CYBERBIT
PROTECTING A NEW DIMENSION

SCADAShield

УНИКАЛЬНОЕ РЕШЕНИЕ, ПРЕДЛАГАЮЩЕЕ КОМПЛЕКСНЫЙ ПОДХОД К КИБЕРБЕЗОПАСНОСТИ ПРОМЫШЛЕННЫХ СИСТЕМ УПРАВЛЕНИЯ

Задачи

Основным вызовом, стоящим перед компаниями, отвечающими за эксплуатацию критических инфраструктур, является взрывное развитие информатизации промышленных сетей управления производственными объектами (АСУ и АСУТП) и их интеграция с офисными корпоративными сетями (ИТ), в связи с чем, уязвимость безопасности офисных сетей становятся серьезной угрозой для промышленных сетей. Практически все известные атаки на промышленные сети, в последнее время, строятся на эксплуатации уязвимостей офисных сетей, имеющих информационное взаимодействие с промышленными сетями. Например, атаки на магистральную электроэнергетическую сеть в Украине (2015, 2016 гг.) или сталелитейный завод в Германии (2015 г.). Злоумышленники научились использовать проблемы с безопасностью офисных сетей для подготовки целевых атак, наряду с «традиционными» проблемами промышленных сетей управления: уязвимыми и незащищенными промышленными протоколами, распределенной инфраструктурой и ее недостаточной наблюдаемостью. Поэтому для обеспечения кибербезопасности промышленных сетей, сегодня, необходимо применять новые подходы и инструменты, которые будут соответствовать вновь появляющимся угрозам и обеспечивать их обнаружение, в независимости от местонахождения источника в офисной или промышленной сети.

ВАШ СЕРЬЕЗНЫЙ И НАДЕЖНЫЙ ПАРТНЕР

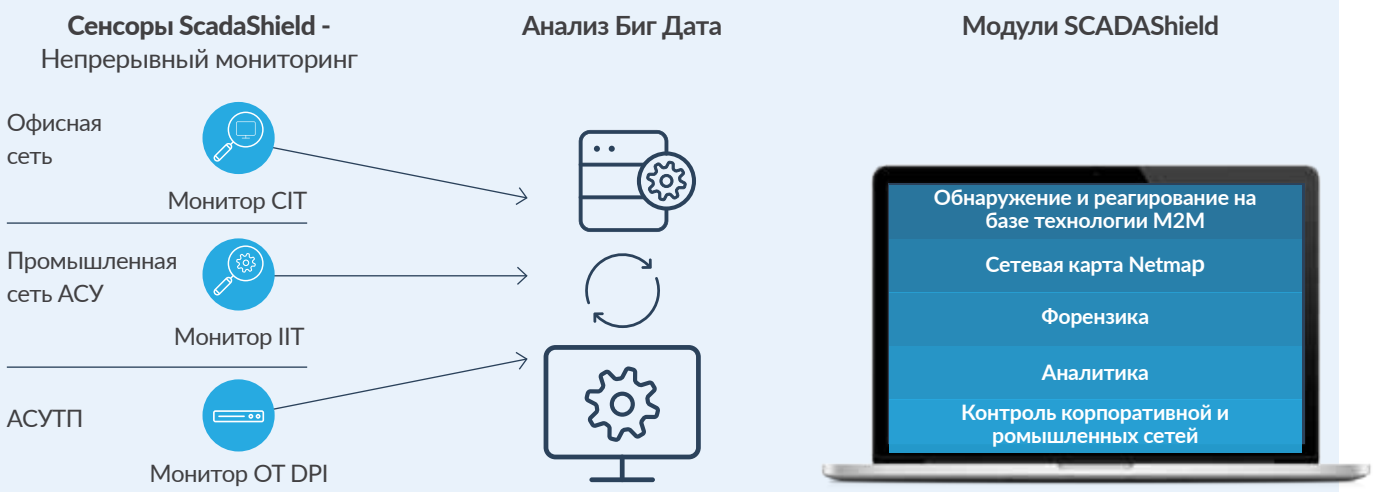
Компания Cyberbit полностью принадлежит компании Elbit Systems (NASDAQ: ESLT), глобальному провайдеру технологических решений по обеспечению защиты и национальной безопасности. Со своими офисами на 4 континентах, компания Cyberbit предоставляет надежные услуги по обеспечению безопасности энергетических и нефтегазовых предприятий, аэропортов, производителей и правительств в качестве долгосрочного партнера, обеспечивающего безопасность операционных сетей данных структур.

SCADAShield - Щит кибербезопасности для промышленных систем управления

Система SCADAShield представляет собой многоуровневое технологическое решение для обеспечения обнаружения угроз, повышения наблюдаемости, экспертного поведенческого анализа и предотвращения атак на промышленные системы управления. Система SCADAShield обеспечивает непрерывный мониторинг и обнаружение, в офисных и промышленных сетях, угроз информационной безопасности и надежности технологических процессов.

Обнаружение и наблюдаемость в корпоративных и промышленных сетях

Многоуровневый подход Системы SCADAShield позволяет обнаруживать векторы атак, направленные из офисных в промышленные сети, а также из АСУ в АСУТП внутри промышленных сетей. Сенсоры системы SCADAShield осуществляют неинвазивный мониторинг сети передачи данных АСУТП, а также мониторинг АСУ, ИТ и шлюзов между сегментами офисной и промышленной сетей. Все данные собираются в Биг Дата хранилище и, используя специализированные инструменты, анализируются на предмет отклонений от стандартных поведенческих моделей, комбинируя данные офисных и промышленных сетей. Автоматически ведется и отображается карта сети передачи данных и информационных потоков в режиме реального времени, все данные непрерывно доступны для исследования и анализа.



Обеспечение сетевой безопасности и целостности промышленной сети

1. Непрерывное обнаружение и реагирование в рамках всего набора угроз - АСУТП, АСУ и ИТ
2. Автоматическое обнаружение, контроль и визуализация объектов в сети АСУТП
3. Автоматическая идентификация изменений в сети АСУТП и их визуализация.
4. Автоматические оповещения о подозрительной деятельности в режиме реального времени
5. Отслеживание несанкционированных устройств, средств связи и действий
6. Снижение уязвимости оборудования и протоколов, эксплойтов и вопросов безопасности
7. Проведение расследований, анализа первопричины атаки и эффективное реагирование
8. Простая и быстрая индивидуальная настройка пользовательских интерфейсов и отчетов, идентификация тенденций и извлечение оперативных данных.
9. Соответствие стандартам промышленных сетей.

Три уровня мониторинга

В состав SCADAShield входят три типа сенсоров для осуществления мониторинга и обнаружения атак на офисные и промышленные сети:

- **Монитор OT DPI** пассивный и неинвазивный анализ пакетов промышленных протоколов (DPI), сетевого взаимодействия в сети АСУТП, с локальным детализированным анализом данных, передаваемых как по сети Ethernet, так и по сериальным последовательным соединениям (RS-485, RS-232). Обеспечена поддержка большинства стандартных промышленных протоколов и части проприориетарных протоколов известных производителей, обеспечивается расширение библиотеки поддерживаемых протоколов по требованиям Заказчиков.
- **Промышленный Монитор IT –** программный агент для конечных устройств в составе АСУ (таких как архивный сервер, контроллер доменов, SCADA сервер, рабочие места оперативного персонала), собирающий детальные данные по поведению пользователей и программных приложений, для построения и анализа поведенческих моделей на центральном сервере системы.
- **Корпоративный Монитор IT –** программный агент, обеспечивающий непрерывный мониторинг критически важных шлюзов между офисной и промышленной сетями, сбор детальных данных по каждому из них. Реагирование и меры предотвращения могут реализовываться непосредственно агентской программой на уровне ядра для быстрого устранения угрозы.

Централизованная аналитика безопасности на базе Больших Данных

В SCADAShield применяются алгоритмы машинного обучения и автоматического формирования правил и поведенческих паттернов, а также анализ и выявление несоответствий в текущих поведенческих моделях. Корреляция и совместный анализ данных офисных и промышленных сетей обеспечивает обнаружение любого аномального поведения, как на базе ранее сформированных автоматически и вручную поведенческих паттернов, так и правил, сформированных на базе известных уязвимостей SCADA и промышленных протоколов. Используемый механизм анализа Биг Дата адаптируется, в соответствии с требованиями Заказчика, обеспечивая его работу, согласно штатным сетевым шаблонам.

Основные характеристики

Обнаружение и Реагирование - в корпоративных и промышленных сетях

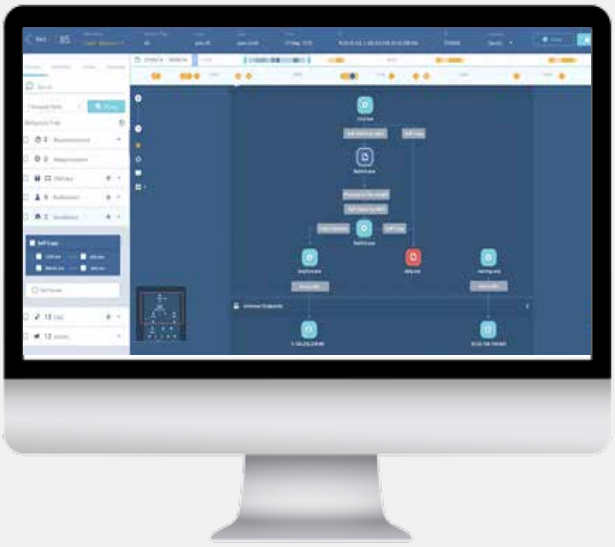
Быстрая идентификация и реагирование на первостепенные угрозы, включая векторы атак из офисной в промышленную сеть. SCADAShield обнаруживает и автоматически классифицирует любые аномальные действия, как в офисной, так и в промышленной сетях. Система проводит корреляцию данных ИТ, АСУ и АСУТП для повышенного качества обнаружения и идентификации угроз. Все оповещения предоставляют подробные данные для расследования и анализа, обеспечивая детальную видимость для аналитиков и операторов. Реагирование может легко осуществляться посредством сенсоров различных типов, позволяя аналитикам быстро действовать и устранять угрозы. Совмещение анализа поведенческих паттернов и известных уязвимостей позволяет предотвратить практические любые типы атак, как известные, так и вновь разрабатываемые.

Основные характеристики

SCADAShield - карта сети передачи данных и информационных потоков

Netmap визуализация сетевого взаимодействия- автоматическое обнаружение и контроль изменений в режиме реального времени

Модуль Netmap системы SCADAShield позволяет обеспечить наблюдаемость топологии и информационных потоков в сети передачи данных, идентифицировать шлюзы между офисными и промышленными сетями, а также проводить экспертно-аналитические расследования. Netmap автоматически формирует карту сети и предоставляет полную наблюдаемость промышленной сети. Модуль отображает, как IP-сегменты, так и сериальные сегменты сети АСУТП, указывает типы конкретных протоколов, используемые между устройствами, выделяет потенциальные риски и сигнализирует о всех изменениях.



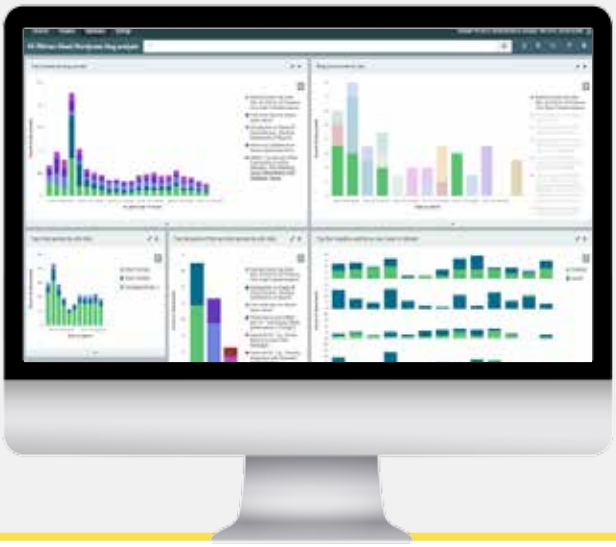
SCADAShield. Форензика - автоматическая визуализация всей истории атаки

Форензика – архивы и данные в режиме реального времени, в сочетании с системой отображения для обеспечения быстрого определения первопричины и реагирования

SCADAShield собирает подробные данные с офисной и промышленной сети, а также предоставляет аналитические инструменты для анализа и проведения расследований на базе собранных данных. Аналитики и сетевые менеджеры с имеют удобный доступ как к архивным данным, так и к данным, получаемым в режиме реального времени для расследования событий, изучения архивов и осуществления упреждающих действий по предотвращению угроз. Форензика SCADAShield предоставляет усовершенствованную графическую визуализацию всей истории атак, как для векторов атак на базе технологии M2M, так и атак из офисных сетей и наоборот, позволяя аналитикам быстро идентифицировать первопричину и незамедлительно реагировать на угрозу.

Аналитика – Усовершенствованный интерфейс, отчеты и инструменты визуализации для повышения удобства работы оперативного персонала

Аналитика SCADAShield обеспечивает индивидуальную настройку интерфейсов и отчетов для идентификации тенденций и обеспечения наблюдаемости данных. Терабайты собранных данных трансформируются в аналитические отчеты, предоставляя возможность пользователям анализировать данные «вдоль и поперек», на основе любого желаемого сочетания. Аналитика SCADAShield поддерживает построение визуальных моделей для всех уровней сети.



SCADAShield Аналитика

О КОМПАНИИ CYBERBIT™

Cyberbit предлагает передовые решения в области кибербезопасности для финансовых организаций, предприятий критической инфраструктуры, военных и правительственных организаций. Портфолио компании предоставляет полный набор продуктов для обнаружения и митигации кибератак, а также помогает нашим Заказчикам решать оперативные задачи управления кибербезопасностью. Портфолио Cyberbit включает в себя решения по обнаружению и реагированию для конечных устройств (EDR), по кибербезопасности и контроля бесперебойной работы SCADA (SCADAShield), по автоматизации процессов управления SOC (SOC 3D), а также по подготовке персонала для обеспечения кибербезопасности на базе полнофункционального симулятора (Range). Продукты компании Cyberbit были выбраны крупными международными корпорациями по всему миру для обеспечения кибербезопасности своих сетей.

Cyberbit является стопроцентной дочерней компанией Elbit Systems Ltd. (NASDAQ и TASE: ESLT)

sales@cyberbit.net | www.cyberbit.net

Офис в Израиле:

CYBERBIT Commercial Solutions Ltd.
22 Zarhin St. Ra'anana
Israel 4310602
Тел.: +972-9-7799800 | E-mail: sales@cyberbit.net

CYBERBIT
PROTECTING A NEW DIMENSION