CYBERBIT
PROTECTING A NEW DIMENSION

SCADAShield

Впервые: платформа безопасности АСУ ТП

Визуализация, безопасность, управление активами и непрерывность OT / СКАДА

Безопасность OT отстает на годы

Созданные задолго до Интернета, одноуровневые архитектуры, без онлайн-доступа, автоматизации или удаленного управления, среды АСУ ТП представляют собой серьезные проблемы как для ИТ-, так и для OT- специалистов:

- **Отсутствие визуализации и «слепые зоны»**
- **OT-угрозы из ИТ-сетей**
- **Неприменимость существующих ИТ-решений**
- **Конфликт ответственности между ИТ и OT**

SCADAShield – проверенная OT-ИТ безопасность

От этих угроз с 2010 года наиболее критические инфраструктуры защищает SCADAShield, используя проверенную технологию для обнаружения и снижения кибер-угроз всему OT-ИТ стеку, останавливающую известные и неизвестные “zero-day” угрозы до того, как они смогут причинить физический ущерб.

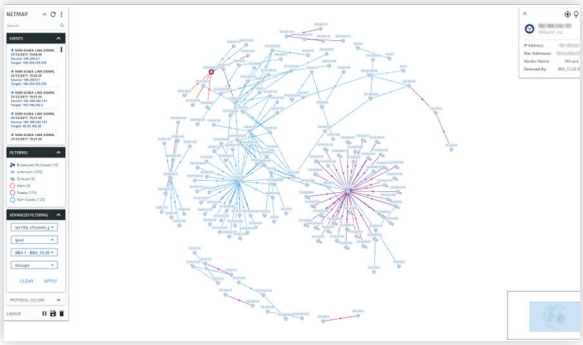
Детальное представление вашей OT-ИТ среды

Практически немедленно после развертывания SCADAShield, в реальном времени Вы получаете полное визуальное представление всех ИТ- и OT- активов, сетевой архитектуры и информационных потоков. Большинство впервые видит все устройства всех сетей - это важнейший первый шаг в обеспечении безопасности. Используя пассивное, неинвазивное зеркалирование портов и детальный анализ пакетов (DPI) 7-ми уровней, SCADAShield обеспечивает:

- **Полное отображение OT-сетей,** создавая в реальном времени карту сети, отображая информационные потоки и OT-ИТ протоколы между всеми устройствами.
- **Мгновенная идентификация рисков** позволяет получать информацию о наиболее уязвимых элементах, и проводить расследование критических инцидентов.

Используйте SCADAShield чтобы:

- **Получить полное представление** о ваших OT- и ИТ-сетях и активах.
- **Определить известные угрозы** и прикрыть уязвимости OT- и ИТ-у-стройств и протоколов.
- **Определить наиболее вероятные неизвестные** ‘zero-day’ угрозы OT
- **Определить и снизить** опера-ционные ошибки и неверные конфигурации
- **Соответствие требованиям**

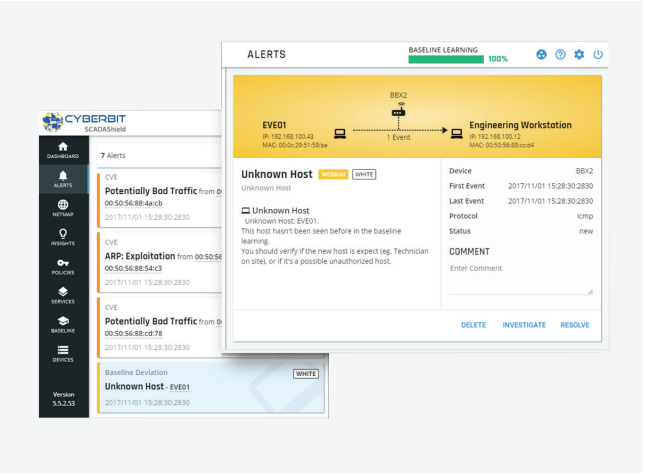


Автоматически генерируемая SCADAShield карта сети

Обнаружение Известных и Неизвестных угроз OT и ИТ.

При подключении у промышленной среде SCADAShield автоматически:

- **Определит исходные условия для организации защиты сети**
- **Автоматически создаст политики управления;** Вы также можете создавать свои политики
- **Обнаружит известные уязвимости Ваших устройств,** и предоставит руководства по восстановлению и реагированию
- **Зафиксирует аномалии поведения,** включая подозрительные инструкции и команды, которые могут указывать на кибератаку
- **Идентифицирует операционные риски** такие как неисправность или ошибки конфигурирования, предоставив возможность немедленного восстановления

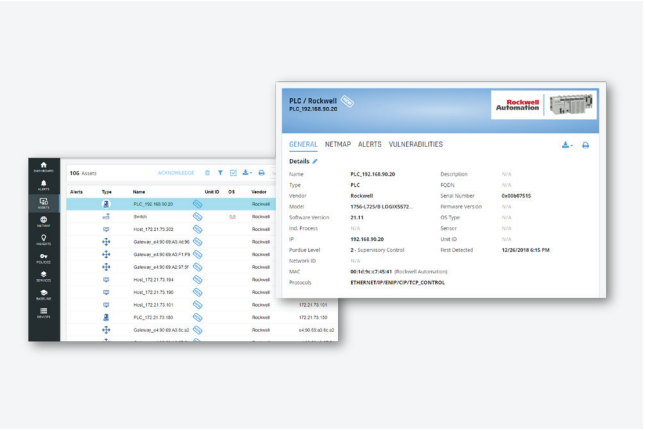


Обнаружения и срабатывания SCADAShield

Управление Активами

SCADAShield позволяет управлять активами, предоставляя следующую информацию:

- **Атрибуты всех ИТ и OT активов,** подключенных к сети, включая тип устройства, производителя, модель, роль, MAC и IP адреса, серийный номер, ОС, версия прошивки и связанные уязвимости, последние время адресации и изменения конфигурации.
- **Анализ протоколов** определяет протокол между любыми двумя узлами сети, будь то SCADA/OT или обычный ИТ-протокол, или их комбинация.



Инвентаризация SCADAShield

Опциональный режим работы SCADAShield: активное противодействие

SCADAShield может быть **опционально** развернута в активном IPS-режиме, позволяющем блокировать угрозы в реальном времени.

Поддержка одной консоли для ИТ-OT-IoT безопасности

Для автоматизации, оркестрации и реагирования в ИТ-OT-IoT безопасности SCADAShield может быть легко интегрирована с системой Cyberbit SOC 3D (SOAR).

Поддержка для компаний с разнородными OT

SCADAShield обеспечивает «из коробки» поддержку более 40 самых популярных и определяемых пользователем протоколов для отраслей, перечисленных ниже. Поддержка новых или проприетарных протоколов может быть добавлена в течение нескольких дней.

- Энергетические сети
- Транспорт
- Аэропорты
- «Умные» здания
- Добыча и переработка
- Производство
- Нефть и газ
- Фармакология
- Военные объекты

О CYBERBIT™

Cyberbit предлагает платформу обнаружения и реагирования для защиты ИТ, OT и IoT сетей: поведенческий анализ, автоматизация и оркестровка обработки инцидентов и защита SCADA и лидирующий в мире кибер-полигон. Продукты Cyberbit разработаны и апробированы в самых жестких условиях. С момента основания в 2015 продукты Cyberbit применяются и крупнейших компаниях, государственных и образовательных организациях и MSSP по всему миру. Cyberbit – подразделение Elbit Systems (NASDAQ: ESLT) имеет офисы в Израиле, Европе и Азии.

sales@cyberbit.com | www.cyberbit.com

US Office:
Cyberbit Inc.
3571 Far West Blvd #168 | Austin, TX 78731 | Tel: +1-512-676-8731

Офис в Израиле:
Cyberbit Ltd.
22 Zarhin St. Ra'anana | Israel 4310602 | Tel: +972-9-7799800

CYBERBIT
PROTECTING A NEW DIMENSION