SOLAR

СИСТЕМА ПОСТАВКИ ДАННЫХ ОБ АКТУАЛЬНЫХ УГРОЗАХ SOLAR TI FEEDS

WHITE PAPER

МОСКВА, 2025

W:RT-SOLAR.RU

Оглавление

1. ПРОБЛЕМАТИКА

88%

ЦЕЛЕВЫХ КИБЕРАТАК
БЫЛО НАПРАВЛЕНО НА ШПИОНАЖ
И ФИНАНСОВУЮ ВЫГОДУ
В 2025 г.*

* Отчет «Хроники DFIR: отчет по итогам первого полугодия 2025».

ТОП-3 СПОСОБОВ ПРОНИКНОВЕНИЯ В ИНФРАСТРУКТУРУ

[01] Уязвимости веб-приложений

[02] Скомпрометированные аккаунты и сервисы удаленного доступа

[03] Фишинг и доверительные отношения

Современные информационные инфраструктуры развиваются быстрее, чем возможности большинства систем защиты информации: облачные сервисы, удаленный доступ и сложные цепочки поставок размывают традиционные периметры безопасности, каждый новый интегрированный сервис создает потенциальные уязвимости, контроль которых зачастую оказывается за пределами возможности конечной организации.

При этом злоумышленники все активнее используют автоматизацию, искусственный интеллект, распределение и координацию действий для совершения атак, что сужает окно для своевременного реагирования.

Службы информационной безопасности все чаще сталкиваются не с нехваткой данных, а с их хаотичностью и несвоевременностью: фрагментированность данных, избыточные оповещения и устаревшая информация, содержащаяся в них, снижают эффективность реагирования:

- аналитики перегружены телеметрией из множества источников, в которой реальные угрозы теряются среди ложных срабатываний;
- существующие процессы сбора и корреляции сведений не обеспечивают требуемую скорость принятия решений;
- отсутствие актуального контекста мешает выявлять взаимосвязанные атаки и прогнозировать дальнейшие действия нарушителей.

В результате защита становится реактивной, а не упреждающей — инциденты выявляются постфактум.

Настоящий документ призван показать, как использование своевременной, достоверной и структурированной информации может повысить точность детектирования, сократить время реакции и обеспечить устойчивость инфраструктуры к атакам через интеграцию знаний, контекста и аналитики.

2. ПРЕДЛАГАЕМОЕ РЕШЕНИЕ

Для формирования превентивной защиты необходим источник актуальных и достоверных сведений о внешних угрозах. Его роль выполняют специализированные системы поставки данных об актуальных угрозах Threat Intelligence Feeds, обеспечивающие непрерывное поступление индикаторов и контекста о вредоносной активности, выявленной во внешней по отношению к организации среде.

Они позволяют сопоставить внутренние события компании с глобальной информацией об угрозах, злоумышленниках, используемых ими техниках, тактиках и процедурах, сокращая время реакции и повышая точность принятия решений.

Ключевые преимущества использования потоков данных об актуальных угрозах:

1. Актуальность — постоянное обновление индикаторов и тактик злоумышленников.
2. Наличие контекста — сопоставление событий с конкретными кампаниями, группировками и секторами.
3. Снижение ложных срабатываний — фильтрация событий и повышение точности детектирования.
4. Приоритизация угроз — выделение наиболее критичных событий для оперативного реагирования.
5. Автоматизация — интеграция с SOC, SIEM, EDR и другими системами для корреляции данных.
6. Повышение эффективности — уменьшение нагрузки на аналитиков за счет автоматизированного обогащения данных.

ПРЕИМУЩЕСТВА SOLAR TI FEEDS ОТ ЦЕНТРА ИССЛЕДОВАНИЙ SOLAR 4RAYS

ДАННЫЕ ОБ АКТУАЛЬНЫХ КИБЕРУГРОЗАХ В РФ ИЗ УНИКАЛЬНЫХ ИСТОЧНИКОВ

- Сведения от сенсоров в сети крупнейшего* телеком-оператора в РФ «Ростелеком»
- Телеметрия сервисов первого и крупнейшего** центра противодействия Solar JSOC в РФ
- Результаты собственной кибервразведки и более 200 расследований Solar 4RAYS

ИНФОРМАЦИЯ О ВРЕДОНОСНЫХ КАМПАНИЯХ 24/7

Ежедневно фиксируются и обрабатываются:

- 200+ млрд событий на сенсорах
- 3+ млн алертов
- 1+ млн действий хакеров

После автоматической и ручной проверки остаются только сведения о самых опасных и актуальных угрозах:

- ИНДИКАТОРЫ КОМПРОМЕТАЦИИ
  IP-адреса, домены, веб-ссылки, хеш-суммы
- ИНДИКАТОРЫ АТАК
  Правила обнаружения Suricata, YARA, Sigma, ModSec

ПРОВЕРЕННЫЕ ЗНАНИЯ БЕЗ ФОЛЗОВ

- Проверяем и обкатываем правила на крупнейшем коммерческом SOC в РФ**
- Подтверждаем полезность фидов при проведении собственных расследований

* По финансовым показателям. Рейтинг четырех крупнейших телекоммуникационных операторов на основе их финансовых показателей за 2024 г. Источник

** По итогам 2023 года. Более 300 клиентов, более 750 экспертов по кибербезопасности. Входит в топ-5 европейских сервис-провайдеров MSSP. Источник

3. ОСНОВНЫЕ ЗАДАЧИ И ФУНКЦИИ SOLAR TI FEEDS

Основной задачей, решаемой системой поставки потоков данных об актуальных угрозах, является предоставление информации для дальнейшего использования заказчиком в следующих сценариях, но не ограничиваясь ими:

1. Мониторинг событий информационной безопасности средствами SOC.
2. Автоматическая фильтрация ложноположительных событий ИБ.
3. Регистрация неправомерных действий, нарушающих политики безопасности заказчика.
4. Автоматическая блокировка вредоносной активности на сетевых сенсорах или конечных точках.
5. Обогащение инцидентов ИБ дополнительным контекстом.

Помимо этого, система Solar TI Feeds позволяет формировать собственные наборы сведений об угрозах, необходимые конкретному пользователю для реализации требуемых сценариев.

СХЕМЫ ПОДКЛЮЧЕНИЯ

Система поддерживает агентскую схему подключения через TI-Cloud-агент, когда поставляется в виде docker image, который можно развернуть в инфраструктуре для автоматизированного получения актуальных данных от сервера (рисунок 1), и с использованием API (рисунок 2).

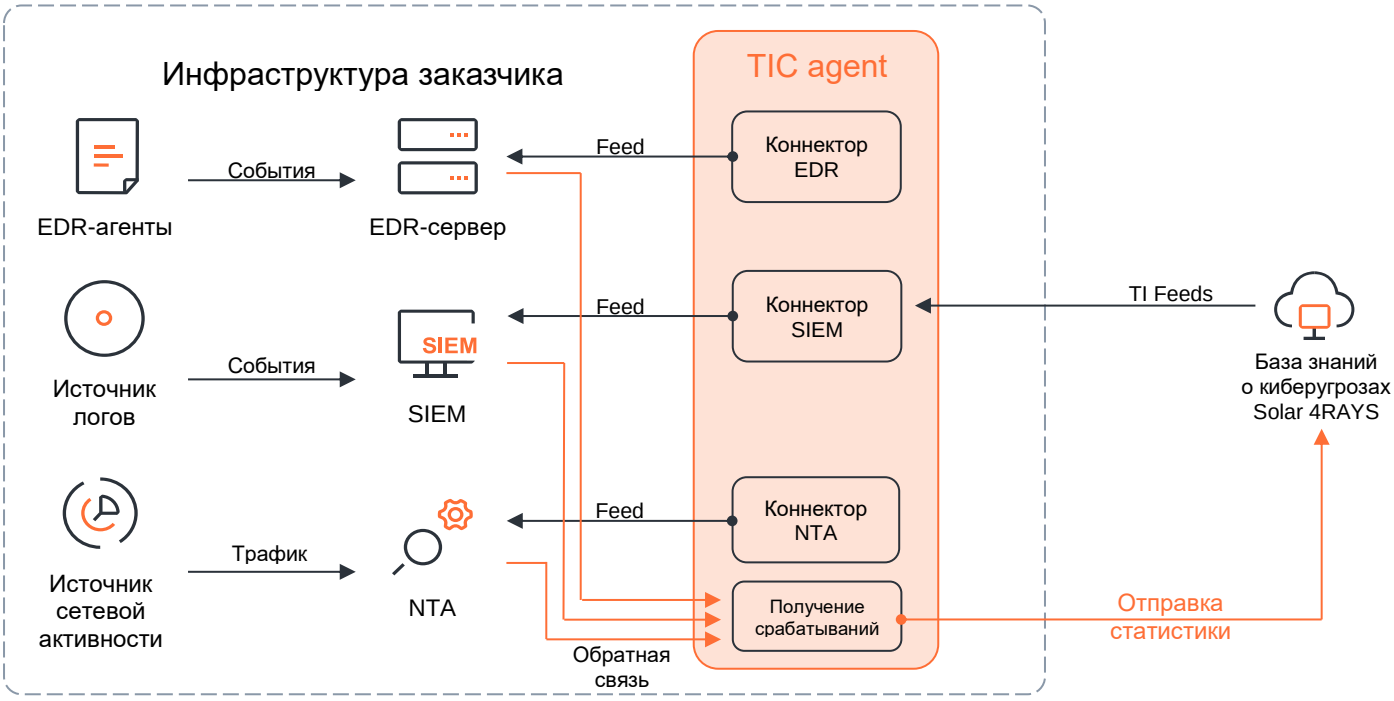

Рисунок 1. Схема подключения через TI-Cloud-агент

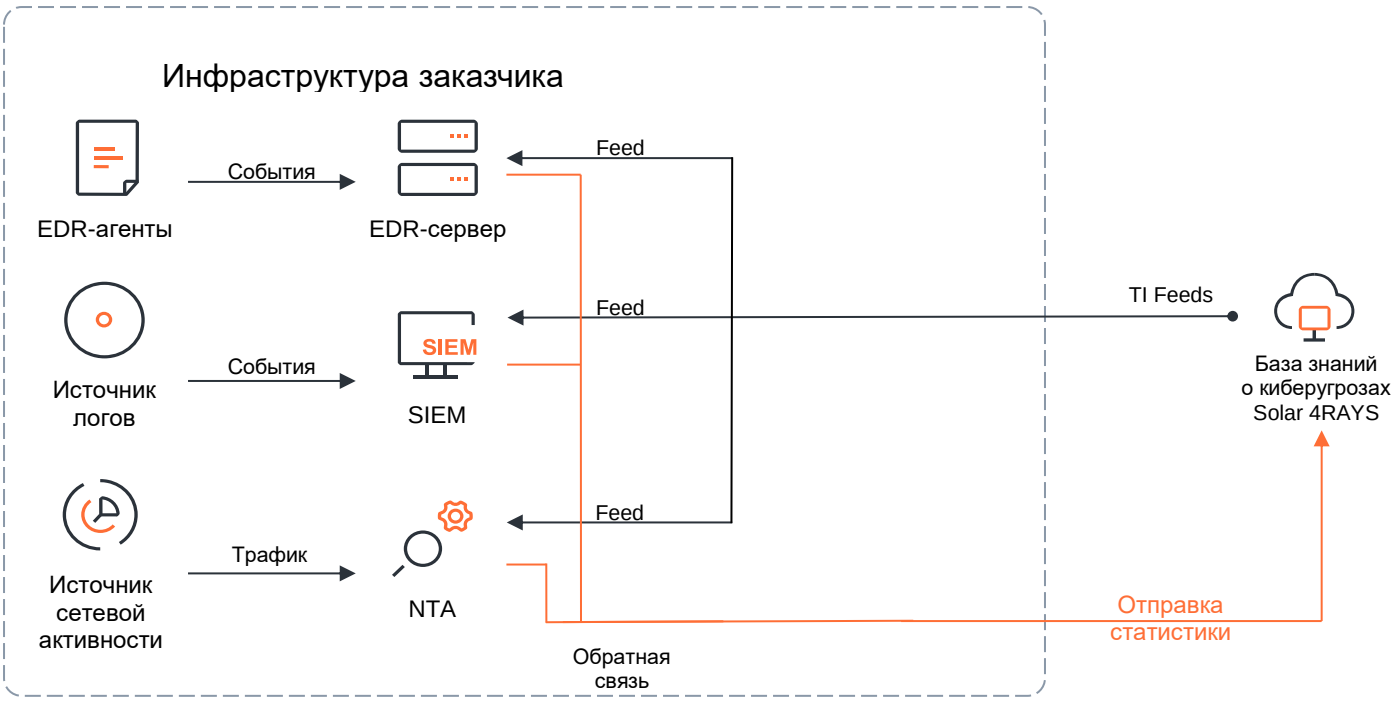

Рисунок 2. Схема подключения с использованием API

ИНТЕГРАЦИЯ С СЗИ

Доступна интеграция со средствами защиты информации и мониторинга*:

- SIEM-, SOAR-СИСТЕМЫ
- NGFW, WEBPROXY
- EDR, XDR
- TI-ПЛАТФОРМЫ

При отсутствии готового способа интеграции со средствами защиты информации специалисты Solar 4RAYS разработают специализированный интеграционный агент.

ОСОБЕННОСТИ ИНТЕГРАЦИИ ЧЕРЕЗ TI-CLOUD-АГЕНТ

- Легковесный docker-образ:
  Контейнер не требует специфичных системных ресурсов (например, 2 CPU, 2 ГБ RAM, 20 ГБ HDD), быстро развертывается, минимизируя затраты на инфраструктуру.
- Поддержка режима инициатора загрузки:
  Как со стороны сервиса, так и со стороны СЗИ (например, через Syslog).
- Настройка частоты запросов данных:
  Из TI-Cloud в зависимости от ваших потребностей — от инкрементальных обновлений до полного актуального набора данных в моменте, а не только выгрузка снимков за текущие сутки.
- Любой формат данных: список, CSV, TSV или JSON; выгрузка всех или выборочных полей для упрощения обработки.
- Поддержка передачи данных в Kafka.

* Подробный список доступен на сайте https://docs.data.rt-solar.ru/category/ti-feeds/.

ПОДДЕРЖАНИЕ АКТУАЛЬНОСТИ СИСТЕМЫ

Специалисты Solar 4RAYS выполняют ряд задач, направленных на обеспечение своевременного обновления и надежной работы системы Solar TI Feeds. Ключевые направления их работы:

- Сбор и анализ данных о текущих киберугрозах с последующей их интеграцией в систему.
- Предоставление инструментов, обеспечивающих доступ к информации об угрозах.
- Мониторинг непрерывного поступления данных об угрозах.
- Поддержание стабильной работы систем передачи информации.

Эти мероприятия способствуют постоянному обновлению данных и поддерживают эффективность системы.

4. СОСТАВ ПОСТАВЛЯЕМЫХ ДАННЫХ

Потоки данных об актуальных угрозах Solar TI FEEDS включают в себя высоко релевантные индикаторы компрометации и атак:

1. Хронологические метки: время обнаружения, время последней активности, а также время изменения информации об индикаторе в потоках данных.
2. Описание угрозы.
3. Связность с другими объектами в потоках данных.
4. Ссылки на внешние ресурсы с дополнительными сведениями.
5. Категория угрозы.

Сведения об угрозах, позволяющие идентифицировать актуальные действия злоумышленников, выделяются в отдельный поток данных.

СОСТАВ ПОТОКОВ ДАННЫХ

ИНДИКАТОРЫ	КАТЕГОРИИ ДАННЫХ
IOC Индикаторы компрометации	APT
	CYBERCRIME
	PHISHING
	ACTIVE_C2
	HONEYPOT
	INTRUSION
	FINCERT
	VPN
	PROXY
	TOR
IOA Индикаторы атак	Сигнатуры IDS
	Сигнатуры IDS_TREND
	Правила WAF
	Правила YARA_WINDOWS
	Правила YARA_LINUX
	Правила YARA_TREND_WINDOWS
	Правила YARA_TREND_LINUX
	Правила SIGMA_WINDOWS
	Правила SIGMA_LINUX
	Правила SIGMA_TREND_WINDOWS
	Правила SIGMA_TREND_LINUX
	Правила SIGMA_KUBERNETES

Solar TI Feeds позволяет подключить необходимый состав потоков данных под текущие задачи с возможностью дальнейшего апгрейда и масштабирования.

ПЕРЕЧЕНЬ ФИДОВ ИНДИКАТОРОВ КОМПРОМЕТАЦИИ

APT	IoCs, выявленные в целевых атаках, осуществляемых высококвалифицированными группировками
CYBERCRIME	IoCs, связанные с вредоносным программным обеспечением, включая программы-шифровальщики (ransomware), стилеры (stealer), ботнеты (botnet), майнеры (cryptomining), а также IP-адреса, используемые для управления (C2)
PHISHING	IoCs, которые были замечены в фишинговых рассылках электронной почты или потенциально могут быть использованы в таких рассылках
ACTIVE_C2	IoCs, используемые злоумышленниками в качестве активных серверов управления, которые Solar 4RAYS отслеживает на текущий момент в атаках с помощью сенсоров
HONEYPOT	IoCs, которые были замечены в качестве вредоносных на специально развернутых «ловушках» (honeypot). С таких адресов осуществляются беспорядочные атаки на любые уязвимые серверы, связанные с глобальной сетью, или дополнительно загружаются вредоносные компоненты
INTRUSION	IoCs, с которых зафиксированы попытки несанкционированного доступа (атаки) к ресурсам жертвы
FINCERT	IoCs, распространяемые ФинЦЕРТ (Центр мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере при Банке России)
VPN	Выходные серверы различных VPN-сервисов, которые злоумышленники могут использовать в своих атаках
PROXY	Выходные серверы различных Proxy-сервисов, которые злоумышленники могут использовать в своих атаках
TOR	Выходные серверы сети Tor, которые злоумышленники могут использовать в своих атаках

ПЕРЕЧЕНЬ АТРИБУТНЫХ ПОЛЕЙ ИНДИКАТОРОВ КОМПРОМЕТАЦИИ

indicator_id	Уникальный идентификатор индикатора
indicator_type	Тип индикатора
action	Событие, связанное с индикатором
updated_at	Время обновления данных по индикатору
value	Значение индикатора
description	Текстовое описание индикатора
rules	Правила детектирования, которыми был обнаружен индикатор
first_seen	Время создания индикатора
last_seen	Последнее время изменения индикатора
relations	Связи с другими индикаторами и иными вредоносными объектами
external_references	Ссылки на внешние источники, в которых упоминается индикатор
feeds	Перечень фидов, к которым относится индикатор
zone	Уровень критичности угрозы (на основе экспертной оценки Solar 4RAYS)

ПЕРЕЧЕНЬ ФИДОВ ИНДИКАТОРОВ АТАК

Сигнатуры IDS	Сигнатуры в формате Suricata для обнаружения ВПО, хакерских инструментов и попыток эксплуатации уязвимостей в сетевом трафике
Сигнатуры IDS_TREND	Небольшой, часто обновляемый срез релевантных сигнатур в формате Suricata для обнаружения вредоносного ПО, хакерских инструментов и попыток эксплуатации уязвимостей в сетевом трафике
Правила WAF	Правила в формате ModSec для обнаружения атак на веб-приложения
Правила YARA_WINDOWS	Правила в формате YARA для обнаружения вредоносного ПО, эксплойтов и хакерских инструментов в файлах для операционной системы Windows и памяти процессов
Правила YARA_LINUX	Правила в формате YARA для обнаружения вредоносного ПО, эксплойтов и хакерских инструментов в файлах для операционной системы Linux и памяти процессов
Правила YARA_TREND_WINDOWS	Небольшой, часто обновляемый срез релевантных правил в формате YARA для обнаружения вредоносного ПО, эксплойтов и хакерских инструментов в файлах для операционной системы Windows и памяти процессов
Правила YARA_TREND_LINUX	Небольшой, часто обновляемый срез релевантных правил в формате YARA для обнаружения вредоносного ПО, эксплойтов и хакерских инструментов в файлах для операционной системы Linux и памяти процессов
Правила SIGMA_WINDOWS	Правила в формате Sigma для обнаружения вредоносного ПО, хакерских инструментов и попыток эксплуатации уязвимостей в событиях операционной системы Windows в качестве шаблонов поведенческих признаков
Правила SIGMA_LINUX	Правила в формате Sigma для обнаружения вредоносного ПО, хакерских инструментов и попыток эксплуатации уязвимостей в событиях операционной системы Linux в качестве шаблонов поведенческих признаков
Правила SIGMA_TREND_WINDOWS	Небольшой, часто обновляемый срез релевантных правил в формате Sigma для обнаружения вредоносного ПО, хакерских инструментов и попыток эксплуатации уязвимостей в событиях операционной системы Windows в качестве шаблонов поведенческих признаков
Правила SIGMA_TREND_LINUX	Небольшой, часто обновляемый срез релевантных правил в формате Sigma для обнаружения вредоносного ПО, хакерских инструментов и попыток эксплуатации уязвимостей в событиях операционной системы Linux в качестве шаблонов поведенческих признаков
Правила SIGMA_KUBERNETES	Правила в формате Sigma для обнаружения вредоносного ПО, хакерских инструментов и попыток эксплуатации уязвимостей в событиях от docker-контейнеров под управлением Kubernetes в качестве шаблонов поведенческих признаков

5. КОМПЛЕКТЫ ПОТОКОВ ДАННЫХ ПОД ЗАДАЧИ ДЛЯ СЛУЖБ ИБ

Отправная точка для определения состава потоков данных — выбор сценария использования фидов или формулирование решаемой ими задачи.

Ниже приведены примеры самых популярных сценариев использования фидов, в то же время команда специалистов Solar 4RAYS может подобрать индивидуальный комплект фидов под конкретные задачи.

ПРИМЕРЫ КОМПЛЕКТОВ ПОД КЛЮЧЕВЫЕ СЦЕНАРИИ ИСПОЛЬЗОВАНИЯ

НАЗВАНИЕ КОМПЛЕКТА	СЦЕНАРИИ ИСПОЛЬЗОВАНИЯ ФИДОВ	СОСТАВ КОМПЛЕКТА ФИДОВ (КАТЕГОРИИ ДАННЫХ)	РЕКОМЕНДУЕМЫЕ СЗИ
Автоблокировка угроз в сети и на хостах	Автоматически блокировать вредоносную активность на сетевых сенсорах или конечных точках	APT ACTIVE_C2 INTRUSION	SEG, SWG, NGFW, Sandbox, FW, EDR, WAF
Контроль политики безопасности организации	Своевременно регистрировать неправомерные действия, нарушающие политики безопасности потребителя данных	VPN PROXY TOR	SWG, IDS, NTA, SIEM
Контекст для снижения нагрузки на SOC	Обогащать контекстом инциденты ИБ	APT CYBERCRIME PHISHING HONEYPOT	SIEM, SOAR, IRP
Гипотезы для обнаружения трендовых угроз	Повысить качество обнаружения на установленных СЗИ	IDS_TREND YARA_TREND_WINDOWS YARA_TREND_LINUX SIGMA_TREND_WINDOWS SIGMA_TREND_LINUX	EDR, NGFW, NTA, SIEM, WAF

6. О ЦЕНТРЕ ИССЛЕДОВАНИЙ КИБЕРУГРОЗ SOLAR 4RAYS

ПРАКТИЧЕСКИЙ ОПЫТ

200+
расследований инцидентов различной сложности

10+
лет опыта отражения атак

60+
отслеживаемых профессиональных группировок

ВСЕГДА АКТУАЛЬНЫЕ ЗНАНИЯ ОБ УГРОЗАХ

Доступ к крупнейшей базе знаний киберугроз Центра исследований Solar 4RAYS

200+ млрд
событий в сутки регистрируют автоматизированные сенсоры

3+ млн
алертов в сутки на автоматизированных сенсорах

1+ млн
действий злоумышленников фиксирует сеть ханипотов

МНОГООТРАСЛЕВОЙ ОПЫТ ПРОТИВОДЕЙСТВИЯ

Финансы, телеком, транспорт, госсектор, промышленность, ИТ, нефтегаз, медицина и другие.

Делимся практическим опытом и исследованиями киберугроз в блоге Solar 4RAYS.

7. О КОМПАНИИ «СОЛАР»

Группа компаний «Солар» — архитектор комплексной кибербезопасности. Ключевые направления деятельности — предоставление услуг и сервисов в области информационной безопасности, разработка собственных ИБ-продуктов, обучение ИБ-специалистов, аналитика и исследование киберинцидентов.

С 2015 года предоставляет ИБ-решения организациям от малого бизнеса до крупнейших предприятий ключевых отраслей. Под защитой «Солара» — более 1000 крупнейших компаний России. Компания работает в направлениях безопасной разработки программного обеспечения, управления доступом, защиты корпоративных данных, детектирования хакерских атак и угроз, что позволяет закрывать максимум потребностей заказчиков.

Группа компаний предлагает сервисы первого и крупнейшего в России коммерческого SOC — Solar JSOC, экосистему управляемых сервисов ИБ — Solar MSS. По данным независимых аналитиков, «Солар» входит в топ-5 европейских и топ-15 мировых сервис-провайдеров по объему бизнеса.

Работа Центра исследования киберугроз Solar 4RAYS нацелена на изучение тактик киберпреступников. Полученные аналитические данные обогащают разработки Центра технологий кибербезопасности.

Линейка собственных продуктов включает DLP-решение Solar Dozor, шлюз веб-безопасности Solar webProxy, межсетевой экран нового поколения Solar NGFW, IdM-систему Solar inRights, PAM-систему Solar SafeInspect, анализатор кода Solar appScreener и другие. Также ГК «Солар» развивает платформу для практической отработки навыков защиты от киберугроз «Солар Кибермир».

Группа компаний «Солар» инвестирует в развитие отрасли кибербезопасности и помогает решать проблему кадрового дефицита. Для поддержки молодых технологичных проектов и насыщения рынка технологиями созданы венчурный фонд Solar Ventures и программа CyberStage. «Солар» реализует образовательные и просветительские проекты, направленные на повышение цифровой грамотности населения.

Под защитой «Солара» находятся крупнейшие государственные информационные системы, а также экономические и общественно-политические события в России, в том числе международного уровня.

Штат компании — около 2500 специалистов. Подразделения «Солара» расположены в Москве, Санкт-Петербурге, Нижнем Новгороде, Самаре, Ростове-на-Дону, Томске, Хабаровске и Ижевске. Технологии компании и наличие распределенных по всей стране центров компетенций позволяют ей работать в режиме 24/7.