Мониторинг событий ИБ АСУ ТП

Ростелеком
Солар

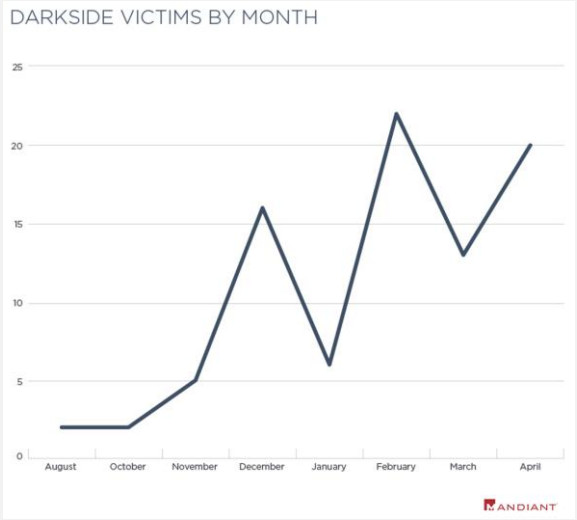
Уровни злоумышленников

	УСЛОВНАЯ КАТЕГОРИЯ НАРУШИТЕЛЯ	ТИПОВЫЕ ЦЕЛИ	ВОЗМОЖНОСТИ НАРУШИТЕЛЯ
1	Автоматизированные системы	Взлом устройств и инфраструктур с низким уровнем защиты для дальнейшей перепродажи или использования в массовых атаках	Автоматизированное сканирование
2	Киберхулиган/ энтузиаст-одиночка	Хулиганство, нарушение целостности инфраструктуры	Официальные и open-source-инструменты для анализа защищенности
3	Киберкриминал/ организованные группировки	Приоритетная монетизация атаки – шифрование, майнинг, вывод денежных средств	Кастомизированные инструменты, доступное вредоносное ПО (приобретение, обфускация или разработка), доступные уязвимости, соц. инжиниринг
4	Кибернаемники/ Продвинутые группировки	Нацеленность на заказные работы – сбор информации, шпионаж в интересах конкурентов, последующая крупная монетизация, хактивизм, деструктивные действия	Самостоятельно разработанные инструменты, приобретенные zero-day-уязвимости ПО
5	Кибервойска/ Прогосударственные группировки	Кибершпионаж, полный захват инфраструктуры для возможности контроля и применения любых действий и подходов, хактивизм	Самостоятельно найденные zero-day-уязвимости ПО, разработанные и внедренные "закладки"

История с Darkside

- Darkside – RaaS-оператор и разработчик ВПО (вируса-шифровальщик**а**)
- Основные цели – компании США из разных отраслей (финансы, промышленность, консалтинг, розничная **торговля** и технологический сектор)
- Типовые последствия – кража данных и шифрование инфраструктуры
- Атака на Colonial Pipeline – выкуп **около 5** млн **$**

Colonial Pipeline Company



Кол-во инцидентов Darkside (08.20 – 04.21)

Ростелеком
Солар

История с Darkside. Хронология событий

Закрепление

- Бэкдоры (SmokedHam)
- F-secure C3

Исследование инфраструктуры

- Встроенные Windows-утилиты
- PowerView
- Сканеры

Первичная компрометация

- Атаки на VPN-шлюзы (подбор пароля)
- CVE-2021-20016 (Sonicwall SSLVPN)
- Фишинг

Повышение привилегий

- CVE-2020-1472 (Zerologon)
- Mimikatz
- LSASS и дампы памяти

Нанесение ущерба

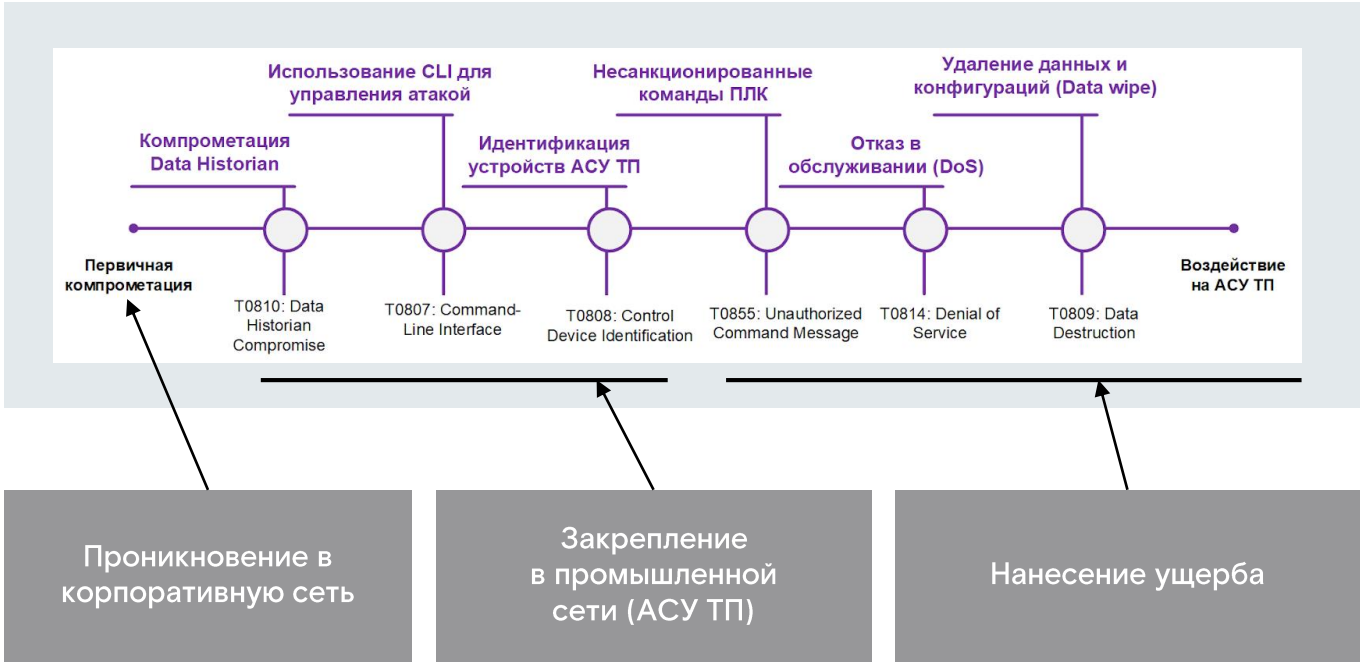
- PsExec (установка и запуск ВПО)
- Копирование данных (Rclone WinSCP)

Типовая атака на АСУ ТП

Украина, 2016 год

Атака INDUSTROYER на подстанцию «Пивнична»

Последствия: отключение электроэнергии



Ростелеком
Солар

Разделы

Организация мониторинга

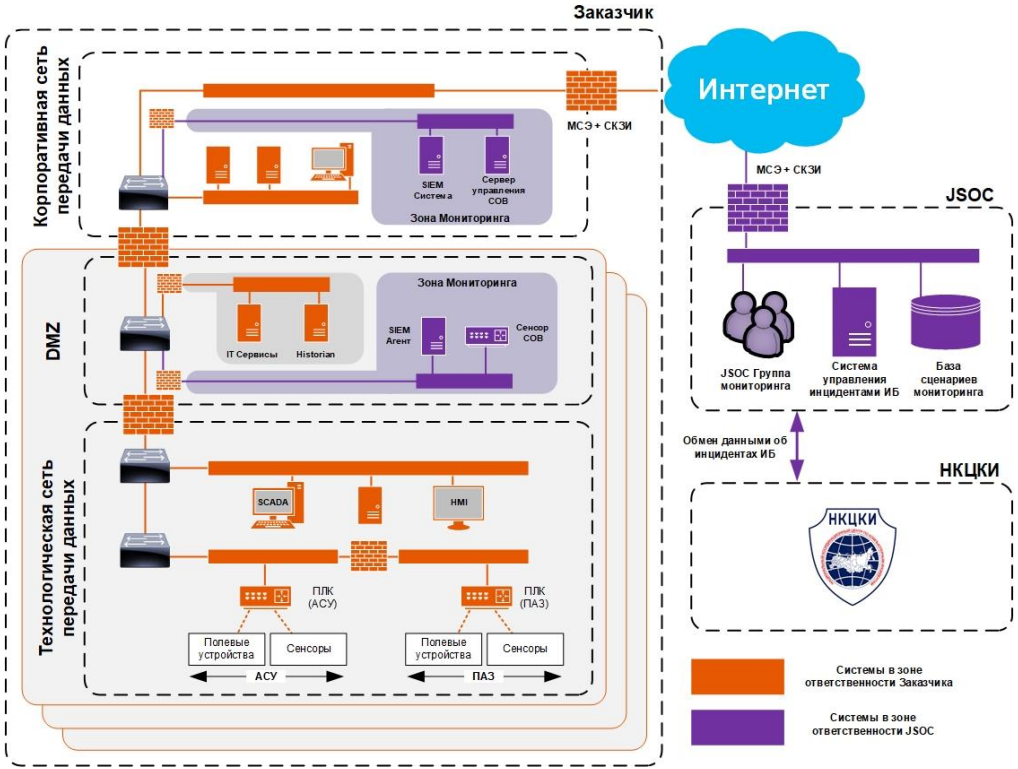
Ростелеком
Солар

Как подключить АСУ ТП к SOC?

Позволяет видеть аномалии в работе узлов промышленной сети (АРМ, серверы, сетевое оборудование)

Позволяет определять атаки на уровне сетевых протоколов и сетевого взаимодействия

Общая схема решения



- **Анализ событий (SIEM) + Анализ сетевого трафика (СОВ)**
- **Гибридный или облачный вариант подключения к JSOC**
- **Взаимодействие с НКЦКИ**

Solar JSOC OT: пакеты сценариев детектирования

Набор сценариев детектирования	Начальный	Стандартный	Продвинутый	Полный
Описание сценариев	• Brute force • Контроль учетных данных • Профилирование • Внешние атаки и т. д.	• Подключение съемных носителей информации • Контроль доступа • (ИТ/ОТ) • Сканирование сети • Вредоносное ПО	• Рестарт процесса • Рестарт контроллера • Контрольные суммы	• Отклонение системы от нормального профиля работы • Изменение критичных параметров проектов и т. д.
Типовые источники событий	АРМ персонала Серверы SCADA/Historian/AD Сетевое оборудование	МСЭ, СОВ, САЗ, РАМ, средства контроля целостности и т. д.	Журналы событий ПЛК, РСУ, ПАЗ	Журналы событий прикладного программного обеспечения

Уровень злоумышленника

- Уровень 5. Кибервойска
- Уровень 4. Кибернаемники
- Уровень 3. Киберкриминал
- Уровень 2. Киберхулиганы
- Уровень 1. Боты

Ростелеком
Солар

Линии аналитиков Solar JSOC

1-я

Задачи

Обработка и расследование **типовых** инцидентов

Построение типовых отчетов

Обработка базовых запросов заказчиков

Приемка новых заказчиков/сценариев

Компетенции

Знание основных механизмов и систем ИТ и ИБ

Умение читать логи

Владение основным инструментарием SIEM

Работа по инструкции (но не ограничиваясь ей)

2-я

Задачи

Обработка и расследование **нетиповых** инцидентов

Построение нетиповых отчетов

Обработка запросов заказчиков

Эскалация по экспертизе с 1-й линии (консультации)

Приемка новых заказчиков/сценариев

Компетенции

Опыт работы на 1-й линии Solar JSOC

Свободное владение всем инструментарием SIEM и др.

«Свободное плавание» при расследовании

3-я (react)

Задачи

Добавление исключений по обратной связи

Работа с контентом SIEM

Подключение новых источников

Обработка отчетов Threat Intelligence

Дорасследование нетиповых технически сложных инцидентов

Эскалация по экспертизе с 1-й и 2-й линий (консультации)

Компетенции

Опыт работы на 2-й линии Solar JSOC

Уверенное знание основного инструментария расследования

Уверенное знание регулярных выражений (regexp)

Базовые знания скриптотехники (PS, bash, python etc.)

Навыки проведения глубокой аналитики

4-я

Задачи

Реагирование на нетиповые критические инциденты своих заказчиков

Анализ аномальных активностей с целью выявления инцидентов

Участие в расследовании инцидентов ИБ вне профиля сработки сценариев

Разработка новых сценариев выявления инцидентов

Компетенции

Опыт разработки контента в SIEM

TechSkills инженера реагирования x3

Soft Skills

Ростелеком
Солар

Взаимодействие с НКЦКИ

Отчетность перед НКЦКИ

- Отправка информации об активах: расширенная информация о периметре
- Отправка информации о состоянии защищенности
- Отправка информации по инцидентам: выявление, разбор, противодействие
- Направление в НКЦКИ предложений по совершенствованию средств ГосСОПКА

Ответы на запросы НКЦКИ

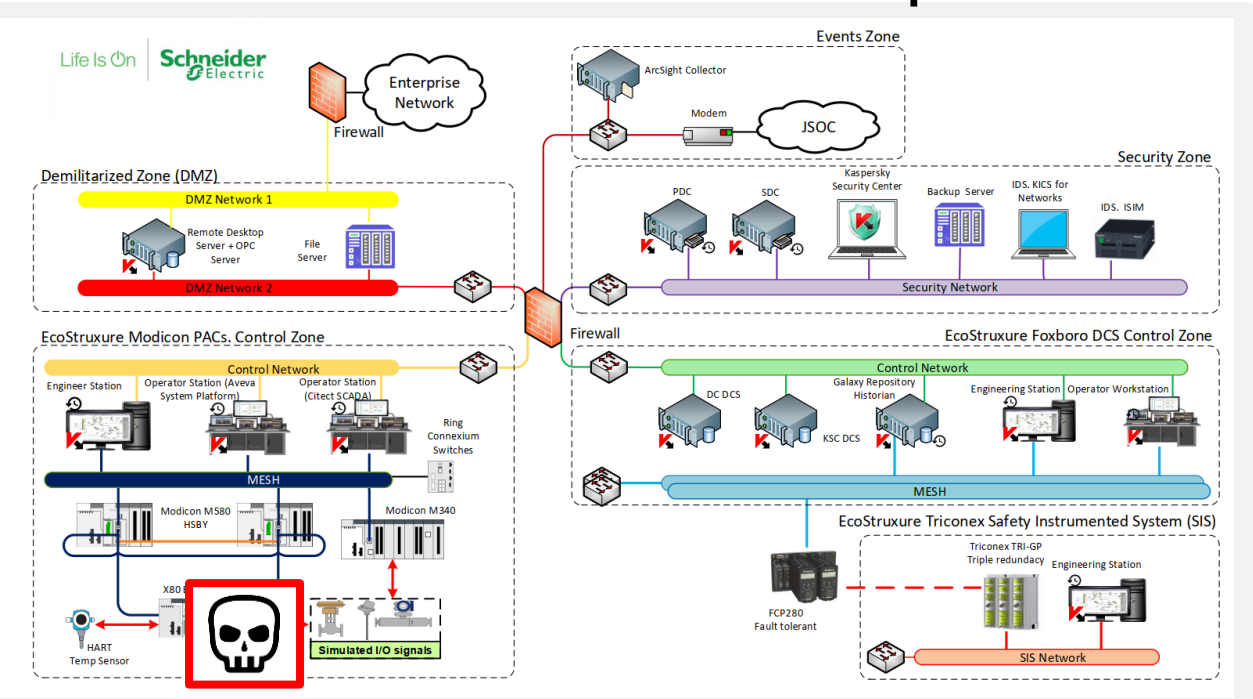
- Актуальная информация о периметре
- Проверка наличия индикаторов в инфраструктуре
- Оперативное принятие мер для противодействия новому вектору

Разделы

Опыт работы с АСУ ТП

Ростелеком
Солар

Schneider Electric – совместное тестирование



- Мониторинг логов (SIEM) и сетевого трафика (COB)
- Интеграция разных линеек оборудования SE: Modicon PLC, FCP, Triconex
- Эмуляция действий злоумышленников (сканирование, brute force, взаимодействие с промышленным оборудованием и т. д.)

Логи: сбор событий с ПЛК

Типовые события:

- События аутентификации
- Отключение и включение сервисов (FTP/TFTP/HTTP)
- Изменение состояния ПЛК (run/stop)
- Изменение прошивки ПЛК
- Загрузка нового проекта, конфигурации
- Подключение новых устройств

Возможности логирования очень сильно зависят от модели оборудования и версии прошивки

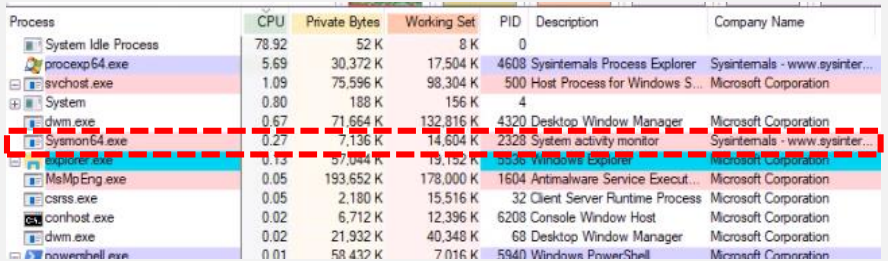
Логи: сбор событий в Windows

Рекомендуем Windows Event Collector (WEC) для сбора событий средствами ОС:

1. Неинвазивный способ (не требует установки дополнительных агентов)

2. Сбор событий Windows, позволяющий определить аномальную активность на АРМ и серверах

3. Порядка 200 сценариев детектирования (RAT, вредоносное ПО, шифровальщики, хакерские утилиты, типовые атаки на Windows-инфраструктуру)

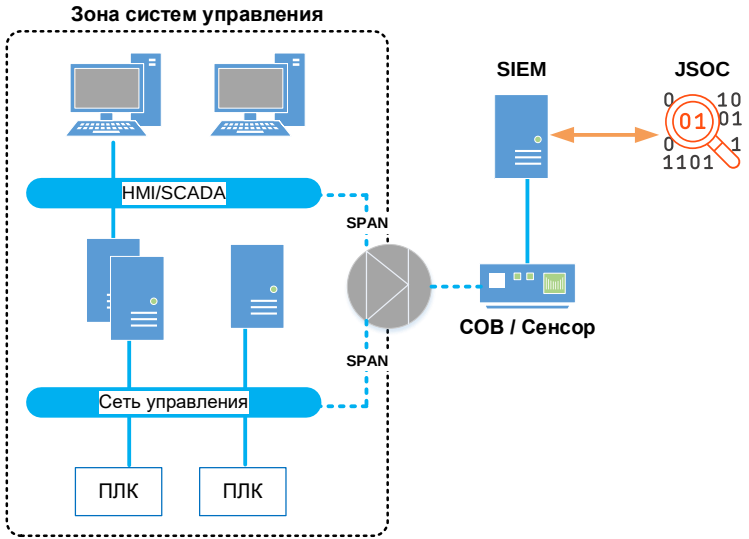


Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
System Idle Process	78.92	52 K	8 K	0		
procexp64.exe	5.69	30,372 K	17,504 K	4608	Sysinternals Process Explorer	Sysinternals - www.sysinter...
svchost.exe	1.09	75,596 K	98,304 K	500	Host Process for Windows S...	Microsoft Corporation
System	0.80	188 K	156 K	4		
dwm.exe	0.67	71,664 K	132,816 K	4320	Desktop Window Manager	Microsoft Corporation
Sysmon64.exe	0.27	7,136 K	14,604 K	2328	System activity monitor	Sysinternals - www.sysinter...
explorer.exe	0.15	97,044 K	79,152 K	5836	Windows Explorer	Microsoft Corporation
MsMpEng.exe	0.05	193,652 K	178,000 K	1604	Antimalware Service Execut...	Microsoft Corporation
csrss.exe	0.05	2,180 K	15,516 K	32	Client Server Runtime Process	Microsoft Corporation
conhost.exe	0.02	6,712 K	12,396 K	6208	Console Window Host	Microsoft Corporation
dwm.exe	0.02	21,932 K	40,348 K	68	Desktop Window Manager	Microsoft Corporation
powershell.exe	0.01	58,432 K	7,016 K	5940	Windows PowerShell	Microsoft Corporation

- Microsoft Windows 2019
- Sysmon
- Атака – загрузка бесфайлового Meterpreter

Пример работы с СОВ

- Работа с копией трафика
- Исключение управляющих воздействий на АСУ ТП
- Четкое разделение зон ответственности между заказчиком и Solar JSOC



Ростелеком
Солар

Контакты

Центральный офис

125009 г. Москва,
Никитский переулок, 7с1

+7 (499) 755-07-70

info@rt-solar.ru

Ростелеком
Солар