TLP:CLEAR

Proposta de integração de controles de segurança baseados nos princípios *Zero Trust* em uma *cyber supply chain*

Thiago Melo Stuckert do Amaral

Orientador: Prof. Dr. João José Costa Gondim CIC/UnB, PPEE/UnB

31/07/2023

TLP:CLEAR

Apresentação pessoal

Graduação e Mestrado

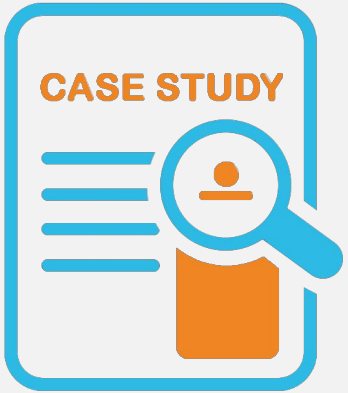
Órgãos e empresas

TLP:CLEAR

Agenda

Checklist de controles

Visualização do *gap*

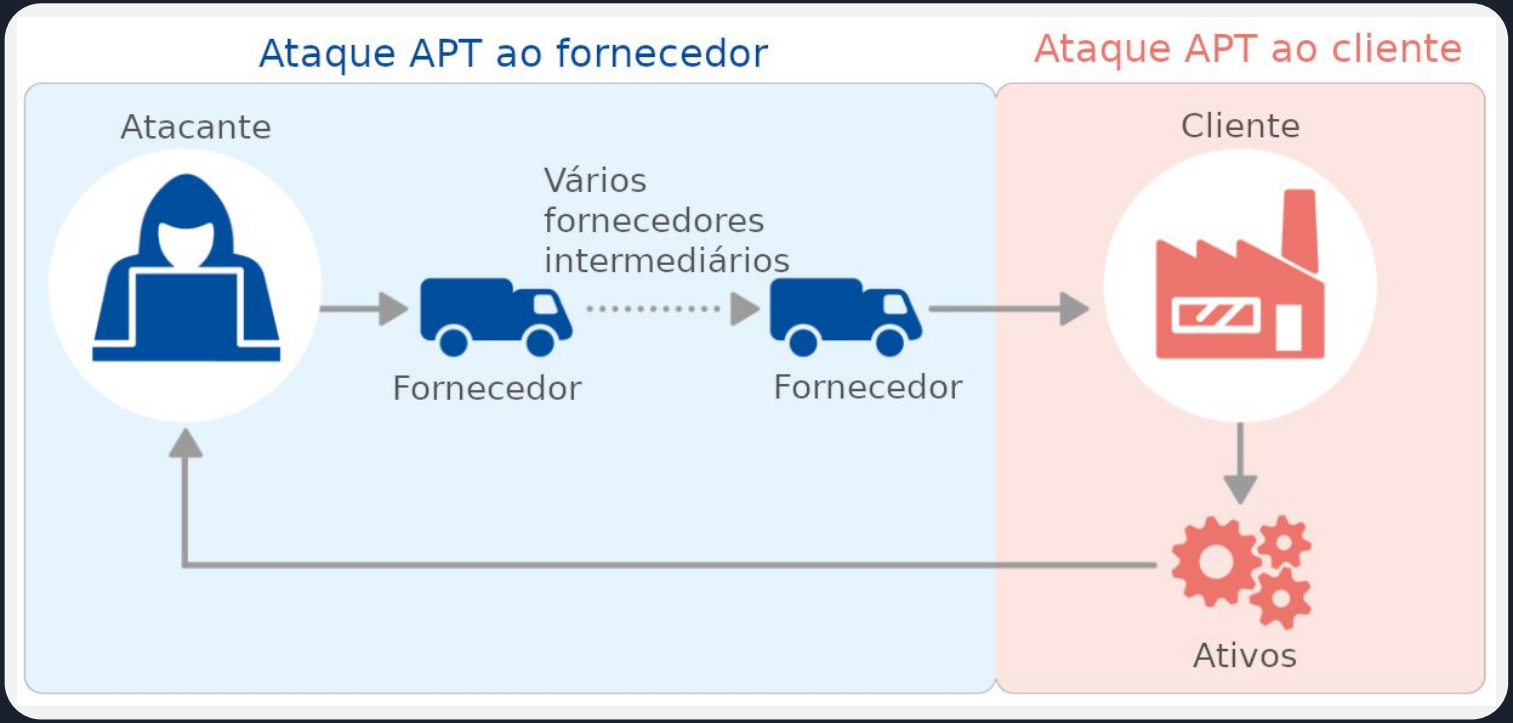


Estudos de caso

TLP:CLEAR

Supply chain

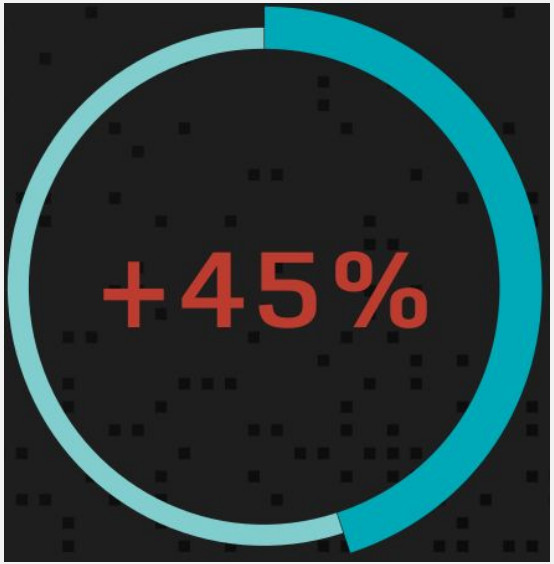
Modo de operação do ataque



Adaptado do relatório da ENISA *Threat Landscape for Supply Chain Attacks*.

TLP:CLEAR

Estimativa de organizações afetadas em 2025



Fonte: Gartner

TLP:CLEAR

Software Bill of Materials (SBOM)

Componentes do Volkswagen Golf Mk1

TLP:CLEAR

Software Bill of Materials (SBOM)

Resumos digitais (hashes) das Eleições 2022 – 1º e 2º turnos

Sistemas em ambiente PC

Nome do arquivo	Programa correspondente
pc1sis1	Subsistema de Instalação e Segurança
pc1TRAN	Transportador
pc1GEDA	Gerenciador de Dados, Aplicativos e Interface com a Urna Eletrônica
pc1CRIP	CriptoSevin
pc1HSFG	Hotswap Flash
pc1HOLO	Holocron
pc1SORT	Apoio ao Sorteio de Auditoria
pc1VOTA	Apoio à Auditoria de Votação

M:\aplic\setot\apps\transportador\prod\lib\jsr305-3.0.1.jar

M:\aplic\setot\apps\transportador\prod\lib\jta-1.1.jar

M:\aplic\setot\apps\transportador\prod\lib\junit-4.13.2.jar

M:\aplic\setot\apps\transportador\prod\lib\log4j-1.2.17.jar

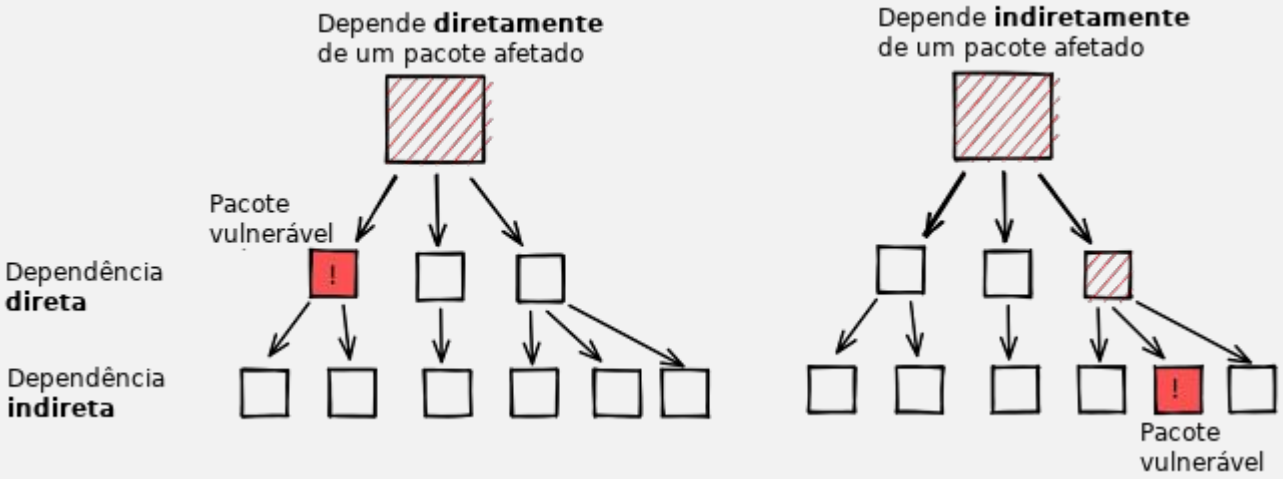
M:\aplic\setot\apps\transportador\prod\lib\log4j-over-slf4j-1.7.36.jar

M:\aplic\setot\apps\transportador\prod\lib\lombok-1.18.24.jar

Fonte: Portal do TSE

TLP:CLEAR

Dependências diretas vs indiretas



Adaptado de estudo do Google

TLP:CLEAR

Análise de repositórios de código-fonte

Dos **1.703** repositórios analisados pela Synopsys em 2022:

- **76%** do código dos repositórios era de **código aberto**;
- **89%** dos repositórios continham **código aberto sem atualização há mais de 4 anos**;
- **48%** dos repositórios possuíam **vulnerabilidades de alto risco**.

Fonte: *Open Source Security and Risk Analysis Report* 2023

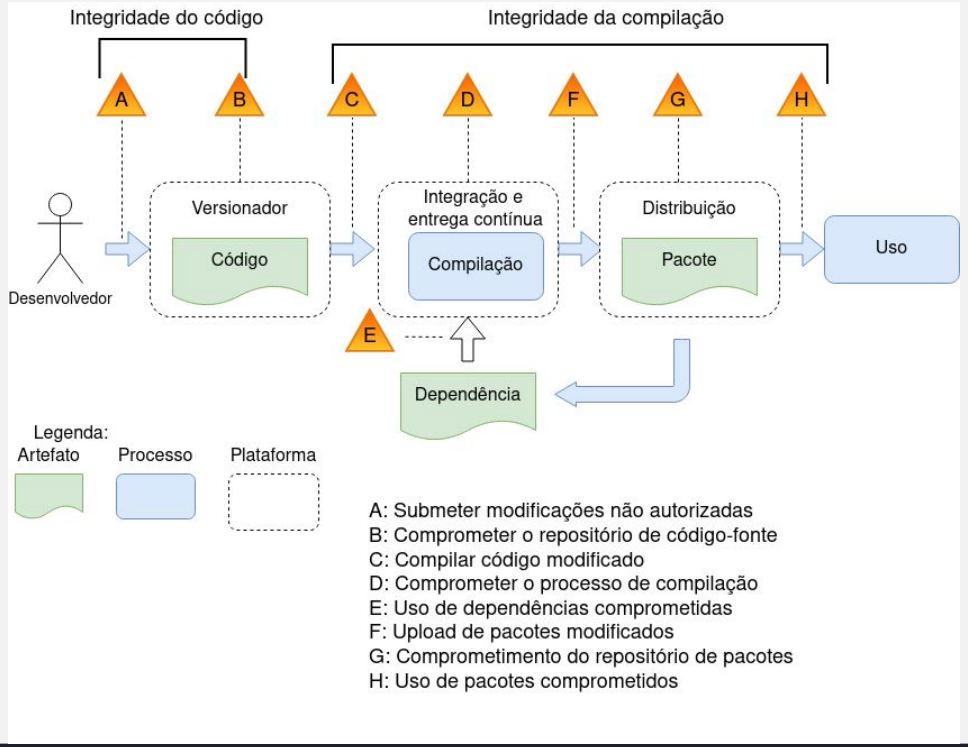
TLP:CLEAR

Trabalhos relacionados

- **OWASP Top 10 CI/CD Security Risks** - OWASP;
- **Guia** de segurança da software supply chain do Center of Internet Security **(CIS) - ISACA, SANS** e outros;
- **Recomendações** da Cloud Native Computing Foundation **(CNCF) - Linux Foundation**.

TLP:CLEAR

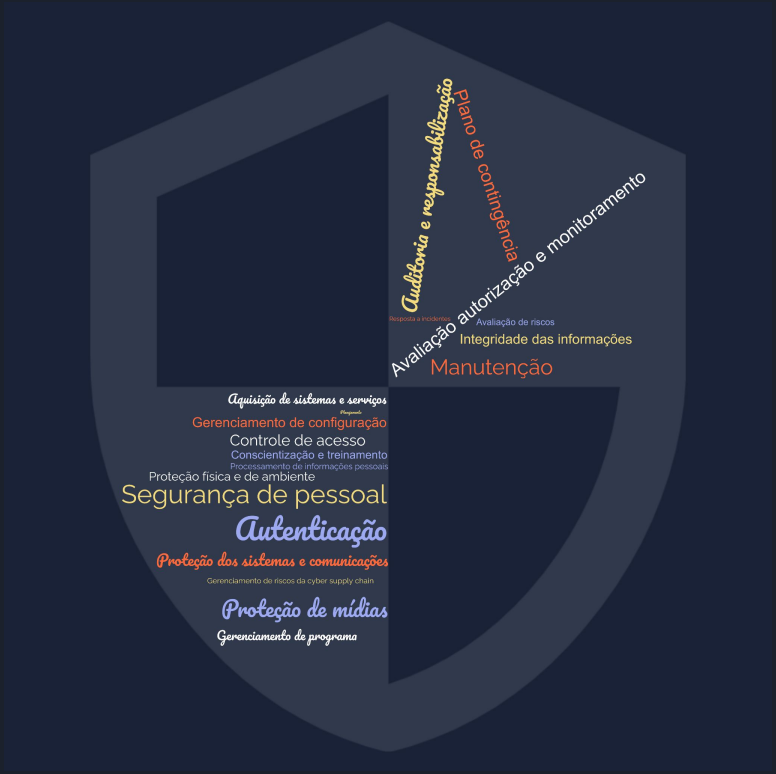
Supply chain Levels for Software Artifacts **(SLSA) - Google**;



Adaptado da iniciativa do Google SLSA

TLP:CLEAR

Famílias de controles elencadas pelo NIST 800- 161



Identificação da oportunidade de pesquisa

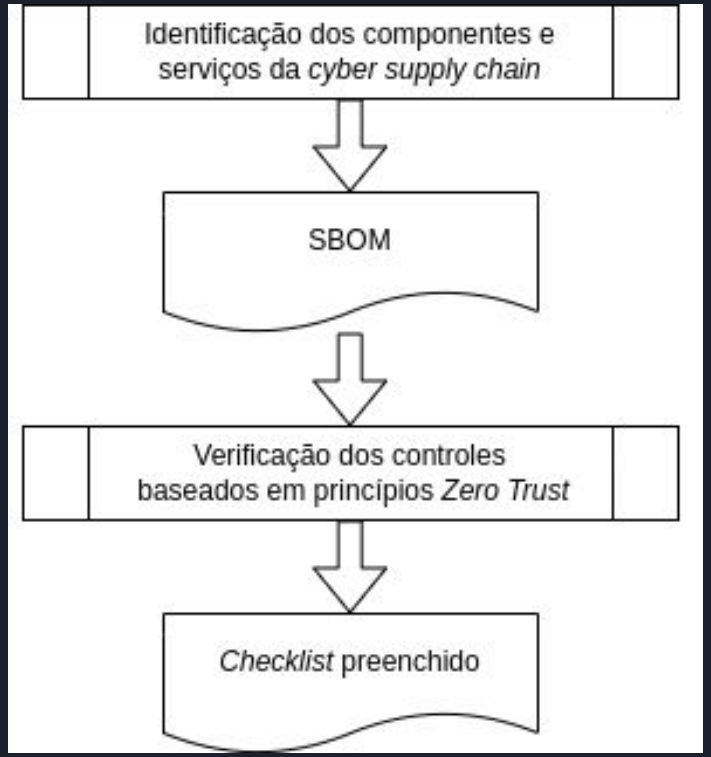
TLP:CLEAR

Controles\Trabalhos correlatos	ENISA	SLSA	OWASP	CIS	CNCF
Controle de acesso	✓	✓	✓	✓	✓
Gerenciamento de configuração		✓	✓	✓	✓
Manutenção	✓				
Proteção dos sistemas e comunicações					
Autenticação	✓	✓	✓	✓	✓
Segurança de pessoal	✓				
Processamento de informações pessoais					
Gerenciamento de riscos da cyber supply chain					✓
Avaliação, autorização e monitoramento					
Plano de contingência	✓				
Proteção física e de ambiente		✓			
Proteção de mídias					
Gerenciamento de programa					
Conscientização e treinamento					
Auditoria e responsabilização	✓		✓	✓	✓
Integridade das informações					
Planejamento					
Aquisição de sistemas e serviços					
Resposta a incidentes					
Avaliação de riscos					

Tabela 2.5: Família de controles implementados pelos trabalhos correlatos

TLP:CLEAR

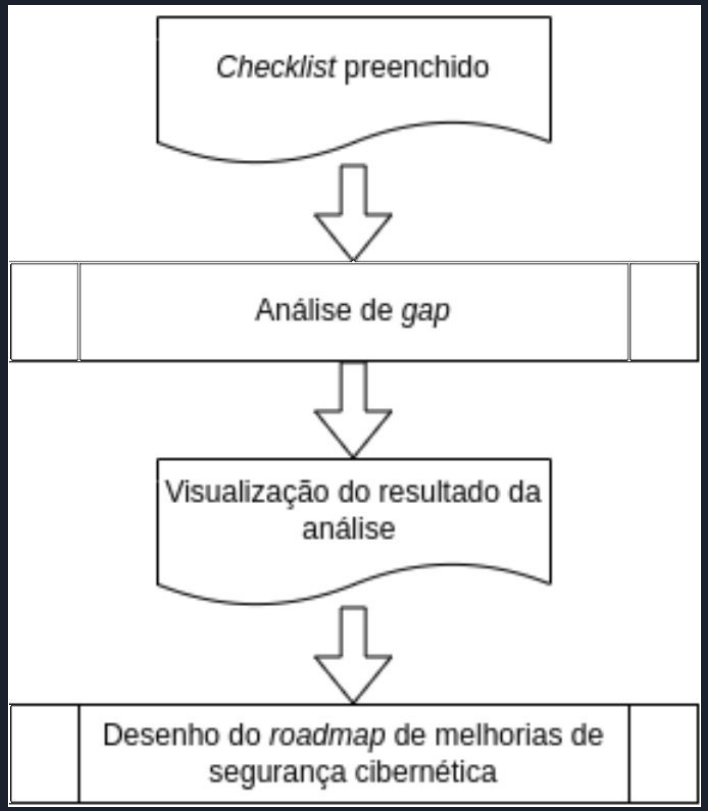
Proposta de integração



As duas primeiras etapas da proposta.

TLP:CLEAR

Proposta de integração



As duas últimas etapas da proposta.

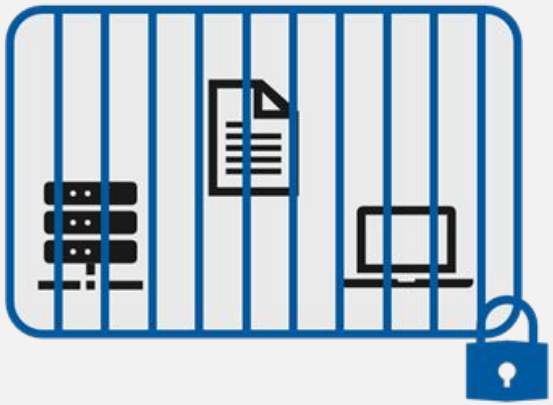
TLP:CLEAR

Mensuração da aderência aos princípios *Zero Trust*

Estrutura da proposta

TLP:CLEAR

Definição conceitual do modelo *Zero Trust*



Abordagem clássica - segurança baseada em perímetro, ativos dentro da rede interna são considerados seguros.

Zero Trust - Proteção dos ativos independente da localização.

Adaptado da documentação da Microsoft

TLP:CLEAR

Domínios

TLP:CLEAR

Desenho do *roadmap*

TLP:CLEAR

Infraestrutura e redes (D1)

Domínio e controles\Estágios		Básico (S.1)	Intermediário (S.2)	Avançado (S.3)
Infraestrutura e redes (D1)	**Controle de acesso (C1)**	Existe uma política de acesso que considera aspectos da *cyber supply chain* ?	O controle de acesso é executado em cada sessão ? As permissões de acesso são revisadas periodicamente ? É concedido o mínimo acesso necessário para que os usuários possam executar suas atividades ? As permissões de acesso são segregadas ? É realizada uma microsegmentação da rede ?	O controle de acesso é baseado em uma política atualizada dinamicamente que permite a tomada de decisões em tempo real ? É possível rastrear todas as ações dos usuários ?
	Gerenciamento de configuração (C2)	Existe uma política definida sobre como realizar o gerenciamento de configuração da *cyber supply chain* ? Existem procedimentos sobre como adicionar ou remover componentes do ambiente organizacional ?	Existe uma linha de base da configuração da *cyber supply chain* ? Existe um controle de mudanças de configuração estabelecido ?	O controle de mudanças de configuração é automatizado ? É possível analisar dinamicamente impactos de maneira a permitir a tomada de decisões em tempo real ?
	Manutenção (C3)	Existem políticas e procedimentos para a manutenção da *cyber supply chain* ?	As informações sobre as manutenções são compartilhadas levando em consideração aspectos de uma arquitetura *Zero Trust* ?	As atividades de manutenção da *cyber supply chain* são automatizadas ? As manutenções são continuamente monitoradas ?
	Proteção dos sistemas e comunicações (C4)	Existe uma política de proteção das comunicações utilizadas na *cyber supply chain* ?	A organização protege suas fronteiras considerando ameaças internas ? As comunicações são protegidas em diversas camadas heterogêneas considerando possíveis falhas em alguns mecanismos ?	Os mecanismos de proteção das comunicação são monitorados e adaptados continuamente?

TLP:CLEAR

Identidade (D2)

Domínio e controles\Estágios		Básico (S.1)	Intermediário (S.2)	Avançado (S.3)
Identidade (D2)	Autenticação (C5)	Existe uma política de autenticação na *cyber supply chain* ?	É realizada a gestão da identidade na *cyber supply chain* ? São utilizados múltiplos fatores de autenticação ?	A autenticação é baseada em uma política atualizada dinamicamente permitindo decisões em tempo real ?
	Segurança de pessoal (C6)	Existe uma política de segurança de pessoal considerando aspectos de segurança da *cyber supply chain* ?	É realizada uma investigação social na contratação de empregados que irão atuar em componentes críticos da *cyber supply chain* ? Existe um monitoramento do comportamento de pessoas que atuam na infraestrutura crítica ?	Os mecanismos de verificação do cumprimento da política de segurança de pessoal são monitorados e aprimorados continuamente ?
	Processamento de informações pessoais (C7)	Existe uma política de processamento de informações pessoais aplicada na *cyber supply chain* ?	Os dados pessoais são manipulados de maneira adequada considerando tanto ameaças internas quanto externas à organização ?	Os mecanismos de proteção de dados pessoais são atualizados constantemente ?
	Gerenciamento de riscos da *cyber supply chain* (C8)	Existe uma política de gerenciamento dos riscos da *cyber supply chain* ?	Existe um inventário dos fornecedores e é possível verificar a autenticidade dos componentes da *cyber supply chain* ?	O plano de gerenciamento dos riscos da *cyber supply chain* é atualizado frequentemente baseado em insumos coletados automaticamente ?

TLP:CLEAR

Dispositivo (D3)

Domínio e controles\Estágios		Básico (S.1)	Intermediário (S.2)	Avançado (S.3)
Dispositivo (D3)	**Avaliação, autorização e monitoramento (C9)**	A política de segurança da informação da organização incorpora aspectos de avaliação da *cyber supply chain* ?	Existe um plano de ações e marcos de avaliação da *cyber supply chain* ?	É realizado um monitoramento contínuo analisando tendências de forma a possibilitar a tomada de decisão em tempo real ?
	Plano de contingência (C10)	Existe um plano de contingência para a *cyber supply chain* ?	Os ativos críticos da *cyber supply chain* são identificados ?	A organização é capaz de prestar serviços alternativos considerando aspectos de uma arquitetura *Zero Trust* ?
	Proteção física e de ambiente (C11)	Existe uma política de proteção física e de ambiente ?	O acesso físico é segregado por papéis ? Existe uma proteção contra modificações físicas?	Os ativos são monitorados e rastreados continuamente ?
	Proteção de mídias (C12)	Existe uma política de proteção de mídias utilizadas na *cyber supply chain* ? A organização emprega criptografia na proteção de dados sensíveis nas mídias ?	A organização sanitiza as mídias ?	Existe um monitoramento contínuo das mídias que possibilita a tomada de decisões em tempo real ?

TLP:CLEAR

Governança e dados (D4)

Domínio e controles\Estágios		Básico (S.1)	Intermediário (S.2)	Avançado (S.3)
Governança e dados (D4)	Gerenciamento de programa (C13)	Existe um programa de atividades de segurança atuando em aspectos da *cyber supply chain*?	Existe um planejamento de execução das atividades com marcos bem definidos ? São coletados indicadores da execução das atividades ?	Os indicadores coletados são utilizados para melhorar o processo continuamente?
	Conscientização e treinamento (C14)	Existe um programa de treinamentos sobre riscos na *cyber supply chain* considerando os diferentes tipos de ameaças e agentes envolvidos ?	A organização registra as informações do programa de treinamentos sobre os riscos da *cyber supply chain* ?	O programa de treinamentos é atualizado continuamente de acordo com tendências identificadas por meio de controles automatizados ?
	Auditoria e responsabilização (C15)	Existe uma política de auditoria considerando ações da *cyber supply chain* ? Essas ações são logadas em um formato que possibilita análises futuras?	Os logs dos eventos coletados são analisados ?	São implementadas técnicas que garantem o não-repúdio das informações da *cyber supply chain* ?
	Integridade das informações (C16)	Existe uma política de integridade das informações da *cyber supply chain* ?	Os mecanismos de integridade das informações levam em consideração ameaças internas como equipamentos infectados por *malwares*?	Falhas nos mecanismos de integridade das informações são reconhecidas e tratadas em tempo real? É realizado um monitoramento contínuo com alertas tempestivos em caso de identificação de violações de segurança?
	Planejamento (C17)	Existe uma política de atualização das normas de segurança referentes a *cyber supply chain* ?	As regras das políticas são atualizadas utilizando princípios *Zero Trust* ?	A política de atualização de normas recebe insumos de controles automatizados?

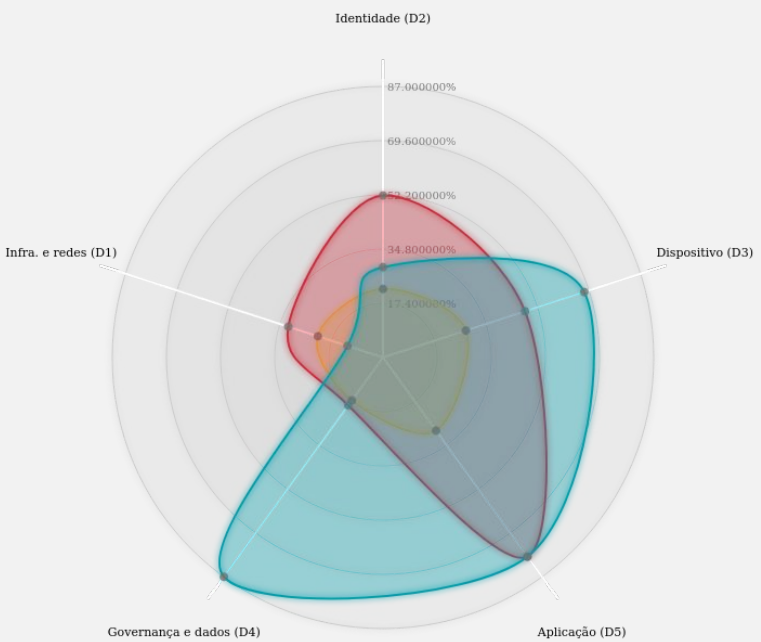
TLP:CLEAR

Aplicação (D5)

Domínios e controles\Estágios		Básico (S.1)	Intermediário (S.2)	Avançado (S.3)
Aplicação (D5)	Aquisição de sistemas e serviços (C18)	Existe uma política de aquisição de sistemas e serviços que considera aspectos de segurança em uma *cyber supply chain* ?	Existe uma gerência de configuração dos sistemas e serviços críticos ? São segregados os papéis com conflito de interesse ?	Os mecanismos de proteção da política de aquisição de sistemas e serviços são atualizados dinamicamente ?
	Resposta a incidentes (C19)	Existe um plano de resposta a incidentes na *cyber supply chain* ?	Existe um compartilhamento de informações de incidentes na *cyber supply chain* ?	O plano de resposta a incidentes é atualizado dinamicamente permitindo a tomada de decisões em tempo real ?
	Avaliação de riscos (C20)	Existe uma política de avaliação de riscos da *cyber supply chain*?	Os componentes da *cyber supply chain* são proativamente analisados em busca por vulnerabilidades? Nessa análise são consideradas tendências no monitoramento e varredura das vulnerabilidades?	Os controles de avaliação de riscos são atualizados frequentemente por meio de mecanismos automatizados ?

TLP:CLEAR

Análise de *gap*

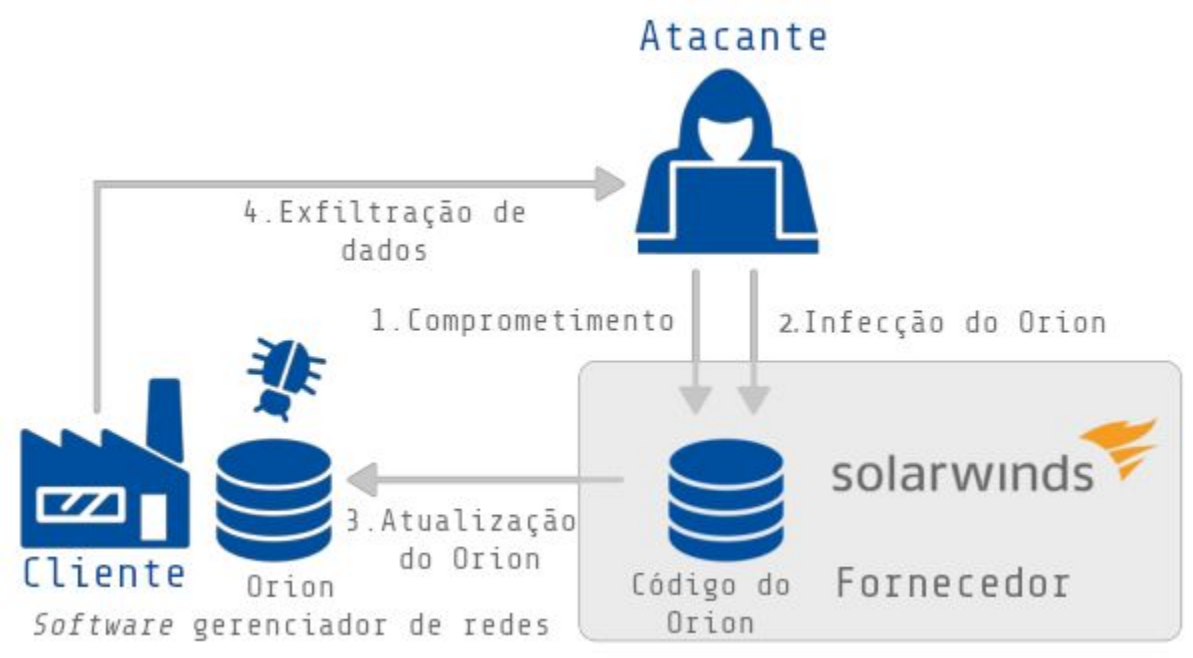


TLP:CLEAR

Estudos de caso

TLP:CLEAR

Cenário 1 - SolarWinds (Sunburst)



Adaptado do relatório da ENISA *Threat Landscape for Supply Chain Attacks*.

TLP:CLEAR

Cenário 1 - SolarWinds (Sunburst)

Adaptado da documentação da Microsoft

TLP:CLEAR

Cenário 1 - SolarWinds (Sunburst)

Falhas identificadas:

- **Controle de acesso** do pipeline;
- Gerenciamento de configuração dos artefatos da solução Orion;
- Proteção dos sistemas e comunicações;
- **Autenticação**;
- Aquisição de sistemas e serviços;

TLP:CLEAR

Cenário 2 - Apache Log4J

- Biblioteca utilizada por **mais de 35k** pacotes java;
- **Execução remota** de código por meio do JNDI;
- Falhas nas seguintes famílias de controles:
  - **Controle de acesso**;
  - Proteção dos sistemas e comunicações; **Autenticação**;
  - Aquisição de sistemas e serviços.

TLP:CLEAR

Cenário 3 - Colonial pipeline

- **Ransomware** que **interrompeu a distribuição de** aproximadamente **metade do combustível** da costa leste dos Estados Unidos;
- Falha na supply chain de **serviço**;
- Falhas identificadas:
  - **Controle de acesso**;
  - Segurança de pessoal;
  - Conscientização e treinamento;
  - **Autenticação**;
  - Aquisição de sistemas e serviços.

TLP:CLEAR

As famílias de controles que não foram efetivas em cada um dos cenários estudados

Domínios e controles\Ataques recentes		Sunburst	Apache Log4Shell/Log4j	Colonial Pipeline
Infraestrutura e redes (D1)	Controle de acesso (C1)	✓	✓	✓
	Gerenciamento de configuração (C2)	✓		
	Proteção dos sistemas e comunicações (C4)	✓	✓	
Identidade (D2)	Autenticação (C5)	✓	✓	✓
	Segurança de pessoal (C6)			✓
Governança e dados (D4)	Conscientização e treinamento (C14)			✓
Aplicação (D5)	Aquisição de sistemas e serviços (C18)	✓	✓	

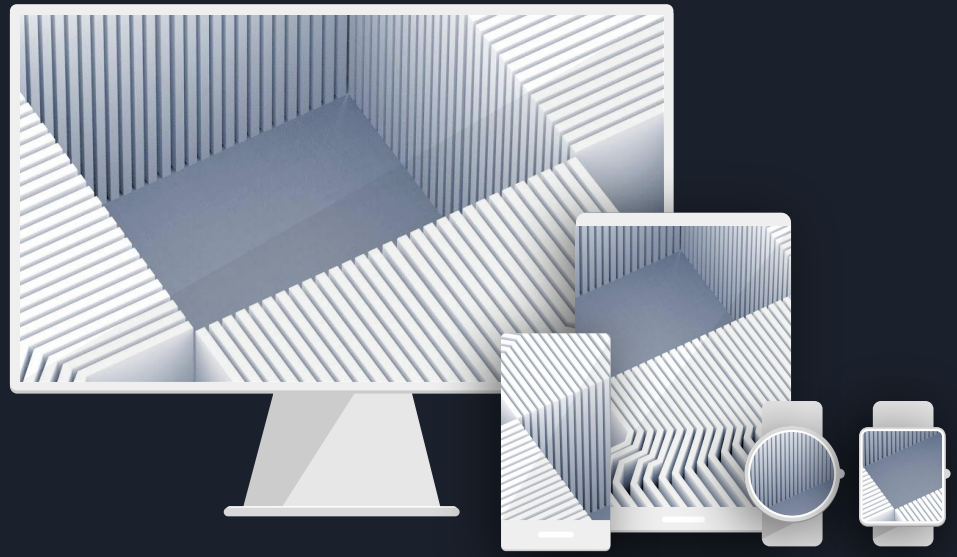
TLP:CLEAR

Conclusão

- Abordagem interessante por **revisar as relações de confiança** e **evitar ataques laterais**;
- **Expandir** as **automações (DevSecOps)** e **análises de dados**.
- É necessário analisar o **custo** de implementação dos controles;
- Precisamos **estimular os fornecedores a reportarem** os incidentes.

TLP:CLEAR

A inteligência só se transforma em conhecimento quando compartilhada!



Obrigado! Estou **aberto para dúvidas e contribuições**!

Estudo publicado em https://tinyurl.com/cyber-supply-chain