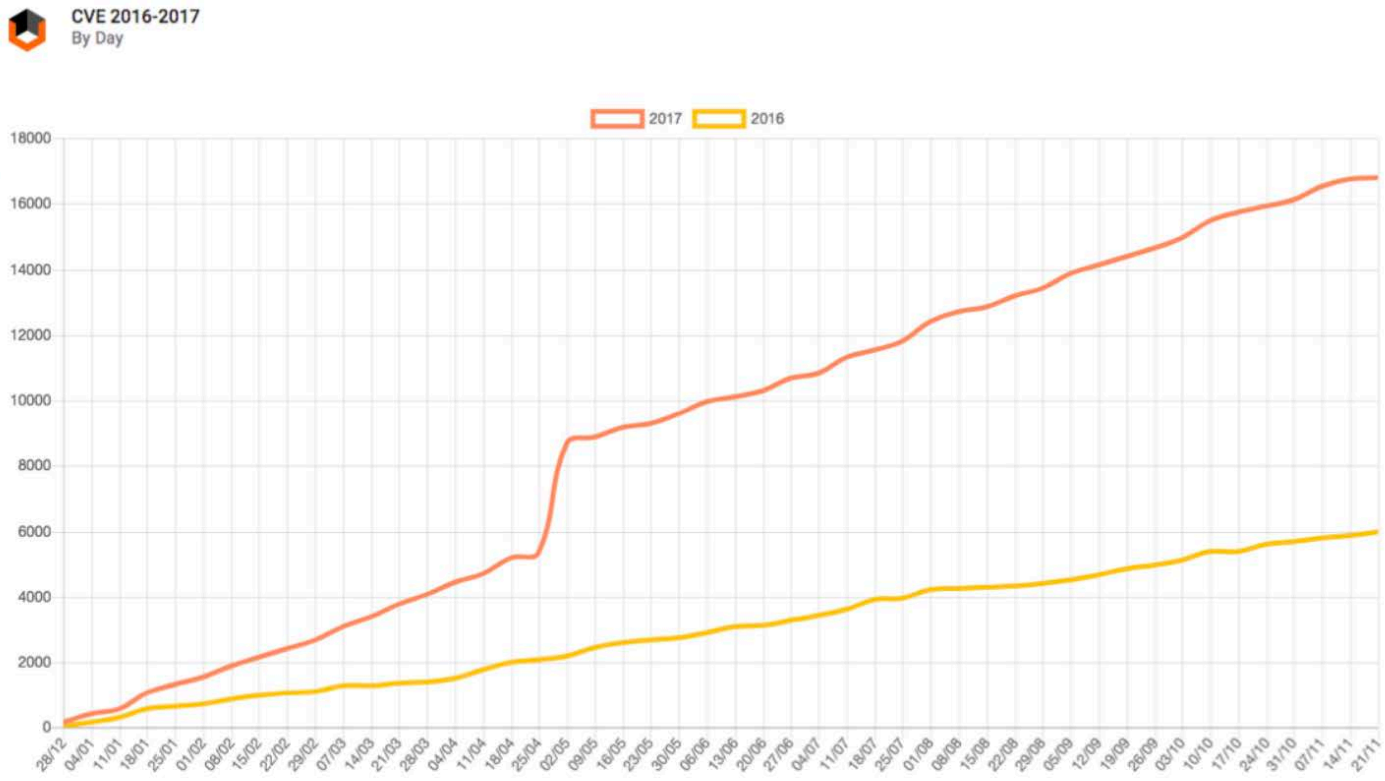
Управление безопасностью

Игорь Булатенко
X Уральский форум

#:whoami

- vulners.com co-founder
- QIWI CISO
- Web penetration tester
- Ex-security developer

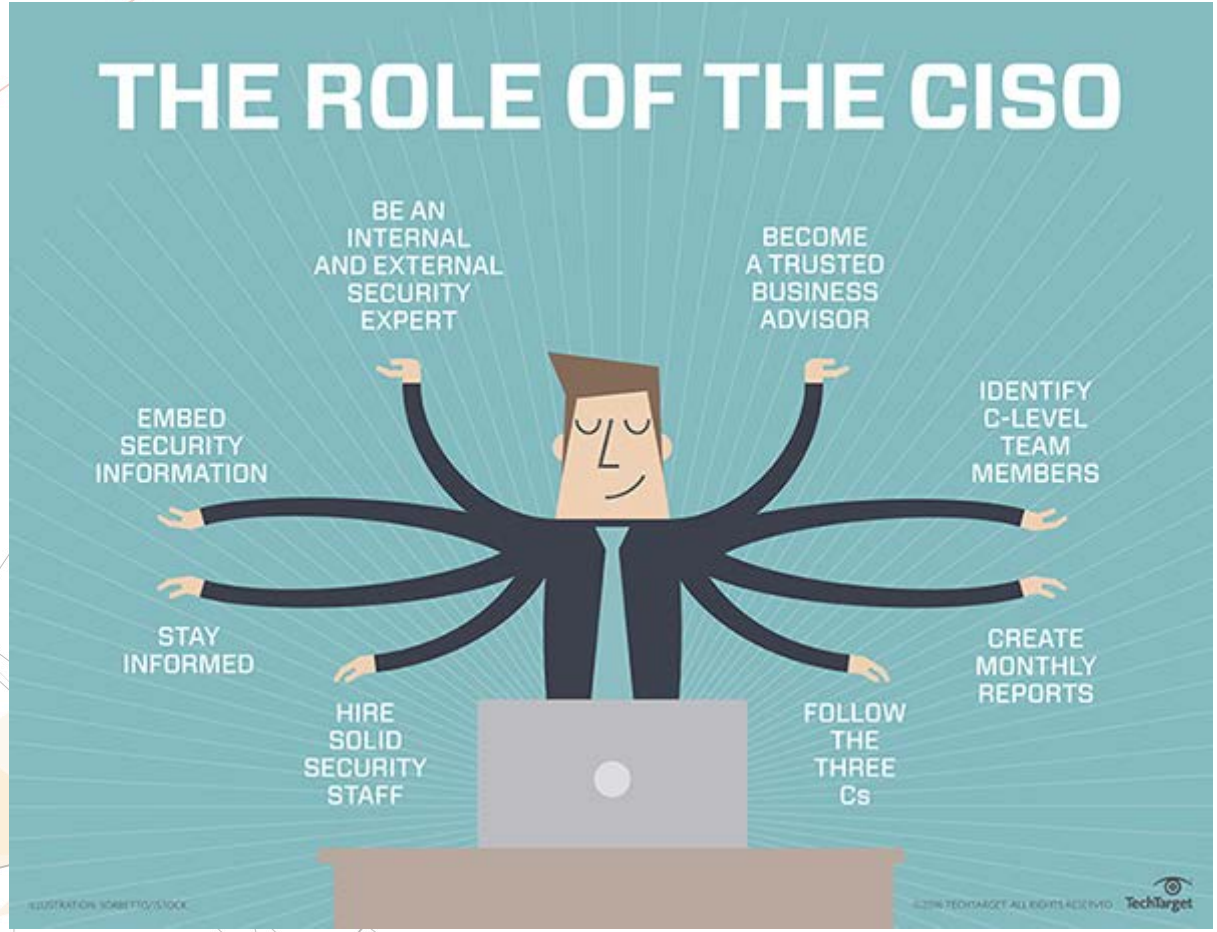
Как страшно жить



Информационная безопасность как функция

- Разработка концепции и политики ИБ
- Классификация активов и оценка защищенности
- Оценка и управление информационными рисками
- Повышение осведомленности в области ИБ
- Обеспечение руководства отчетами

CISO


THE ROLE OF THE CISO
BE AN INTERNAL AND EXTERNAL SECURITY EXPERT
BECOME A TRUSTED BUSINESS ADVISOR
EMBED SECURITY INFORMATION
IDENTIFY C-LEVEL TEAM MEMBERS
STAY INFORMED
CREATE MONTHLY REPORTS
HIRE SOLID SECURITY STAFF
FOLLOW THE THREE Cs
TechTarget

ИБ в СБ

- Нехватка квалификации руководителя
- Проблема коммуникации с людьми
- Преобладание орг. мер
- Конфликт с IT
- Отсутствие влияния на процессы

ИБ в ИТ

- Конфликт интересов
- Исполнители в смежном отделе
- Подчиненное положение

ИБ в роли аудитора

- ИБ проводит самооценку
- ИБ не совещается с ИТ
- ИБ выдает рекомендации
- ИТ не может применить рекомендации

Проблемы

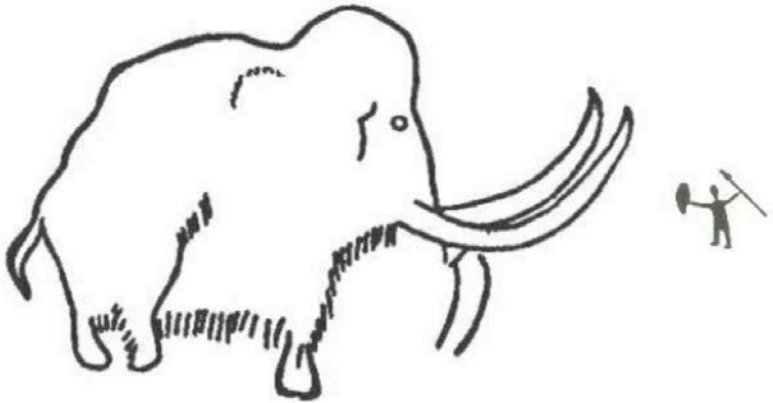
- Отсутствие asset management
- Невозможность внедрения функционала
- Отсутствие доступов или информации
- Вынужденность использовать суррогатные средства
- Отсутствие переиспользования средств
- ИТ не знает о доступном инструментарии

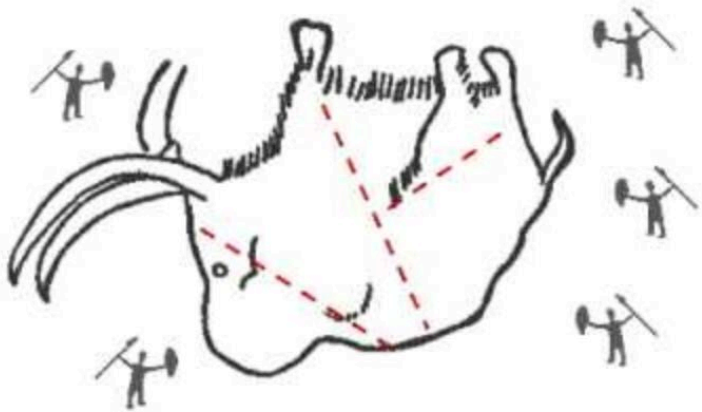
Как следствие проблем

- Низкая эффективность
- Безопасность на низком уровне

Выход есть

Кооперация





ИБ + Windows admins

- Управление уязвимостями и обновлениями
- Установка и обновление агентов
- Переиспользование агентов - EDR, SCCM

ИБ + unix admins

- Автоматизация установки обновлений
- WAF by default
- Общие системы логирования (relk, siem и др.)

ИБ + dba

- Использование DAM
- Триггерная логика при необходимости
- Auth в СУБД

ИБ + internal dev

- Контроль периметра as a service
- Аудит рабочих станций и агентов
- Автоматизированный поиск возможных утечек исходного кода
- Обнаружение новых приложений

Контроль периметра

79.142.	80	2017-11-08 23:52:35	2017-12-07 18:25:46	tcpwrapped
79.142.	443	2017-11-08 23:52:35	2017-12-07 18:25:46	http @ nginx
79.142.	443	2017-11-08 23:52:35	2017-12-07 18:25:44	http @ nginx
79.142	8443	2017-11-08 23:52:35	2017-12-07 18:25:45	http @ nginx
79.142.	8443	2017-11-08 23:52:34	2017-12-07 18:25:45	http @ nginx
79.142.	443	2017-11-08 23:52:34	2017-12-07 18:25:44	http @ nginx
79.142	80	2017-11-08 23:52:34	2017-12-07 18:25:44	tcpwrapped
79.142	80	2017-11-08 23:52:33	2017-12-07 18:25:45	tcpwrapped
79.142	443	2017-11-08 23:52:33	2017-12-07 18:25:44	http @ nginx
79.142.	443	2017-11-08 23:52:33	2017-12-07 18:25:46	http @ nginx
79.142	80	2017-11-08 23:52:33	2017-12-07 18:25:44	tcpwrapped

Как это получилось

- Доверие через компетенции
- Сеансы «черной магии»
- Вместе ищем лучшее решение
- «Заразить» безопасностью