Как ломают контейнеры: Уязвимости микросервисной архитектуры глазами Red Team

Whoami

Вадим Шелест

Руководитель группы анализа защищенности Wildberries & Russ

- Более 15 лет в ИБ, занимаюсь анализом защищенности веб и мобильных приложений, проведением классических инфраструктурных пентестов, а также Red/Purple Teaming проектов
- Спикер на конференциях: Positive Hack Days, KazHackStan, Zero Nights, Standoff Talks, AM Live, AM Talk, Digital Security ON AIR, IT SecurityDay, Wrike TechClub и многих других.
- Преподаю в НИЯУ МИФИ на кафедре «Криптология и кибербезопасность»
- Лауреат премии «Киберпросвет» в номинации «За популяризацию Purple Team»
- Член жюри ежегодной премии «Pentest award»

@purple_medved

Цели Red Team

1

Технологии

2

Процессы

3

Люди

Задачи Red Team

1

Тестирование на проникновение

Анализ защищенности веб и мобильных приложений, проведение классических инфраструктурных пентестов, аудитов беспроводных сетей, и социо-технических этапов тестирований на проникновение

2

Purple Teaming

Эмуляция действий атакующих. Реализация атомарных тест-кейсов, а также полноценных сценариев по всей модели cyber kill chain (Adversary Emulation) в рамках проведения киберучений в формате активного взаимодействия с подразделением SOC

3

Red Teaming

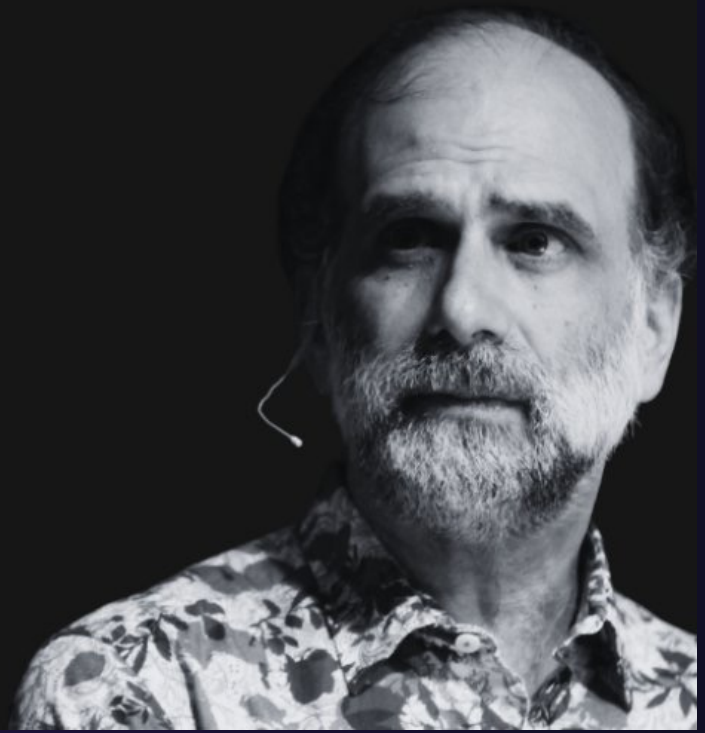
Симуляция действий атакующих в формате активного противодействия с подразделением SOC в условиях максимально приближенных к боевым

“

Complexity is the worst enemy of security, and our systems are getting more complex all the time

”

— Bruce Schneier




Red team —
команда катализатор

«Карта» взаимодействий

AppSec

SOC

K8s Security

Endpoint Sec

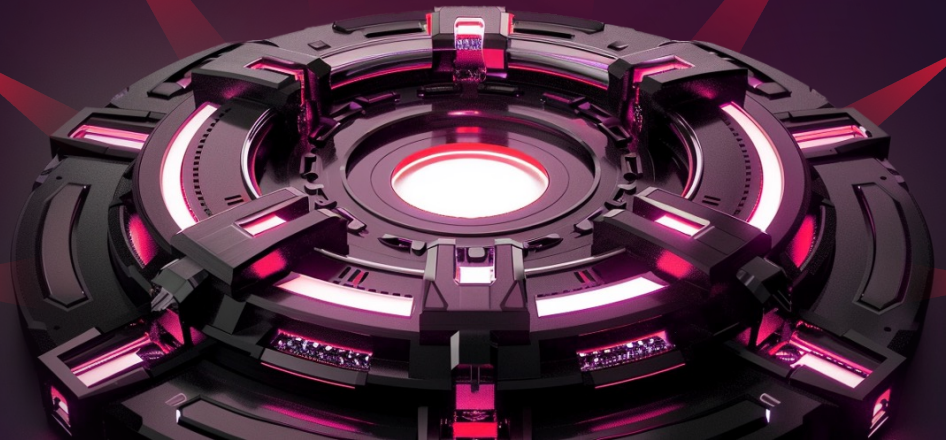
Red team

DevSecOps

DataSec

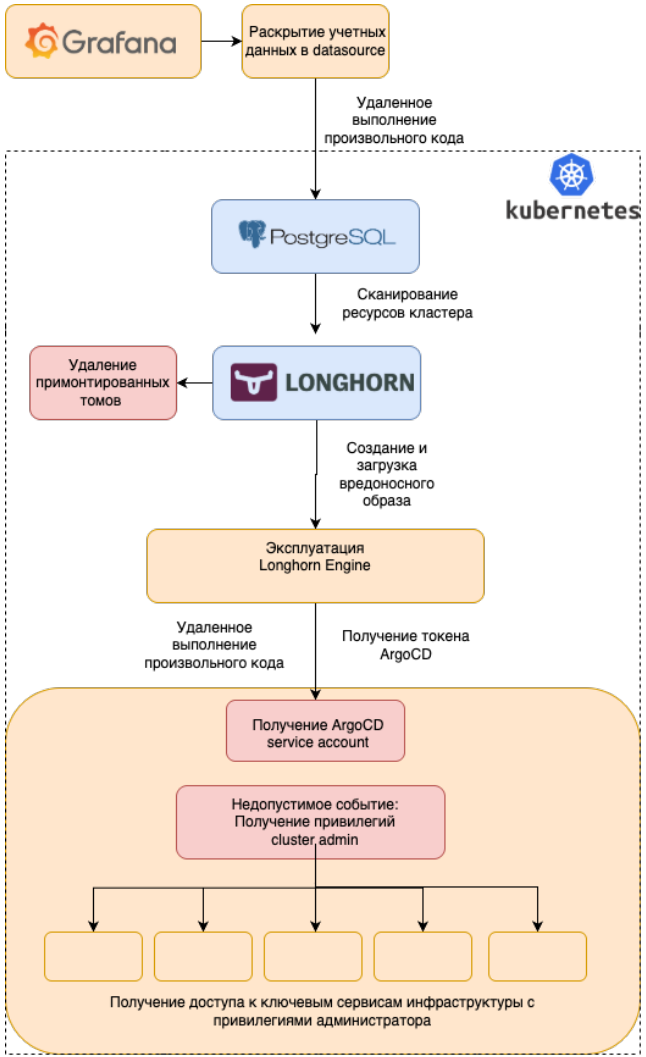
CloudSec

VM



Кейс из практики

- Слабый пароль учетной записи для веб-интерфейса Grafana
- Раскрытие учетных данных для источника PostgreSQL
- RCE на хосте PostgreSQL в кластере по причине небезопасной конфигурации
- Сканирование ресурсов кластера k8s
- Обнаружение веб-интерфейса Longhorn Dashboard ,без аутентификации
- Возможность удаления примонтированных томов
- Создание и загрузка вредоносного образа контейнера Longhorn Engine
- Извлечение токена Service account пода Longhorn
- Получение доступа к ArgoCD
- Получение прав администратора кластера
- Получение доступа к ключевым сервисам и компонентам инфраструктуры с привилегиями администратора



Рекомендации по кейсу

Основные рекомендации:	CorpSec	SOC	K8s Sec	DBA	AppSec
Использовать SSO для доступа к сервисам	☺				☺
Привести конфигурацию кластера Kubernetes в соответствие со стандартом безопасности	☺		☺		
Установить и сконфигурировать Kyverno Admission Controller с набором политик в блокирующем режиме			☺		
Настроить доставку логов Kube API Server в SIEM для возможности расследования инцидентов при обнаружении подозрительных действий		☺			
Не использовать привилегированные учетные записи баз данных PostgreSQL				☺	

Выводы

1

Глубокая интеграция

Понимание бизнеса позволяет очень эффективно искать сценарии компрометации.

Интеграция позволяет быстро реагировать на любые изменения бизнеса.

Выводы

1 Глубокая интеграция

Понимание бизнеса позволяет очень эффективно искать сценарии компрометации.

Интеграция позволяет быстро реагировать на любые изменения бизнеса.

2 Обеспечение взаимодействия

Red Team, как команда-катализатор позволяет объективно оценить и оптимизировать процессы

Выводы

1 Глубокая интеграция

Понимание бизнеса позволяет очень эффективно искать сценарии компрометации.

Интеграция позволяет быстро реагировать на любые изменения бизнеса.

2 Обеспечение взаимодействия

Red Team, как команда-катализатор позволяет объективно оценить процессы, используя комплексный подход

3 Инсайты и самоконтроль

Команды ИБ получают системную обратную связь о здоровье своих процессов и понимают точки роста

А теперь ваши вопросы

Вадим Шелест
Head of Red Team
Wildberries & Russ