ГИБКАЯ КИБЕРБЕЗОПАСНОСТЬ НА ОТКРЫТОЙ ПЛАТФОРМЕ

Александр Бодрик, CISA, CCSK, ITIL Expert
Аналитик по кибербезопасности, Wikistrat

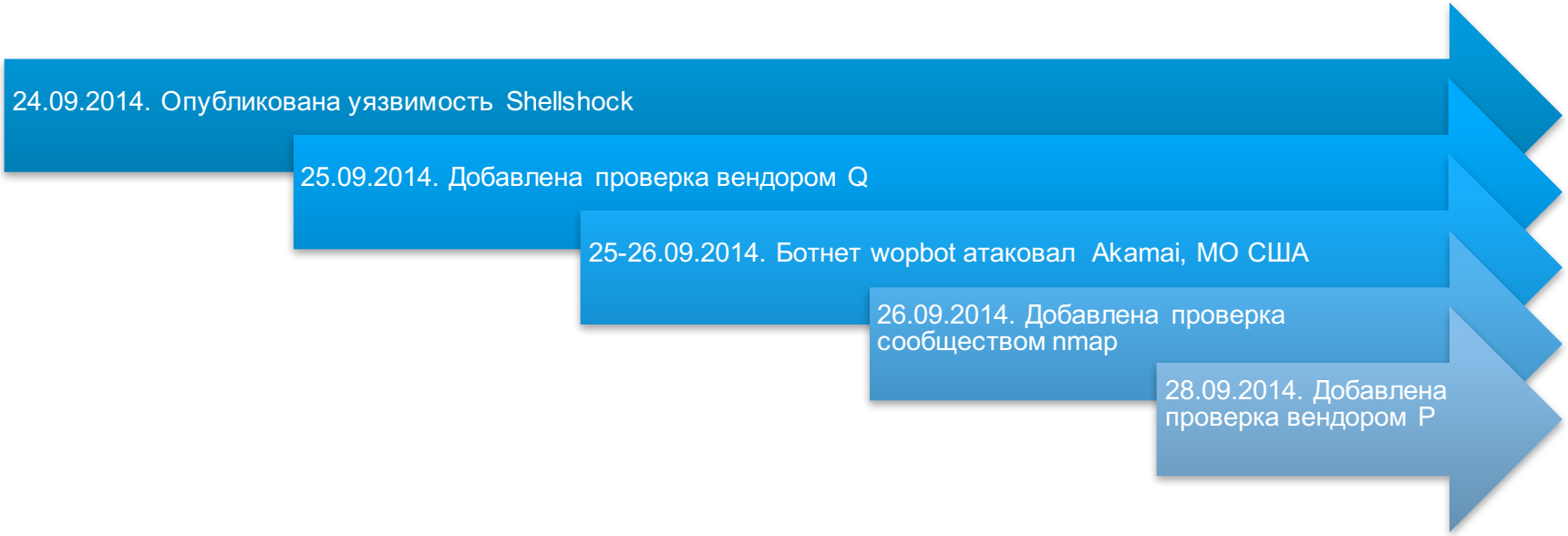
ЦЕЛИ ПРЕЗЕНТАЦИИ

1. Показать как Open Source помогает обеспечению гибкой кибербезопасности
2. Обрисовать контуры эффективной модели кибербезопасности на Open Source
3. Разбудить интерес к дальнейшему изучению и тестированию подхода

О ЧЕМ НЕ БУДЕМ ГОВОРИТЬ

- Нужна ли безопасность
- Безопасность гостайны, АСУ ТП\IoT, безопасность облаков, BYOD и third party risk
- Детальная экономика использования Open Source

ОДНА НЕДЕЛЯ В БЕЗОПАСНОСТИ



14.04.2015. Лютиков Виталий (ФСТЭК): Из 10 отечественных сертифицированных разработок на базе ОС Linux уязвимость Shellshock устранили 4.

ОДИН ГОД В БЕЗОПАСНОСТИ – ЦЕНА И ВОЛАТИЛЬНОСТЬ КУРСА ПОДДЕРЖКИ

	Цена	Волатильность
2014	↑ + 20%	32,66 – 72,27 (121%)
2015	↑ + 57%	49,18 – 81 (65%)
2016	↑ + XX ? %	?
2017	↑ + XX ? %	?

- Сокращение бюджетов?
- Инфляция?

БИЗНЕС-КЕЙСЫ OPEN SOURCE

Когда рационально использовать Open Source при обеспечении кибербезопасности?

- Проблема бизнеса переходного класса (SMB > Corporate)
- Непредсказуемый бурный рост бизнеса (Business Capacity Management)
- Импортозамещение и валютные риски
- ИТ - Commodity
- Тестирование идей по развитию бизнеса

КОНКУРЕНТЫ OPEN SOURCE

А если не Open Source?

- Freeware
- Cloud
- Подписки
- Лизинг
- Страхование

С финансовой точки зрения
ДА

С точки зрения возможности тестирования agile-like процессов
НЕТ

РИСКИ OPEN SOURCE

Все слишком хорошо что бы быть правдой..

1. Производительность
2. Отказоустойчивость
3. Масштабирование
4. Централизованное управление
5. Финансовая устойчивость
6. Наличие поддержки
7. Обновления

Обратная сторона преимуществ идеологии

Разнятся от продукта к продукту

В силу разнообразия выбора и гибкости идеологии - управляемы

ПРОФЕССИОНАЛЬНОЕ УПРАВЛЕНИЕ РИСКАМИ НА ТРАССЕ

1. Планируем какой болид нам нужен и какой можем себе позволить (Управление архитектурой)
2. Создаем и тестируем болид
3. Используем и модернизируем
4. Учимся у конкурентов, повышаем наше умение использовать особенности болида и трассы
5. Возвращаемся на уровень выше если на этом проблему не решим

УПРАВЛЕНИЕ РИСКАМИ В ГИБКОЙ КИБЕРБЕЗОПАСНОСТИ НА OPEN SOURCE

4 КОМПОНЕНТА УПРАВЛЕНИЯ АРХИТЕКТУРОЙ КИБЕРБЕЗОПАСНОСТИ

- Учет внешних и внутренних контекстов
  - Социальный, Политический, Валютный, Юридический
  - Технологический, Культурный и Организационный
- Баланс между гибкостью и проверенными решениями
- Нефункциональные возможности
  - Производительность и отказоустойчивость
  - Горизонтальное и вертикальное масштабирование
- Риски использования Open Source
  - Обновления и коммерческая поддержка
  - Финансовая устойчивость

ЗРЕЛОСТЬ OPEN SOURCE В СЕГМЕНТАХ КИБЕРБЕЗОПАСНОСТИ

Заслуживают внимания

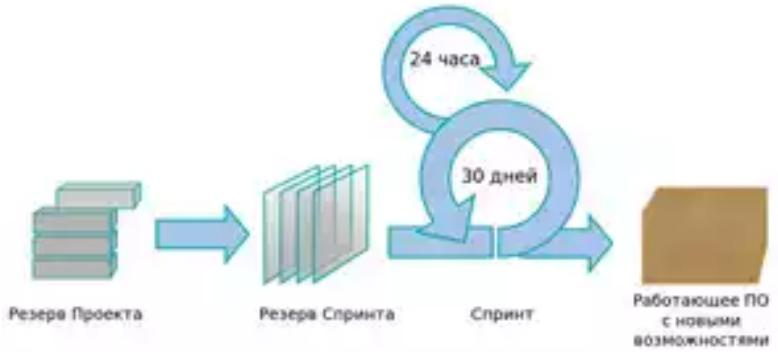
- Управление уязвимостями
- SIEM, NSM
- WAF, Anti-DDoS
- NAC, Endpoint Security
- Strong authentication, SSO
- GRC, Operations Management
- Secure sharing (Dropbox-like)

«Трудные дети»

- DLP
- IDM
- Endpoint AV
- DAM
- IRM
- Forensic
- Cloud security

ГИБКОЕ УПРАВЛЕНИЕ СРЕДСТВАМИ ИБ НА ОСНОВЕ ЗНАНИЙ

Множество требований к настройке технологий защиты (Project Pipeline)



ЧТО БУДЕТ ЕСЛИ НЕ УПРАВЛЯТЬ ЗНАНИЯМИ?

Раскрытие тактики скрытия хищения данных в DNS запросах

- 1998 – Neohapsis (Cisco)
- 2001, 2007, 2009, 2010 – SANS
- 2009 – конференция Shakacon – 6 инструментов!
- …. 2016 – ИБ Банк 2016

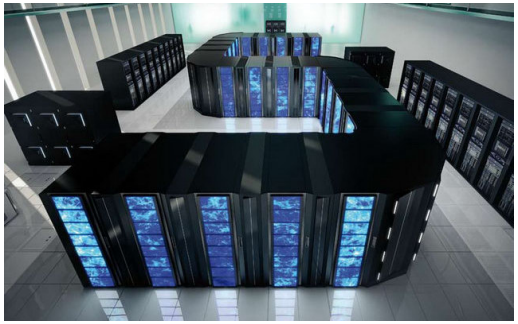
ЛЮДИ, ИХ ВОСПРИЯТИЕ И КОМПЕТЕНЦИИ – ПРЕДПОСЫЛКИ

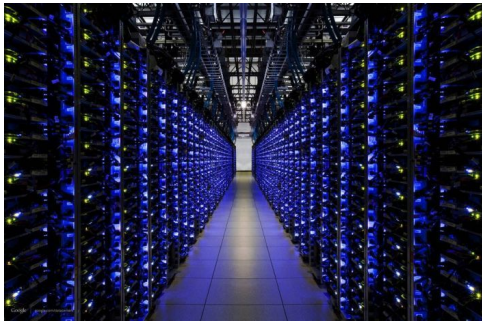
- ФОТ 
- Существующих компетенций не достаточно

- Логичные варианты:
  - Регионы
  - Молодые специалисты

ЛЮДИ, ИХ ВОСПРИЯТИЕ И КОМПЕТЕНЦИИ – ВОЗМОЖНЫЙ ВАРИАНТ

Характеристики	COTS	Открытая платформа
Размер команды	X	X<
Ключевые компетенции	Профессиональные	Личные
Средний размер оклада	XXX XXX	< XXX XXX
Bus-фактор	X	Существенно меньше
Месторасположение	Вместе с пользователями	Центры оказания услуг





ИТОГО

- Open Source – не просто бесплатный софт, а значимый элемент (enabler) гибкой кибербезопасности
- Использование Open Source прямо показано в ряде случаев
- Без изменения мировоззрения и переподготовки кадров не обойтись

ПОТРЕБИТЕЛИ OPEN SOURCE SECURITY

- ТОП-10 нефтяная компания мира (A) – ELK, OTRS, Cuckoo
- ТОП-10 нефтяная компания мира (B) – OTRS, Cuckoo
- ТОП-5 финансовая группа России - OTRS
- ТОП-10 вендор России (A) – ELK
- ТОП-10 вендор России(B) – ELK
- ТОП-10 вендор России (C) - seccubus
- ТОП-5 картографический сервис мира – modsecurity
- ТОП-5 цифровой банк России - OpenAM

ЧТО ДАЛЬШЕ

Что почитать

Детальнее о подходе

- PC Week/RE «Обеспечение кибербезопасности на открытой платформе»
- Agile manifesto
- Scrum guide

Об управлении архитектурой кибербезопасности

- TOGAF\SABSA
- Cobit 5 for Information Security\стандарты C2M2 Минэнерго США

Хочу сразу делать!

- Почитать сколько возможно
- Начать с малого

Вопросы и продолжение обсуждения:

- Кулуары
- E-mail - alex.bodryk@gmail.com