Kaspersky Industrial Cybersecurity Conference 2023

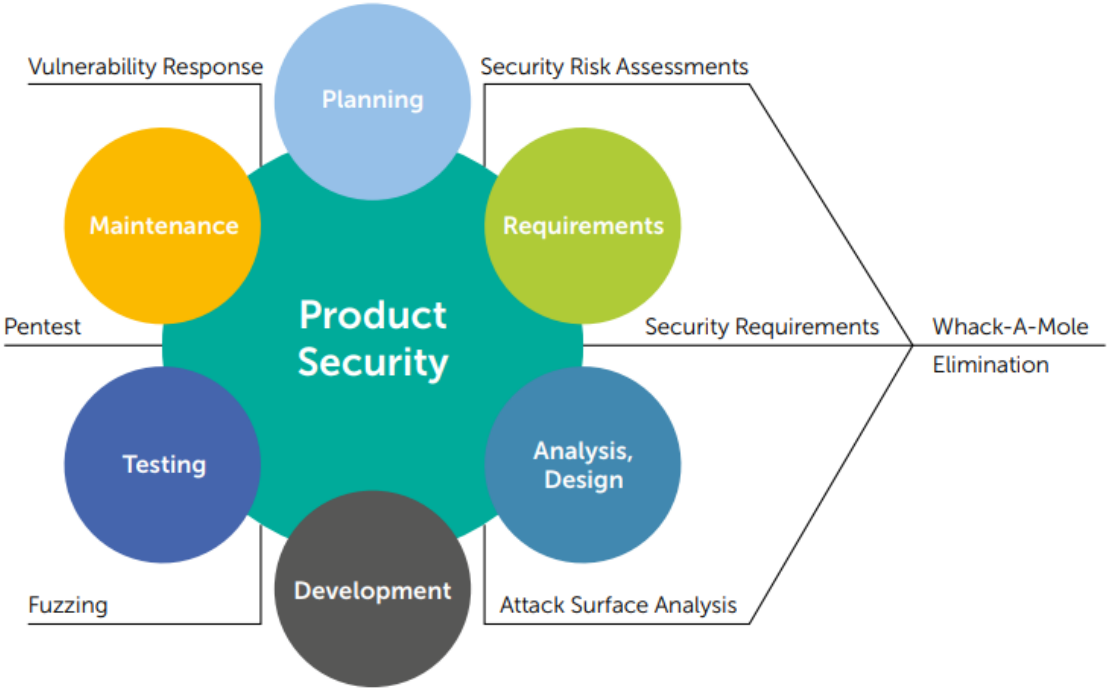
Supply chain угрозы для типовых сценариев эксплуатации и разработки ПО

Дмитрий Шмойлов

Руководитель отдела безопасности программного обеспечения

kaspersky

~~Кто я?~~ Про команду Product security @kaspersky



Product security:

- **Безопасная разработка для ~ 90 приложений kaspersky**
- **Требования по безопасной разработке**
- **Моделирование угроз**
- **Стратегия митигаций**
- **Security тестирование**
- **Fuzzing тестирование**
- **Application pentest (в том числе прошивок KasperskyOS)**
- **Bugboutny**

Содержание

- **Что такое Supply Chain в реальной жизни**
- **Supply Chain в ИТ инфраструктуре**
- **Supply Chain в разработке**
- **Вопросы для моделирования угроз при митигации рисков Supply Chain**

Supply Chain в реальной жизни

Supply Chain – что это такое? В реальной жизни

Сырьё

Элементы

Продукт

Supply Chain – что это такое? В реальной жизни

Сырьё

Элементы

Продукт

Supply Chain – что это такое? В реальной жизни

Сырьё

Элементы

Продукт

Supply Chain – что это такое? В реальной жизни

Сырьё

Элементы

Продукт

Supply Chain – что это такое? В реальной жизни

Сырьё

Элементы

Продукт

Supply Chain – что это такое? В реальной жизни

Сырьё

Элементы

Продукт

Supply Chain – что это такое? В реальной жизни

Сырьё

Элементы

Продукт

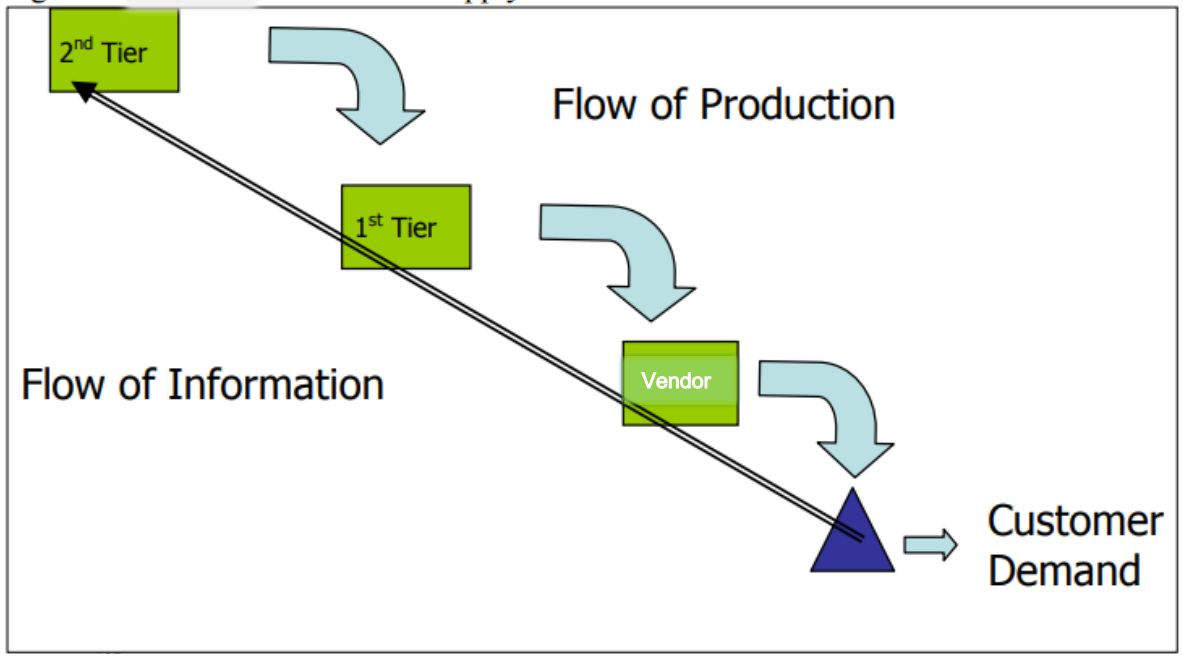
…

…

Supply Chain – что это такое? В реальной жизни

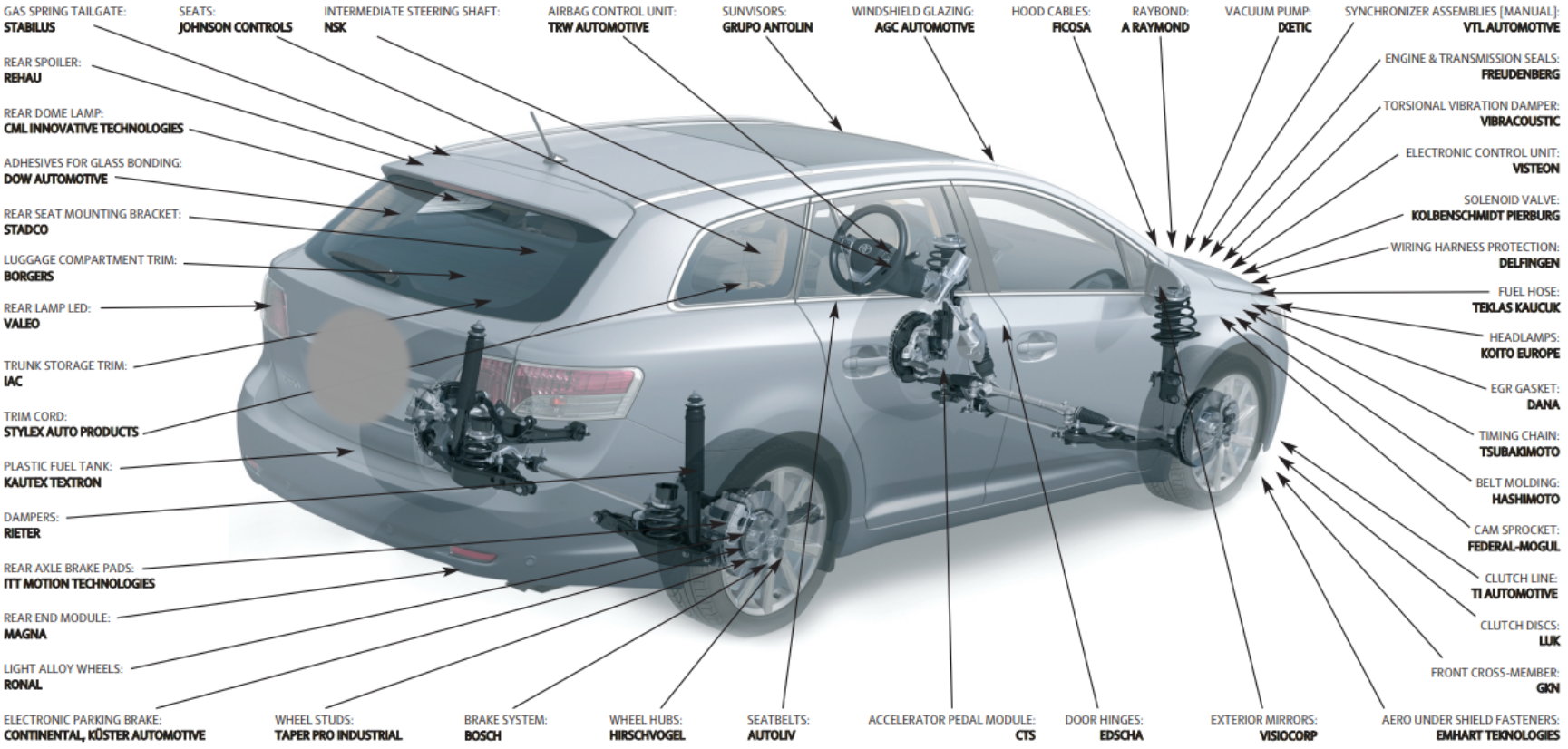
Сырьё Элементы Продукт

Figure 7: Just in Time Supply Chain



Supply Chain – что это такое? В реальной жизни

Suppliers to the



Supply Chain – что это такое? В реальной жизни

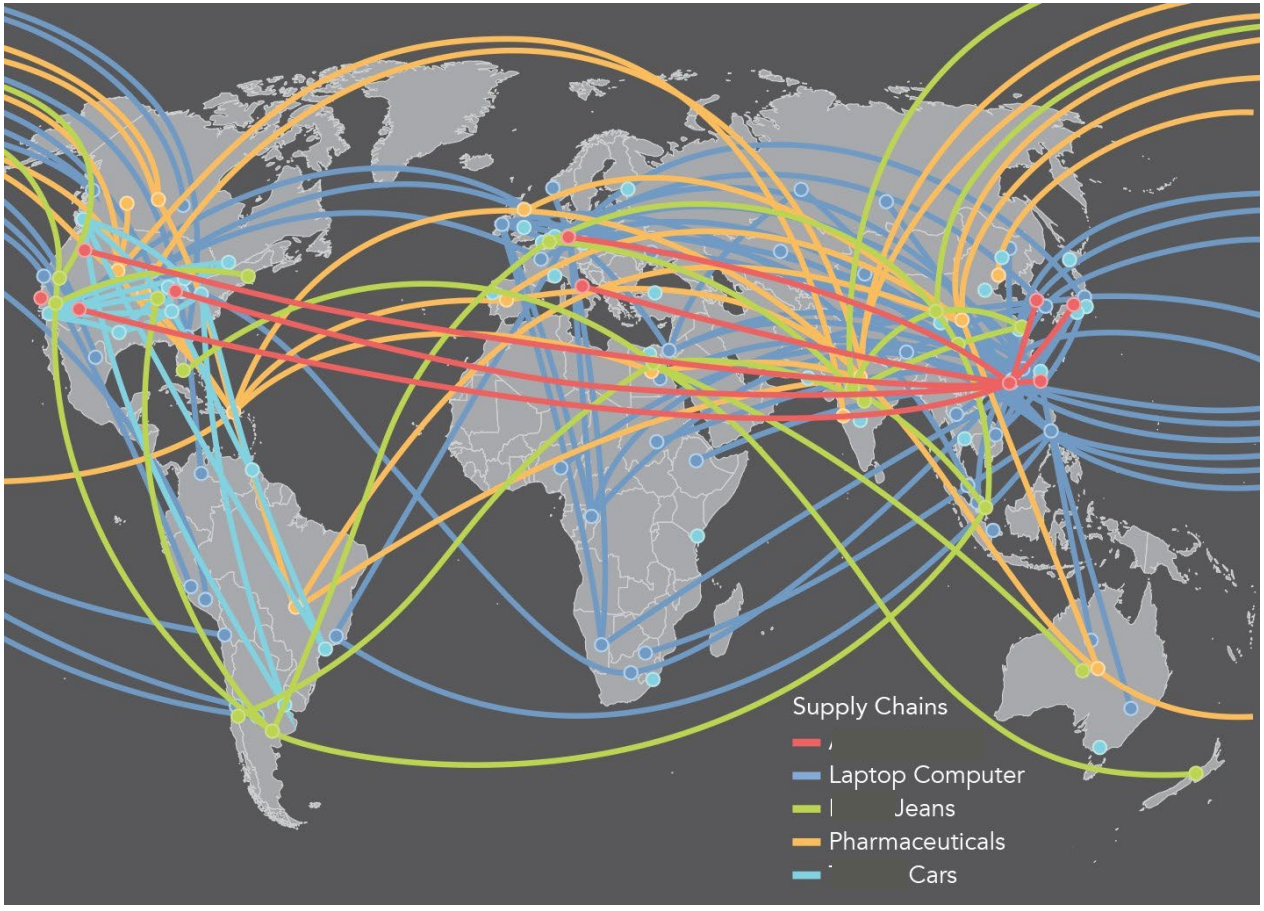


Photo via Twitter User @paragkhanna

Supply Chain в реальной жизни

Множество подрядчиков

Сложная логистика

Ответственность производителя

Supply Chain в ИТ

Software Supply Chain. История

ShadowPad in corporate networks

APT REPORT | 15 AUG 2017

// AUTHORS

Expert GREAT

Popular server man… chain attack

ShadowPad, part 2: Technica… Details (PDF)

In July 2017, during an investigation, suspicious … The partner, which is a financial institution, disc… in the processing of financial transactions.

THE SOLARWINDS HACK_

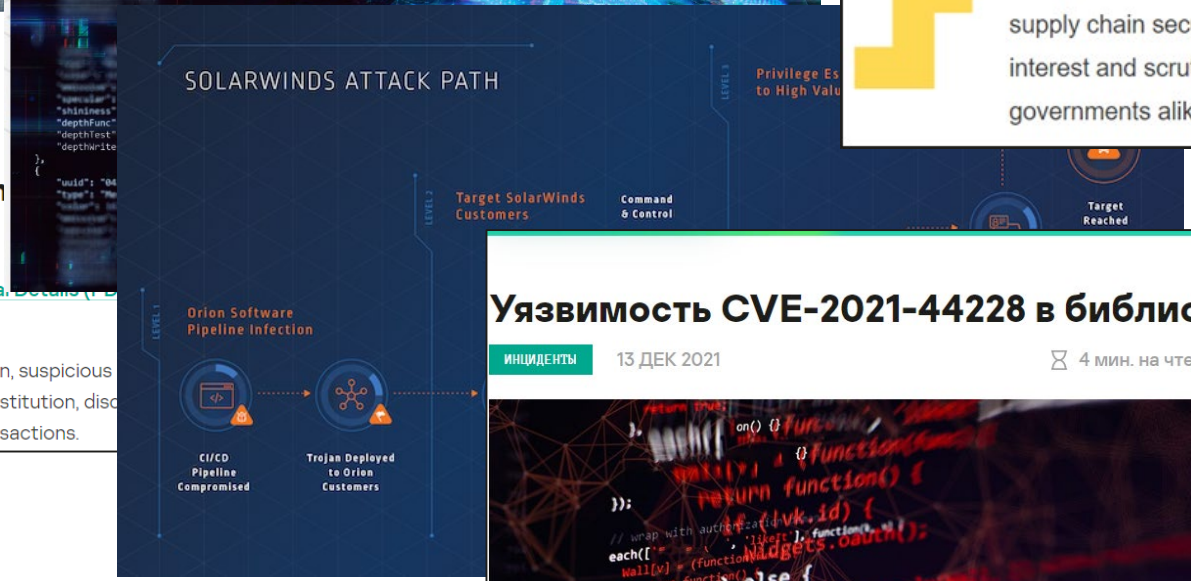


Image Credits: Olemedia / Getty Images

olarWinds and Log4j have made software supply chain security issues a topic of intense interest and scrutiny for businesses and governments alike.

Уязвимость CVE-2021-44228 в библиотеке Apache Log4j

ИНЦИДЕНТЫ | 13 ДЕК 2021 | 4 мин. на чтение

Содержание

Software Supply Chain. История

241 npm and PyPI packages caught dropping Linux cryptominers

By Ax Sharma

August 19, 2022 04:11 PM

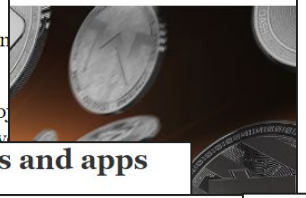
Two more malicious Python packages in the PyPI

INCIDENTS 16 AUG 2022 4 minute read

Python library 'ctx' uploads secrets to a Heroku endpoint

Heavily downloaded PyPI package 'ctx' has been compromised sometime this month with n
published versions exfiltrating your environment variables to an external server.

'ctx' is a minimal Python module that lets developers manipulate their dictionary ('dict') ob
variety of ways. The package, although popular, had not been touched since 2014 by its dev



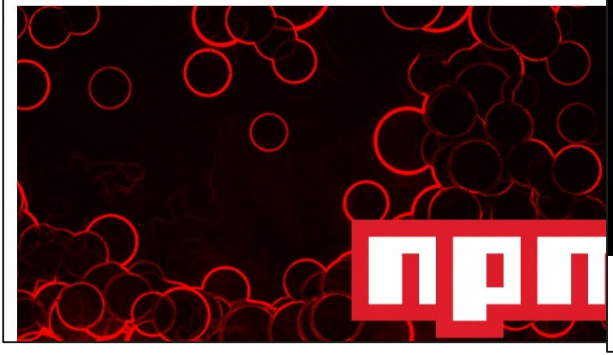
Nitrokey
secure your digital life

Company News Products Solutions Support Shop

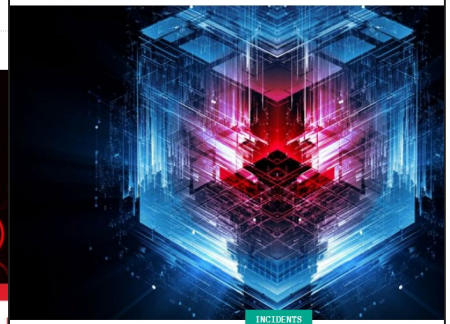
Smartphones With Popular Qualcomm Chip Secretly Share Private Information With US Chip-Maker

NPM supply-chain attack impacts hundreds of websites and apps

By Sergiu Gatlan



SECURELIST



INCIDENTS

LofyLife: malicious npm packages steal D
tokens and bank card data

28 JUL 2022 1 minute read

Not just an infostealer: Gopuram backdoor deployed through 3CX supply chain attack

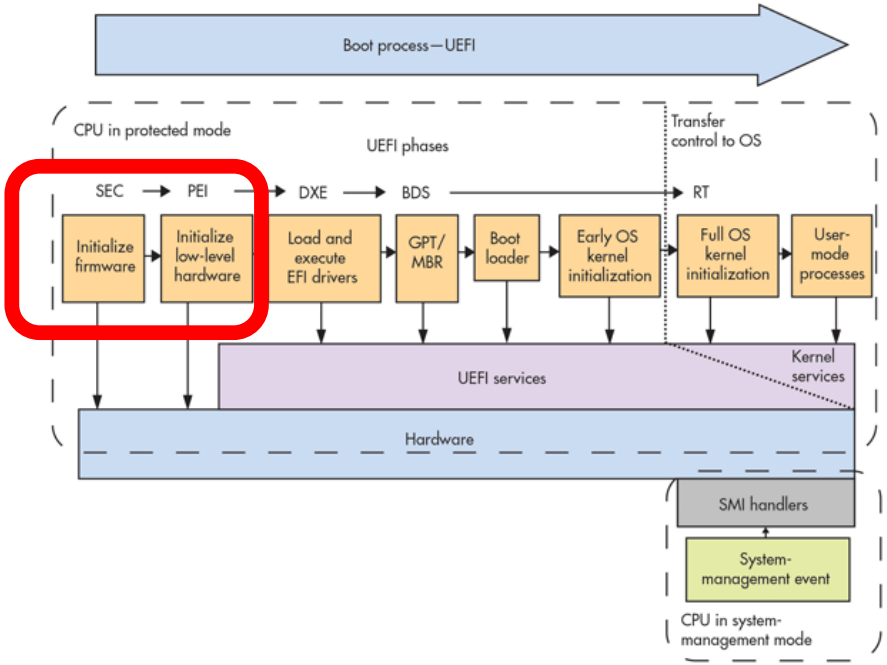
APT REPORTS 03 APR 2023 4 minute read

GREAT WEBINARS

13 MAY 2021, 1:00PM
GReAT Ideas. Bala
BORIS LARIN, DENIS LEGEZO

26 FEB 2021, 12:00PM
GReAT Ideas. Gree
JOHN HULTQUIST, BRIAN BARTH
SUGURU ISHIMARU, VITALY KAM
YUSUKE NIWA, MOTOHIKO SATO

Supply Chain в аппаратной начинке ИТ решения



Где «корень доверия»?

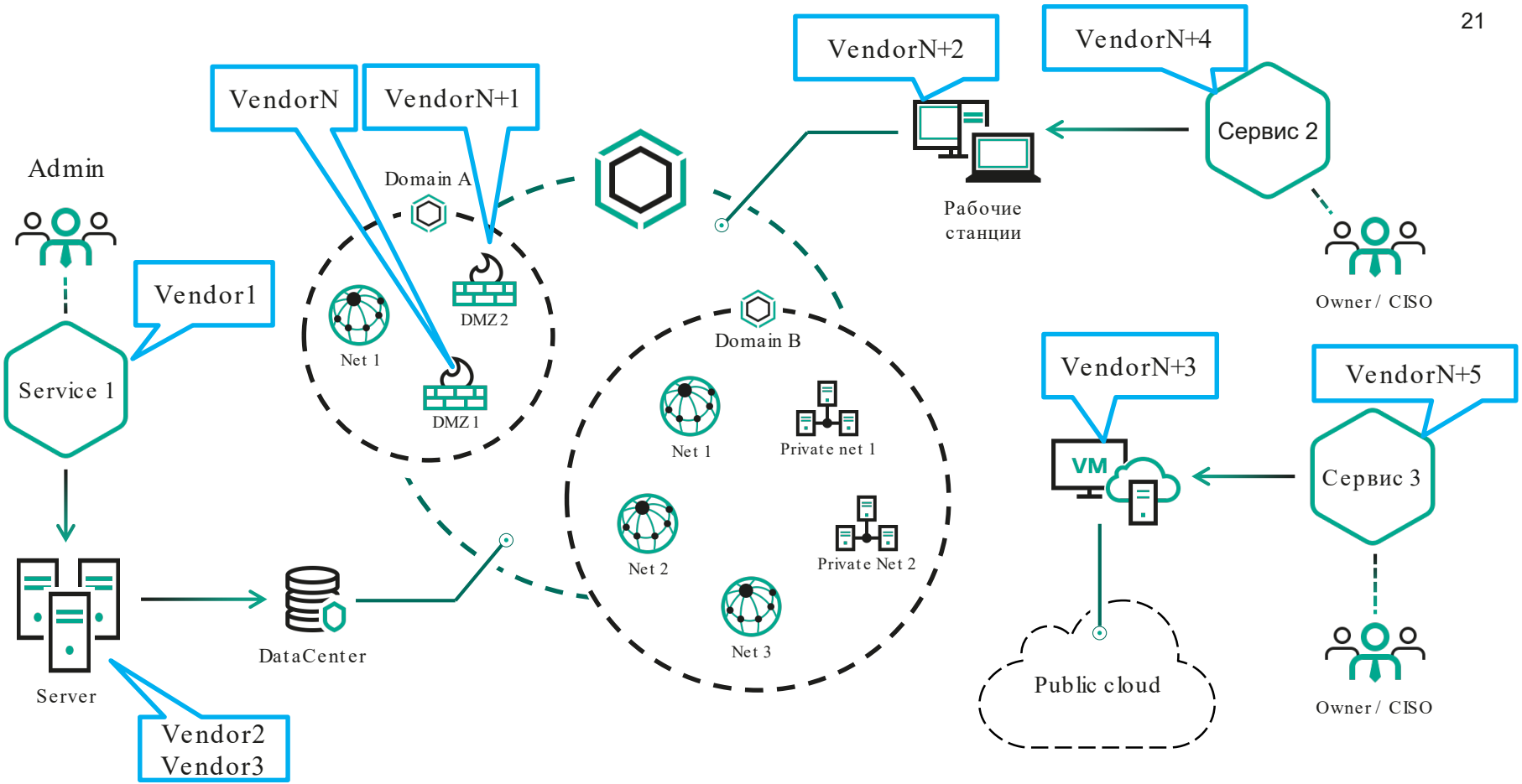
Микрокод для:
- **CPU**
- **HDD**
- **Периферии**
  - **(модем, GPU, контроллер и т д)**

Прошивка устройства/модуля

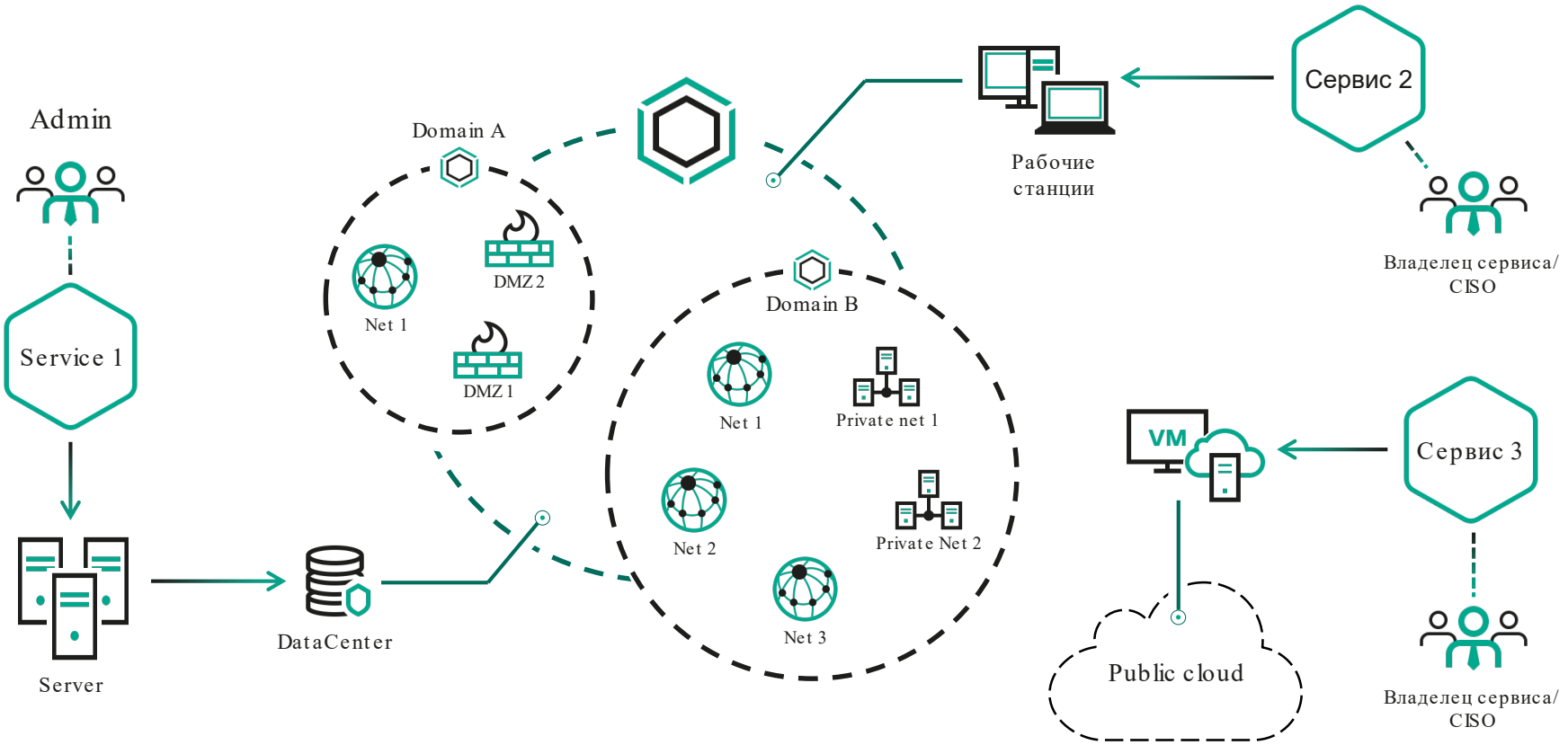
Удаленные соединения, которые могут совершать аппаратные модули

Supply Chain в ИТ инфраструктуре

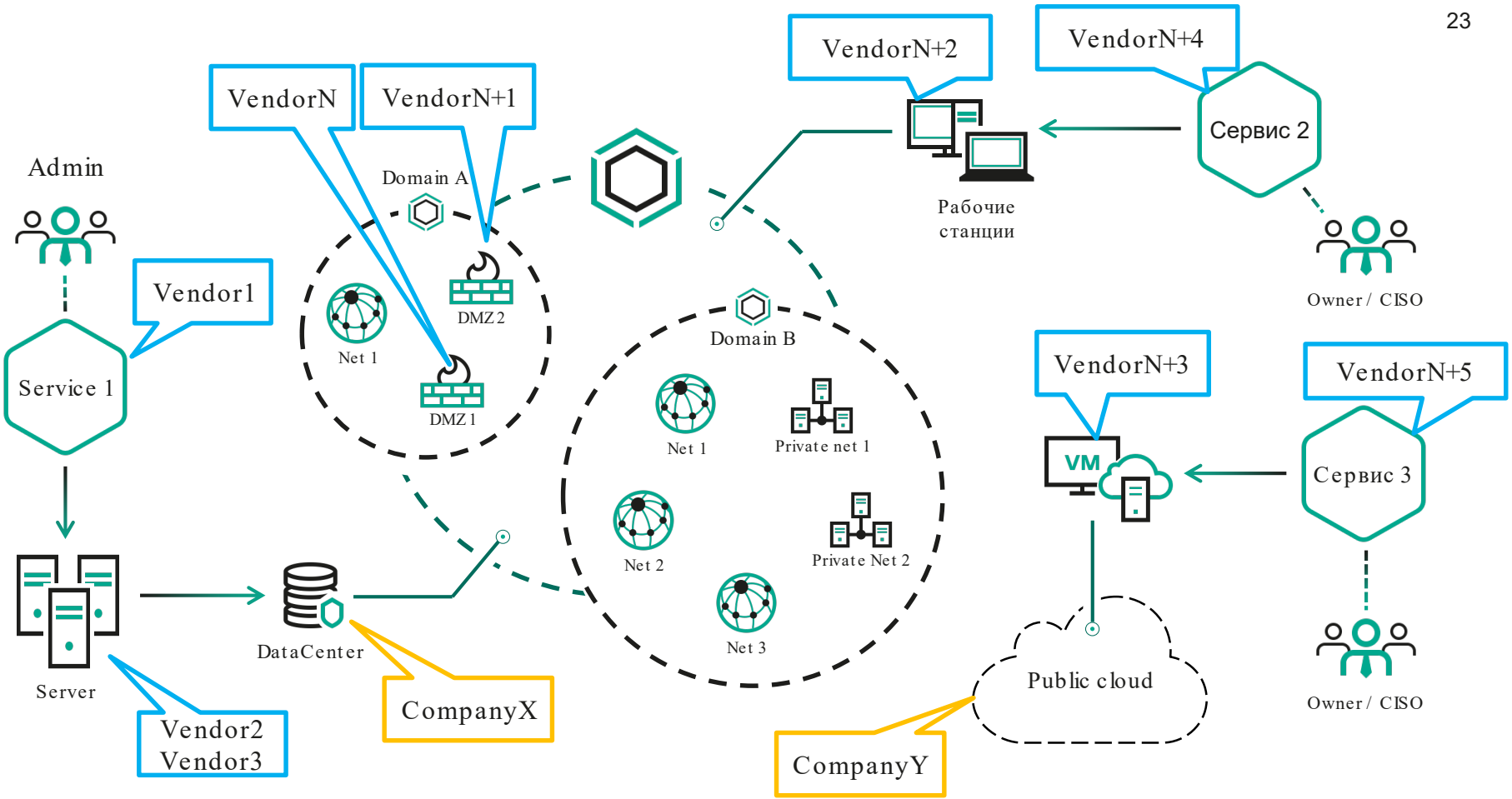
Supply Chain для типовой ИТ инфраструктуры



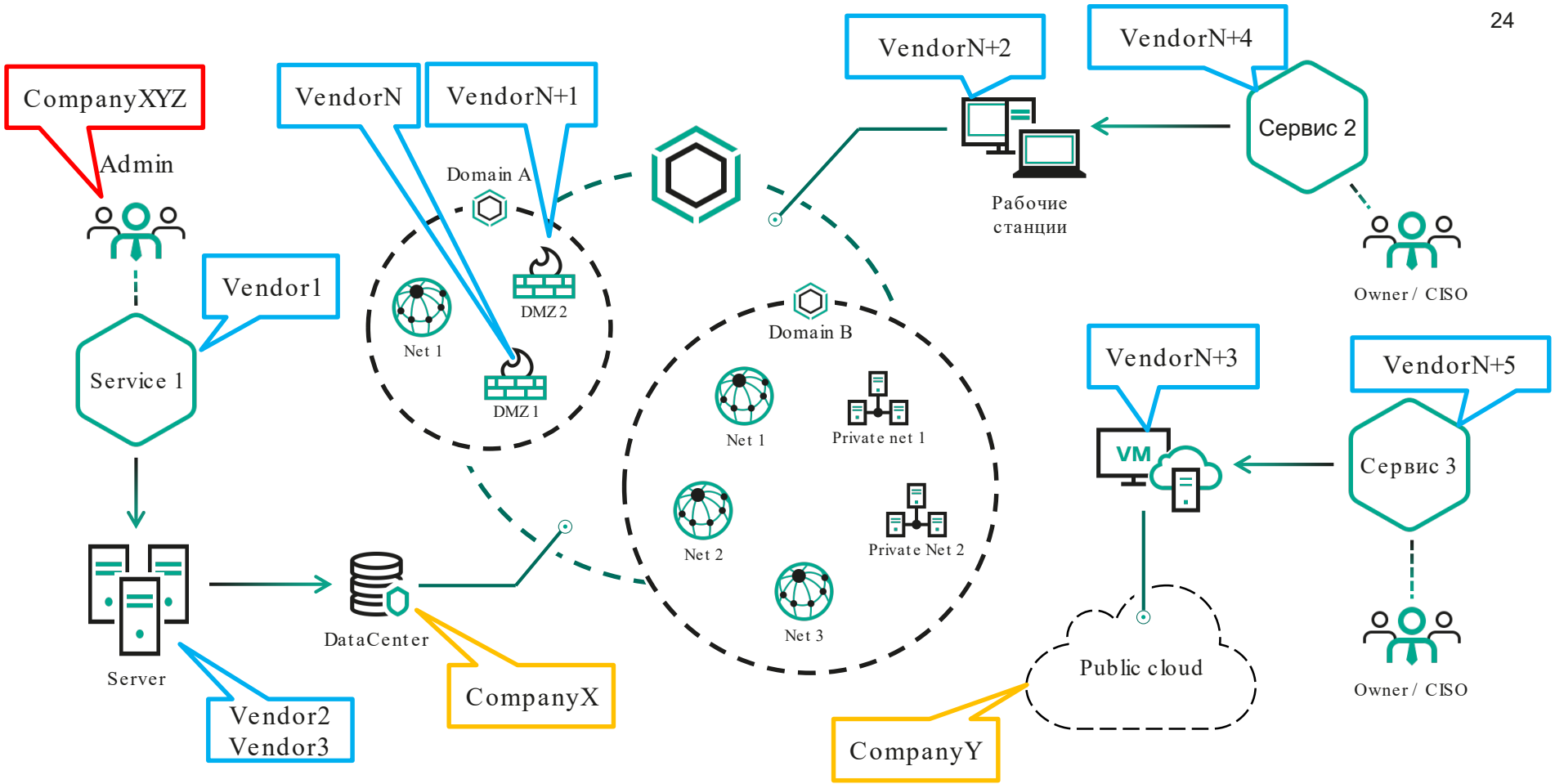
Supply Chain для типовой ИТ инфраструктуры



Supply Chain для типовой ИТ инфраструктуры



Supply Chain для типовой ИТ инфраструктуры



Что требовать от подрядчиков

Базовые требования
идентификация и аутентификация, антивирусная защита и т.д. и т.п.

Сертификация и аттестация
ФСТЭК, РКН, ГОСТ
ISO 27001, SOC2, и т.д.

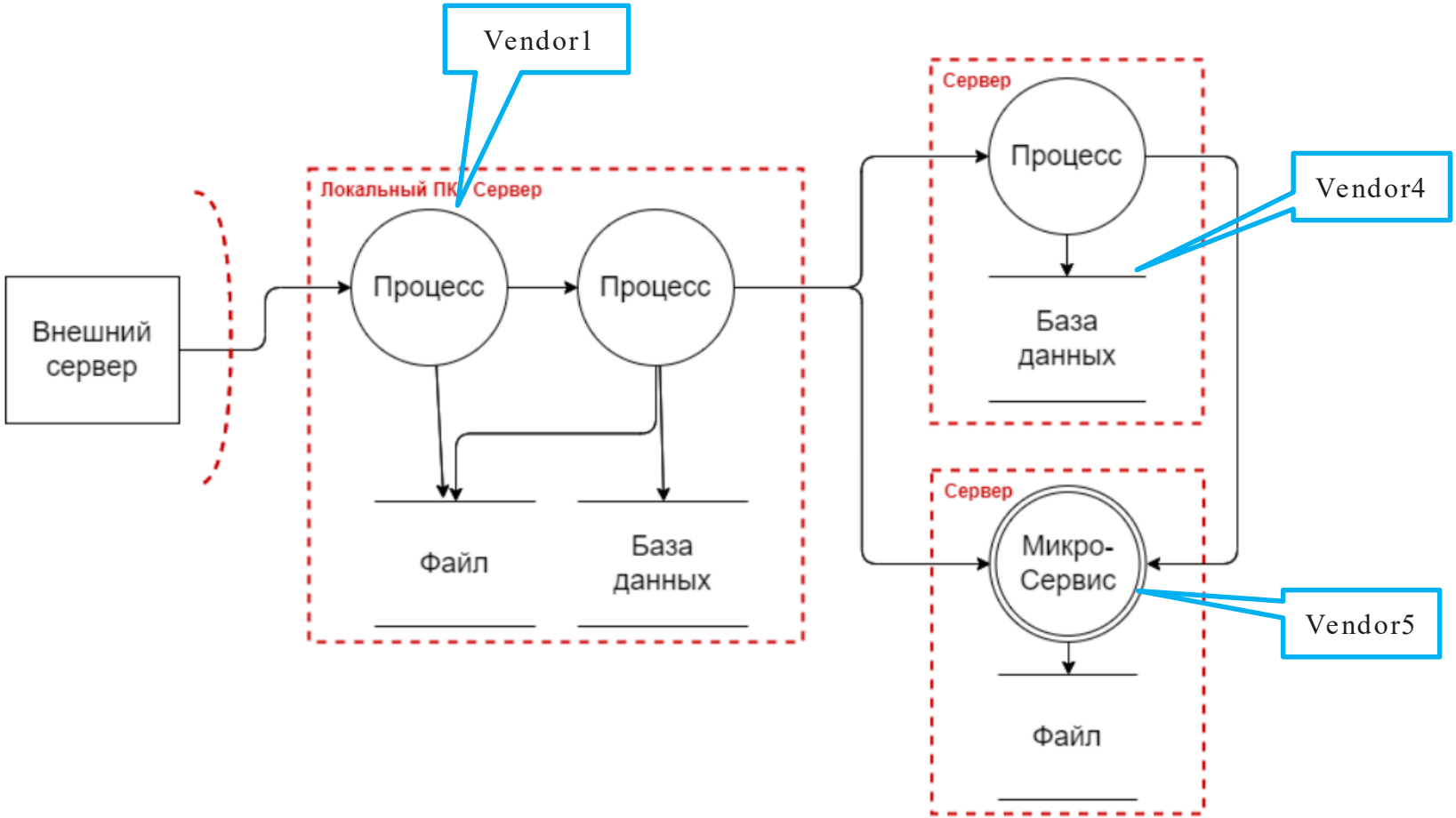
Возможные метрики
BitSignt, LEETSecurity, CSA.

Договор!
границы ответственности и обязательства в случае инцидентов.

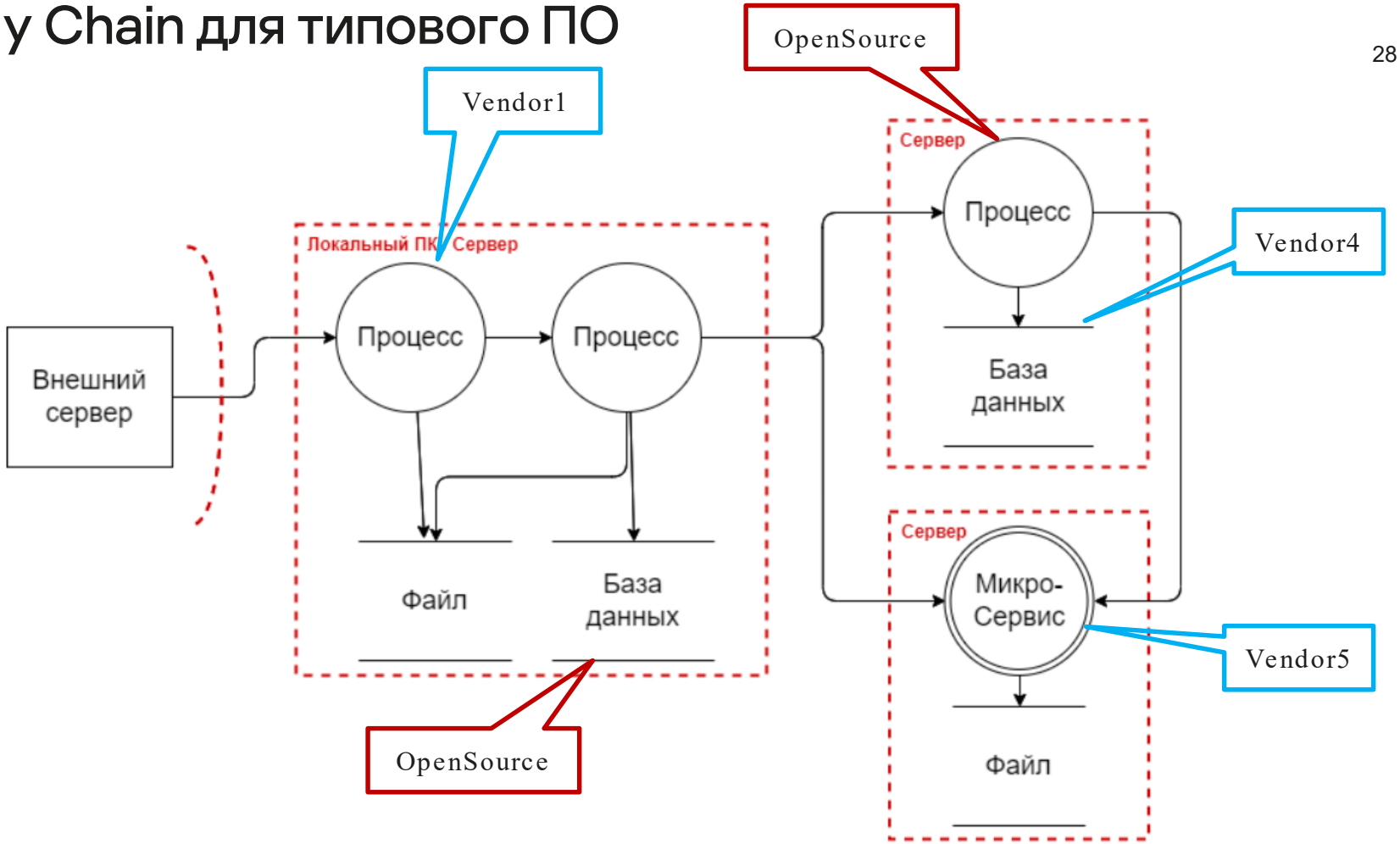
Ваши требования! Не типовой договор, а с учетом ваших ИБ политик!

Supply Chain для разрабатываемого программного обеспечения

Supply Chain для типового ПО

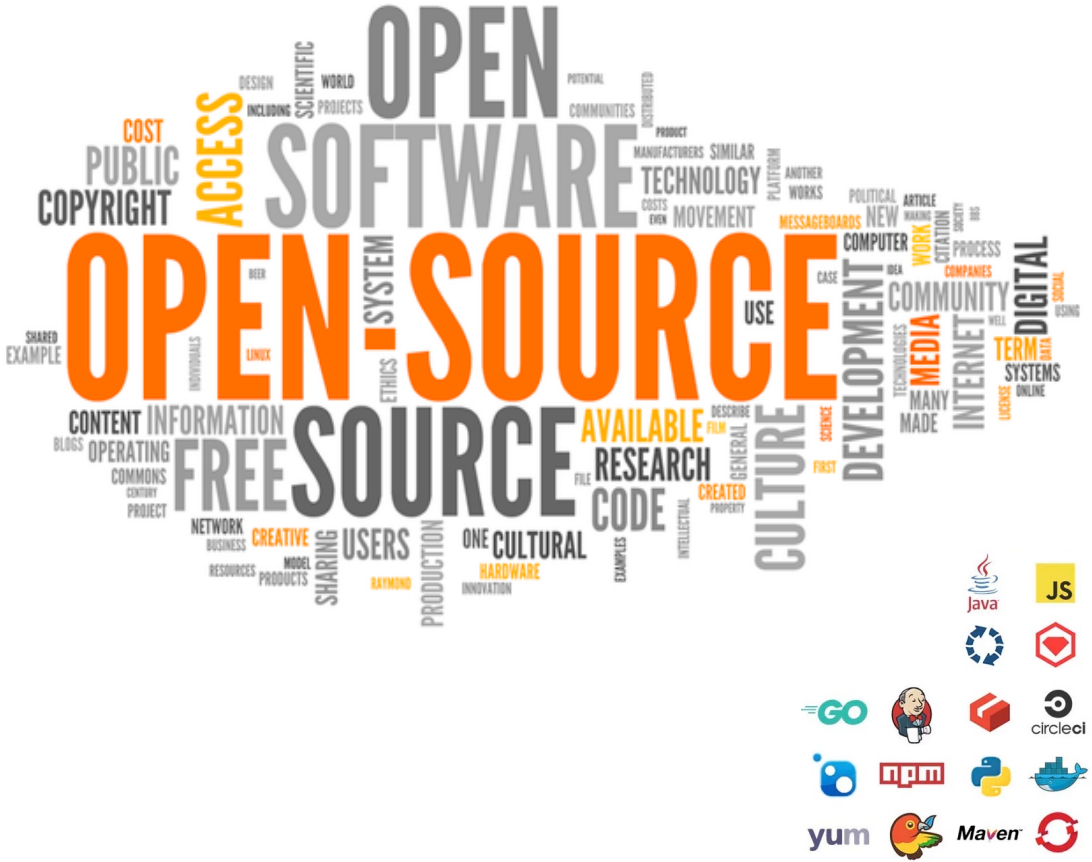


Supply Chain для типового ПО

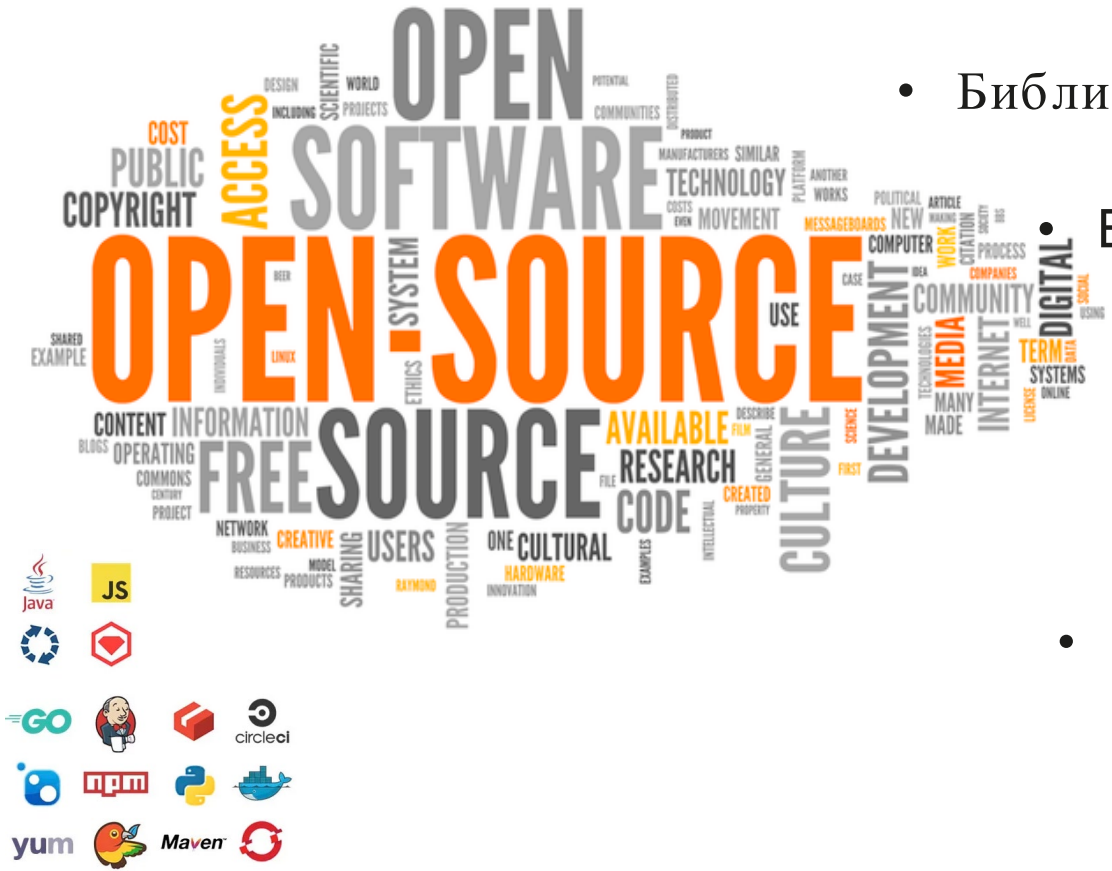


Opensource? Да, opensource!

- Ускорение разработки
- Концентрация на важном
- Разработка сообществом в тысячи девелоперов



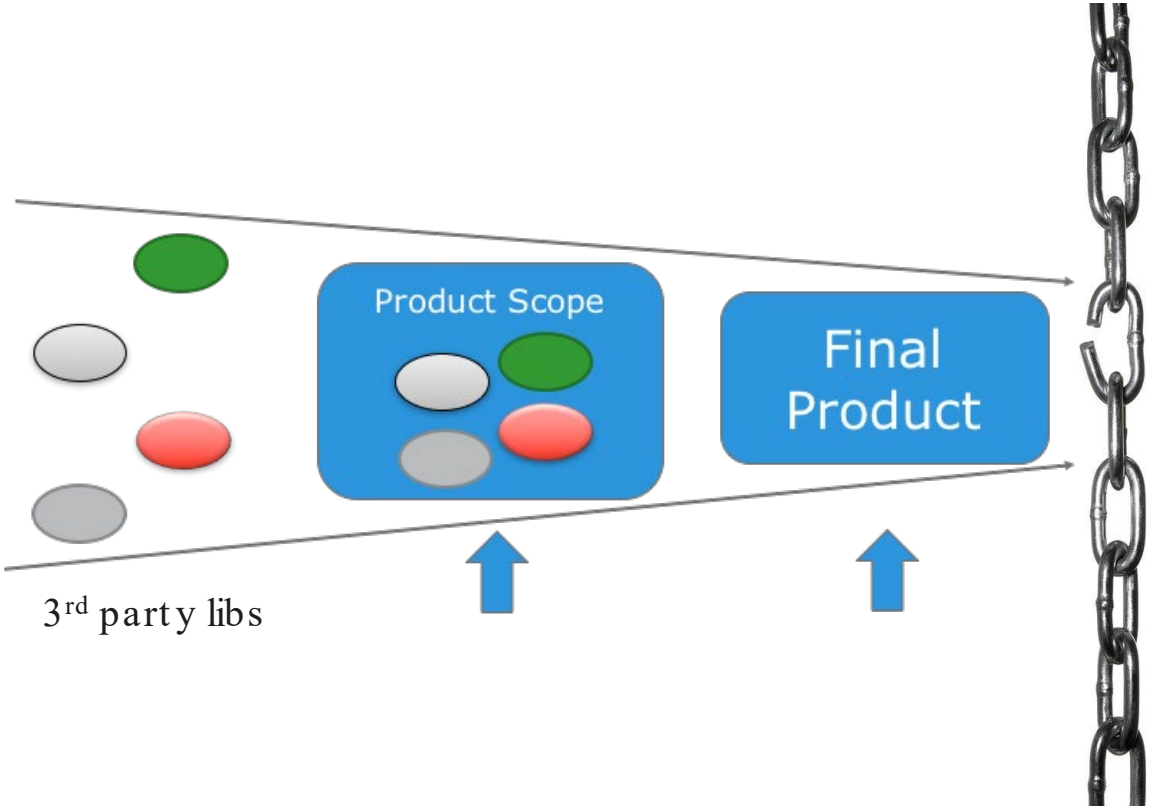
Opensource? Каковы риски?



- Библиотеки с 1-2 контрибьюторами?
- Есть ли проверки безопасности?
- Постоянный поток CVE
- А что с поддержкой?
- Supply Chain?

Opensource? Каковы риски?

- Ua-parser-js – 10.2021
- Npm (14M downloads) – 11.2021
- MS - CVE-2021-26443 – 11.2021
- Log4j – 12.2021
- samba. CVE-2021-44142 – 02.2022
- Spring4Shell – 04.2022
- Python &php – 05.2022
- Iconbrust npm – 07.2022
- etc..etc..etc...



Opensource. Риски.

Apache LOG4J™ 2 CVE (зато какие...)

OpenSSL Cryptography and SSL/TLS Toolkit 2020: 3 CVE 2021: 8 CVE

curl:// 2020: 6 CVE 2021: 13 CVE

SURICATA 2020: 0 CVE 2021: 3 CVE

docker 2020: 3 CVE 2021: 6 CVE

python™ 2020: **88** CVE 2021: **114** CVE

npm 2020: **110** CVE 2021: **145** CVE

Java 2020: **780** CVE 2021: **1015** CVE

php 2020: **1464** CVE 2021: **41656** CVE

Opensource. Риски.

Apache Log4j — 2 CVE (зато какие...)

OpenSSL — 2020: 3 CVE 2021: 8 CVE

curl — 2020: 6 CVE 2021: 13 CVE

Suricata — 2020: 0 CVE 2021: 3 CVE

docker — 2020: 3 CVE 2021: 6 CVE

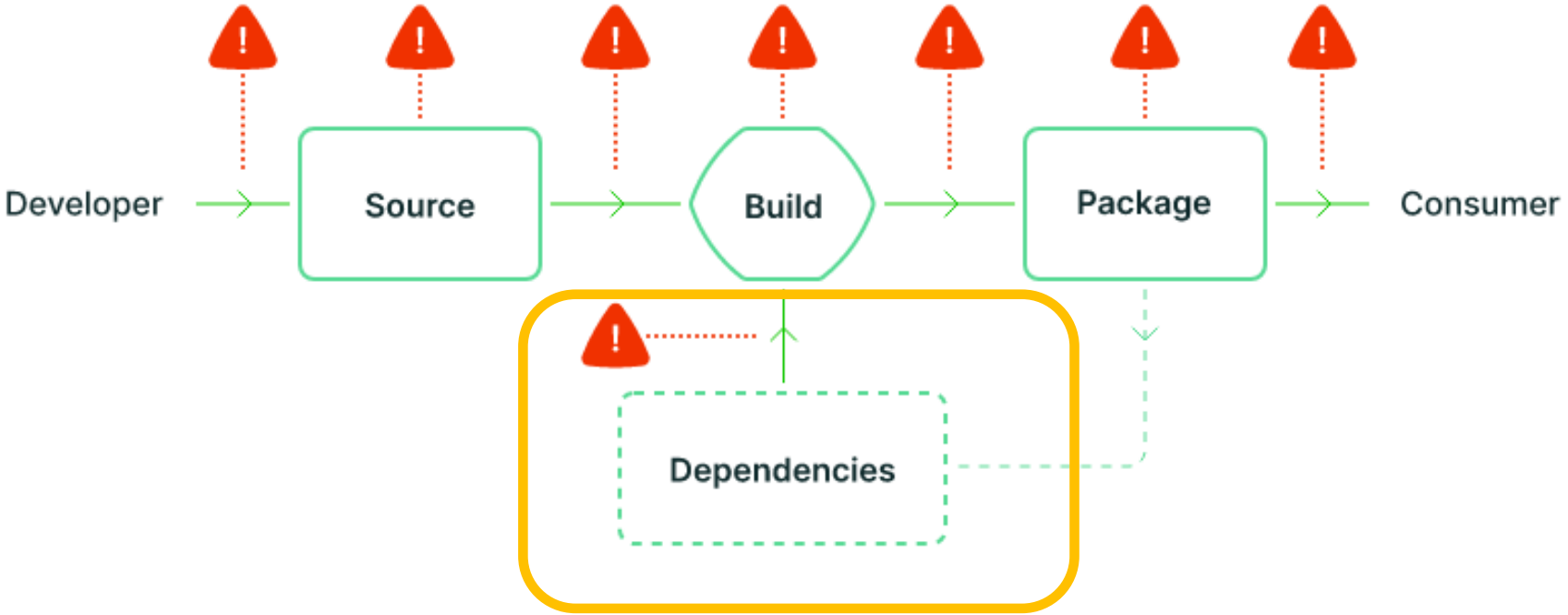
python — 2020: **88** CVE 2021: **114** CVE

npm — 2020: **110** CVE 2021: **145** CVE

Java — 2020: **780** CVE 2021: **1015** CVE

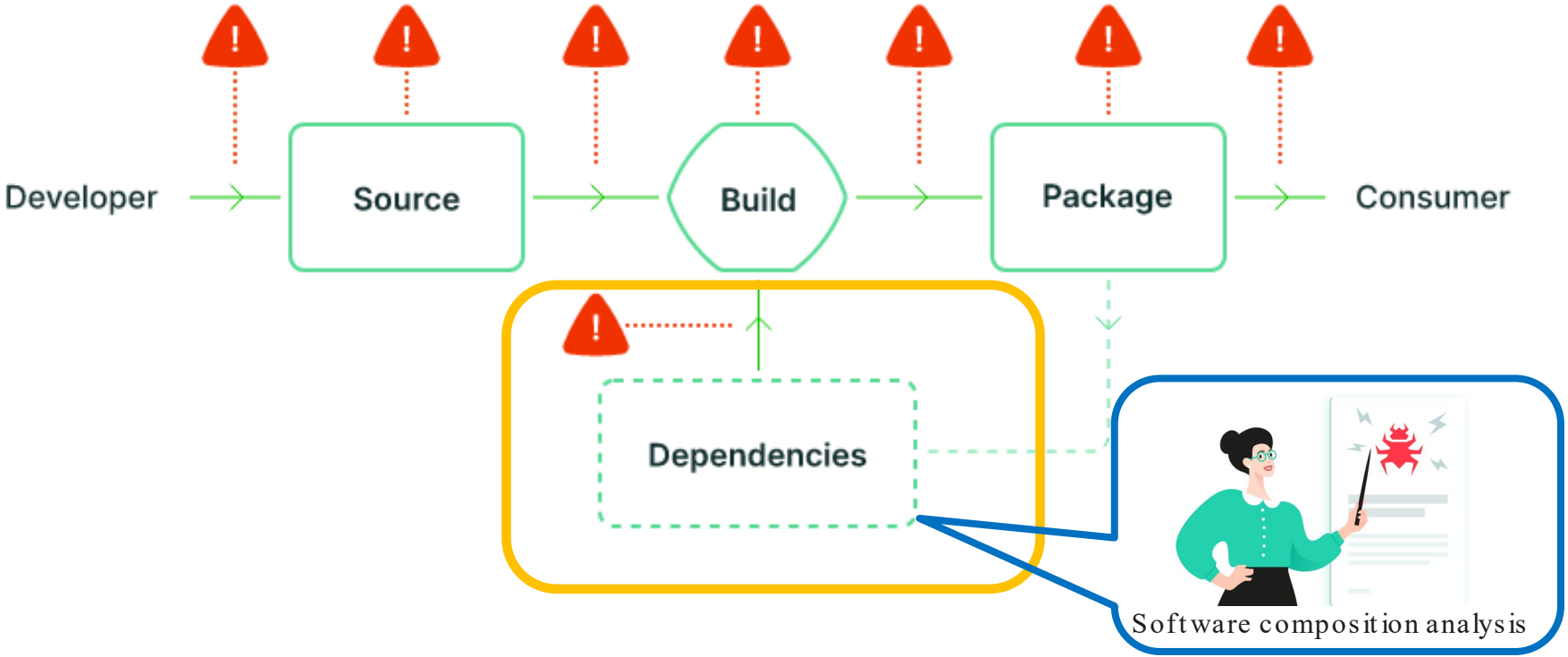
php — 2020: **1464** CVE 2021: **41656** CVE

Opensource. Supply Chain



https://slsa.dev/

Opensource. Supply Chain



https://slsa.dev/

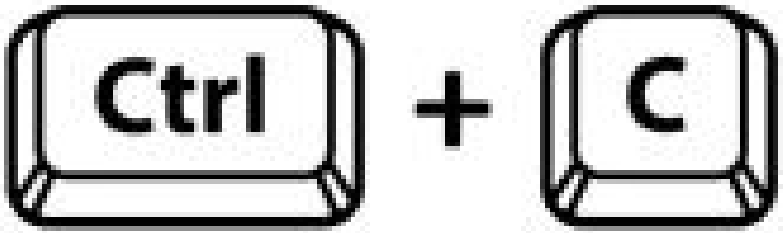
Opensource. Неконтролируемое использование. «Серый» opensource

Казалось бы

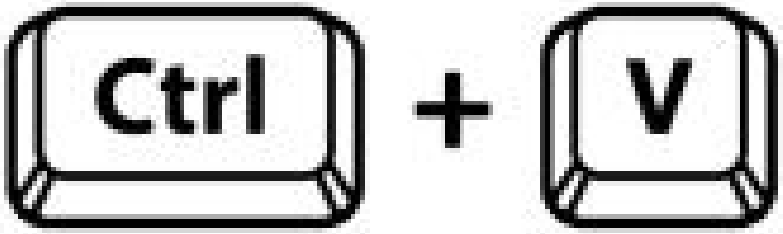
–НО!

- **Вы знаете какие библиотеки используете**
- **Вы делаете проверки на безопасность**
- **Вы регулярно обновляете до последней версии**

Opensource. Неконтролируемое использование. «Серый» opensource



ваш код:



=

Opensource. Ответственность

Мы в ответе за тех, кого приручили

opensource ~~кот~~ код это не беспризорный ~~кот~~ код!

opensource код в вашем проекте – ваш код!

но и риски его использования – ваши риски

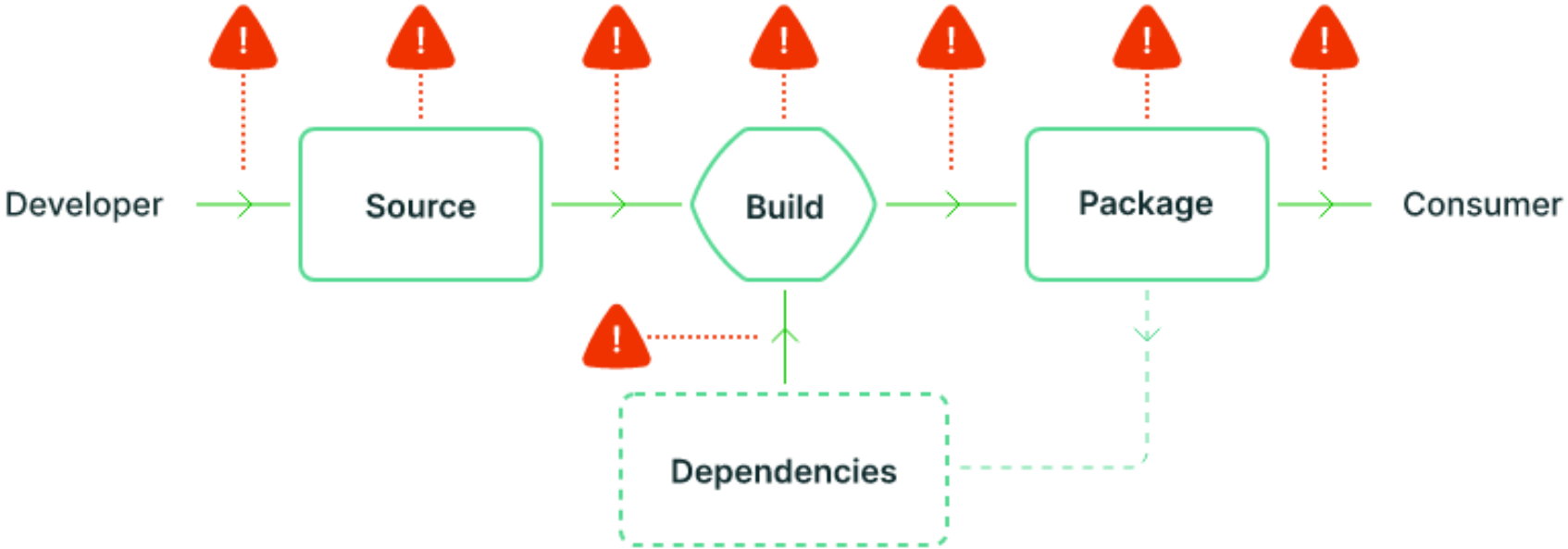
не забудьте про проприетарные библиотеки (лицензия+контракт)

стоит принять это

Типовые угрозы для цепочки поставок при разработке и эксплуатации

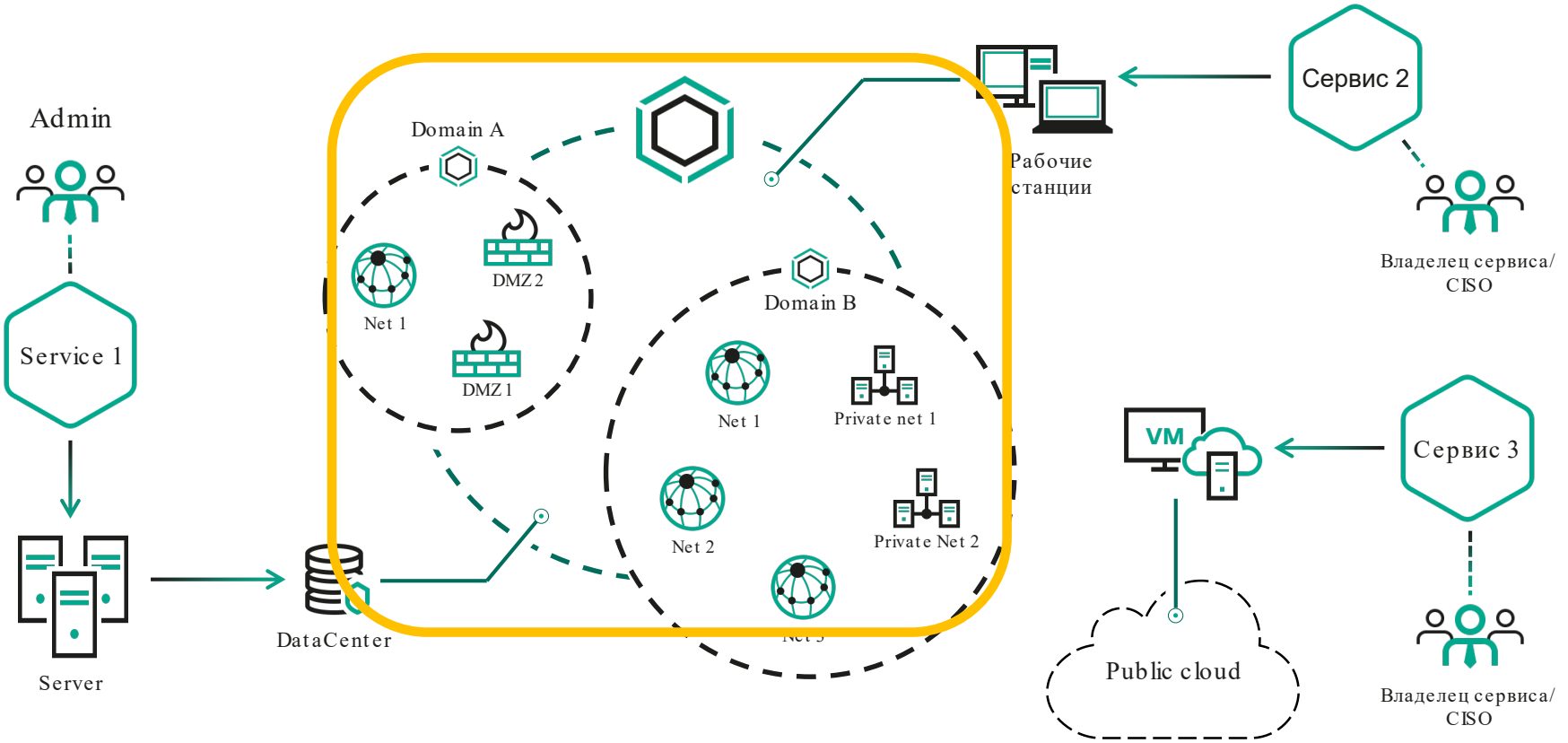
...и вопросы для модели угроз

Supply Chain. Типовой ландшафт разработки ПО

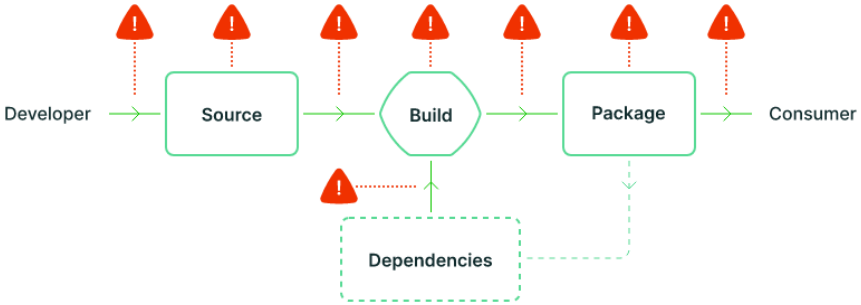


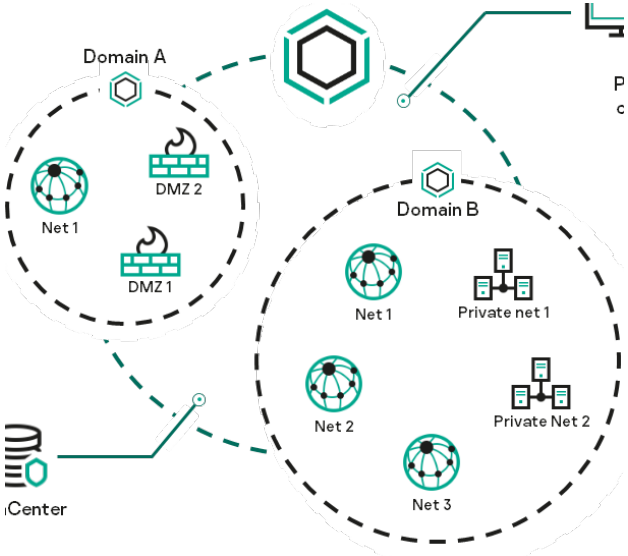
https://slsa.dev/

Supply Chain. Типовой ландшафт сети



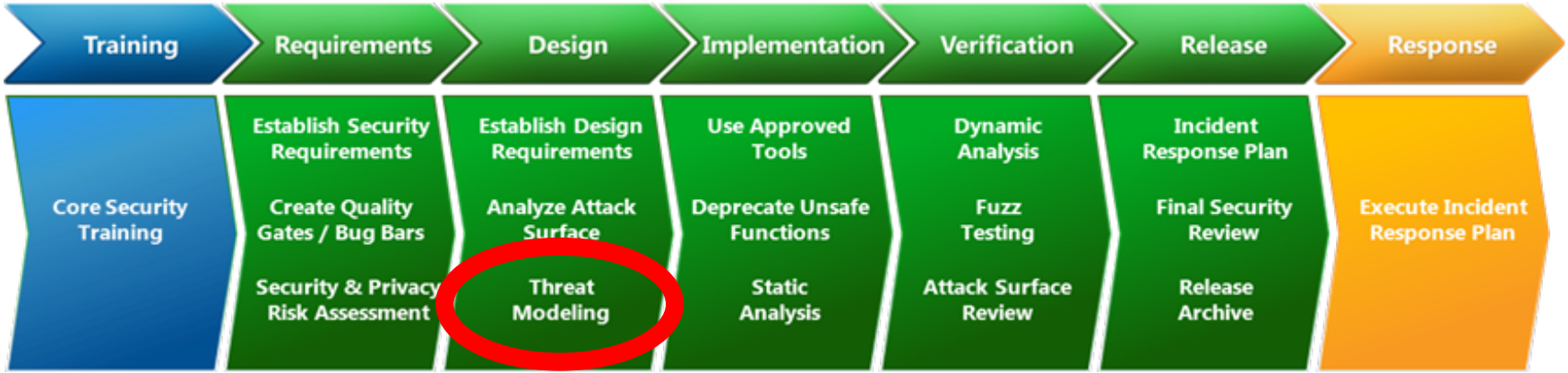
Supply Chain. Общая ИБ гигиена



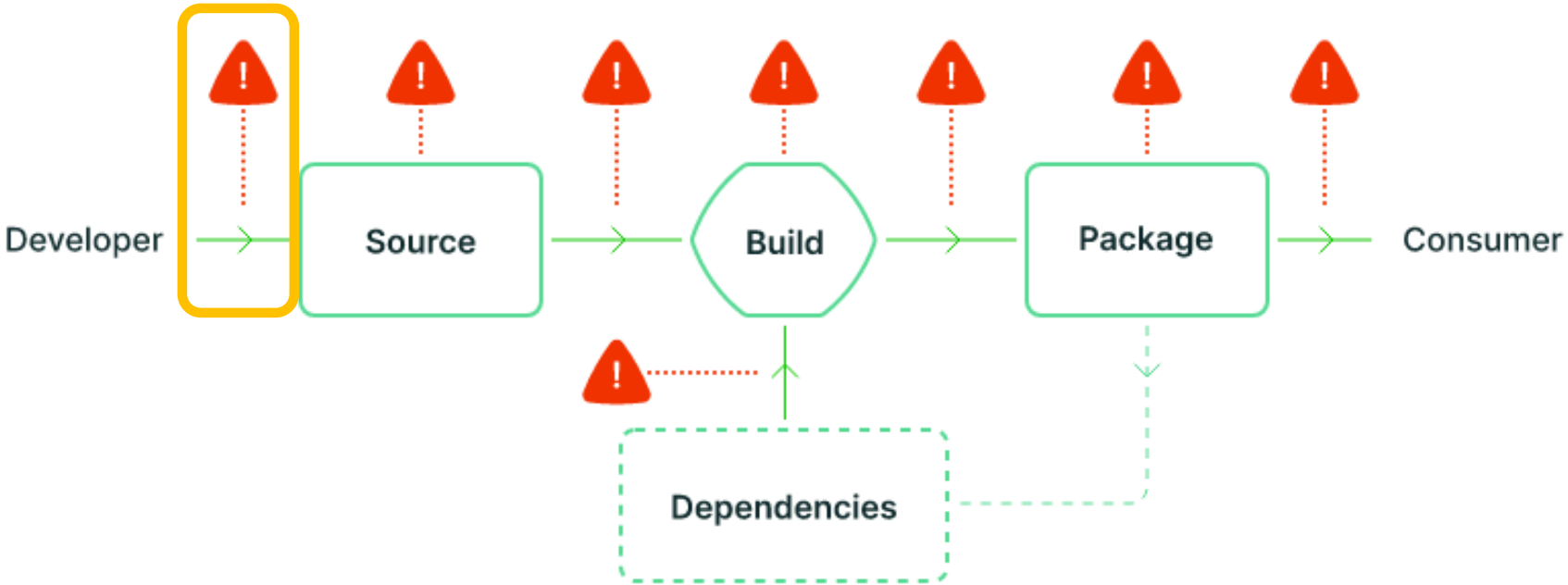


- Базовая ИБ-гигиена
  - Идентификация, аутентификация
  - AV
  - Логирование (хотя бы локальное)
- Инвентаризация активов
- RBAC
- Секреты под контролем
- Харденинг ОС в соответствии с рекомендациями вендора
- Контейнерная безопасность
- Сетевая безопасность

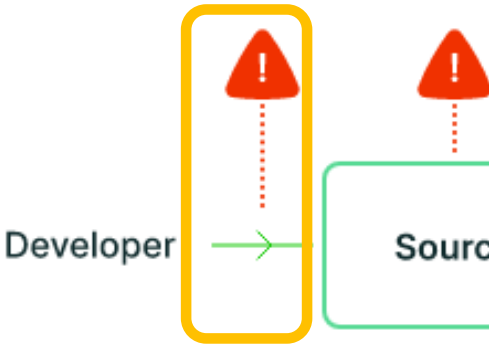
Supply Chain. Моделирование угроз

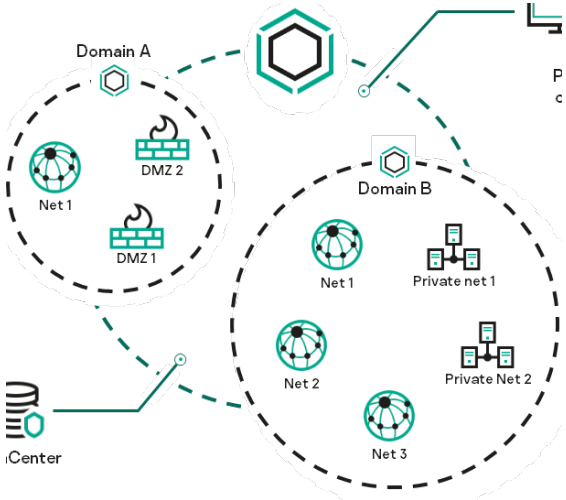


Supply Chain. Vector 1



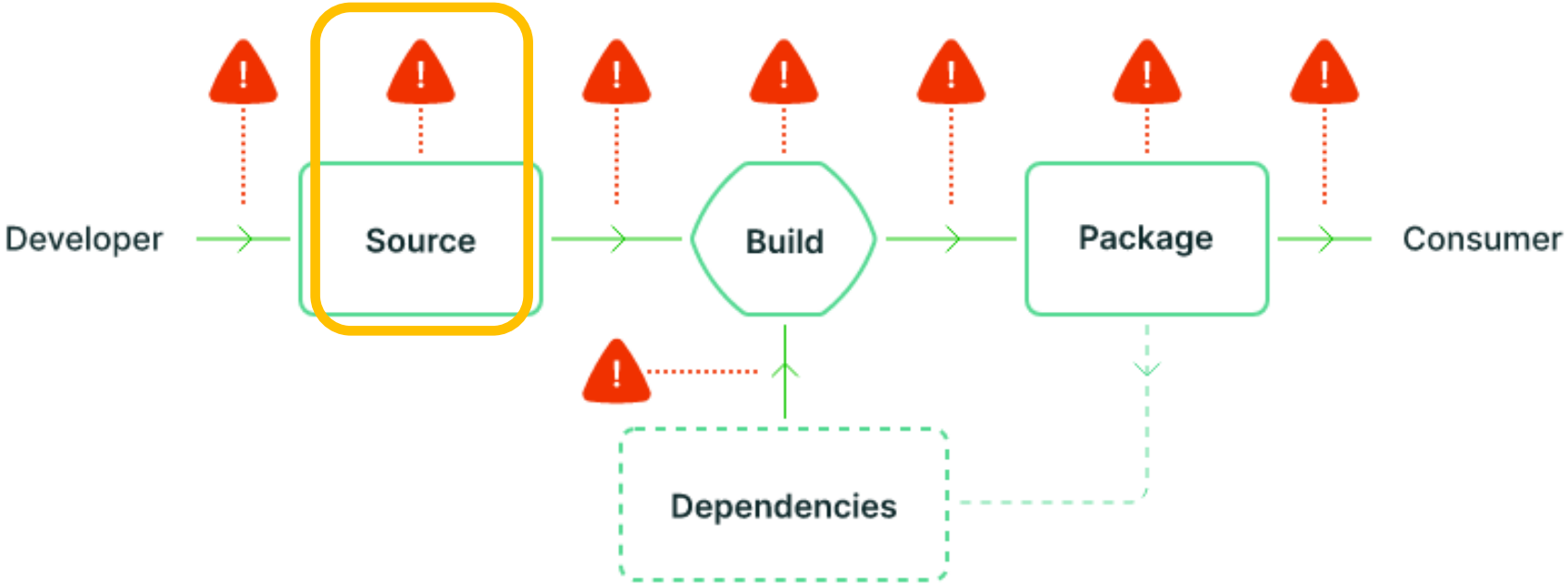
Supply Chain. Vector 1



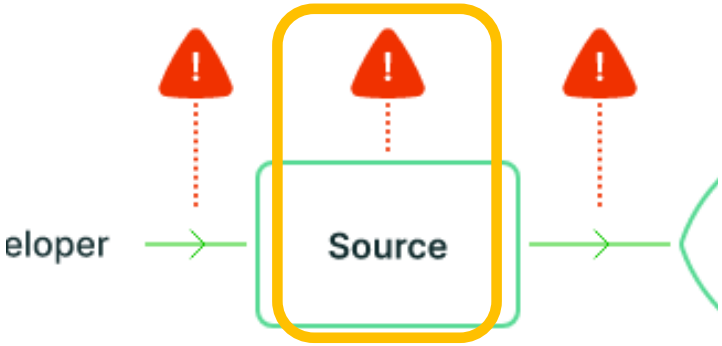


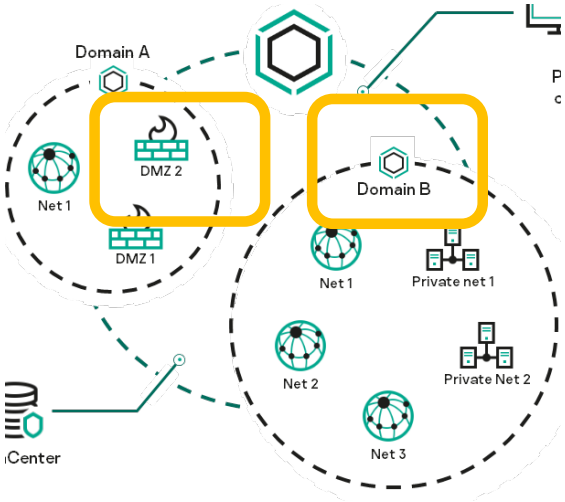
- Как и где Программист пишет код?
- Как можно изменить код?
  - рядовой сотрудник?
  - DevOps?
  - Программист?
- Как распределены права на изменение кода?
- Какие инструменты для заливки кода?
  - Их можно подменить?
- Изменения кода контролирует (Code review)?
- Что если Программист оставил "левый" код?

Supply Chain. Vector 2



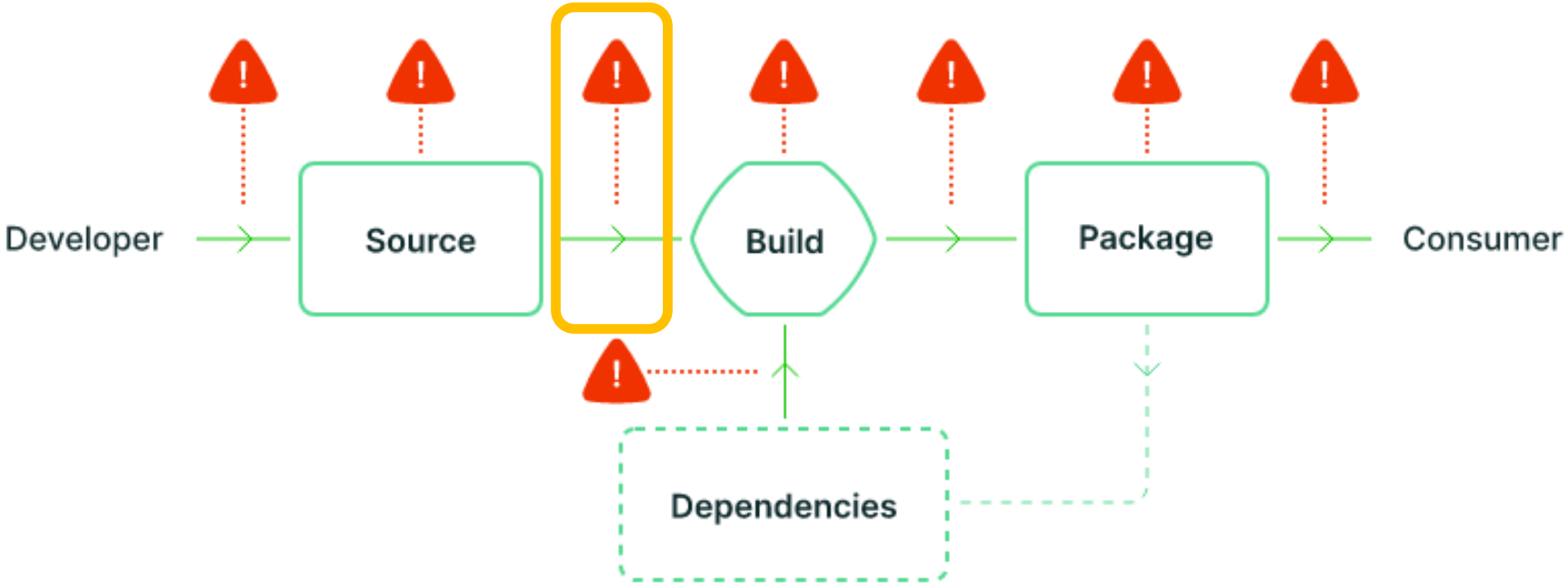
Supply Chain. Vector 2



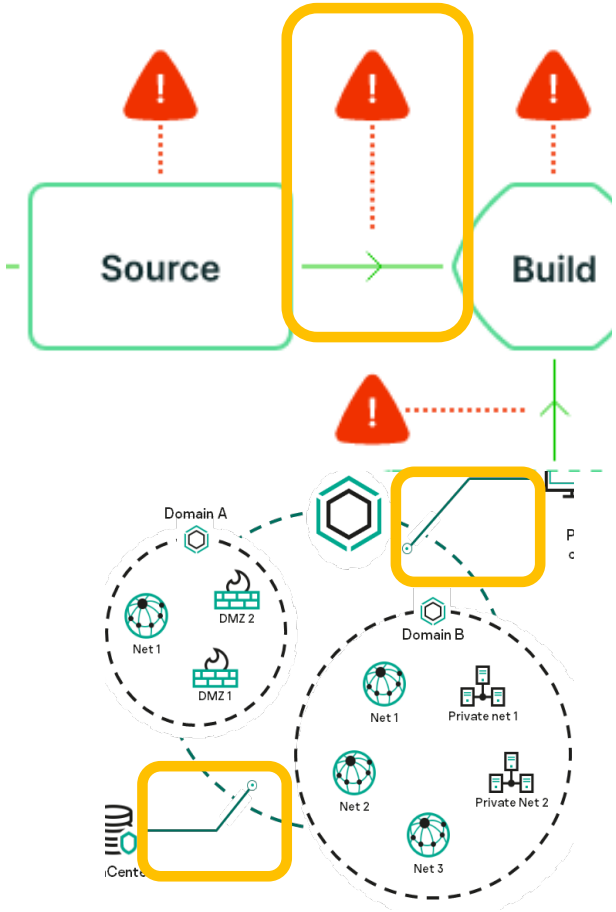


- Как и где хранится код?
- Как может подменить код?
- Кто может подменить конфигурации (от FW например)?
  - В репозитории?
  - В БД?
  - На серверах хостинга репозитория?
- Как часто и откуда обновляются инструменты / окружение работы с кодом?
- Кто может изменить права доступа к конфигурациями?
- Как часто и откуда обновляются инструменты работы с кодом?
- Есть ли доверие к окружению?
- Есть ли журналирование доступа?
- Есть ли доверие к инструментам?
- Есть ли журналирование доступа?

Supply Chain. Vector 3



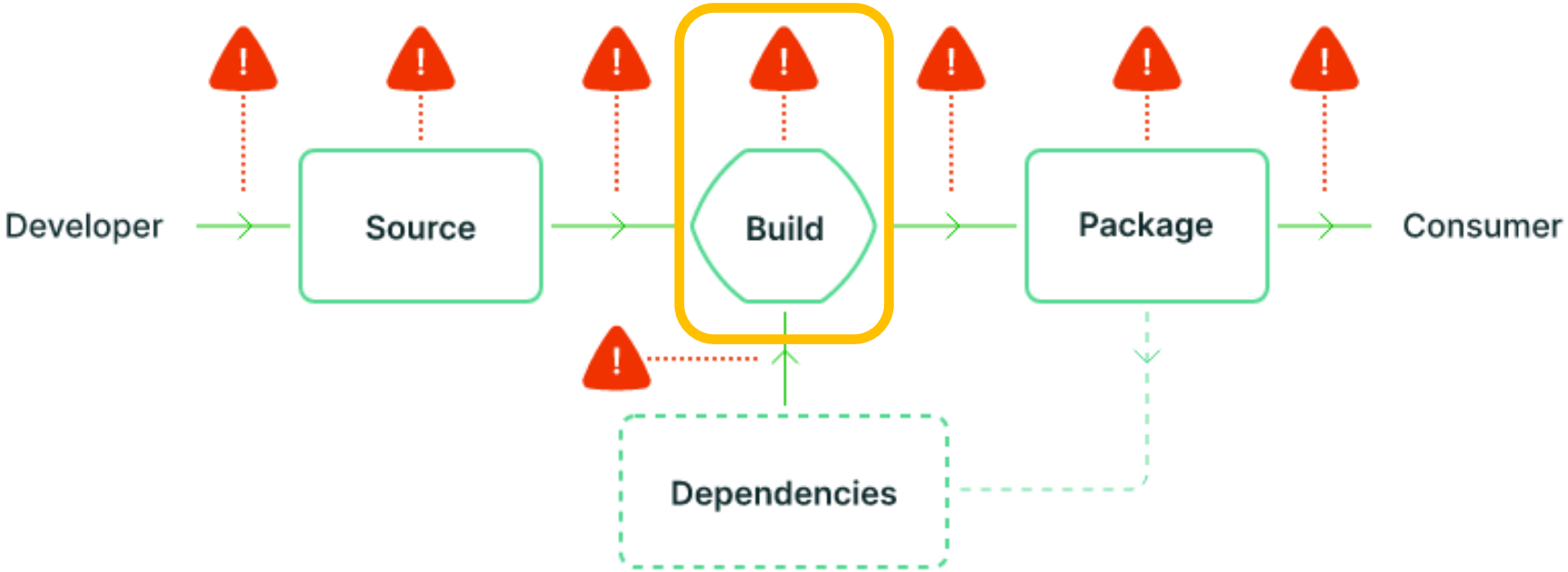
Supply Chain. Vector 3



- Как осуществляется защита сети?
- Не используется ли NTLMv1?
- Везде ли используется Kerberos?
- Сколько у вас «старых приложений» не использующих TLS?
- Какие приложения не контролируют целостность?
- А точно ли «закрытые сегменты» сети не имеют доступ в «дикий» интернет?

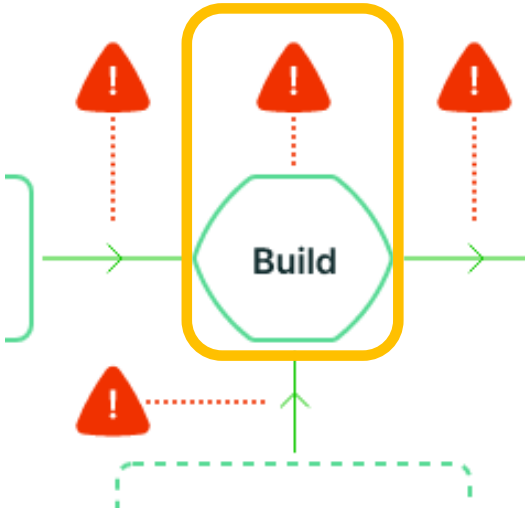
- Как осуществляется защита сети?
- Можно ли подменить трафик
- Можно ли подменить трафик
- Как build агенты
- Авторизуются в Source control?
- Понимают какой код надо брать для сборки (нет ли подмены)?
- Кто и чем контролирует целостность?
- Разграничение доступа?
- А точно ли исходники не скачиваются из «дикого» интернет?
- А кто проверял? Точно есть исключения.
- А кто проверял?
- Нужны ли эти исключения?

Supply Chain. Vector 4



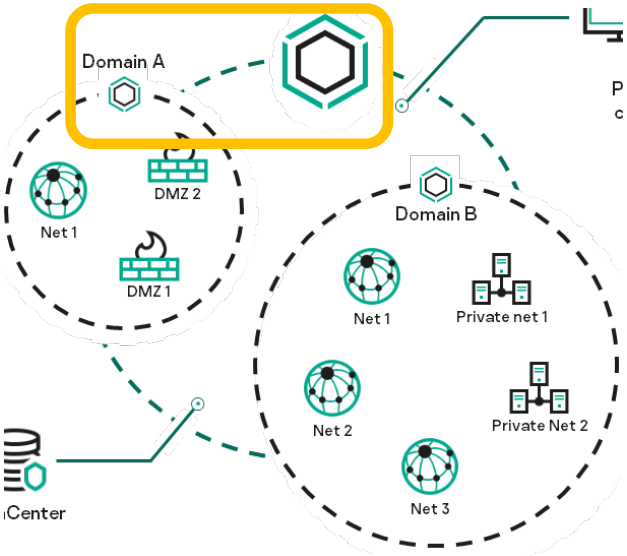
https://slsa.dev/

Supply Chain. Vector 4



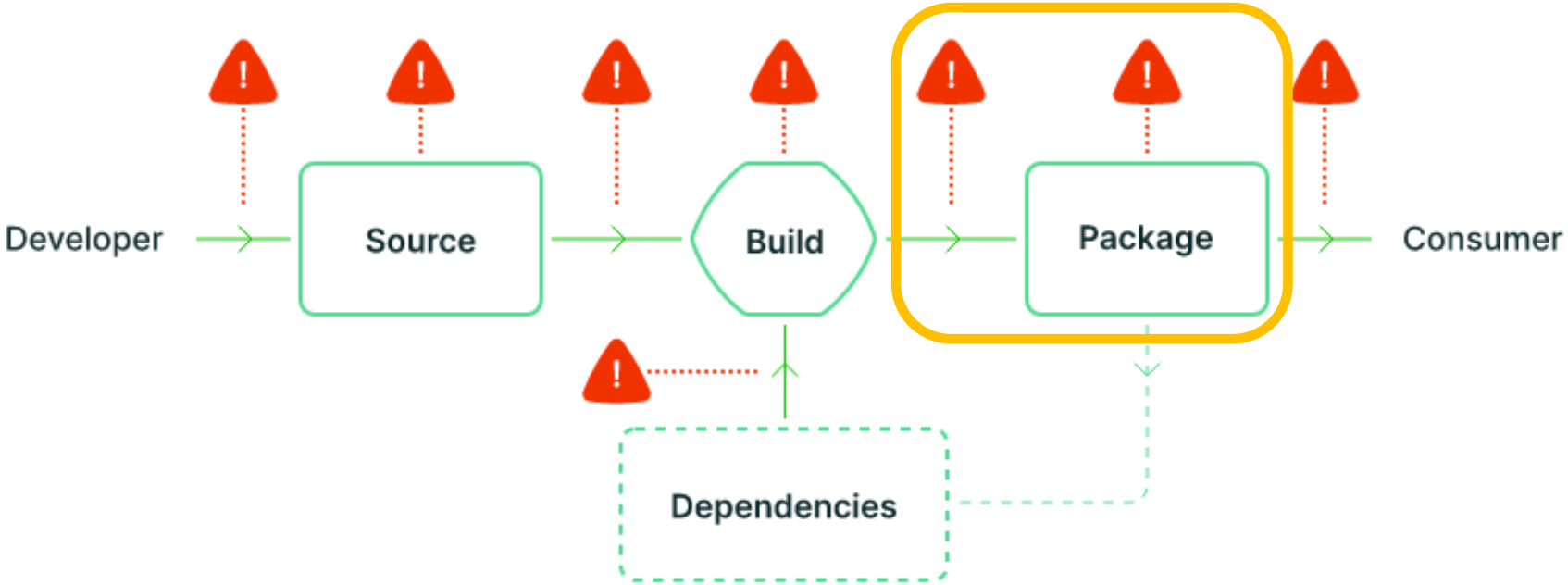
- Как обеспечивается контроль целостности окружения сборки?
- Контроль целостности инструментов
  - Сборки (компиляторы, сборщики)
  - SAST
  - Электронной подписи
- Есть ли доступ в интернет?
- Используется ли доверенный репозиторий?
- Имеется ли доверие к артефактам на выходе

Supply Chain. Vector 4

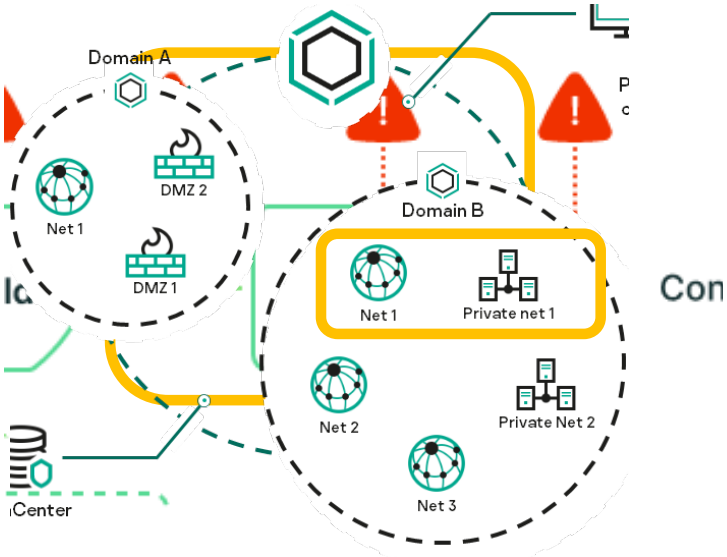


- Обеспечен hardening AD?
  - AV? Логирование? SIEM?
- Есть сетевые ограничения?
  - Есть ли доступ в интернет с DC?
  - Зачем?
  - Репликации домена идут по защищенному протоколу?
- Каковы доверия с другими доменами?
- Каковы доверия с другими, «дружественными» сетями
  - Нет у вас «друзей» ☺ это **ваша** ответственность

Supply Chain. Vector 5



Supply Chain. Vector 5

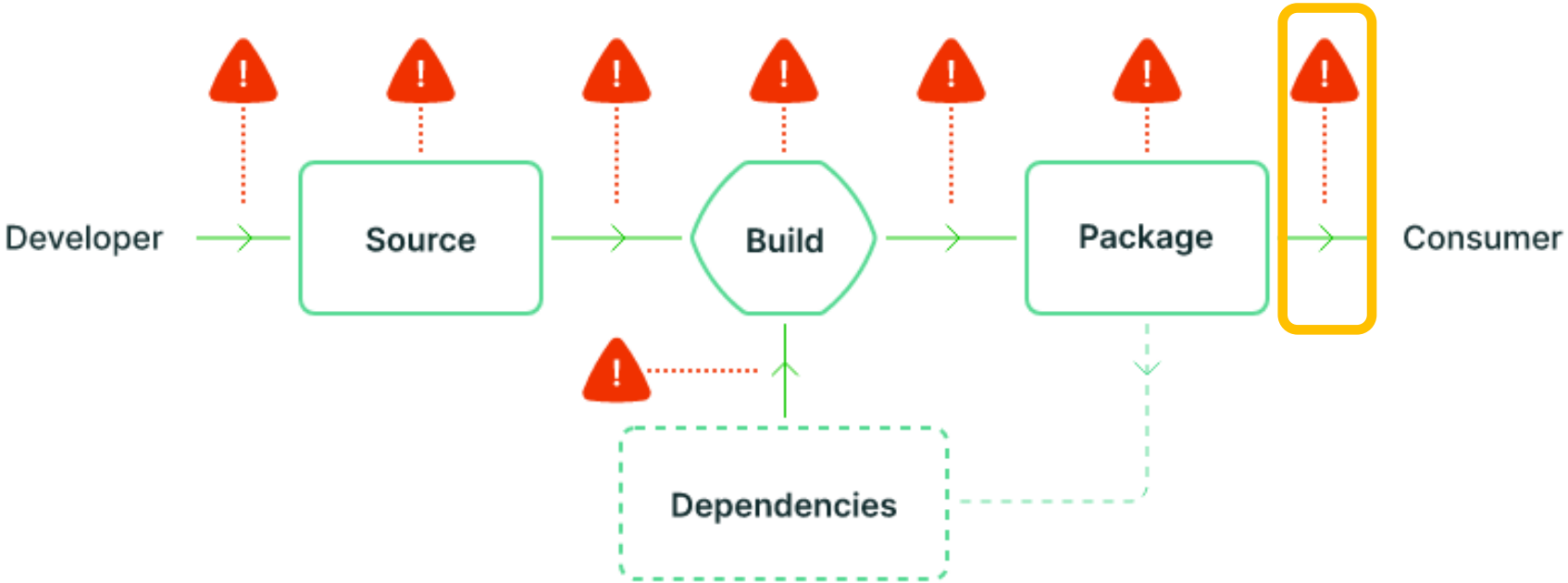


- Можно ли доверять сети?
- Каковы проверки ICS-модулей перед установкой?
- Какова цель ICS-инструментов?
  - ЭЦП? Хэш сумма? Откуда ее берем?
- Осуществляется ли подпись пакетов?
- Каково доверие к артефактам на выходе?
- Как ICS может проверить пользователь?

Можно ли доверять сети?
Каковы проверки ICS-модулей перед установкой? Можно ли доверять?
Какова цель ICS-инструментов?
ЭЦП? Хэш сумма? Откуда ее берем?
Осуществляется ли подпись пакетов?
Каково доверие к артефактам на выходе?
Как ICS может проверить пользователь?
Есть ли проверка целостности того, что сейчас работает?
Где и как хранятся «секреты» для доступа к ним?

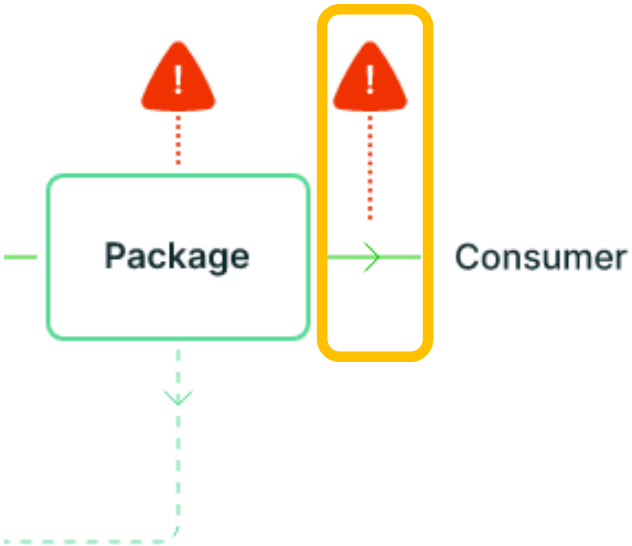
Supply Chain. Vector 6

Типовые векторы атаки на цепочку поставок



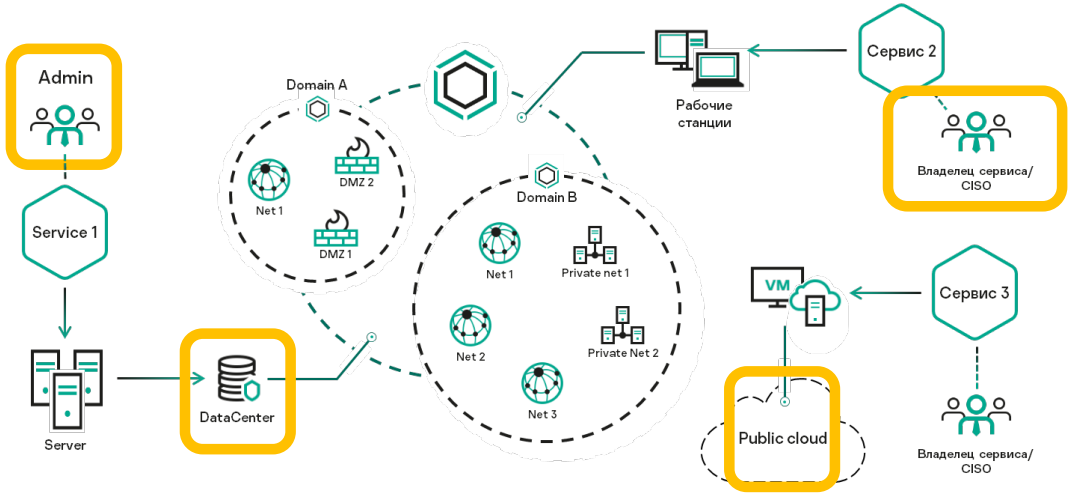
https://slsa.dev/

Supply Chain. Vector 6



- Возможна ли проверка канала получения продукта? Доверен ли канал?
- TLS? Локальные проверки?
    - Доверие к сертификату?
- Используем CDN? Можно ли доверять?
    - Нужны ли локальные проверки?
- Организована ли поддержка пользователя?
- Используется дополнительный контент (картинки, маркетинг и пр.) без защиты?
- Используем DDOS защиту?

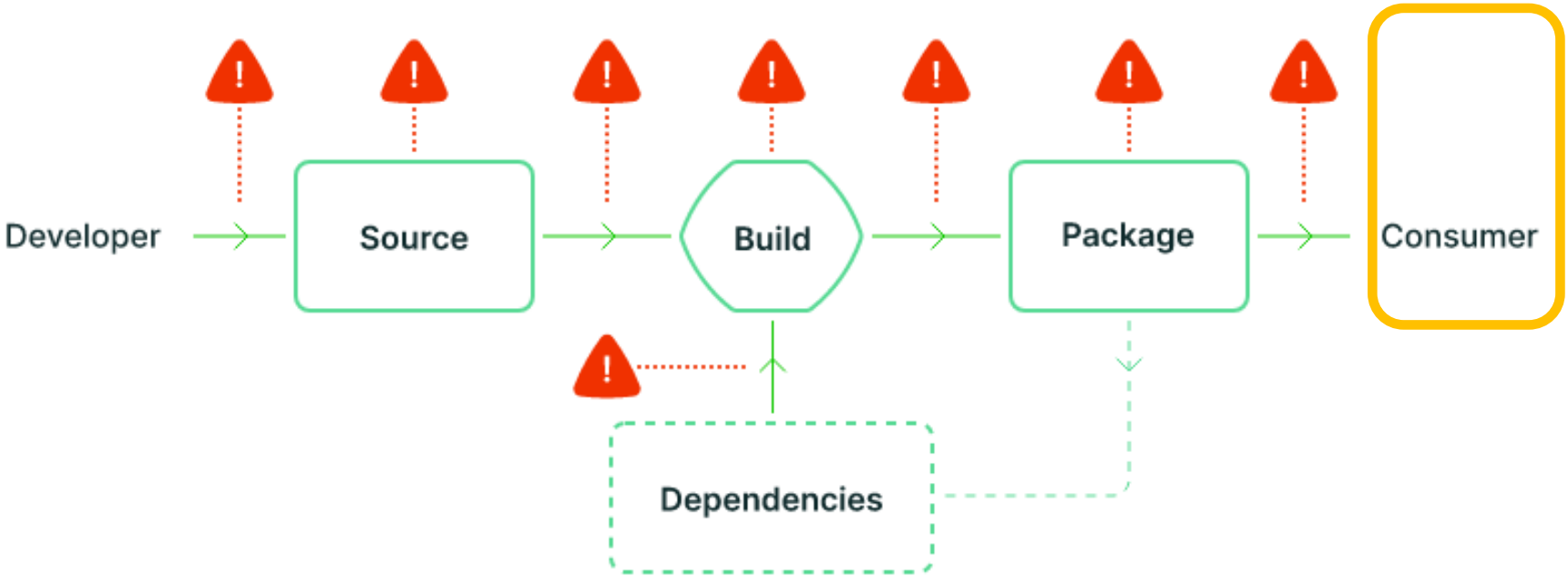
Supply Chain. Vector 6



- Администраторы: кто они? Сотрудники? Подрядчики?
- Техподдержка вендора? Как подключится? С какими секретами? Есть контроль отключения?
- Как часто проводится Аудит доступа (права, FW, версии прошивок и т.д.)?

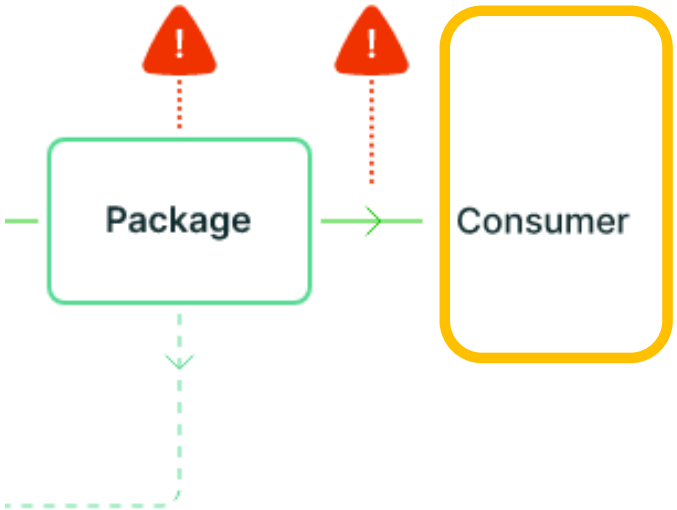
Supply Chain. Vector 7

Типовые векторы атаки на цепочку поставок



https://slsa.dev/

Supply Chain. Vector 7



- Пользователь имеет возможность проверить «что я получил-то?»
  - Если нет – все выше применённое не важно
- У пользователя должна быть возможность пожаловаться ☺
  - И получить ответ!

Supply Chain. Чем подтвердить митигацию рисков

ISO 27001

SOC2 audit

Внутренний аудит

EU Cyber Resilience Act

Регулярный анализ и пересмотр рисков

Supply Chain. Что почитать на досуге

OWASP Top 10 CI/CD Security Risks

slsa.dev

OWASP DevSecOps Guideline

Kaspersky for DevSecOps (OSSFeed)

Спасибо!

SECURITY IS EVERYONE'S RESPONSIBILITY

Дмитрий Шмойлов

kaspersky