Контроль удаленного доступа в сетях АСУ ТП

Мониторинг работы удаленных сотрудников и подрядчиков

ptsecurity.com

БИЗНЕС-РИСКИ

В период общей обеспокоенности распространением вируса COVID-19, когда большинство компаний вынужденно отменяют командировки своих сотрудников на обслуживаемые ими предприятия, удаленный доступ становится незаменимым инструментом для поддержания непрерывной работы производственных процессов. Удаленное подключение может использоваться для наладки оборудования, диагностики и оперативного исправления проблем. Это удобно и позволяет быстро решить необходимые задачи.

Вместе с тем удаленный доступ порождает и серьезные риски безопасности предприятия: учетные данные для доступа в сеть АСУ ТП могут быть переданы третьим лицам или украдены; личные компьютеры пользователей, с которых производится удаленный доступ, могут быть заражены вредоносным ПО.

Отсутствие должного контроля за удаленным доступом в АСУ ТП может привести к серьезным последствиям: к полной остановке технологического процесса из-за распространения вирусов-шифровальщиков или целенаправленного саботажа, краже коммерческих секретов компании, злонамеренным манипуляциям параметрами тех. процесса в целях кражи доли сырья или выхода продукции.

КАК СНИЗИТЬ РИСКИ

В условиях, когда невозможно контролировать непосредственно компьютеры удаленных пользователей, на помощь приходят средства инструментального мониторинга действий пользователей, подключенных к сети АСУ ТП.

Решение для контроля удаленного доступа в АСУ ТП от Positive Technologies позволяет:

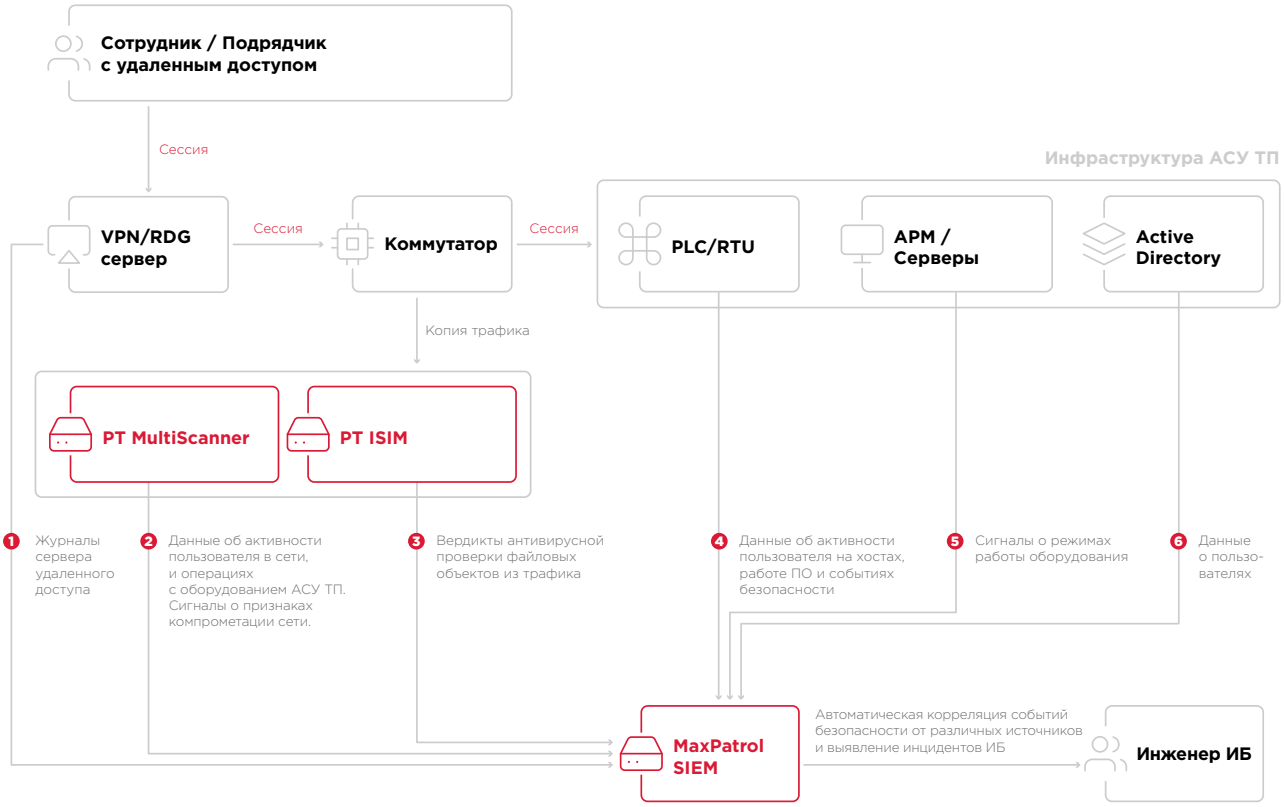
- Выявлять нелегитимные соединения, сопоставляя ключевые данные о сотрудниках с данными сервера удаленного доступа.
- Журналировать взаимодействие удаленных пользователей с оборудованием АСУ ТП (изменение проектов и конфигураций ПЛК, изменение режимов работы ПЛК и так далее).
- Выявлять следы проникновения вредоносного ПО в сеть АСУ ТП через удаленные соединения.
- Выявлять следы компрометации сети АСУ ТП через удаленные соединения.
- Оценивать активность подключенных пользователей, обнаруживать аномалии в их действиях и сигнализировать о нарушениях политик безопасности.
- Выявлять установку/запуск нелегитимного ПО на узлах сети (АРМ-ы, серверы SCADA, HMI).
- Хранить полную копию трафика пользовательских сессий в целях аудита и расследования.

Для решения задачи контроля удаленного доступа могут быть использованы следующие продукты:

Система анализа трафика промышленных сетей **PT ISIM**
Система многоуровневой защиты от вредоносного ПО **PT Multiscanner**
Система выявления инцидентов ИБ **MaxPatrol SIEM**

КАК ЭТО РАБОТАЕТ

PT ISIM анализирует копию трафика сессий удаленных пользователей. Продукт поддерживает более 80 сетевых протоколов, включая популярные промышленные (Siemens S7, Emerson DeltaV, Schneider Electric UMAS, ModBus, IEC 60870-5-104, IEC 61850, BacNet и другие). Это позволяет полностью реконструировать активность пользователя в сети АСУ ТП, выявлять команды управления оборудованием (ПЛК/RTU/РЗА), фиксировать подозрительные действия удаленных пользователей, а также факты компрометации сети АСУ ТП и закрепления злоумышленника в ней. PT ISIM также хранит полную копию трафика сессий пользователей, что крайне важно для организации эффективного расследования инцидентов ИБ.



Трафик сессий удаленных пользователей также проверяется с помощью PT MultiScanner. Продукт проверяет все файлы, попадающие в инфраструктуру, с использованием нескольких антивирусов и уникальных репутационных списков Positive Technologies. Продукт хранит файловые объекты, извлеченные из трафика, и производит их регулярную перепроверку — это позволяет обнаружить ранее неизвестную угрозу, предотвратить её распространение, а также существенно облегчает расследование инцидентов ИБ.

PT ISIM и PT MultiScanner передают данные об активности пользователей в сети, факты манипуляций с оборудованием АСУ ТП и сигналы о проникновения ВПО в периметр сети АСУ ТП в MaxPatrol SIEM.

MaxPatrol SIEM сопоставляет данные, полученные из разных источников: о пользователях АСУ ТП из Active Directory, информацию о подключениях к VPN/RDG-серверу, данные об активности пользователей от PT ISIM, информацию от PT MultiScanner о пользователях, в чьих сессиях обнаружено ВПО, информацию о манипуляциях с ПО на узлах сети (АРМ-ы и серверы SCADA), данные о текущем состоянии работы оборудования АСУ ТП если это возможно и необходимо.

Таким образом, совокупность возможностей PT ISIM, PT Multiscanner и MaxPatrol SIEM помогает специалисту ИБ предприятия увидеть полную картину действий удаленных пользователей в сети АСУ ТП и вовремя предпринять необходимые меры по предотвращению нарушений ИБ, несущих угрозу непрерывности производства.

ВАШИ НОВЫЕ ВОЗМОЖНОСТИ

С помощью решения для контроля удаленного доступа в АСУ ТП от Positive Technologies ответственный специалист службы ИБ предприятия:

1. Узнает о случаях, когда обнаружено нелегитимное подключение удаленного пользователя к сети АСУ ТП через VPN/RDG-сервер: подключение в нерабочие часы или в несогласованное время, подключение с подозрительных адресов, подключение через подбор пароля и так далее.
2. Сможет оперативно выявлять операции, совершенные конкретным пользователем с оборудованием АСУ ТП в ходе подключения к сети (пуск/останов ПЛК, чтение и загрузка проектов в ПЛК, перенастройка конфигураций ПЛК/RTU) и выявлять нелегитимную активность.
3. Сможет получать оперативные вердикты о вредоносности файловых объектов, загружаемых пользователем на ресурсы в сети АСУ ТП, а также видеть признаки активности вредоносного ПО, действующего со стороны компьютера удаленного пользователя.
4. Сможет получать оповещения об установке и запуске удаленным пользователем нелегитимного программного обеспечения на узлах сети АСУ ТП.
5. Сможет провести полный ретроспективный анализ действий удаленного пользователя, используя записанную PT ISIM копию трафика сессии, копию файловых объектов, извлеченных из трафика сессии PT Multiscanner, а также информацию о критических событиях, полученных с сервера удаленного доступа, узлов сети АСУ ТП и другого оборудования, доступную в MaxPatrol SIEM.

Таким образом, решение задач контроля удаленного доступа в АСУ ТП на базе продуктов от Positive Technologies позволяет ответственным подразделениям предприятия:

- Полностью контролировать соблюдение регламентов и политик ИБ в АСУ ТП при обеспечении удаленного доступа к технологическим сетям.
- Выполнять проактивный поиск угроз (Threat Hunting), исходящих от удаленных пользователей (как сотрудников, так и подрядных организаций), нацеленных на нарушение работы технологических процессов предприятия со стороны.

ptsecurity.com
pt@ptsecurity.com
facebook.com/PositiveTechnologies
facebook.com/PHDays

ICS_remote_control_security_A4.RUS.0001.01.MAY.13.2020