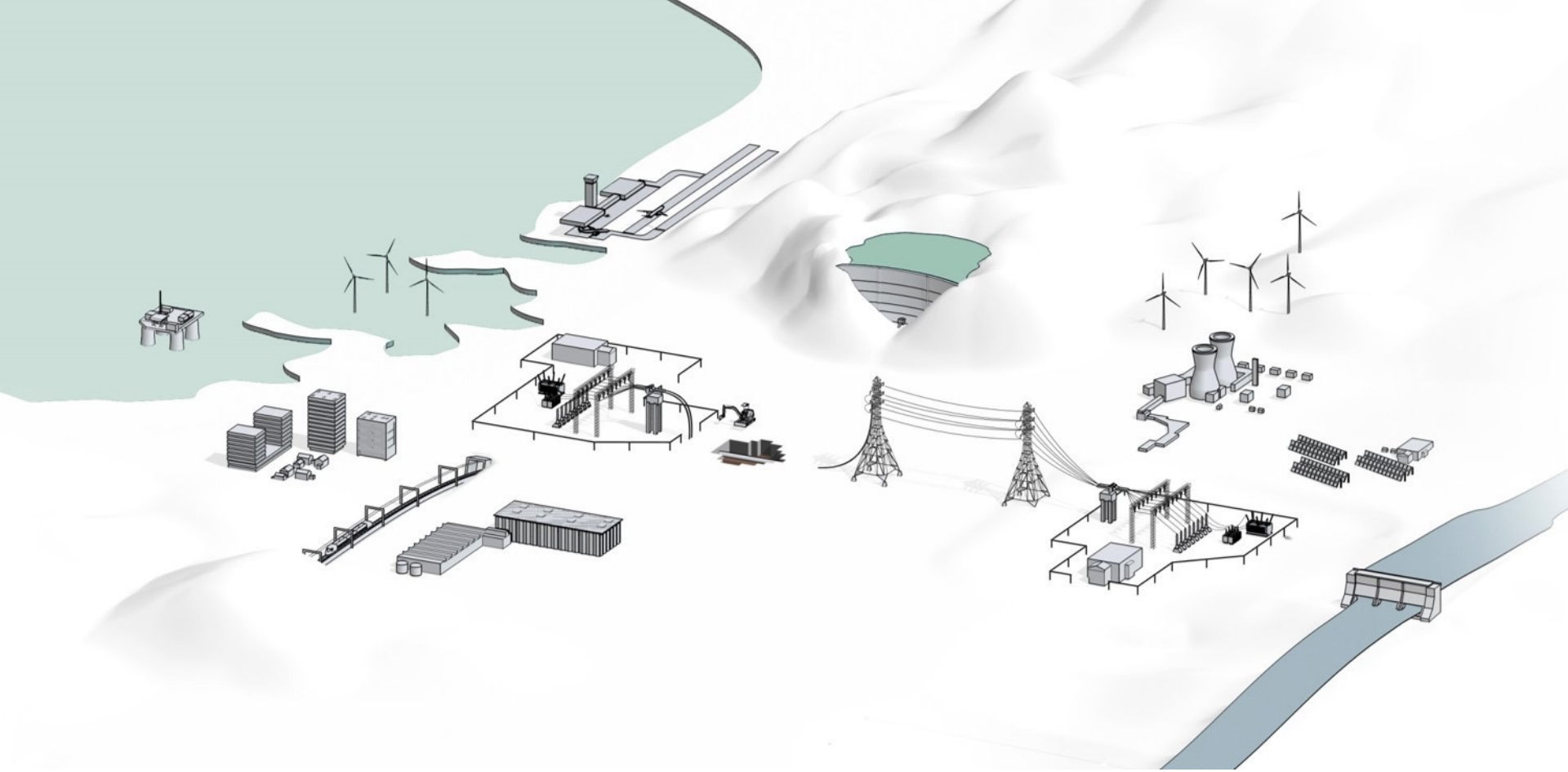


Scribbler
Log Manager

Centralized Log Management Solution

Data Sheet

SyskeyOT

Overview

Today, secure operation of the Industrial Control System is one of the mandatory needs to protect Critical Infrastructures around the world. Ensuring such secure operation relies on the implementation of security systems meeting IEC62443 standards.

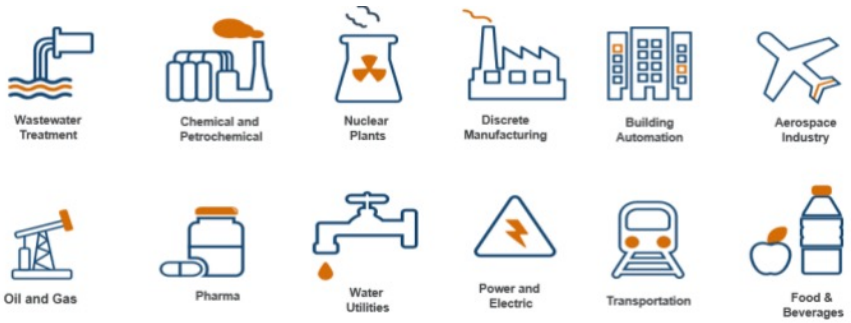
Logs and Log Management System is one of the foundational pillars of Cyber security systems which comply to standards like IEC62443/ISO27001, etc.

Scribbler Log Manager, a highly secure, scalable and reliable centralized log management solution comply to Industrial Control System security standards. Featuring as an invaluable tool for administrators to identify and diagnose problems on their infrastructure, it consists of multiple components to

Collect, Filter, Store, Analyze and Forward Logs in Real–Time.

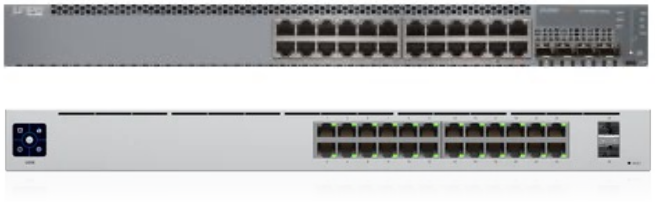
Scribbler relies on standard protocols and compatible with industry leading SIEM solutions.

Industries/Critical Infrastructure that We Secure



Edge Computing and Log Management in harsh, Industrial Cybersecurity Environments

Providing a secure and future-proof way to integrate Edge computing into industrial networks in harsh environments, bringing intelligence and Log processing on a decentralized level in real-time – a key requirement for digitalization and the Industrial Internet of Things (IIoT).



*Picture for representation purpose only

The APE/Industrial Computing Module is an excellent platform to deploy "Scribbler" – A Centralized Log Management solution to further enhance the network security with lower configuration and without the need to install an external industrial PC.

Scribbler Deployment and Processing Capabilities were demonstrated on leading Industrial Computing Modules.

SyskeyOT

The Scribbler Difference

Key Features

Visibility & Analytics
Collect, Filter, Store, Forward & Search Logs at Real-Time. A web–based analytical dashboard provides a good insight about the logs

Powerful REGEX Filter
Rule Engine to filter out junk logs from the system and thus save cost on both hardware resources and network bandwidth

Role **B**ased **A**ccess **C**ontrol and **Active Directory** Single Sign On
Supports **Encryption** at REST

Performant- every millisecond matters when working with enterprise scale data Scribbler from the ground up designed to be efficient and performant. The log collection and search has blazing fast response times

Backup your logs to Local drive or to an external Network Attached Storage**(NAS)** over SMB

Built in **SNMP Agent** to report service Health status to an external Asset Monitoring solution

Protocols/Formats & Standard
Syslog over UDP/TCP/TCP TLS, CEF, LEEF, SNMP Traps
RFC 3164, RFC 5424, RFC 5425, RFC 5426, RFC 6587

SNMP Traps & Syslog Collects SNMP Traps and Forward to upstream **NMS,** meanwhile transform the Traps to Syslog which can be stored and forwarded to any upstream **SIEM**

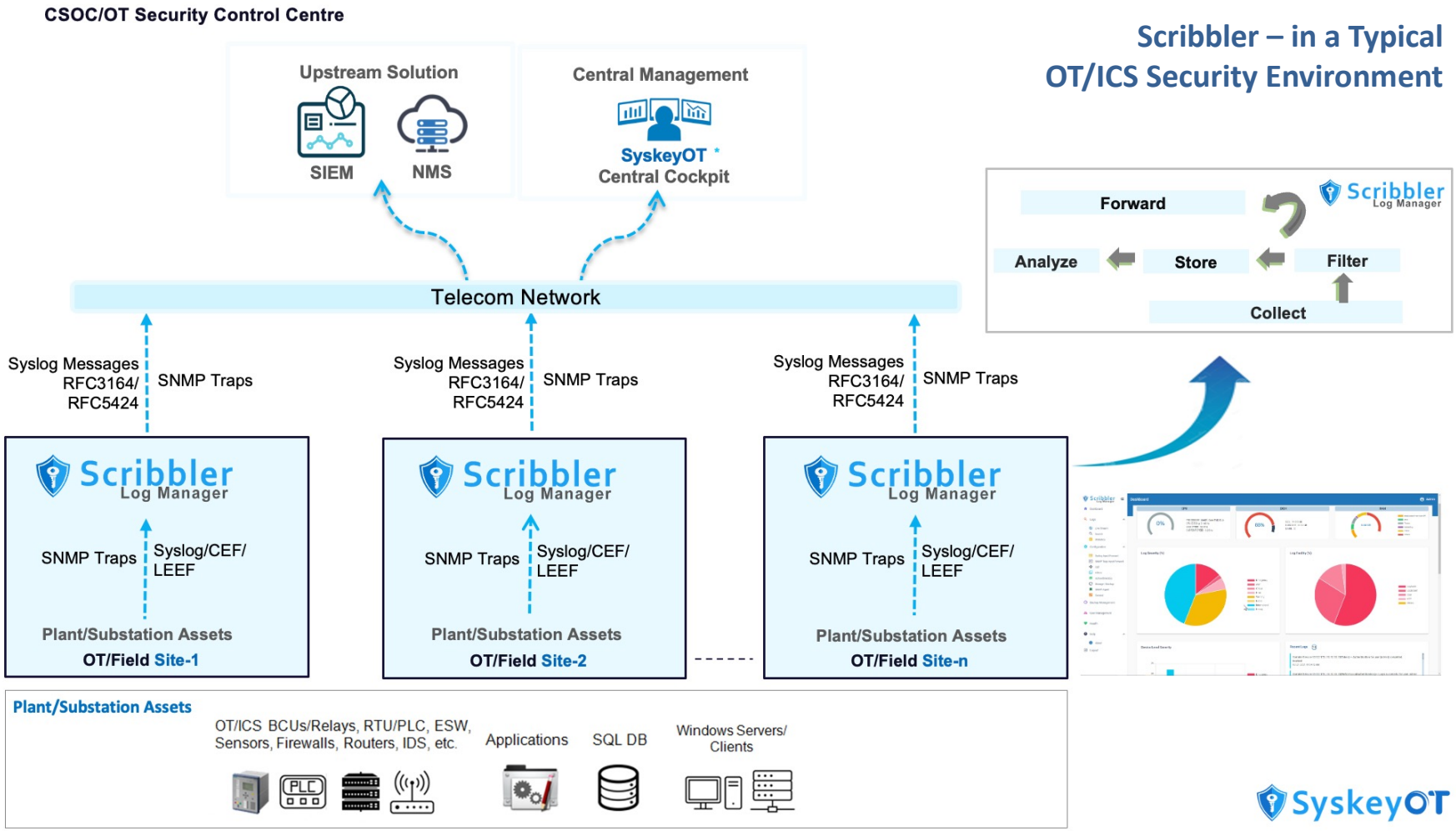
Value Proposition

Solution Delivery & Customization
Scribbler is a modular solution designed from the scratch to address different customer needs. The team engage with the customer and identify their needs and customize the solution as per their requirement

Interoperability & Integration
Scribbler is standard complaint with all forms of Syslog standards and protocols. Also, scribbler nicely integrates with any SIEM solutions for log ingestion through Syslog

Perpetual Validity and Standard 3 Years support with FREE upgrades.
Unlimited Log Sources and
Unlimited Log Volume

Scribbler – in a Typical OT/ICS Security Environment



System Requirement

Scribbler Enterprise Windows (Bare Metal / VM)

OS - Windows Server 2016 or Higher

CPU - 4 Core, 2.5 Ghz or Higher

RAM - 8 GB (16 GB Preferred)

Storage (SSD) - 100 GB or more

TPM (Hardware / Software) for disk encryption

Scribbler Enterprise Linux (Bare Metal / VM / Appliance)

OS - Scribbler Linux (Based on Debian 11 x64)

CPU - 4 Core, 1.8 Ghz or Higher

RAM - 8 GB or higher

Storage (SSD) - 100 GB or more

TPM (Hardware / Software) for disk encryption

Use Case

- IT/OT Integration
- Regulatory Compliance Requirements
- Cyber Security Forensic Analysis
- Improved Visibility and Observability
- Reduce SIEM Ingestion Cost – Log Filter

Delivery Options

- Bare Metal Windows/Windows VM
  - Windows Server 2016 x64+
- Bare Metal Linux/Dedicated Linux VM/HW Appliance
  - Bundled with OS (Debian 11 x64, Kernel 5.10)
- Perpetual Validity with Standard 3 years support
- Unlimited Nodes and Bandwidth

About Syskey Softlabs

An emerging Software Development firm from India, offering Cybersecurity products/solutions for Operation Technology/Industrial Control Systems (OT/ICS) networks.
Syskey helps the businesses with customized software products for tasks such as obtaining data to help identify security breaches, comply and maintaining the security level of the highest standards within the organization.

Reach us at
sales@syskeysoftlabs.com
support@syskeysoftlabs.com

Southeast & MEA
#19 tower B, PSR Aster, Chambenahalli,
Sarjapura Road, Bangalore- 562125, India.