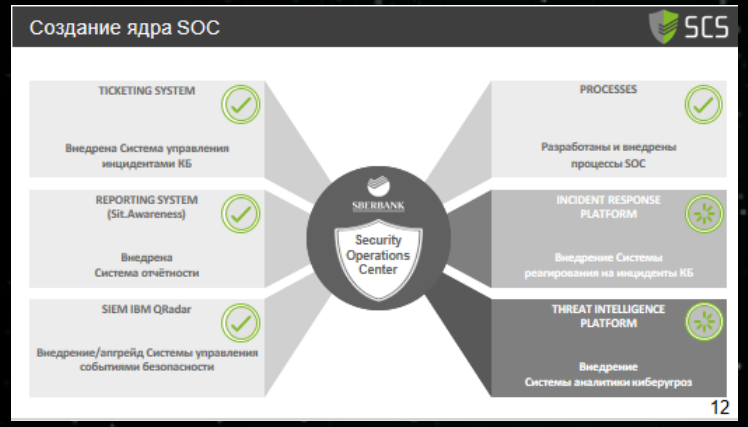
SCS SBERBANK CYBER SECURITY

РАЗВИТИЕ ТЕХНОЛОГИЙ И ПРОЦЕССОВ SOC 2019

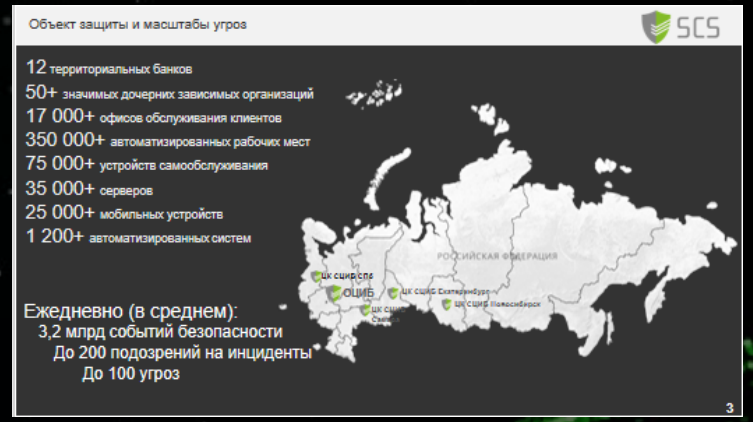
Алексей Качалин
Управляющий директор
Центр Киберзащиты
ПАО Сбербанк

SCS SOC: 2018→2019

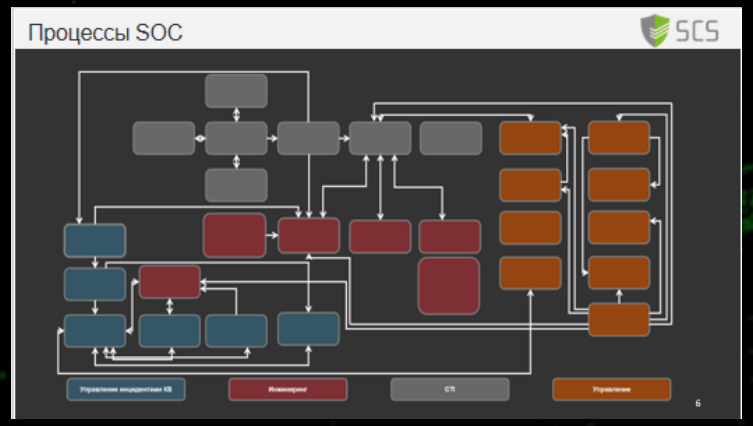
https://www.youtube.com/watch?v=yh1YYFgIWt4



Разработана и внедрена TIP
Внедрена IRP



Событий безопасности –
до 7 млрд ежедневно



«Отладка» процессов
метрики и ценность для бизнеса

Повышения уровня автоматизации

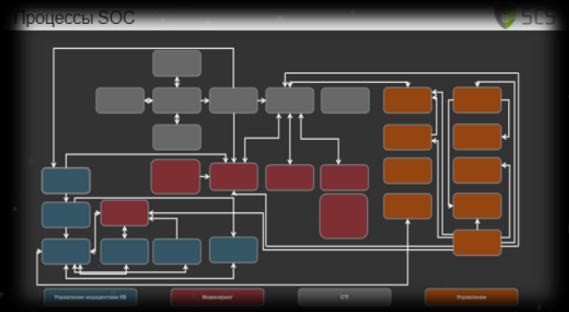
Развитие команды: обучение,
в том числе
Академия кибербезопасности

Основной вызов: долгосрочные цели развития

SCS SBERBANK CYBER SECURITY

2025

SOC
2019



SOC
2018

Служба ИБ
2015

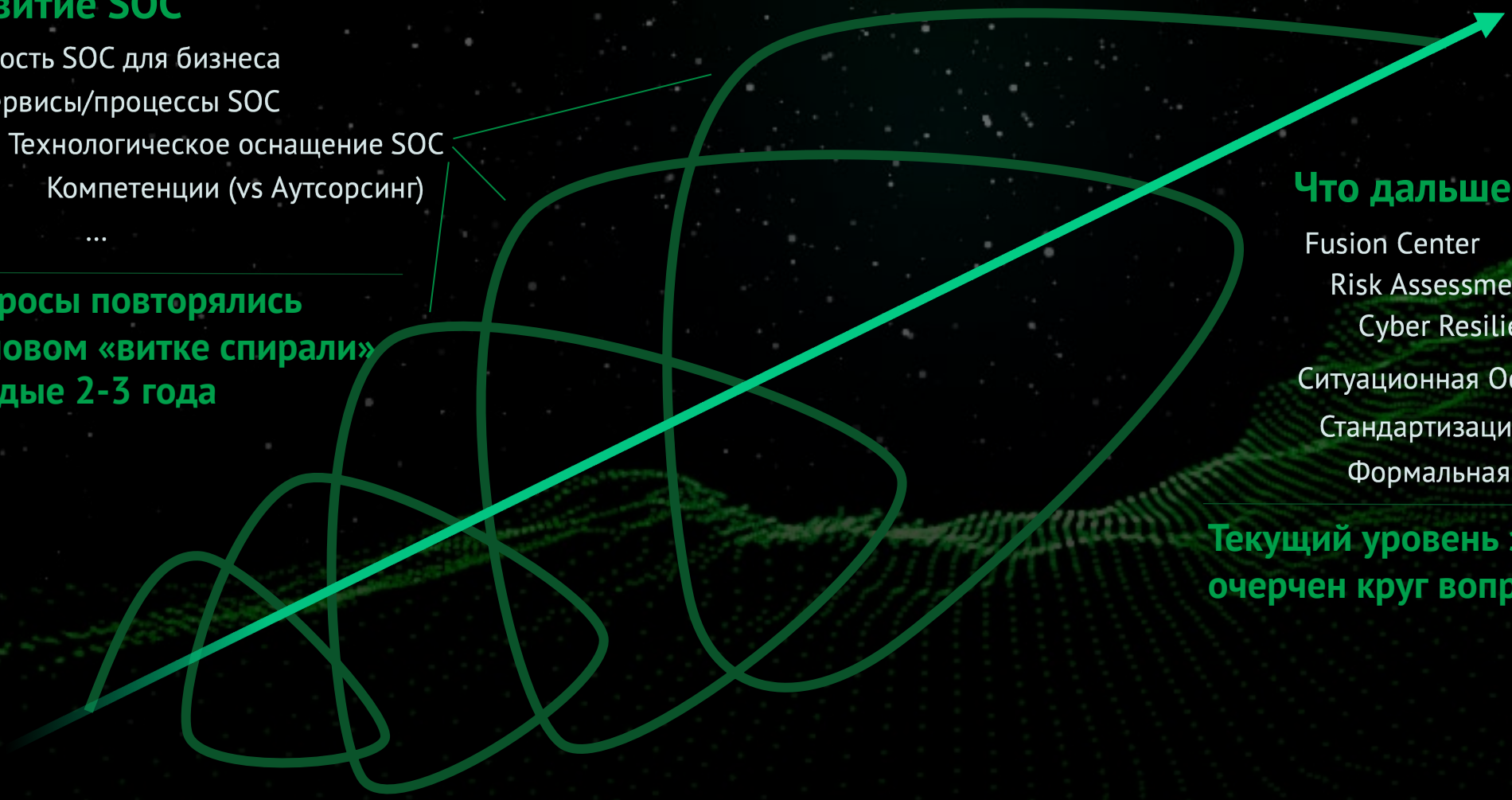
Становление Security Operations и SOC

2010-2020

Развитие SOC

Ценность SOC для бизнеса
Сервисы/процессы SOC
Технологическое оснащение SOC
Компетенции (vs Аутсорсинг)
…

Вопросы повторялись на новом «витке спирали» каждые 2-3 года



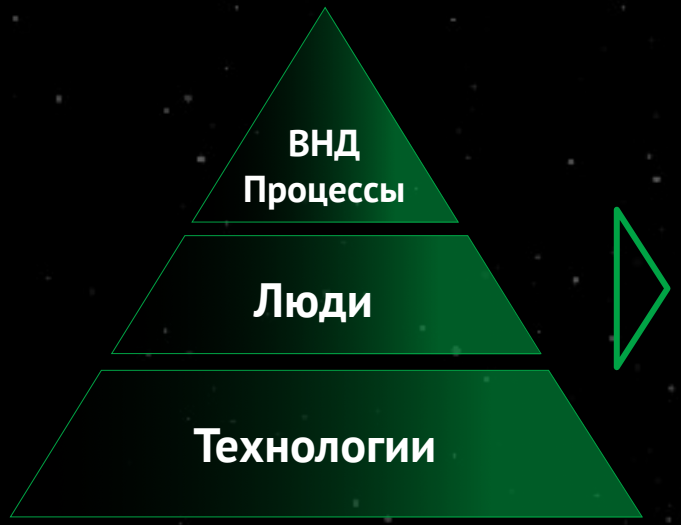
2020+

Что дальше? SOC

Fusion Center
Risk Assessment Center
Cyber Resilience Center
Ситуационная Осведомленность
Стандартизация сервисов SOC
Формальная модель зрелости SOC

Текущий уровень зрелости: очерчен круг вопросов SOC

Базовые практики и процессы SecOps/SOC



Справочники ИТ
Справочники ИБ

Активы
Конфигурации
Изменения
Проблемы
Релизы
Инциденты

Логи инфраструктуры
Логи бизнес-систем

Данные о злоумышленниках/TTP
Данные об угрозах
Данные об уязвимостях

Сырые данные инф.обмена

Описания нормального поведения

Базовые практики и процессы SecOps/SOC

ИДЕНТИФИКАЦИЯ

ПРЕДОТВРАЩЕНИЕ

МОНИТОРИНГ

РЕАГИРОВАНИЕ

ВОССТАНОВЛЕНИЕ

	ИДЕНТИФИКАЦИЯ	ПРЕДОТВРАЩЕНИЕ	МОНИТОРИНГ	РЕАГИРОВАНИЕ	ВОССТАНОВЛЕНИЕ
Базовые SOC – 2015+		○	●	○	
SOC – 2018+	○	○	●	●	○
SOC – 2020+	●	●	●	●	●

Расширение практик SOC:

- Внутренние + внешние (Threat Intel)
- Реактивные + проактивные (Threat Hunting)
- Входящие + исходящие (Коммуникации)

… сочетания

Развитие технологий SOC: потребности 2020+

SCS SBERBANK CYBER SECURITY

Скорость работы SOC, директивное время

- Автоматизация и роботизация вспомогательных процессов
- Автоматизация и роботизация

Интеграция SecOps с прочими доменами КБ

- Получение параметров/отчетность governance и оценки риска
- Интеграция с разработкой/DevSecOps

Повышение эффективности аналитики

- Дефрагментация процессов SOC
- Автоматизация и роботизация аналитики
- Интегрированные инструменты визуализации
- Возможности AdHoc настройки/разработки

Новый уровень ситуационной осведомленности

- Динамические дэшборды и библиотеки
- Системы совместной работы на всех этапах SecOps
- Возможность интеграции с любыми системами

Новые практики SecOps: качества, полнота, глубина данных

- Решение вопроса долгосрочного хранения/анализа
- Обработка холодных/теплых/горячих данных

Непрерывный тренинг и обучение

- Платформа обучения и отслеживания компетенций
- Тренажеры для отработки практик SecOps
- Автоматизация Awareness-программ

Самые сложные вопросы: поддержка новых решений в существующих ИБ- и ИТ-системах

АКАДЕМИЯ КИБЕРБЕЗОПАСНОСТИ СБЕРБАНКА

SCS SBERBANK CYBER SECURITY

Security Engineering

Risk Assessment

Secure Software Development

Threat Intelligence

Security Operations

Physical and Environmental Security

Governance

Human Resources Awareness & Security


SCS
SBERBANK
CYBER
SECURITY
СПАСИБО!