verificado quanto a vulnerabilidades
- Benefícios do DevSecOps
  - aumenta a eficiência e a velocidade do desenvolvimento
- Desafios do DevSecOps
  - garantir que toda a equipe esteja alinhada com as práticas de segurança

Testes de Segurança no Desenvolvimento de Software

Tempest
[ACADEMY]
Conference

- Testes Estáticos (SAST, *Static application security testing*)
- Testes Dinâmicos (DAST, *Dynamic application security testing*)
  - OWASP ZAP ou Burp Suite são comumente utilizadas para DAST
- Testes de Penetração
  - vão além da identificação automatizada de vulnerabilidades, incluindo uma abordagem mais exploratória e manual

Testes de Segurança no Desenvolvimento de Software

Tempest
[ACADEMY]
Conference

- Integração com o Ciclo de Desenvolvimento através da implementação de pipelines de CI/CD
- Um exemplo prático é uma organização que implementa testes SAST no início do ciclo de desenvolvimento e testes DAST e de penetração nas fases de homologação e pré-lançamento.
  - Isso ajuda a garantir que as vulnerabilidades sejam identificadas e corrigidas o mais cedo possível

Gerenciamento de Dados e Privacidade

Tempest
[ACADEMY]
Conference

Envolve não apenas a proteção contra acessos não autorizados, mas também a garantia de que a privacidade dos usuários seja mantida

Práticas de Gerenciamento de Dados ['Privacidade por Design' é fundamental]

- classificação de dados
- o controle rigoroso de acesso
- implementação de políticas de retenção de dados

- Conformidade com as Leis de Proteção de Dados

Proteção de APIs e Interfaces de Dados

Tempest
[ACADEMY]
Conference

Fundamentais na arquitetura de software moderna

Riscos Comuns em APIs [ataques de injeção, exposição de dados sensíveis, ataques man-in-the-middle, entre outros]

Práticas de Segurança para APIs

i. autenticação forte, geralmente com tokens Oauth
ii. controle rigoroso de acesso
iii. limitação de taxa
iv. monitoramento contínuo para detectar atividades suspeitas

Proteção de APIs e Interfaces de Dados

Tempest [ACADEMY] Conference

- Exemplo?
  - Strava expôs inadvertidamente localizações de bases militares secretas devido a dados de GPS compartilhados publicamente através de sua API
- Autenticação e Autorização
- Gerenciamento de API [Apigee, AWS API Gateway], fornece camadas adicionais de segurança

Casos de Uso e Melhores Práticas

Tempest
[ACADEMY]
Conference

Caso de Uso 1: Sistema Bancário [autenticação multifatorial e criptografia de dados]

Caso de Uso 2: Comércio Eletrônico [SSL/TLS para transmissões seguras e sistemas de detecção de fraude]

Caso de Uso 3: Saúde e Telessaúde [proteção de informações de saúde é regulamentada, VPNs e criptografia de ponta a ponta]

Melhores Práticas na Indústria

- Realização regular de testes de penetração, adoção da política de menor privilégio para acesso a dados e sistemas, e a implementação de um plano de resposta a incidentes]

Ferramentas e Tecnologias Emergentes

Tempest
[ACADEMY]
Conference

- Inteligência Artificial e Machine Learning
  - Darktrace: monitoramento de rede e detecção de anomalias
- Blockchain para Segurança de Dados
  - registros imutáveis e descentralizados podem ser utilizados para proteger dados sensíveis e garantir a integridade das transações
- Computação Quântica e Segurança
  - quebrar algoritmos criptográficos atuais; criar formas de criptografia praticamente inquebráveis
- Automação e Orquestração de Segurança
  - SOAR (Security Orchestration, Automation, and Response), respostas mais rápidas e eficientes

Preparando Equipes para a Segurança de Dados

Tempest
[ACADEMY]
Conference

A segurança de dados não é apenas uma questão técnica; é também uma questão de cultura organizacional

Treinamento e Conscientização Contínuos

Incorporação de Segurança no Ciclo de Vida do Desenvolvimento

Ferramentas de Colaboração e Automação

Promoção de uma Mentalidade de Segurança

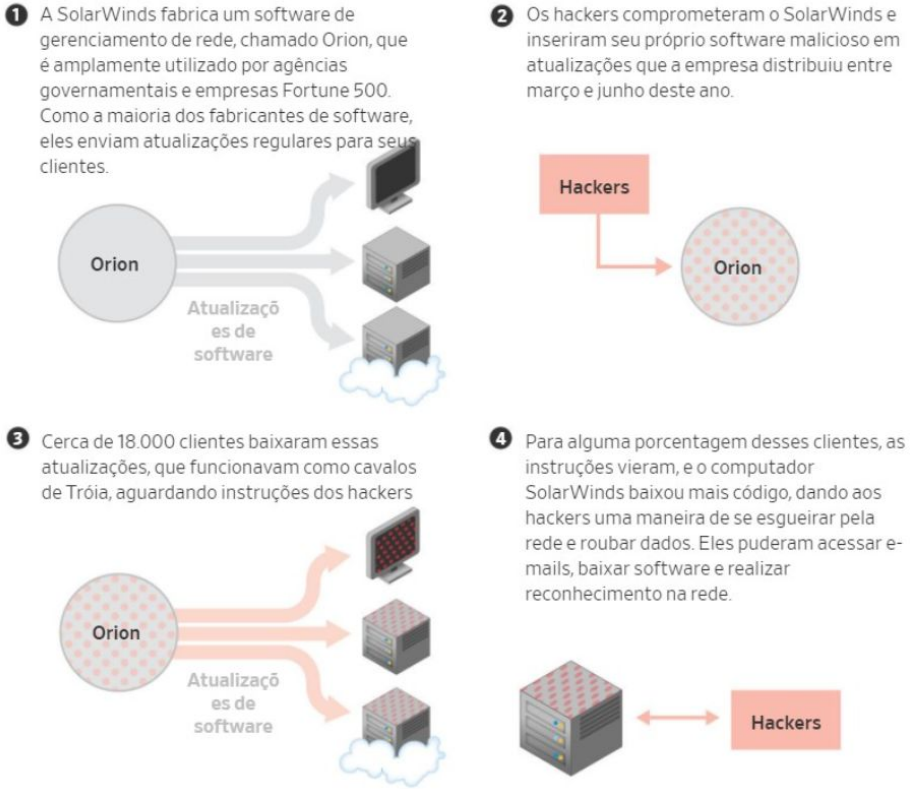
Desafios Futuros e Tendências

Tempest
[ACADEMY]
Conference

- Aumento de Ataques Cibernéticos Mais Sofisticados
  - Com a evolução da IA e do machine learning, esperamos ver ataques mais complexos
  - Por exemplo, ataques que utilizam IA para imitar comportamentos humanos, tornando mais difícil sua detecção
- Privacidade de Dados e Regulamentações
- Impacto da Computação Quântica
- Internet das Coisas (IoT) e Segurança
  - Mais dispositivos estarão conectados à internet, aumentando a superfície de ataque

Ataque a SolarWinds

Tempest
[ACADEMY]
Conference



O ataque começou com a inserção de um backdoor em uma atualização de software da SolarWinds, uma empresa que desenvolve software para gerenciamento de redes. Esse backdoor permitiu aos atacantes acessar redes de organizações que usavam o software

Este incidente nos ensinou sobre a importância da segurança na cadeia de suprimentos de software. Destaca a necessidade de verificações rigorosas de segurança, não apenas no próprio código, mas também em componentes de terceiros

Fonte: Minuto da Segurança / SolarWinds

Conclusão

Como a Inteligência Artificial, em especial os LLMs, podem ser usados para melhorar a cibersegurança, e quais são os riscos potenciais associados ao seu uso neste contexto?

De que forma as metodologias de desenvolvimento ágil podem integrar a cibersegurança de maneira eficaz, sem comprometer a velocidade e a flexibilidade que caracterizam estas metodologias?

Referências e Leituras Recomendadas

'The Art of Invisibility' de Kevin Mitnick para uma visão prática sobre segurança e privacidade online

Para uma abordagem mais técnica, 'Applied Cryptography' de Bruce Schneier

'Security and Privacy in Internet of Things (IoTs): Models, Algorithms, and Implementations' aborda os desafios de segurança no contexto de IoT

Sites como SecurityWeek e Krebs on Security, blog do Bruce Schneier

Integrando Cibersegurança e Proteção de Dados nas Metodologias de Desenvolvimento de Software Orientado a Dados

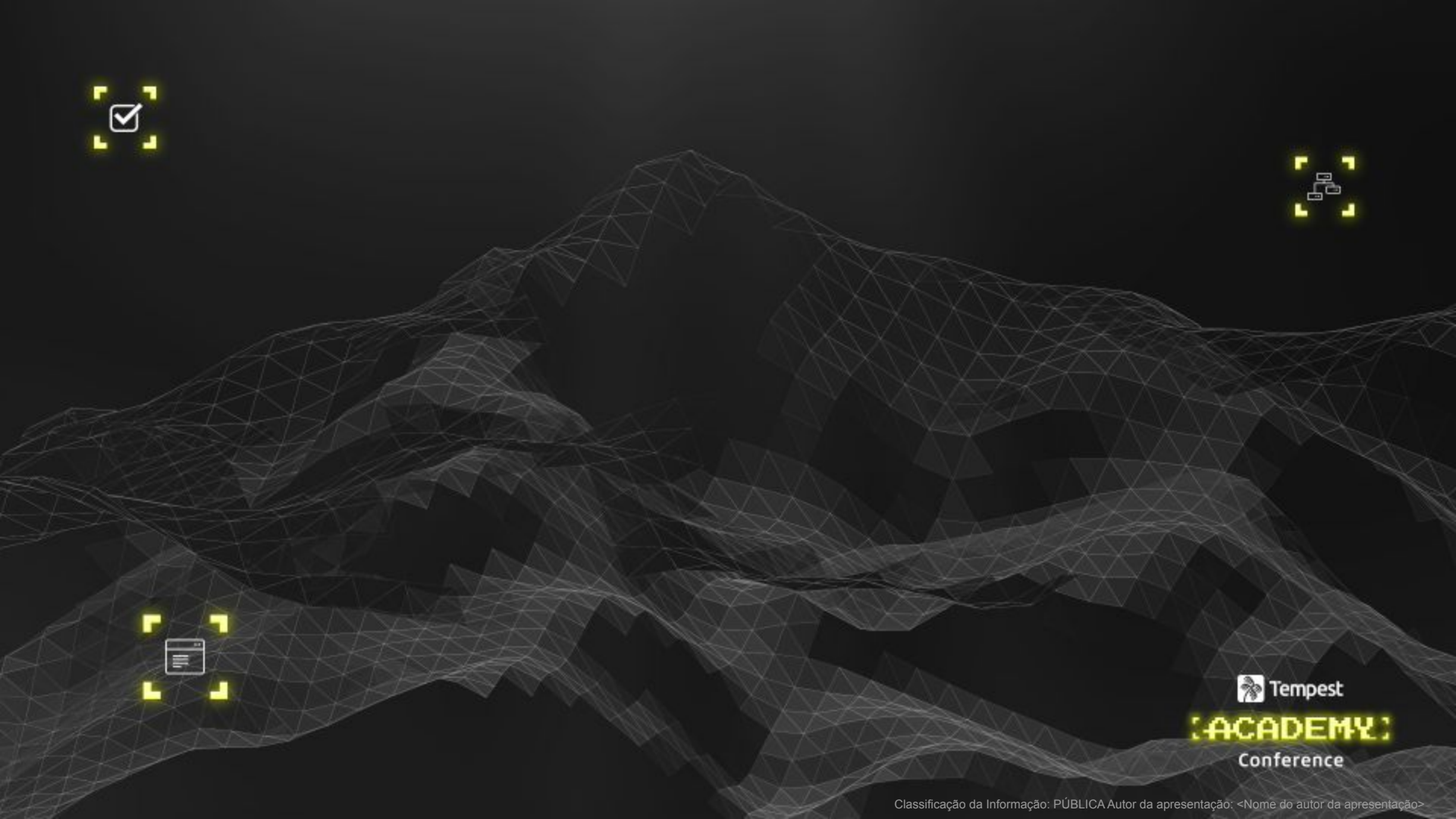
Desenvolvendo Software Seguro em uma Era Data-Driven

por Vinicius Cardoso Garcia, PhD

Professor Associado, Cin @ UFPE

Classificação da Informação: PÚBLICA Autor da apresentação: <Nome do autor da apresentação>

Classificação da Informação: PÚBLICA Autor da apresentação: <Nome do autor da apresentação>



Classificação da Informação: PÚBLICA Autor da apresentação: <Nome do autor da apresentação>