Kaspersky
Security Day
2021

Консалтинг по построению SOC

Павел Таратынов,
архитектор центров
информационной безопасности

kaspersky

Легитимная активность

Легитимное ПО
Легитимные сайты
Разрешенное сетевое взаимодействие

.....

Вредоносная активность

Вирусы
Шифровальщики
Эксплойты
Трояны

....

Ландшафт угроз

Атаки на цепочку поставок

Новые цели
IoT, индустриальные объекты, «Умные города», автомобили

Кибервойны
Промышленный шпионаж, диверсии, терроризм… и рынок кибероружия

Атаки без использования ВПО
Использование инструментов администратора для проведения атак

Легитимная активность

Легитимное ПО
Легитимные сайты
Разрешенное сетевое взаимодействие

.....

???

- Средства администрирования
- Офисные документы с макросами
- Зараженные обновления ПО
- Взломанный легитимный сайт
- Целевое ВПО
- «Бестелесное» ВПО

Вредоносная активность

Вирусы
Шифровальщики
Эксплойты
Трояны
....

Security Operation Center (SOC)

Персонал

Процессы

Технологии

Сложности создания SOC

Интернет вещей

Взаимодействие со смежными департаментами

Специфика АСУ ТП

Не существует типового SOC

Умные автомобили

Разработка актуальных Use-cases и плейбуков

Облачные инфраструктуры

Регуляторные ограничения

Надежные источники TI

Недостаток интеграции технических средств

Аутсорсинг или in-house?

Недостаток финансирования

Недостаток знаний об инфраструктуре

Ценность SOC не ясна бизнесу

APT

Недостаток экспертов

Консалтинговые сервисы SOC от «Лаборатории Касперского»

Анализ зрелости SOC

Проектирование SOC

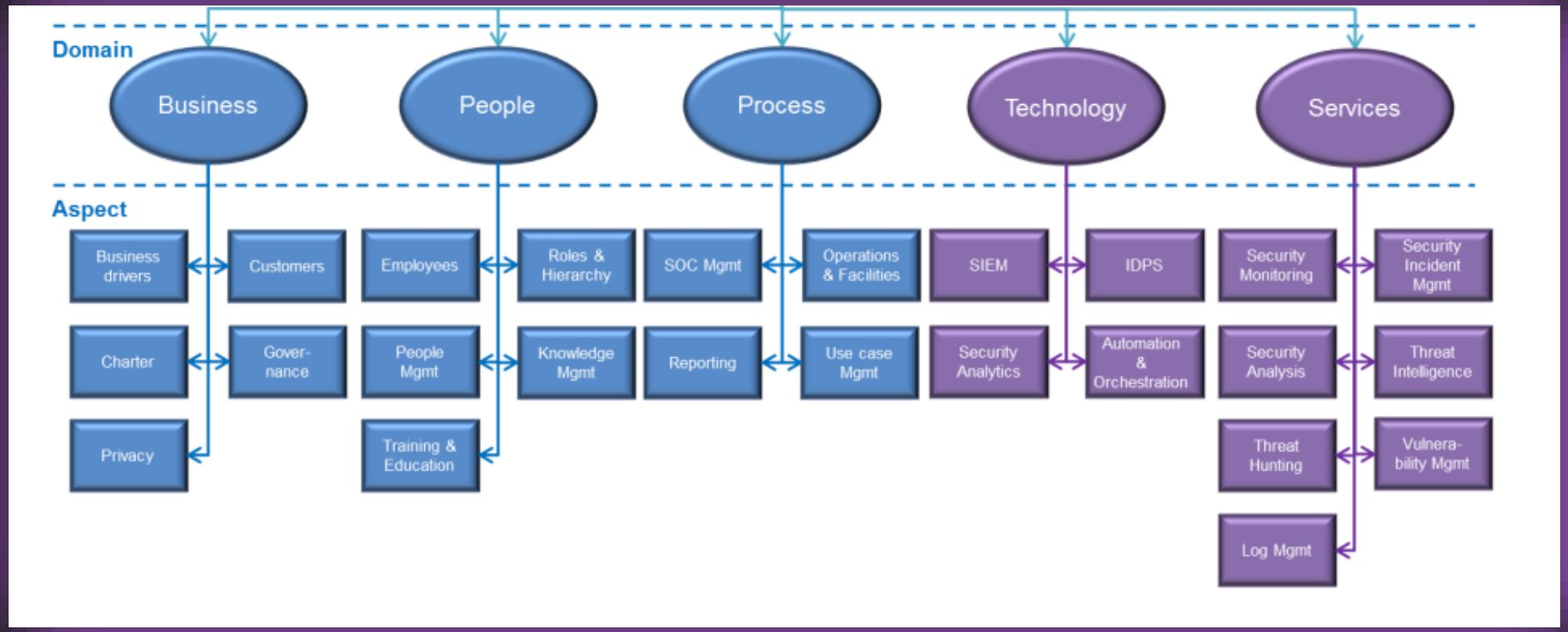
Оценка зрелости SOC

> Нельзя управлять тем, что невозможно измерить

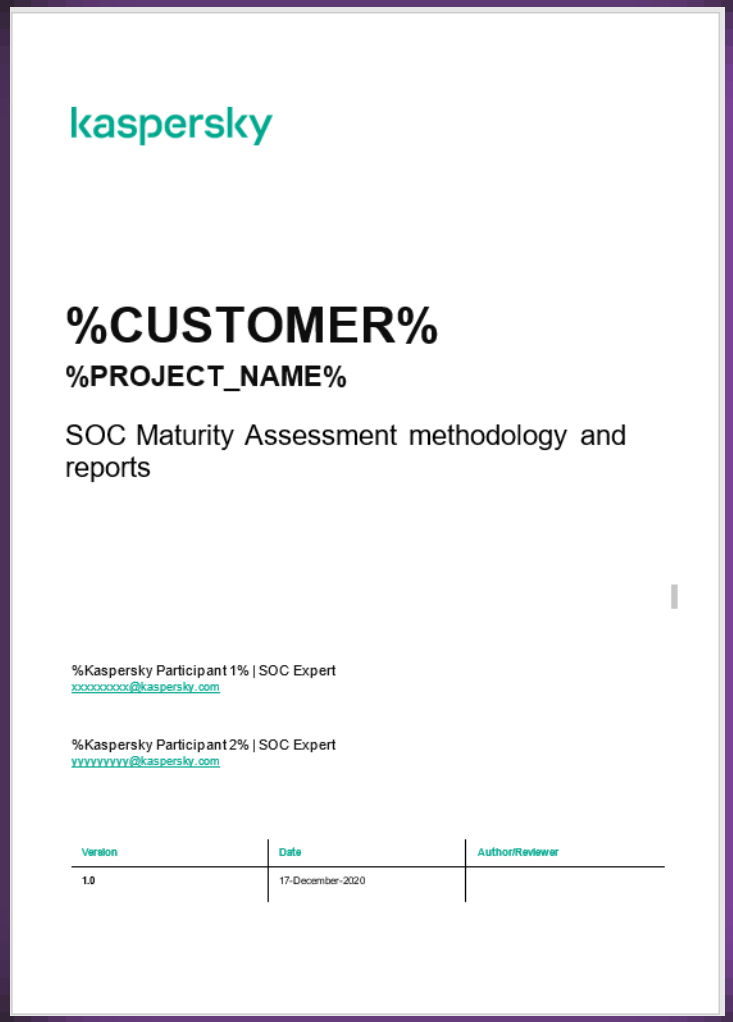
Джек Уэлч, исполнительный директор General Electric

Оценка зрелости SOC

- Модифицированная модель SOC-CMM (CMMI-based)
- 5 доменов, 25 сабдоменов, ~750 критериев
- Вендор-независимая модель



Результаты



kaspersky

%CUSTOMER%

%PROJECT_NAME%

SOC Maturity Assessment methodology and reports

%Kaspersky Participant 1% | SOC Expert
xxxxxxxxx@kaspersky.com

%Kaspersky Participant 2% | SOC Expert
yyyyyyyyy@kaspersky.com

Version	Date	Author/Reviewer
1.0	17-December-2020	

Содержание отчета:

- Краткое резюме
- Описание методологии
- Оценка текущего уровня зрелости и возможностей SOC
- Описание целевого состояния
- GAP анализ
- Дорожная карта по достижению целевого состояния

Проектирование SOC

> Построение SOC –
> это марафон, а не спринт

Gartner, «How to Plan, Design, Operate and Evolve a SOC», 2018

Как мы можем помочь

Проектирование SOC

Технологии

Техническая архитектура и компоненты SOC

Стратегия

Миссия, стейкхолдеры, стратегия, дорожная карта, задачи и цели, операционная модель и т.д.

Сценарии обнаружения и реагирования

Фреймворк управление жизненным циклом + библиотека сценариев

Процессы

Детальное описание процессов и процедур, use-cases, плейбуков

Персонал

Детальное описание оргштатной структуры, ролей, требований и обязанностей

Наш подход

Основан на практике

Сбалансированный

Комплексный

Результаты проекта

Комплект документов

~ 12 документов, начиная со стратегии и заканчивая пошаговыми процедурами в рамках процессов

Технические решения Kaspersky

KUMA, KEDR, KATA, Research Sandbox, Threat Intelligence, CyberTrace TIP, KICS и т.д.

Пост-проектная поддержка

Консультации, техподдержка, профессиональные сервисы

Поддерживающие сервисы и экспертные тренинги

Managed сервисы DFIRMA, MDR, red teaming и другие

Примеры проектов

Россия

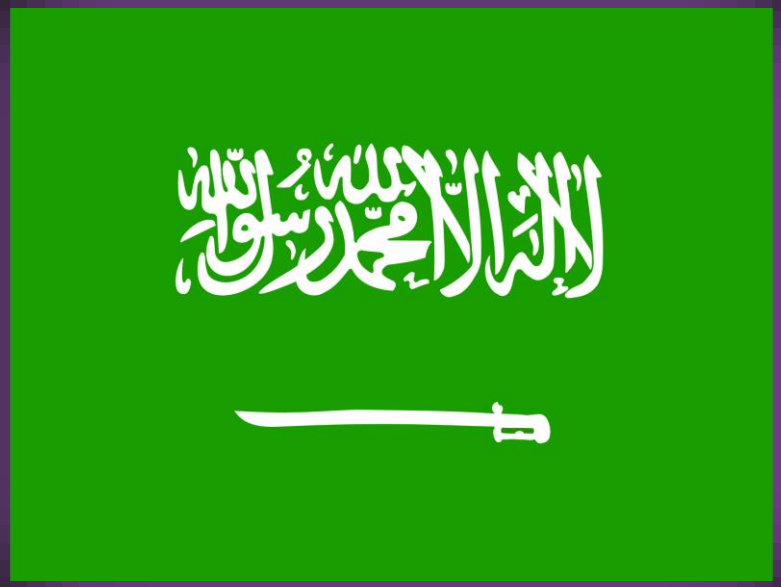
Профиль заказчика

- Индустрия: государственная организация
- Кол-во площадок: 4
- Кол-во хостов: >10.000
- Кол-во ЦОД: 3

Технические средства SOC (основные)

- **SIEM** - KUMA
- **EDR** – KEDR
- **Anti-APT** - KATA
- **TIP** - Kaspersky CyberTrace
- **TI** - Kaspersky Threat Data feeds, Kaspersky APT reporting, Kaspersky Threat lookup + сторонние поставщики
- **IRP** – сторонний поставщик

Саудовская Аравия



Профиль заказчика

- Индустрия: MSSP
- Кол-во заказчиков: >10 (I этап)
- Режим работы: 24x7
- Сервисы: Мониторинг и реагирование, Threat Hunting, VM, пентесты, DF/MA

Технические средства SOC (основные)

- **SIEM** – сторонний поставщик
- **Репутационная БД** – Kaspersky Private Security Network
- **Anti-APT**– KATA
- **«Песочница»** - Kaspersky Research Sandbox
- **TIP** - Kaspersky CyberTrace
- **TI** - Kaspersky Threat Data feeds, Kaspersky Threat lookup
- **IRP, SOAR** – сторонний поставщик

Объединенные Арабские Эмираты

Профиль заказчика

- Индустрия: Технологическая компания
- Облачная инфраструктура (3 ЦОД)
- Режим работы: 24x7
- Сервисы: мониторинг и реагирование, Threat Hunting, Threat Intelligence, анализ ВПО

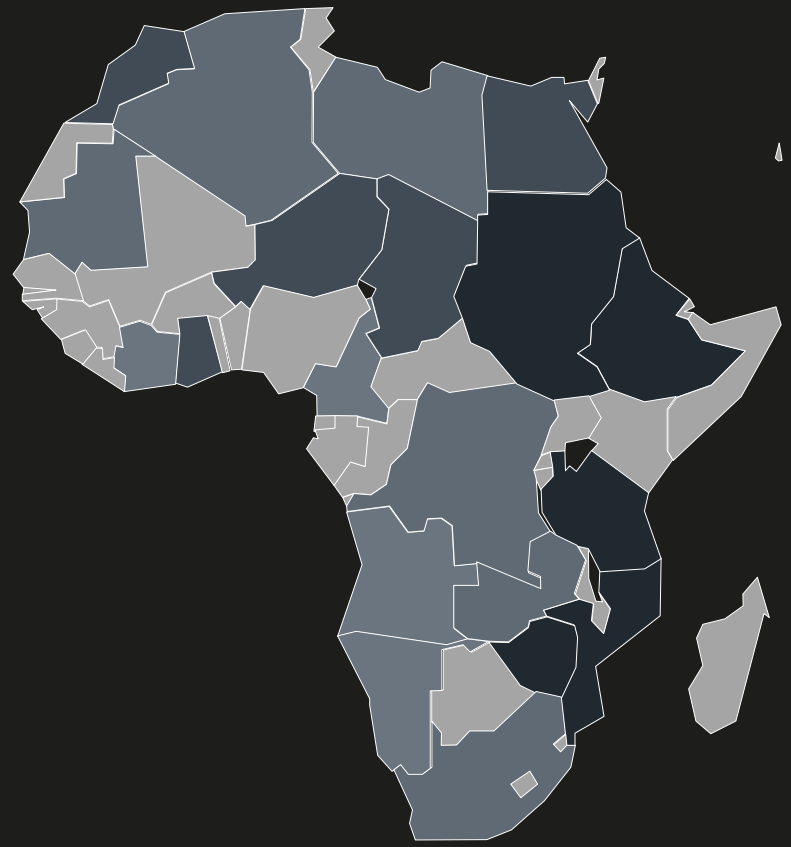
Технические средства SOC (основные)

- **SIEM –** сторонний поставщик
- **Сканнер защищенности –** сторонний поставщик
- **TIP -** Kaspersky CyberTrace
- **TI -** Kaspersky Threat Data feeds
- **IRP, SOAR –** сторонний поставщик

Африка (непубличный)

Профиль заказчика

- Национальный SOC
- 5 организаций из различных отраслей КИИ (пилотная зона)
- ~18k хостов (пилотная зона)
- Иерархический структура с координирующим и подчиненными SOC



Технические средства SOC (основные)

- **SIEM** – KUMA
- **Репутационная БД** – Kaspersky Private Security Network
- **Anti-APT**– KATA
- **«Песочница»** - Kaspersky Research Sandbox, Kaspersky Sandbox
- **TIP** - Kaspersky CyberTrace
- **TI** - Kaspersky Threat Data feeds, Kaspersky Threat lookup, Отчеты APT
- **Атрибуция угроз** – Kaspersky Threat Attribution Engine

Спасибо!

kaspersky