SECURITY OPERATIONS В УСЛОВИЯХ ЦИФРОВОГО ХАОСА

Сергей Лебедь

Вице-президент, директор
Департамента кибербезопасности
ПАО Сбербанк

Тренды хаоса цифровизации

SCS SBERBANK CYBER SECURITY

Отсутствие стандартов и регулирования

Поколения Y и Z выбирают свободу, а не регулирование. Agile Манифест

Культура и скорость изменений

10,000+ Изменений в день в Google!

Готовность инфраструктуры

>25% Более 20% CIO говорят, что устаревшие технологии являются ключевым барьером для перехода к цифровому миру 2018 году, Accenture

Конкурентное давление и отраслевые тенденции

16,000+

Значительный рост количества уязвимостей по годам

Более 16 000 в 2018 году, согласно исследованию Skybox Security

> $4 трлн

Значительно более тяжелые потери

2018, IFs 7.15

> 2 млн

Сильный кризис талантов

Более 2 млн вакансий по всему миру в 2019 году, источник: ISACA

> 3 млрд

Количество инцидентов взлетело до небес

Более 3 млрд счетов взломано к 2018 году

191 дней

Слабые технологии

191 день - это среднее время для обнаружения атаки / утечки в компаниях Источник: techbeacon.com

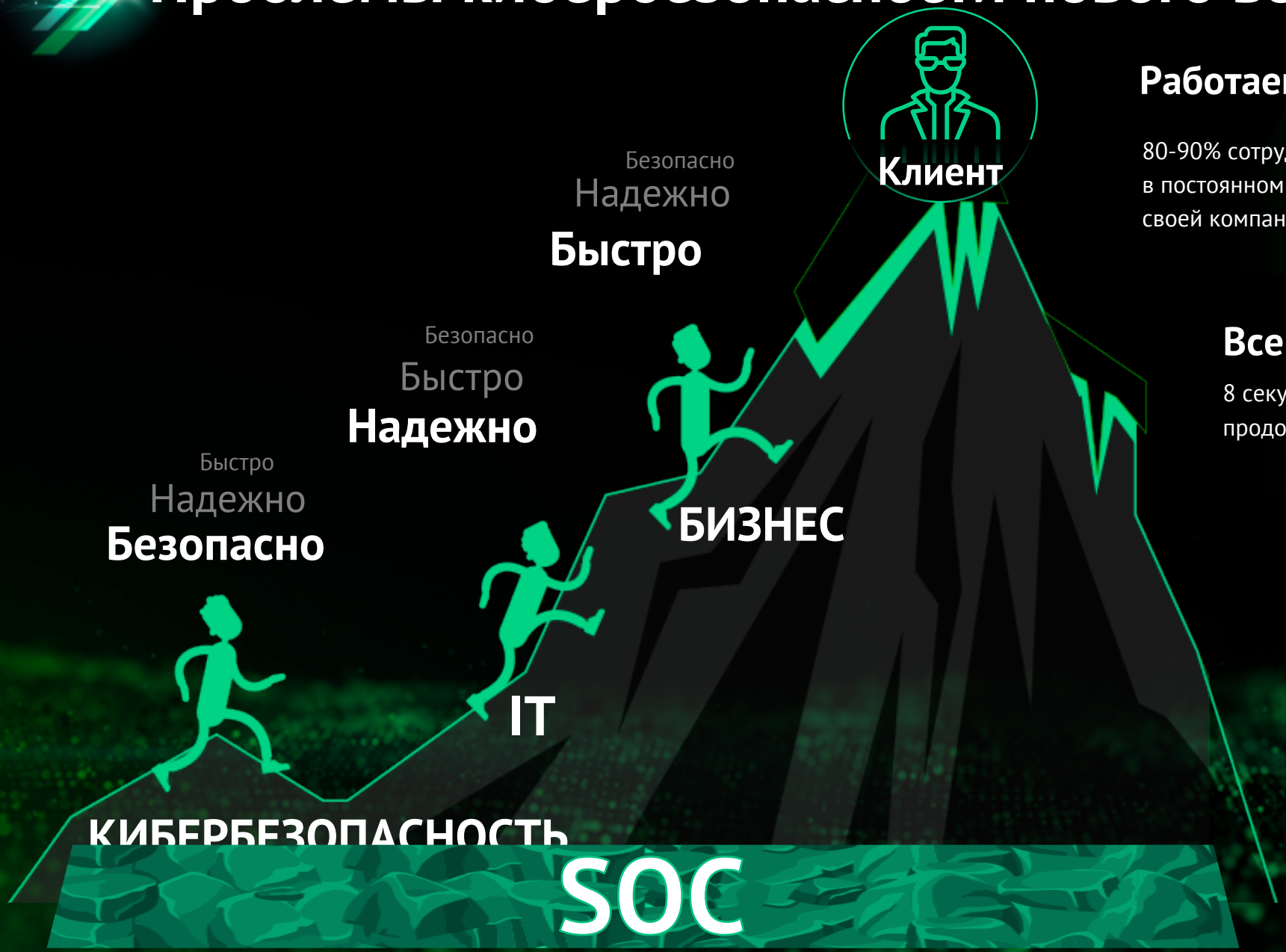
66 дней

Нехватка навыков

66 дней - это среднее время, необходимое для восстановления после кибератаки. Источник: techbeacon.com

Проблемы кибербезопасности нового века

SCS SBERBANK CYBER SECURITY



Работаем: всегда и везде

80-90% сотрудников нуждаются в постоянном доступе к ресурсам своей компании

Все вместе!

8 секунд - это средняя продолжительность внимания

Больше данных!

90% данных были получены за последние 2 года

...и киберриски

> 1 млн атак регистрируется каждый день

Уровень зрелости КБ ≤ Уровень зрелости IT

SCS SBERBANK CYBER SECURITY

Кибербезопасность

Коммуникации | Видимость | Интеллект | Реагирование

Возможности SOC

Идентификация | защита | выявление | Реагирование | восстановление

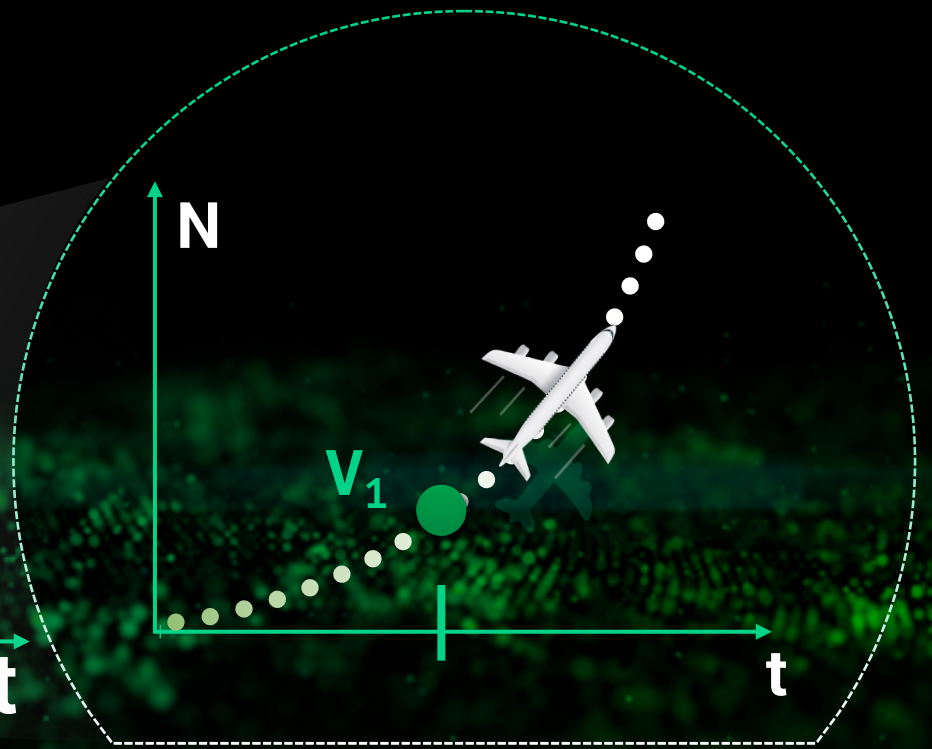
Ключевые функции

IT

Киберустойчивость

КИБЕРУСТОЙЧИВОСТЬ

- План восстановления
- Бэкапы
- Кризисная команда
- Навыки и тренировки



Что нужно сделать?

Управление знаниями

Управление знаниями

об инфраструктуре и бизнес-процессах

Управление рисками

Управление рисками

Угрозы – Уязвимости – Возможности – Компромисс

Операционные практики

Операционная практика радикально изменилась

Threat Intelligence – SecDevOps – Управление уязвимостями

Управление данными

Изменение подхода к обработке данных

Машинное обучение– Ситуационная осведомленность – Искусственный интеллект

Роботизация и интеграция

Активное использование средств автоматизации

Роботизация – Управление уязвимостями– Ситуационная осведомленность

Переосмысление технологий

Использование скрытых возможностей и новых технологий

Поведенческая аналитика – Корреляция данных

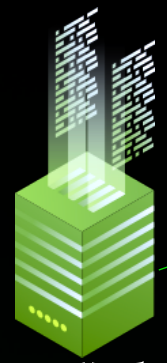
БЕЗОПАСНОСТЬ = ДОВЕРИЕ + КОЛЛАБОРАЦИЯ

SBERBANK CYBER SECURITY

Ассоциации

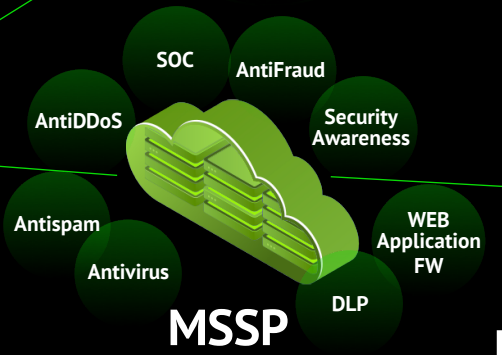
Гос. органы

Обмен информацией о киберугрозах



CERT

Крупный бизнес



MSSP

Малый и средний бизнес

Проф. сообщества

CERT

Источник: аналитика Сбербанка


SCS
SBERBANK
CYBER
SECURITY
СПАСИБО!