SOC как сервис. Опыт HeadHunter

Терентьев Виталий, директор ДСП HeadHunter

Виталий Терентьев

Директор Департамента специальных проектов, HeadHunter

- Управляющий партнер HeadHunter Центральная Азия
- Профессиональный управленец, реализовывал различные проекты по внедрению технологий, созданию и развитию инновационных бизнесов

Внешний SOC - центр

Причины выбора:

- Экономическая эффективность;
- Масштабирование своего персонала;
- Поддержка непрофильных компетенций;
- Качество сервиса.

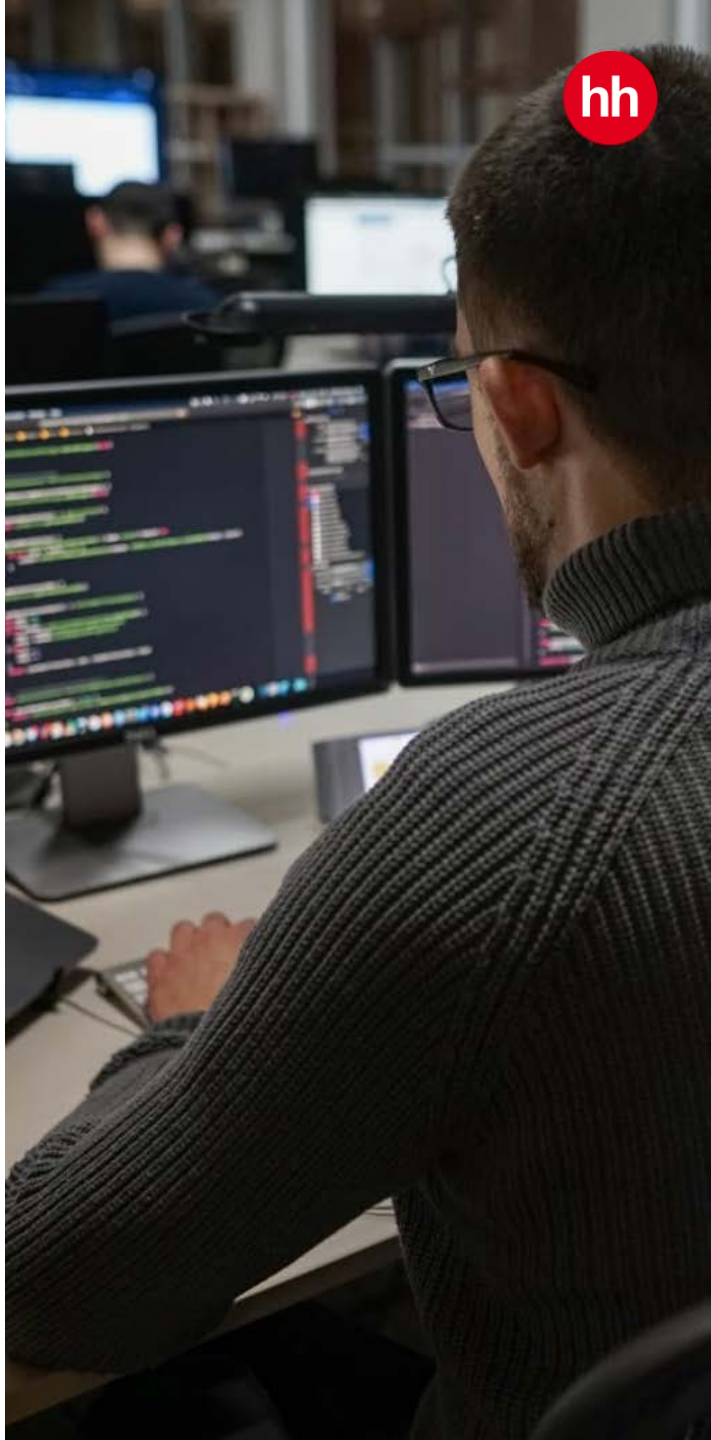
Тонкости внедрения

Получаемый сервис: мониторинг киберугроз.

Реагирование: получение от поставщика сервиса SOC рекомендаций по реагированию, но весь процесс внесения изменений в нашу инфраструктуру находится полностью под нашим контролем и управлением.

Процессы: отсутствие жесткой формализации позволяет гибко подходить к вопросу что является инцидентом и определять степень его критичности в момент реагирования.

Масштабирование: в связи с территориальной распределенностью мы используем одну площадку как модель для дальнейшего распространения на остальные.

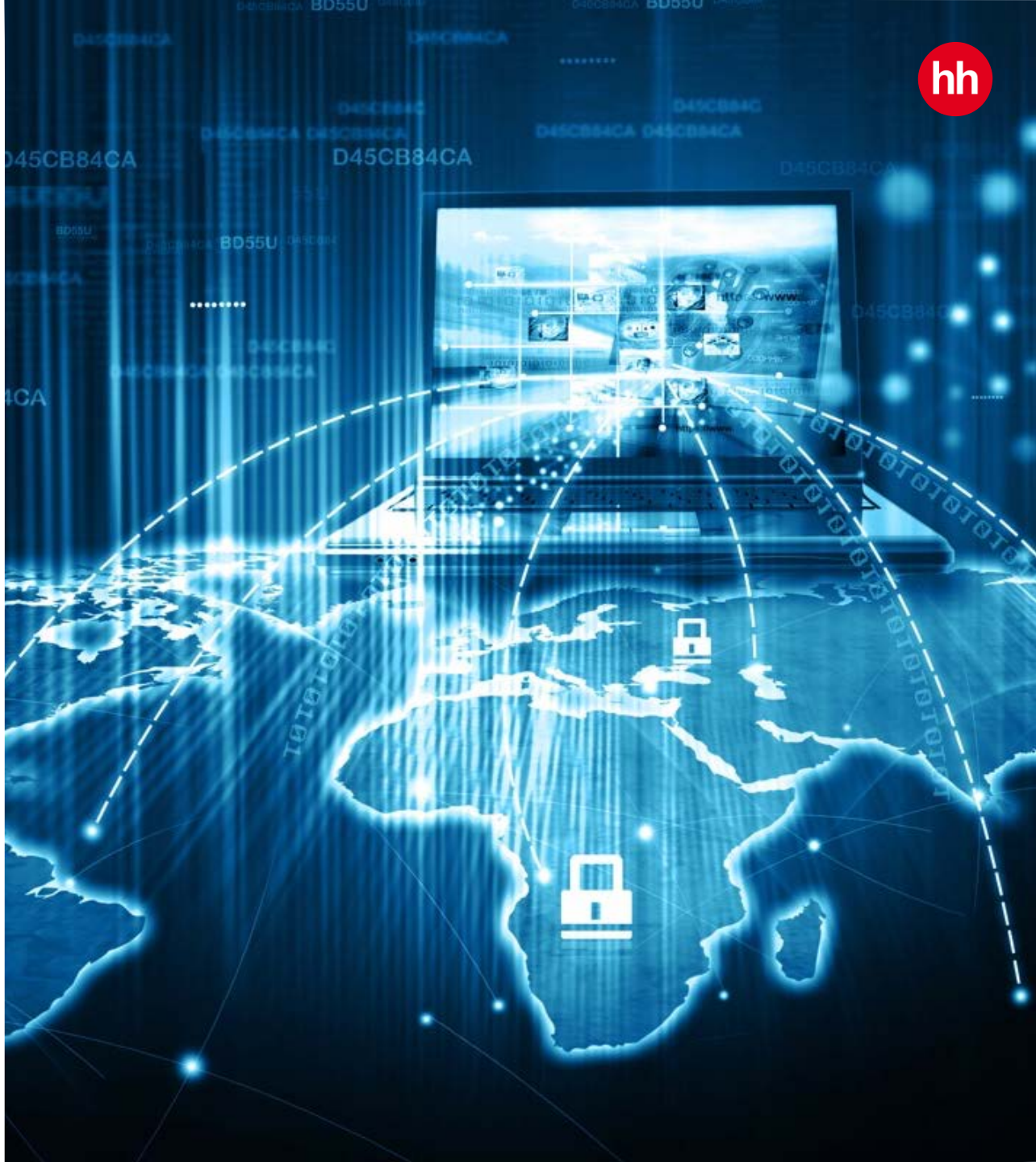


Места для подъема

Прозрачность для бизнес-заказчиков

Большое количество технической информации и полное отсутствие динамически формируемых отчетов бизнес уровня с привязкой к степени защиты активов.

SLA с сервисом не учитывает потенциальных последствий от пропуска критичного инцидента.



Коммуникации

Несмотря на наличие постоянных каналов коммуникации в почте и мессенджерах, было много задержек в ответах и предоставлении информации и с той и с другой стороны.

Удачи

Мы получили сценарии мониторинга направленные на выявление базовых индикаторов компрометации, которые используются практически во всех техниках проникновения, вне зависимости от используемого злоумышленником инструментария или способа попадания внутрь.
В частности, мы видим инциденты, связанные с
- обращением к области памяти критичных процессов;
- созданием посторонних потоков в процессы;
- инжектами вредоносных библиотек в процессы;
- закреплением или изменением в реестре бестелесных вирусов;
- отслеживанием популярных утилит для кражи учётных записей таких как IMCPAKET;
- отслеживанием подозрительных служб и процессов на машине;
- аномалиями в работе операционных системы.

Благодарю за внимание!