Enterprise Security Configuration and Compliance Road Map

Author: Brian Nelson

# System Vision

The Enterprise Security Configuration and Compliance (ESC2) system is designed as an open source based security platform. The platform will track the configurations necessary to properly secure systems. It will also provide a platform for managing a company’s compliance requirements around the subject of technology security.

ESC2 is targeted towards small and mid-sized companies that wish to minimize their risks to security intrusions and other technology-based disruptions.

ESC2 will be designed and implemented to be quickly setup and configured by the companies that wish to utilize it. It will need to be easy to patch and upgrade to minimize the risk that it becomes a source of vulnerability.

While the initial designs were to implement an isolated Security Warehouse, the reality is that the system needs to have integrated operational and warehouse functionality. The implementation of the warehouse data marts will utilize operational tables as their dimensions. Aggregation workflows will be implemented to populate the fact tables in a near real-time manner.

The drivers for this merging of operational and warehouse functionality include:

* Simplified implementation and upgrades for companies using ESC2
* Near Real-Time view of system loads and activities
* Single source of company security and compliance information

# Overview of Implementation Steps

The following steps will be required to fully implement the ESC2 system.

Steps 1 through 7 will provide the Minimum Viable Product (MVP) needs of the system. After the MVP is completed it can be launched and made fully available for users. Steps 8 and beyond will be implemented as enhancements to the MVP.

## Steps towards Production

1. Implement the Operational Systems Screens
2. Add support for PostgreSQL database
3. Implement the SysLog Integration
4. Implement the Log Fact Star Schema
5. Implement additional Log Integrations
6. Add new Logs to the Log Fact Star Schema
7. Implement Integration with National Vulnerability Database
8. Implement Audit and Implementation Fact Star Schemas
9. Implement hosted library of Implementation Guides
10. Implement Full 800-171 Compliance Requirements
11. Implement Log Tracking Machine Learning
12. Implement System Dependency Tracking

## Implement the Operational System Screens

Getting data into the operational system is the initial priority. This will allow the most fundamental set of capabilities that allow companies to track the secure implementation of technology. See the attached document *ESC2 User Interface Designs* document for more information on the look and functionality of the basic system.

These user interfaces will be implemented through web-based technologies.

## Add Support for PostgreSQL database

Current implementation of the database is on Microsoft SQL Server. This was done due to initial requirements for the project. To meet the ESC2 systems goal of being fully open source based the database needs to transition to an open source database. PostgreSQL is the target for this migration.

## Implement the SysLog Integration

Integration with SysLog file publishing will provide the system the ability to track system activity for routers, switches and firewalls.

## Implement the Log Fact Star Schema

The Log Fact table will enable load monitoring of one or more devices. These metrics will be displayed on the web-based user interface.

## Implement additional Log Integrations

Further log integrations will be needed to view server loads and web server activities. The exact integrations will be prioritized later.

Types

* Apache Logs
* NGINX Logs
* IIS Logs
* Windows Logs
* Ubuntu Logs
* API for company systems to publish logs

## Add new Logs to the Log Fact Star Schema

Once additional log sources are added the aggregation workflow will be adjusted to include their data into the Log Fact tables.

## Implement Integration with National Vulnerability Database

Integration with the National Vulnerability Database will allow the company to monitor and be aware of emerging threats to the company systems.

## Implement Audit and Implementation Fact Star Schemas

These tables will be implemented to assist with the calculation of cost to implement and secure technology. This will assist the company in long term planning and pricing of services.

## Implement hosted library of Implementation Guides

Stig files will initially be used. The hosted library will simplify the importing of Stig files and future independently developed security implementation guides.

## Implement Full 800-171 Compliance Requirements

Many companies will need to track their full compliance with 800-171 handling of Controlled Unclassified Information to receive Federal contracts. The system will be expanded to cover the tracking of all 800-171 requirements and documentation.

## Implement Log Tracking Machine Learning

Once log history is captured, use machine learning techniques to identify abnormalities of behavior. This will assist the company in determining if a system has failed, or if it is under attack.

## Implement System Dependencies Tracking

Allow for tracking software dependencies of systems. This will allow the company to quickly become aware of their exposure to emerging threats.

Resources

<https://nvd.nist.gov/>

<https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final>