Как построить надёжный SOC

Февраль 2024

самолет

ИТ-ландшафт в Самолете

быстрый взгляд

18

Сервисов в собственной технологической платформе для команд разработки

1500+

ИТ-специалистов

359

Систем в ИТ-ландшафте

10+ млрд руб.

Бюджет на ИТ в 2023 году

>100 ИТ-команд

- Цифра
- Проектный институт
- Централизованные сервисы
- HR Tech
- Финтех
- 10D
- Самолет+
- ИИ Данные
- Образование
- Фонды
- Гостеприимство

2 ЦОД

Георапределенный метрокластер

99.95%

Доступность

до 2.7 ПБ

x2 рост объема данных

самолет

ИТ-ландшафт и бизнес-сервисы Самолета

2022 и ранее · 2023 · Планы на 2024

Продажи

- Цифровая платформа Самолет Плюс
- CRM
- Контакт-центр
  Речевая аналитика

Девелопмент

- Цифровой девелоперский цикл S.Платформа
- Проектирование
  BIM-моделирование

Гостеприимство

- ЖКХ, ТОиР
- Приложение для жителей

Управление финансами

- Базовый учет, отчетность
- Казначейство
- Фин. моделирование
- Договорной учет
- Бюджетирование S.AXP

Управление данными

- MDM
- КХД
- BI
- Единый профиль клиента Самолет ID

HR

- HR-сервисы S.Team
- Кадровый учет
- Подбор персонала
- Управление эффективностью и развитием сотрудников

ЭДО

- Электронный архив
- Электронный документооборот

Автоматизация бизнес-процессов

- Robot Process Automation
- BPM система

Банк

- Платформа Финтех
- Платежный шлюз
- GateWay
- Админ панель

Образование

- Электронный журнал

Фонды

- Платформа Управление паевыми фондами

самолет

Ландшафт угроз

Факторы изменения киберугроз и рисков в 2024 г.:*

- AI&ML, эволюция социальной инженерии
- геополитические факторы
- органический рост прежних угроз и рисков
- инновации в средствах защиты
- инновации в инструментах злоумышленников

*Источник: https://www.anti-malware.ru/analytics/Threats_Analysis/2024-Forecast

самолет

SOC в Самолете

- Более 15 млрд. событий в месяц
- более 1000 карточек с подозрением на инцидент в месяц
- мультивендорный подход, применяются средств защиты разных вендоров
- автоматизированы процессы реагирования на типовые инциденты
- реагирование выстраивается в виде мини-сценариев, которые запускают друг друга в зависимости от условий, типа инцидента и доступного окружения (используются динамические плейбуки)
- автоматизировано обогащение информации по инцидентам

самолет

Оценка эффективности и надёжности SOC

1. Оценка проводится собственными силами 1 раз в квартал:

Выявляем актуальные угрозы → Формируем перечень векторов атак, реализующих указанные угрозы → Имитируем реализацию каждого из векторов атак → Оцениваем корректность отработки средств защиты, процессов и команды → Корректируем настройки систем защиты, корректируем процессы реагирования на инциденты, обучаем команду

2. Оценка проводится в рамках внешнего тестирования на проникновение – 1 раз в 6 месяцев. Привлекается внешняя команда пентестеров. Команда SOC не знает точное время проведения тестирования на проникновение. По итогам тестирования осуществляется анализ протокола действий в контексте выявленных командой SOC инцидентов.

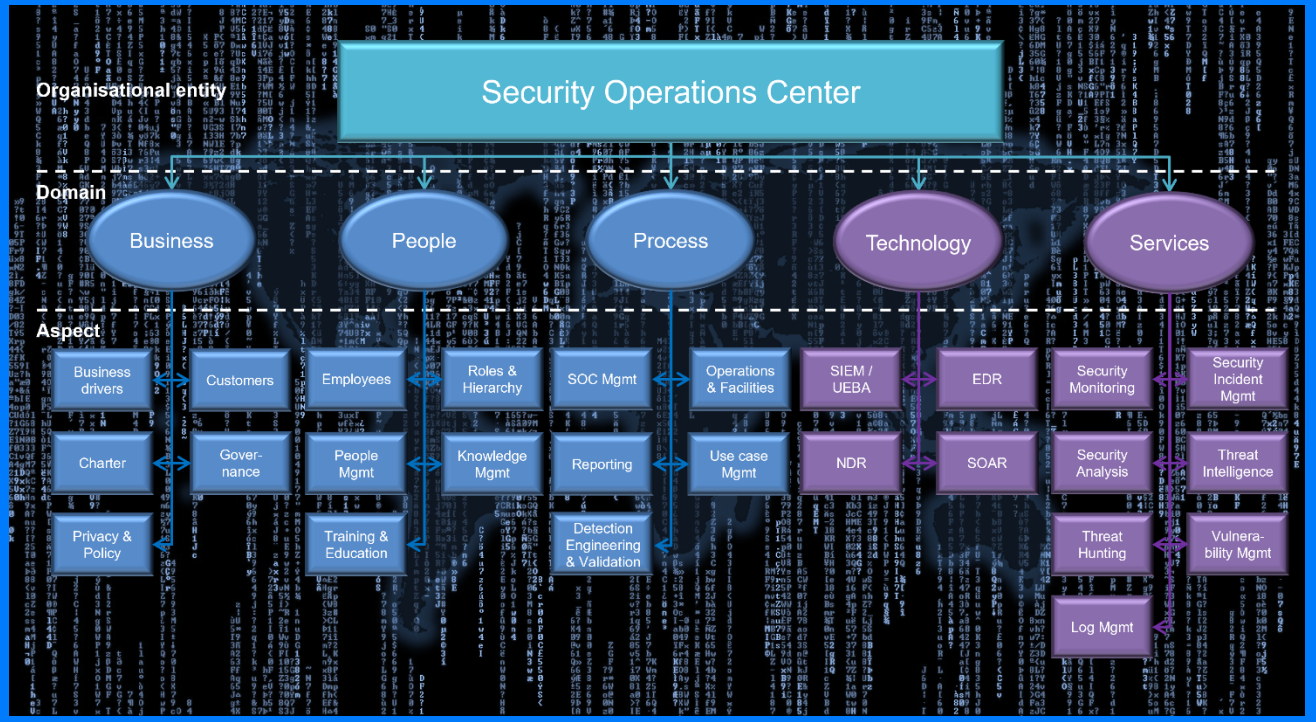
Pentest с фиксацией протокола действий → Оцениваем корректность отработки средств защиты, процессов и команды → Корректируем настройки систем защиты, корректируем процессы реагирования на инциденты, обучаем команду

Оценка эффективности и надёжности SOC

3. Анализируем следующие метрики:

- время обнаружения угрозы (TTD, Time-to-detect)
- время локализации угрозы (TTC, Time-to-Contain)
- время реагирования на угрозу (TTR, time-to-Response)

4. Оценка уровня зрелости (SOC-CMM):



самолет