DevOops 2023

(Не)стандартный подход к моделированию Supply Chain Attack

Васин Вячеслав

Deputy Head of Security Assessment, Kaspersky

Whoami

- Увлекаюсь наступательной безопасностью. Начинал с анализа защищенности приложений.
- Последние несколько лет занимаюсь анализом защищенности, тестированием на проникновение и проектами по оценке в формате Red Teaming.

Вячеслав Васин
@anywhere808

Agenda

- Что такое Supply Chain Attack
- Примеры и последствия Supply Chain Attack
- Методы атак и причины их возникновения
- Как защититься, лучшие практики и фреймворки
- Истории из жизни и рекомендации

Disclaimer

Доклад предназначен для образовательных целей и не заменяет стороннего независимого профессионального мнения на эту тему.

Факты и мнения, содержащиеся в презентации, отражают только личную точку зрения автора и не имеют никакого отношения к точке зрения или позиции компании.

Что такое Supply Chain Attack?

Что такое цепочка поставок?

Что такое цепочка поставок?

Взаимосвязанная система ресурсов, участвующая в жизненном цикле продукта, от момента его проектирования до передачи конечному пользователю/потребителю.

В цепочку поставок включаются человеческие, организационные, материальные и интеллектуальные ресурсы, необходимые для создания и реализации товара.

https://encyclopedia.kaspersky.ru/glossary/supply-chain

Что такое Supply Chain Attack?

Злонамеренная атака, инициированная через доверенную стороннюю систему, программное обеспечение или механизмы доставки продуктов, совершенная до момента их получения конечным потребителем с целью компрометации данных или системы.

https://attack.mitre.org/techniques/T1195

Какие бывают Supply Chain Attack?

Обычно:

- Software
- Hardware
- Firmware

Согласно MITRE:

- T1195.001 Compromise Software Dependencies and Development Tools
- T1195.002 Compromise Software Supply Chain
- T1195.003 Compromise Hardware Supply Chain

Какие бывают Supply Chain Attack?

Обычно:

- Software
- Hardware
- Firmware

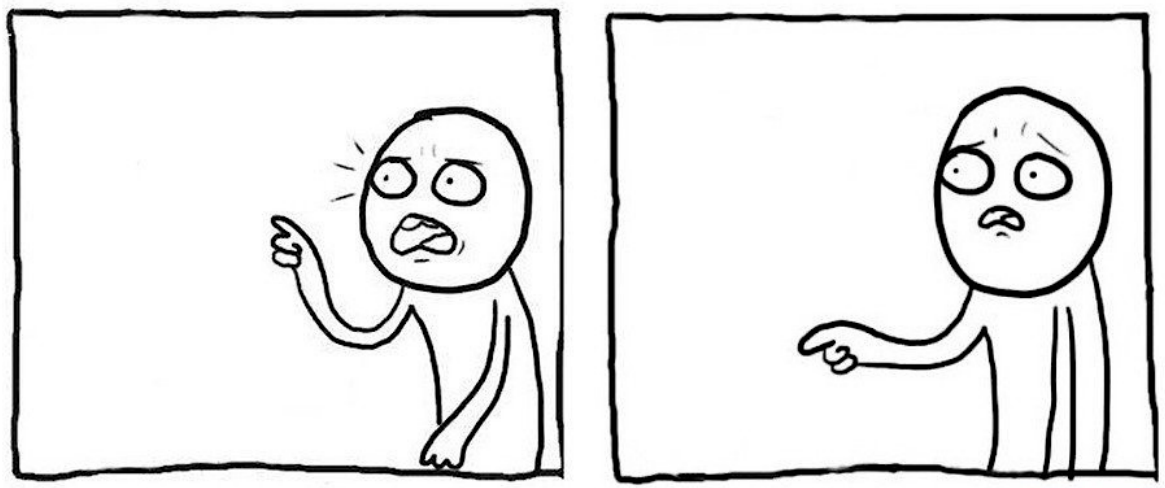
Согласно MITRE:

- T1195.001 Compromise Software Dependencies and Development Tools
- T1195.002 Compromise Software Supply Chain
- T1195.003 Compromise Hardware Supply Chain

Если посмотреть на активы, которые влияют на поставку:

- Hardware
- Software
- Services
- People

Но… как же Software Supply Chain Attack?



Software Supply Chain Attack

Нацелены на разработчиков и поставщиков ПО. Цель состоит в том, чтобы получить доступ к исходным кодам, механизмам обновления или процессам сборки путем компрометации легитимных приложений.

https://learn.microsoft.com/en-us/microsoft-365/security/intelligence/supply-chain-malware

Software Supply Chain Attack

- Направлены на менее безопасное, но доверенное стороннее ПО
- Направлены на распространенные компоненты и зависимости
- Атака на стороннюю компанию может затронуть ваших пользователей

Ок, почему это важно?

- Современная разработка представляют собой сложные среды с широким спектром инструментов CI/CD. Разработчики используют opensource, а каждый проект опирается на десятки зависимостей.
- Согласно отчетам аналитических компаний, риск применения Supply Chain Attack входит в ТОП-5 наиболее критичных и вероятных среди других типов операционных рисков за последние три года.

В 2021 число атак на цепочки поставок увеличилось более чем на 300 %

https://blog.aquasec.com/software-supply-chain-attacks-2021

Ок, почему это важно?

7 Top Trends in Cybersecurity for 2022:
Trend No. 3: **Digital supply chain risk**

- По прогнозам Gartner, к 2025 году 45% организаций во всем мире столкнутся с Software Supply Chain Attack.
- *«Руководители служб ИБ и управления рисками должны совместно с другими подразделениями определять приоритетность рисков, связанных с цепочками поставок».*

www.gartner.com/en/articles/7-top-trends-in-cybersecurity-for-2022

Тренды в 2023

742%

- зафиксирован среднегодовой рост атак за последние 3 года

3,4 миллиарда

- уязвимых загрузок можно избежать ежемесячно

https://www.sonatype.com/resources/2023-software-supply-chain-report

Примеры Supply Chain Attack

Примеры Supply Chain Attack в жизни

- SolarWinds
- British Airways
- 3CX
- Atlassian
- Codecov
- Kaseya
- GitHub
- CCleaner
- …

Software Supply Chain Attack

Short Summary

What

Компрометация ПО или одной из его зависимостей на любом этапе:

- разработки
- поставки
- использования

How

Несанкционированный доступ к средам разработки и инфраструктуре, таким как:

- системы контроля версий
- open sources репозитории
- линии непрерывной интеграции
- серверы сборки
- серверы приложений

Software Supply Chain Attack

Short Summary

What

Компрометация ПО или одной из его зависимостей на любом этапе.

How

Несанкционированный доступ к средам разработки и инфраструктуре.

Impact

Позволяет злоумышленнику модифицировать исходный код, скрипты и пакеты, а также оставлять «бэкдоры» для кражи данных из среды атакуемого. Атаки могут исходить и от инсайдеров.

Типовые методы атак и причины их возникновения

Давайте сначала разберем последствия?

Последствия Supply Chain Attack

- Финансовые потери (прямые и косвенные)
- Потеря конфиденциальных данных
- Нарушение операционной деятельности
- Ущерб репутации
- Юридические и нормативные последствия
- Национальная безопасность (критически важные ресурсы и жизнь)

Типы и основные источники (мотивы)

Источники:

- внешние субъекты угроз
- злонамеренные инсайдеры
- прогосударственные субъекты угроз
- бизнес конкуренты
- незащищенный поставщик
- скомпрометированное программное обеспечение

Мотивы:

- just for fun: потренироваться
- саботаж
- денежный
- получение важной информации
- использование ПДн (OSINT)
- сократить циклы разработки (украсть код, алгоритмы и т.д.)

Какие методы атак используются

Метод	Пример
Заражение вредоносным ПО	Шпионское ПО для кражи учетных записей сотрудников вашей организации
Социальная инженерия	Фишинг, фейковые приложения, тайпсквоттинг, поддельные точки доступа Wi-Fi для того, чтобы убедить поставщика/сотрудника сделать что-то
Брутфорс (перебор «грубой силой»)	Перебор SSH паролей, подбор аутентификационных данных для логин форм
Эксплуатация уязвимостей ПО	SQL инъекции, переполнение буфера в приложениях
Эксплуатация уязвимостей конфигураций	Использование проблем конфигураций
Физические атаки или модификация	Модификация оборудования, физическое вторжение
Разведка по открытым источникам (OSINT)	Поиск ключей, логинов, паролей в открытом доступе

Как с этим всем бороться

Мы явно не первые кто об этом задумался...

Protection/Maturity: Frameworks

OWASP

Software Component Verification Standard

- v.1 от 2020:
  (в последние годы почти нет обновлений)
- https://owasp.org/scvs

SLSA ("salsa")

- Supply-Chain Levels for Software Artifacts
- v.1 от 2023:
  (долго была в альфе)
- https://slsa.dev

OWASP SCVS

SCVS – созданный сообществом открытый фреймворк, который используется для определения общих видов активностей, средств контроля и лучших практик, которые могут помочь в выявлении и снижении рисков связанных с Software Supply Chain.

SCVS – преследует цель: определить базовый уровень и путь к повышению зрелости по мониторингу рисков и проблем в Software Supply Chain.

OWASP SCVS: Control Families

6 направлений контроля:

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

3 уровня проверки:

- SCVS Level 1 (низкая степень)
- SCVS Level 2 (средняя степень)
- SCVS Level 3 (высокая степень)

SLSA

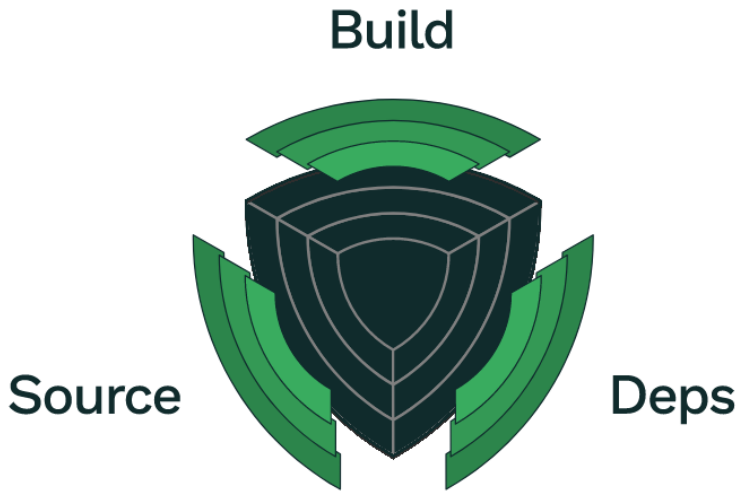
Фреймворк (гайдлайн), содержащий чек-лист стандартов и средств контроля для предотвращения несанкционированного доступа, повышения целостности и защиты пакетов и инфраструктуры.

Производители могут следовать рекомендациям SLSA, чтобы сделать свою цепочку поставок программного обеспечения более безопасной, а потребители могут использовать SLSA для принятия решений о том, доверять ли пакету программного обеспечения.

SLSA: Security Levels

Каждый уровень содержит требования к источнику кода (Source), процессу сборки (Build), а также к дополнительной информации о происхождении артефактов (Provenance).

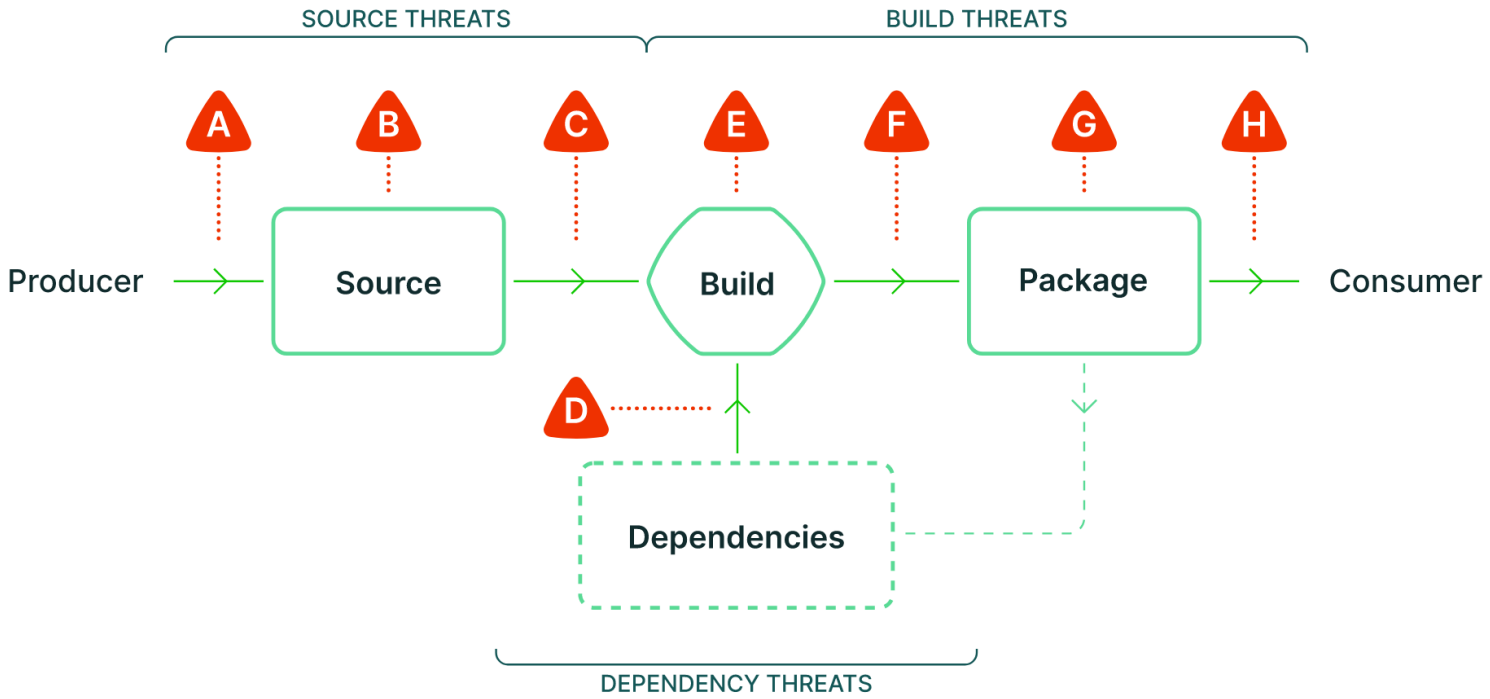
- L0: Никаких гарантий
- L1: Процесс сборки задокументирован
- L2: Сборка устойчива к компрометации
- L3: Дополнительная устойчивость
- L4: Высочайший уровень доверия



https://slsa.dev/spec/v0.1/requirements

https://slsa.dev/spec/v1.0/levels

SLSA: Supply Chain Threats & Mitigations



SOURCE THREATS

- A Submit unauthorized change
- B Compromise source repo
- C Build from modified source

DEPENDENCY THREATS

- D Use compromised dependency

BUILD THREATS

- E Compromise build process
- F Upload modified package
- G Compromise package repo
- H Use compromised package

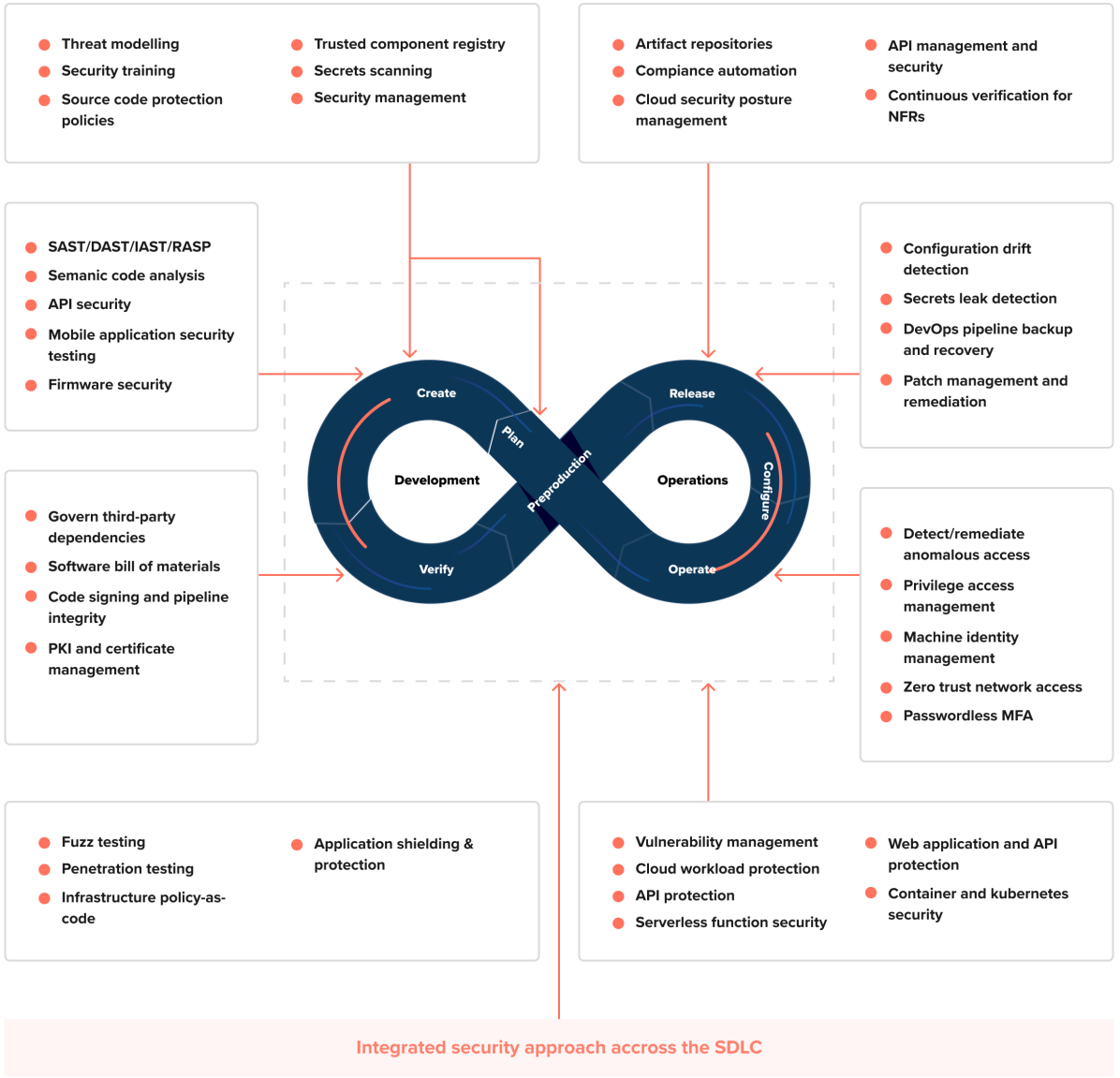
Это все или есть что-то еще?

Как с этим всем бороться

(Не)стандартный подход

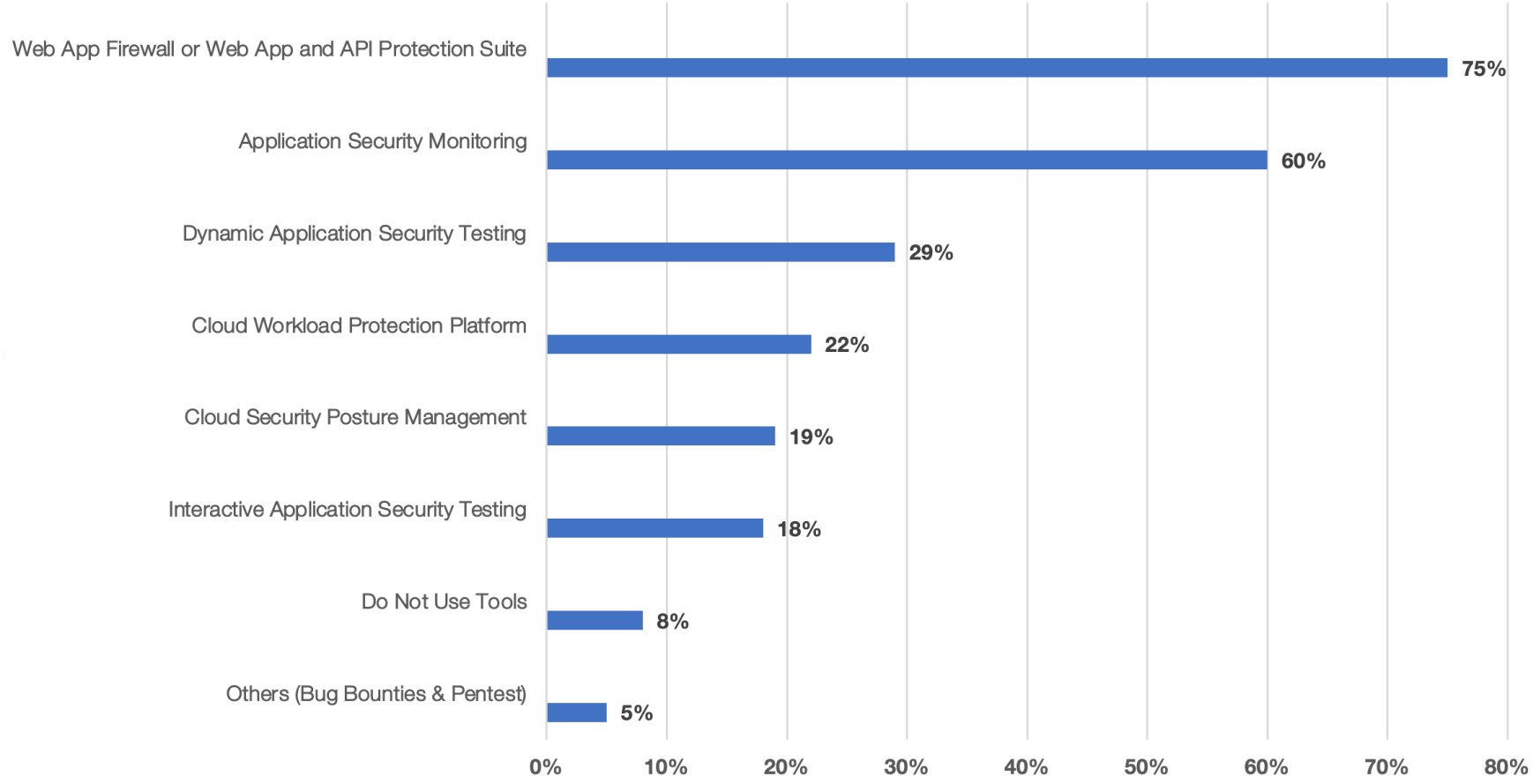
Какие подходы используют DevSecOps?

Map Security Needs to DevSecOps Tools in the SDLC



Source: Gartner и Appknox

Инструменты для защиты Cloud-Native Apps



Source: Gartner 2021 Enabling Cloud-Native DevSecOps Survey

Ок, так в чем (не)стандартность ?

- **Scenario-Based Penetration Testing** – вариант альтернативного мышления и комплексного взгляда на все аспекты со стороны потенциального злоумышленника.
- Поможет вам определить проблемы бизнес-технологий и предоставить возможные альтернативные/применимые решения безопасности для защиты ваших продуктов, сетей, процессов и многого другого.

продемонстрировать реальные риски; определить способы получения доступа; помочь IT, DevSecOps и Blue Team

Пример сценария для Supply Chain

Reconnaissance

- Разработчики, QA, DevOps (DevSecOps)
- Репозитории, Pipeline

Credential Access

- Утечки учетных данных, фишинг – для доступа к компьютеру компании
- Кража Cookies/Session – для доступа к Github
- Кража учетных данных – для доступа к другим релевантным системам

Discovery & Deploy

- Контроль разрешений/доступов
- Доступ к репозиториям кода, истории коммитов
- Поиск точек входа для внедрения коммита/кода

Как это применить?

Protection/Maturity: Frameworks

A New Open Framework For Releasing Secure Products

OSC&R (OSCAR)

Open Software Supply Chain
Attack Reference

A pipeline bill of materials
https://pbom.dev

OSC&R

Открытый фреймворк, который направлен на комплексный, систематический и практический способ понять поведение и методы злоумышленников в отношении Software Supply Chain.

Как и MITRE ATT&CK, OSC&R представляет собой структурированное представление о тактиках, методах и процедурах (TTP), используемых злоумышленниками.

OSC&R vs SLSA

SLSA — направлен на отслеживание различных типов артефактов программного обеспечения в цепочке поставок на основе уровня их целостности. Целостность подразумевает гарантию того, что артефакт не был подделан или изменен несанкционированным образом.

OSC&R — направлен на понимание поведения и методов атакующих, используемых для компрометации цепочки поставок программного обеспечения. OSC&R предоставляет обзорную информацию о цели атаки и ее текущей стадии.

OSC&R направления

- Container Security
- Open Source Security
- SCM Posture
- Secrets Hygiene
- Code Security
- Cloud Security
- CI/CD Posture
- Artifact Security
- Infrastructure as code

OSC&R направления

- **Cloud Security**

Reconnaissance (11)	Initial Access (25)	Execution (12)	Persistence (8)	Defense Evasion (7)	Credential Access (8)	Lateral Movement (2)	Collection (5)	Exfiltration (3)	Impact (5)
Active scanning	Compromised token	Installation scripts	Implant in zombie instance	Misconfigured traffic log settings	Harvest tokens from environment variables	Overprivileged user account	Unencrypted data at rest	Bypass of outbound traffic control	Resource hijacking
Scan configuration on public resources	Compromised user account	Cloud workload	Create access token	Misconfigured audit logs settings			Unencrypted data in transit		Misconfiguration of serverless workloads
Accidental public disclosure of internal resources	Compromised service account		Untagged resources	Malicious compiler or interpreter			Weak encryption		Malicious code in artifacts
Exposed storage	Shadow IT			SaaS sprawl			Sensitive information in logs		
	Exposed internal API			Misconfigured security measures			Sensitive information in environment variables		
	Exposed storage								
	Exposed database								
	Permissive network access								
	Weak authentication methods								
	External user accounts								

Codecov Breach: Techniques

Reconnaissance	**T0103 - Scan Public Artifacts For Secrets** The attackers scanned Docker Hub and discovered git credentials in the official Codecov image T0103 page
	T0142 - Accidental Public Disclosure Of Internal Resources The git credentials was indeliberately saved in the public docker image T0142 page
Initial Access	**T0114 - Compromised Service Account** The attackers gained access to Codecov's Git repo T0114 page
Impact	**T0191 - Malicious Code In Artifacts** The Bash Uploader script was modified to exfiltrate environnent variables of the running system T0191 page

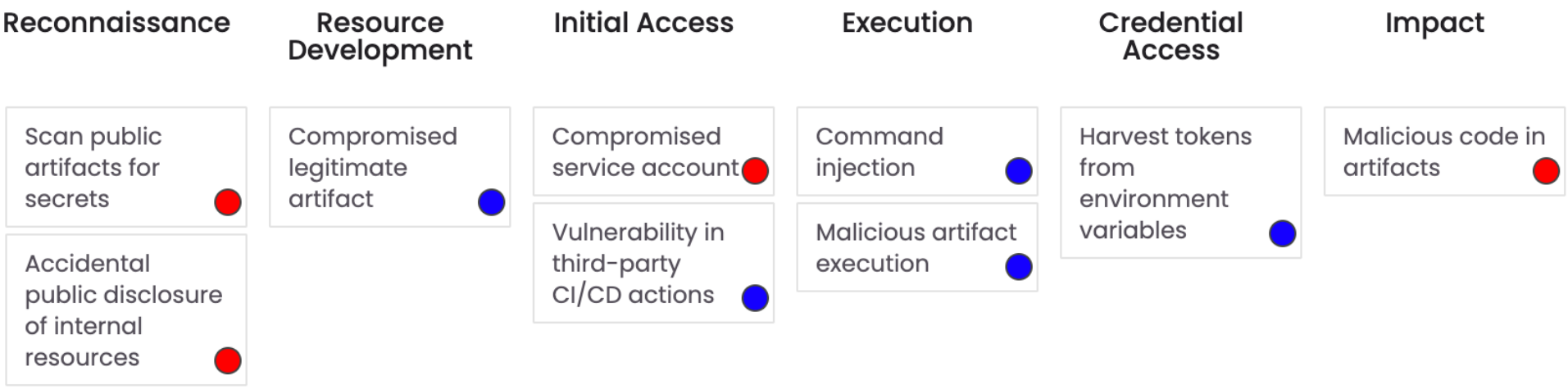
Resource Development	**T0121 - Compromised Legitimate Artifact** T0121 page
Initial Access	**T0122 - Vulnerability In Third-Party CI/CD Actions** The Bash Uploader script was used as part of 3rd party Github actions T0122 page
Execution	**T0118 - Command Injection** When the Codecov image was executed - the malicious implant in the Bash Uploader script exfiltrated environment variable to the attacker controlled T0118 page
	T0159 - Malicious Artifact Execution Customers that utilized the Codecov image were impacted T0159 page
Credential Access	**T0140 - Harvest Tokens From Environment Variables** T0140 page

LEGEND

- Codecov
- Codecov users

https://pbom.dev/campaign/?cid=AS3

Codecov Breach: Campaign Map



LEGEND

- Codecov
- Codecov users

https://pbom.dev/campaign-map/?cid=AS3

Примеры из жизни

Дисклеймер: Все события вымышлены, любые совпадения случайны

Пример А

Финтех, стартап

Пример А

Финтех, стартап

Начальные условия

Небольшая компания на 50-100 сотрудников, новое приложение:

- отсутствует периметр
- распределенная команда
- macOS и облачные сервисы

Пример A

Финтех, стартап

Начальные условия

Небольшая компания на 50-100 сотрудников, новое приложение:

- отсутствует периметр
- распределенная команда
- macOS и облачные сервисы

Результат

Доступ к клиентской базе, а также к исходным кодам бэкенда:

I. утечка личных учетных данных
II. вход в Slack с подобным паролем
III. отправка в «бро» IntelliJ IDEA проекта с вредоносным плагином
IV. доступ к IDE и соседним проектам

Пример Б

ИТ, корпорация

Пример Б

ИТ, корпорация

Начальные условия

Крупная компания, оказывают различные сервисы по ИТ:

- защищенный периметр
- все работают из офиса
- собственные сервисы, разработка и другие используют тонкий клиент

Пример Б

ИТ, корпорация

Начальные условия

Крупная компания, оказывают различные сервисы по ИТ:

- защищенный периметр
- все работают из офиса
- собственные сервисы, разработка и другие используют тонкий клиент

Результат

Компрометация исходного кода и персональных данных клиентов:

I. незащищенный подрядчик
II. .git на staging
III. множество CVE для CI/CD
IV. IDOR в исходном коде **=> доступ к данным на проде**

Рекомендации

7 ~~deadly sins~~ базовых советов

- Проведите комплексную проверку своих поставщиков и обучайте их
- Предполагайте, что вы пострадаете от утечки или вас уже взломали
- Проводите регулярно обучение по ИБ для всех участников команд
- Имплементируйте концепцию Zero-Trust и сегментацию сети
- Только доверенные зависимости и регулярная оценка opensource
- Используйте расширенную аутентификацию и принцип минимальных привилегии совместно с управлением привилегированным доступом
- Используйте инструменты кибербезопасности (не только AV и WAF, но и Threat Intelligence и External Attack Surface Management платформы)

7 ~~deadly sins~~ базовых советов

- Проведите комплексную проверку своих поставщиков и обучайте их
- Предполагайте, что вы пострадаете от утечки или вас уже взломали
- Проводите регулярно обучение по ИБ для всех участников команд
- Имплементируйте концепцию Zero-Trust и сегментацию сети
- Только доверенные зависимости и регулярная оценка opensource
- Используйте расширенную аутентификацию и принцип минимальных привилегии совместно с управлением привилегированным доступом
- Используйте инструменты кибербезопасности (не только AV и WAF, но и Threat Intelligence и External Attack Surface Management платформы)

Frame works

Penetration Testing & Red Teaming

Conclusion

- Увлекайтесь информационной безопасностью
- Разработайте и имплементируйте стратегию защиты
- Обучайте всех сотрудников основам информационной безопасности

Q&A