kaspersky

Kaspersky Industrial Cybersecurity Conference 2020

Алексей Лукацкий

Бизнес-консультант по безопасности, Cisco

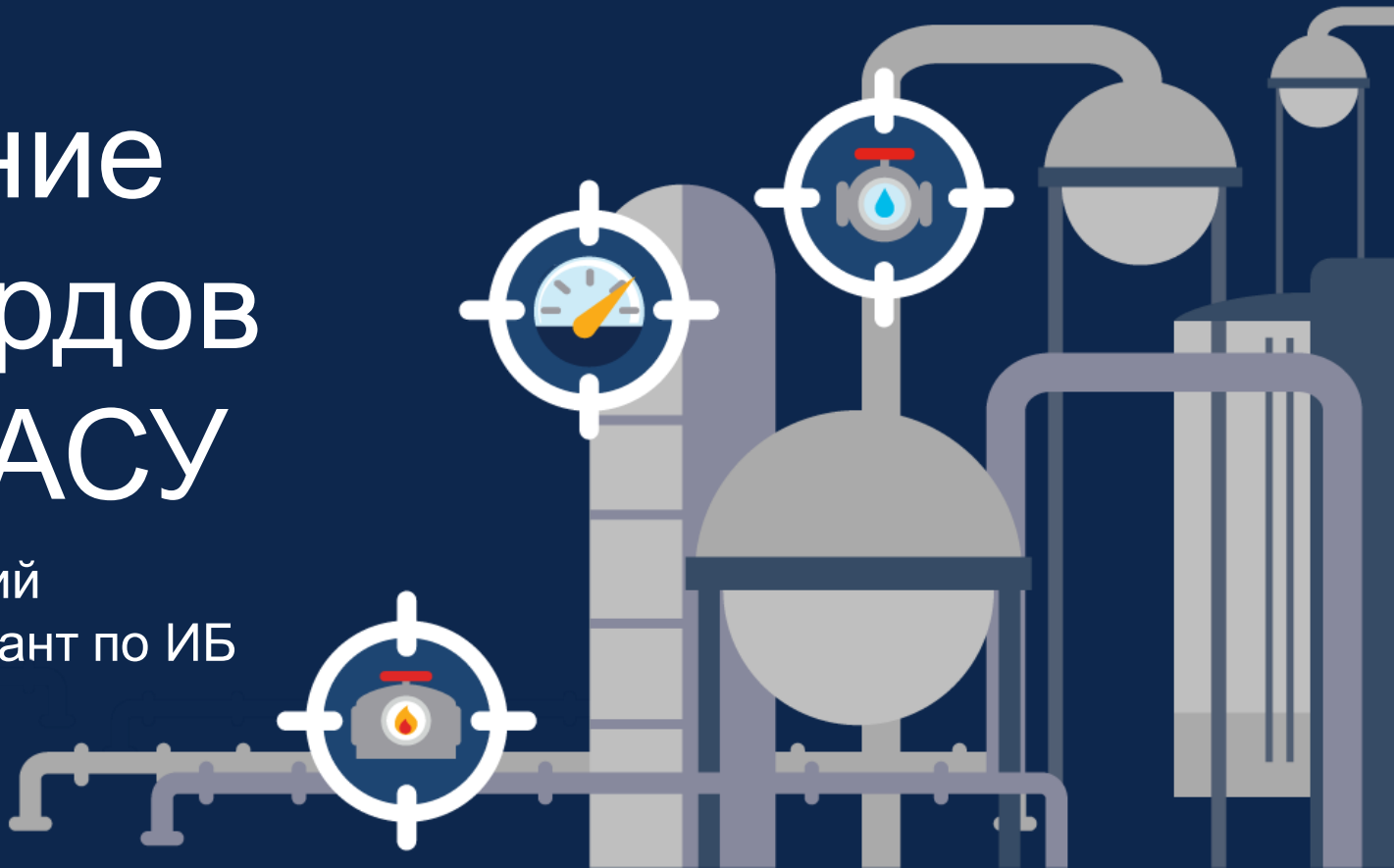
#KasperskyICS

Чат конференции: https://kas.pr/kicscon

cisco Secure

Создание дашбордов по ИБ АСУ ТП

Алексей Лукацкий
Бизнес-консультант по ИБ

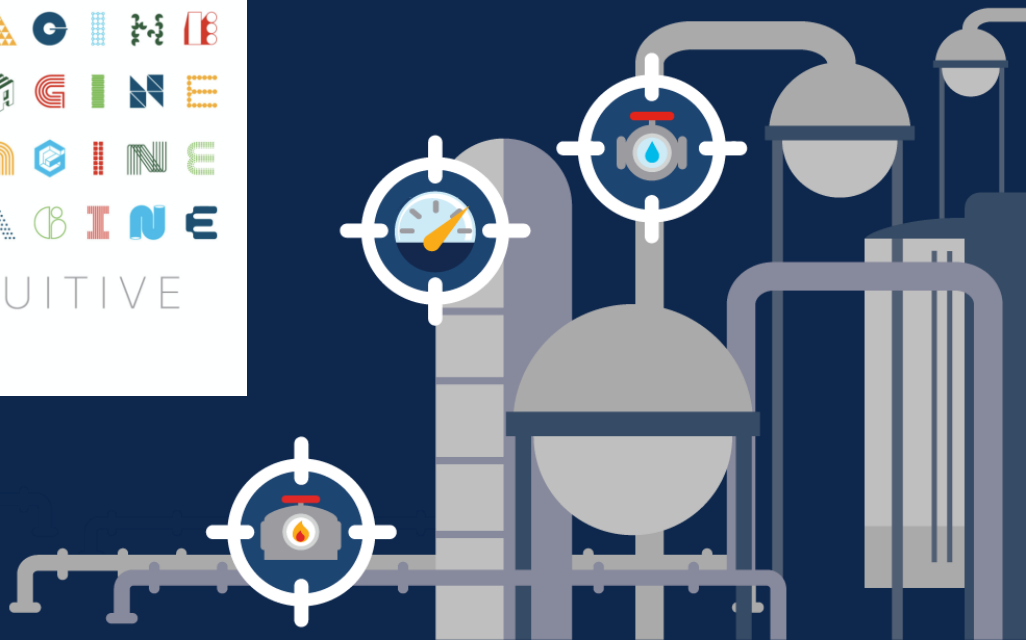


Я продолжаю прошлогоднее выступление ☺

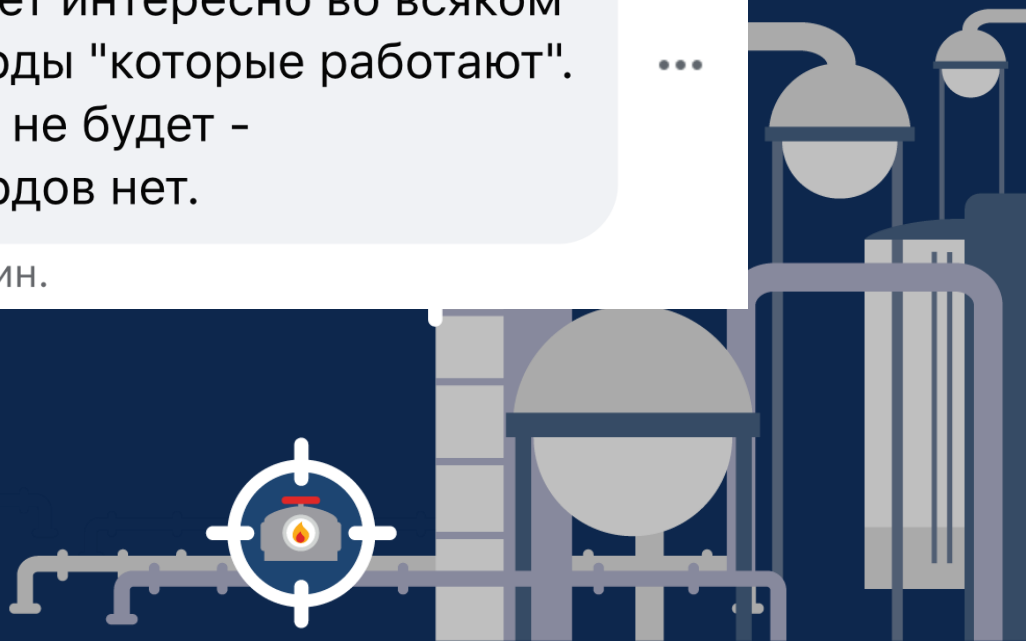
cisco

Измерение эффективности ИБ промышленных систем

Лукацкий Алексей, бизнес-консультант по ИБ



Универсальных дашбордов нет!



Как же нет?..

Tenable

CyberX

Splunk for OT

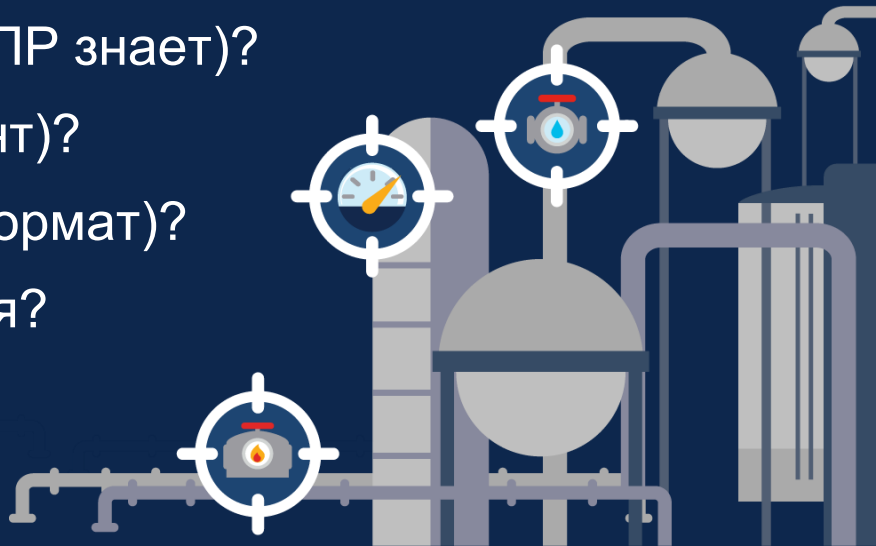
Cisco Cyber Vision

Что вам позволит сделать хороший дашборд?

- Для кого дашборд?
- Цель дашборда (что должна сделать ЦА)?
- Формат
- Дедлайн
- Технические ограничения
- Знание принципов визуализации

Надо отталкиваться от целевой аудитории

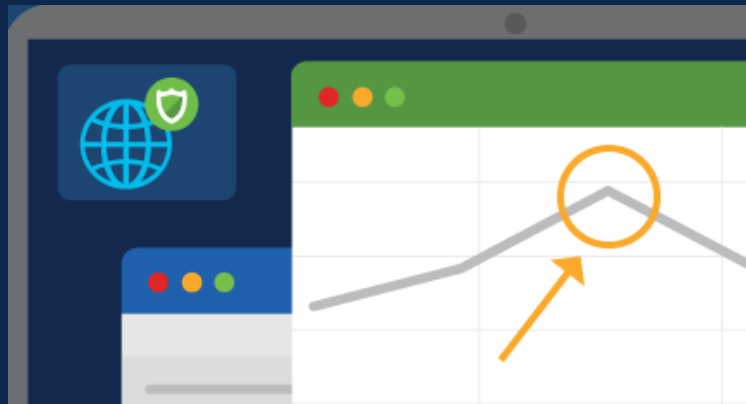
1. Кто ваш ЛПР?
2. Топ3 потребностей ЛПР
3. Что должен сделать ЛПР после просмотра дашборда?
4. Уровень погружения в тему (что ЛПР знает)?
5. Что для ЛПР самое главное (акцент)?
6. Как ЛПР будет на это смотреть (формат)?
7. Как до этого принимались решения?



А какая у вас цель (что должен сделать ЛПР)?

- Получить денег на ИБ АСУ ТП
- Получить людей для ИБ АСУ ТП
- Выбить денег на обучение персонала
- Получить полномочия
- Получить одобрение начальства
- Получить одобрение на действия
- Выдрать технологов за «саботаж» ИБ

Просто показать число инцидентов – это не цель!



Подробный чеклист: анализ целевой аудитории

Какой уровень знаний?

- Она понимает о чем речь?
- Это первый контакт?
- Необходимы пояснения?
- Какая конкретика нужна?

Какие интересы?

- Какие KPI у нее сейчас?
- Какими временными промежутками меряет?
- Насколько ей нужна техника?

Какая лояльность?

- Отношение к вам?
- Вас будут слушать?
- Нужны доказательства?
- Готовиться к каверзным вопросам?

Какой формат?

- Удаленка или очно?
- Лично или без вас?
- Интерактив нужен или печатный отчет?
- Рассылка по почте?

Сколько времени?

- Сколько времени на подготовку?
- Сколько времени на представление?
- Когда/как часто будут использоваться?

Что вам надо от нее?

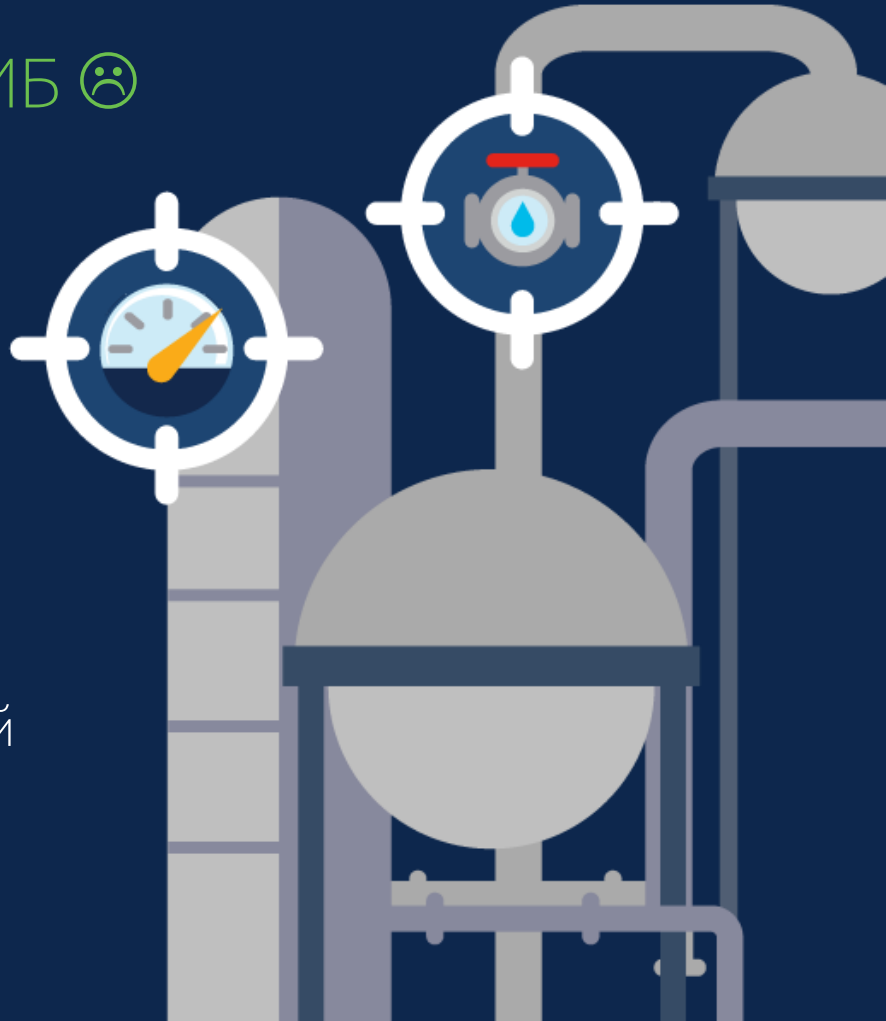
- Деньги
- Время
- Полномочия
- Внимание
- Обожание

Принцип ноля кликов

- Самый главный признак отличного дашборда — это ноль кликов
- Не заходить, а видеть!
- Информация должна быть доступна на кончиках пальцев, в уголке глаза, в строке меню, на обоях рабочего стола, на заблокированном экране телефона и т.д.
- Как ваш ЛПР смотрит KPI?

ЛПР не нужны дашборды по ИБ ☹

- Вы уверены, что руководство будет постоянно смотреть на дашборд по ИБ (хорошо, если раз в месяц)?
- Исключая CISO, для большинства руководителей ИБ не входит в Топ3 интересов
- Можно рассчитывать только на свой виджет в чужом/общем дашборде (если повезет)




Report
Shift

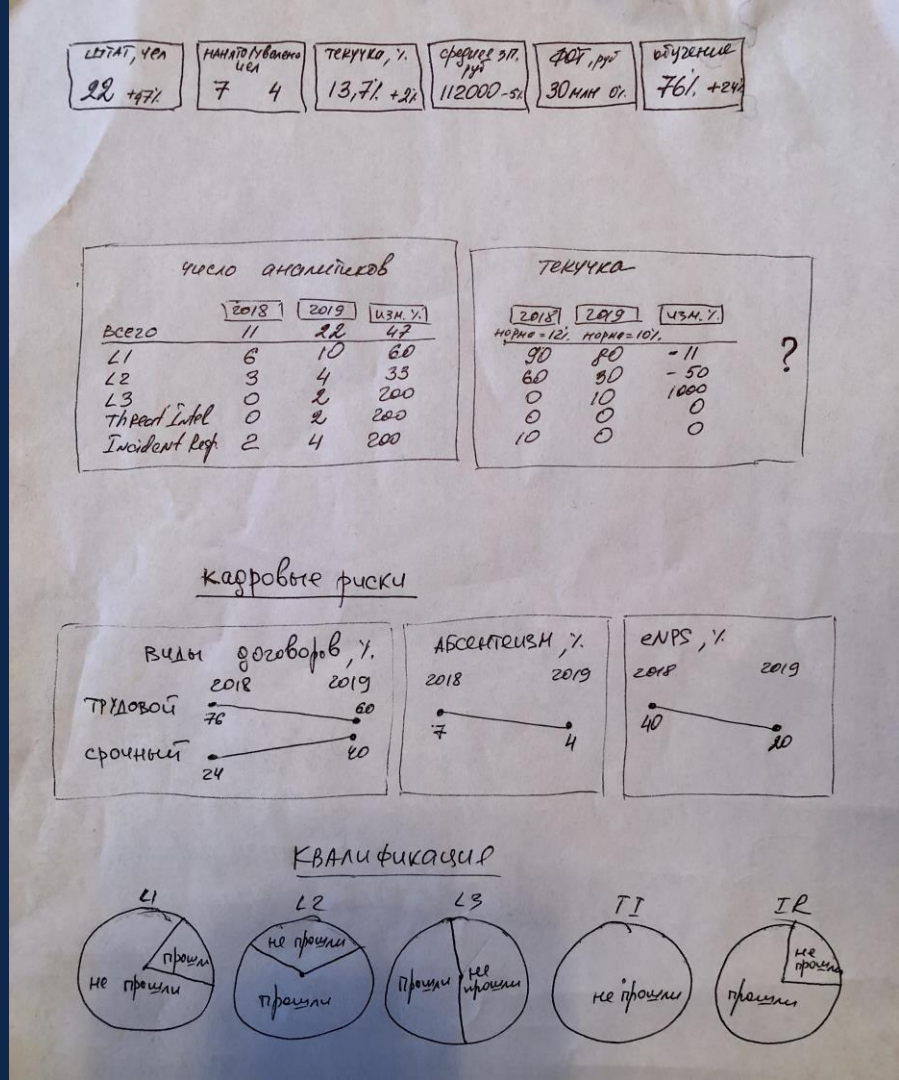
Не только дашборд

Дашборд	• Визуальное представление наиболее важной информации, сгруппированной по смыслу на одном **интерактивном** экране так, чтобы ее было легко понять
Отчет	• Документ, визуально представляющий наиболее важную информацию, сгруппированную по смыслу так, чтобы ее было легко понять **(нет интерактива)**
Слайдумент	• Документ из серии слайдов, в котором лаконично представлен большой объем данных. Не для выступлений. Этот формат используется для передачи смысла будущего выступления без присутствия докладчика

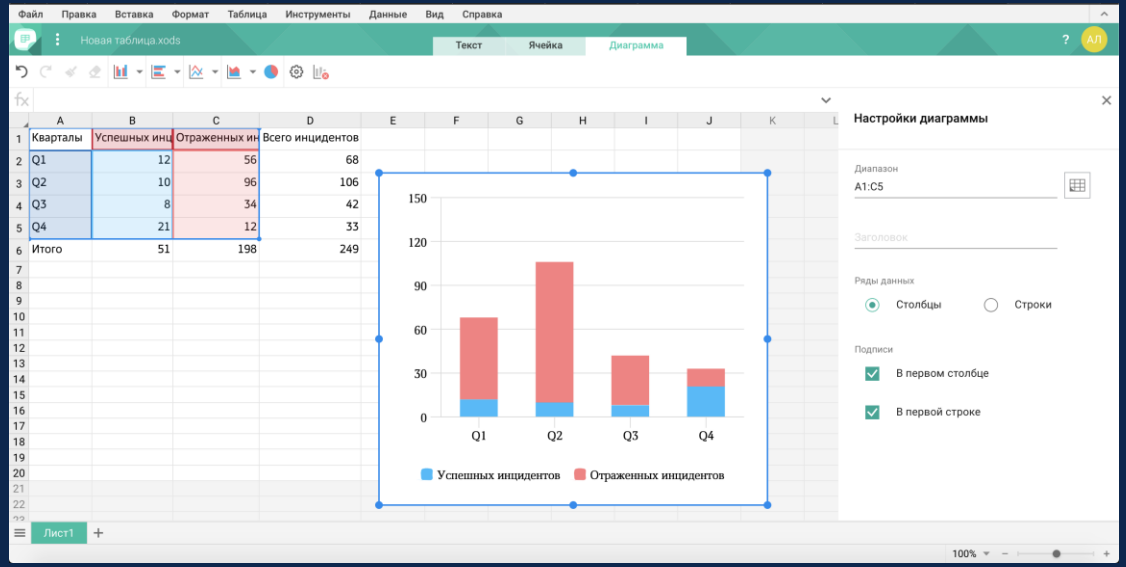
Единые принципы визуализации

Инструмент не так важен

- ~~Мой офис~~
- Excel
- Google.Sheets
- PowerBI
- Qlik Sense
- Tableu
- QlikView
- KIbana
- Grafana
- Splunk
- …



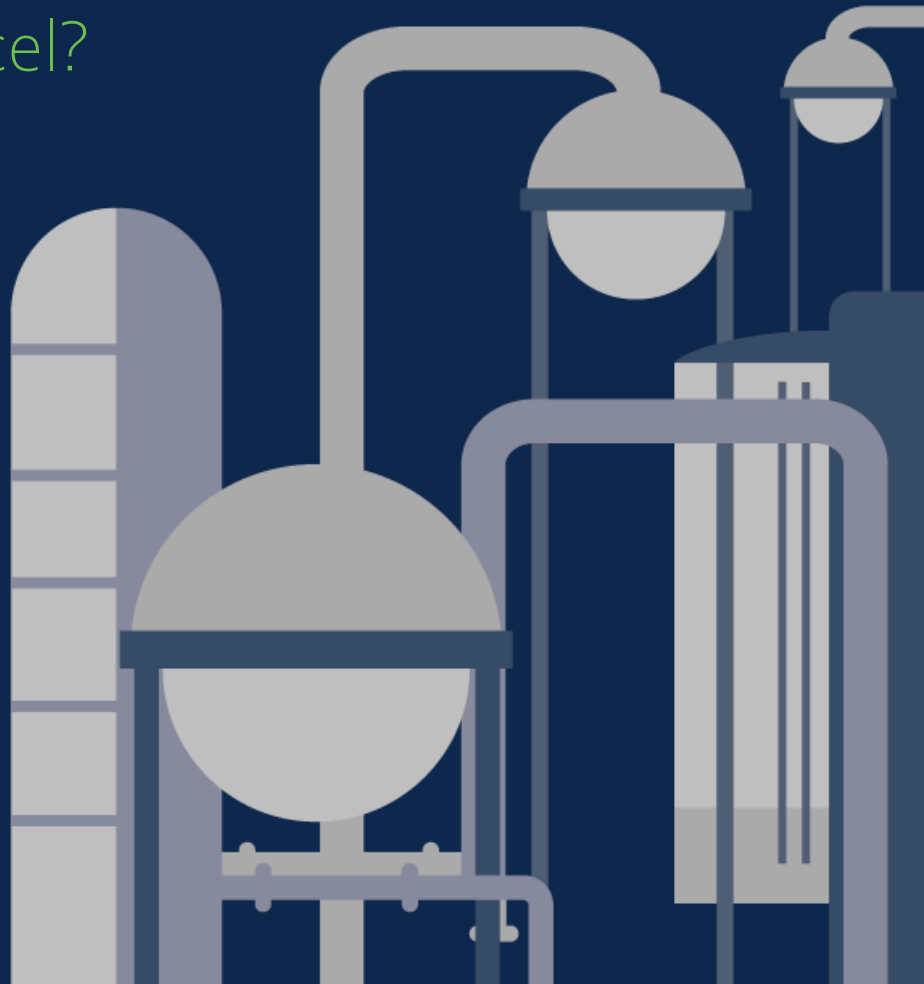
А почему не «Мой офис»?



Практически полное отсутствие возможностей по созданию и настройке визуализации

Почему стоит начинать с Excel?

- Есть у всех
- Привычен для ЛПР (именно для них, а не для ИБшников)
- Позволяет делать дашборды (через срезы/slice),
  а также отчеты и готовить данные для слайдументов
- Дешев



Лайфхак: сервисы дашбордов vs Plash

- Сервисы дашбордов развиваются в сторону расширения числа визуализаций, вычислений… но внутри своего приложения или сайта
- Динамические обои на десктопе
- Отображение портала, сайта, канала фидов, html-страницы
- https://sindresorhus.com/plash

Основные типы дашбордов / отчетов

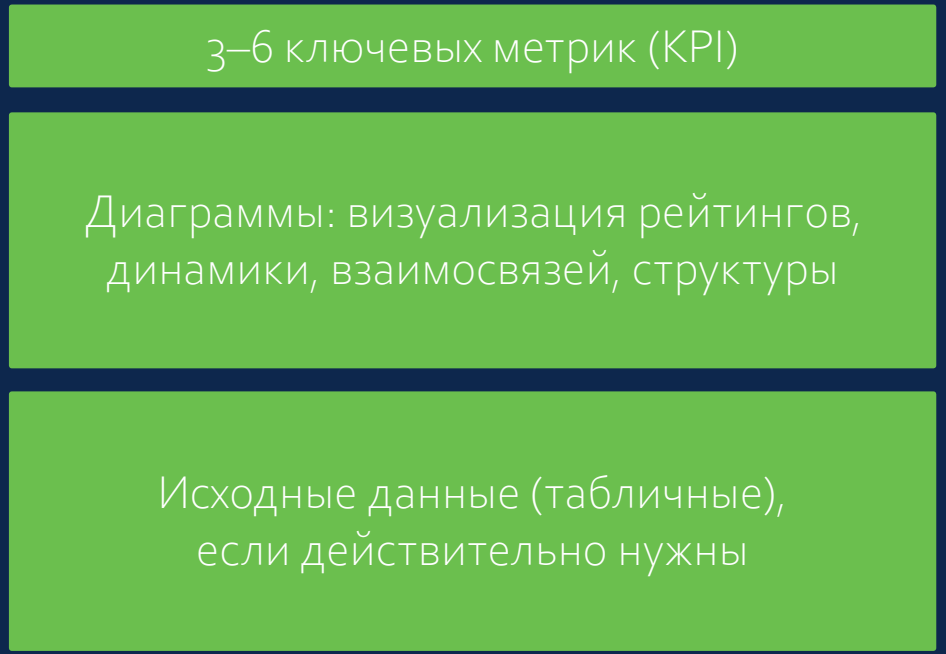
Для топ-менеджмента

Для руководителей среднего звена

Для исполнителей

Структура правильного дашборда

- Обычно мы начинаем с исходных данных, разбираем/анализируем их и делаем выводы
- В дашбордах все наоборот – сначала выводы и KPI, потом аналитика и, может быть, исходные данные (если понадобятся)



Разница в восприятии топ-менеджмента и аналитика

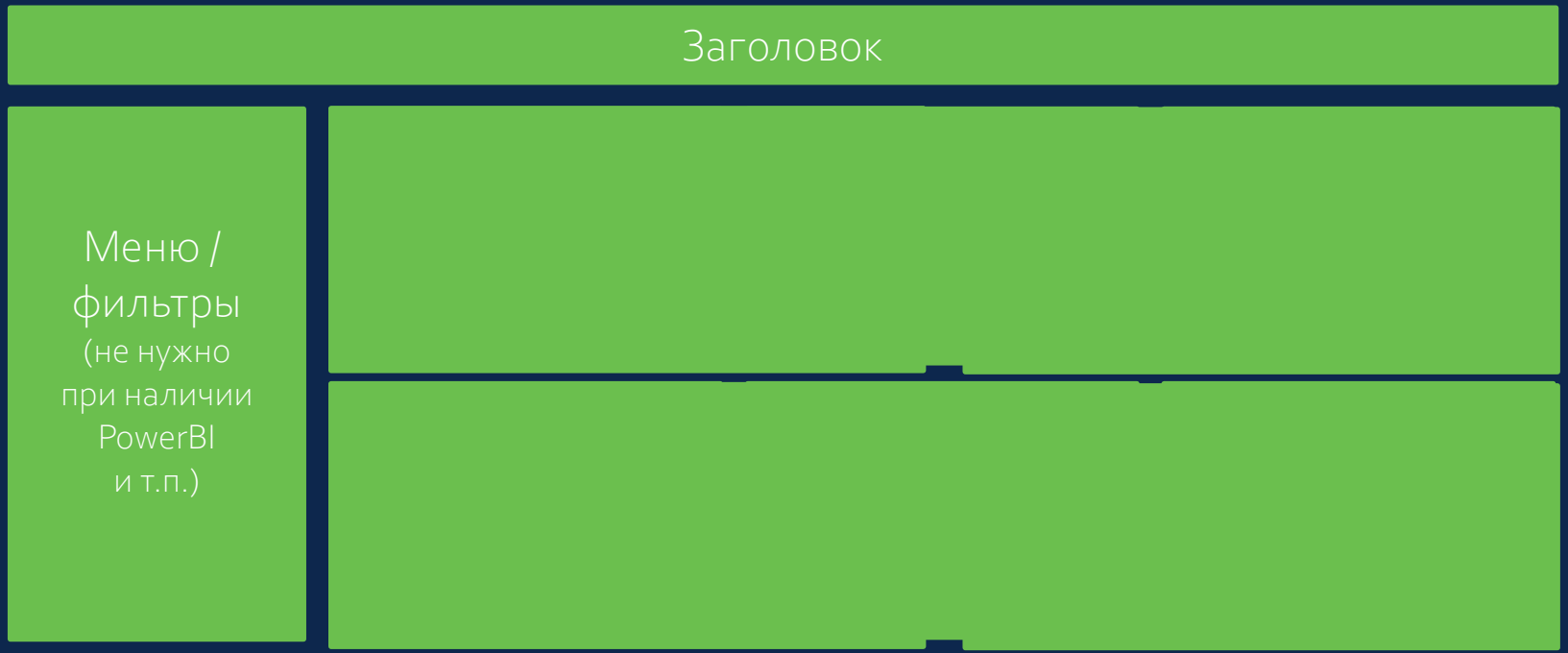
Специалист по ИБ

- Погружение в детали
- Нежелание расстаться с собранными данными
- Данные ради данных
- Что? Где? Когда?

Топ-менеджмент

- Нужна общая картина
- Данные для принятия решения
- Что будет? Что делать?

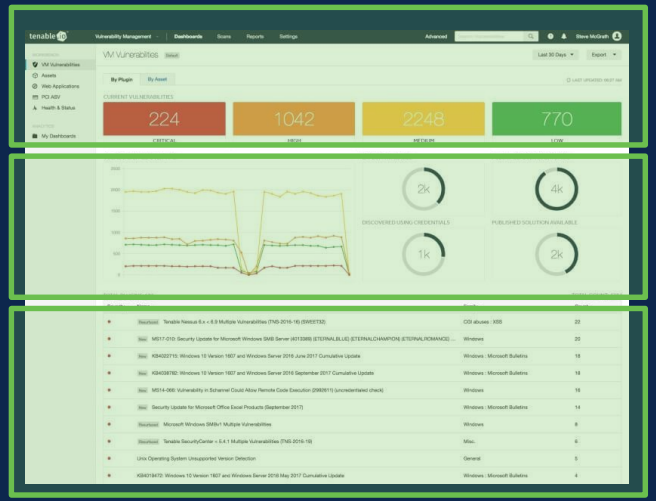
Правило сетки дашбордов – 2 x 2 или 2 x 3



Симметрия! Нет симметрии ⇒ страдает логика

Примеры структуры дашбордов

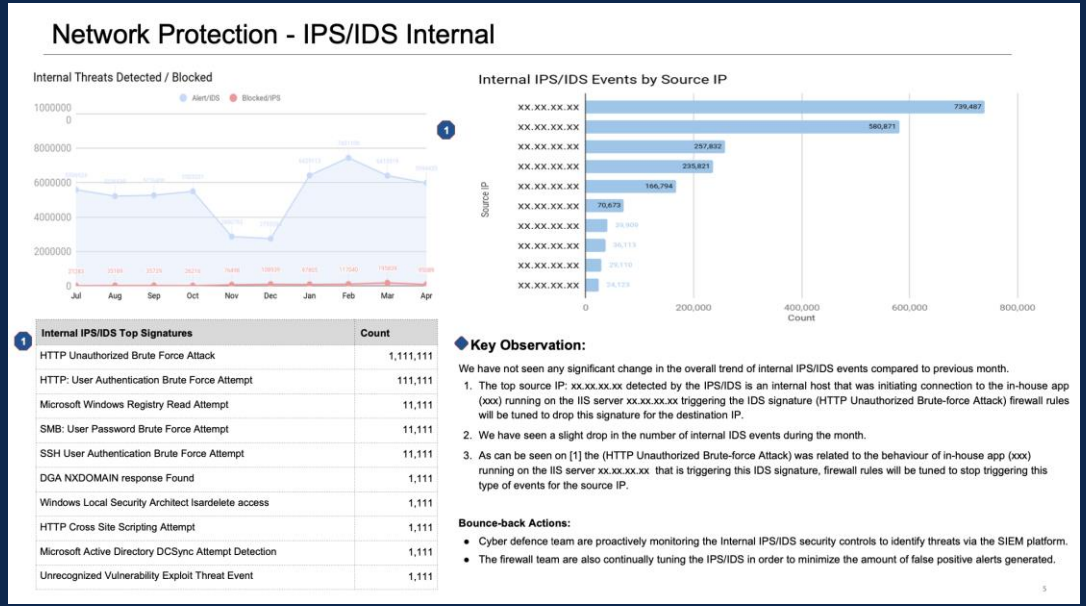
Cisco SecureX



Tenable

Удачный пример?

- Обнаруженные / заблокированные угрозы
- Топ сигнатур атак
- Внутренние источники атак
- Ключевые наблюдения



Network Protection - IPS/IDS Internal

Internal Threats Detected / Blocked

Internal IPS/IDS Events by Source IP

Internal IPS/IDS Top Signatures	Count
HTTP Unauthorized Brute Force Attack	1,111,111
HTTP: User Authentication Brute Force Attempt	111,111
Microsoft Windows Registry Read Attempt	11,111
SMB: User Password Brute Force Attempt	11,111
SSH User Authentication Brute Force Attempt	11,111
DGA NXDOMAIN response Found	1,111
Windows Local Security Architect Isardelete access	1,111
HTTP Cross Site Scripting Attempt	1,111
Microsoft Active Directory DCSync Attempt Detection	1,111
Unrecognized Vulnerability Exploit Threat Event	1,111

Key Observation:

We have not seen any significant change in the overall trend of internal IPS/IDS events compared to previous month.

1. The top source IP: xx.xx.xx.xx detected by the IPS/IDS is an internal host that was initiating connection to the in-house app (xxx) running on the IIS server xx.xx.xx.xx triggering the IDS signature (HTTP Unauthorized Brute-force Attack) firewall rules will be tuned to drop this signature for the destination IP.
2. We have seen a slight drop in the number of internal IDS events during the month.
3. As can be seen on [1] the (HTTP Unauthorized Brute-force Attack) was related to the behaviour of in-house app (xxx) running on the IIS server xx.xx.xx.xx that is triggering this IDS signature, firewall rules will be tuned to stop triggering this type of events for the source IP.

Bounce-back Actions:

- Cyber defence team are proactively monitoring the Internal IPS/IDS security controls to identify threats via the SIEM platform.
- The firewall team are also continually tuning the IPS/IDS in order to minimize the amount of false positive alerts generated.

Удачный пример?

- Рейтинг видимости компании в Darknet / Deep Web
- Число утекших учетных записей в публичных утечках и в Darknet / Deep Web
- Динамика утекания учетных записей в Darknet / Deep Web
- Число упоминаний компании в Darknet / Deep Web

Organization
DARKINT™ Footprint August 2017

DARKOWL™

DARKINT™ Score

6.14

An organization's DARKINT™ score involves assessing how much data is available on the darknet that can be misused by hackers or criminals. A greater availability of data implies a higher risk profile, as more attack vectors are available. This is a point-in-time snapshot for August 2017.

DARKINT Threats Detected

Credentials Exposed: @organization.com

455	120	87	368
DETECTED	DARKNET	DEEP WEB	DATA LEAKS

Company + Domain Mentions: Organization, Organization.com

1078	522	317	239
DETECTED	DARKNET	DEEP WEB	SURFACE

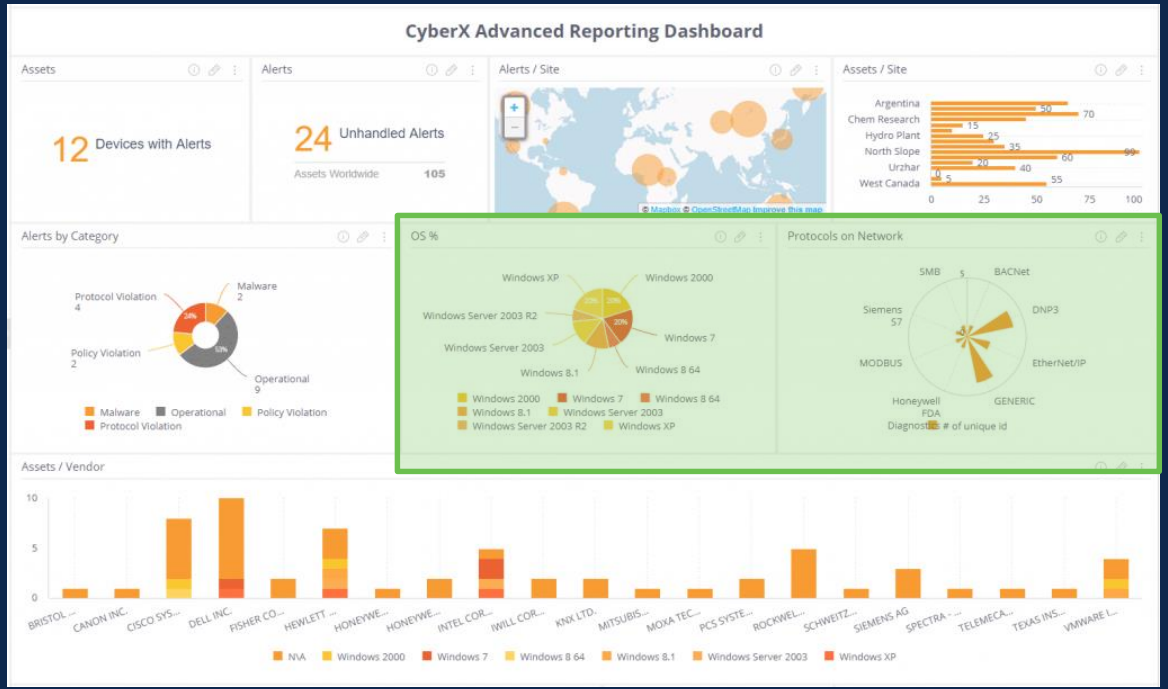
About DARKINT Content

Intelligence gained from monitoring the darknets (Tor and other interconnected sources including IRC, I2P, and other forums), as well as FTP servers, paste sites, high-risk surface internet sites and more, constitutes what DarkOwl calls DARKINT™, or darknet intelligence. A high volume of criminal activity has migrated to these locations, attracting threat actors seeking to sell, purchase, or expose data.

DARKINT™ Footprint Report | DarkOwl | 303.376.6265 | www.DarkOwl.com

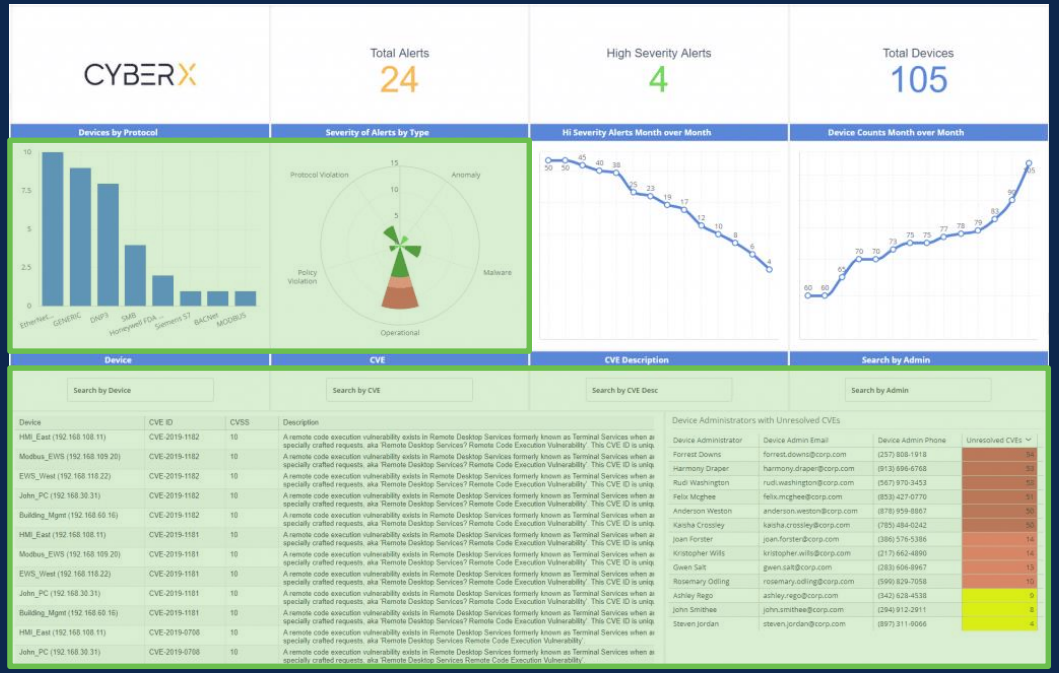
Удачный пример?

- Сигналы тревоги для каждой площадки
- Типы сигналов тревоги
- Ландшафт промышленных активов



Удачный пример?

- Динамика критичных уязвимостей
- Динамика числа устройств
- Информация по CVE
- Виновники неустранения CVE



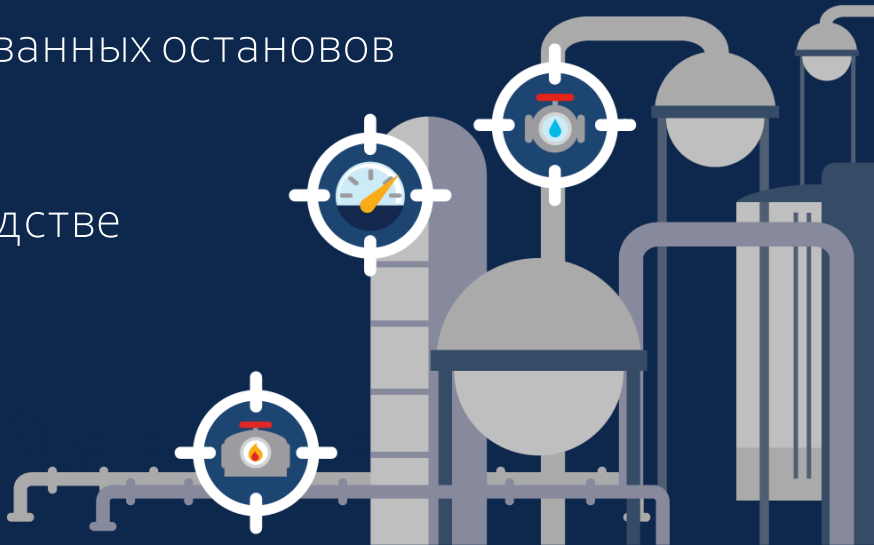
Наполнение дашборда промышленного SOC

Ключевые показатели	Число инцидентов	Число просроченных инцидентов, %	Среднее время разбора инцидента, в часах	Число аналитиков SOC
Аналитические показатели	Динамика инцидентов	Распределение инцидентов по типам	Распределение инцидентов по источникам	Трудозатраты по аналитикам

Хороший пример дашборда для промышленного SOC, но что он дает для ЛПР?

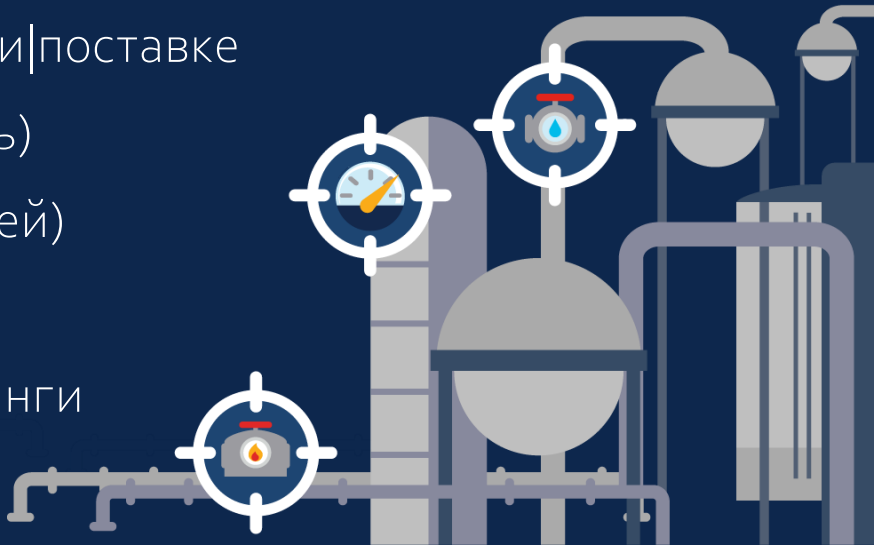
А что сейчас измеряет ваш ЛПР?
Производство

1. Общее объем|число выпущенной продукции
2. Объем|число дефектной|хорошей продукции
3. Объем|число заказов, выпущенных|доставленных в срок
4. Число запланированных|незапланированных остановов
5. Замедление цикла производства
6. Число инцидентов|аварий на производстве
7. Производительность оборудования
8. Доступность оборудования



А что сейчас измеряет ваш ЛПР?
Электроэнергетика

1. SAIDI (длительность прерываний)
2. SAIFI (число прерываний)
3. Число клиентов, передающих показания со счетчиков
4. Потери электроэнергии при генерации|поставке
5. ASAI|ASUI (доступность|недоступность)
6. CAIFI (число отключенных потребителей)
7. Точность выставления счетов
8. Число сотрудников, прошедших тренинги



Наполнение дашборда «Инциденты в АСУ ТП»

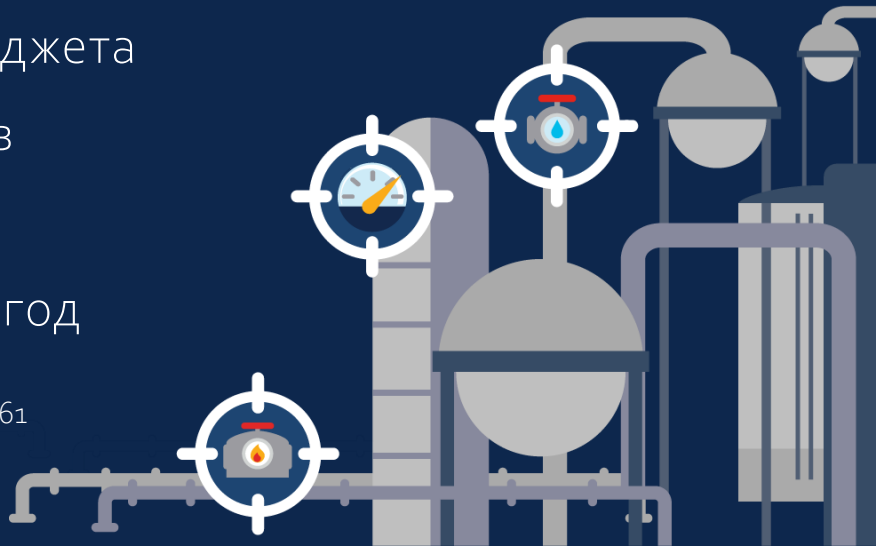
Ключевые показатели	Число инцидентов с АСУ ТП	Время простоя от инцидентов	Ущерб по контрактным обязательствам
Аналитические показатели	Динамика инцидентов (по площадкам, по времени…)	Количество инцидентов по источникам	

В качестве ключевых показателей также могут быть указаны число пострадавших (люди/организации), уровень деградации процесса и т.п.

А что сейчас измеряет ваш ЛПР?
Водоснабжение (помимо предыдущих KPI)

1. Сумма штрафов за нарушение законодательства
2. Число инцидентов, связанных с утечками ПДн и данных клиентов
3. % организаций, интегрирующих ERM в процессы управления
4. % проектов, завершенных в рамках бюджета
5. % отклонений от расписания проектов
6. Среднее время простоя вакансии
7. Длительность обучения сотрудника в год

Ссылка: https://sfwater.org/modules/showdocument.aspx?documentid=861



Наполнение дашборда «Регуляторика»

Ключевые показатели	% выполнения НПА по КИИ (АСУ ТП)	Число проверок / запросов регуляторов	Число известных административных и уголовных дел по КИИ
Аналитические показатели	Динамика штрафов за несоблюдение (число и суммы) по КИИ	Динамика выданных предписаний	Динамика административных и уголовных дел по КИИ
	Рекомендации или первоочередные/планируемые шаги по приведению в соответствие		

Дашборды могут содержать живые примеры, мнения и комментарии

Наполнение дашборда «КИИ»

Ключевые показатели

- Число объектов КИИ
- Число значимых объектов КИИ
- Инвестиции на защиту одного ЗОКИИ в среднем
- Нехватка персонала

Аналитические показатели

- Распределение объектов КИИ по площадкам
- Площадки-лидеры по категорированию
- Уровень реализации защитных мероприятий

Препятствия для категорирования
«Отказники» от категорирования
Предложения по экономии

Управление учетными записями администраторов промышленных систем

Ключевые показатели

Повышение осведомленности пользователей

Обучение персонала с целью снижения числа инцидентов – одна из задач безопасности, в том числе и информационной

Ключевые показатели	Число сотрудников, прошедших тренинг	Средняя стоимость инцидента	Число инцидентов
Аналитические показатели	Динамика числа сотрудников, прошедших тренинги	Число сотрудников, непрошедших тренинги	Динамика инцидентов	Динамика потерь от инцидентов

Разумеется, если у ЛПР есть такой KPI

Пример дашборда для ЛПР

Financial/Stewardship

Q4 % Product Development Budget Allocated to Security

Target 5% ✓
Trend ➔

5%

- Increased support for legal as they piloted their case management system

Q4 & YTD Security Budget Allocation

	Q1	Q2	Q3	Q4	YTD
Products	$575,000	$597,000	$425,000	$732,000	
Services	$1,590,000	$1,320,000	$1,190,000	$1,090,000	
Training	$326,000	$315,000	$427,000	$301,000	
Actuals	$2,491,000	$2,232,000	$2,042,000	$2,123,000	
Budget	$2,190,000	$2,211,900	$2,234,019	$2,256,359	
$ Variance	-$301,000	-$20,100	$192,019	$133,359	

Customer / Stakeholder

Q4 % of Products Delivered On Time and On Budget

Target 95% ✓
Trend ↑

95%

- 18% increase over Q3 in on-time and on budget delivery. Security staffed temporary PMO team to meet goal

Customer Satisfaction

Target 90% ✗
Trend ↑

85%

- 8% increase over Q3 in customer satisfaction rating of 4 or higher out of 5 possible

Internal Business Process

Q4 % of Developers Training in Secure Coding Principles

Target 95% ✓
Trend ↑

97%

- 100% of flagship application developers completed training reducing overall risk to organization

Q4 % of Developers Attaining Certification

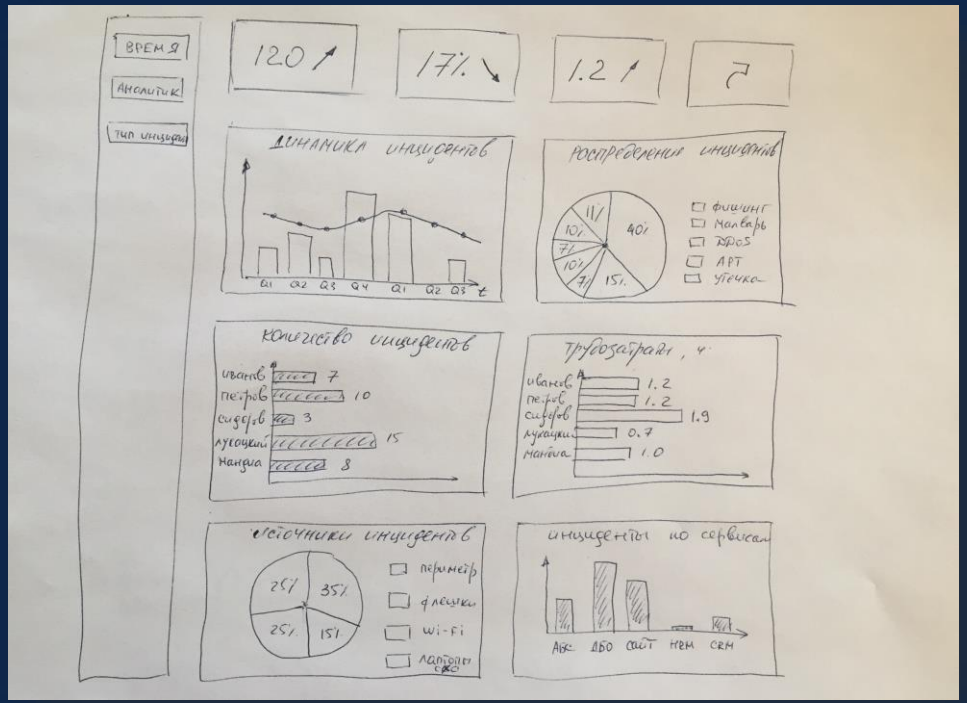
Target 95% ✗
Trend ↑

42%

- Mitigation plan: Follow-up with developers after training is complete for certification

Не бойтесь рисовать

- Отрисовка макета позволяет «увидеть» то, как будет выглядеть ваш дашборд
- Занимает минут 10-15
- Не надо быть Пикассо или Верещагиным



Приоритет должен быть отдан тому, ЧТО показывать, а не КАК!

Рейтинг

- Это самый распространенный вариант анализа, который позволяет сравнивать данные по принципу больше/меньше. Число незакрытых или просроченных инцидентов, число непропатченных ПК, размер ущерба, число IoC, обработанные заявки на доступ и т.п.
- Демонстрировать данный анализ позволяют линейчатые диаграммы и

Динамика

- Это вид анализа, который обычно демонстрируется графиком или гистограммой, показывает тренд, сезонность, изменение во времени суток и т.п.

Структура

- Этот вид анализа показывает часть, долю целого. Например, распределение затрат на ИБ, распределение инцидентов по типам или источникам, соотношение закрытых и просроченных инцидентов и т.п.
- Единственным способом отобразить данный вид анализа позволяет круговая диаграмма.

Взаимосвязи

- Это гораздо более редкий, но все-таки важный вид анализа, который помогает показать наличие или отсутствие (а иногда и характер) взаимосвязей между несколькими показателями.

Правило Паретто при выборе диаграмм

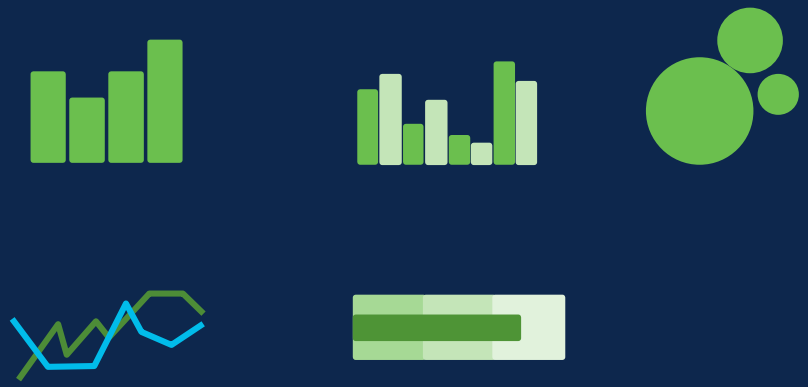
	Линия	Столбец	Круг
Рейтинг Больше/меньше			
Динамика Время			
Структура Доли			

80% всех диаграмм – это всего три типа

Задача: показать динамику

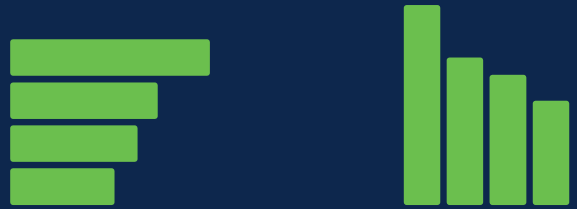
- Хронология инцидента в АСУ ТП
- Динамика уязвимостей в АСУ ТП
- Изменение уровня соответствия стандарту IEC 62443 / приказу 239
- Расходы на ИБ АСУ ТП

Задача: сравнить категории



- Число сотрудников ИБ по подразделениям / площадкам
- Инциденты в АСУ ТП по последствиям
- Распределение инцидентов разного типа по времени реагирования

Задача: ранжировать / посчитать рейтинги

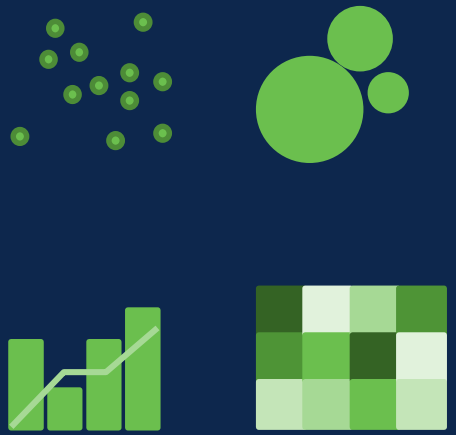


- Производительность аналитиков промышленного SOC
- Рейтинг эффективности средств защиты АСУ ТП
- Уровень культуры ИБ на площадках АСУ ТП

Задача: показать доли

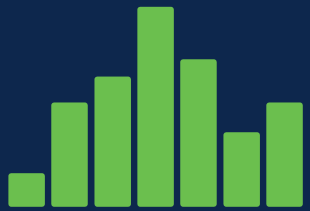
- Доли инцидентов разного типа
- Распределение времени аналитика промышленного SOC в течение дня
- Бюджет на ИБ АСУ ТП
- Структура службы ИБ АСУ ТП
- Структура use case / playbook
- Наиболее уязвимые / атакуемые площадки

Задача: показать корреляцию



- Зависимость времени реагирования на инциденты АСУ ТП от времени суток
- Удаленный доступ на промышленную площадку из разных местоположений

Задача: показать распределение

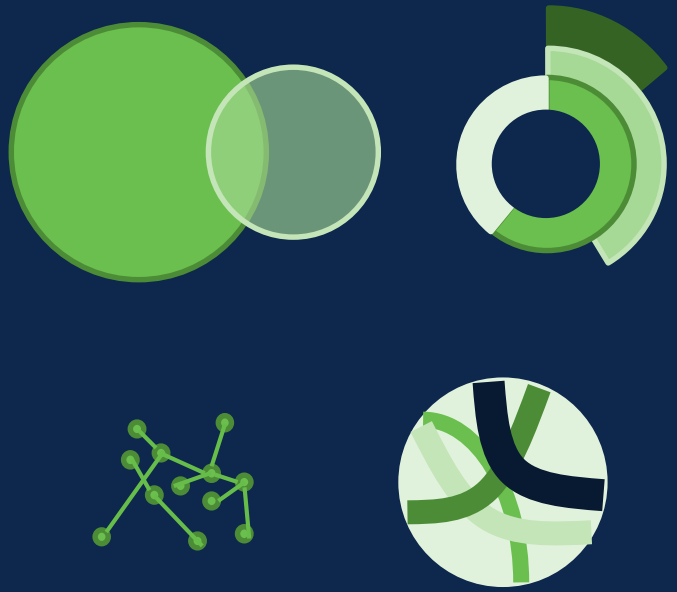


- Зарплаты в разных отделах службы ИБ АСУ ТП (если они есть)
- Зарплатные запросы/вилки в разных регионах
- Нарушители по возрастам / подразделениям / площадкам
- Моделирование угроз
- Распределение инцидентов по времени реагирования

Задача: показать потоки

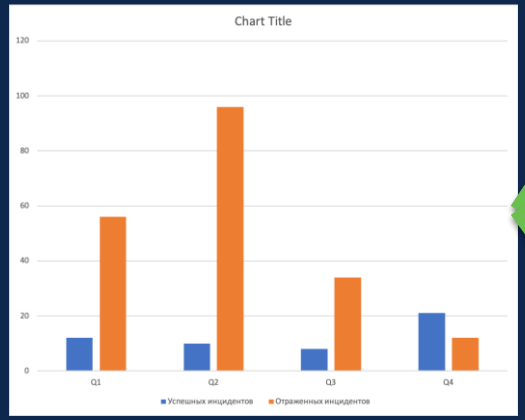
- Взаимодействие людей, промышленных приложений, узлов, подразделений
- Выявление центров силы внутри организации
- Информационные потоки между промышленными узлами
- Выплаты вымогателям на криптовалютные кошельки

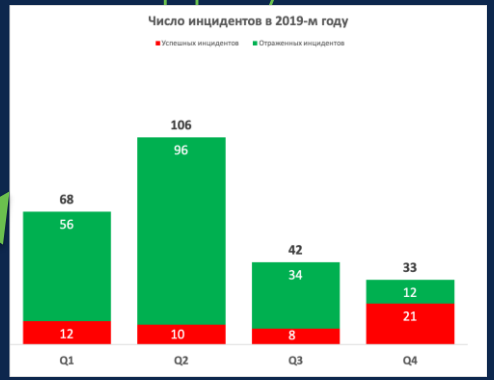
Задача: показать связи

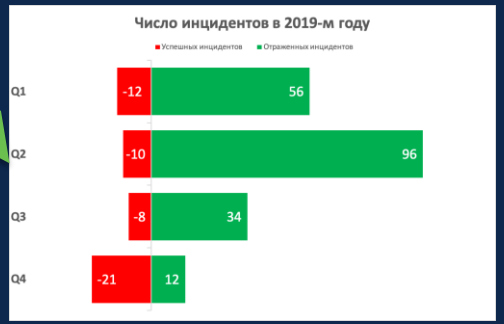


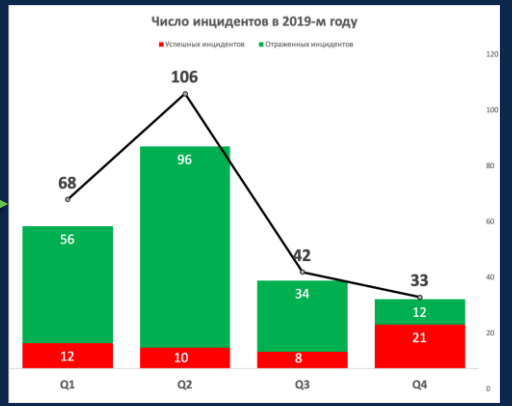
- Взаимодействие людей, промышленных приложений, узлов, подразделений и площадок

Лайфхак: Excel’ем тоже надо уметь пользоваться



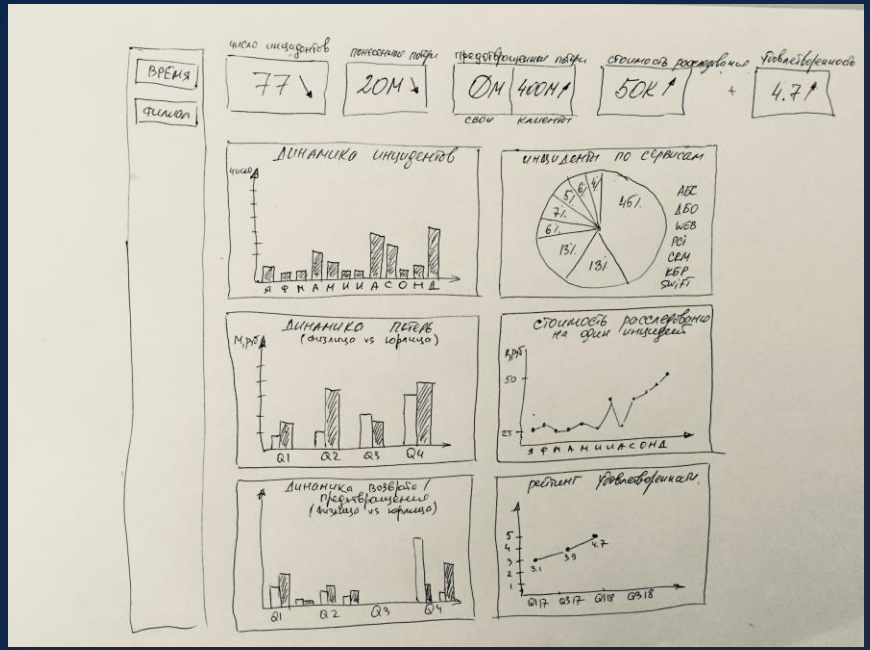






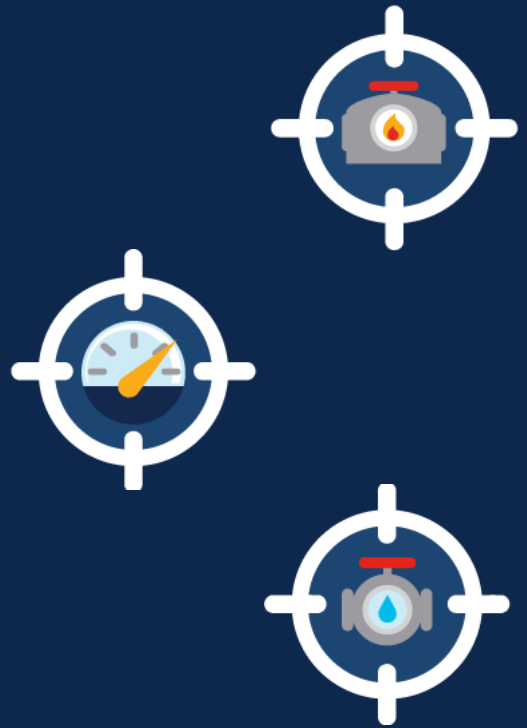
Еще пример макета: SOC для бизнеса

- Ключевые показатели для промышленного SOC в контексте бизнеса
- Оценка в контексте работы промышленного SOC для организации и для ее клиентов разных типов
- Оценка удовлетворенности



В качестве заключения

- С первого раза проекты по сквозной аналитике и их визуализации получаются не всегда
- Аналитика и ее визуализация – это процесс. Начинается с MVP и улучшается
- Первый дашборд обычно не устраивает ЛПР, но он показывает слабые места в ваших процессах
- Дашборды перестают приносить пользу, когда становятся самоцелью



Спасибо!

alukatsk@cisco.com

cisco SECURE