Kaspersky Industrial Cybersecurity Conference 2023

Аудит безопасности промышленных и информационных систем. Возможности современных средств управления уязвимостями, их координация с решениями по защите инфраструктуры промышленных предприятий.

Сергей Уздемир
Заместитель генерального директора по ИТ
АЛТЭКС-СОФТ

kaspersky

Вопросы

1. История вопроса аудита безопасности в России
2. Репозитории уязвимостей. Открытые стандарты проведения аудита безопасности, результатов проверок и их оценки
3. Выявление уязвимостей в общесистемном программном обеспечении и в промышленном оборудовании.
4. Преимущества применения открытых стандартов для конечного пользователя, интегратора, вендора XDR-системы.
   Опыт интеграции с KICS.
5. Оценка соответствия (compliance) на соответствие стандартам в области ИБ, отраслевым, промышленным стандартам с использованием САЗ и XDR-систем.

АЛТЭКС-СОФТ – российский разработчик средств анализа защищённости

- 10+ лет разработки средства анализа защищённости RedCheck
- OVALdb - база уязвимостей в формате SCAP
- Консалтинг по сертификации СЗИ
- Участие в БДУ ФСТЭК России (ScanOVAL, описания уязвимостей в формате OVAL)

САЗ RedCheck. Соответствие требованиям регуляторов

REDCheck

Сертификат ФСТЭК

Реестр Российского ПО

Процедуры обновления, база уязвимостей и конфигураций сертифицированы ФСТЭК наравне с базовыми функциями САЗ.

Плановое и постоянное внесение изменений в сертифицированную версию новых функций.

Соответствие Приказам ФСТЭК №17, №21, №31, 239

В Реестре Российского ПО с 16 мая 2016 г., №765

История развития рынка САЗ в России

2003

Первые коммерческие продажи сканера Xspider

2003 -2015

Развитие отечественных САЗ. Приход иностранных вендоров. САЗ выполняют функции поиска уязвимостей на рабочих станциях и серверах

2015 -2022

Интеграция со смежными системами (SIEM). САЗ сканируют уязвимости промышленного оборудования

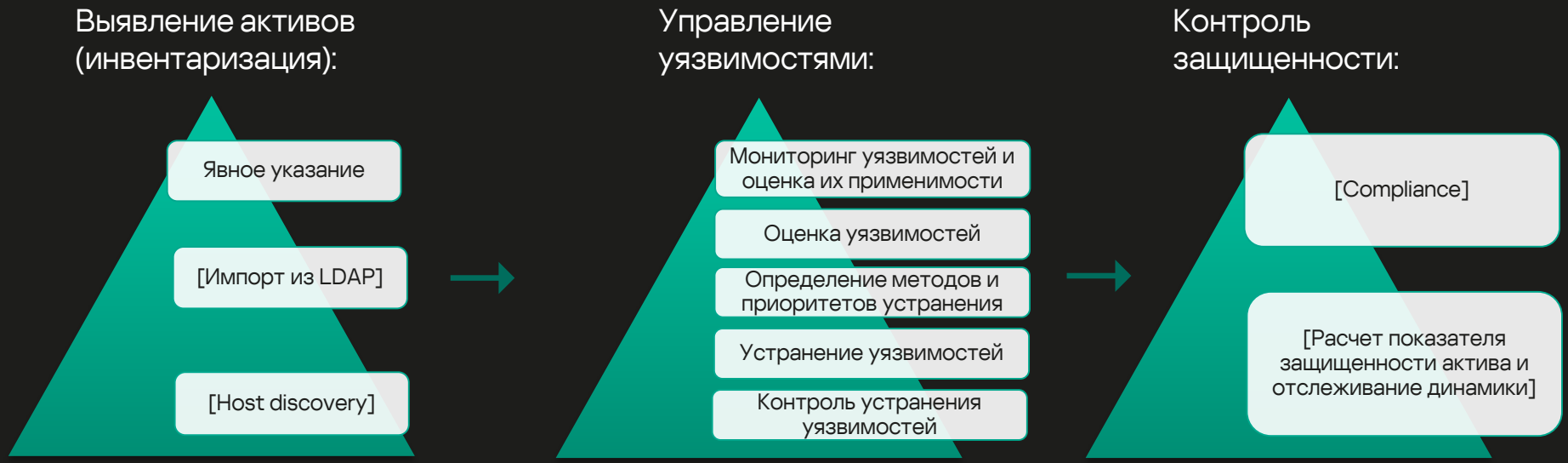
2022

Уход иностранных сканеров

2022 – н. в.

САЗ из коробки реализуют цикл VM. Тесная интеграция с комплексными XDR (EDR)-системами

Функции инфраструктурного сканера безопасности (САЗ)



Типы уязвимостей по ГОСТ Р 56546-2015

Тип уязвимости	Причина появления	Как выявляется	Как устраняется
Уязвимость кода	Ошибка разработчика.	1. Известные уязвимости по правилу определения (сигнатура). 2. Эвристические методы поиска уязвимостей. 3. Pentest.	Устранение – установка обновлений. Компенсирующие меры, например, за счет применения жестких значений параметров безопасности и контроль их значений
Уязвимость конфигурации	Отсутствие руководства по безопасной настройке. Ошибочные настройки ПО пользователя или пренебрежение таковой	Аудит конфигураций безопасности	Настройка параметров на значения (диапазоны значений), указанные в конфигурациях
Архитектурная уязвимость	Уязвимость, появившаяся в процессе проектирования информационной системы	Может быть косвенно выявлена в результате поиска уязвимостей	Заменить ПО с большим количеством уязвимостей, EOL и т.д.
Организационная уязвимость	Отсутствие организационных мер ЗИ в ИС и (или) несоблюдение правил эксплуатации, в т.ч. неверное использование САЗ или их неиспользование	Технически, как правило, не выявляется	Внедрение требуемых организационных мер и регламентов

Сетевой сканер

[Вспомогательные и сервисные функции]

- [аудит обновлений]
- [контроль целостности]
- [API]

Собственная разработка

- ✓ **Несколько режимов сканирования: агент, безагент, легкий агент**
- ✓ **Несколько уровней привилегий**

Условно свободно распространяемый сетевой сканер

- ✓ **1 режим сканирования**
- ✓ **Как правило, 1 уровень привилегий**

База данных уязвимостей и проверок

Собственная база

- ✓ Собственные идентификаторы со связями на другие источники: CVE, БДУ, ФСТЭК, бюллетени НКЦКИ
- ✓ Экспертиза и предопределение метрик уязвимостей (Temporal, Environmental CVSS)
- ✓ [Открытый репозиторий уязвимостей]

Заимствованная база или ее отсутствие

- ✓ Неопределенная мощность сканирования (количество потенциально детектируемых уязвимостей) по каждому поддерживаемому продукту
- ✓ Атрибуты уязвимостей не меняются в течение жизненного цикла

Варианты реализации аудита защищённости

- На основе собственных компетенций, а также доступных отечественных отрытых сервисов.
- Аудит и оценка защищенности с использованием САЗ
- XDR (EDR), SIEM-системы с функциями оценки защищенности

База данных Регулятора и Репозиторий САЗ, в чём разница?

	Свободная база данных и сервисы Регулятора	Репозиторий САЗ
Цель создания	1. Повышение информированности о существующих угрозах и уязвимостях.	1. Ссылки на описания уязвимостей из отчётов САЗ. 2. Определение реальной мощности сканирования каждого программного продукта без использования сканера в том числе и для экспертов, контролирующих органов. 3. Публикация правила детектирования уязвимости в формате OVAL
Сервисы	1. Бесплатные утилиты для локального поиска уязвимостей операционных систем и некоторого общесистемного ПО. 2. Списки уязвимостей с атрибутами в формате электронных таблиц и XML.	Экспорт правил определения уязвимостей формате OVAL для использования в любом сканере или для разработки на их основе собственных правил детектирования.
Источники сведений	1. Для отечественных продуктов – списки уязвимостей, полученные от вендора. 2. Для иностранных продуктов – данные общедоступных источников.	Собственная экспертиза, коррелированная с данными вендора, общедоступных источников.
Что даёт для конечного пользователя	Информацию о том, насколько «ответственно» относится вендор к публикации информации о уязвимостях своих продуктов, информация об обновлениях и бюллетенях безопасности.	Экспертная оценка потенциального списка известных уязвимостей для того или иного продукта.

Преимущества использования сканера с открытым форматом описания уязвимостей и проверок безопасности (OVAL, XCCDF)

- Нет зависимости от определённого вендора САЗ.
- Простота миграции на свободно распространяемое ПО или другой сканер с поддержкой SCAP.
- Проще передавать данные в смежные XDR (EDR), SIEM-системы, собственные разработки.

SCAP (Security Content Automation Protocol)

SCAP (Security Content Automation Protocol)

Классификаторы	Языки описаний	Метрики	Форматы отчётов	Целостность
• Common Platform Enumeration (CPE) • Software Identification (SWID) • **Common Configuration Enumeration (CCE)** • **Common Vulnerabilities and Exposures (CVE)**	• **Extensible Configuration Checklist Description Format (XCCDF)** • **Open Vulnerability and Assessment** Language (OVAL) • Open Checklist Interactive Language (OCIL)	• **Common Vulnerability Scoring System (CVSS)** • **Common Configuration Scoring System (CCSS)**	• Asset Reporting Format (ARF) • Asset Identification (AI)	• Trust Model for Security Automation Data (TMSAD)

Как определять уязвимости АСУ ТП. Декомпозиция на компоненты ПО и оборудование

Siemens AG

АСУ ТП

Simatic WinCC
Simatic STEP7
Simatic PCS7
Simatic Sicam PAS

ПЛК

Simatic S7-200
300, 1200, 1500

ПО

Siemens ALM
(Менеджер
Лицензий)

Schneider Electric

АСУ ТП

Wonderware InTouch
Wonderware Application
Server
Wonderware Information
Server
Wonderware InTouch Access
Anywhere
Wonderware InTouch
Historian
Citect SCADA
Citect Historian
Citect Anywhere

ПЛК

Modicon PLC

Открытый репозиторий OVAL-определений OVALdb

Список уязвимостей в БД сканера для конкретного оборудования (компонента ПО)

OVAL > OVAL определения

Критерии поиска: Продукт: Simatic S7-1200

Страница 1 из 2 (Всего элементов: 44) 1 2

OVALid	Версия	Название	Класс
oval:ru.altx-soft.scada:def:10	4	Уязвимость микропрограммного обеспечения программно-аппаратного обеспечения АСУ фирмы Siemens (CVE-2017-12741)	уязвимость
oval:ru.altx-soft.scada:def:15	3	Уязвимость микропрограммного обеспечения программируемых логических контроллеров SIMATIC S7-1200 (CVE-2018-13800)	уязвимость
oval:ru.altx-soft.scada:def:17	4	Уязвимость микропрограммного обеспечения программируемых логических контроллеров Siemens Simatic S7-1200 (CVE-2018-13815)	уязвимость
oval:ru.altx-soft.scada:def:47	3	Уязвимость микропрограммного обеспечения Siemens SIMATIC S7-1200 (CVE-2012-3037)	уязвимость
oval:ru.altx-soft.scada:def:50	4	Уязвимость веб-сервера Siemens SIMATIC S7-1200 (CVE-2012-3040)	уязвимость
oval:ru.altx-soft.scada:def:51	4	Уязвимость программного обеспечения PROFINET DCP Siemens (CVE-2017-2680)	уязвимость
oval:ru.altx-	4	Уязвимость программного обеспечения PROFINET DCP Siemens (CVE-2017-2681)	уязвимость

Открытый репозиторий OVAL-определений OVALdb

Правило детектирования уязвимости

Критерии

Раскрыть всё | Свернуть всё

OR

CRITERION cpe:2.3:[oh]:siemens:simatic_s7-1200:.*

VARIABLE_TEST (ID = oval:ru.altx-soft.scada:tst:20) comment=cpe:2.3:[oh]:siemens:simatic_s7-1200:.*, check=at least one, check_existence=at_least_one_exists, version=3

variable_object (ID = oval:ru.altx-soft.scada:obj:1)

var_ref oval:ru.altx-soft.scada:var:1

variable_state (ID = oval:ru.altx-soft.scada:ste:20)

value *datatype=string | operation=pattern match | entity_check=at least one | value=^cpe:2.3:[oh]:siemens:simatic_s7-1200:.*$*

CRITERION cpe:2.3:[oh]:siemens:simatic_s7-1500:.*

VARIABLE_TEST (ID = oval:ru.altx-soft.scada:tst:24) comment=cpe:2.3:[oh]:siemens:simatic_s7-1500:.*, check=at least one, check_existence=at_least_one_exists, version=3

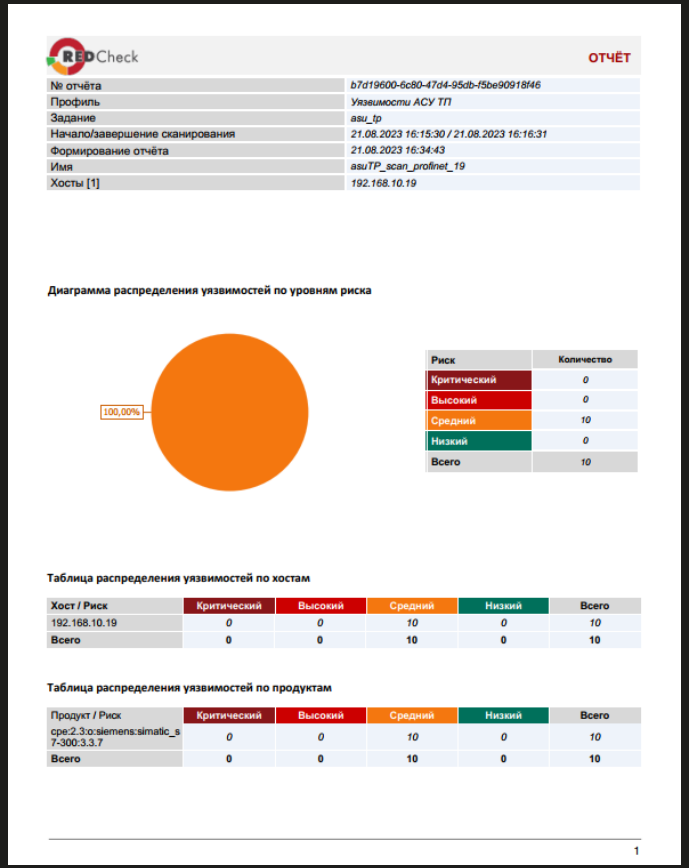
variable_object (ID = oval:ru.altx-soft.scada:obj:1)

var_ref oval:ru.altx-soft.scada:var:1

variable_state (ID = oval:ru.altx-soft.scada:ste:24)

value *datatype=string | operation=pattern match | entity_check=at least one | value=^cpe:2.3:[oh]:siemens:simatic_s7-1500:.*$*

Сводная диаграмма.
Распределение уязвимостей по критичности



RED Check ОТЧЁТ

№ отчёта	b7d19600-6c80-47d4-95db-f5be90918f46
Профиль	Уязвимости АСУ ТП
Задание	asu_tp
Начало/завершение сканирования	21.08.2023 16:15:30 / 21.08.2023 16:16:31
Формирование отчёта	21.08.2023 16:34:43
Имя	asuTP_scan_profinet_19
Хосты [1]	192.168.10.19

Диаграмма распределения уязвимостей по уровням риска

Риск	Количество
Критический	0
Высокий	0
Средний	10
Низкий	0
Всего	10

Таблица распределения уязвимостей по хостам

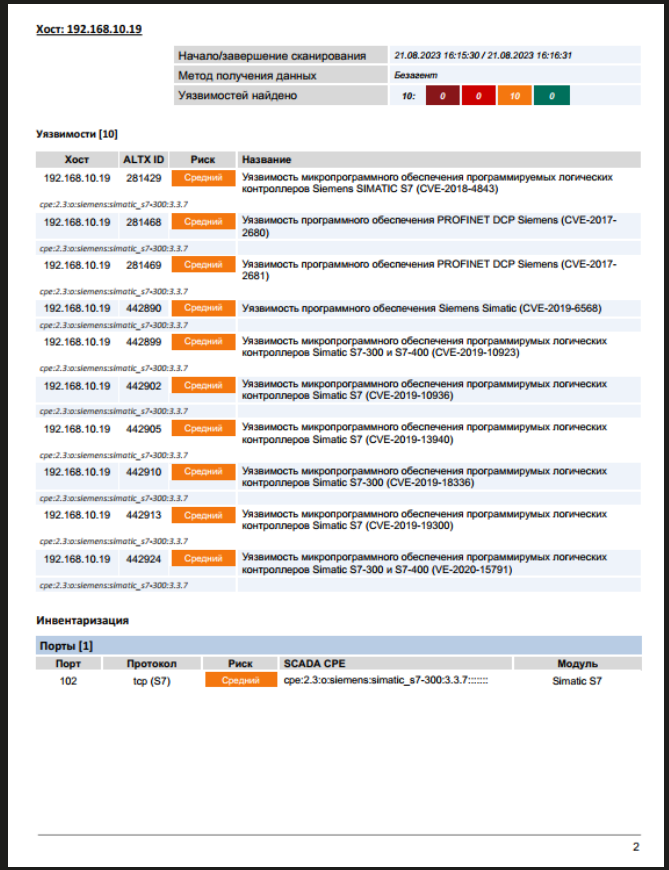
Хост / Риск	Критический	Высокий	Средний	Низкий	Всего
192.168.10.19	0	0	10	0	10
Всего	0	0	10	0	10

Таблица распределения уязвимостей по продуктам

Продукт / Риск	Критический	Высокий	Средний	Низкий	Всего
cpe:2.3:o:siemens:simatic_s7-300:3.3.7	0	0	10	0	10
Всего	0	0	10	0	10

1

Общий список уязвимостей



Хост: 192.168.10.19

Начало/завершение сканирования	21.08.2023 16:15:30 / 21.08.2023 16:16:31
Метод получения данных	Безагент
Уязвимостей найдено	10: 0 0 10 0

Уязвимости [10]

Хост	ALTX ID	Риск	Название
192.168.10.19	281429	Средний	Уязвимость микропрограммного обеспечения программируемых логических контроллеров Siemens SIMATIC S7 (CVE-2018-4843)
cpe:2.3:o:siemens:simatic_s7-300:3.3.7			
192.168.10.19	281468	Средний	Уязвимость программного обеспечения PROFINET DCP Siemens (CVE-2017-2680)
cpe:2.3:o:siemens:simatic_s7-300:3.3.7			
192.168.10.19	281469	Средний	Уязвимость программного обеспечения PROFINET DCP Siemens (CVE-2017-2681)
cpe:2.3:o:siemens:simatic_s7-300:3.3.7			
192.168.10.19	442890	Средний	Уязвимость программного обеспечения Siemens Simatic (CVE-2019-6568)
cpe:2.3:o:siemens:simatic_s7-300:3.3.7			
192.168.10.19	442899	Средний	Уязвимость микропрограммного обеспечения программумых логических контроллеров Simatic S7-300 и S7-400 (CVE-2019-10923)
cpe:2.3:o:siemens:simatic_s7-300:3.3.7			
192.168.10.19	442902	Средний	Уязвимость микропрограммного обеспечения программумых логических контроллеров Simatic S7 (CVE-2019-10936)
cpe:2.3:o:siemens:simatic_s7-300:3.3.7			
192.168.10.19	442905	Средний	Уязвимость микропрограммного обеспечения программумых логических контроллеров Simatic S7 (CVE-2019-13940)
cpe:2.3:o:siemens:simatic_s7-300:3.3.7			
192.168.10.19	442910	Средний	Уязвимость микропрограммного обеспечения программумых логических контроллеров Simatic S7-300 (CVE-2019-18336)
cpe:2.3:o:siemens:simatic_s7-300:3.3.7			
192.168.10.19	442913	Средний	Уязвимость микропрограммного обеспечения программумых логических контроллеров Simatic S7 (CVE-2019-19300)
cpe:2.3:o:siemens:simatic_s7-300:3.3.7			
192.168.10.19	442924	Средний	Уязвимость микропрограммного обеспечения программумых логических контроллеров Simatic S7-300 и S7-400 (VE-2020-15791)
cpe:2.3:o:siemens:simatic_s7-300:3.3.7			

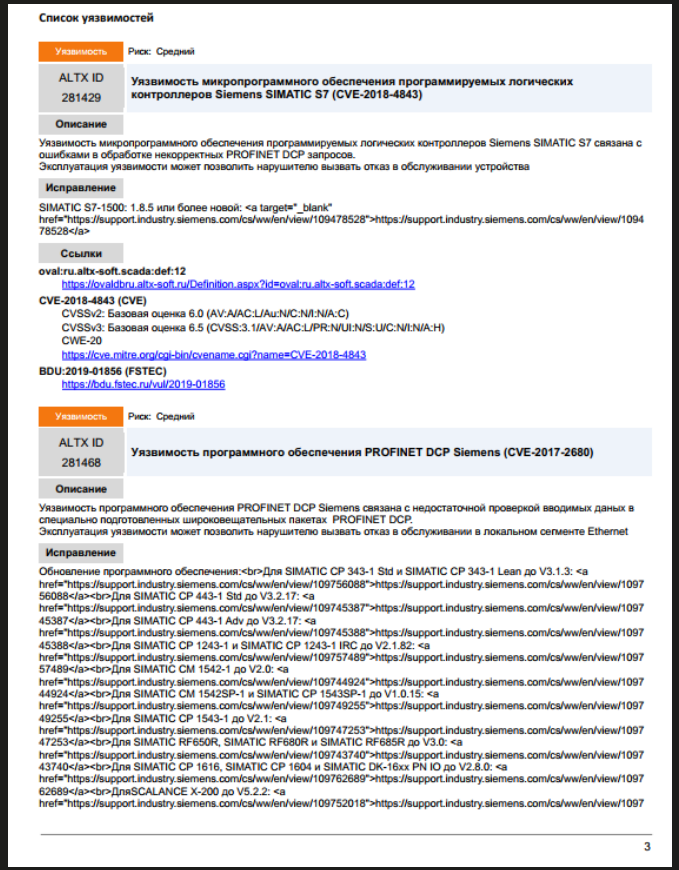
Инвентаризация

Порты [1]

Порт	Протокол	Риск	SCADA CPE	Модуль
102	tcp (S7)	Средний	cpe:2.3:o:siemens:simatic_s7-300:3.3.7::::::	Simatic S7

2

Меры по устранению уязвимостей



Список уязвимостей

Уязвимость | Риск: Средний

ALTX ID 281429 — **Уязвимость микропрограммного обеспечения программируемых логических контроллеров Siemens SIMATIC S7 (CVE-2018-4843)**

Описание

Уязвимость микропрограммного обеспечения программируемых логических контроллеров Siemens SIMATIC S7 связана с ошибками в обработке некорректных PROFINET DCP запросов.
Эксплуатация уязвимости может позволить нарушителю вызвать отказ в обслуживании устройства

Исправление

SIMATIC S7-1500: 1.8.5 или более новой: https://support.industry.siemens.com/cs/ww/en/view/109478528

Ссылки

oval:ru.altx-soft.scada:def:12
https://ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.scada:def:12

CVE-2018-4843 (CVE)
CVSSv2: Базовая оценка 6.0 (AV:A/AC:L/Au:N/C:N/I:N/A:C)
CVSSv3: Базовая оценка 6.5 (CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)
CWE-20
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-4843

BDU:2019-01856 (FSTEC)
https://bdu.fstec.ru/vul/2019-01856

Уязвимость | Риск: Средний

ALTX ID 281468 — **Уязвимость программного обеспечения PROFINET DCP Siemens (CVE-2017-2680)**

Описание

Уязвимость программного обеспечения PROFINET DCP Siemens связана с недостаточной проверкой вводимых даных в специально подготовленных широковещательных пакетах PROFINET DCP.
Эксплуатация уязвимости может позволить нарушителю вызвать отказ в обслуживании в локальном сегменте Ethernet

Исправление

Обновление программного обеспечения:
Для SIMATIC CP 343-1 Std и SIMATIC CP 343-1 Lean до V3.1.3: https://support.industry.siemens.com/cs/ww/en/view/109756088
Для SIMATIC CP 443-1 Std до V3.2.17: https://support.industry.siemens.com/cs/ww/en/view/109745387
Для SIMATIC CP 443-1 Adv до V3.2.17: https://support.industry.siemens.com/cs/ww/en/view/109745388
Для SIMATIC CP 1243-1 и SIMATIC CP 1243-1 IRC до V2.1.82: https://support.industry.siemens.com/cs/ww/en/view/109757489
Для SIMATIC CM 1542-1 до V2.0: https://support.industry.siemens.com/cs/ww/en/view/109744924
Для SIMATIC CM 1542SP-1 и SIMATIC CP 1543SP-1 до V1.0.15: https://support.industry.siemens.com/cs/ww/en/view/109749255
Для SIMATIC CP 1543-1 до V2.1: https://support.industry.siemens.com/cs/ww/en/view/109747253
Для SIMATIC RF650R, SIMATIC RF680R и SIMATIC RF685R до V3.0: https://support.industry.siemens.com/cs/ww/en/view/109743740
Для SIMATIC CP 1616, SIMATIC CP 1604 и SIMATIC DK-16xx PN IO до V2.8.0: https://support.industry.siemens.com/cs/ww/en/view/109762689
ДляSCALANCE X-200 до V5.2.2: <a href="https://support.industry.siemens.com/cs/ww/en/view/109752018">https://support.industry.siemens.com/cs/ww/en/view/109

3

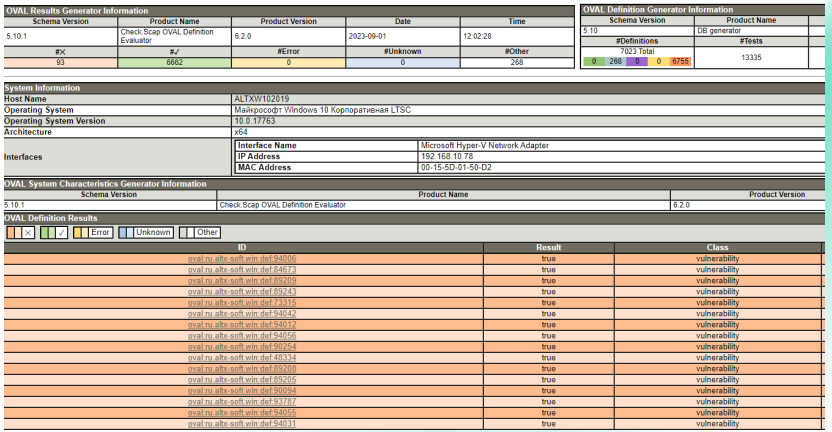
Если вы выбираете поставщика (разработчика) описаний уязвимостей
и конфигурации параметров безопасности (Compliance) в отрытых форматах OVAL, XCCDF

1. Использование коммерческого сканера

2. Использование свободного ПО: OpenSCAP, OVALdi

3. Использование XDR (ERP), SIEM

Результаты проверок в стандартизированном виде XML (HTML)



OVAL Results Generator Information

Schema Version	Product Name	Product Version	Date	Time
5.10.1	Check.Scap OVAL Definition Evaluator	6.2.0	2023-09-01	12:02:28

#X	#✓	#Error	#Unknown	#Other
93	6662	0	0	268

OVAL Definition Generator Information

Schema Version	Product Name
5.10	DB generator

#Definitions	#Tests
7023 Total: 0 268 0 0 6755	13335

System Information

Host Name	ALTXW102019
Operating System	Майкрософт Windows 10 Корпоративная LTSC
Operating System Version	10.0.17763
Architecture	x64
Interfaces	Interface Name: Microsoft Hyper-V Network Adapter IP Address: 192.168.10.78 MAC Address: 00-15-5D-01-50-D2

OVAL System Characteristics Generator Information

Schema Version	Product Name	Product Version
5.10.1	Check.Scap OVAL Definition Evaluator	6.2.0

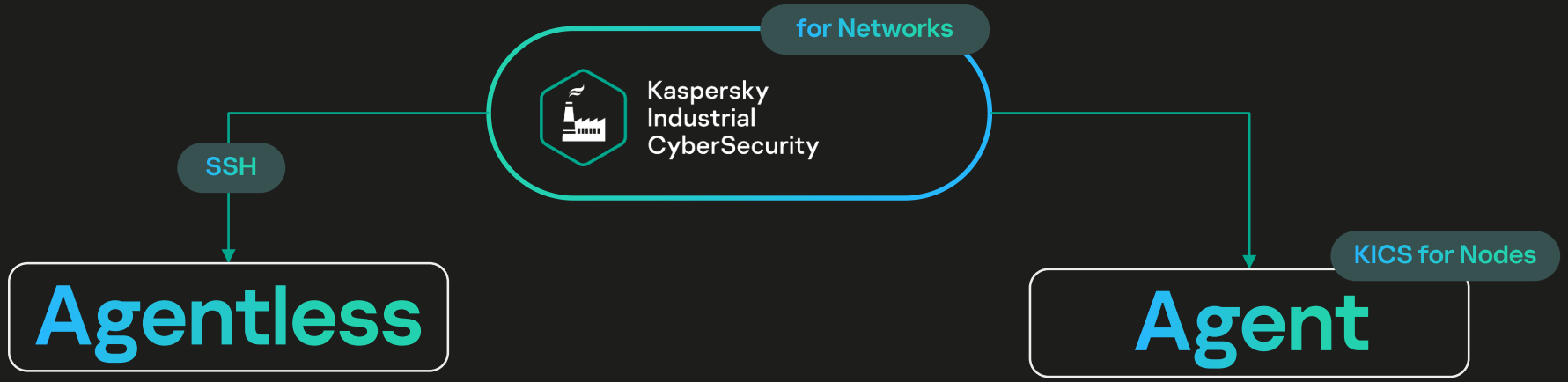
OVAL Definition Results

✗ | ? | ✓ | Error | Unknown | Other

ID	Result	Class
oval:ru.altx-soft.win:def:94006	true	vulnerability
oval:ru.altx-soft.win:def:84673	true	vulnerability
oval:ru.altx-soft.win:def:89209	true	vulnerability
oval:ru.altx-soft.win:def:89243	true	vulnerability
oval:ru.altx-soft.win:def:73315	true	vulnerability
oval:ru.altx-soft.win:def:94042	true	vulnerability
oval:ru.altx-soft.win:def:94017	true	vulnerability
oval:ru.altx-soft.win:def:94056	true	vulnerability
oval:ru.altx-soft.win:def:89254	true	vulnerability
oval:ru.altx-soft.win:def:48334	true	vulnerability
oval:ru.altx-soft.win:def:89208	true	vulnerability
oval:ru.altx-soft.win:def:89205	true	vulnerability
oval:ru.altx-soft.win:def:90094	true	vulnerability
oval:ru.altx-soft.win:def:93787	true	vulnerability
oval:ru.altx-soft.win:def:94055	true	vulnerability
oval:ru.altx-soft.win:def:94031	true	vulnerability

```
<?xml version="1.0" encoding="UTF-8"?>
- <oval_results xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:oval="http://oval.mitre.org/XMLSchema/oval-common-5"
xmlns="http://oval.mitre.org/XMLSchema/oval-results-5">
  - <generator>
      <oval:product_name>Check.Scap OVAL Definition Evaluator</oval:product_name>
      <oval:product_version>6.1.1</oval:product_version>
      <oval:schema_version>5.10.1</oval:schema_version>
      <oval:timestamp>2023-02-14T18:22:57</oval:timestamp>
    </generator>
  - <directives include_source_definitions="false">
      <definition_true reported="true" content="full"/>
      <definition_false reported="true" content="full"/>
      <definition_unknown reported="true" content="full"/>
      <definition_error reported="true" content="full"/>
      <definition_not_evaluated reported="true" content="full"/>
      <definition_not_applicable reported="true" content="full"/>
    </directives>
  - <results>
    - <system>
      - <definitions>
        - <definition version="15" class="compliance" result="true" definition_id="oval:ru.altx-soft.nix:def:26124">
          - <criteria result="true" operator="AND">
              <criterion version="1" result="true" test_ref="oval:ru.altx-soft.nix:tst:22278"/>
            </criteria>
          </definition>
        - <definition version="11" class="compliance" result="false" definition_id="oval:ru.altx-soft.nix:def:26082">
          - <criteria result="false" operator="AND">
              <criterion version="1" result="false" test_ref="oval:ru.altx-soft.nix:tst:22189"/>
              <extend_definition version="1" result="true" definition_ref="oval:ru.altx-soft.nix:def:23103"/>
            </criteria>
```

Centralized system for automated security audit



Workstations and Servers Configuration:

Linux security settings (XCCDF)

Network devices Configuration:

Active network equipment

Workstations and Servers Configuration:

Windows security settings (XCCDF)

Vulnerabilities:

ICS software inventory and vulnerability detection

Конфигурации в формате XCCDF разработки АЛТЭКС-СОФТ в составе KICS

Клиентские и серверные операционные системы Microsoft

Linux ОС (в т.ч. и российские ROSA Linux, Ред ОС, Альт Линукс, Astra Linux и др.)

Средства виртуализации и контейнеризации и оркестрации (Vmware, docker, Kubernetes и др.)

Отечественные наложенные СЗИ от НСД (Secret Net, Secret Studio, Dallas Lock и др.), криптопровайдеры (КриптоПро CSP)

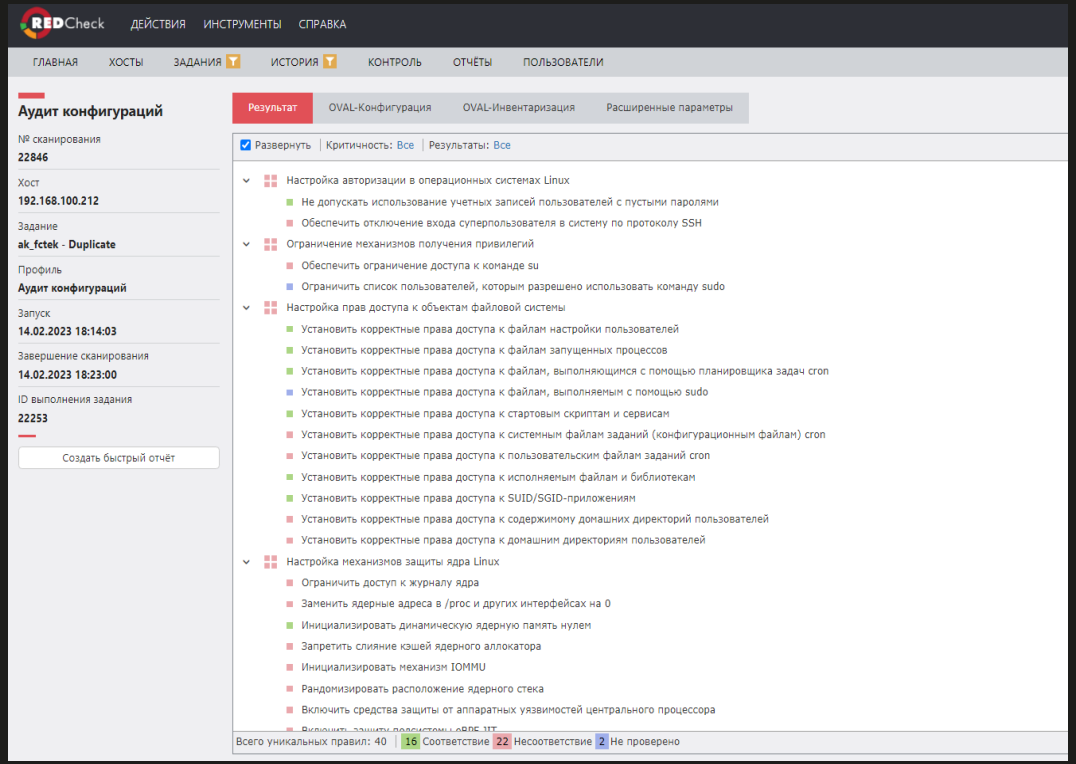
СУБД (MySQL, Postgres, SQL Server, Oracle)

Web-сервера, сервера приложений и framework (Apache, .Net, PHP и др.)

Всего 90 конфигураций на соответствие приказам Регуляторов, экспертные best practice от АЛТЭКС-СОФТ

Конфигурация безопасности «Linux - Рекомендации по безопасной настройке - ФСТЭК России, ИО от 30 декабря 2022 г. N 240/22/6933». Результат выполнения

Дерево проверок конфигурации в формате XCCDF

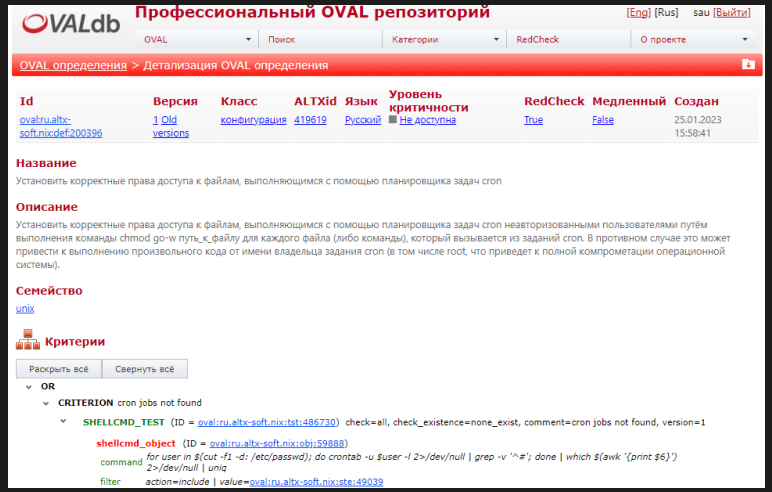


Конфигурация безопасности «Linux - Рекомендации по безопасной настройке - ФСТЭК России, ИО от 30 декабря 2022 г. N 240/22/6933». Результат выполнения.

Детализация проверки и правило её определения в формате XCCDF

	ALTX ID	Название
⌄	419619	Установить корректные права доступа к файлам, выполняющимся с помощью планировщика задач cron

ALTX ID 419619
OVAL oval:ru.altx-soft.nix:def:200396 (Версия 1)
Название Установить корректные права доступа к файлам, выполняющимся с помощью планировщика задач cron
Описание Установить корректные права доступа к файлам, выполняющимся с помощью планировщика задач cron неавторизован
вызывается из заданий cron. В противном случае это может привести к выполнению произвольного кода от имени влад
Детализация
Показать собранные OVAL-элементы



Спасибо за внимание!

REDCheck

Чат-группа в Telegram
@REDCHECK_COM

Сергей Уздемир
sau@altx-soft.ru

kaspersky