VANTICO

vantico.com.br

Segurança em **Supply Chain** (Cadeia de Suprimentos)

Quem sou eu

Analista de Segurança na Fiotec/Fiocruz;

Tecnólogo em Análise e Desenvolvimento de Sistemas;

Mestre em Ciências pela USP;

Criador de Conteúdo sobre Segurança de Aplicações.

↘ Somos especialistas em *** Pentest e Cibersegurança.

O que testamos

- Web
- API
- Networks
- Mobile
- Cloud

Como testamos

Penetration Testing

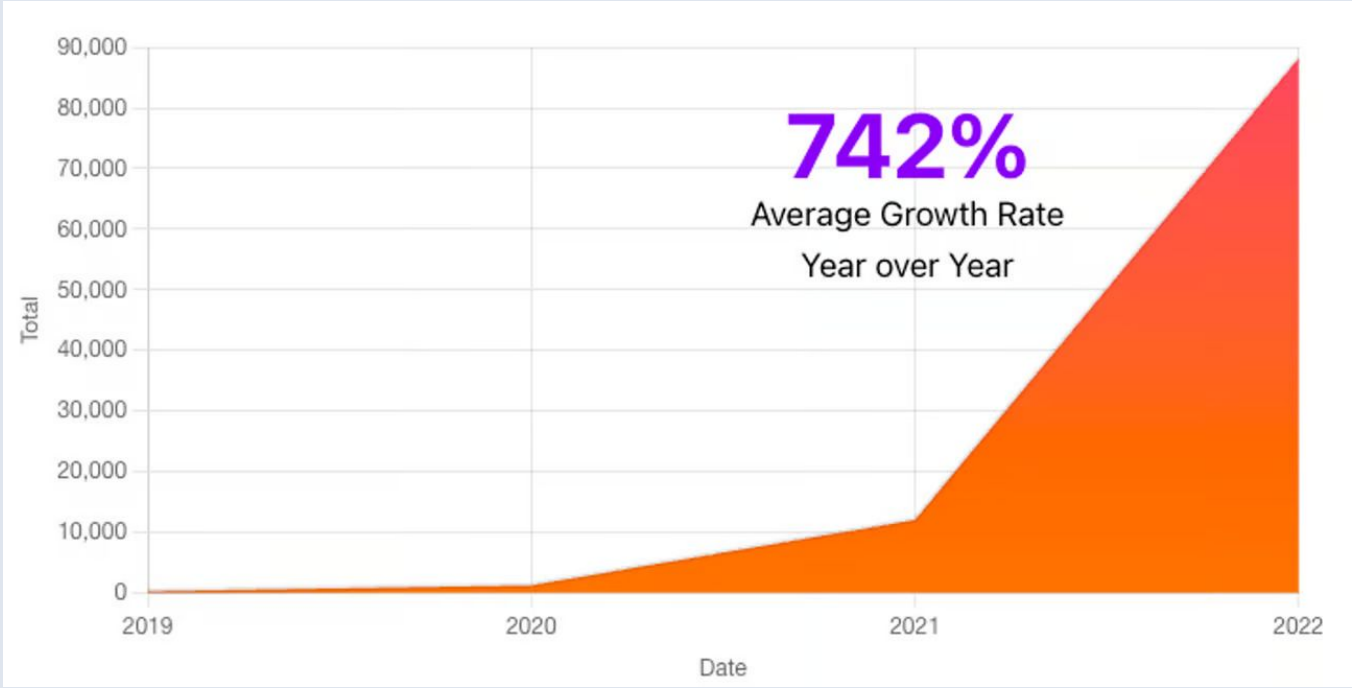
Especializados	Missões
Compliance	Novas telas
M&A Due Diligence	Novos endpoints
Customizados	IPs públicos
	Revisão de código
	Testes de CVE

- Revisão Segura de Código
- Modelagem de Ameaças
- Operações de Red Team
- Engenharia Social via Phishing & Whatsapp
- Testes de IOT e Dispositivos
- Threat Intelligence / OSINT

Por que testamos

- Integrar com SDLC
- Melhorar o Programa de Segurança Ofensiva
- Reduzir a Superfície de Ataque

Aumento de Ataques de Cadeia de Suprimentos de Software



Sonatype, 2023.

Cibersegurança em 2024

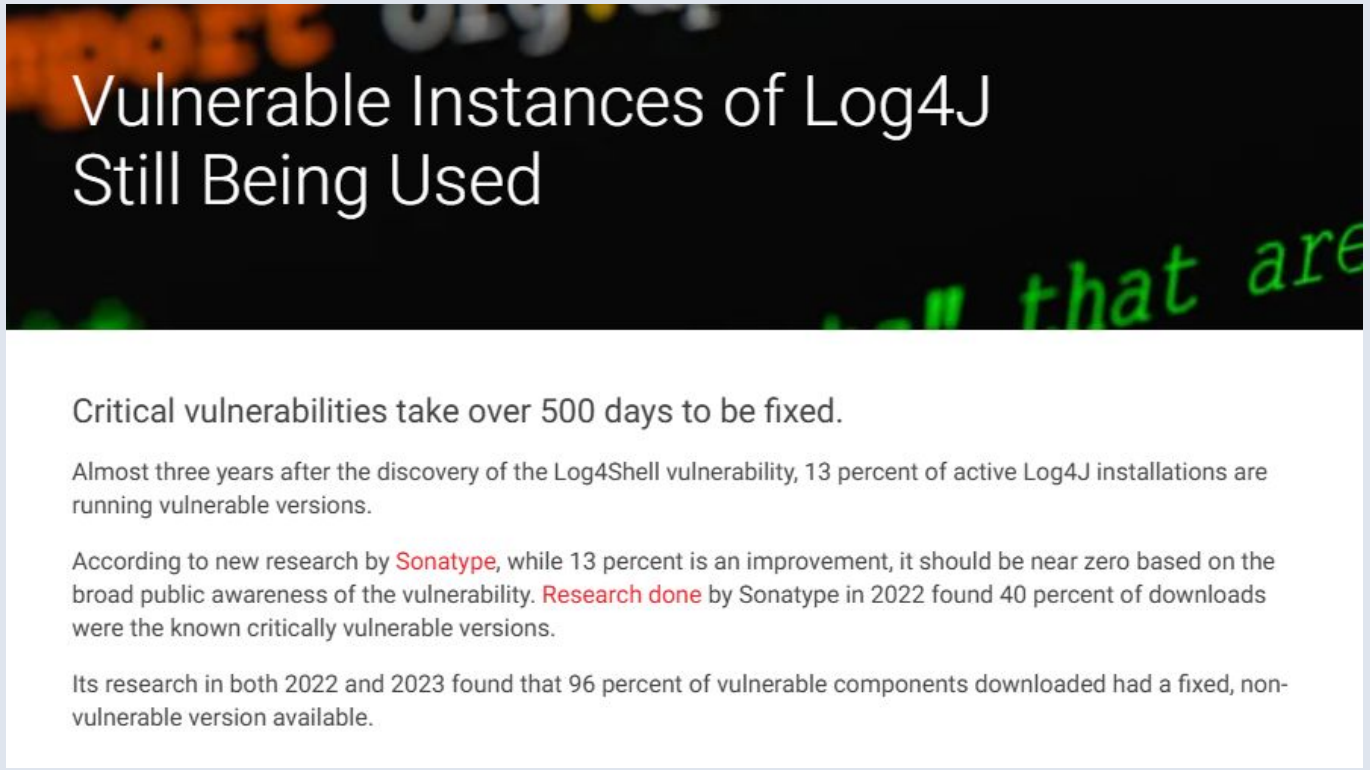
05. Ataques de Supply-Chain & Third Party

Os ataques de Supply-Chain & Third Party continuaram a aterrorizar as organizações em 2024, e duas situações deixaram isso bem evidente[20].

Falha no CrowdStrike
Uma falha de atualização no sensor de segurança CrowdStrike Falcon gerou um apagão nos sistemas que **afetou mais de 8 milhões de dispositivos – o pior da história.** Apesar de não ter sido um ataque criminoso, ele revela o potencial de impacto e destruição que esse tipo de situação pode causar[21].

Backdoor no XZ Utils
O mundo chegou muito perto de vivenciar um incidente no XZ Utils, uma ferramenta de compressão de arquivos e biblioteca de códigos. Isso porque um backdoor escondido foi encontrado acidentalmente por um engenheiro, em um software que faz parte do sistema operacional Linux. **Esse poderia ter sido um dos piores ataques cibernéticos à cadeia de suprimentos da história[22].**

Caso antigo que ainda continua vigente: Log4J



Vulnerable Instances of Log4J Still Being Used

Critical vulnerabilities take over 500 days to be fixed.

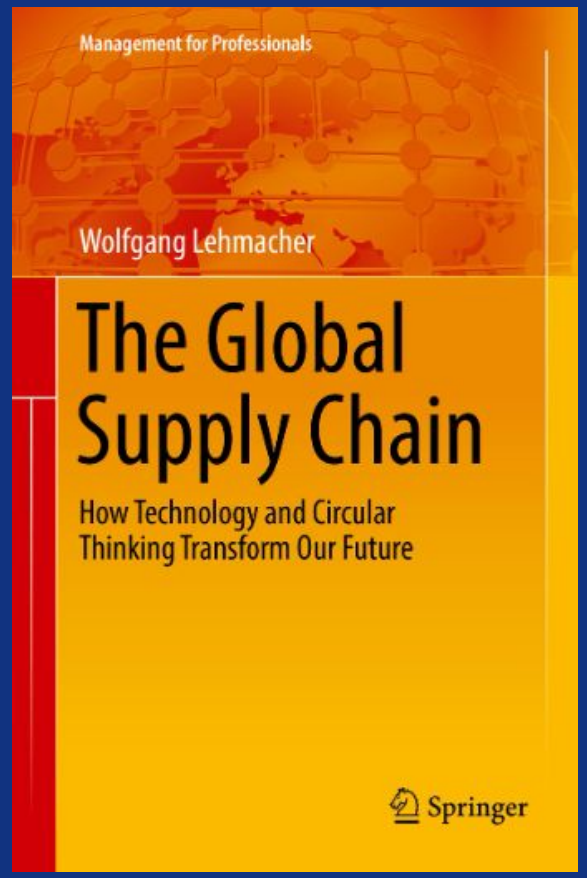
Almost three years after the discovery of the Log4Shell vulnerability, 13 percent of active Log4J installations are running vulnerable versions.

According to new research by Sonatype, while 13 percent is an improvement, it should be near zero based on the broad public awareness of the vulnerability. Research done by Sonatype in 2022 found 40 percent of downloads were the known critically vulnerable versions.

Its research in both 2022 and 2023 found that 96 percent of vulnerable components downloaded had a fixed, non-vulnerable version available.

SC Magazine UK, 2024.

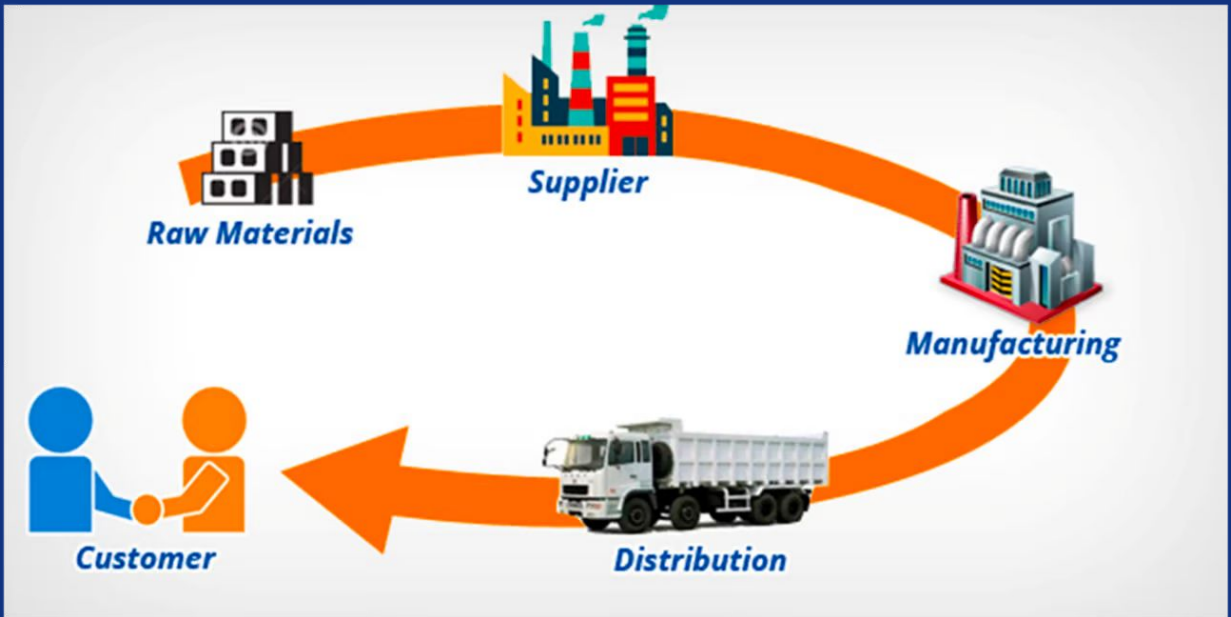
Mas o que é uma Cadeia de Suprimentos?



The Global Supply Chain
How Technology and Circular Thinking Transform Our Future

© 2017

Software Supply Chain (SSC)



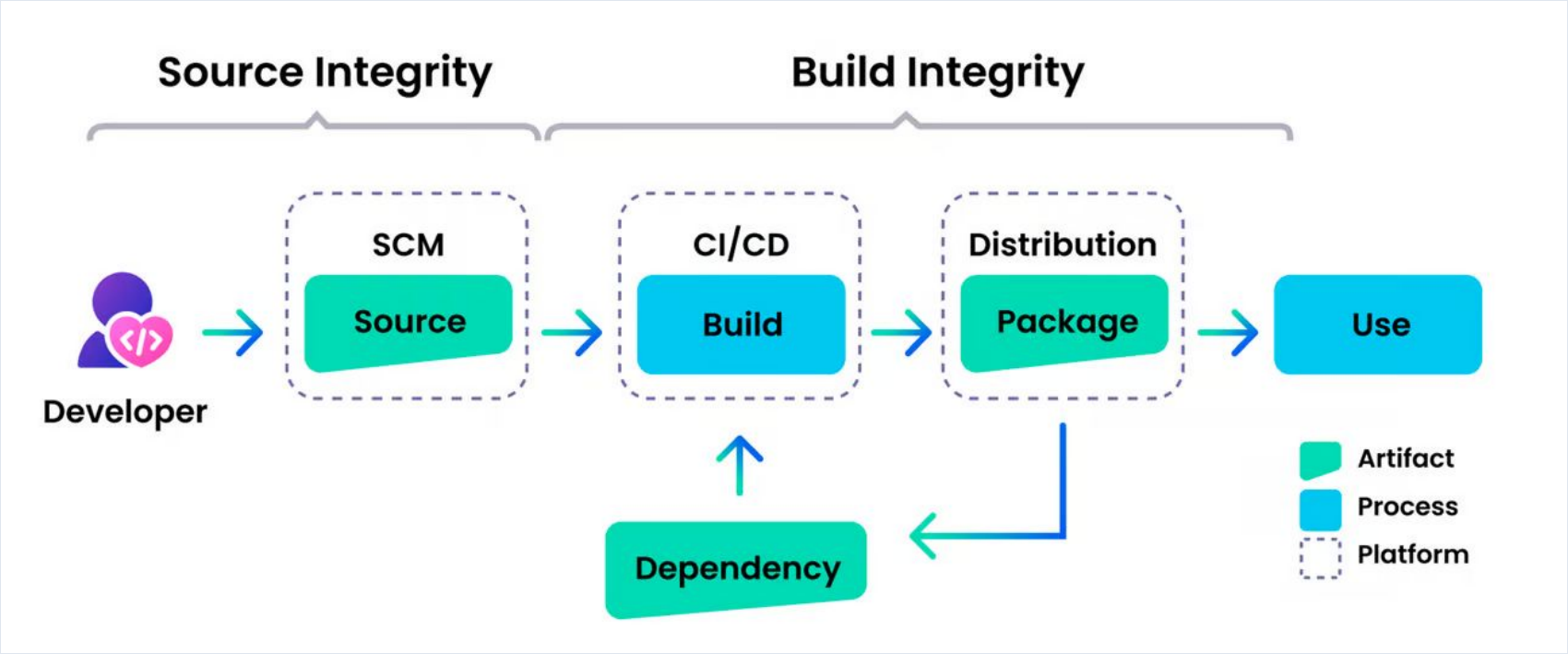
Fonte: Gibler, Odum (2023)

- Pode ser vista como uma cadeia de suprimentos tradicional onde as matérias-primas são adquiridas, montadas e transformadas em produtos acabados antes de serem distribuídas a varejistas ou clientes.
- Essa estrutura também se aplica ao funcionamento da cadeia de suprimentos de software.

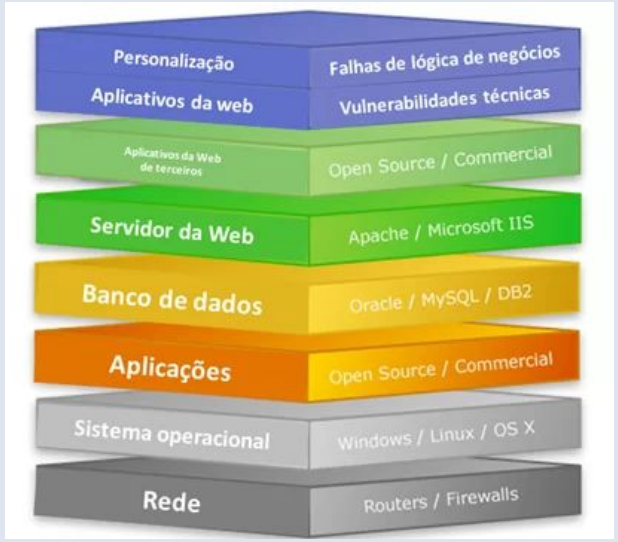
De acordo com o NIST a **cadeia de suprimentos de software envolve um ecossistema complexo, globalmente distribuído e interconectado, que inclui várias entidades e múltiplos níveis de terceirização**. Este ecossistema abrange tecnologias de informação, comunicação e operação, e envolve todas as etapas do ciclo de vida de um sistema, desde o design, desenvolvimento, distribuição, implantação, aquisição, manutenção até a destruição.

NIST Cybersecurity Supply Chain Risk Management

SSC nas fases de Desenvolvimento de Software



TechnologyDecisions, 2022.

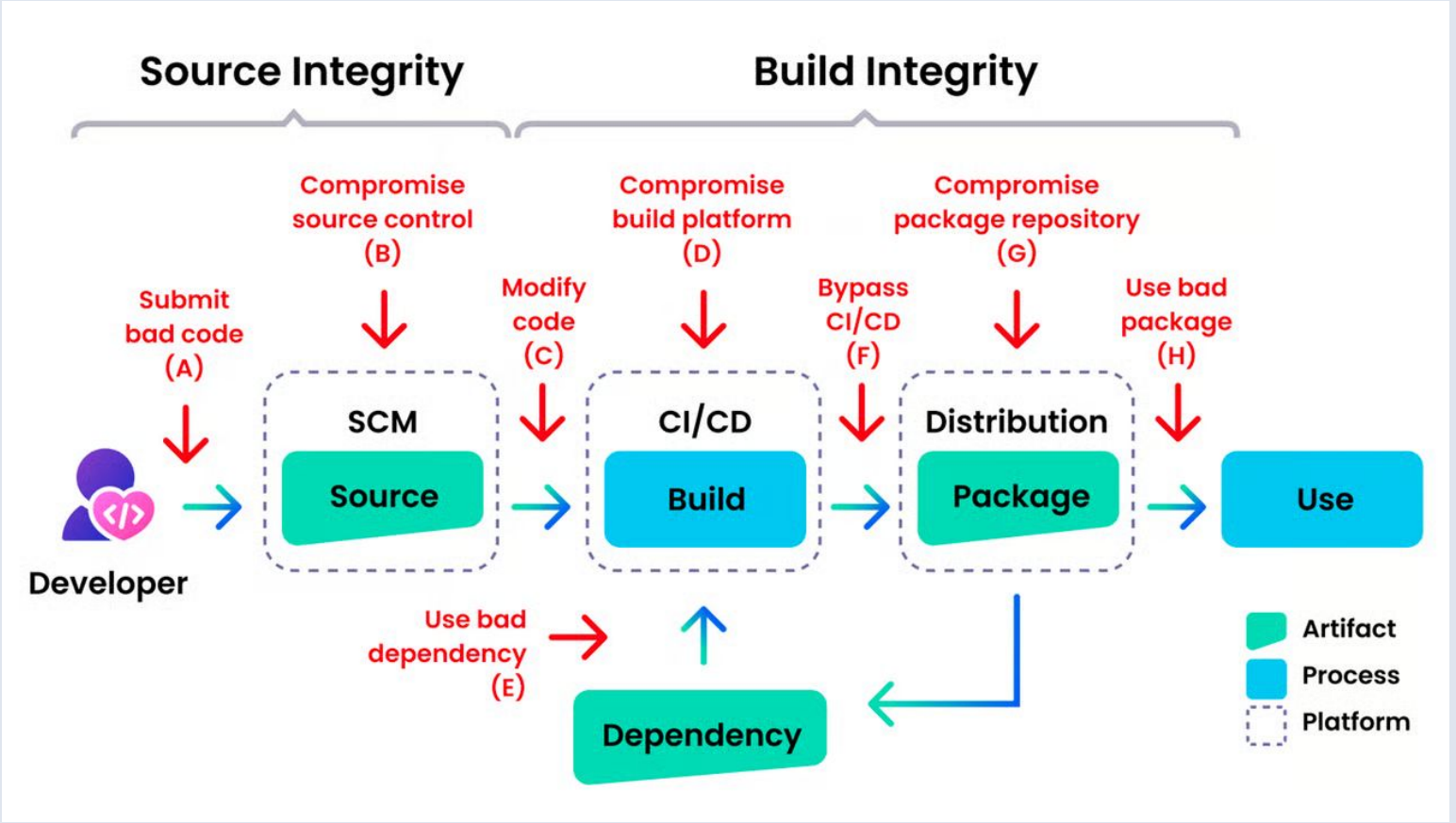


E os riscos na SSC?

Importância da visão em camadas

- De acordo com o guia do NIST, um ataque SSC ocorre quando uma parte mal-intencionada adultera etapas, artefatos ou atores dentro da cadeia de suprimentos de software.
- O objetivo é comprometer os consumidores de um artefato de software no futuro.
- Para realizar um ataque SSC, um invasor precisa subverter, remover ou introduzir uma etapa no processo SSC.
- Essas ações modificam o produto de software resultante.

Áreas que um atacante pode visar a SSC

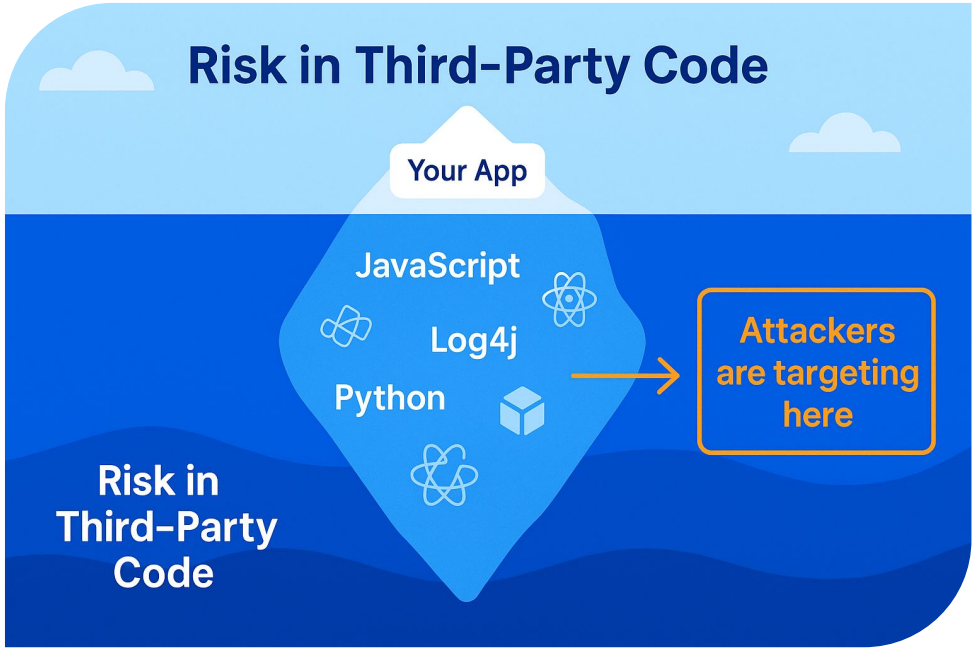


TechnologyDecisions, 2022.

Riscos de Segurança na Cadeia de Suprimentos de Software

Criação do código fonte

- O código é o principal componente da cadeia de suprimentos de software, podendo ser desenvolvido internamente ou de fontes externas.
- Durante alterações no código-fonte em sistemas de controle de versão (VCS), há risco de agentes mal-intencionados modificarem o código ou os repositórios.
- Vazamentos de código-fonte, como o ataque de 2022 ao Azure DevOps da Microsoft pelo grupo Lapsus$, destacam a importância de proteger sistemas de gerenciamento de código-fonte (SCM) como GitHub e GitLab.
- Ferramentas como Visual Studio Code (VS Code) e suas extensões de código aberto podem comprometer a segurança do IDE, permitindo roubo de dados ou injeção de malware.
- Código open-source, além copia e cola de códigos pela internet.

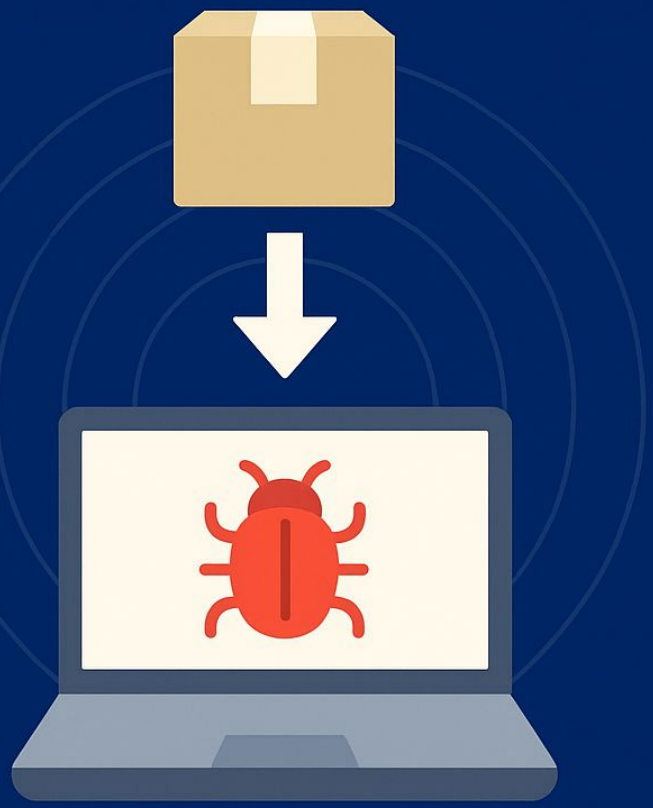


Visual Studio Code

GitHub

Por que atacar diretamente o software da empresa se sei que ela vai baixar pacotes de um componente confiando que é legítimo?

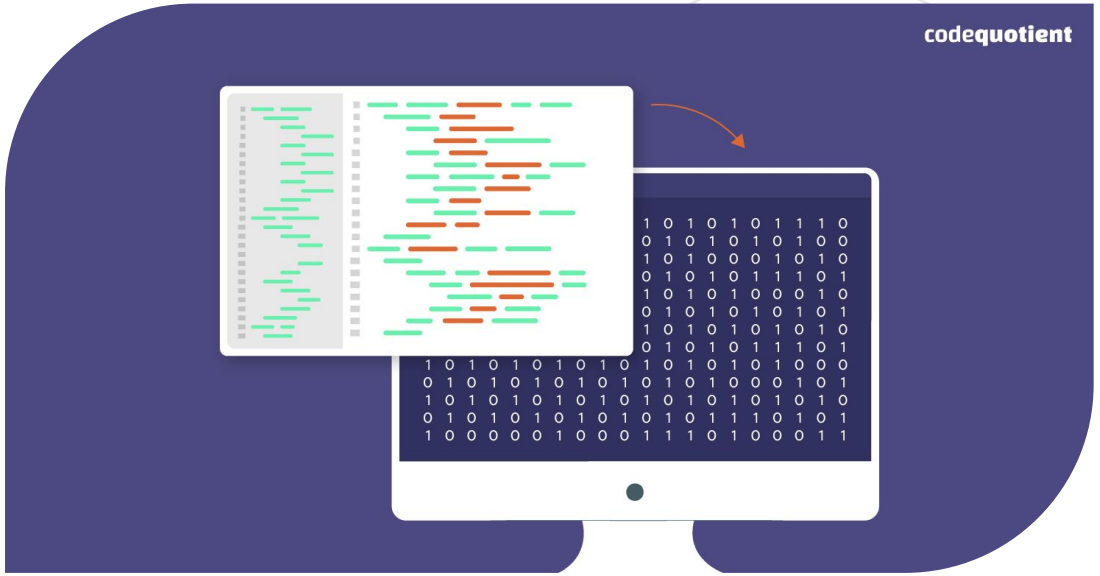
Técnica foi usada em ataques como o do SolarWinds (inserção de backdoor em update de software).



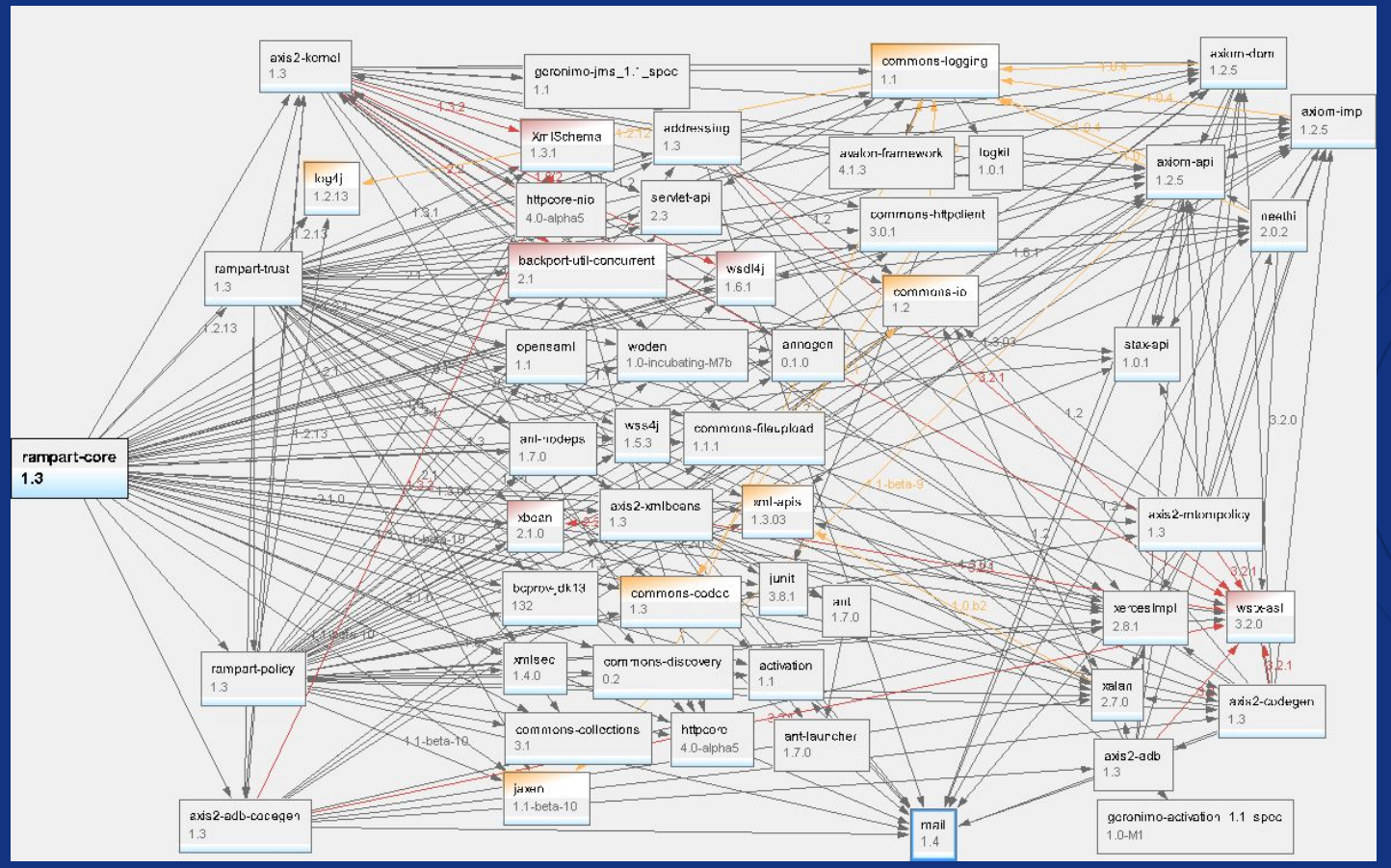
Riscos de Segurança na Cadeia de Suprimentos de Software

Estágio de compilação

- Compilação: transforma código-fonte em binários, executáveis ou bibliotecas.
- Integrações como autenticação e APIs representam riscos. Violações ou indisponibilidade podem causar efeito cascata.
- Ataques podem ocorrer durante a criação, afetando dependências, pipelines de CI/CD, contêineres e registros, introduzindo vulnerabilidades no software.



O cuidado com as dependências!



Exemplo de Dependências em Java

Dependências transitivas e as diretas/indiretas

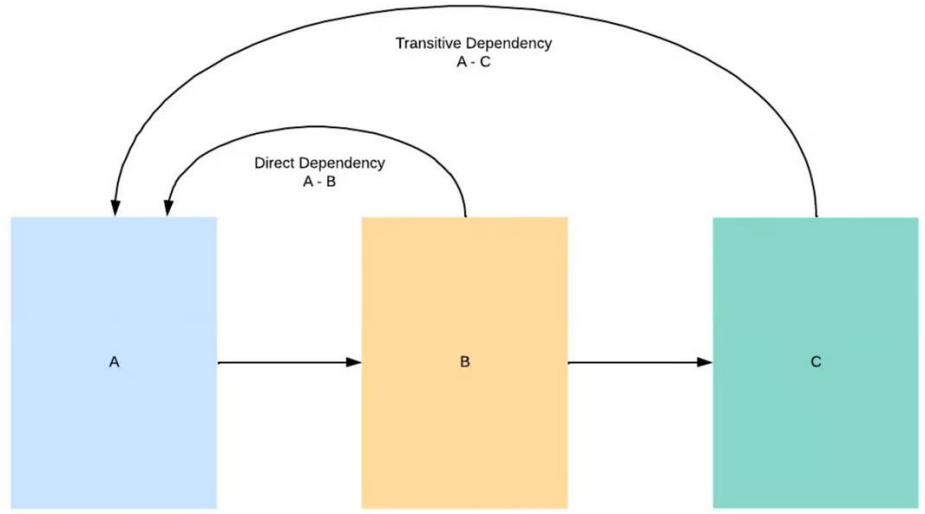


Figure I : Direct dependency vs Transitive dependency

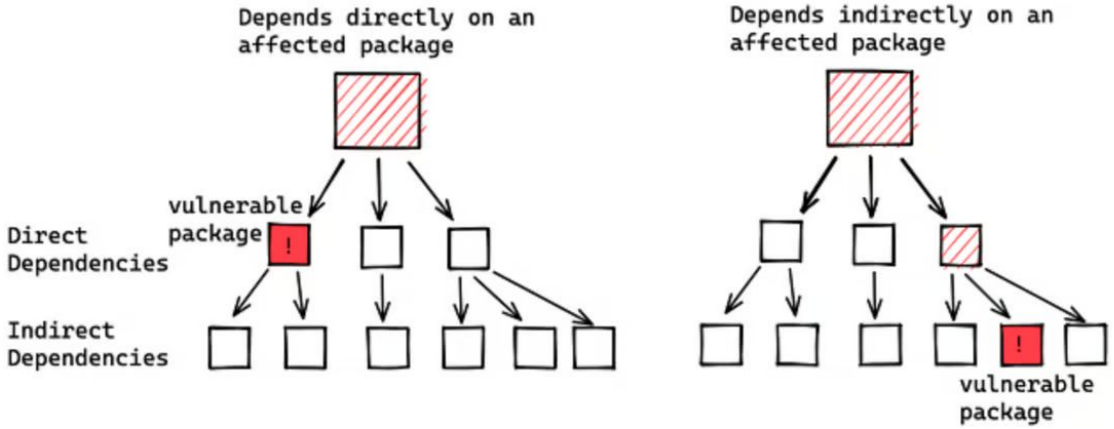


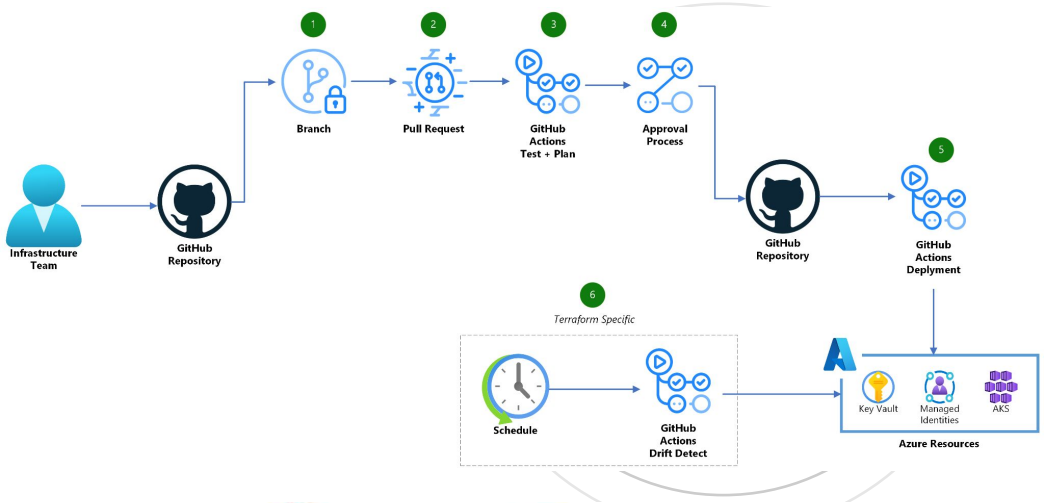
Figure II : Direct vulnerabilities vs Indirect(transitive) vulnerabilities [4]

Fonte: Rajapaksha, 2022.

Riscos de Segurança na Cadeia de Suprimentos de Software

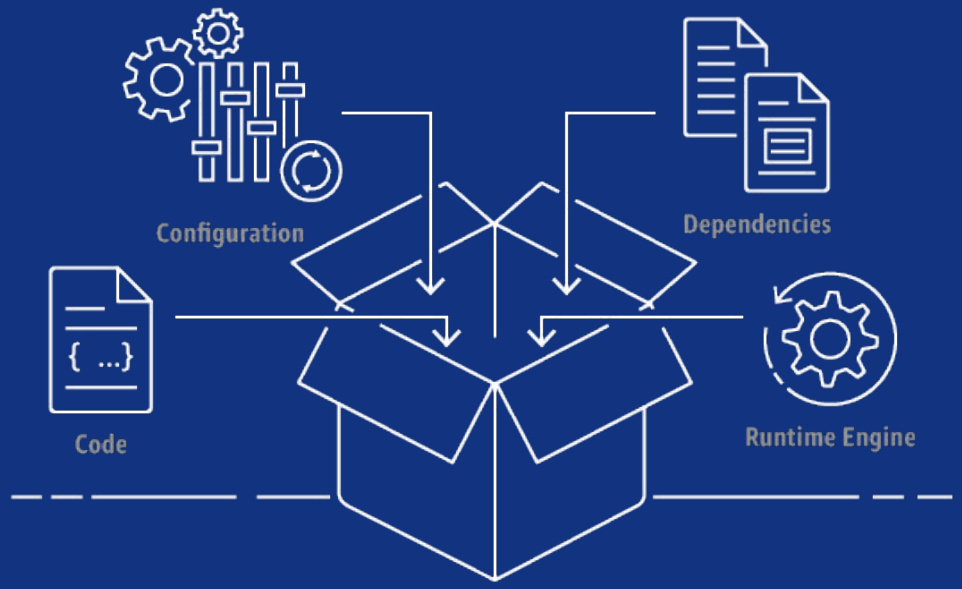
CI/CD Pipeline

- Um pipeline de CI/CD automatiza o teste e a implantação de alterações de código, garantindo atualizações contínuas e consistentes com mínima intervenção manual. Soluções populares incluem GitHub Actions, Azure DevOps...
- Mesmo com testes rigorosos, erros dos desenvolvedores podem introduzir vulnerabilidades no código, seja ele próprio ou de terceiros, ou em sistemas de compilação inseguros.
- Invasores podem atacar pipelines de CI/CD para inserir vulnerabilidades ou códigos maliciosos. Se os artefatos de compilação não forem protegidos, podem ser adulterados, levando a implantações não autorizadas.



Azure DevOps

SSC e Containers



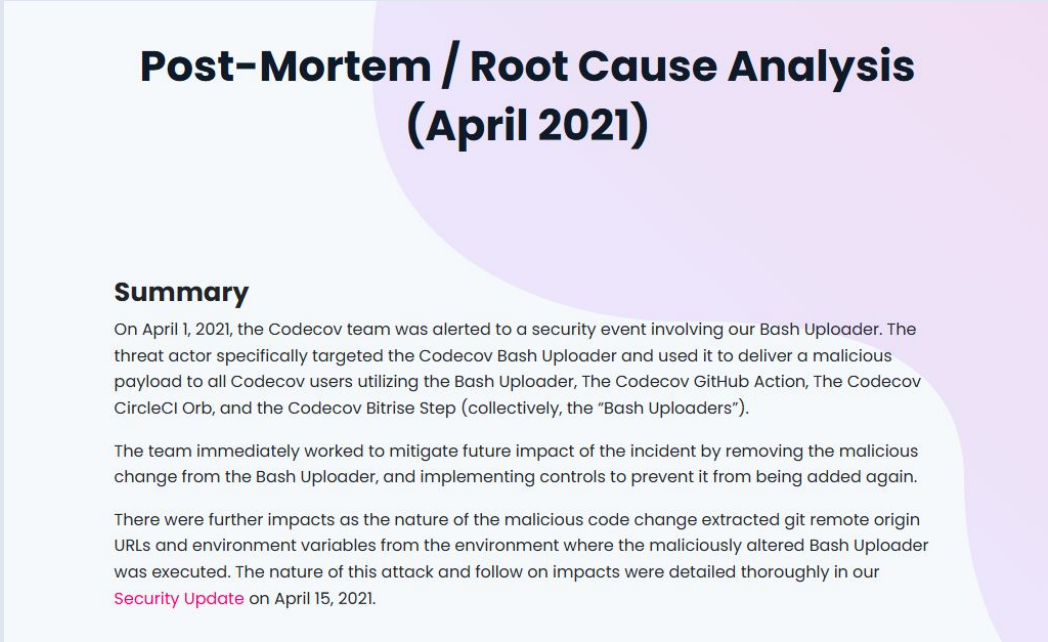
- Desafios em torno de muitas imagens de contêiner sem informações de proveniência, dificultando a verificação de onde vieram ou se alguém as adulterou.
- Invasores que obtêm credenciais para registros de contêiner, como Docker Hub ou Elastic Container Registry (ECR), podem carregar imagens mal-intencionadas, levando a violações de segurança.

Riscos de Segurança na Cadeia de Suprimentos de Software

Packaging & Deployment

- A etapa de empacotamento e implantação é crítica na SSC porque é onde o software é preparado para distribuição e uso final.
- Durante o empacotamento, invasores podem adulterar o processo, por exemplo, usando gerenciadores de pacotes como yarn para inserir código malicioso ou alterar metadados. Isso pode levar a distribuições de software comprometidas.

Credenciais vazadas foram usadas para fazer upload de artefatos maliciosos: CodeCov



Post-Mortem / Root Cause Analysis (April 2021)

Summary

On April 1, 2021, the Codecov team was alerted to a security event involving our Bash Uploader. The threat actor specifically targeted the Codecov Bash Uploader and used it to deliver a malicious payload to all Codecov users utilizing the Bash Uploader, The Codecov GitHub Action, The Codecov CircleCI Orb, and the Codecov Bitrise Step (collectively, the "Bash Uploaders").

The team immediately worked to mitigate future impact of the incident by removing the malicious change from the Bash Uploader, and implementing controls to prevent it from being added again.

There were further impacts as the nature of the malicious code change extracted git remote origin URLs and environment variables from the environment where the maliciously altered Bash Uploader was executed. The nature of this attack and follow on impacts were detailed thoroughly in our Security Update on April 15, 2021.

Fonte: CodeCov, 2021

Por que esses riscos importam?

Uma única brecha na cadeia de suprimentos pode escalar para um incidente com grande impacto.

Investir na segurança da cadeia de suprimentos deve ser preventivo e estratégico!

Framework e Normativa de Referência

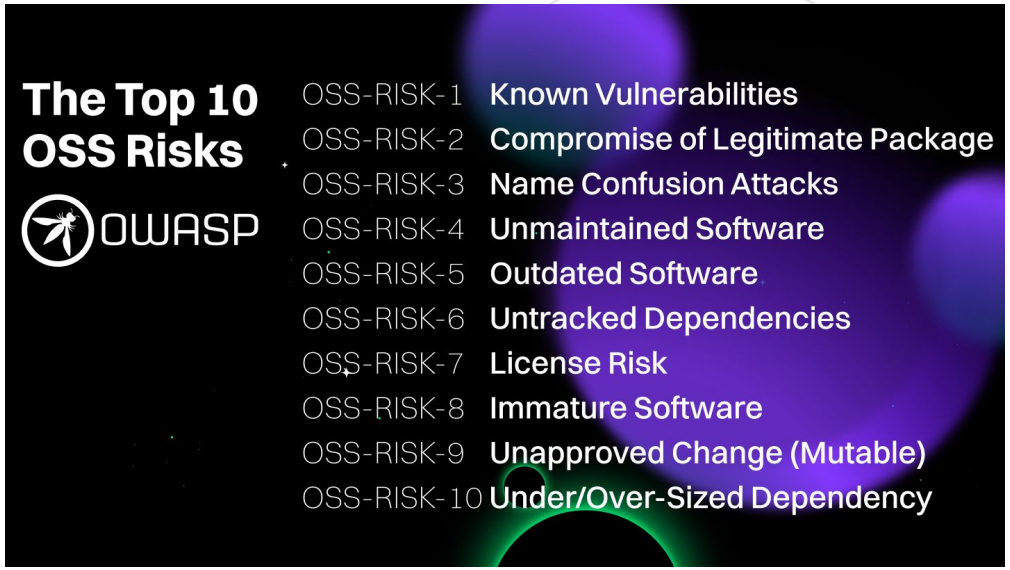
OWASP Software Component Verification Standard (SCVS)

- Um padrão da OWASP focado em reduzir riscos na supply chain de software, agrupando controles de segurança em 6 famílias:

- V1: Inventory
- V2: Software Bill of Materials (SBOM)
- V3: Build Environment
- V4: Package Management
- V5: Component Analysis
- V6: Pedigree and Provenance

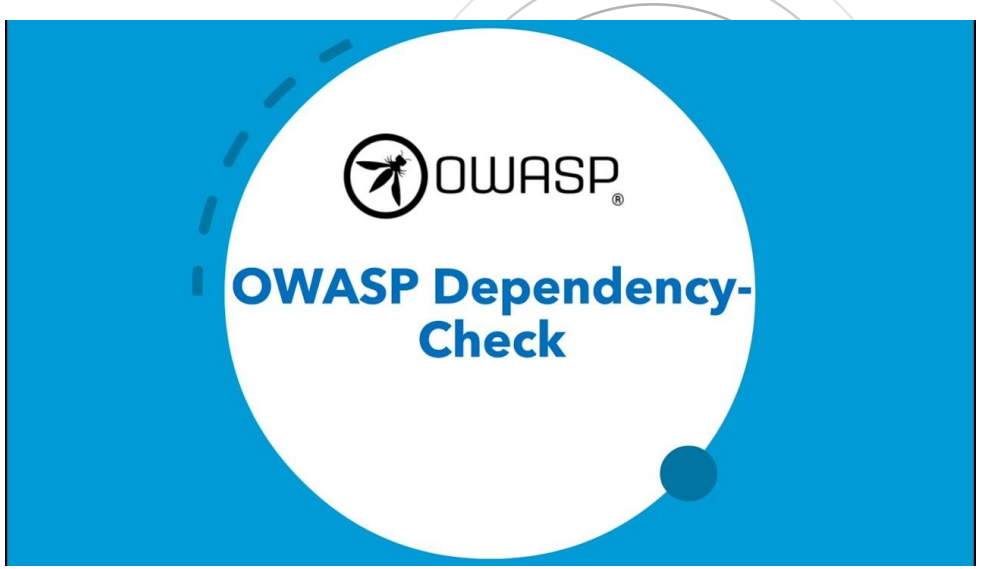
Práticas Recomendadas para Proteger a Cadeia de Suprimentos de Software

- Mantenha um inventário completo de todas as dependências de terceiros. Avalie a procedência de cada novo componente para evitar pacotes obscuros ou maliciosos.
- Baixe bibliotecas apenas de fontes oficiais e habilite verificações dos pacotes para garantir integridade, como assinaturas GPG ou checksums.
- Estabeleça critérios e um processo para introdução de novas dependências, incluindo verificação de licença, análise de vulnerabilidades e aprovação técnica. Documente a política e treine os desenvolvedores para segui-la.



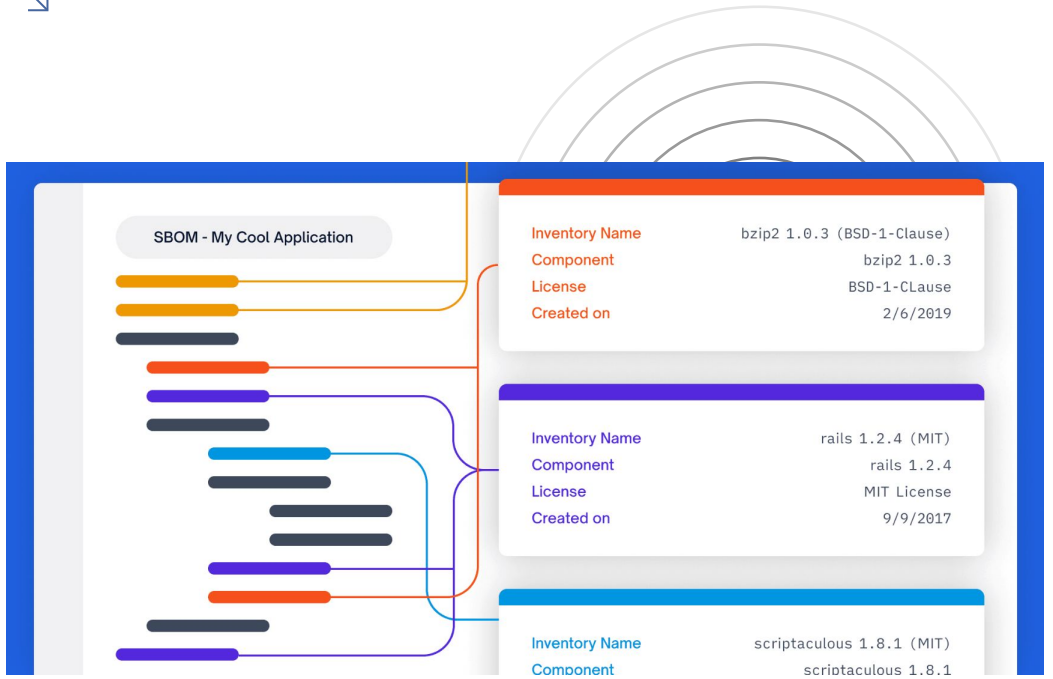
Práticas Recomendadas para Proteger a Cadeia de Suprimentos de Software

- Use ferramentas para monitorar atualizações e novas vulnerabilidades. Realize "health checks" periódicos nos principais pacotes para evitar riscos de projetos abandonados.
- Software Composition Analysis (SCA):
  - Utilize ferramentas automatizadas de SCA para escanear o projeto em busca de vulnerabilidades conhecidas e alertar sobre CVEs abertas. Integre esse processo ao CI para uma análise contínua.



SBOM (Software Bill of Materials)

- Uma SBOM é uma lista estruturada de todos os componentes e suas versões em um produto de software. Ela é gerada automaticamente durante o build e fornece transparência total da composição do software.
- Adote padrões industriais como SPDX ou CycloneDX para suas SBOMs. Muitas ferramentas de build e SCA já geram SBOMs, que devem ser versionadas e armazenadas junto com a release do software.
- SBOM permite identificar rapidamente se você é afetado por novas vulnerabilidades públicas, agilizando a resposta a incidentes de supply chain.
- Solicite SBOMs ao adquirir software de terceiros para verificar componentes e suas vulnerabilidades, aumentando a confiança na solução e estabelecendo visibilidade na cadeia.



Políticas de Fornecedores e Controle de Riscos

- Antes de contratar ou usar um software/serviço de terceiros, avalie o fornecedor sob o aspecto de segurança. Isso pode incluir questionários de segurança e análise de certificações como ISO 27001.
- Verifique se a empresa possui certificações relevantes e busque referências no mercado para garantir a confiabilidade do fornecedor.
- Fornecedores críticos exigem investigação mais profunda, como auditorias in loco e análise do histórico, enquanto fornecedores de risco baixo podem passar por um processo simplificado.

Melhore a **Segurança em Supply Chain** com a Vantico!

Quando contratar um Pentest?

Métricas para **Acompanhamento das correções de Vulnerabilidade**

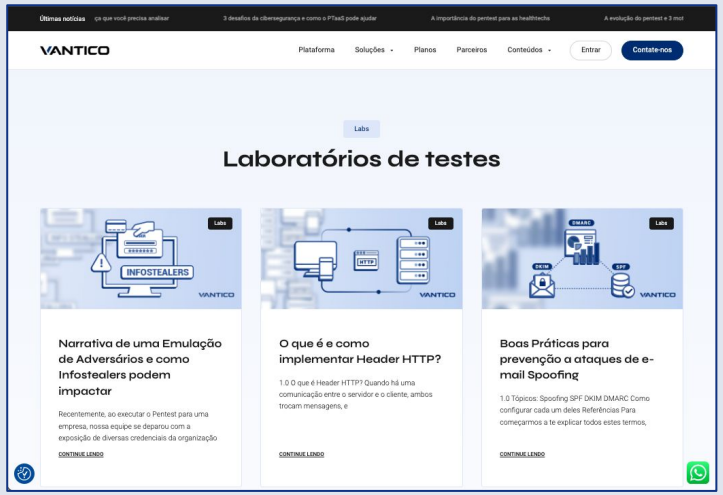
Recursos da **Vantico**

Insights do setor de nossos especialistas em segurança cibernética

Notícias e insights sobre o setor de segurança cibernética e tendências.

HTTPS://VANTICO.COM.BR/BLOG

HTTPS://VANTICO.COM.BR/LABS



Insights técnicos da Vantico

O Laboratório de testes é nossa área de P&D.

vantico.com.br

VANTICO

Vamos **transformar** os testes de segurança?

Kaique Bonato

kaique@vantico.com.br