DATAPK

DATAPK на страже АСУ ТП

Алексей Шанин
Директор лаборатории DATAPK

Модель мониторинга безопасности АСУ ТП

Защищаемая АСУ ТП
- Безопасная настройка компонентов
- Ограничение доступа оперативного персонала (режим «киоска»)
- Отключение инженерных (сервисных) станций

Контролируемый канал связи (МЭ, диод данных)

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

Мониторинг безопасности в лучших практиках по обеспечению ИБ АСУ ТП

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 – специализированный программно-аппаратный комплекс, обеспечивающий:

- Выявление изменений в составе АСУ ТП
- Выявление атак на компоненты АСУ ТП
- Сбор и контроль конфигураций компонентов АСУ ТП
- Сбор и корреляция событий
- Анализ защищенности и контроль выполнения требований ИБ
- Трехуровневая иерархия
- Интеграция со смежными системами

- Сертификат соответствия ФСТЭК России №3731 от 12.04.2017 г.
- Запись в реестре отечественного ПО №4732, на основании приказа №475 Минкомсвязи России
- Наличие успешных внедрений на предприятиях промышленности

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	✗	✗	✓

Источники информации

USSC

DATAPK

Анализ групп данных:

Сетевой трафик

Конфигурации

События

Контроль состояния

Источники информации: сетевой трафик

Технологии:

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

Анализ промышленных протоколов:
S7comm, TPKT, COTP, OMRON FINS, IEC104, IEC 61850, Suitelink, MDLC, BSAP, Modbus TCP, OPC DA и другие

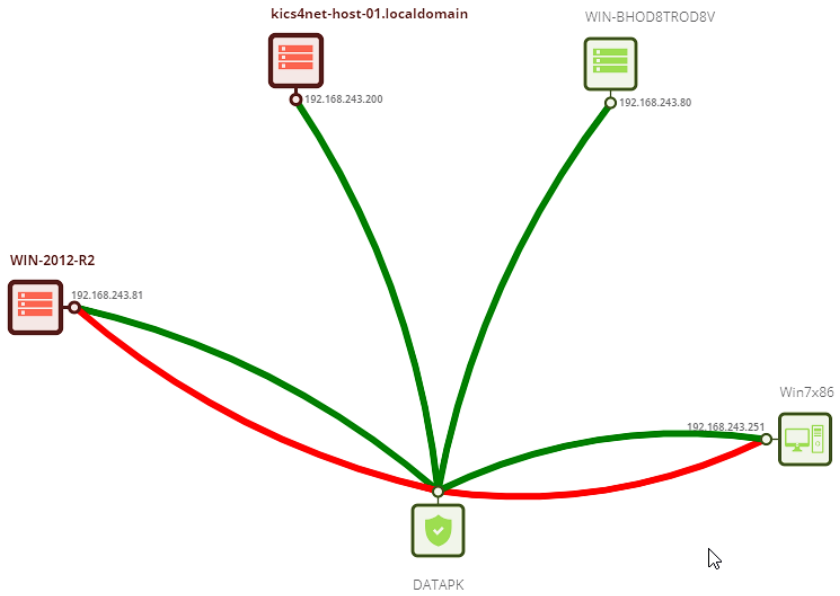
Средство обнаружения вторжений:
Snort-подобные правила

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

Различие	Заголовок	Описание	Путь
	Print1.exe	Print1.exe	C:\PROGRA~2\SIEMENS\WINCC\BIN\Print1.exe
++	notepad.exe	notepad.exe	C:\Windows\system32\notepad.exe
++	svchost.exe	svchost.exe	C:\Windows\System32\svchost.exe

Особенности:

- Поддержка новых объектов защиты без изменения кода

Функции:

- Ведение каталога конфигураций
- Контроль соответствия эталонным конфигурациям

Протоколы:

- 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

SCADA

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

Операционные системы

- Windows (с Win98), семейства Linux и UNIX

СУБД

- MSSQL, MySQL, OracleDB, PostgreSQL

ПЛК

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

Источники информации: события

Технологии:

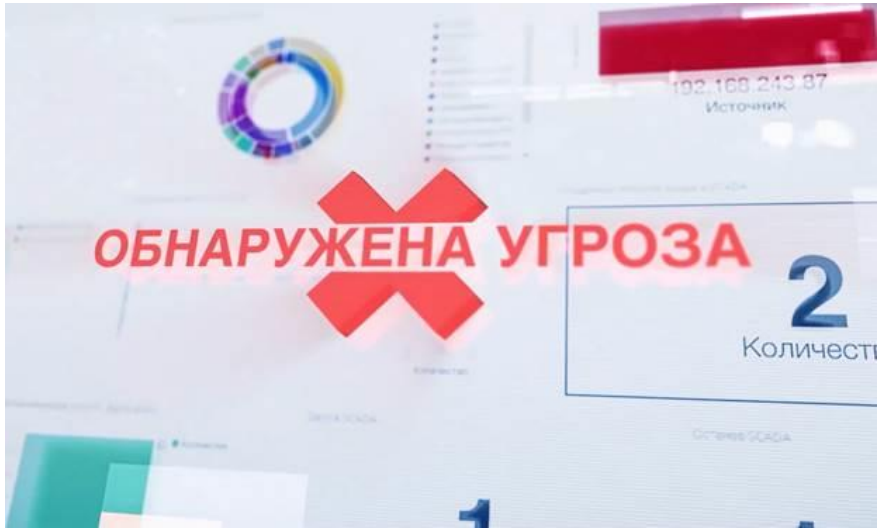
- Пассивный и активный режимы
- Нормализация и обогащение событий
- Корреляция событий
- Визуализация данных

Особенности:

- Поддержка новых объектов защиты без изменения кода

Функции:

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



	Время создания	Название	Объекты защиты
⌄	10.10.2019, 17:03:05	Подбор пароля на Alt Linux	SCO1-vSIR-03 ALT

Описание:
На ОЗ 192.168.243.46 обнаружен подбор пароля к учетной записи пользователя root

Время обновления:
10.10.2019, 17:03:05
Комментарий:
Подробная информация: скрыть/раскрыть
История инцидента: скрыть/раскрыть

Источники информации: контроль состояния

Технологии:

- Механизм OVAL (Open Vulnerability and Assessment Language)

Особенности:

- Безагентный сбор и 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

Трехуровневая иерархия

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

Отзывы заказчиков

USSC

DATAPK

Выявление инцидентов ИБ в АСУ ТП

Повышение уровня осведомленности о состоянии ИБ в АСУ ТП

Соответствие требованиям законодательства

Средства обеспечения ИБ АСУ ТП (приказ №235)

Возможна реализация средствами DATAPK

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)

Преимущества DATAPK

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

DATAPK

Алексей Шанин

Директор лаборатории DATAPK
ООО «УЦСБ»

ashanin@ussc.ru

+7 (343) 379-98-34 (доб. 1193)