Ростелеком
Солар

Опыт построения СОИБ на отечественных решениях. Непросто, но интересно!

Виталий Сиянов
Менеджер
по развитию
направления
«Solar
Интеграция»

Андрей Прошин
Руководитель
направления
Solar JSOC

Трансформация зарубежных СЗИ в России в 2022 году

Было

Стало

Ростелеком Солар

Зрелость российских технологий*

52%

Зрелые и полностью готовые к использованию технологии

27%

Практически готовые к использованию технологии

21%

Технологии в стадии развития

* Аналитическое исследование проведено экспертами направления «Solar Интеграция»

FW/UTM/NGFW | IDS/IPS | NAC | ГОСТ VPN | ANTI-DDOS | WAF | SIEM | AV | EDR/XDR | MFA | СЗИ НСД | ANTI-APT

PIM/PAM | DLP | SWG | IDM | SAST | DAM | VM | MDM | NAD/NTA | DCAP/DAG | CONTAINER SECURITY | HONEYPOT

SEG | VDI | SSO | IRP/SOAR | SGRC | PKI | EPP | HSM | DATA ENCRYPTION | CASB | BACKUP | SCADA SECURITY

Ростелеком Солар

Особенности работы с отечественными решениями

1. Производительность
2. Отказоустойчивость
3. Автоматизация развертывания решений в Linux-среде
4. Отсутствие API
5. Интеграция с российскими ОС и платформами виртуализации
6. Соответствие требованиям
7. Проблема не всегда в безопасности

Отсутствие оборудования

Статья «Семь распространенных проблем при внедрении отечественных средств защиты: практика интегратора»

securitylab.ru/analytics/532718.php

Выбор решений

Ростелеком
Солар

Подготовка технико-коммерческих сравнений

Что нужно сравнить у промышленных СОВ

Основные функциональные требования

- Мониторинг технологических параметров, обнаружение неизвестных тегов, самообучение тегам
- Контроль проектов ПЛК
- Обнаружение изменения установок технологического процесса
- Поддерживаемые протоколы
- Поддержка российских операционных систем

Общие сведения

- Сертификат ФСТЭК
- Сертификат ФСБ
- Проведение аудита жизненного цикла безопасной разработки программного обеспечения

Дополнительный функционал

- Автоматическое построение карты сетевых взаимодействий
- Автоматическое формирование белых списков сетевых соединений
- Интеграция со средством защиты конечных узлов

Стоимость владения

- Стоимость покупки и внедрения
- Стоимость поддержки на 3 или 5 лет

Ростелеком Солар

Таблица сравнения решений

Наименование решения	Наименование группы критериев	Показатель соответствия	Итоговый показатель соответствия
Решение 1	Основные функциональные требования	5,00	18,87
	Дополнительные функциональные возможности	3,00	
	Общие сведения	2,00	
	Стоимостные характеристики	8,87	
Решение 2	Основные функциональные требования	4,22	17,29
	Дополнительные функциональные возможности	2,21	
	Общие сведения	0,86	
	Стоимостные характеристики	10,00	
Решение 3	Основные функциональные требования	3,45	13,19
	Дополнительные функциональные возможности	1,79	
	Общие сведения	0,29	
	Стоимостные характеристики	7,66	

Проверить на стенде

Функциональное тестирование

Нагрузочное тестирование

Совместимость средств защиты

Как заставить технологии работать (на примере OT-SOC)

Общие задачи при построении СОИБ:

#1 Перестроить СОИБ в рамках импортозамещения

#2 Перестроить процессы работы с новым оборудованием/ПО

#3 Накопить экспертизу по работе с продуктами и по новым угрозам

Какая группа киберпреступников может атаковать вас?

profiles.rt-solar.ru/

Ростелеком Солар

#1 Перестроить СОИБ в рамках импортозамещения

Собираем решение

NTA
Аномалии в сетевом трафике АСУ ТП (KICS 4 Networks)

SIEM
События ИБ со всех узлов АСУ ТП

EDR
Защита конечных точек (KICS 4 Nodes)

Выбираем платформу

On-premise
Собственные серверы, СХД, СРК

Облако

MSSP-лицензии
+ защищенное облако Solar JSOC

Сравнение решений по обнаружению атак на АСУ ТП (MITRE)

https://attackevals.mitre-engenuity.org/ics/triton/

Ростелеком Солар

#2 Перестроить процессы работы с новым оборудованием и ПО

Как не утонуть в потоке алертов и продолжать работать с важными событиями ИБ

АСУ ТП
на 1000 узлов
(включая ПЛК)

~500
алертов/мес.

~85% — Несоответствие сетевому профилю (ARP, DNS, TCP, UDP)

~12-14% — Необычная активность в технологических протоколах + изменение конфигураций

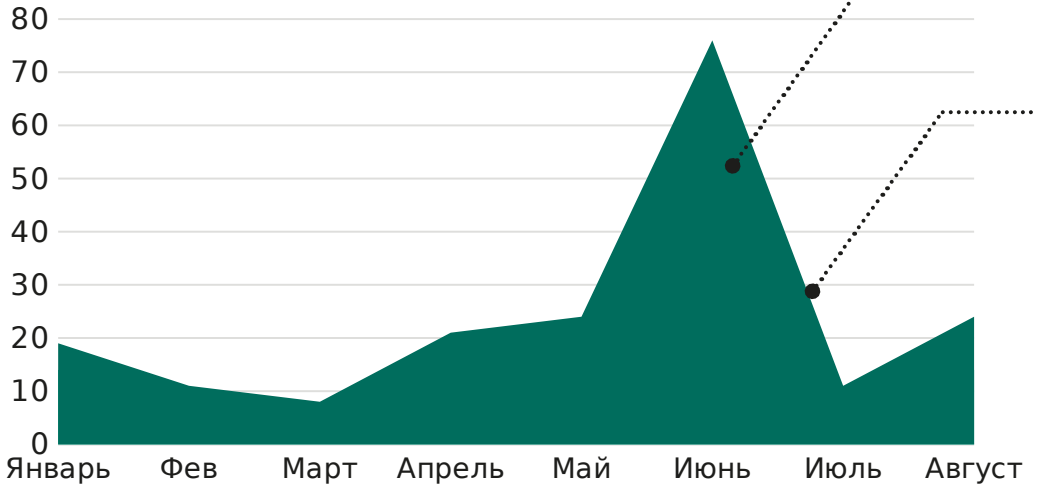
~1-3% — Активность ВПО, сканирование, брутфорсы и т. д.

Ростелеком Солар

#3 Накопить экспертизу по работе с новыми угрозами

Любое СЗИ – это просто инструмент для минимизации рисков, и оно быстро устаревает без постоянной аналитики новых угроз.

Уязвимости АСУ ТП в БДУ ФСТЭК, 2022



Все уязвимости в БДУ ФСТЭК

Сетевые уязвимости (CVSS Network и Adjacent)

Десятки новых сетевых уязвимостей каждый месяц

Отчет по количеству уязвимостей от «Ростелеком-Солар»

rt-solar.ru/events/news/2866/

Как противостоять продвинутым злоумышленникам без отлаженного процесса Threat Hunting?

Ростелеком Солар

Чем может помочь сервисный ИБ-партнер

Сервисы Solar JSOC по защите АСУ ТП

rt-solar.ru/projects/asutp/solarJSOC/

Ростелеком Солар

Обеспечение кибербезопасности высокотехнологичного ИТ-пространства

Что было сделано в рамках проекта:

- Обеспечение безопасности 5000 АРМ
- Предоставление услуг защищенной связи и защищенного виртуального ЦОД
- Предоставление услуг мониторинга и реагирования на инциденты безопасности
- Предоставление услуг ГосСОПКА
- Миграция ИС в облако ПАО «Ростелеком», обеспечение безопасности информации и эксплуатация

Используемые классы решений

- Межсетевые экраны (NGFW)
- Защита от несанкционированного доступа (СЗИ от НСД)
- Защита среды виртуализации (ЗСВ)
- Защита каналов связи (СКЗИ)
- Антивирусная защита рабочих станций и серверов (AV)
- Контроль доступа к веб-ресурсам (SWG)
- Контроль привилегированных пользователей (PAM)
- Анализ сетевого трафика (NTA)
- Система обнаружения вторжений (IDS/IPS)
- Многофакторная аутентификация (MFA)
- Защита от DDoS-атак (Anti-DDoS)
- Защита мобильных устройств (MDM)
- Управление событиями ИБ (SIEM)
- Защита почты (Email Security)
- Сканер уязвимостей
- Предотвращение утечек информации (DLP)

Ростелеком
Солар

Шаги по выбору решений

1. Анализ рынка
2. Отбор по необходимым критериям
3. Составление технико-коммерческого обоснования
4. Оценка применимости использования сервисной модели
5. Тестирование на совместимость (отечественные операционные системы и другие средства защиты)

Или позвать

Ростелеком Солар

Ростелеком
Солар

Виталий Сиянов
Менеджер
по развитию
направления
«Solar
Интеграция»

Андрей Прошин
Руководитель
направления
Solar JSOC