#CODEIB

КАК организовывать защиту современных IT-инфраструктур с использованием концепции Kill chain

Расстрыгина Анастасия,
ITSumma

ITSumma

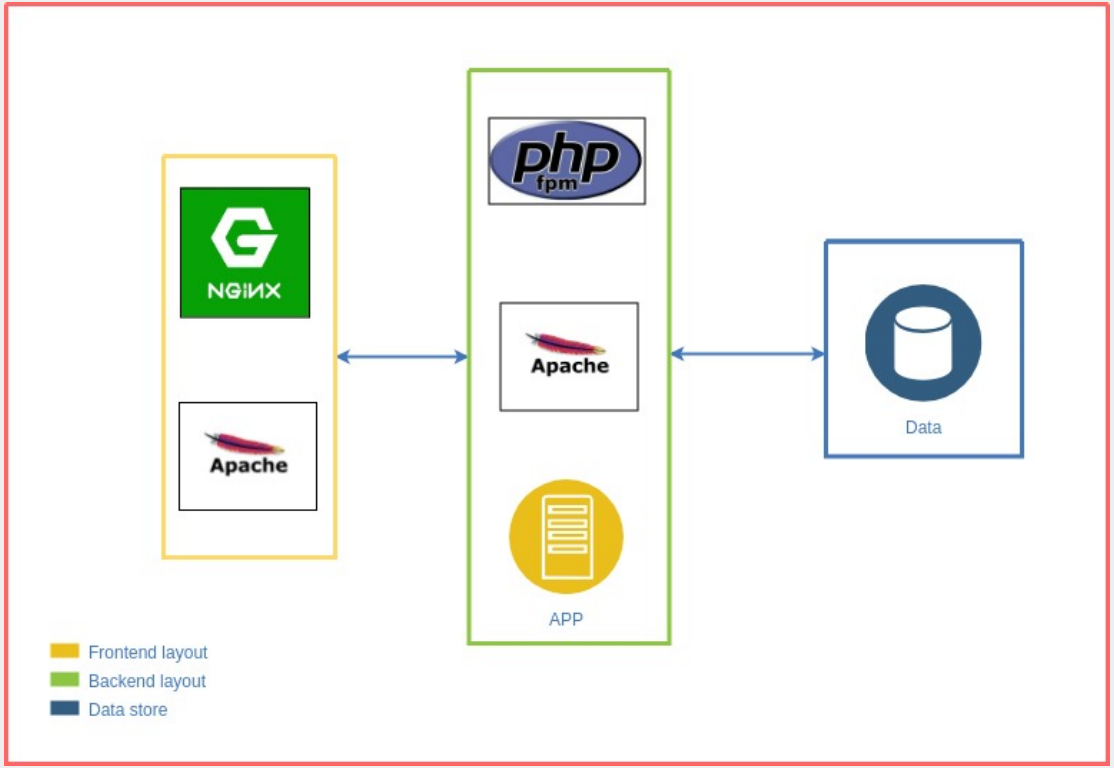
- **Управление инфраструктурой**
- **Создание и поддержка платформ аналитики**
- **Построение частных облаков**
- **Управление инфраструктурой**
- **Индустриальный интернет вещей**
- **Big Data**
- **Круглосуточная техническая поддержка и мониторинг**

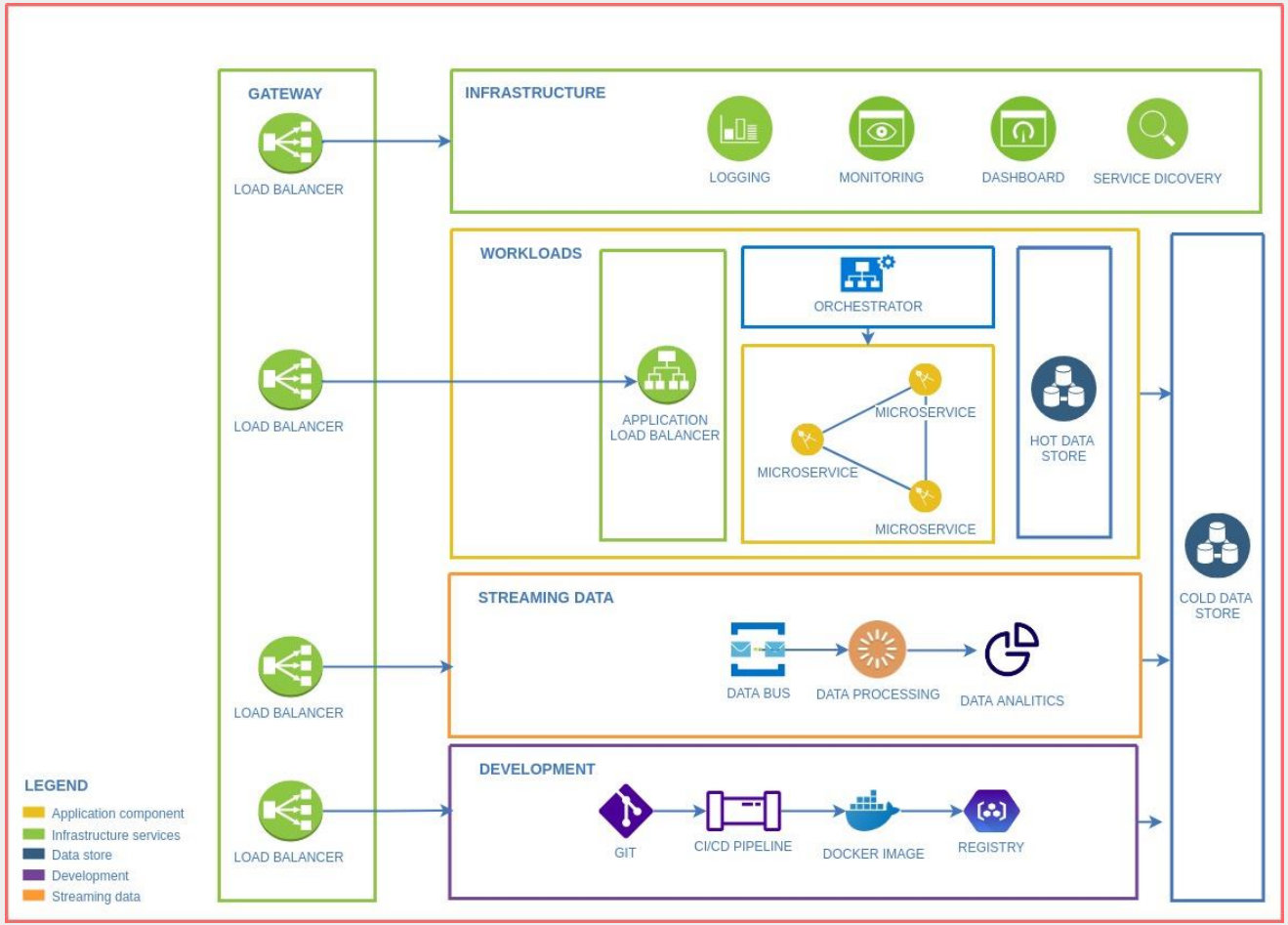
Работаем с **2008** года.

Более **10 000** «серверов» на поддержке.

95 сотрудников, 3 офиса.

- Монолитная архитектура приложений
- Вертикальная масштабируемость
- Единая среда для развертывания приложения
- Простой процесс доставки новой версии
- Отсутствие компонентов для поддержания инфраструктуры
- Отсутствие разнообразия ролей доступа



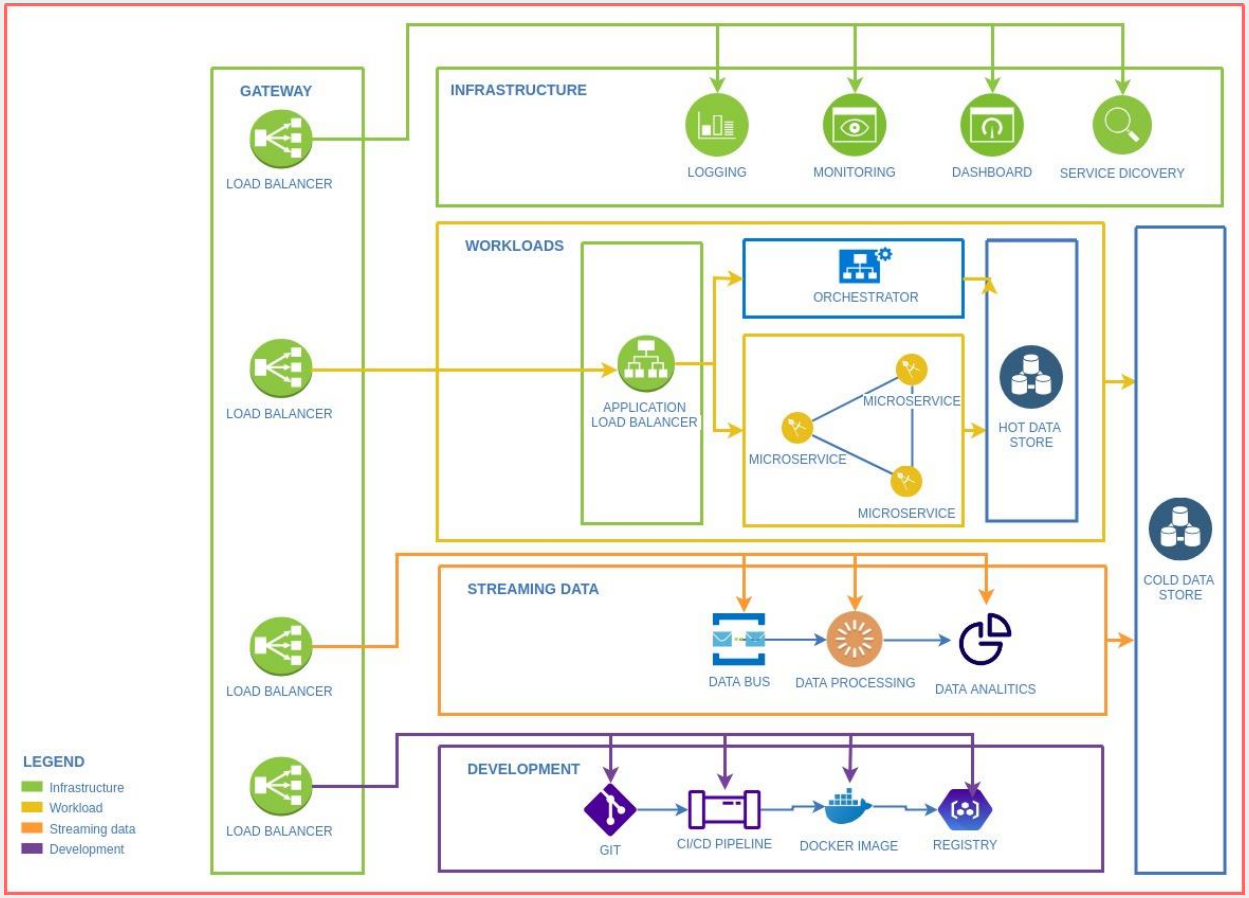


- Микросервисная архитектура
- Системы потоковой обработки данных
- Облачные инфраструктуры
- Горизонтальная масштабируемость
- Оркестрация
- Инфраструктурные процессы

Kill chain

Разведка	Исследование, идентификация и выбор целевой системы для взлома
Вооружение	Оснащение утилитами и системами для совершения нападения
Доставка	Донесение вредоносного контента до целевой системы
Заражение	Запуск вредоносного кода или эксплуатация уязвимости системы
Установка	Открытие удаленного доступа и другие действия с зараженной системой
Получение управления	Управление зараженной системой
Выполнение действий	Сбор, кража, отправка данных, шифрование файлов, подмена и удаление данных

Контуры



- Инфраструктурный контур
- Основной рабочий контур с микросервисами
- Контур сбора, обработки и анализа данных
- Контур разработки и непрерывной доставки

Модель нарушителя

Сторонний пользователь	- веб-интерфейсы системы открытые в internet
Разработчик	- development контур
Аналитик данных	- веб-интерфейс системы аналитики
Администратор процессов непрерывного развертывания	- development контур - workloads контур
Администратор виртуальной инфраструктуры	- workloads контур - infrastructure контур
Администратор системных и прикладных сервисов Администратор безопасности	- полный доступ до всех контуров проекта

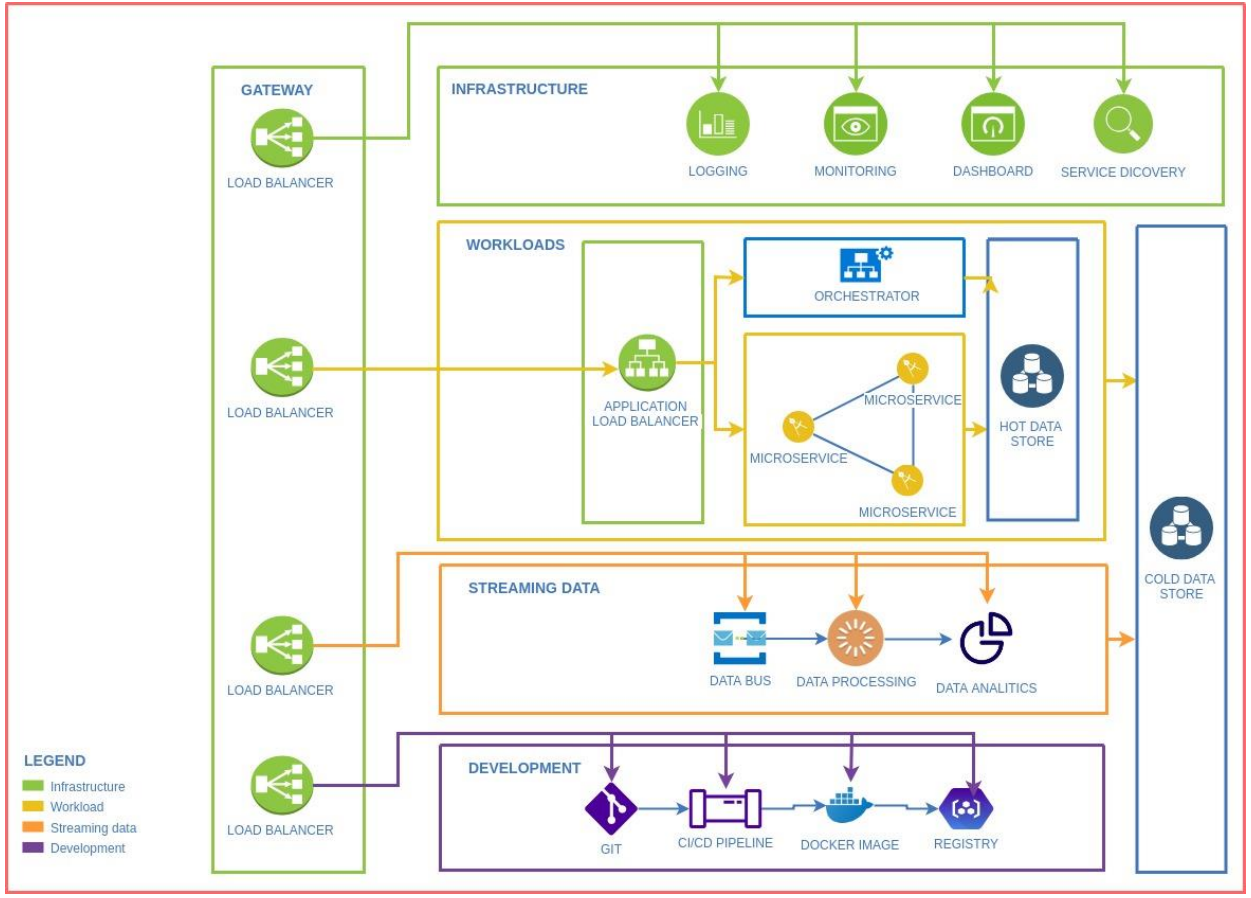
Определяем возможные роли доступа к инфраструктуре. Отталкиваемся от того, что любая роль может быть скомпрометирована

Векторы угроз

- A1:2017-Внедрение: разного рода инъекции
- A2:2017- Недостатки аутентификации
- A3:2017- Разглашение конфиденциальных данных
- A4:2017-Внешние сущности XML (XXE)
- A5:2017- Недостатки контроля доступа
- A6:2017-Некорректная настройка параметров безопасности
- A7:2017- Межсайтовое выполнение сценариев (XSS)
- A8:2017- Небезопасная десериализация
- A9:2017- Использование компонентов с известными уязвимостями
- A10:2017- Недостатки журналирования и мониторинга

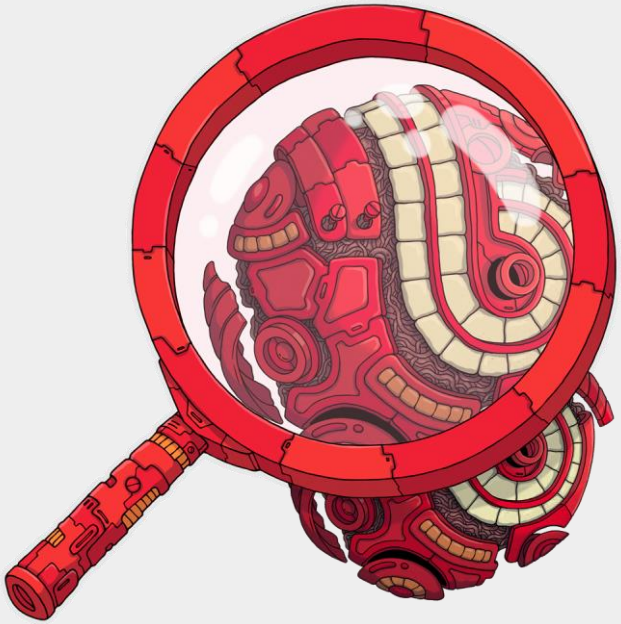
Применение Kill chain (основной рабочий контур)

	A1:2017-Внедрение
Разведка	Веб-аналитика
Вооружение	IDS/IPS
Доставка	WAF, Инструктаж
Заражение	Безопасное конфигурирование сервисов и систем
Установка	HIDS
Получение управления	СРД, RBAC
Выполнение действий	Журналирование



#CODEIB

Спасибо за внимание



Расстрыгина Анастасия,

заместитель руководителя направления информационной безопасности ITSumma,

arasstrygina@itsumma.com