

ЛИЦЕНЗИОННЫЙ ДОГОВОР С КОНЕЧНЫМ ПОЛЬЗОВАТЕЛЕМ

Солар Программный Комплекс Обнаружения и Реагирования©

ВАЖНО! Прочитайте внимательно нижеизложенное, прежде чем воспроизводить, копировать или иным способом использовать программное обеспечение Солар Программный Комплекс Обнаружения и Реагирования (далее – «ПО»).

Настоящий Лицензионный договор с Конечным пользователем (далее – «Договор») регулирует отношения, возникающие между Компанией и Вами – физическим или юридическим лицом, и определяет порядок и условия использования Вами ПО. Договор заключается в упрощенном порядке и является договором присоединения, условия которого изложены в электронном виде и доведены до Вашего сведения.

Договор вступает в силу с момента, когда Вы начинаете использовать ПО, либо, если это предусмотрено функциональными возможностями ПО, с момента, когда Вы принимаете условия Договора, отметив в процессе установки ПО на своем устройстве пункт «Я согласен с условиями Лицензионного договора» или «Я принимаю условия Лицензионного договора» или иным, предложенным образом выражаете свое согласие на экране Вашего устройства с помощью интерфейса установки ПО. Договор, изложенный в электронном виде, при Вашем акцепте, как указано выше, считается заключенным в письменной форме в соответствии с п. 3 ст. 434 и п. 3 ст. 438, п.5 ст. 1286 Гражданского кодекса Российской Федерации.

В любом случае, начало использования ПО означает Ваше полное и безоговорочное согласие с условиями Договора. Вы подтверждаете, что Договор был Вами прочитан, условия его Вам понятны и Вы с ними полностью согласны. Если Вы не согласны с условиями Договора, не используйте ПО.

Предоставление прав на использование ПО может сопровождаться отдельным соглашением, заключенным между Компанией или Партнером Компании и Вами. В случае расхождений в содержании между текстом Договора в электронном виде и текстом соответствующего отдельного соглашения, преимущественную силу имеет текст отдельного соглашения (как правило, составленного в бумажной форме и подписанного сторонами), кроме условия о гарантиях и обязательствах Пользователя (п. 3.3. Договора). Данное требование применимо ко всем пользователям в равной степени.

Права на ПО охраняются законодательством Российской Федерации и международными соглашениями. Некоторые части (компоненты) ПО могут охраняться законодательством о патентах и ноу-хау. Нарушение условий Договора и прав на ПО, влечет за собой ответственность, предусмотренную Договором и законодательством Российской Федерации.

1. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

1.1. **«Компания»** – Акционерное общество «СОЛАР СЕКЬЮРИТИ», юридическое лицо, зарегистрированное и осуществляющее свою деятельность в соответствии с законодательством Российской Федерации, основной государственный регистрационный номер (ОГРН) № 1257700041829, зарегистрировано по адресу: 127015, Г.МОСКВА, ВН.ТЕР.Г. МУНИЦИПАЛЬНЫЙ ОКРУГ САВЕЛОВСКИЙ, УЛ ВЯТСКАЯ, Д. 35, СТР. 4.

1.2. **«ПО Солар Программный Комплекс Обнаружения и Реагирования»¹**, - программное обеспечение (программный комплекс) из линейки Solar EDR представляющее собой систему обнаружения и предотвращения целевых атак, с целью повышения уровня киберзащищенности. ПО

¹ Все положения и условия Соглашения применяются к Программному обеспечению в целом, так и к каждому компоненту (подсистеме) Программного обеспечения.

зарегистрировано в Федеральной службе по интеллектуальной собственности РФ. Компания является правообладателем ПО.

1.3. **«Вы», «Пользователь»:**

- (i) **физическое лицо**, которое приобрело лицензию на ПО для личного использования, а не для перепродажи или оказания услуг с помощью ПО третьим лицам.
- (ii) **юридическое лицо**, для которого ПО было загружено или приобретено для некоммерческого использования и которое поручило уполномоченному физическому лицу принять данное соглашение от своего лица. В случае, если у Вас нет такого права (на акцепт и принятие настоящего Договора) от имени юридического лица Вы должны немедленно прекратить использование ПО.

1.4. **«Лицензия»** - предоставленное Вам Компанией ограниченное право на установку, запуск и использование функциональности ПО на условиях простой (неисключительной) лицензии.

1.5. **«Партнер»** - юридическое лицо, которому Компания предоставила право на предоставление (сублицензирование) и/или иное использование ПО. Лицензия на ПО может быть приобретена Пользователем у Партнера.

1.6. **«Устройство»** - физическое или виртуальное устройство, посредством которого Вы используете ПО.

1.7. **«Метрика лицензирования ПО»** – объем использования ПО, который определяется в отдельном лицензионном соглашении с Компанией. Виды метрик лицензирования ПО изложены в Приложении №1. Компания вправе определить и заключить лицензионный договор на иные метрики лицензирования, не указанные в Договоре.

2. ЛИЦЕНЗИЯ НА ПО

2.1. Компания предоставляет Вам право использования ПО на условиях простой (неисключительной) лицензии сроком 1 (Один) год на территории Российской Федерации путем инсталляции (воспроизведение и установка), запуска и использования функционала ПО согласно условиям Договора.

Указанные права относятся к 1 (Одному) экземпляру ПО, который устанавливается на 1 (Одном) Устройстве, и для 1 (Одного) Устройства² с максимально доступным на момент предоставления права объемом прав в отношении функционала ПО.

Отличные от указанных в настоящем пункте параметры предоставления лицензии (способы использования, сроки использования, территория использования и т.д.) могут быть установлены в отдельном соглашении с Компанией или Партнером Компании.

Условия отдельного соглашения с Компанией или Партнером Компании отличные от условий настоящего Договора, имеют преимущественную силу.

2.2. Любое использование ПО или компонентов ПО, в нарушение условий Договора, либо отдельного лицензионного соглашения, заключенного Вами с Компанией или Партнером Компании, является нарушением исключительных прав Компании и/или третьих лиц и служит основанием для одностороннего прекращения Вашего права использования ПО по инициативе Компании или уполномоченного Компанией лица, а также применения иных мер ответственности, предусмотренных применимым законодательством (по умолчанию – законодательством Российской Федерации).

2.3. Компания сохраняет за собой все права на ПО, ничто в Договоре не может быть истолковано, как передача (отчуждение) Вам или иным третьим лицам исключительных прав на ПО.

2.4. Лицензионное вознаграждение по Договору с Пользователем не уплачивается, если иное не следует из обстоятельств предложения ПО. При этом лицензионное вознаграждение за использование ПО может быть уплачено Пользователем в размере выбранного Пользователем тарифа, установленного на сайте Компании, если иное не согласовано в отдельных лицензионных соглашениях, заключенных Пользователем с Компанией или Партнером.

3. ГАРАНТИИ И ОБЯЗАТЕЛЬСТВА

3.1. Гарантии и обязательства Компании:

² Под устройством в данном пункте понимается конечное устройство, на котором установлен агент ПО.

3.1.1. Компания гарантирует, что обладает всеми необходимыми правами на ПО и его компоненты, а также (при наличии) на сопровождающие ПО документацию, материалы, изображения.

3.1.2. Компания не может гарантировать и не гарантирует результаты, которые Вы можете получить при использовании ПО, а также, что работа ПО будет соответствовать Вашим требованиям и ожиданиям или уровню и функционалу подобного рода программ, разработанных третьими лицами.

3.1.3. Компания предоставляет ПО «КАК ЕСТЬ», не предоставляет и не может предоставить гарантий, не оговоренных в Договоре специально, в том числе относительно компонентов ПО, а также не гарантирует полную и бесперебойную работоспособность, производительность и результаты, которые Вы можете получить посредством использования ПО, подсистем ПО, обновлений и/или новых версий ПО.

3.1.4. Компания не дает каких-либо гарантий относительно программного обеспечения третьих лиц, использованного в ПО, либо поставляемого (передаваемого) с ПО, в том числе удовлетворительную работу такого программного обеспечения.

3.1.5. Компания не может гарантировать и не гарантирует, что ПО не содержит ошибок, что ПО будет нормально функционировать при использовании совместно с иным программным обеспечением. Компания не может гарантировать и не гарантирует, что ПО будет нормально функционировать при использовании на операционных системах и оборудовании, не указанных в качестве совместимых с ПО.

3.1.6. В случае, если ПО было приобретено на материальном носителе, а также если этого требует применимое право страны приобретения прав на ПО, Компания гарантирует качество и работоспособность материальных носителей, на которых было предоставлено ПО.

3.1.7. Компания в течение 1 (одного) года с момента приобретения ПО осуществляет устранение дефектов ("bug fixing"), допущенных в процессе разработки и препятствующих нормальной эксплуатации ПО Пользователем. Bug fixing не является услугами технической поддержки. Срок устранения выявленных дефектов ПО устанавливается Компанией. С целью сообщения о дефекте ПО Пользователю необходимо направить соответствующее обращение на адрес электронной почты support@rt-solar.ru.

3.1.8. Техническая поддержка, услуги по сопровождению ПО, инженерные и/или аналитические работы приобретаются отдельно.

3.2. Компания вправе:

3.2.1. Расторгнуть Договор в одностороннем, внесудебном порядке, в случае нарушения условий использования ПО Пользователем. Расторжение Договора влечет невозможность дальнейшего использования ПО.

3.3. Гарантии и обязательства Пользователя:

3.3.1. Пользователь обязуется использовать ПО в соответствии с условиями Договора, исключительно в законных целях.

3.3.2. Пользователь обязуется не совершать самостоятельно и не способствовать третьим лицам осуществлять следующие действия:

3.3.2.1. Изучать, исследовать или испытывать функциональные возможности ПО в целях определения идей и принципов, лежащих в основе любого элемента или компонента ПО, дизассемблировать, декомпилировать (воспроизводить и преобразовывать объектный код в исходный текст) или иным способом осуществлять попытку получить исходный текст ПО или любой части ПО за исключением случаев, разрешенных применимым правом, несмотря на данное ограничение, и только в объеме, разрешенном применимым правом. Если применимое право запрещает ограничение указанных действий, любая информация, полученная таким способом, (i) не должна использоваться для создания программного обеспечения, по своему виду существенно схожего с ПО или для осуществления других действий, нарушающих исключительное право Компании на ПО или права авторов ПО, (ii) не должна раскрываться третьим лицам, если только такое раскрытие не предусмотрено применимым правом, и (iii) должна быть немедленно сообщена Компании.

Любая информация, полученная Пользователем в результате действий, указанных в настоящем пункте, является конфиденциальной и принадлежит Компании.

В случае, если декомпиляция ПО требуется Пользователю для возможности взаимодействия ПО с другими программами на Устройстве Пользователя, последний обязан обратиться в Компанию с письменным запросом на совершение указанных действий. Компания обязуется предпринять разумные и экономически обоснованные меры для обеспечения взаимодействия ПО с программами Пользователя. Пользователь может декомпилировать ПО самостоятельно для указанных выше целей только в случае письменного отказа Компании от принятия соответствующих мер.

3.3.2.2. Модифицировать, адаптировать (в том числе вносить в ПО изменения исключительно в целях его функционирования на конкретных технических средствах Пользователя или под управлением конкретных программ Пользователя), вносить любые изменения в объектный код ПО, программы и базы данных, содержащиеся в ПО, за исключением тех изменений, которые предусмотрены ПО и описаны в документации;

3.3.2.3. Осуществлять исправление ошибок в ПО или переводить ПО без предварительного письменного согласия Компании;

3.3.2.4. Сублицензировать, передавать или уступать права, предоставленные Вам по Договору, и любые другие права, связанные с ПО, любому другому лицу, а также разрешать копировать ПО, подсистемы или части на другие Устройства, если иное не оговорено в отдельном письменном договоре с Компанией или Партнером Компании;

3.3.2.4.1. Запрещается сдавать экземпляры ПО в аренду, прокат, лизинг или во временное пользование.

3.3.2.5. Распространять ПО в пользу третьих лиц на возмездной или безвозмездной основе;

3.3.2.6. Способствовать или создавать условия для доступа к ПО или использования ПО третьими лицами, не имеющими прав на использование данного ПО;

3.3.2.7. Удалять, изменять или делать малозаметными любые уведомления об авторских правах, правах на товарные знаки или патенты, которые указаны на предоставленном Вам ПО;

3.3.2.8. Использовать ПО для предоставления платных или бесплатных услуг иным юридическим или физическим лицам;

3.3.2.9. Осуществлять иные действия, прямо не разрешенные условиями Договора или отдельного соглашения с Пользователем.

4. ОЗНАКОМИТЕЛЬНАЯ ВЕРСИЯ ПО (TRIAL)

4.1. Компания вправе предоставить Пользователю ПО, являющееся ознакомительной версией. Указанное ПО может иметь ограниченный срок действия, неполный набор функционала. Ознакомительная версия ПО предназначена для проведения испытания, ознакомления, тестирования или демонстрации функциональных возможностей ПО.

4.2. Если указанное в п. 4.1. ПО предоставляется Пользователю на материальном носителе, оно может быть промаркировано, как «Испытательная версия», «Ознакомительная версия» (либо «Trial»).

4.3. Компания не взимает вознаграждение за предоставление права использования ознакомительной версии ПО, если иное не следует из отдельного лицензионного соглашения либо не установлено при предложении использования ознакомительной версии ПО.

4.4. В случае предоставления ознакомительной версии ПО с Пользователем может быть заключено отдельное соглашение, регламентирующее порядок и условия использования такой версии ПО. В случае, если с Пользователем было заключено отдельное соглашение, условия такого соглашения имеют преимущественную силу.

4.5. В отношении ознакомительной версии ПО действуют гарантии, предусмотренные п.3.1. Договора.

4.6. В отношении ознакомительной версии ПО Пользователь обладает тем же обязанностями и предоставляет те же гарантии, которые описаны в п. 3.3 Договора.

5. СБОР ИНФОРМАЦИИ ОБ ИСПОЛЬЗОВАНИИ ПО И ПРОВЕДЕНИЕ АУДИТА

5.1. Пользователь принимает и соглашается с тем, что в процессе использования настоящего ПО, такое ПО в автоматическом режиме может передавать Компании следующие сведения:

- а) Логи некатегоризированных ресурсов;
- б) Статистические данные об утилизации лицензии;

в) Версию установленного ПО Солар Программный Комплекс Обнаружения и Реагирования;

г) Используемый браузер и его версия;

д) Конфигурации оборудования, на котором установлено ПО;

е) Утилизации CPU, RAM, HDD, каналов коммуникации;

ж) Баг-репорты и логи работы сервисов.

5.2. Компания настоящим гарантирует, что вышеуказанные данные будут использоваться Компанией исключительно для целей улучшения стабильности работы ПО и выявления угроз.

5.3. Целью сбора данных, приведенных в п.5.1., не является получение персональных данных, конфиденциальной информации Пользователя либо третьих лиц. При этом, Пользователь вправе самостоятельно отключить в ПО автоматическую настройку по сбору указанной п.5.1 информации.

5.4. Условия, предусмотренные в пунктах 5.1.-5.3. Договора подлежат применению, если отдельным соглашением не было предусмотрено иное.

5.5. АУДИТ:

5.5.1. В период действия Лицензии на ПО и года после истечения данного срока, Компания имеет право своими силами и за свой счет проводить проверку соблюдения условий лицензионного договора Пользователем (далее – аудит).

5.5.2. Компания вправе без согласования с Пользователем привлекать для проведения аудита третьих лиц (далее – аудитор).

5.5.3. Пользователь обязан обеспечить доступ Компании и/или аудитора к информации, документам, информационным системам, необходимым для аудита, и оказать иное содействие. Пользователь обязан в течение 5 (пяти) рабочих дней с даты поступления запроса от Компании (как до, так и в процессе аудита) направлять ответы на такие запросы в письменном виде (предоставление сведений, пояснений, материалов и т.п.). Отсутствие ответа в указанный срок приравнивается к нарушению использования ПО.

5.5.4. Аудит проводится в обычные рабочие часы Пользователя без вмешательства в оперативную деятельность Пользователя.

5.5.5. Компания обязуется использовать сведения, полученные в ходе аудита только для того, чтобы удостовериться, что Пользователь полностью выполняет свои обязательства, вытекающие из лицензионного договора.

5.5.6. Если в процессе аудита будет установлено, что Пользователь нарушил условия использования ПО, то Компания имеет право требовать, а Пользователь обязуется возместить стоимость аудиторской проверки и возместить Компании убытки. В свою очередь, Компания вправе расторгнуть Договор в одностороннем порядке, аннулировать Лицензию и требовать возврата предоставленных Пользователю экземпляров ПО независимо от возмещения Пользователем убытков (выплаты компенсации), компенсации аудита.

5.5.7. Компания обязуется обеспечить надлежащий уровень защиты информации, полученной в рамках проведения Аудита.

6. ОТВЕТСТВЕННОСТЬ СТОРОН

6.1. В случае нарушения условий Договора Стороны несут ответственность в соответствии с условиями Договора, а также законодательством Российской Федерации.

6.2. Компания не несет ответственности за убытки, вынужденные перерывы в деловой активности, потерю данных, за претензии третьих лиц или расходы, косвенные или случайные убытки, а также за упущенную выгоду и утерянные сбережения, вызванные в результате использования или невозможности пользования ПО, а также за ущерб, вызванный возможными ошибками и опечатками в ПО. Указанные ограничения действуют в той степени, насколько это разрешено применимым правом. В любом случае ответственность Компании ограничивается суммой, которую Пользователь уплатил за предоставленное право в пользу Компании, либо суммой, которую уплатил Партнер в пользу Компании за предоставленное право на использование ПО, которое в последствии было передано (сублицензировано) Пользователю.

6.3. Компания не несет ответственности за законность использования ПО Пользователем в отношении третьих лиц (работников Пользователя и т.д.). Пользователь самостоятельно несет

ответственность перед третьими лицами, чьи права он нарушил в связи с Использованием ПО и результатов, полученных при использовании ПО.

6.4. В случае нарушения условий Договора или законодательства Российской Федерации при использовании ПО, Пользователь обязуется возместить Компании все причиненные убытки, включая реальный ущерб и упущенную выгоду.

7. ИНТЕЛЛЕКТУАЛЬНАЯ СОБСТВЕННОСТЬ

7.1. Компания является обладателем исключительного права на ПО, в отношении которого Вы акцептуете Договор (правообладатель ПО). В соответствии со ст. 1229 ГК РФ иные лица не могут использовать соответствующий результат интеллектуальной деятельности, если такое использование осуществляется без согласия правообладателя.

7.2. Наименование ПО, а также иные обозначения в ПО могут являться товарными знаками соответствующих владельцев. Все товарные знаки Компании являются ее интеллектуальной собственностью и предоставлены для Вашего сведения. Компания не предоставляет Вам никаких прав в отношении товарных знаков Компании.

7.3. ПО может содержать иное программное обеспечение сторонних производителей. Информация о подобном программном обеспечении сторонних производителей и об условиях его лицензирования доступна непосредственно в ПО и (или) в сопроводительной документации к ПО.

8. РАСТОРЖЕНИЕ ДОГОВОРА

8.1. Если иное не оговорено в отдельном соглашении с Компанией или Партнером Компании, Договор действует в течение срока действия предоставленной Вам Лицензии на ПО, либо до тех пор пока не будет расторгнут.

8.2. Пользователь может расторгнуть Договор прекратив использование ПО и деинсталлировав ПО с Устройств, а также уничтожив все копии ПО (в том числе архивные) с Устройств.

8.3. По выбору Компании, в случае нарушения Пользователем любого из условий, предусмотренных Договором, Компания имеет право расторгнуть Договор, уведомив об этом Пользователя посредством электронной почты, либо в письменном виде на бумажном носителе, либо, если это применимо и технически осуществимо, заблокировав логин и пароль Пользователя и уведомив Пользователя о причинах.

9. ПРИМЕНИМОЕ ПРАВО И РАЗРЕШЕНИЕ СПОРОВ

9.1. В отношении условий Договора и обязательств, вытекающих из Договора, применяется законодательство Российской Федерации.

9.2. Для разрешения споров, возникших между Пользователем и Компанией в связи с использованием ПО, устанавливается следующий обязательный претензионный порядок:

9.2.1. Пользователь, полагающий, что его права и интересы нарушены в связи с использованием ПО, направляет Компании претензию на адрес электронной почты: info@rt-solar.ru.

9.2.2. Не позднее 30 (Тридцати) рабочих дней со дня получения претензии, Компания составляет и направляет Пользователю ответ или запрос дополнительной информации на обратный адрес Пользователя (с которого была получена претензия Пользователя), либо на адрес, указанный Пользователем в претензии.

9.2.3. Компанией не рассматриваются анонимные претензии или претензии, не позволяющие идентифицировать Пользователя на основе предоставленных им в претензии данных.

9.2.4. В случае недостижения разрешения спора путем претензионного порядка, спор подлежит рассмотрению в соответствии с законодательством Российской Федерации, по месту нахождения Компании.

9.3. В случае если Компании были предъявлены претензии со стороны третьих лиц в связи с неправомерным использованием Пользователем ПО, последний обязуется компенсировать любые расходы и издержки Компании (включая судебные издержки, вознаграждение консультантам, представителям и адвокатам, представляющим интересы Компании, вознаграждение аудиторов).

10. ПРОЧИЕ УСЛОВИЯ

10.1. Ничто в Договоре не может пониматься как установление между Пользователем и Компанией агентских отношений, отношений товарищества, отношений по совместной деятельности, отношений личного найма, либо каких-то иных отношений, прямо не предусмотренных Договором. Стороны признают, что Договор по своему существу является лицензионным договором, то есть направленным на предоставления прав использования объекта интеллектуальной собственности на определенных условиях. Использование в отношении Договора, отношений сторон где бы то ни было (в том числе, но не ограничиваясь, в рекламных материалах, презентациях) слов «продажа», «купить» и иных аналогичных выражений не означает выражения воли Компании на изменение сущности и переквалификацию Договора.

10.2. Признание судом какого-либо положения Договора недействительным или не подлежащим принудительному исполнению не влечет недействительности иных положений Договора.

10.3. **Вы соглашаетесь на добровольную передачу** Ваших персональных данных Компании, если предоставление соответствующих персональных данных необходимо для начала использования ПО. Вы выражаете свое согласие на обработку (включая, но не ограничиваясь сбором и иным использованием) Ваших персональных данных Компанией и/или ее аффилированными лицами в соответствии с применимым законодательством и при условии соблюдения конфиденциальности и обеспечения защиты данных в соответствии с применимым законодательством. Любые персональные данные, предоставленные Вами Компании, будут храниться и использоваться только Компанией и/или ее аффилированными лицами и не будут предоставлены третьим лицам, за исключением случаев, предусмотренных применимым законодательством. Все персональные данные будут обрабатываться исключительно в целях выполнения обязательств Компании по Договору или иных договоров, заключенных между Пользователем и Компанией в связи с использованием ПО. В случае если Вы предоставляете, в том числе данные о юридическом лице, Вы подтверждаете, что имеет для этого достаточно полномочий, а предоставляемая Вами информация является полной и достоверной.

10.4. Контактные данные Компании:

АО «СОЛАР СЕКЬЮРИТИ»

Адрес местонахождения: 127015, Г.МОСКВА, ВН.ТЕР.Г. МУНИЦИПАЛЬНЫЙ ОКРУГ САВЕЛОВСКИЙ, УЛ ВЯТСКАЯ, Д. 35, СТР. 4

Адрес почтовый: 125009, г. Москва, Никитский пер., 7, стр. 1

Контактный телефон/факс: +7 499 755 07 70

email: info@rt-solar.ru

Дата создания документа: «31»мая 2026

10.5. Приложения к Договору:

Приложение №1 – Метрики лицензирования ПО.

Приложение №2 - Функциональные характеристики ПО.

Метрики лицензирования для ПО линейки Солар Программный Комплекс Обнаружения и Реагирования

- По количеству конечных устройств (узлов) с установленным агентом Солар Программный Комплекс Обнаружения и Реагирования

Функциональные характеристики ПО

Общие функциональные характеристики ПО Солар Программный Комплекс Обнаружения и Реагирования

- **Непрерывный сбор телеметрии:** Фоновый мониторинг в реальном времени всех событий на конечных точках: запуск и завершение процессов, обращения к файловой системе, изменения в реестре, сетевые соединения, действия пользователей и вход в учетные записи.
- **Продвинутое детектирование угроз:** Выявление сложных целевых атак и скрытых угроз на основе поведенческого анализа, машинного обучения, сигнатурного анализа и сопоставления с индикаторами компрометации и индикаторами атак.
- **Расследование инцидентов:** Визуализация цепочек атак, полнотекстовый поиск по всей накопленной телеметрии, анализ первопричин инцидента с отображением точки входа и затронутых ресурсов.
- **Активное реагирование:** Изоляция скомпрометированных хостов от сети, принудительное завершение вредоносных процессов, удаленный запуск диагностических и исправляющих сценариев.
- **Интеграция со сторонними системами:** Поддержка стандартизированных протоколов обмена данными об угрозах, открытые программные интерфейсы для взаимодействия с системами управления событиями безопасности, системами автоматизации реагирования и внешними источниками данных об угрозах.

Солар Программный Комплекс Обнаружения и Реагирования включает в себя следующие подсистемы:

1. Сервер управления Солар Программный Комплекс Обнаружения и Реагирования
2. Агент Солар Программный Комплекс Обнаружения и Реагирования для Windows
3. Агент Solar EDR для Linux

Сервер управления

- **Централизованное управление:** Единая консоль для настройки политик безопасности, массового развертывания и обновления агентов на всех конечных точках, управления группами устройств и назначения прав администраторам.
- **Аналитическая обработка:** Агрегация телеметрии со всех агентов, нормализация данных к единому формату, корреляция событий между различными узлами для выявления распределенных атак.
- **Долгосрочное хранение:** Сохранение всей телеметрии и событий безопасности в централизованном хранилище с настраиваемым сроком хранения, поддержка полнотекстового поиска по историческим данным за весь период.

- **Программные интерфейсы:** Открытые программные интерфейсы для интеграции со сторонними системами безопасности, возможность автоматизированного получения данных об инцидентах и отправки команд реагирования.
- **Защита самой системы:** Ролевая модель управления доступом с разделением обязанностей администраторов, подробное логирование всех действий операторов в консоли, поддержка многофакторной аутентификации.

Агент для Windows

- **Сбор телеметрии:** Глубокий мониторинг в реальном времени с использованием встроенной подсистемы трассировки событий операционной системы и перехвата программных вызовов, что обеспечивает высокую детализацию без значительной нагрузки на систему.
- **Объекты мониторинга:** Отслеживание запуска и завершения процессов, создания дочерних процессов, изменений в системном реестре, операций с файлами на диске, сетевых соединений, загрузки драйверов и модулей в память процессов.
- **Поведенческий анализ:** Выявление безфайловых атак, горизонтального перемещения злоумышленников между узлами, попыток повышения привилегий, внедрения кода в легитимные процессы и других аномалий поведения.
- **Функции реагирования:** Локальная изоляция хоста от сети с сохранением канала связи с сервером управления, принудительное завершение подозрительных процессов, удаленный сбор образцов памяти и дисков для экспертизы.
- **Производительность и совместимость:** Оптимизированное потребление ресурсов процессора и оперативной памяти, поддержка всех актуальных клиентских и серверных версий операционной системы Windows, включая 32- и 64-разрядные архитектуры.

Агент для Linux

- **Сбор телеметрии:** Глубокий мониторинг на уровне ядра операционной системы с использованием технологии расширенного мониторинга ядра или перехвата системных вызовов, что обеспечивает полную видимость событий без модификации ядра.
- **Объекты мониторинга:** Отслеживание деревьев процессов, системных вызовов, изменений в критических каталогах файловой системы, операций с исполняемыми файлами, сетевой активности, загрузки модулей ядра и действий привилегированных пользователей.
- **Поддержка дистрибутивов:** Совместимость с основными дистрибутивами, включая коммерческие и отечественные операционные системы на базе ядра Linux, с поддержкой различных версий ядра и пакетных менеджеров.
- **Функции реагирования:** Блокировка вредоносных процессов, изоляция узла от сети, удаление вредоносных артефактов, удаленный запуск диагностических сценариев, сбор информации о состоянии системы для расследования.

- **Производительность:** Легковесная архитектура в виде служебного процесса пользовательского пространства или с использованием технологии расширенного мониторинга ядра, обеспечивающая минимальное влияние на производительность защищаемой системы.