



BI.ZONE

SOaaS. Особенности взаимодействия с Заказчиком

Александр Скоркин

Главный инженер

Нур-Султан, 12 Апреля 2019

BI.ZONE сегодня

- Ведущая компания по кибербезопасности в России и странах СНГ
- 250+ сотрудников
- 100+ клиентов из разных отраслей
- 150+ успешно выполненных проектов
- Член различных международных организаций по координации борьбы с киберпреступностью
- Активный игрок на рынках Европы, Южной и Центральной Азии, предоставляющий различные услуги в области кибербезопасности
- Стратегический партнер INTERPOL Global Complex for Innovations
- Сбербанк - партнер-основатель Центра кибербезопасности WEF (C4C)



BI.ZONE



Наш опыт



Sberbank SOC

- Сбербанк сегодня - крупнейший банк России и крупная международная корпорация. Сбербанк имеет 12 региональных банков, которые отвечают за функционирование более 14 000 отделений в 83 регионах России.
- Крупнейший SOC в Европе
- 400+ специалистов
- Сертификат BSI ISO/IEC 27001
- Проект занял третье место на IPMA Global Project Excellence Awards 2018



Продукты и услуги



Профессиональные услуги

- Построение SOC
- Модернизация SOC
- Аудит SOC
- Проведение учений
- Консалтинг
- MSS/MDR

Продукты

- BI.ZONE ThreatVision
- BI.ZONE Feeds
- BI.ZONE Defzone
- TI.Sensors
- BI.ZONE Cloud Froud Prevention
- SOAR/GRC
- BI.ZONE SIEM

Экспертные сервисы

- Компьютерная криминалистика
- Тестирования на проникновения
- Расследование инцидентов кибербезопасности
- Тестирование защищенности мобильных и веб-приложений
- Нагрузочное и функциональное тестирование

Что мы видим?



BI.ZONE



Инфраструктура

Незнание своей инфраструктуры



Компетенции

Отсутствие необходимых компетенций



Скомпрометированные системы

Выявляется значительное число скрытых инцидентов ИБ



Источники

Нет понимания по источникам событий



Уязвимости

Управление уязвимостями отсутствует



Реакция

Длительная скорость реакции на инциденты и рекомендации.
От нескольких часов до ∞



Владельцы активов

Не определены



Эффективность имеющих СЗИ

Средства ИБ не настроены должным образом



Коммуникации

Отсутствие коммуникации между департаментами и внутреннего SLA. Обратная связь с провайдером услуги

Что мы видим?



BI.ZONE



Инфраструктура

Незнание своей инфраструктуры



Управление активами

Нет понимания по источникам инцидентов



Владельцы активов

Не определены



Обучение и повышение осведомленности



Уязвимости

Управление уязвимостями отсутствует

Управление уязвимостями и оценка защищенности



Эффективность средств ИБ

Средства ИБ не настроены должным образом



Скомпрометированные системы

Выявляется значительное число скрытых инцидентов ИБ



Управление инцидентами

Длительная скорость реакции на инциденты и рекомендации. От нескольких часов до ∞



Коммуникации

Отсутствие коммуникации между департаментами и внутреннего SLA. Обратная связь с провайдером услуги

В результате

- Неудовлетворенность работой SOC
- Неэффективность работы SOC
- Неоправданные ожидания
- Психологическая напряженность



BI.ZONE



Управление активами



BI.ZONE

- Учет информация по основным активам (сети, оборудование, ПО, ИС, бизнес-процессы)

- Интеграция с внешними источниками данных и их анализ

- Классификация и категорирование активов

- Оценка рисков

- Выбрать ключевые активы для защиты на основе:

- План непрерывности
- Критичные для бизнеса
- Понятные всем активы
- «Внутренние чемпионы»

Управление уязвимостями и оценка защищенности



BI.ZONE

- Внедрены процедуры по устранению уязвимостей
- Анализ выявленных уязвимостей
- Анализ соответствия требованиям
- Оценка угроз
- Отчёты

Управление инцидентами



BI.ZONE

- Регламент взаимодействия
- Комплект документов по управлению инцидентами
- Согласован перечень инцидентов
- Созданы рабочие группы
- Разработаны сценарии реагирования на инциденты
- Учения по отработке инцидентов

Обучение и повышение осведомленности



BI.ZONE

- Обучение
- Контроль знаний
- Инструкции
- База знаний



Что в итоге?



BI.ZONE

1

Выполнен учет и классификация активов

4

Выполняется управление и анализ уязвимостями

7

Service Desk,
база знаний

2

Осуществляется сбор событий со всех значимых систем

5

Выполняется управление инцидентами

3

Выполняется управление событиями безопасности

6

Выстроен процесс реагирования. Четкое выполнение регламентов и инструкций.

Global Cyber Security Week



17-21 ИЮНЯ, 2019



17-18 ИЮНЯ, 2019

offzone.moscow



Cyber Polygon

19 ИЮНЯ, 2019

cyberpolygon.bi.zone



20-21 ИЮНЯ, 2019

icc.moscow





www.bi.zone

Москва, Ольховская 4с2

+7 (495) 123-45-67

info@bi.zone