Блокировать или следить – вот в чем вопрос!?

Элекснет

Элекснет

Ключевые проблемы на рынке

- **Удаленка и все что с ней связано**
  Пандемия затронула все сферы экономики
- **Размываемое понятие периметра - BYOD**
  Все больше бизнес процессов и решений завязано на мобильные устройства
- **Сложная нормативная база**
  Одного трудового договора мало. Положение о ПДн, коммерческой тайне и еще много всего интересного
- **Опыт мошенников против современных систем**
  Святая простота еще хуже злого умысла

Элекснет

Нормативная часть

✓ **Например положение о коммерческой тайне**

- Положение о КТ;
- Режим КТ;
- Места хранения КТ;
- Листы ознакомления с КТ;
- Маркировка…
- и т.д.

✓ **Персональные данные**

- Положение о ПД;
- Политика в отношении ПД;
- Перечислить места (системы) хранения ПД;
- Ответственные лица\должности и т.д.

✓ **Внедрение требований регуляторов**

Тут бесконечное перечисление!

Элекснет

Блокировать, нельзя детектировать

1. Простые политики для детектирования угроз – как правило готовые шаблоны от производителя;
2. Относительно дешевый сервис, с точки зрения стоимости часа работы аналитика – все сводится к практике: «Казнить нельзя помиловать»
3. Хорошо применимо, где в компании идеально выстроены процессы;

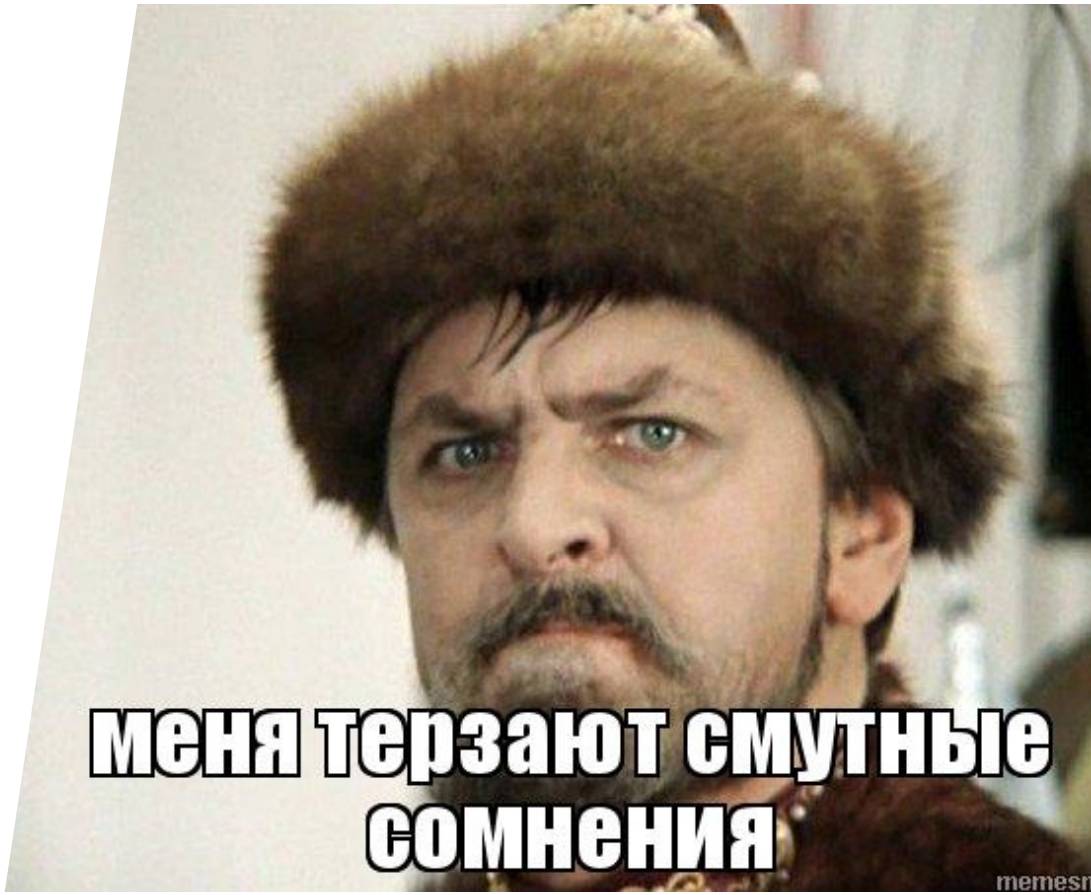
1. В чистом виде сложно предугадать фантазию пользователя;
2. Потенциальный злоумышленник всегда может сказать «сделал по ошибке», будет искать иные пути обхода;
3. Факта утечки – не будет.

Элекснет

Блокировать, нельзя детектировать

1. Легче контролировать все каналы коммуникации;
2. Инциденты – это не только копирование на флешку или оправка на почту;
3. Аудитор всего и вся в любой компании;
4. Идеальный вариант подхода «Показать то, что скрыто»!

1. Дороже с точки зрения часов аналитики;
2. Дороже с точки зрения инфраструктуры и каналов связи;

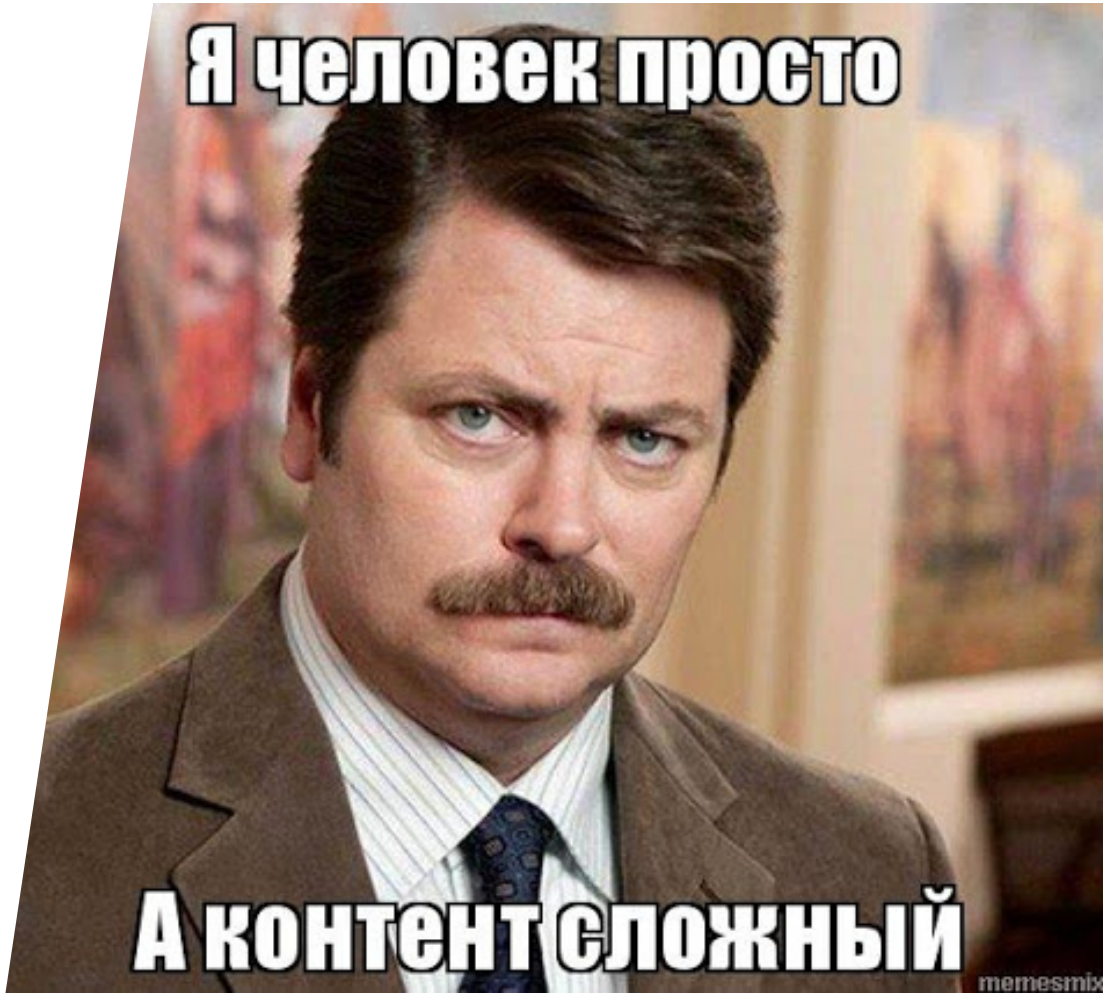


Элекснет

Типовые кейсы

1. Легче контролировать все каналы коммуникации;
2. Инциденты – это не только копирование на флешку или оправка на почту;
3. DLP as DAM$$$ update/insert/select
4. Аудитор всего и вся в любой компании;
5. Идеальный вариант подхода «Показать то, что скрыто»!

1. Дороже с точки зрения часов аналитики;
2. Дороже с точки зрения инфраструктуры и каналов связи;



Элекснет

(НЕ)Типовые кейсы (или почему детект лучше)

Клиенты жалуются, что их данные утекают, но никто не понимает что где и как. А надо всего лишь…

- ✓ аудит доступа к данным;
- ✓ аудит интеграции систем;
- ✓ аудит мест хранения данных;
- ✓ аудит информационных потоков;
- ✓ аудит трафика;

Элекснет

Мы пойдем другим путем

Аудит процесса продажи

Какие системы и как участвуют в этом процессе?

Как пользователи получают доступ в систему?

Как у пользователей забирают доступ к системе?

Что пользователи могут делать в системе?

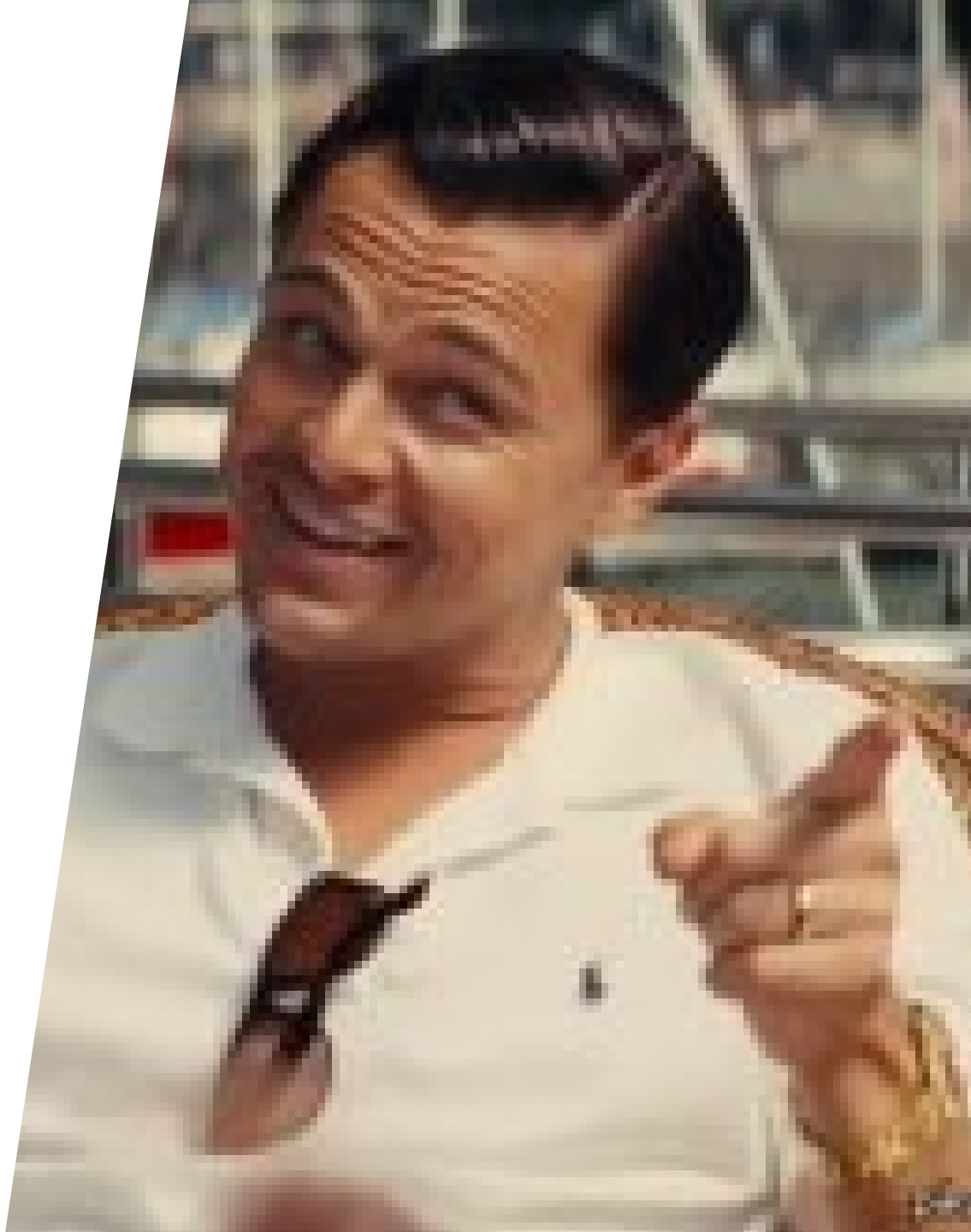
Есть ли логи доступа на стороне системы?

Кто и как получает доступ к данным о сделке?

Элекснет

Business value наше все

- Изменение процесса найма/увольнения сотрудника;
- Изменение CRM контрагента (3-го лица);
- Изменение процесса передачи учетных данных в CRM;
- Изменение договоров на ИТВ между контрагентами;



Элекснет

Спасибо за внимание!

Шубин Иван Александрович

shubinia@elecsnet.ru
Руководитель Службы
информационной безопасности
АО НКО «Элекснет»