
Яндекс

Яндекс Облако

DevSecOps для облачного провайдера: опыт Яндекс.Облака

Антон Жаболенко, инженер по информационной безопасности

Содержание

Backend United #6: Табаско

Особенности безопасности облаков

Есть ли концептуальные различия в подходах к обеспечению ИБ в облаке?

Пожалуй, да

- Разделение ответственности
- Другие средства безопасности

Разделение ответственности

Клиент Яндекс.Облако

	Собственная инфраструктура	IaaS	PaaS / SaaS
Управление доступом к данным	✓	✓	✓
Безопасность ОС и приложений	✓	✓	●
Сетевая безопасность (Overlay)	✓	✓	●
Резервное копирование	✓	✓	●
Шифрование	✓	✓	●
Логи аудита	✓	●	●
Безопасность хранилища данных и оборудования	✓	●	●
Сетевая безопасность (Underlay)	✓	●	●
Физическая безопасность и катастрофоустойчивость (DR)	✓	●	●

Разделение ответственности в процессах

- Threat Detection
- Incident Response
- Patching/Updating

Правила в Облаке

- Данные пользователя принадлежат пользователю
- Доступом к данным управляет пользователь

Вызовы для security-команды Облака

- Нужно думать как о безопасности собственной инфраструктуры, так и о безопасности клиентов

Backend United #6: Табаско

Наш подход к обеспечению безопасности

Yandex Cloud Security Approach

Defense in depth: multiple protection layers

Yandex Cloud Security Approach

Security Development Lifecycle

- Security Culture
- Security Design Review
- Code Analysis
- Penetration Tests
- Response processes

Physical Security

- Own DCs
- Video surveillance
- Strict regulations for server maintenance

Infrastructure Security

- Security baselines depending on host or VM profile
- Security Operational Center

Credential Protection

- Employee Awareness
- Hardware token-based authentication
- Workstation security
- Bastion

Data Protection

- Virtual machine disks and files are stored in encrypted form
- MDB backups are encrypted for storage
- TLS

Backend United #6: Табаско

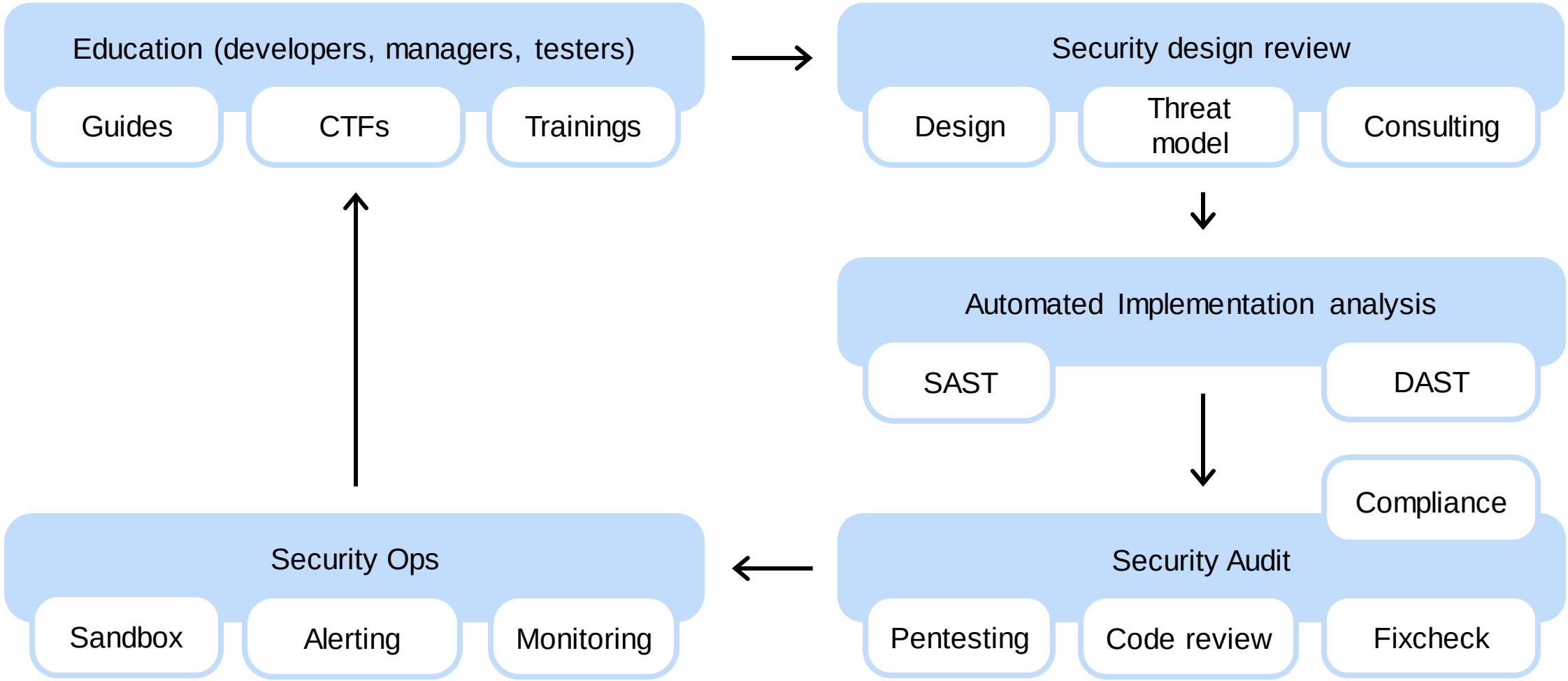
SDL в Яндекс.Облаке

Основные принципы

Ultimate responsibility на командах

- Ответственность за безопасность сервисов лежит на командах разработки
- Команда безопасности помогает сделать правильно и не ошибаться на разных этапах разработки

Secure Development Lifecycle в Яндекс.Облаке



Обучение

Команда безопасности регулярно готовит материалы для обучения разработчиков и поддерживает их в актуальном состоянии

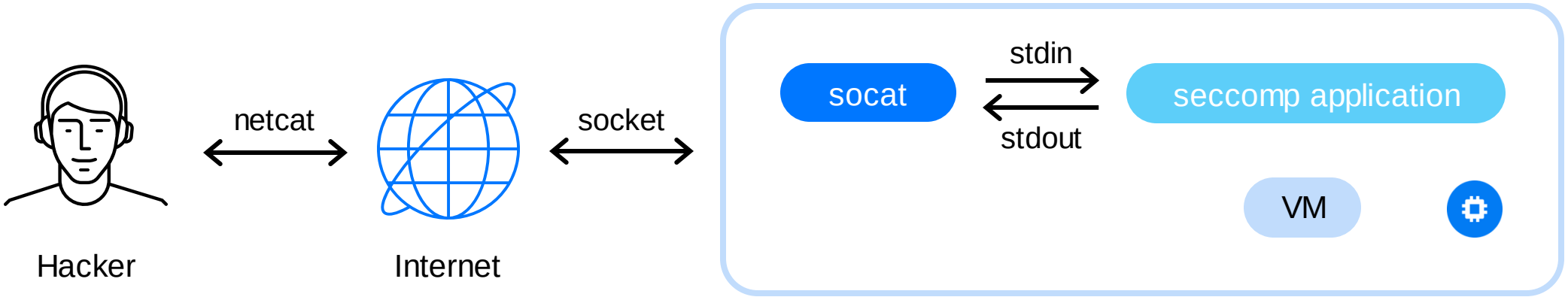
- Разбор уязвимостей, найденных командой безопасности во время аудитов
- Linux hardenings и контейнеризация
- Защита приватных данных
- Антифишинг
- NDA в Яндексе
- Требования стандарта ISO-270x в области управления ИБ
- Разработка безопасных приложений
- ...

CTF

Раз в год команда безопасности проводит внутренний CTF

- Задания готовит команда безопасности и заинтересованные сотрудники
- Призы за победу
- Задания по всем направлениям: от криптографии до бинарной эксплуатации и веба

Пример задачки на бинарщину с нашего CTF



Knowledge Exchange

Еженедельная встреча, на которой команды делятся своим опытом

- Команды рассказывают о частях облака, за которые они ответственны
- Любой может рассказать про свой сервис и его внутренности

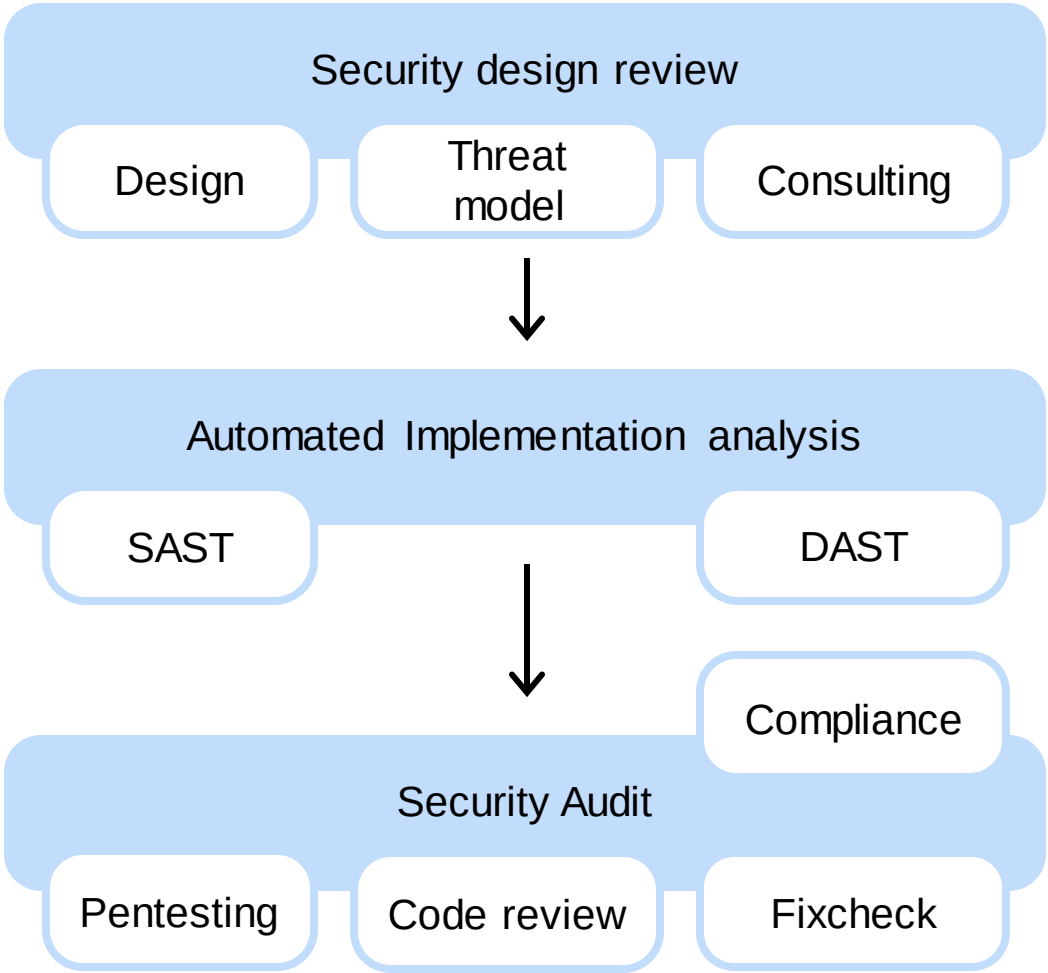
- Примеры:
  - Отладка memory leaks с помощью IDA
  - NetInfra: устройство андерлейной сети, текущее состояние и планы
  - Application Security 101 Part 1

Security Champions

Security Champions — точка входа в команду по вопросам ИБ

- Помогают внедрять процессы и контроли ИБ, работают со стеком технологий ИБ (*сканеры уязвимости*, *статический динамический и анализ кода*)
- Стараются разобраться в сути уязвимостей в сервисе и объяснить всей команде, что происходит и как лучше исправить проблему
- Помогают следить за безопасностью, участвует в разборе инцидентов и алертов
- Консультируют команду по вопросам ИБ, участвуют в ревью кода
- Следят за состоянием безопасности в сервисе, отстаивают безопасность, если планируются какие-то изменения, отрицательно влияющие на защищенность сервиса

Security design review and audit



Vulnerability management

Используем автоматизацию для vulnerability management

- Osquery регулярно отправляет информацию по пакетам в Splunk
- Периодически наша автоматика выкачивает эту информацию
- Раз в сутки автоматика обновляет собственную базу информацией по обновлениям для Ubuntu USN и по уязвимостям CVE
- Раз в день на основании этой информации по каждой группе автоматика формирует (или обновляет существующий) тикет на установку обновлений

/duty security

> **У команды security есть дежурный, который оперативно отвечает на вопросы разработчиков**

- Помощь в проектировании сервисов
- Помощь при работе с криптографией
- Помощь в оценке критичности уязвимостей
- Помощь в правильном размещении секретов
- ...

Культура безопасной разработки. Факторы успеха

- Вовлечение и участие руководства
- Внятные и понятные регламенты
- Опыт Application Security у сотрудников безопасности
- Правильное распределение ответственности
- Умение договариваться

Backend United #6: Табаско

Типовые уязвимости облачных сервисов

Уязвимости

Ошибка конфигурации:

- Опыт атакующего — низкий
- Распространенность — высокая

Атака на цепочку поставки:

- Опыт атакующего — высокий
- Распространенность — низкая

Атаки на механизмы аутентификации:

- Опыт атакующего — средний
- Распространенность — средняя

Нарушение принципов изоляции:

- Опыт атакующего — высокий
- Распространенность — низкая

Пример: MDB

CVE-2018-14669

- ClickHouse MySQL client had “LOAD DATA LOCAL INFILE” functionality enabled that allowed a malicious MySQL database read arbitrary files from the connected ClickHouse server
- Движок MySQL позволяет выполнять запросы SELECT над данными, хранящимися на удалённом MySQL сервере

Уязвимости

Ошибка конфигурации:

- Опыт атакующего — низкий
- Распространенность — высокая

Атака на цепочку поставки:

- Опыт атакующего — высокий
- Распространенность — низкая

Атаки на механизмы аутентификации:

- Опыт атакующего — средний
- Распространенность — средняя

Нарушение принципов изоляции:

- Опыт атакующего — высокий
- Распространенность — низкая

Алертинг нарушения изоляции между VM

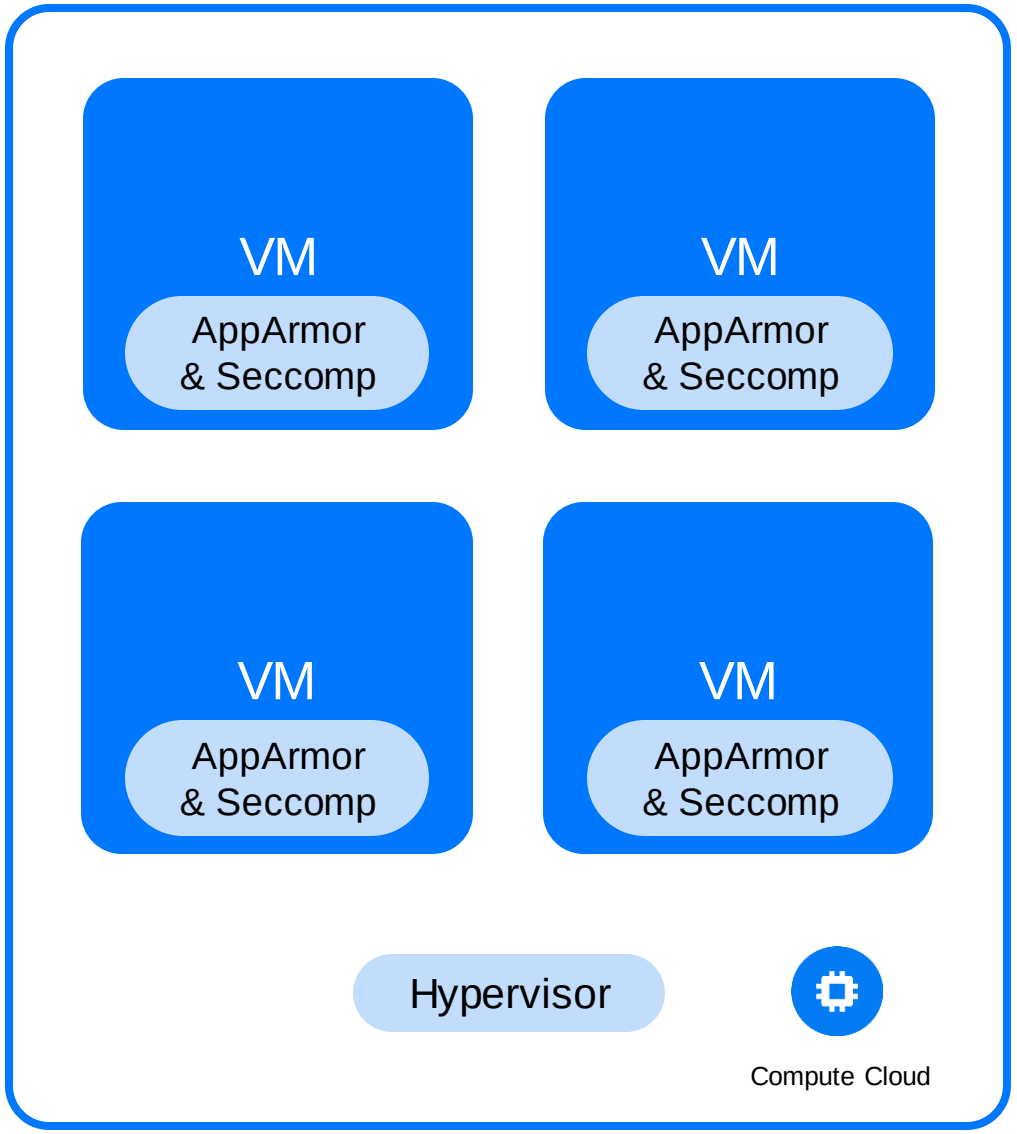
- В Облаке есть специфичные алерты, которые требуют участия команд разработки для их анализа и разбора

Backend United #6: Табаско

Application Sandboxing

Цели

- Быстро получать информацию об атаках на приложение в проде
- Понимать что происходит в процессе эксплуатации и постэксплуатации уязвимости


VM
AppArmor
& Seccomp
VM
AppArmor
& Seccomp
VM
AppArmor
& Seccomp
VM
AppArmor
& Seccomp
Hypervisor
Compute Cloud

AppArmor

AppArmor - система мандатного управления доступом, предназначенная для ограничения доступных приложению ресурсов

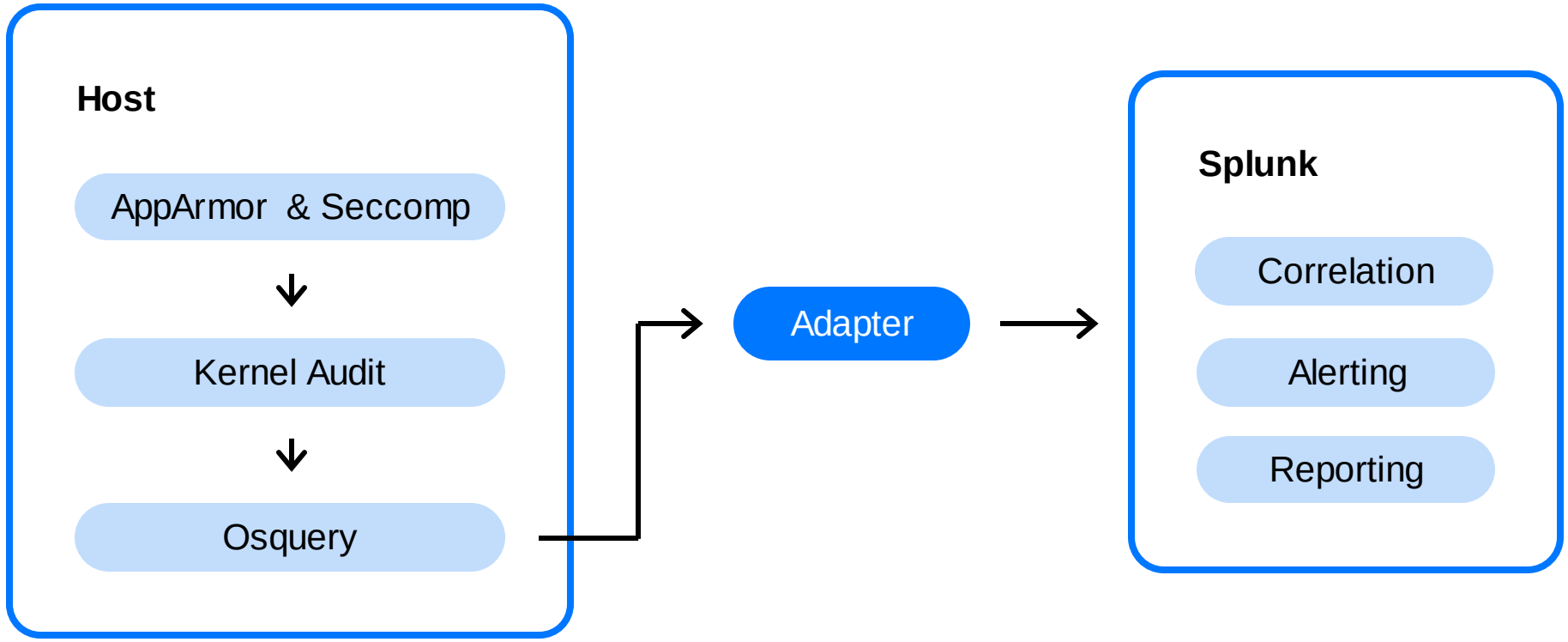
- Позволяет задавать *профили*, которые определяют, к каким системным ресурсам и с какими привилегиями может получить доступ то или иное приложение

Seccomp

> **Seccomp (secure computing) — это механизм безопасности ядра Linux, который позволяет ограничивать набор доступных для приложения системных вызовов**

- Позволяет ограничивать поверхность атаки на ядро, фильтрует разрешенные системные вызовы и их параметры
- Является базовым компонентом любой песочницы

Архитектура



Участие команд разработки в разборах алертов

Заводим алерты на дежурных сервисов в случае нарушения профилей

- Команда, ответственная за сервис, проводит первичный разбор алерта и привлекает специалистов SOC в случае необходимости
- Специалисты SOC проводят ревью вносимых в профиль изменений, если было выяснено, что алерт — это false positive
- Команда SOC заводит инцидент и проводит расследование, если было выяснено, что алерт — это true positive

Backend United #6: Табаско

Compliance

Compliance приносит свои особенности в процесс разработки и деплоймента

- ФЗ-152
- GDPR
- ISO 27001
- ISO 27017 (cloud security — безопасность облачных технологий) and ISO 27018 (Protecting Personal Data in the Cloud — защита персональных данных в облаке)
- PCI DSS (для ЦОД)
- PCI DSS для облачных сервисов — Q3 2020

Compliance и разработка

- Регламенты должы быть внятными и понятными
- Регламенты должны быть "живыми" и отражать действительность
- Регламенты должны однозначно отвечать, как выполнять "опасные действия"

Backend United #6: Табаско

Production access control hardenings

YubiKey

- Приватный ключ генерируется и хранится в токене
- Может хранить несколько пар ключей и сертификатов
- Приватный ключ защищен пин-кодом
- Необходимость касания токена для выполнения криптографических операций
- Строгая аутентификация

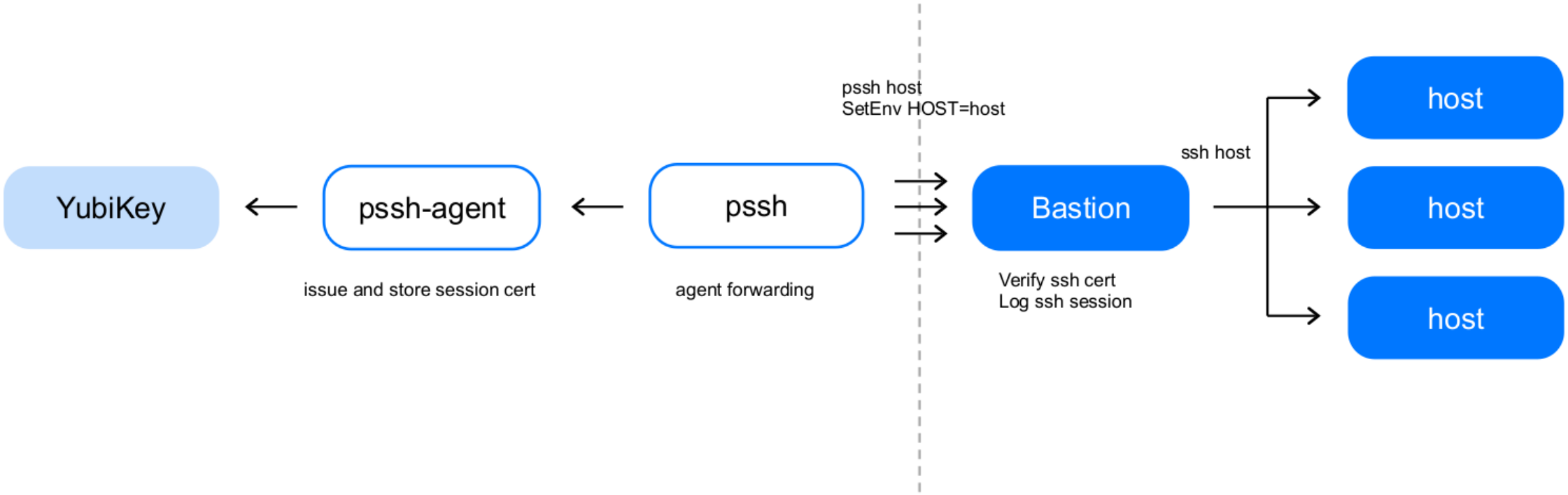
YubiKey self-enroll

- Авторизация по бэйджам
- Не больше одного в руки

Bastion

- Прозрачное проксирование с поддержкой scp
- Отказоустойчивость и балансировка
- Запись сессий в формате sudoreplay (sudo i/o)
- Экспорт зашифрованных сессий в storage
- Экспорт сессий и логов в Splunk
- Гранулярные разрешения на использование сертификатов и ключей
- Централизованный отзыв доступа

YubiKey + CA + pssh + Bastion



Куда мы идём и что хотим улучшить

- Zero Trust Network
- Лучшее от Zero Touch Prod

Вопросы?

Яндекс Облако

Спасибо

Антон Жаболенко

Инженер по информационной безопасности

a-zhabolenko@yandex-team.ru

@ShantonRU