

Безопасность ОТ

Надёжное и лояльное обеспечение безопасности в области пищевой промышленности и производства напитков SCADAfence



Проблемы безопасности, характерные для производства продуктов питания и напитков

Системы кибербезопасности выходят за пределы ИТ-безопасности и сегментации промышленных сетей, в то же время они должны защищать промышленные системы управления (ICS), которые лежат в основе производственных процессов в сфере изготовления продуктов питания и напитков. Данные системы ведут контроль качества производства и соответствия рецептуре, а именно смешивание ингредиентов и розлив напитков, а также температура хранения перед отгрузкой продукции. Любые несанкционированные изменения в контроле ICS, произошедшие из-за сложной кибератаки или невинной субъективной ошибки, могут привести к производству брака и вредных для здоровья продуктов, цена же такой ошибки может достигать очень высоких цифр. Например, брак производственной партии из-за ошибочного соотношения ингредиентов, изменения уровня сахара или температуры молока, может стоить компаниям по производству продуктов питания и напитков миллионы долларов. Вывод: безопасность производства пищевых продуктов требует нулевой толерантности к нежелательным изменениям в производственных процессах. В случае появления проблем с безопасностью у компаний по производству продуктов питания и



напитков нет иного выбора, кроме как закрыть пострадавшую производственную линию до тех пор, пока проблема не будет устранена. В связи с тем, что производитель в этой индустрии как правило работает круглосуточно и без выходных, управляя несколькими производственными линиями, затраты, вызванные простоями из-за киберинцидентов, связанных с ICS, могут быть астрономическими.

Необходимость решения проблем безопасности частной сети OT

Использование ориентированных на ИТ инструментов безопасности в сетях OT не защищает их от злоумышленников. Более того применение инструментов ИТ-безопасности в сети OT опасно, поскольку они создают ложное представление о безопасности. Сети, оборудование и протоколы OT отличаются от своих ИТ-эквивалентов, следовательно, требуют другого подхода. Планирование надежной архитектуры сетевой безопасности OT требует адаптированных к их характеристикам решений в сфере безопасности и должны специально разрабатываться для высокой точности и специфического трафика сети OT.

Сınıfının En İyisi OT Güvenliđi

Endüstri Lideri Doğruluk
Mikro tanecikli uyarlanabilir temel oluşturma, en düşük yanlış pozitif oranıyla en yüksek algılama oranını sunar.

Anında Deđer Verme Süresi
Esnek dağıtım seçenekleri ve minimum konfigürasyon ile platform, nominal kurulum süresi ile anında deđer sağlar.

Tasarıma Göre Sadelik
Her büyüklükteki şirket, daha küçük ekiplerin daha az kaynakla daha fazla şey yapmasına olanak tanıyan basit bir kullanıcı deneyiminden yararlanır.



Eksiksiz IoT Kapsamı

Patentli IoT Yetenekleri
100'lerce yönetim sistemini tek bir platformda birleştiren patentli IoT yapılandırma düzenlemesi.

Birleşik Politika Uygulaması
Tüm IoT cihazlarında politika uygulanmasını sağlamak için toplu işlemler gerçekleştirir.

Güvenliđi ihlal edilmiş Cihaz Algılama
Tehdit algılama ve güvenlik açığı yönetimini etkinleştirmek için güvenlik içgörülerini çıkarmak için IoT verilerini analiz eder.

Güçlü Yönetim Yetenekleri

En Geniş Kapsam
IEC 62443, NERC CIP, NIST ve diğer uzak sahaları kapsar.

Merkezi Politika Uyumluluđu
Uzak sahaların merkezi yönetimi, seyahat ve yerinde denetim ihtiyacını ortadan kaldırır.


Платформа SCADAfence

Непрерывный мониторинг и защита сетей OT в реальном времени

Платформа SCADAfence — это система мониторинга промышленных сетей, обеспечивающая кибербезопасность и видимость для сетей ICS / SCADA. Платформа SCADAfence предоставляет следующие услуги: автоматическое обнаружение активов, учёт товарно-материальных запасов, обнаружение угроз и управление рисками. Используя большое количество алгоритмов, машинное обучение и искусственный интеллект, ведёт обнаружение аномалий и инцидентов безопасности, которые могут помешать соблюдению требований и повлиять на безопасность и надёжность сетей OT и сетевых активов.



Платформа SCADAfence является единственным решением на рынке, которое может поддерживать специфические требования крупномасштабных промышленных сетей с точки зрения их размера, сложности и объёма производства при сохранении доступной совокупной стоимости владения.



SCADAfence

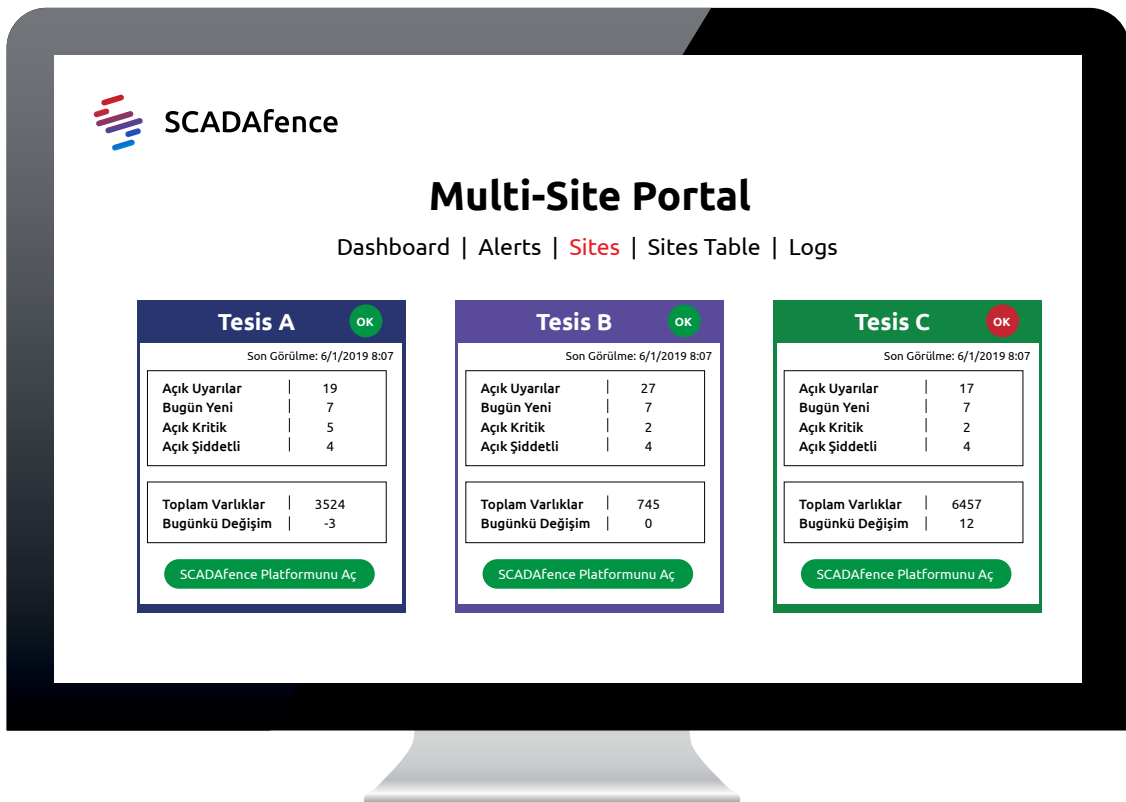
Платформа SCADAfence это бесперебойное решение на основе ПО, предназначенное для снижения следующих рисков.

- О Сбои в работе и управлении производственным процессом
- Заражение вредоносными программами и программами-вымогателями
- Внешние и внутренние кибератаки
- Субъективные ошибки, неправильные конфигурации и сбои работы устройства

Платформа SCADAfence обеспечивает высокую степень защиты сетей ОТ с перечисленными ниже мощными функциями:

- Учёт товарно-материальных запасов с автоматическим обнаружением и полной видимостью
- Сетевые панели для обеспечения должного трафика и безопасности
- Картографирование сети и регрессионный анализ
- Обнаружение подозрительных активностей, уязвимостей и атак вредоносного ПО
- Оперативное оповещение о соответствии активов и услуг и о проблемах с показателями производства
- Способные побудить к действию упреждающие оповещения относительно рисков и проблем сети ОТ
- Подробный анализ промышленного протокола и деятельности оборудования
- Отчеты на уровне автоматического управления

Платформа SCADAfence без проблем интегрирует существующие сети друг с другом. Благодаря функциям мониторинга и предупреждения выступает дополнением к решениям межсетевого экрана и SIEM. Наша платформа подключается к портам зеркалирования и интегрируется с существующими продуктами безопасности и инструментами обработки событий с помощью стандартных отраслевых интерфейсов.



SCADAfence

Multi-Site Portal

Dashboard | Alerts | Sites | Sites Table | Logs

Site	Alert Type	Count
Tesis A	Açık Uyarılar	19
	Bugün Yeni	7
	Açık Kritik	5
	Açık Şiddetli	4
Tesis A	Toplam Varlıklar	3524
	Bugünkü Değişim	-3
Tesis B	Açık Uyarılar	27
	Bugün Yeni	7
	Açık Kritik	2
	Açık Şiddetli	4
Tesis B	Toplam Varlıklar	745
	Bugünkü Değişim	0
Tesis C	Açık Uyarılar	17
	Bugün Yeni	7
	Açık Kritik	2
	Açık Şiddetli	4
Tesis C	Toplam Varlıklar	6457
	Bugünkü Değişim	12

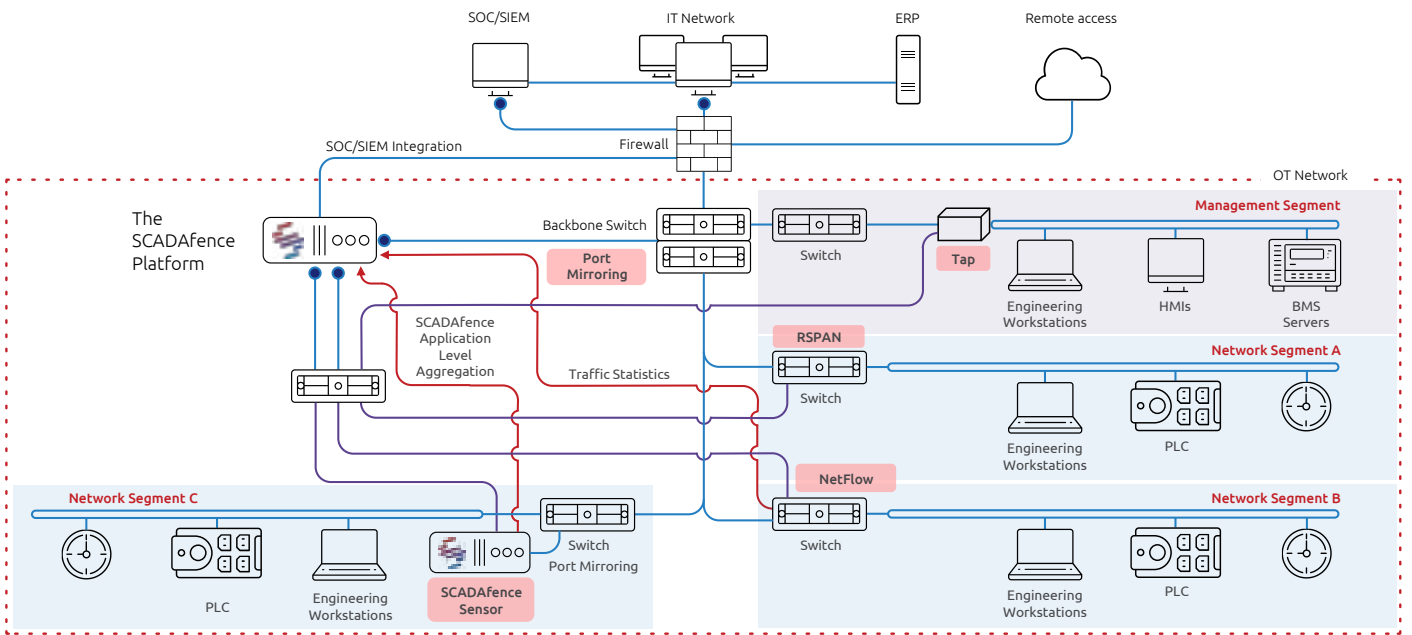
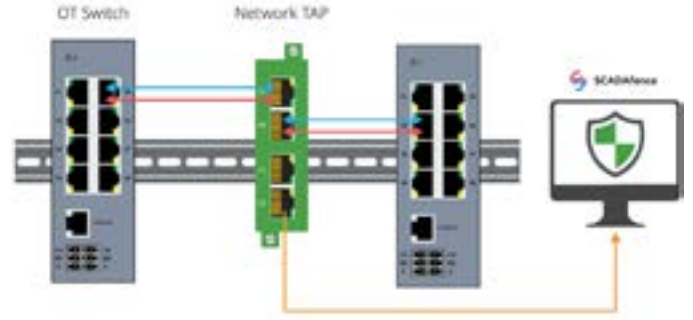
SCADAfence Platformunu Aç

SCADAfence идеальная для многозонального управления

SCADAfence Senaryoları



Otomasyon networkleri ihtiyaç sebebiyle artık kısa süreli yada uzun süreli erişilebilir ve yönetilebilir hale gelmektedir. Bu sebeple IT network katmanından OT network katmanına güvenli erişimleri sağlayabilmek için IT / OT segmentasyonu yapılması gerekmektedir, OT networkünüzün sürekli izlenmesi ile olası bir Siber Saldırısı yada şüpheli aktivitelere karşı proaktif olmanızı sağlamaktadır.



Почему SCADAfence?

Лучшая производительность в отрасли

The only solution to provide full coverage of network traffic monitoring (no sampling, no filtering)

Многозональный мониторинг

Разработана для обеспечения централизованного мониторинга состояния безопасности в нескольких зонах

Простота развёртывания

Автоматическое обучение и адаптация

Рентабельность

Эффективное развёртывание с высокой производительностью и низкой совокупной стоимостью владения

Не оказывает влияния беспереывность производства

За счёт бесперебойности решения можно добавлять в функционирующие сети

РЕАЛЬНОЕ-ВРЕМЯ

Выявление риска, повышение прозрачности и надёжности сети

Выявление угроз, ошибок трафика и неразрешённых действий

Авто обнаружение активов

Управление активами

Карта сети

Анализ трафика

Новые / Потерянные девайсы

Сбои устройств / сервисов

Неразрешенные команды OT

Заражение вредоносным ПО

Аномальная активность сети

Неразрешенные подключения к Интернету

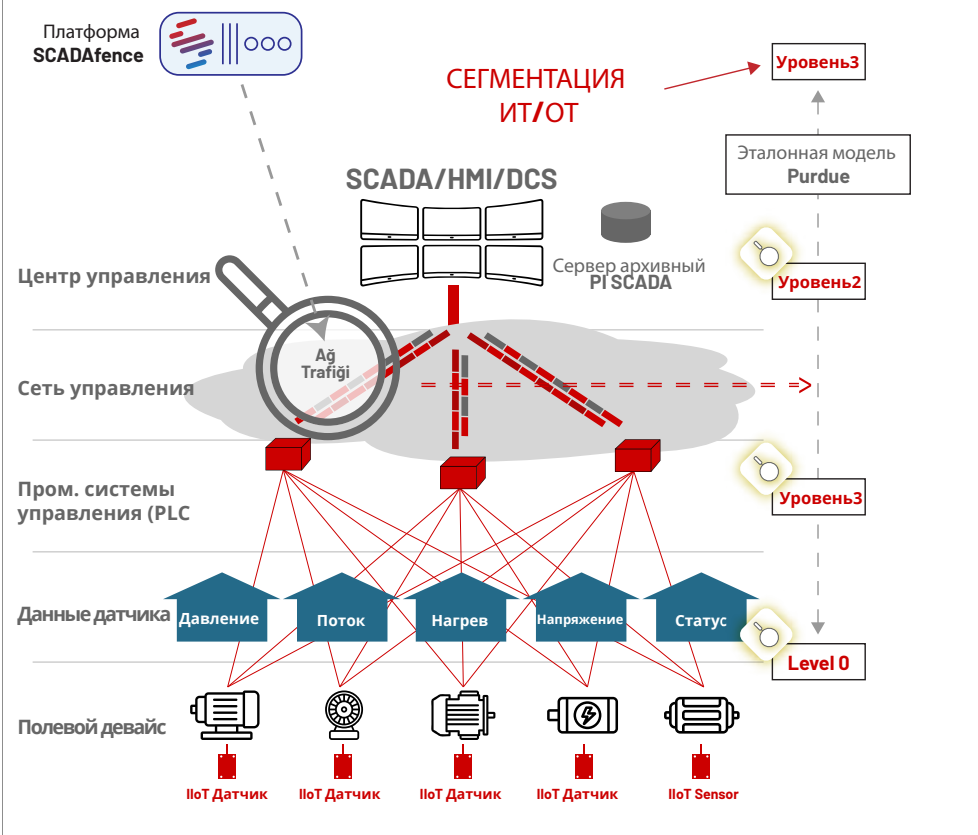
Обнаружение незащищённых служб

Управление инцидентами

Cyber Security Platform for Critical IT & OT Infrastructure

Non-intrusive Scadafence platform ensures absolute visibility of OT network by offering constant OT network monitoring, OT asset exploration, OT network communication mapping, in-dept traffic package analysis and risk identification skills and user experience.

АНАЛИЗ ТРАФИКА СЕТИ OT



Segmentation & Constant OT Network Traffic Analysis Need

Level Systems conducts advanced security network traffic analysis in Level 0/1/2 layers and makes OT risks more visible in day -1, and increase your OT network dominance continuously. Creates data for effective segmentation by monitoring without leaving Blind Spot.

Ürünler hakkında daha detaylı görüşmek isterseniz "OTD Bilişim" satış ekibi ile otd.salesgrp@onlineteknikdestek.com mail adresi üzerinden ve +90 216 912 10 05 numaralı telefonumuzdan iletişime geçebilirsiniz.