udv|group

Адекватная защита промышленных сетей объектов ТЭК

Алексей Шанин
Директор ООО «СайберЛимфа»
UDV Group

НАШ ОПЫТ РАБОТЫ С ПРЕДПРИЯТИЯМИ ТЭК

- ГУП ТЭК СПб
- Ленинградская АЭС
- Крупнейшие энергетические компании (генерация)
- Крупнейшие газотранспортные, газодобывающие и газоперерабатывающие предприятия

МОНИТОРИНГ ИБ*

АНАЛИЗ СОБЫТИЙ БЕЗОПАСНОСТИ И ИНЫХ ДАННЫХ

- Сбор, подготовка и анализ событий безопасности и иных данных мониторинга
- Выявление инцидентов ИБ
- Контроль, учет и анализ действий пользователей и администраторов
- Сбор и анализ данных о результатах контроля потоков информации
- Выявление скрытых уязвимостей
- Информирование ответственных лиц

КОНТРОЛЬ (АНАЛИЗ) ЗАЩИЩЕННОСТИ

- Выявление уязвимостей
- Контроль установки обновлений безопасности ПО, включая ПО средств защиты информации
- Контроль состава программно-технических средств, ПО и средств ЗИ (инвентаризация)
- Контроль соответствия настроек ПО и средств ЗИ установленным требованиям к защите информации (политикам безопасности)
- Информирование ответственных лиц

АНАЛИЗ И ОЦЕНКА ФУНКЦИОНИРОВАНИЯ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ

- Контроль работоспособности ПО и средств ЗИ
- Проверка соответствия среды функционирования требованиям, предъявленным в документации на средства ЗИ
- Контроль потоков информации, влияющих на производительность информационных (автоматизированных) систем, при межсетевом взаимодействии
- Информирование ответственных лиц

АНАЛИЗ ИЗМЕНЕНИЯ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

- Получение новых данных об индикаторах компрометации, уязвимостях и угрозах безопасности информации
- Выявление новых угроз безопасности информации
- Разработка новых и уточнение действующих правил анализа событий безопасности и иных данных мониторинга
- Разработка рекомендаций по реализации дополнительных мер и мероприятий ЗИ

* - ГОСТ Р 59547-2021 Защита информации. Мониторинг информационной безопасности. Общие положения. Введен 01 апреля 2022

МОНИТОРИНГ ИБ

АНАЛИЗ СОБЫТИЙ БЕЗОПАСНОСТИ И ИНЫХ ДАННЫХ

- Сбор, подготовка и анализ событий безопасности и иных данных мониторинга
- Выявление инцидентов ИБ
- Контроль, учет и анализ действий пользователей и администраторов
- Сбор и анализ данных о результатах контроля потоков информации
- Выявление скрытых уязвимостей
- Информирование ответственных лиц

КОНТРОЛЬ (АНАЛИЗ) ЗАЩИЩЕННОСТИ

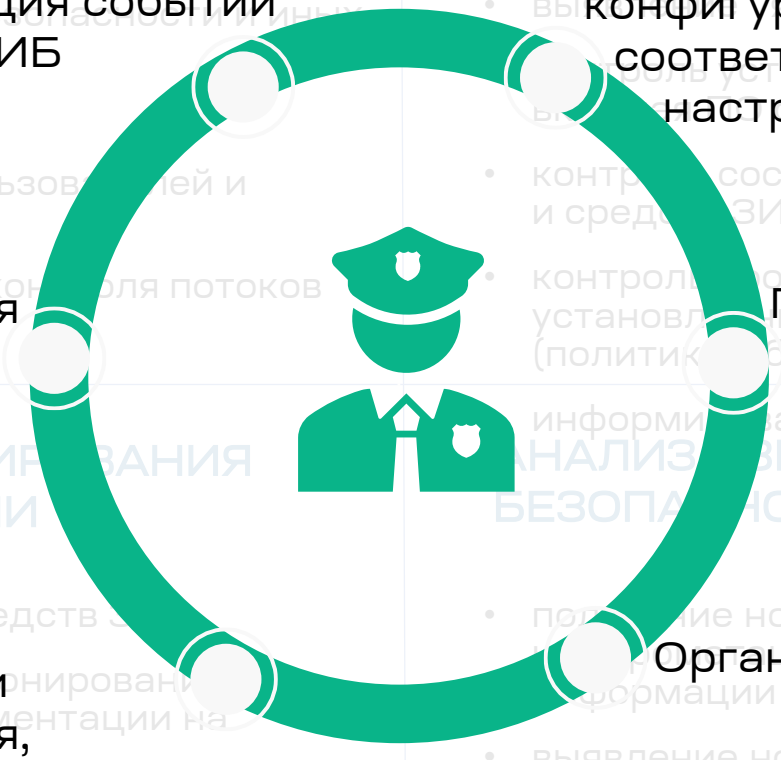
- выявление уязвимостей
- контроль установки обновлений безопасности ПО, выполнения мер средств защиты информации
- контроль состава программно-технических средств, ПО и средств ЗИ (инвентаризация)
- контроль соответствия настроек ПО и средств ЗИ установленным требованиям к защите информации (политике безопасности)
- информирование ответственных лиц

АНАЛИЗ И ОЦЕНКА ФУНКЦИОНИРОВАНИЯ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ

- контроль работоспособности ПО и средств ЗИ
- проверка соответствия конфигурирования требованиям, предъявленным в документации на средства ЗИ
- контроль потоков информации, влияющих на производительность информационных (автоматизированных) систем, при межсетевом взаимодействии
- Информирование ответственных лиц

АНАЛИЗ ИЗМЕНЕНИЯ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

- получение новых данных об индикаторах компрометации, уязвимостях и угрозах безопасности информации
- выявление новых угроз безопасности информации
- разработка новых и уточнение действующих правил анализа событий безопасности и иных данных мониторинга
- разработка рекомендаций по реализации дополнительных мер и мероприятий ЗИ



АДЕКВАТНЫЙ МОНИТОРИНГ ИБ

- Комплексный и непрерывный процесс наблюдения и корректировки СрЗИ и защищаемой системы
- Максимально эффективен с учетом **всех ограничений**, предъявляемых защищаемой системой

ОГРАНИЧЕНИЯ:

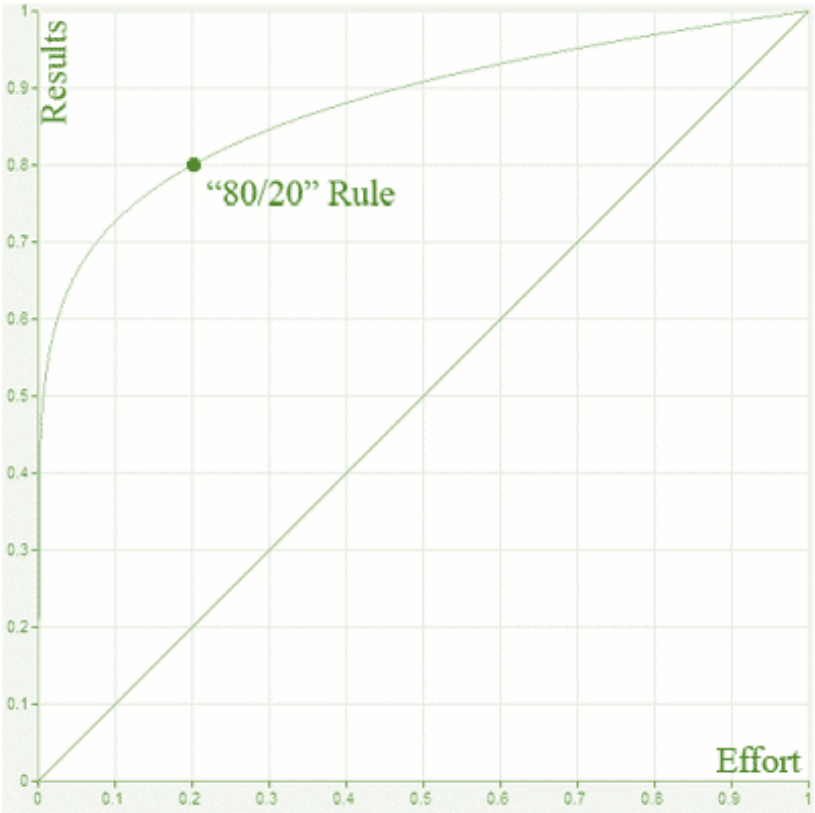
организационные

технические

экономические

...

ОГРАНИЧЕНИЕ. ИНФРАСТРУКТУРА



Использование существующего активного сетевого оборудования и каналов связи

Минимальная нагрузка на каналы связи и оборудование (RSPAN и передача данных)

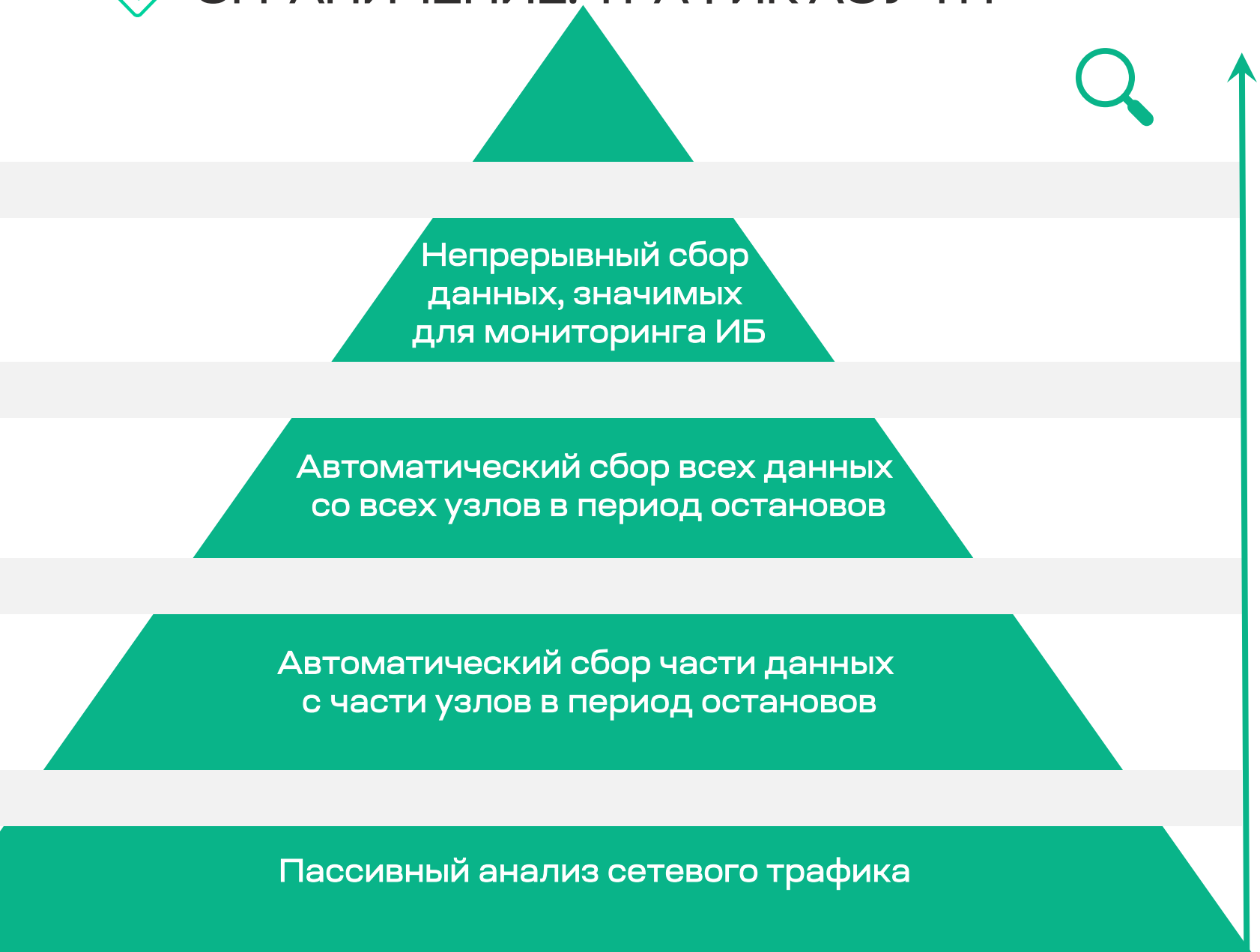
Выбор наиболее репрезентативных точек подключения к инфраструктуре

Получение данных без установки дополнительного ПО

ОТСУТСТВИЕ МОНИТОРИНГА

БЕСКОМПРОМИССНЫЙ МОНИТОРИНГ

ОГРАНИЧЕНИЕ. ТРАФИК АСУ ТП



- Отсутствие влияния на защищаемые системы и технологические процессы
- Поддержка специального оборудования и ПО
- Поддержка особенностей сетей передачи данных и специализированных протоколов
- Фокусирование на атаках и угрозах, актуальных для промышленных систем автоматизации

Не только анализ трафика

Не все угрозы ИБ сетевые

- Подключение съемных устройств
- Изменения настроек безопасности
- Выключение конечного устройства

Внедрение шифрования трафика:

Уже сейчас:

- RDP, SSH, HTTPS, ...
- OPC UA
- Modbus TLS
- S7CommPlus

Дальше - больше

Технологические сложности обеспечения полного покрытия IDS:

- Обеспечение сбора трафика во всех точках обмена
- Потери пакетов при зеркалировании трафика
- Ограничения со стороны сетевого оборудования

ОГРАНИЧЕНИЕ. Не только анализ трафика

Dale Peterson

ICS security researcher

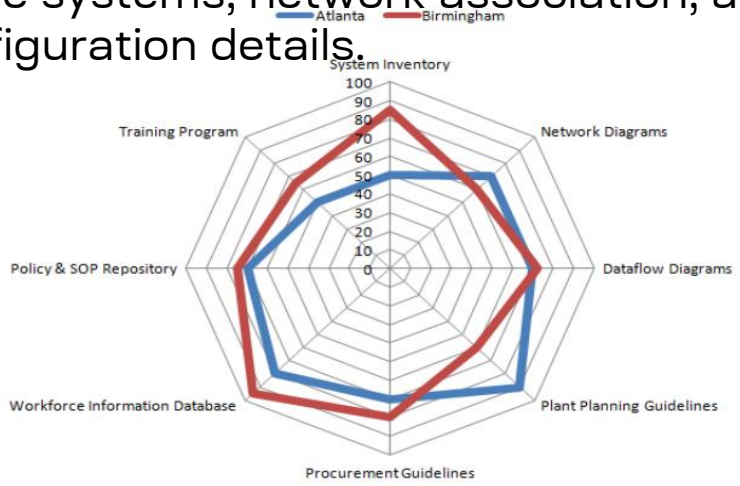
- Passive-only is a phase that will end soon
- You would want to ingest firewall logs, application whitelisting events, Windows, Linux and ICS application security events, switch logs and eventually PLC/controller events
- IDS/IPS is only part of a detection solution. It has proved to be a viable product category and it would be relatively simple to add ICS anomaly detection technology to their sensors and management systems.

https://dale-peterson.com/2018/07/23/the-future-of-the-ics-cyber-security-detection-market/

Ralph Langner

(OT Security Analyst, создатель RIPE framework)

- ACTIVE discovery — because it's better and cheaper
- Documentation: A cyber system inventory, manifested as a database, stores information on hardware systems, the software running on those systems, network association, and configuration details.



https://www.langner.com/wp-content/uploads/2017/04/The-RIPE-Framework.pdf

КОНТРОЛЬ И ОБНАРУЖЕНИЕ

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score
1	CVE-2021-46161	787		Exec Code	2022-02-09	2022-02-11	6.8
A vulnerability has been identified in S... V2021.1 (All versions). A parsing specially crafted NEU files. Th...							
2	CVE-2021-46160	787					

Свойства: Администраторы

Общие

Администраторы

Описание: Администраторы имеют полные, ничем не ограниченные права доступа к компьютеру или домену

Члены группы:
admin
User
Администратор

Добавить... Удалить

Изменения членства в группах вступят в силу после следующего входа пользователя в систему.

OK Отмена Применить Справка

Управление компьютером (л...
Служебные программы
Планировщик заданий
Просмотр событий
Общие папки
Локальные пользовате...
Пользователи
Группы

Имя
admin
DefaultAccount
WDAGUtilityAccount
Администратор
Гость

Create permanent shared objects
Create symbolic links
Debug programs

Debug programs Properties

Security Policy Setting | Explain

Debug programs

Define these policy settings:

Group Policy Management Editor

Policy
Network security: Restrict NTLM: Outgoing NTLM traffic to remote servers — Not De...
Network security: Restrict NTLM: NTLM authentication in this domain — Not De...
Network security: Restrict NTLM: Incoming NTLM traffic — Not De...
Network security: Restrict NTLM: Audit NTLM authentication in this domain — Not De...
Network security: Restrict NTLM: Audit Incoming NTLM Traffic — Not De...
Network security: Restrict NTLM: Add server exceptions in this domain — Not De...
Network security: Restrict NTLM: Add remote server exceptions for NTLM authentic... — Not De...
Network security: Minimum session security for NTLM SSP based (including secure ... — Not De...
Network security: Minimum session security for NTLM SSP based (including secure ... — Not De...
Network security: LDAP client signing requirements — Not De...
Network security: LAN Manager authentication level — Not De...

Network security: LAN Manager authentication lev...

Security Policy Setting | Explain

Network security: LAN Manager authentication level

Define this policy setting

Send LM & NTLM responses
- Send LM & NTLM responses
- Send LM & NTLM - use NTLMv2 session security if negotiated
- Send NTLM response only
- Send NTLMv2 response only
- Send NTLMv2 response only. Refuse LM
- Send NTLMv2 response only. Refuse LM & NTLM

Group Policy Management Editor

File Action View Help

Default Domain Policy [DC.CONTOSO.COM] Policy
- Computer Configuration
  - Policies
    - Software Settings
    - Windows Settings
      - Name Resolution Policy
      - Scripts (Startup/Shutdown)
      - Security Settings
        - Account Policies
        - Local Policies
          - Audit Policy
          - User Rights Assignment
          - Security Options
        - Event Log
        - Restricted Groups
        - System Services

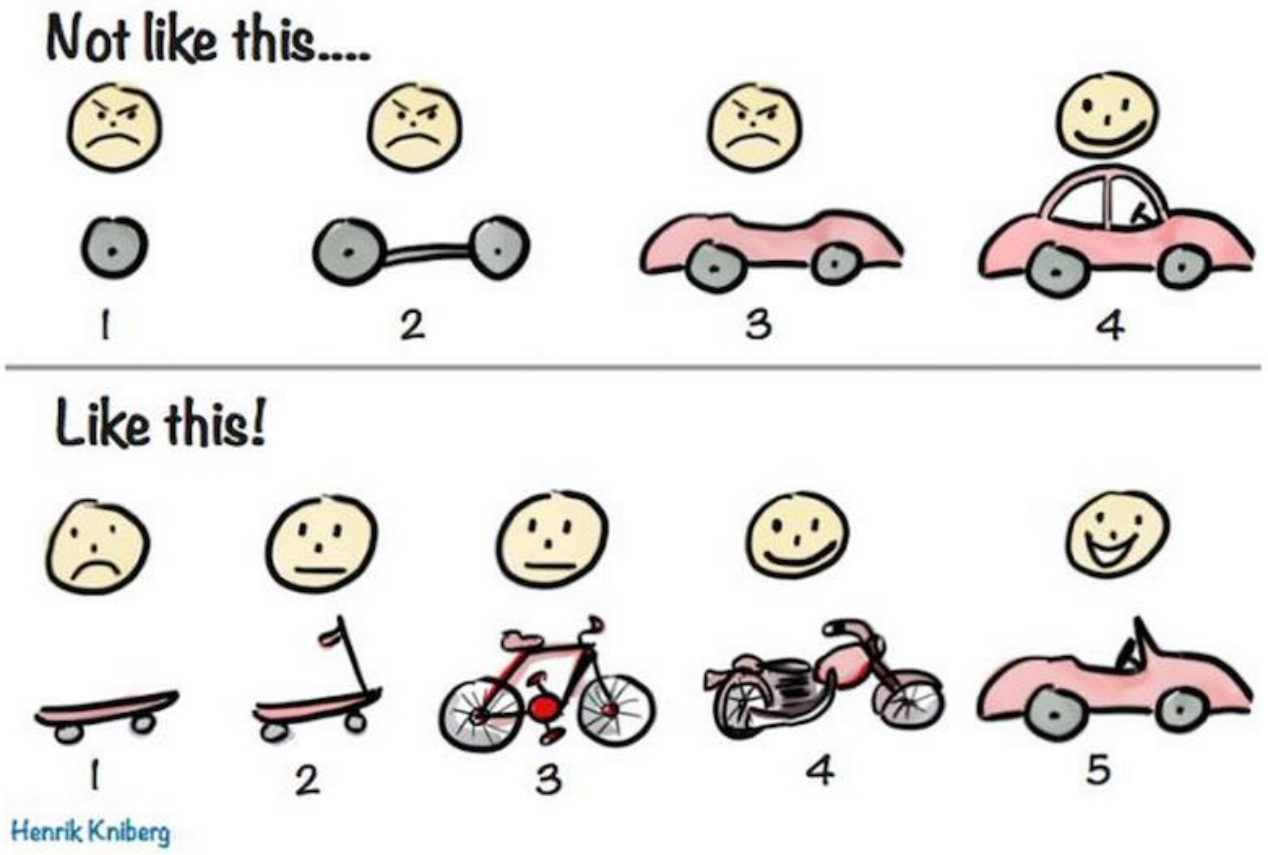
Policy	Policy Setting
Audit account logon events	Not Defined
Audit account management	Not Defined
Audit directory service access	Not Defined
Audit logon events	Not Defined
Audit object access	Not Defined
Audit policy change	Not Defined
Audit privilege use	Not Defined
Audit process tracking	Not Defined
Audit system events	Not Defined

ОГРАНИЧЕНИЕ. ЭТАПНОСТЬ

На первых этапах закладывается масштабируемая основа и стратегически корректная архитектура

Базовая функциональность, позволяющая получать 80% результата при 20% бюджета

По мере развития система «обрастает» дополнительными возможностями



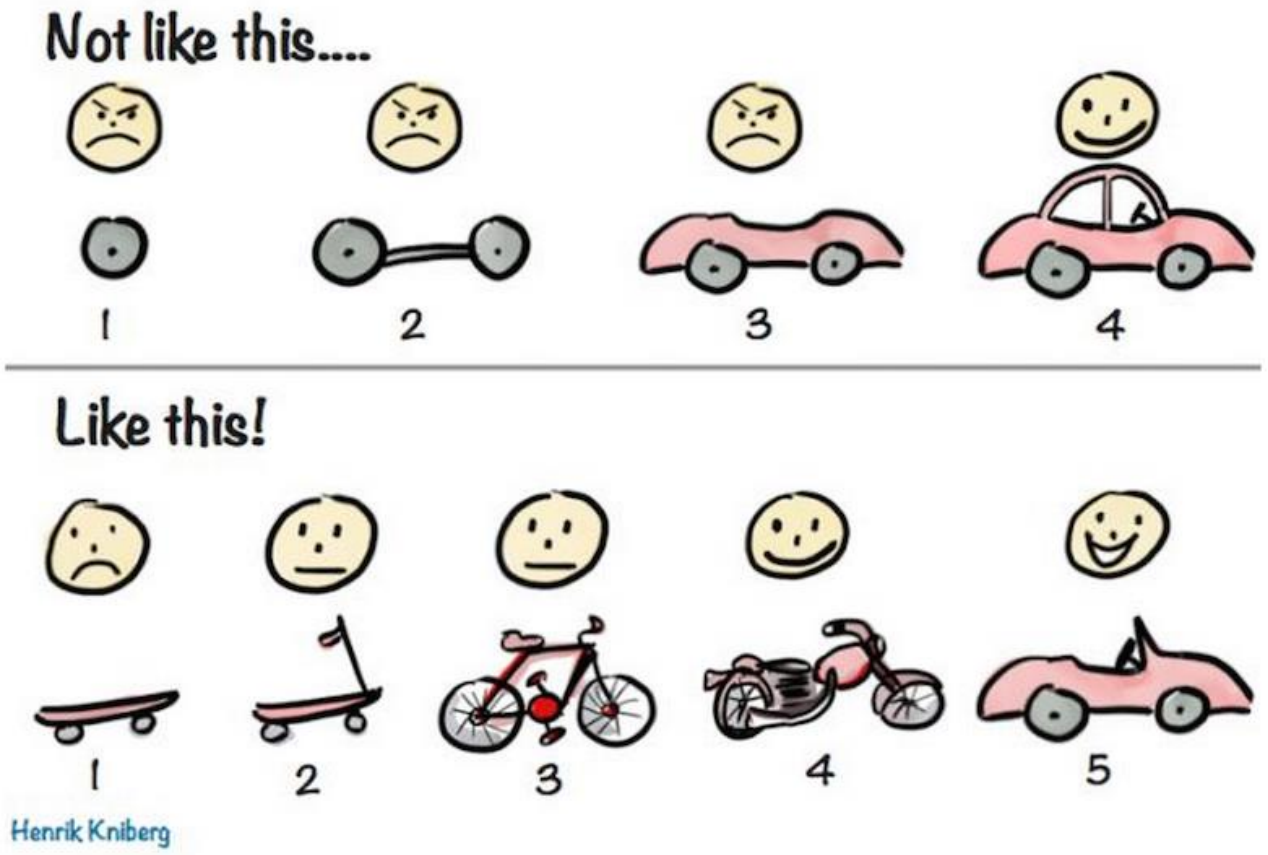
ОГРАНИЧЕНИЕ. ЭТАПНОСТЬ

На первых этапах закладывается масштабируемая основа и стратегически корректная архитектура

Базовая функциональность, позволяющая получать 80% результата при 20% бюджета

По мере развития система «обрастает» дополнительными возможностями

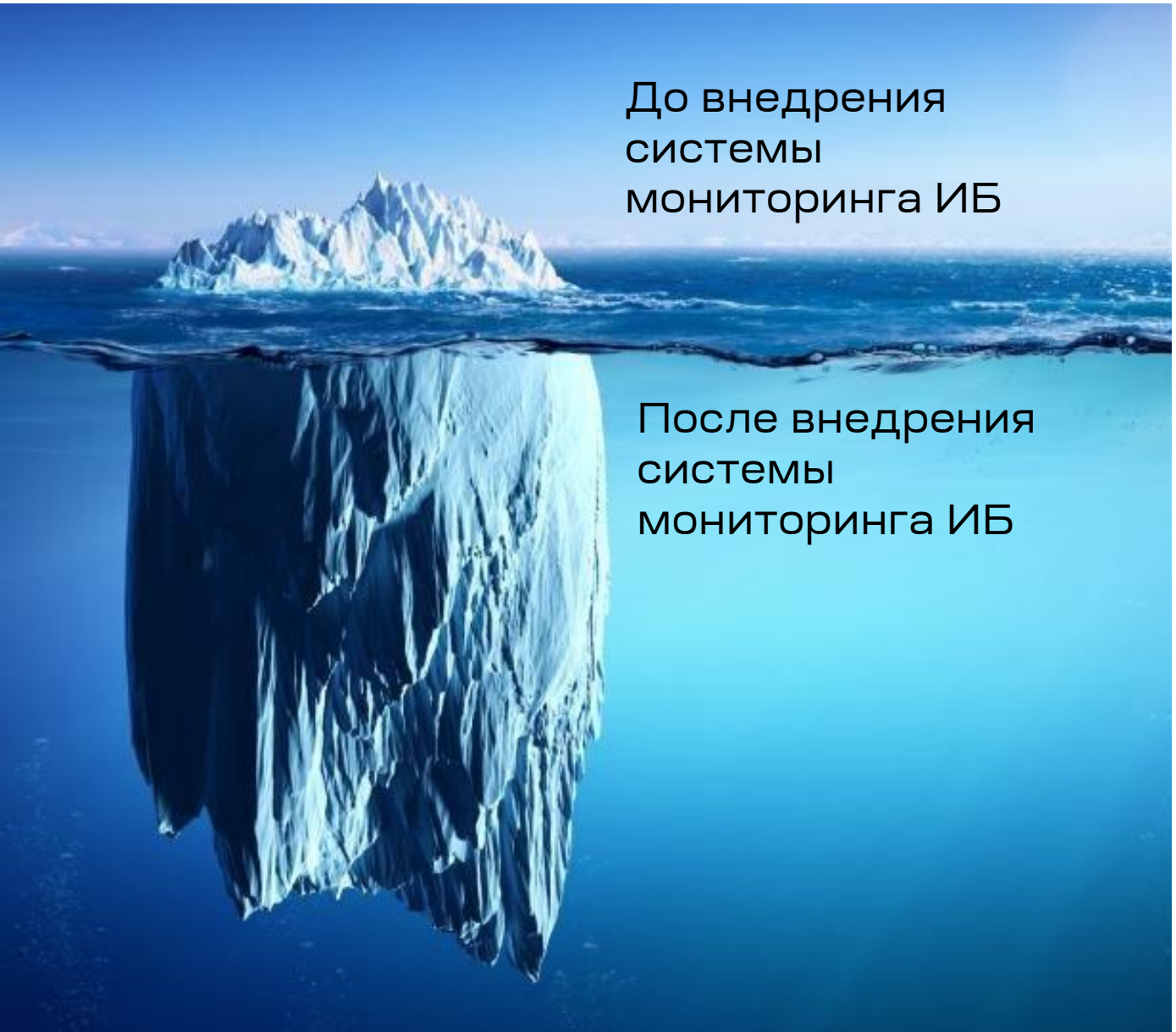
ДА, НО!



Приведение защищаемой системы к безопасному состоянию

Мониторинг и выявление отклонений от безопасного состояния

ОГРАНИЧЕНИЕ. ПЕРСОНАЛ



- Квалифицированный штат 24x7
- Обнаружение, нейтрализация и расследование инцидентов
- Обработка ложных срабатываний
- Ведение базы решающих правил
- Актуализация угроз безопасности информации

МОНИТОРИНГ ИБ

АНАЛИЗ СОБЫТИЙ БЕЗОПАСНОСТИ И ИНЫХ ДАННЫХ

- Сбор, подготовка и анализ событий безопасности и иных данных мониторинга
- Выявление инцидентов ИБ
- Контроль, учет и анализ действий пользователей и администраторов
- Сбор и анализ данных о результатах контроля потоков информации
- Выявление скрытых уязвимостей
- Информирование ответственных лиц

АНАЛИЗ И ОЦЕНКА ФУНКЦИОНИРОВАНИЯ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ

- контроль работоспособности ПО и средств ЗИ
- проверка соответствия [illegible] требованиям, предъявленным в документации на средства ЗИ
- контроль потоков информации, влияющих на производительность информационных (автоматизированных) систем, при межсетевом взаимодействии
- Информирование ответственных лиц

КОНТРОЛЬ (АНАЛИЗ) ЗАЩИЩЕННОСТИ

- выявление [illegible]
- контроль установки обновлений безопасности ПО, [illegible] средств защиты информации
- контроль состава программно-технических средств, ПО и средств ЗИ (инвентаризация)
- контроль соответствия настроек ПО и средств ЗИ установленным требованиям по защите информации (политике безопасности)
- информирование ответственных лиц

АНАЛИЗ ИЗМЕНЕНИЯ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

- получение новых данных об индикаторах [illegible] и угрозах безопасности информации
- выявление новых угроз безопасности информации
- разработка новых и уточнение действующих правил анализа событий безопасности и иных данных мониторинга
- разработка рекомендаций по реализации дополнительных мер и мероприятий ЗИ

МОНИТОРИНГ ИБ

АНАЛИЗ СОБЫТИЙ БЕЗОПАСНОСТИ И ИНЫХ ДАННЫХ

- Сбор, подготовка и анализ событий безопасности и иных данных мониторинга
- Выявление инцидентов ИБ
- Контроль, учет и анализ действий пользователей и администраторов
- Сбор и анализ данных о результатах контроля потоков информации
- Выявление скрытых уязвимостей
- Информирование ответственных лиц

КОНТРОЛЬ (АНАЛИЗ) ЗАЩИЩЕННОСТИ

- выявление уязвимостей
- контроль установки обновлений безопасности ПО, включая ПО средств защиты информации
- контроль состава программно-технических средств, ПО и средств ЗИ (инвентаризация)
- контроль соответствия настроек ПО и средств ЗИ установленным требованиям к защите информации (политике безопасности)
- информирование ответственных лиц

АНАЛИЗ И ОЦЕНКА ФУНКЦИОНИРОВАНИЯ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ

- контроль работоспособности ПО и средств ЗИ
- проверка соответствия среды функционирования требованиям, предъявленным в документации на средства ЗИ
- контроль потоков информации, влияющих на производительность информационных (автоматизированных) систем, при межсетевом взаимодействии
- Информирование ответственных лиц

АНАЛИЗ ИЗМЕНЕНИЯ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

- получение новых данных об индикаторах компрометации и угрозах безопасности информации
- выявление новых угроз безопасности информации
- разработка новых и уточнение действующих правил анализа событий безопасности и иных данных мониторинга
- разработка рекомендаций по реализации дополнительных мер и мероприятий ЗИ

DATAPK Industrial Kit

+Организационные меры

udv|group

СПАСИБО ЗА ВНИМАНИЕ!

Закажите пилотный проект или персональную демонстрацию наших решений

commercial@udv.group

udv.group