SOLAR

SOLAR AURA

Инструкция по эксплуатации

МОСКВА, 2024

W:RT-SOLAR.RU

Описание работы и принципы классификации событий

ОБЩИЕ СВЕДЕНИЯ

Программный комплекс (ПК) Solar AURA предоставляется по модели SaaS. Для работы с ПК требуется веб-браузер. Доступ и администрирование может осуществляться как с персональных компьютеров, так и с мобильных устройств. AURA не требует применения дополнительных технических решений на стороне заказчика и их интеграции в его инфраструктуру.

Взаимодействие с ПК осуществляется через веб-интерфейс, расположенный по адресу: https://aura.rt-solar.ru.

Доступ в личный кабинет осуществляется по паролю. На этапе подключения для заказчика формируется учетная запись администратора. В дальнейшем заказчик может самостоятельно создавать учетные записи для сотрудников и назначать им соответствующие права.

В случае получения первоначального доступа вам придёт приветственное письмо с адреса aura@rt-solar.ru, где будут указаны логин и пароль. После этого пароль следует поменять. Если приветственное письмо не пришло либо возникли проблемы со входом, а также по всем остальным вопросам, связанным с получением доступа в веб-интерфейс AURA, следует написать на адрес aura@rt-solar.ru.

Доступ в личный кабинет осуществляется по паролю. На этапе подключения для заказчика формируется учетная запись администратора. В дальнейшем заказчик может самостоятельно создавать учетные записи для сотрудников и назначать им соответствующие права.

Структура ПК представляет собой 12 независимых направлений, каждое из которых является самостоятельной аналитической системой, оперирующей своими специфическими источниками данных и предназначенной для выявления определенных категорий событий и реагирования на них.

Каждое направление имеет собственную статистическую информационную панель (дашборд), а также деление на отдельные категории событий для простоты поиска и классификации угроз.

Антифишинг в составе Solar AURA обеспечивает полный цикл противодействия фишингу: от выявления доменных имен и интернет-ресурсов, которые могут быть использованы в целях осуществления противоправных действий в отношении Заказчика или от имени Заказчика (например, для введения в заблуждение клиентов и последующего хищения денежных средств или конфиденциальной информации), до реализации комплекса мер, направленных на прекращение функционирования подобных ресурсов.

Для удобства работы **Антифишинг** включает в себя три основных подраздела: «Домены», «Контент» и «Блокировка сайтов».

ДОМЕНЫ

Принцип работы

В целях выявления потенциально опасных доменных имен используются методы сбора информации, позволяющие обнаруживать доменные имена, визуально или морфологически схожие с доменным именем Заказчика. Например, если мы допустим, что официальным доменом заказчика является домен company.ru, то в поле зрения системы попадут, например, такие доменные имена, как c0mpany.ru, company-s.ru, connpany.ru, company.freepay.online и т.д.

Выявленные домены попадают в базу данных AURA и проходят процедуру оценки, после чего попадают к аналитику, который определяет категорию события и оценивает ресурсы на предмет наличия маркеров угрозы.

КОНТЕНТ

Подраздел входит в направление «Антифишинг» и позволяет выявлять потенциально опасные для Заказчика сайты и отдельные страницы сайтов, не использующие в доменном имени каких-либо отсылок к названию официального ресурса.

В случае выявления сайтов, содержащих в теле страницы соответствующие ключевые слова, они проходят оценку аналитиком, после чего попадают в соответствующий раздел в личном кабинете AURA.

БЛОКИРОВКА ВРЕДОНОСНЫХ РЕСУРСОВ

Направление «Антифишинг» Solar AURA обеспечивает полный цикл противодействия фишингу: от выявления фишинговых сайтов до их блокировки. ПК позволяет одним кликом отправлять опасные домены на блокировку из личного кабинета, минуя переписку по почте, что делает реагирование на инцидент более оперативным.

Данная аналитическая система предназначена для поиска в сети Интернет информации ограниченного доступа, а также сведений о прямых или косвенных утечках, затрагивающих заказчика.

Для удобства пользования выявляемые события разделены на три подраздела: «Массивы данных», «Аккаунты» и «Репозитории».

МАССИВЫ ДАННЫХ

В раздел «Массивы данных» попадают сведения, которые можно поделить на три глобальные категории.

1. Информация об обнаруженных в открытых источниках конфиденциальных документах и сведениях ограниченного доступа, имеющих отношение к заказчику. Это могут быть как непосредственно документы (файлы), так и различные площадки для совместной работы или групповые чаты в мессенджерах, в которых размещается конфиденциальная информация. Главным критерием отбора событий является доступность сведений для неограниченного круга лиц.

2. Прямые утечки. Данная категория аккумулирует информацию о выставленных на продажу или размещенных на специализированных ресурсах массивах конфиденциальных данных или предложениях о продаже массивов конфиденциальных данных, имеющих прямое отношение к Заказчику.

3. Косвенные утечки – анализ размещаемых в открытом доступе баз данных сторонних организаций на предмет наличия в них информации о компании заказчика таких, как корпоративные адреса электронной почты, пароли и прочие чувствительные сведения.

АККАУНТЫ

Solar AURA в автоматическом режиме осуществляет анализ данных о попадании корпоративных адресов электронной почты в открытый доступ в сочетании с паролями. Источниками данных являются базы публичных утечек и собственные массивы аналитических данных.

РЕПОЗИТОРИИ

Данная аналитическая подсистема предназначена для выявления случаев попадания в публичные репозитории конфиденциальных данных.

Также в данный раздел попадают репозитории, содержащие вредоносное программное обеспечение или цели для DDoS-атак, в случае если в них фигурирует упоминание инфраструктуры заказчика.

УСЛУГИ

В рамках данного направления система аккумулирует данные, накопленные в процессе автоматизированного мониторинга более двух десятков активных российских и зарубежных даркнет-форумов в зоне .onion, нескольких тысяч активных Telegram-каналов и сотен других «теневых» интернет-площадок на предмет выявления предложений или запросов оказания нелегальных или потенциально опасных услуг, имеющих непосредственное отношение к Заказчику. Ежедневное количество обрабатываемых сообщений составляет более 20 тысяч.

Перечень информационных источников ежедневно дополняется и корректируется. Для доступа в закрытые части форумов создаются и поддерживаются десятки учетных записей, осуществляется внедрение в закрытые и законспирированные информационные сообщества.

БРЕНД

В контексте данного направления Solar AURA выявляет аккаунты в социальных сетях и мессенджерах, а также иные публичные ресурсы, неправомерно использующие средства индивидуализации, и отслеживает факты публикации мобильных приложений на неофициальных и небезопасных площадках.

В подразделе «Мобильные приложения» отражается информация об обнаруженных мобильных приложениях, использующих наименование и логотип, схожие до степени смешения с официальными приложениями Заказчика.

Это могут быть как факты размещения фейковых приложений в официальных маркетплейсах, так и публикации приложений на неофициальных площадках, что встречается значительно чаще. Такие площадки не могут гарантировать безопасность и неизменность корпоративного приложения, поэтому подобные факты являются нежелательными.

Каждое обнаруженное приложение проходит базовую проверку на наличие вредоносного программного обеспечения.

Так же, как и в случае с направлением «Антифишинг», в рамках направления «Бренд» возможна блокировка обнаруженных системой или переданных Заказчиком мобильных приложений.

МЕДИА

Система мониторинга упоминаний компании и её первых лиц на основе анализа широкого перечня открытых источников в сети «Интернет». В рамках направления осуществляется классификация по типам площадок: «Социальные сети», «СМИ», «Сайты-отзовики» и так далее, для чего созданы соответствующие подразделы.

ЮРИДИЧЕСКИЕ ЛИЦА

Автоматически пополняемая в ежедневном режиме база потенциально неблагонадежных организаций: юридических лиц и ИП, выставленных (или выставлявшихся ранее) на продажу на теневом рынке в тематических каналах и на форумах. Информация, представленная в этой базе, не имеет аналогов ни в одном сервисе проверки контрагентов. Она позволяет оперативно отслеживать компании и ИП, которые могут быть использованы для противоправных действий: обналичивания, фиктивных сделок, налоговых махинаций.

Источниками для пополнения базы являются тематические теневые сайты и форумы в сети Интернет и DarkNet, а также Telegram-каналы, в том числе закрытые чаты, и другие сетевые сообщества.

ЛИЧНЫЙ БРЕНД

Раздел собирает информацию из разделов «Утечки», «Медиа» и «Бренда», связанную с ключевыми персонами заказчика, перечень которых содержится в договоре, приложении к нему или соглашении о пилотном подключении.

В раскрывающемся списке отображается перечень ключевых лиц, в отношении которых осуществляется мониторинг.

ЭКВАЙРИНГ

В данном разделе фиксируются события, накопленные в процессе мониторинга ресурсов противоправной тематики и анализа используемых ими платежных инструментов.

В случае выявления нелегальных платежных шлюзов, оперирующих посредством интернет-эквайринга банка-заказчика или с использованием эмитированных им банковских карт, в системе фиксируется ключевая информация по каждому выявленному факту.

ИНФРАСТРУКТУРА

В отличие от других направлений, целью которых является сбор данных из внешних источников информации, задачей направления «Инфраструктура» является постоянный автоматизированный мониторинг внешней IT-инфраструктуры заказчика на предмет выявления признаков уязвимостей и векторов возможной компрометации, в том числе открытых портов, устаревших версий программного обеспечения, протоколов и так далее.

Направление включает в себя три подраздела: «Серверы», «Хосты», «Домены и сертификаты» и «Конечные точки».

СЕРВЕРЫ

Данная подсистема отвечает за круглосуточное сканирование всех портов корпоративного хоста, имеющего выход в сеть интернет, на предмет выявления различных угроз, в том числе появления новых открытых портов, обнаружения признаков используемого программного обеспечения, имеющего незакрытые критические уязвимости и т.д.

ХОСТЫ

В рамках данного направления осуществляется сканирование диапазонов IP-адресов. В рамках сканирования отслеживается появление новых рабочих хостов в подсетях и производится сканирование **базовых используемых портов** на выявленных активных хостах.

Подсистема может применяться для объективного контроля широкого перечня доступных извне корпоративных ресурсов, не относящихся к критической инфраструктуре.

ДОМЕНЫ И СЕРТИФИКАТЫ

Подсистема предназначена для регулярного (еженедельного) контроля сроков окончания действия SSL-сертификатов и сроков регистрации доменных имен. Помимо отслеживания окончания срока действия сертификатов система может оповещать о смене удостоверяющего центра, выдавшего сертификат.

КОНЕЧНЫЕ ТОЧКИ

В модуле показаны эндпоинты, уязвимости, открытые порты и другая любая информация, которой могут воспользоваться хакеры на этапе подготовки к атаке на компанию, которую они

ОБЩИЕ ДАННЫЕ

Все направления и подразделы Solar AURA базируются на едином дружественном пользователю интерфейсе и имеют общие принципы вывода информации. Все направления и подразделы снабжены внутренними поисковиками, позволяющими создавать выборки по разным критериям и лучше ориентироваться в выдаваемой Заказчику информации.

Угрозы, выявленные ПК и подтвержденные аналитиками, появляются в личном кабинете Клиента в режиме реального времени.

ОТЧЕТЫ

Solar AURA позволяет в автоматическом режиме сформировать отчет за любой период времени. В данном разделе можно выбрать период, за который требуется сформировать отчет, и при необходимости ограничить его лишь критическими сработками.