

**OT/ICS Cybersecurity**

**Vulnerability management – High Level Design**

Contents

[1 Introduction 3](#_Toc22793498)

[2 System components 3](#_Toc22793499)

[3 High Level Design – Operational Construct 4](#_Toc22793500)

[3.1 Discovery of assets 4](#_Toc22793501)

[3.2 Vulnerability database 5](#_Toc22793502)

[3.3 Vulnerability and Configuration Assessment 5](#_Toc22793503)

[3.4 Network Monitoring and Anomaly Detection 5](#_Toc22793504)

[3.5 Vulnerability Lifecycle Management 5](#_Toc22793505)

[3.6 Architectural and Other Requirements 5](#_Toc22793506)

[3.7 Reporting 5](#_Toc22793507)

[3.8 Integration 5](#_Toc22793508)

[4 High Level Design Architecture 6](#_Toc22793509)

# Introduction

The purpose of this document is to provide high-level design of the system to meet the requirement of the Inpex OT vulnerability management proof of value project. The following are the overall features to be demonstrated by the project.

* Discovery of assets
* Vulnerability and Configuration Assessment
* Network Monitoring and Anomaly Detection
* Vulnerability Lifecycle Management
* Meeting architectural Requirements
* Reporting
* Integration with existing system

# System components

The solution uses Skybox network aggregation and visualization tool and Indegy OT sensor to cater to the overall requirement. These will be integrated into the existing Inpex environment and aggregated with existing Inpex software solutions, specifically Qualys.

Skybox integrates data from these various software, merges and normalizes this data in central repositories to establish a common reference for infrastructure, asset and vulnerability data. Skybox will therefore obtain and aggregate data from the following sources:

* Indegy OT sensor
* Qualys Vulnerability Manager
* WSUS/SCCM patching tool
* McAfee Nitro SIEM

The following Skybox modules will be used to deliver the requirements:

* Firewall Assurance module
* Change Manager Module
* Network Assurance module
* Vulnerability Control module

Skybox supports import and export of CSV based events from and to the McAfee Nitro SIEM.

Skybox has native API (application programming interface) based integration with Indegy OT sensor and Qualys. This will allow the vulnerabilities and anomalies to be found from the Indegy sensor to be displayed at Skybox.

INPEX currently using WSUS/SCCM tool for patching windows based systems. The Skybox integration with WSUS/SCCM will enable us to manage vulnerability management life cycle in better manner including compliance assessment or reports.

Illustrated below is the overall architecture concept of the system components in the system.

Skybox uses the Qualys vulnerability scanner to accesses vulnerabilities scan results to aide network visualization and modelling.

Skybox Vulnerability Control

Firewall Assurance module

Change Manager Module

Network Assurance module

Vulnerability Control module

McAfee Nitro SIEM

WSUS/SCCM Patch Management

Qualys Vulnerability Scanner

Indegy OT Sensor

# 

# High Level Design – Operational Construct

The Skybox collector task is used to collect data from different security solutions. Collector tasks can run on the server or can be distributed across different systems for larger installations.

For this project, the collector will be installed on the server and it will collect data from Indegy OT sensor and Qualys Vulnerability Manager.

WSUS collector should reside on Windows platform. Therefore, the WSUS collector will be installed on a Windows machine, which should be on the same domain as WSUS machine.

Skybox collector task can set up automated data collection on any time schedule required – daily, hourly, or as often as needed.

The network model can be updated quickly and heuristically to utilize the latest information on network topology, OT Devices, firewalls, network devices, threats, vulnerabilities, and assets.

An architecture overview diagram connecting Skybox and Indegy is illustrated at Section 4.

The capabilities of Skybox and Indegy OT sensor is used to meet the requirements as detailed below.

# Discovery of assets

Indegy collects the software and hardware asset data from the OT environment on a wide verity of OT protocols. Skybox then combines this information with the feed from the IT environment to create a centralized data repository. This results in the single console with information and in depth visibility to support a variety of security processes in IT and OT networks.

# Vulnerability database

Indegy collects the vulnerability scan data from devices on various OT protocols and updates the Skybox vulnerability database/model.

# Vulnerability and Configuration Assessment

The Indegy Networks SCADA Guardian solution detects deviations from a network traffic baseline, which is established based on traffic patterns. Skybox support agentless assessment using vulnerability detector. Skybox vulnerability detector will derive/deduce vulnerabilities on assets for which Skybox has patch data.

# Network Monitoring and Anomaly Detection

The Indegy system identifies and logs changes made over the network to controller firmware, state, code and configurations. The Skybox system detects deviations from a network traffic baseline, which is established based on traffic patterns.

# Vulnerability Lifecycle Management

The Skybox technology is designed to assist continuously monitoring of risks within the organization across IT/OT. Skybox provides continuous risk assessments to determine the current risk posture of the organization.

# Architectural and Other Requirements

Indegy Security Platform can support up to 50,000 devices. Skybox supports role based access into the platform and can additionally customize dashboards for relevant users. Skybox can export the directly and indirectly exposed vulnerabilities to external McAfee SIEM solutions in a CSV formatted file.

# Reporting

Skybox provides a fully customizable management dashboard whereby individual users are able to build specific dashboards based upon their requirements.

# Integration

Skybox integrates data from various networking and security technologies, merges and normalizes this data in central repositories to establish a common reference for infrastructure, asset and vulnerability data.

# High Level Design Architecture