SCADAfence

Value-Added Distributor
OTD BİLİŞİM
www.onlineteknikdestek.com

ICT OTD PREFER EXPERIENCE ONLINE Since 2011

SCADAfence Platform

Monitoring and Securing Multiple Distributed Sites

OT Security. At Scale.

Table of Contents

NEW YORK, 462 W Broadway New York, NY 10012, ABD +1-646-475-2173

TOKYO, Clip Nihonbashi, 3-3-3 Nihonbashi-Honcho Chuo-ku, Tokyo 103-0023, Japan +81-3-4588-5432

MUNCHEN, Schellingstr. 109a80798 Munchen Germany +49-322-2109-7564

Contact: info@scadafence.com

Chapter 1
Introduction

This document describes the deployment of the SCADAfence platform for multiple sites, spread across multiple geographical locations. Use cases for such a deployment can be electrical substations, manufacturing plants who are under a single organization unit, disperse building management sites, oil facilities and gas facilities.

1.1 SCADAfence Platform Overview

The SCADAfence Platform allows administrators to significantly increase their network's security level, while ensuring the peace-of-mind that no unnecessary risks are added to the operational environment (ICS/SCADA/BMS network). The solution is available either as a virtual appliance or as a physical appliance. The installation process requires no downtime to the operational network, and system algorithms are automatically configured without any input from the user.

SCADAfence Platform offers full visibility of day-to-day operations and real-time detection of anomalous behavior, based on deviations from normal behavioral profiles. Once a deviation is detected, the user receives a real-time alert. The user can track alerts via the SCADAfence Platform dashboard or can receive instant messages and emails. The Platform can also be easily integrated with customer's existing tools and be a part of the organizational security architecture and processes.

1.2 Network Deployment

The SCADAfence Platform sensors are deployed in critical traffic junctions, where they listen to the network in order to perform deep packet inspection of all data flows from within the organization.

The SCADAfence Platform's default mode is to work as a non-intrusive solution, therefore it has no impact on the production process. It does not inherently require production downtime or lengthy maintenance windows. An active mode is also available for further asset data collection.

The SCADAfence Platform is designed so it will integrate with central security management systems such as SIEM or Incident Management systems and become an integral part of the security and resilience architecture of the OT network.

Chapter 2
SCADAfence's Scalable Architecture

The SCADAfence Platform supports multiple architecture models, comprised from one or multiple hierarchical layers, and is suitable for managing a small or large number of sites and monitoring points.

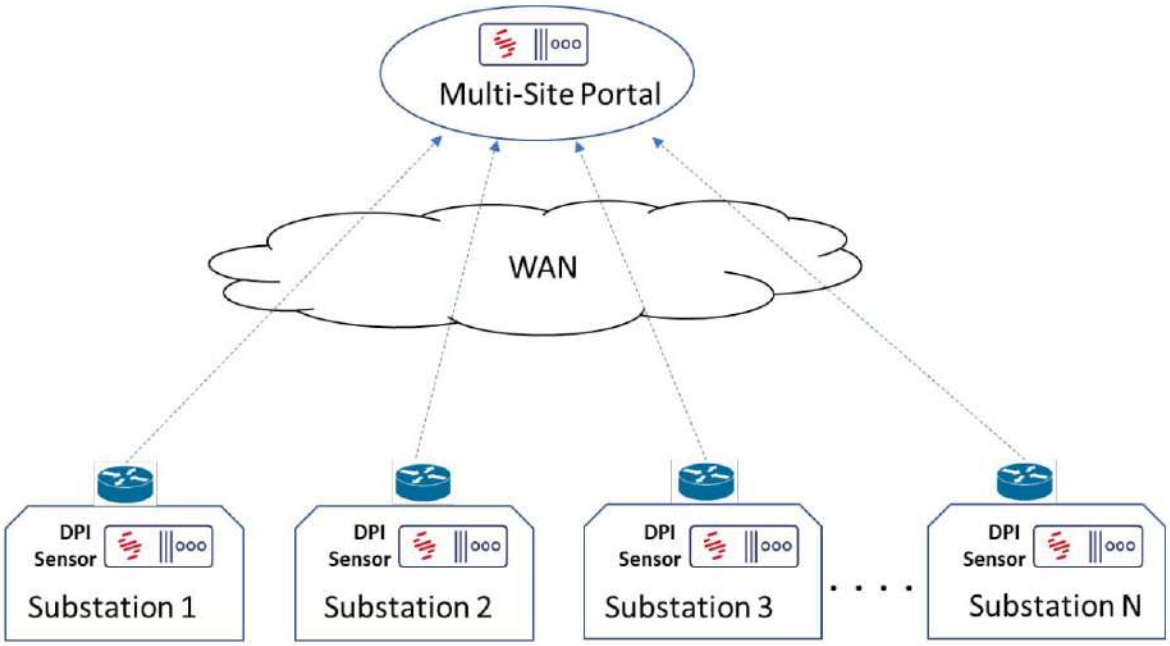


Diagram #1: SCADAfence's Multi-Layer Architecture

2.1 SCADAfence Industrial DPI Sensors

SCADAfence Industrial DPI Sensors are installed in distributed locations, in order to discover and monitor the assets of that location. In each site, the SCADAfence sensor will discover and monitor assets such as RTUs, IEDs, smart meters and actuators.

The sensor will perform the analysis of the network traffic on that site. The sensor will automatically discover the site assets, perform DPI of the network traffic including industrial traffic such as IEC-104 and DNP3, and raise alerts on cyber-security and operational events.
The SCADAfence Industrial DPI sensor can be deployed in one of the following ways:

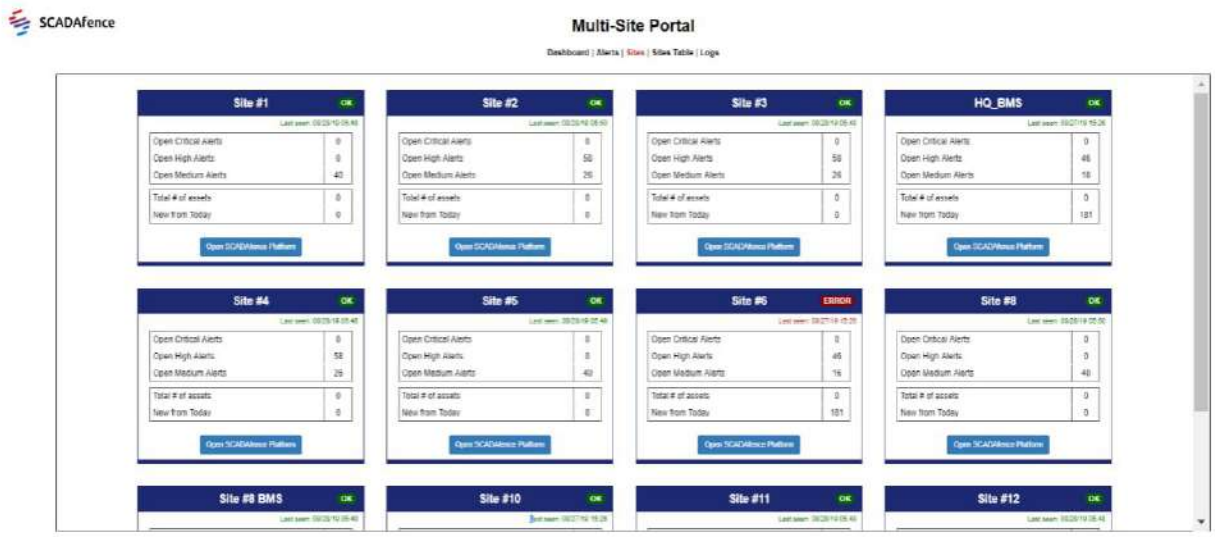
- **Software Solution**. In this mode, the SCADAfence platform is installed on a pre-installed Ubuntu server, or on a Virtual Machine over VMware vSphere, Microsoft Hyper-V or other.

2.2 Central Aggregation Dashboard

SCADAfence's Multi-Site technology is used to aggregate information from distributed sensors, such as alerts, compliance and asset inventory, in central control centers. The SCADAfence Multi-Site Portal shows aggregated information such as:

- Summary of assets and alerts status form the various sites.
- Alerts aggregation from all sites.
- Aggregation of assets health data from all sites.
- URLs to access detailed information on the distributed sensors.

The information from each site is relayed to the central site portal over the WAN/Internet. Since the raw network traffic is being processed locally by the SCADAfence Sensor, the data relayed towards the central site consists of aggregated data only, and will not significantly load the WAN.



Screenshot #1: Aggregation of Multiple Sites in a Central Location

NEW YORK, 462 W Broadway New York, NY 10012, ABD +1-646-475-2173

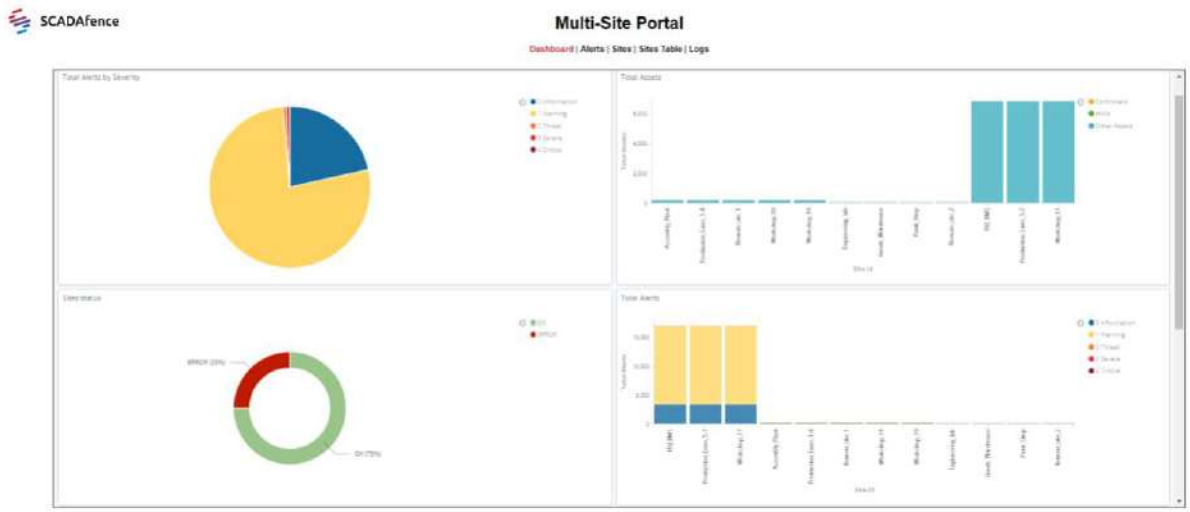
TOKYO, Clip Nihonbashi, 3-3-3 Nihonbashi-Honcho Chuo-ku, Tokyo 103-0023, Japan +81-3-4588-5432

MUNCHEN, Schellingstr. 109a80798 Munchen Germany +49-322-2109-7564

Contact: info@scadafence.com

2.3 High Performance Leading to Cost-Efficiency

The SCADAfence Platform's DPI algorithms are designed with performance optimization in mind. This results in very efficient traffic analysis components that fit in any topology. The SCADAfence Industrial DPI Sensors can use small hardware form factors with minimal specifications and the central SCADAfence Platform server can scale to hundreds of distributed sensors, serving tens of thousands of devices, without performance degradation.



Screenshot #2: Central Security Management Dashboard

NEW YORK, 462 W Broadway New York, NY 10012, ABD +1-646-475-2173

TOKYO, Clip Nihonbashi, 3-3-3 Nihonbashi-Honcho Chuo-ku, Tokyo 103-0023, Japan +81-3-4588-5432

MUNCHEN, Schellingstr. 109a80798 Munchen Germany +49-322-2109-7564

Contact: info@scadafence.com