DATAPK

DATAPK
на страже АСУ ТП

Алексей Шанин
Директор лаборатории DATAPK

Модель мониторинга ИБ АСУ ТП

Контролируемый канал связи (МЭ, диод данных)

Защищаемая АСУ ТП

- Безопасная настройка компонентов
- Ограничение доступа оперативного персонала
- Отключение инженерных (сервисных) станций

»

Смежная система

Непрерывный мониторинг отклонений от эталонной модели:

- Состав компонентов АСУ ТП
- Конфигурации ПО и оборудования
- Схема информационных потоков
- Анализ событий ИБ
- Анализ конфигураций на соответствие требованиям/наличие известных уязвимостей

DAT APK

Лучшие практики

Приказ ФСТЭК России №239 «Об утверждении требований по обеспечению безопасности значимых объектов КИИ РФ»:

- Группа мер управление конфигурацией (УКФ)
- Меры: АУД.1 – инвентаризация информационных ресурсов, АУД.4 – регистрация событий безопасности, АУД.5 – контроль и анализ сетевого трафика, АУД.7 – мониторинг безопасности, ОЦЛ.1 – контроль целостности ПО, ОЦЛ.2 – контроль целостности информации,

SP 800-137 «Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations»:

- Домены автоматизации безопасности: управление уязвимостями, управление событиями, управление инцидентами, управление активами, управление конфигурацией, управление сетью
- Трёхуровневая референсная модель непрерывной системы мониторинга ИБ

RIPE Framework:

- System population characteristics – инвентаризационная информация об АСУ ТП
- Network Architecture – схема сети
- Component Interaction – информация о сетевом взаимодействии компонентов АСУ ТП

DATAPK – основа системы анализа и мониторинга состояния ИБ АСУ ТП

DATAPK – специализированное решение:

- Пассивный анализ сетевого трафика (DPI & IDS)
- Сбор данных без агентов
- Управление событиями ИБ, корреляция и визуализация
- Анализ защищенности и оценка соответствия

Отрасль


Нефть и газ


Энергетика и генерация


Химическая промышленность


Металлургия


Производство


Телеком

DATAPK

Выявление инцидентов ИБ

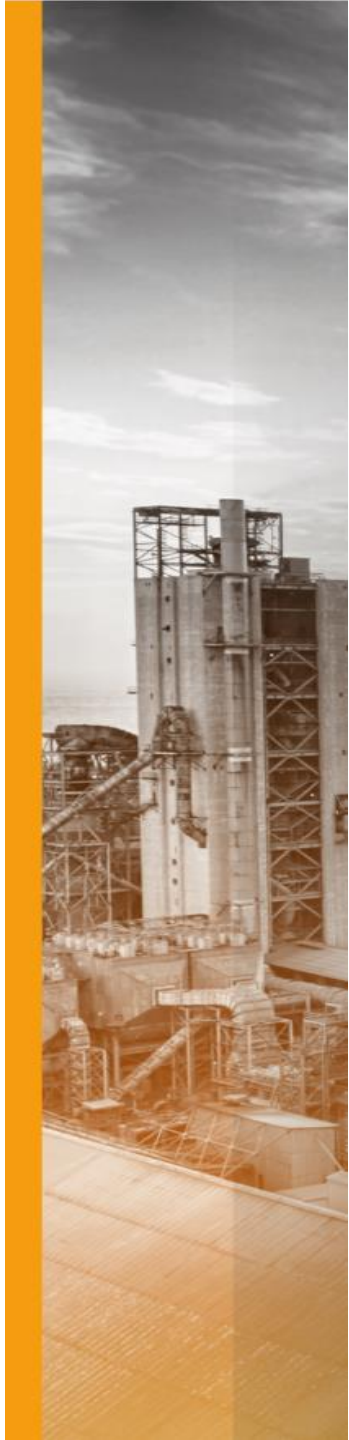
Инвентаризация АСУ ТП

Оценка состояния

DATAPK

Источники данных:

- **Сетевой трафик**
- **Конфигурации**
- **События**
- **Уязвимости и соответствие**



Источники информации: сетевой трафик

Технологии:

- Глубокая инспекция пакетов (DPI)
- Обнаружение вторжений (IDS)

Поддерживаемые протоколы:
S7, TPKT, COTP, IEC104, IEC61850, Profinet IO, Modbus TCP, Modbus RTU over TCP, Suitelink, Omron FINS, MDLC, BSAP, OPC UA, OPC DA, VNET/IP и другие
Обнаружение вторжений:
Snort-подобные правила

Ключевые особенности:

- Получение данных исключительно в пассивном режиме со SPAN/Mirror портов коммутаторов

Функции:

- Обнаружение сетевых узлов и ведение каталога активов
- Выявление информационных потоков и ведение их базы
- Визуализация карты сети
- Выявление запрещенных коммуникаций и управляющих команд
- Обнаружение вторжений

Источники информации: конфигурации

Технологии:

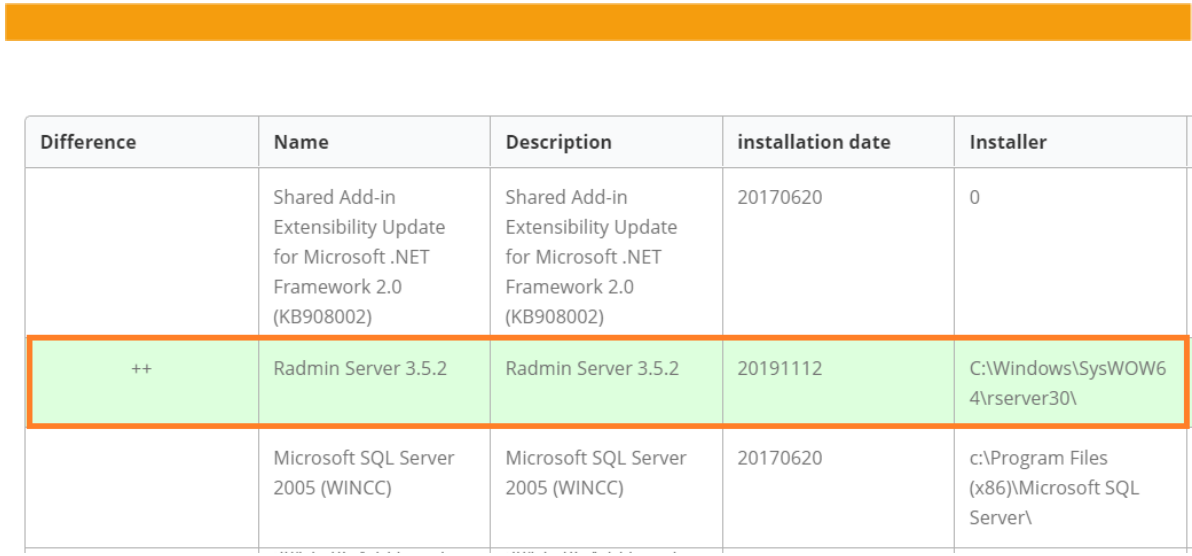
- Активный режим
- Безагентный сбор с использованием штатных механизмов обмена данными

Ключевые особенности:

- Поддержка новых объектов защиты без изменения кода

Функции:

- Ведение каталога конфигураций
- Контроль соответствия эталонным конфигурациям



Difference	Name	Description	installation date	Installer
	Shared Add-in Extensibility Update for Microsoft .NET Framework 2.0 (KB908002)	Shared Add-in Extensibility Update for Microsoft .NET Framework 2.0 (KB908002)	20170620	0
++	Radmin Server 3.5.2	Radmin Server 3.5.2	20191112	C:\Windows\SysWOW64\rserver30\
	Microsoft SQL Server 2005 (WINCC)	Microsoft SQL Server 2005 (WINCC)	20170620	c:\Program Files (x86)\Microsoft SQL Server\

Коннекторы:

- RPC, WinRM, SSH, Telnet, SNMP, SMB, SCP, FTP, NFS, MSSQL, Oracle DB, MySQL, S7comm, PROFINET, Modbus TCP, OPC UA

Сетевое оборудование

- Cisco, HP, Hirschmann, MOXA, Advantech, Check Point, Siemens, Fortinet

SCADA

- Simatic WinCC, TrainView, TRACE MODE Runtime, Wonderware Intouch, ICONICS GENESIS-32, MasterSCADA, RSLinx

Операционные системы

- Windows, Linux, UNIX

СУБД

- MSSQL, MySQL, OracleDB, PostgreSQL

ПЛК

- Siemens (S7comm), другие (PROFINET TCP, MODBUS TCP, SNMP, FTP и пр.)

Источники информации: события

Технологии:

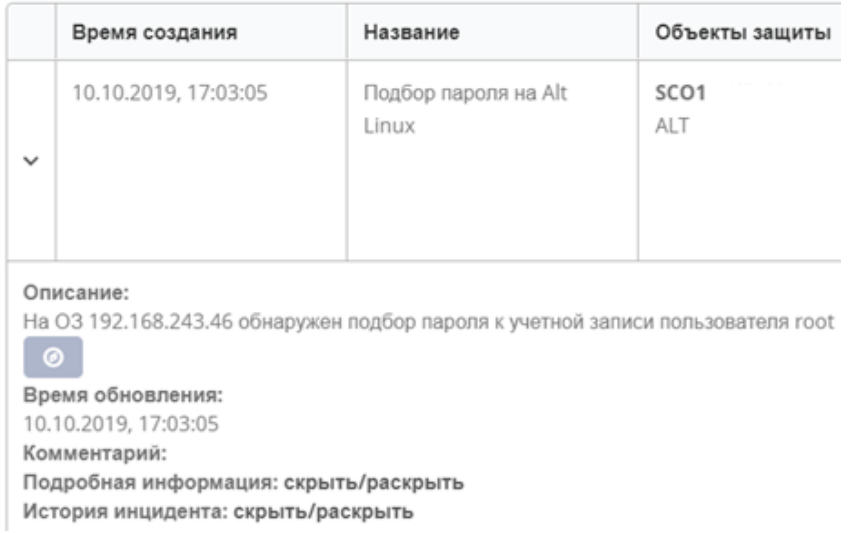
- Пассивный и активный режимы
- Нормализация и обогащение событий
- Корреляция событий
- Визуализация данных

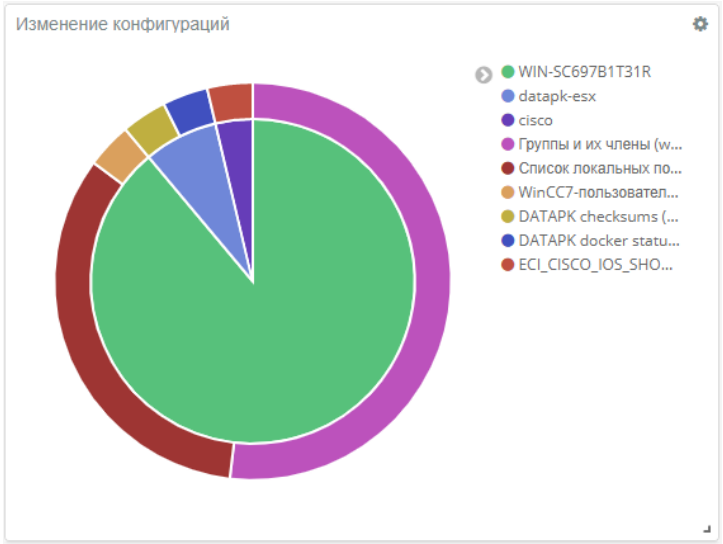
Функции:

- Сбор событий с объектов защиты
- Визуальное представление данных
- Выявление инцидентов ИБ на основе правил
- Управление статусами инцидентов ИБ

Ключевые особенности:

- Поддержка новых объектов защиты без изменения кода





Источники информации: контроль состояния

Технологии:

- Механизм OVAL (Open Vulnerability and Assessment Language)

Ключевые особенности:

- Сбор данных без агентов
- Поддержка сторонних баз

Функции:

- Анализ уязвимостей
- Контроль соответствия требованиям ИБ

Definition ID	Class	Title
oval:org.cisecurity:def:5689	vulnerability	Windows Hyper-V Denial of Service Vulnerability - CVE-2018-8436
oval:org.cisecurity:def:3248	vulnerability	Scripting Engine Memory Corruption Vulnerability - CVE-2017-8660
oval:org.cisecurity:def:3884	vulnerability	Windows Information Disclosure Vulnerability - CVE-2018-0747
oval:org.cisecurity:def:3263	vulnerability	Scripting Engine Memory Corruption Vulnerability - CVE-2017-8756

Идентификатор	Название	Описание	Класс	Результат
oval:mil.disa.fso.windows:def:103	Automatic blocking of user sessions	Automatic blocking of user sessions	COMPLIANCE	FALSE

Централизованное управление

Передача вниз:

- Управляющие команды
- Группы и метки
- Политики сбора данных
- Правила нормализации событий
- Правила корреляции событий
- Правила обнаружения вторжений
- Определения OVAL

ПАК DATAPK верхнего уровня

ПАК DATAPK среднего уровня

ПАК DATAPK базового уровня

Передача вверх:

- Объекты защиты
- Информационные потоки
- Карты сети
- Конфигурации
- События
- Инциденты ИБ
- Результаты проверок OVAL

Режимы функционирования

Пассивный мониторинг:

- Однонаправленное получение данных
- Прослушивание трафика и прием событий

Активный мониторинг:

- Получение конфигураций и событий
- Взаимодействие в режиме «Запрос - Ответ» с использованием штатных механизмов объектов защиты

Сканирование защищенности:

- Выявление уязвимостей и проверки на соответствие требованиям ИБ
- Взаимодействие в режиме «Запрос - Ответ» с использованием штатных механизмов объектов защиты

Функции	Пассив-ный	Актив-ный	Скани-рование
Сбор событий ИБ	✗ ✓	✓	✓
Обнаружение атак	✓	✓	✓
Выявление сетевых аномалий	✓	✓	✓
Сбор конфигураций	✗	✓	✓
Определение текущего состава ОЗ	✓	✓	✓
Выявление изменений в составе ОЗ	✓	✓	✓
Проверка ОЗ на наличие уязвимостей	✗	✗	✓

Меры по защите информации (приказы №31 и №239)

- **идентификация и аутентификация (ИАФ)**
- **управление доступом (УПД)**
- **ограничение программной среды (ОПС)**
- **защита машинных носителей информации (ЗНИ)**
- **аудит безопасности (АУД)**
- антивирусная защита (АВЗ)
- **предотвращение вторжений (компьютерных атак) (СОВ)**
- **обеспечение целостности (ОЦЛ)**
- **обеспечение доступности (ОДТ)**
- **защита технических средств и систем (ЗТС)**
- **защита информационной (автоматизированной) системы и ее компонентов (ЗИС)**
- **реагирование на компьютерные инциденты (ИНЦ)**
- **управление конфигурацией (УКФ)**
- **управление обновлениями программного обеспечения (ОПО)**
- **планирование мероприятий по обеспечению безопасности (ПЛН)**
- обеспечение действий в нештатных ситуациях (ДНС)
- информирование и обучение персонала (ИПО)

Ключевые преимущества:

Всесторонний мониторинг ИБ АСУ ТП – комплексный анализ данных из различных источников:

- Сетевой трафик, конфигурации, события, состояние защищенности

Получение данных от АСУ ТП без инсталляции стороннего ПО:

- Пассивное получение данных в режиме прослушивания
- Опрос компонентов АСУ ТП с использованием их штатных механизмов сетевого взаимодействия

Адаптация к АСУ ТП Заказчика без привлечения разработчика:

- Расширение перечня анализируемых протоколов, параметров конфигураций, выявляемых инцидентов ИБ
- Расширение источников и типов событий

Поддержка распределенных инсталляций:

- Централизованное управление всей инсталляцией и консолидация данных трехуровневой иерархии
- Адаптация под реальные каналы связи – обмен результатами обработки данных и минимальная нагрузка на сеть передачи данных

Куда мы движемся?

Функции:

- Автоматизация действий пользователей
- Экспертиза вендора «из коробки»
- Максимум информации при пассивном анализе

Интерфейс:

- Новые карты сети
- Развитие единого интерфейса представления данных

Внедрение:

- Мастер установки и предварительно настроенные образы

Лицензирование:

- Поставка в виде ПАК, ПО и виртуальных аплаенсов
- Модель подписки

Спасибо за внимание!

ООО «УЦСБ»

info@ussc.ru

+7 (343) 379-98-34

Уральский центр систем безопасности

USSC.RU