Информзащита
Системный интегратор

Внешний SOC

www.infosec.ru

Знакомство

Информзащита
IZ:SOC

Иван Мелехин
Директор по развитию IZ:SOC
i.melekhin@infosec.ru

- Сбор и хранение событий
- Мониторинг и анализ киберугроз
- Расследование
- Threat intelligence
- Red team
- Управление уязвимостями
- Госсопка

- **24x7x365**
- **9x5**
- **Индивидуальные SLA**
- **Заказные use-case**

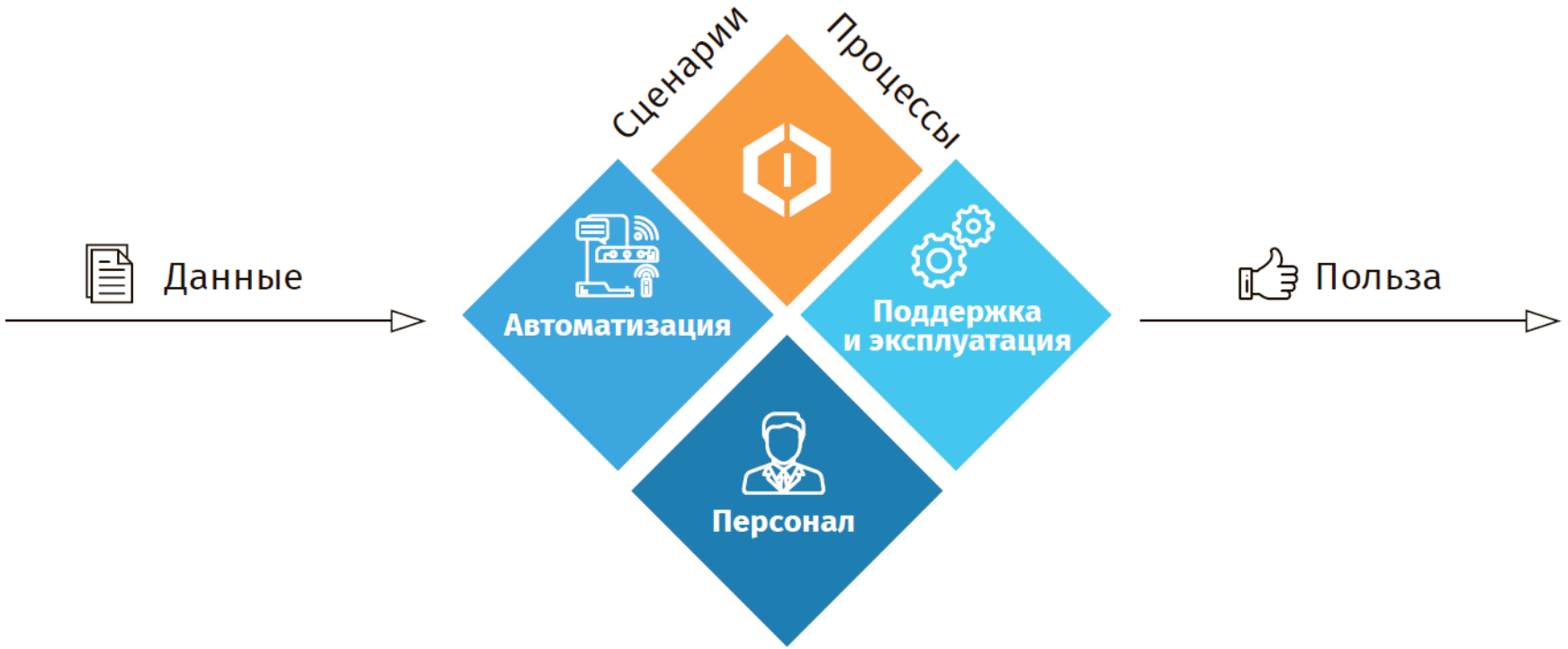
Выбор поставщика

Выбор: Что делать?

Нам нужен SIEM!

Нам нужна функция мониторинга, реагирования и предотвращения киберугроз!

Мониторинг и реагирование – штука комплексная

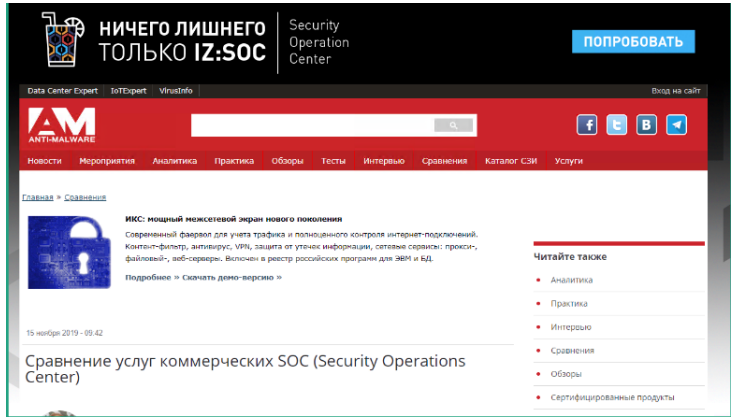


Выбор: Что делать?

1. Составить список вопросов (любых)

3. Задавать вопросы (любые)

2. Написать\позвонить\заполнить форму на сайте и попросить ознакомительный конф-колл .



Выбор: Что учитывать?

1. Скорость ответа
2. Открытость
3. Комфорт в общении
4. Общие ценности
5. Готовность идти навстречу

……

992830. 196 пунктов сравнения Anti-malware

Архитектура SOC

Архитектура SOC

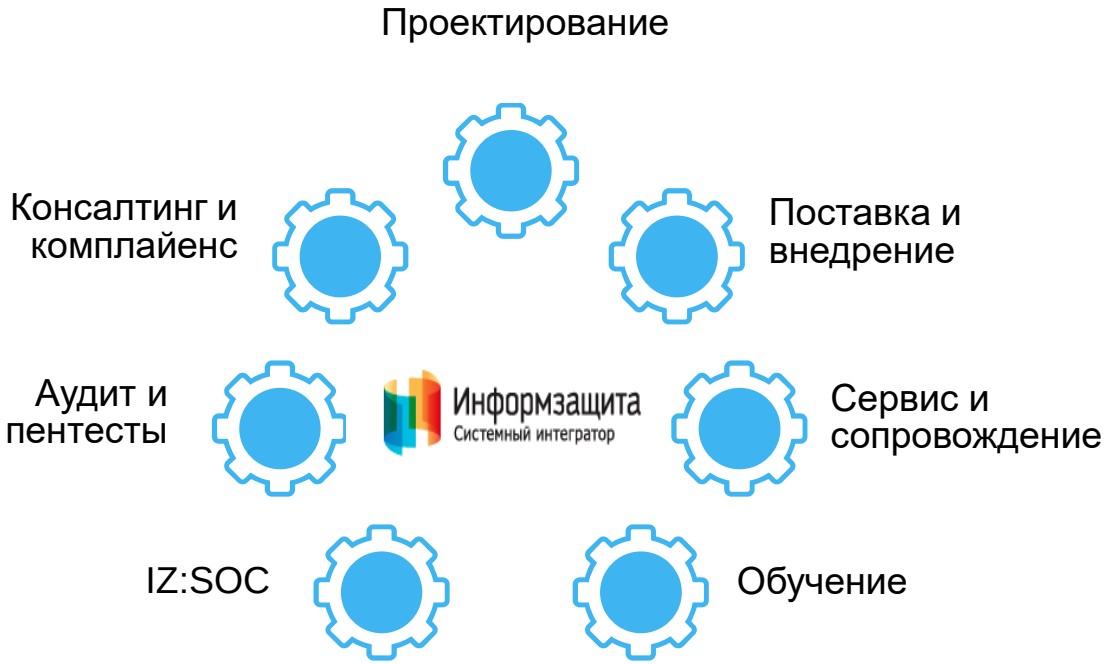
- А какая архитектура вашего SOCa?
- Работающая….

1. Стоимость и что на нее влияет
2. Вариативность подключения
3. Возможность интеграции
4. Гибридные схемы
5. Облачные схемы
6. Госсопка
7. Доступ к событиям
8. Каналы взаимодействия
9. Выгрузка данных

Функционал

Функционал

1. Автоматизированный мониторинг и информирование
2. Ручная обработка, анализ и рекомендации
3. Расследования
4. Реагирование
5. Разработка сценариев
6. Управление уязвимостями\пен-тесты
7. Управление СЗИ
8. Рекомендации, смежные проекты



Стоимость

Стоимость

1. Структура:
    1. Ежегодный (регулярный) платеж
    2. Платеж за подключение (скрыт в платеже первого года)
    3. Страхование
2. Зависит от:
    1. Объём данных и сроки хранения
    2. Функционал
    3. Набор сценариев
    4. Режим работы

Персонал

Персонал

- А как у вас обстоят дела с персоналом?
- С персоналом дела обстоят хорошо, без него плохо….

1. С кем вы будете взаимодействовать?
2. Кто за что отвечает?
3. Кому жаловаться?
4. А можно ли поговорить с «головой» ?

Пилот

Пилот

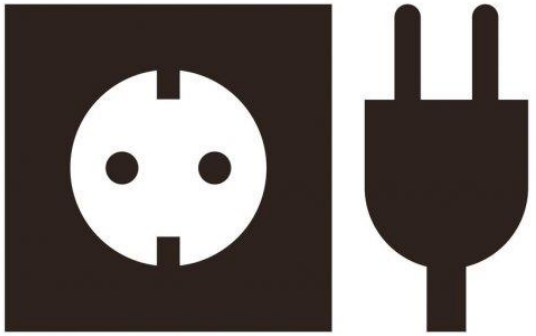
1. Возможен!
2. Подключение - от трех недель до шести месяцев
3. А нам помогут?
4. Скорее всего, ничего ужасного
5. Но вскроет массу проблем

Подключение и использование

Внешний SOC – подводная часть айсберга

Подключение и эксплуатация

1. Доработка сценариев
2. Обучение правил
3. Отладка каналов взаимодействия
4. От вас все время будут что-то хотеть …..
5. Ваша заметность вырастет на порядок
6. Возможно, вас начнут ненавидеть (ИТ)
7. Уважение, уважение, уважение…



Подключение и эксплуатация

1. Новые сценарии
2. Новые источники
3. Отчетность, доработка отчетов
4. Нас ломали, а вы не заметили…
5. Вчера мы случайно отгрузили вам 30 000 ЕПС вместо купленных 1000….

Смена поставщика

Вывод из эксплуатации

Резюме

DYI - кратко

2 месяц

Выбор платформы

Импортозамещение
Санкции
Цена
Производительность

4 месяц

Расчёты, расчёты, бюджет

А СХД не забыл?
А почему вендор просит 20 виртуалок 8х64?
А у нас 1000 епс или 100 000?

7 месяц

Бюджетирование, смотрины, подготовка к конкурсу

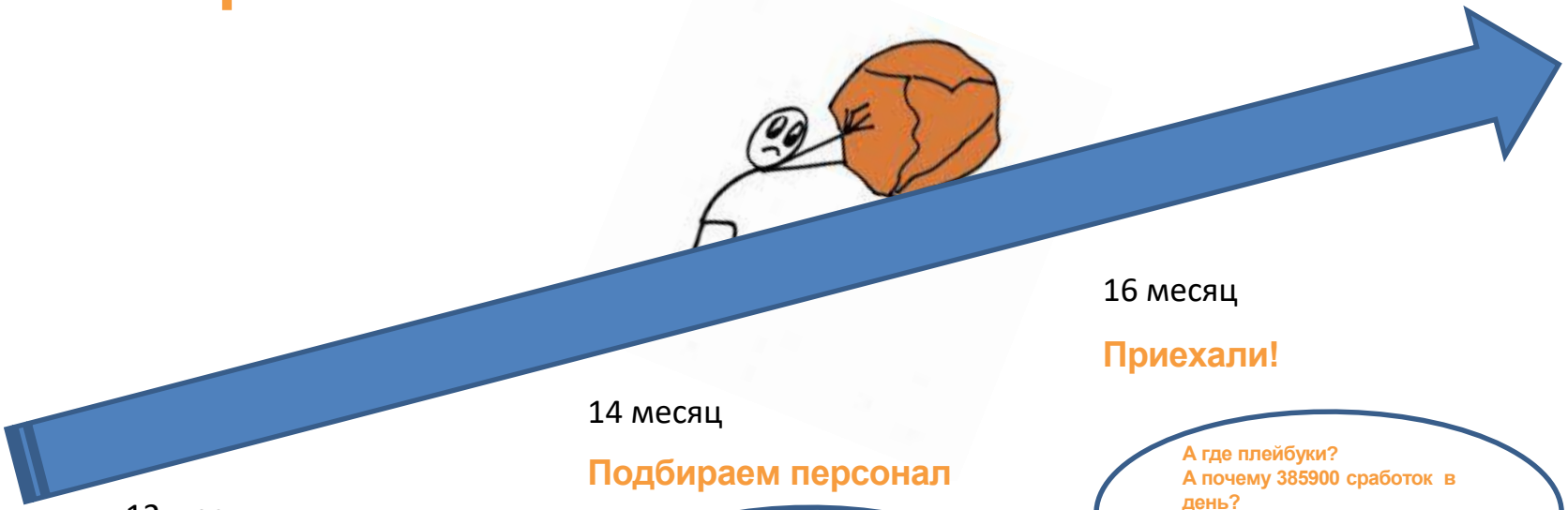
Сколько, сколько?
Ага, а техподдержку забыли
А на кораблике круче было…
Персонал? Какой персонал?!!

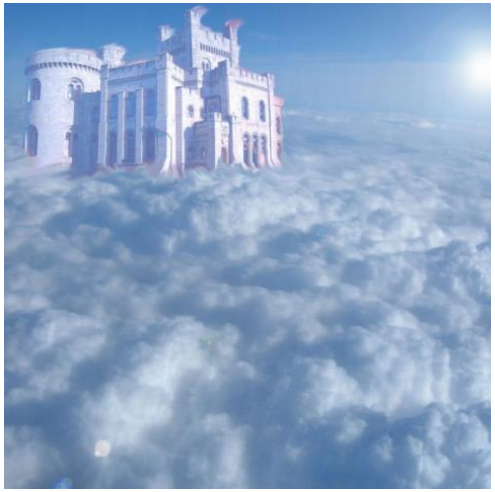
9 месяц

Поехали!!

Конец года… может в январе?
А вы в ТЗ это не написали
Вы скажите как хотите, а мы так и сделаем
Да, мы вам включим сценарии вендора

DYI - кратко





12 месяц

Проектирование, монтаж, пусконаладка

А в ТЗ 1000 ЕПС, а у вас 100 000
Вот ваши 4 правила

14 месяц

Подбираем персонал

Да посадим в Вологде 2 админов вот вам и аналитики!
Зачем мне к вам в Москву ехать..
Я L1 аналитик! Денег мне, и побольше…
А обучение?

16 месяц

Приехали!

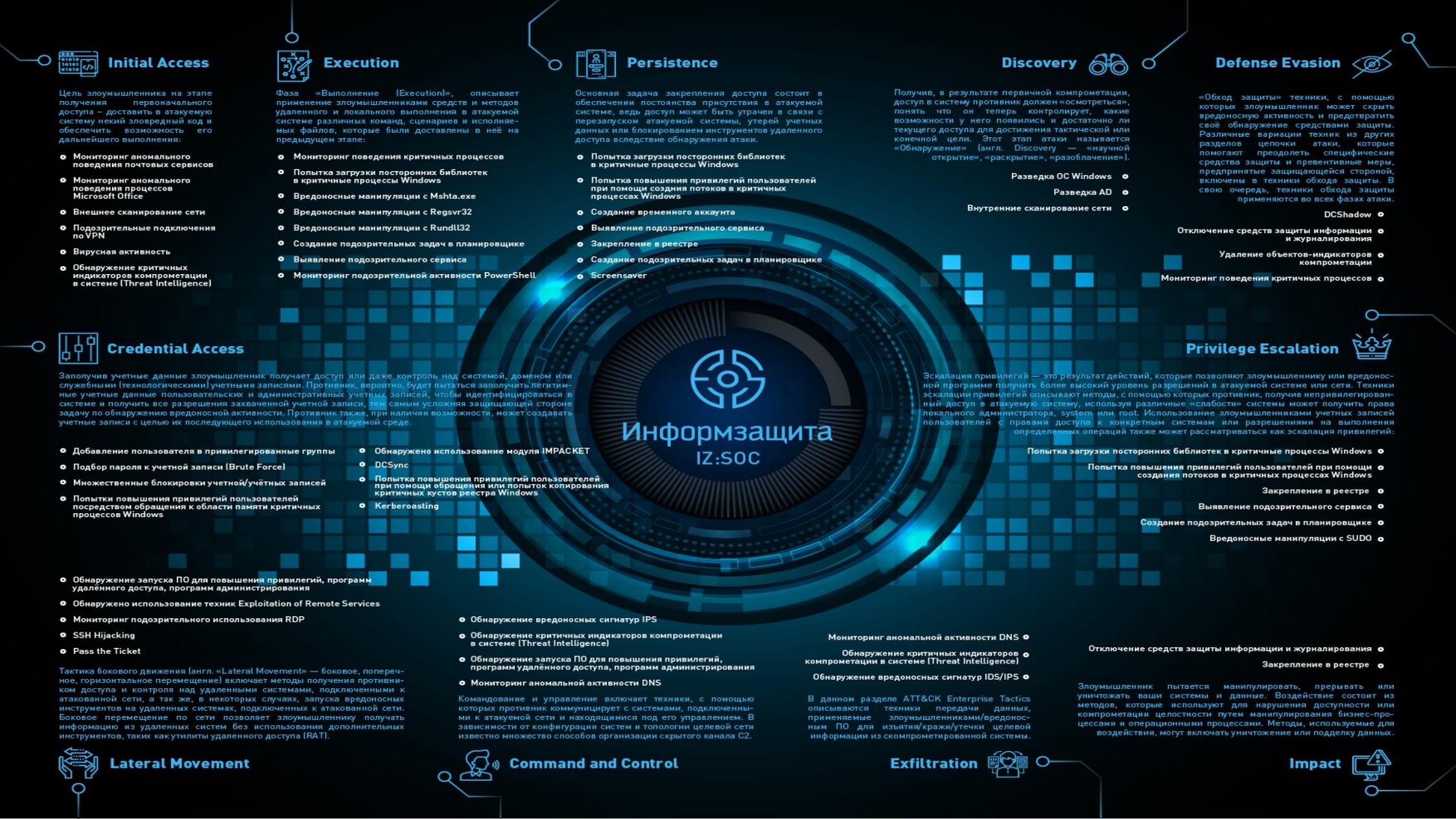
А где плейбуки?
А почему 385900 сработок в день?
А как это работает?
Вот вам 1 ставка на 50 000р.
Денег на ТП нет!

Внешний SOC - кратко

8 месяцев	2 месяца	2 месяца	2 месяца	1 неделя
Внешний SOC	**Отладка Подключение**	**Бюджет Контракт**	**Пилот**	**Пообщались с поставщиками сервиса**

- **Другой поставщик**
- **Свой SOC**
- **Своя IRP, SOAR …**

А еще….


Initial Access
Цель злоумышленника на этапе получения первоначального доступа – доставить в атакуемую систему некий зловредный код и обеспечить возможность его дальнейшего выполнения:
Мониторинг аномального поведения почтовых сервисов
Мониторинг аномального поведения процессов Microsoft Office
Внешнее сканирование сети
Подозрительные подключения по VPN
Вирусная активность
Обнаружение критичных индикаторов компрометации в системе (Threat Intelligence)
Execution
Фаза «Выполнение (Execution)», описывает применение злоумышленниками средств и методов удаленного и локального выполнения в атакуемой системе различных команд, сценариев и исполняемых файлов, которые были доставлены в неё на предыдущем этапе:
Мониторинг поведения критичных процессов
Попытка загрузки посторонних библиотек в критичные процессы Windows
Вредоносные манипуляции с Mshta.exe
Вредоносные манипуляции с Regsvr32
Вредоносные манипуляции с Rundll32
Создание подозрительных задач в планировщике
Выявление подозрительного сервиса
Мониторинг подозрительной активности PowerShell
Persistence
Основная задача закрепления доступа состоит в обеспечении постоянства присутствия в атакуемой системе, ведь доступ может быть утрачен в связи с перезапуском атакуемой системы, утерей учетных данных или блокированием инструментов удаленного доступа вследствие обнаружения атаки.
Попытка загрузки посторонних библиотек в критичные процессы Windows
Попытка повышения привилегий пользователей при помощи создания потоков в критичных процессах Windows
Создание временного аккаунта
Выявление подозрительного сервиса
Закрепление в реестре
Создание подозрительных задач в планировщике
Screensaver
Discovery
Получив, в результате первичной компрометации, доступ в систему противник должен «осмотреться», понять что он теперь контролирует, какие возможности у него появились и достаточно ли текущего доступа для достижения тактической или конечной цели. Этот этап атаки называется «Обнаружение» (англ. Discovery — «научной открытие», «раскрытие», «разоблачение»).
Разведка ОС Windows
Разведка AD
Внутренние сканирование сети
Defense Evasion
«Обход защиты» техники, с помощью которых злоумышленник может скрыть вредоносную активность и предотвратить своё обнаружение средствами защиты. Различные вариации техник из других разделов цепочки атаки, которые помогают преодолеть специфические средства защиты и превентивные меры, предпринятые защищающейся стороной, включены в техники обхода защиты. В свою очередь, техники обхода защиты применяются во всех фазах атаки.
DCShadow
Отключение средств защиты информации и журналирования
Удаление объектов-индикаторов компрометации
Мониторинг поведения критичных процессов
Credential Access
Заполучив учетные данные злоумышленник получает доступ или даже контроль над системой, доменом или служебными (технологическими) учетными записями. Противник, вероятно, будет пытаться заполучить легитимные учетные данные пользовательских и административных учетных записей, чтобы идентифицироваться в системе и получить все разрешения захваченной учетной записи, тем самым усложняя защищающей стороне задачу по обнаружению вредоносной активности. Противник также, при наличии возможности, может создавать учетные записи с целью их последующего использования в атакуемой среде.
Добавление пользователя в привилегированные группы
Подбор пароля к учетной записи (Brute Force)
Множественные блокировки учетной/учётных записей
Попытки повышения привилегий пользователей посредством обращения к области памяти критичных процессов Windows
Обнаружено использование модуля IMPACKET
DCSync
Попытка повышения привилегий пользователей при помощи обращения или попыток копирования критичных кустов реестра Windows
Kerberoasting
Информзащита
IZ:SOC
Privilege Escalation
Эскалация привилегий — это результат действий, которые позволяют злоумышленнику или вредоносной программе получить более высокий уровень разрешений в атакуемой системе или сети. Техники эскалации привилегий описывают методы, с помощью которых противник, получив непривилегированный доступ в атакуемую систему, используя различные «слабости» системы может получить права локального администратора, system или root. Использование злоумышленниками учетных записей пользователей с правами доступа к конкретным системам или разрешениями на выполнения определенных операций также может рассматриваться как эскалация привилегий:
Попытка загрузки посторонних библиотек в критичные процессы Windows
Попытка повышения привилегий пользователей при помощи создания потоков в критичных процессах Windows
Закрепление в реестре
Выявление подозрительного сервиса
Создание подозрительных задач в планировщике
Вредоносные манипуляции с SUDO
Обнаружение запуска ПО для повышения привилегий, программ удалённого доступа, программ администрирования
Обнаружено использование техник Exploitation of Remote Services
Мониторинг подозрительного использования RDP
SSH Hijacking
Pass the Ticket
Тактика бокового движения (англ. «Lateral Movement» — боковое, поперечное, горизонтальное перемещение) включает методы получения противником доступа и контроля над удаленными системами, подключенными к атакованной сети, а так же, в некоторых случаях, запуска вредоносных инструментов на удаленных системах, подключенных к атакованной сети. Боковое перемещение по сети позволяет злоумышленнику получать информацию из удаленных систем без использования дополнительных инструментов, таких как утилиты удаленного доступа (RAT).
Lateral Movement
Обнаружение вредоносных сигнатур IPS
Обнаружение критичных индикаторов компрометации в системе (Threat Intelligence)
Обнаружение запуска ПО для повышения привилегий, программ удалённого доступа, программ администрирования
Мониторинг аномальной активности DNS
Командование и управление включает техники, с помощью которых противник коммуницирует с системами, подключенными к атакуемой сети и находящимися под его управлением. В зависимости от конфигурации систем и топологии целевой сети известно множество способов организации скрытого канала C2.
Command and Control
Мониторинг аномальной активности DNS
Обнаружение критичных индикаторов компрометации в системе (Threat Intelligence)
Обнаружение вредоносных сигнатур IDS/IPS
В данном разделе ATT&CK Enterprise Tactics описываются техники передачи данных, применяемые злоумышленниками/вредоносным ПО для изъятия/кражи/утечки целевой информации из скомпрометированной системы.
Exfiltration
Отключение средств защиты информации и журналирования
Закрепление в реестре
Злоумышленник пытается манипулировать, прерывать или уничтожать ваши системы и данные. Воздействие состоит из методов, которые используют для нарушения доступности или компрометации целостности путем манипулирования бизнес-процессами и операционными процессами. Методы, используемые для воздействия, могут включать уничтожение или подделку данных.
Impact

Информзащита
Системный интегратор

IZ:SOC 24x7x365

IZ:SOC

+7 495 980 23 45
izsoc@infosec.ru
www.izsoc.ru

Fraud management
antifraud@infosec.ru

Press office
pr@infosec.ru

System integrator

+7 495 980 23 45
market@infosec.ru
www.infosec.ru

Service

+7 495 981 92 22
support@itsoc.ru
www.itsoc.ru