ESTCP

FINAL REPORT

Patch Management/Continuous Monitoring and Detection for Energy Management Control Systems

Paul Riggins
Chris Murphy
FoxGuard Solutions

November 2022

ESTCP Project EW18-5310

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
11/11/2022	ESTCP Final Report	11/28/2018 - 11/27/2022

4. TITLE AND SUBTITLE

Patch Management/Continuous Monitoring and Detection for Energy Management Control Systems

5a. CONTRACT NUMBER
19-C-0003

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Paul Riggins and Chris Murphy

5d. PROJECT NUMBER
EW18-5310

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

FoxGuard Solutions
2285 Prospect Dr.
Christiansburg, VA 24073

8. PERFORMING ORGANIZATION REPORT NUMBER
EW18-5310

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Office of the Deputy Assistant Secretary of Defense (Energy Resilience & Optimization)
3500 Defense Pentagon, RM 5C646
Washington, DC 20301-3500

10. SPONSOR/MONITOR'S ACRONYM(S)
ESTCP

11. SPONSOR/MONITOR'S REPORT NUMBER(S) EW18-5310

12. DISTRIBUTION / AVAILABILITY STATEMENT

DISTRIBUTION STATEMENT A. Approved for public release: distribution unlimited.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

The objective of this project was to provide a platform for deploying a standard set of security controls for Utility Monitoring Control System (UMCS) / Energy Management and Control Systems (EMCS), including building automation, micro-grid control, smart metering, load sensors, and other energy management Platform Information Technology (PIT) systems installed in DoD buildings and critical infrastructure. The security platform and work within this project have enabled patching and continuous monitoring of these systems, to support simplifying the security posture and management of the assets. The schedule of work was on time and on budget and made possible through the support of the site team and FoxGuard. The completion of this project brings an enhancement to the current system that includes patch management and vulnerability management support through the use of the Sentrigard Enterprise Appliance.

15. SUBJECT TERMS

Patch Management, Continuous Monitoring and Detection, Energy Management Control Systems, cybersecurity

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			Paul Riggins
UNCLASS	UNCLASS	UNCLASS	UNCLASS	34	**19b. TELEPHONE NUMBER** *(include area code)* 276-620-0886

FINAL REPORT
Project: EW18-5310

TABLE OF CONTENTS

Page

LIST OF FIGURES

Page

LIST OF TABLES

Page

ACRONYMS AND ABBREVIATIONS

CDM	Continual Diagnostics and Monitoring
COTS	commercial off-the-shelf
CRN	Closed Restricted Network
DoD	Department of Defense
EMCS	Energy Management and Control Systems
EOS	End of Support
HBSS	host-based security system
HIDS	Host-based Intrusion Detection System
IA	Information Assurance
IDS	Intrusion Detection System
ISR	Intelligence, Surveillance, and Reconnaissance
IT	Information Technology
JVM	Java Virtual Machine
NREL	National Renewable Energy Laboratory
OEM	Original Equipment Manufacturer
OSes	Operating Systems
OT	operational technology
PAR	Patch Availability Report
PBA	Patch Binary Acquisition
PIT	Platform Information Technology
SDN	Software Defined Network
SIEM	Security Information and Event Management
SME	Subject Matter Expert
UMCS	Utility Monitoring Control System
VEES	value of electrical energy security
VOC	Voice of the Customer

ACKNOWLEDGEMENTS

Individuals contributed from FoxGuard Solutions Inc. are:

John Collins
Paul Riggins
Roger Rademacher
Scott Hudson
Jonathan Couch
Lindsey Hale
Patrick Patterson
Michael Trautman
Derek Kolakowski
Steven Wirt
Darrell DeWeese
Ray Swingle

Individuals contributed from Fort Belvoir – NVESD Team

William H Horner
Kevin Brady
William Elliot

Individuals contributed from Spectrum Solutions Inc.

Owen Green
Ryan Cormier
Shelby Hempstead
David Junghans

Individuals contributed from 3 Territory Solutions LLC

Michael Schroeder
David Becker
Frank Reid

1.0 INTRODUCTION

The objective of this project was to provide a platform for deploying a standard set of security controls for Utility Monitoring Control System (UMCS) / Energy Management and Control Systems (EMCS), including building automation, micro-grid control, smart metering, load sensors, and other energy management Platform Information Technology (PIT) systems installed in DoD buildings and critical infrastructure. The security platform and work within this project have enabled patching and continuous monitoring of these systems, to support simplifying the security posture and management of the assets. The schedule of work was on time and on budget and made possible through the support of the site team and FoxGuard. The completion of this project brings an enhancement to the current system that includes patch management and vulnerability management support through the use of the Sentrigard Enterprise Appliance.

1.1 BACKGROUND

FoxGuard Solutions provided a security platform to assist with continuous monitoring of the EMCS, as well as patch management of the virtual infrastructure that supports the environment. The security platform can help detect changes to device/application configurations, changes to system/device baseline configurations, and network anomalies such as new devices or new network communication paths. The security platform also includes centralized log collection to collect events from various devices in one location. Current practices in the industry often include a manual review of device/application configurations and periodic review of log files and event logs. These technologies reduce that manual effort and make it easier to detect when something has changed in the environment.

The patch management portion of the solution allows for centralized scanning and deployment of OS and many third-party patches. Along with FoxGuard Solutions' Patch Availability Report (PAR) and Patch Binary Acquisition (PBA) service, which are subscription-based services that provide monthly reporting on patch updates and monthly delivery of patch update files make it easier for system operators to determine which patches are required in their environment, and in many cases deploy those patches to all systems at once.

1.2 OBJECTIVE OF THE DEMONSTRATION

As mentioned in section 1.1, FoxGuard Solutions' security platform provides features to facilitate configuration and baseline change detection, network anomaly detection, centralized log collection, and patch management. During the demonstration, these technologies were successfully employed to help reduce manual efforts and provide additional insight into the state of the ECMS network, as well as keep systems up to date with the latest security patches.

1.2.1 REGULATORY DRIVERS

NIST 800-53 Security Controls Alignment for Access and Authorize, which includes:

Anomaly Detection

- AC- Access Control
- IA- Identification and Authentication

- MA- Maintenance
- PL- Planning
- SC- System and Communication Protection
- RA- Risk Assessment
- SC- System and Communication Protection
- SI- System and Information Integrity

Configuration Manager

- AC- Access Control
- AU- Audit & Accountability
- CM- Configuration Management
- RA- Risk Assessment
- SC- System and Communication Protection
- SI- System and Information Integrity

Patch Orchestration

- CP- Contingency Planning
- CM- Configuration Management
- IA- Identification and Authentication
- MA- Maintenance
- PL- Planning
- RA- Risk Assessment
- SA- System and Services Acquisition
- SI- System and Information Integrity
- PM- Program Management

Log Manager

- AU- Audit and Accountability
- IA- Identification and Authentication
- IR- Incident Response
- MA- Maintenance
- PS- Personnel Security
- SI- System and Information Integrity

Back Up Recovery

- CP- Contingency Planning
- CM- Configuration Management
- IR- Incident Response
- MA- Maintenance
- SC- System and Communications Protection

2.0 TECHNOLOGY DESCRIPTION

2.1 TECHNOLOGY DESCRIPTION

FoxGuard Solutions' security platform consists of a 1U rackmount server chassis from an enterprise server vendor and a 1U rackmount sensor for network anomaly detection.

The server uses a combination of virtualization and container technologies to provide a secured platform for hosted applications. The server runs Microsoft Windows Server 2019 as the base operating system and utilizes the Microsoft Hyper-V feature to host three virtual machines:

- A hardened Linux virtual machine that hosts several container-based applications
- A hardened Linux virtual machine that hosts the baseline change detection module
- A hardened Windows virtual machine that hosts the patch management software, and optionally a centralized malware protection platform

Figures 1 and 2 present the overall solution design, including each component of the solution and how they interact:

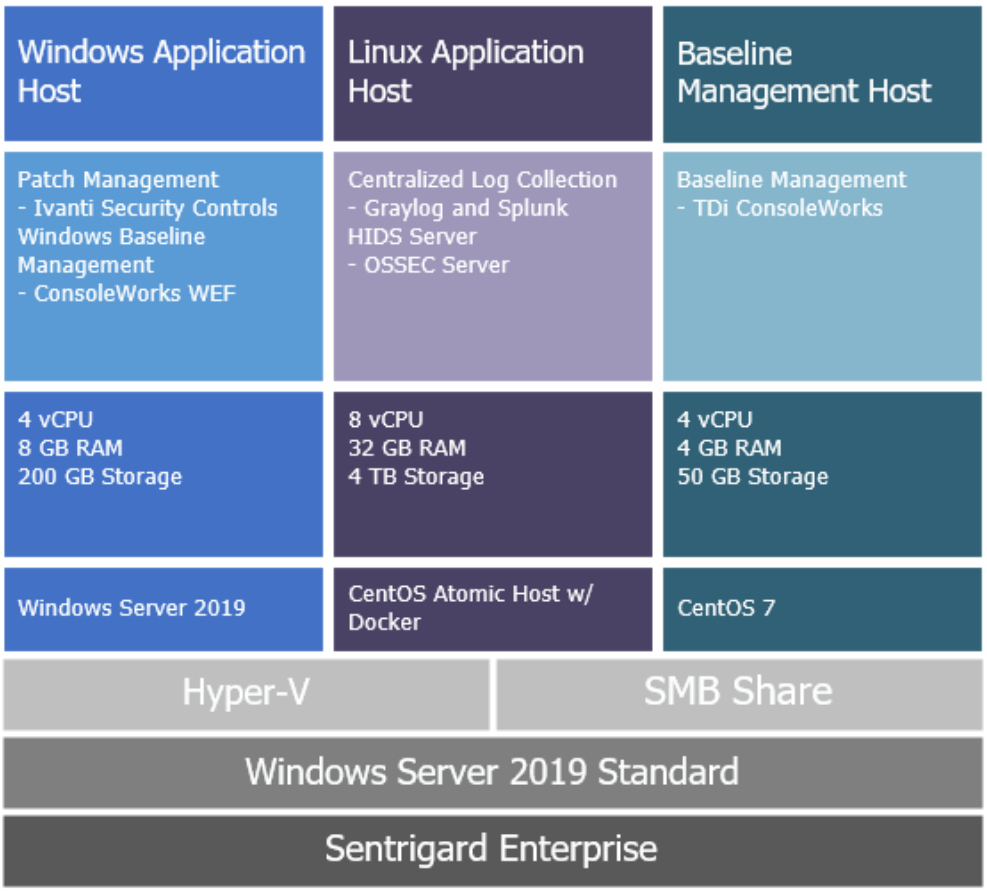


Figure 1. Sentrigard Enterprise Solution Components

Nozomi Guardian Sensor (Network Anomaly Detection)

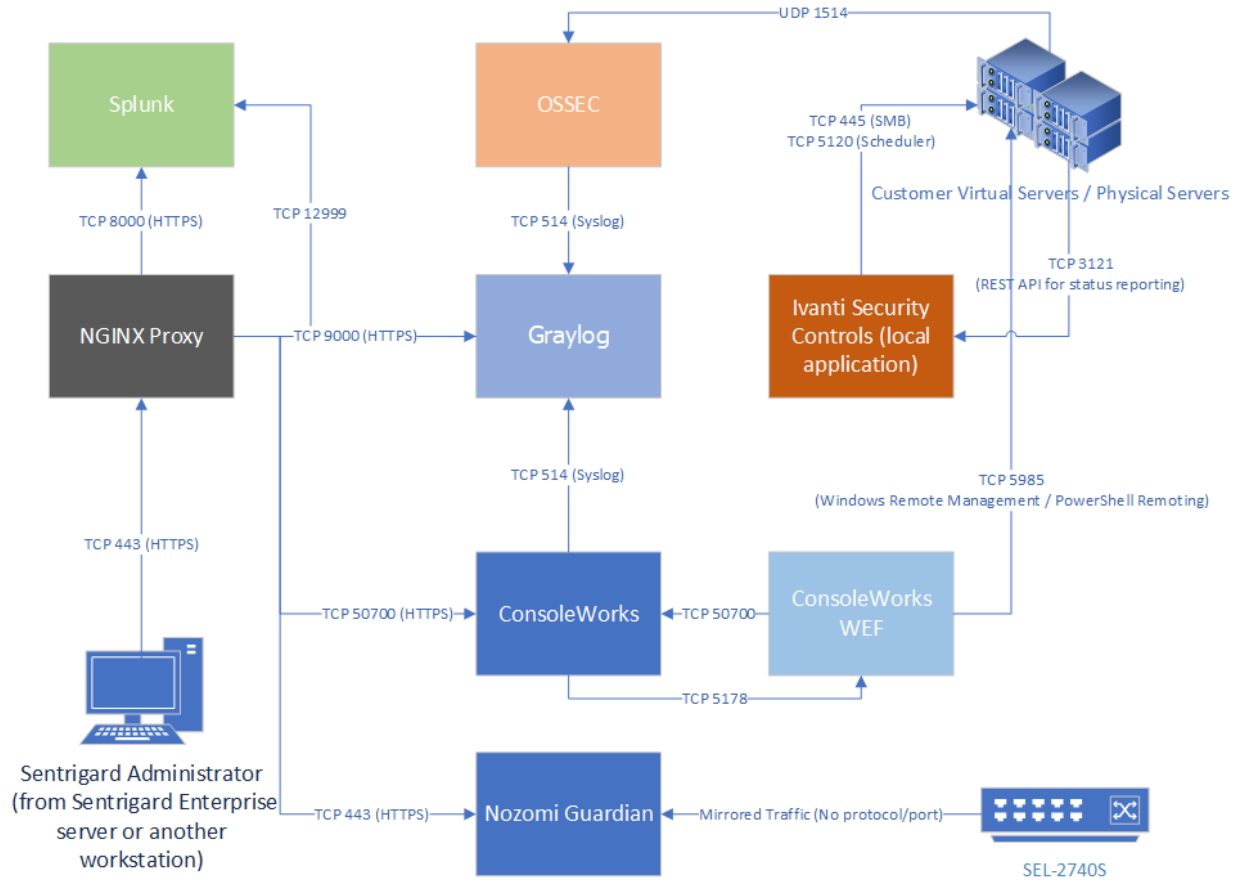


Figure 2. Sentrigard Enterprise Connectivity Diagram

The solution is designed to perform critical monitoring functions and collect data for review by administrators. The baseline change detection module periodically queries devices to collect configuration details and compare them against a known baseline, and if any differences are found, send that information to the centralized log collection module. The network anomaly detection solution monitors the network by listening to one or more mirrored network ports and can be configured to develop a baseline of "normal" network traffic. Any new behavior or potentially malicious network behavior also gets reported to the centralized log collection module.

The centralized log collection module can then be configured to generate email alerts for desired events, eliminating the need for periodic manual review of events and alerts.

In addition to the monitoring functionality, administrators can utilize the patch management solution to determine if operating systems and third-party applications require updates. Administrators can obtain the patch definitions on their own and manually download patches, and then bring them into the environment via network shares or removable media. Alternatively, FoxGuard Solutions provides a subscription service to report on all required patches (based on a customer's asset list) and provide the patch files.

FoxGuard Solutions developed this technology solution to assist customers in the operational technology (OT) space with the automation of many of the manual tasks required. A large portion of FoxGuard Solutions' customer base is in the power generation industry where NERC CIP standards must be adhered to. The solution that FoxGuard Solutions developed addresses several key NERC CIP requirements. In particular, the following requirements are directly addressed by components of the solution (either in part or in their entirety):

- **CIP-007-6 R2:** This requirement focuses on patch identification, evaluation, and installation or mitigation. The patch management software included in the solution plus the optional FoxGuard service satisfy this requirement
- **CIP-007-6 R3**: This requirement focuses on malware deterrence, detection, and prevention. The solution included a centralized malware detection module, but it is not the HBSS solution mandated by the DoD, and therefore was not utilized in the demonstration environment.
- **CIP-007-6 R4:** This requirement focuses on ensuring that at minimum, login success, login failure, and malicious code detection events are logged at either the asset level or in a central location. The solution includes a centralized log collection module to collect this information in a single location for ease of access for incident response and event correlation. The requirement also calls for a review or sampling of logged events at set intervals. The centralized log collection module makes this task much easier than manually sampling logs from multiple devices.
- **CIP-010-3 R1**: This requirement focuses on ensuring that asset owners develop and audit against baseline configurations for each asset. The baseline detection module performs periodic checks of system configurations to help customers meet this requirement.

Development of the solution began in late 2017 as a technology demonstration for a large financial services company to assist with securing and monitoring their building automation systems. While that demo did not lead to a sale, FoxGuard Solutions saw the potential to use the solution in other industry verticals, specifically with some of the existing customer base in the power generation industry. Development was then shifted toward ensuring the solution would meet specific NERC CIP compliance needs and was successfully deployed to a small number of power plants in 2018. In response to customer feedback, improvements were made to the solution over the course of the next year to help improve user experience and provide more functionality.

While the solution was developed primarily with power generation and similar customers in mind, the components help meet other industry and regulatory requirements. This technology solution can be applied in many OT environments due to its flexible and modular nature.

2.2 TECHNOLOGY DEVELOPMENT

Since the solution provided for the demonstration environment was largely based on an existing offering, FoxGuard Solutions focused efforts on the following areas:

- Improving the stability of the platform
- Incorporating an existing patch management solution that was not part of previous releases
- Incorporation of network anomaly detection into the overall solution

Prior to the project award, some improvements to the solution were introduced that had an unintended side effect that occasionally occurred upon system restart. This issue was easily addressed by restarting a service, but to ensure platform stability and reduce the maintenance burden on customers, the first development task was focused on eliminating this issue.

FoxGuard Solutions has another Product Sentrigard Patch developed to help customers with patch management in offline or disconnected environments. This was not a module of the previous core solution, so work was done to incorporate the patch management technology as an optional module.

The inclusion of the network anomaly detection module started in early 2018 but did not gain traction due to lack of customer interest. This module was a much better fit for the demonstration environment, so integration work resumed, and the network anomaly detection module was integrated with the centralized log collection module.

2.3 ADVANTAGES AND LIMITATIONS OF THE TECHNOLOGY

The only alternate technology in place in the Closed Restricted Network (CRN) test environment was an existing Syslog server. The CRN test environment utilized Kiwi Syslog Server for collecting logs from each device. The product can collect information, but it does not have robust search, dashboard, and alerting capabilities. While this product is low cost and does help meet compliance needs, it requires additional man-hours or exporting data to third-party tools to effectively find certain log events in the case of an investigation. The Sentrigard Enterprise technology solution that was integrated as part of this demonstration offers more robust search, reporting, dashboard, and alerting capabilities, which will reduce man-hours required to perform investigations.

The remaining technologies included as part of the Sentrigard Enterprise solution were not in place within the CRN test environment.

3.0 PERFORMANCE OBJECTIVES

The Sentrigard appliance assists in the reduction of service disruptions due to operational anomalies and cybersecurity threats.

The primary objective for the Sentrigard appliance is to monitor the availability and operation of PIT systems and devices. Proper monitoring provides advanced notice of system outages and abnormal behavior to enable reactive and proactive maintenance measures to shorten the duration and impact of adverse events.

The Sentrigard appliance will provide insight into the continued availability of PIT systems. System outages are often preceded by a loss of equipment availability or network services. Loss of PIT systems will impact labor costs (unable to work) and undue stress on systems (increased energy costs). Actively monitoring PIT systems availability allows technicians to take action to minimize the duration of an outage and decrease the return to service time.

The Sentrigard appliance will provide insight into cybersecurity events. Centralized event collection allows administrators to correlate security events to better differentiate between user error and malicious activity. Insider threats and other actors may pose a greater threat to PIT systems and devices with goals often including permanent damage and shortened equipment lifespans.

A 2012 study by the National Renewable Energy Laboratory (NREL) discussed the value of electrical energy security (VEES), which is a metric for the cost of utility outages. In that study, Ft. Belvoir 300 Compound Area was shown to have a VEES of almost $4 million with an average outage duration of 2 hours (NREL/ TP-7A30-55913, Oct 2012). A more recent analysis conducted by the site indicates that the same area experiences a VEES of almost $3 million with an average duration of 2.7 hours (ERCYP FY19). Additional data to include correlation between energy expenditure and service loss is not available. However, the energy expenditure required to return to the setpoint will increase non-linearly given the distance gap between current and target.

Whether from utility failures, failing equipment, misconfiguration, or an insider threat, the Sentrigard appliance will assist in monitoring service availability and operation and potentially contribute to reducing event duration and return to service times.

Table 1. Performance Objectives

Performance Objective	Metric	Data Requirements	Success Criteria
Quantitative Performance Objectives			
Decreased Downtime	Average Event Duration (hrs./event)	Start/end times for events as detected by Sentrigard and other monitoring systems	Decrease in event duration
Decreased Labor Loss	Total Labor Loss from Events ($)	Duration of events, number of employees impacted, and average labor rate	Decreased labor loss attributed to events
Decreased Energy Consumption	Energy Consumption Deviation (kWh$\underline{\Delta}$)	kWh consumption of facilities before, during, and after events	Decrease in energy consumption deviation between event recovery and non-event operation
Meantime to vulnerability mitigation	Change in speed to patch software	Jan 2020 MS vulnerability of crypto libraries to future state	Decrease mitigation length by a least a week
Qualitative Performance Objectives			
Voice of the Customer	Reviews on patch deployment appliance	End of project VOC survey	High return rate of information from surveys
Technology Transfer	Results from presentations at conferences like SAME JET	Audience surveys from conferences	High rating of presentations about technology transfer

Name and Definition

Decreased labor Loss.

Purpose

Decrease the unavailability of facilities due to service interruption.

Metric

Service disruptions are recorded in hours and totaled across all event occurrences. This total is used, along with total employees impacted and average labor rates, to calculate the total labor cost.

Data

The total number of employees and average labor rates is needed to calculate total labor cost for the duration of all events,

Analytical Methodology

A comparison can be made between historical service interruption data and expected efficiency to determine a baseline understanding of potential labor cost efficiency. This analysis can be applied to estimated forecasts for service interruption.

Success Criteria

Success is indicated as a decrease in the cost of interruption as defined as the total labor cost (hours x employees x rate).

4.0 FACILITY / SITE DESCRIPTION

The ESTCP Project site is located at Fort Belvoir, a US Army facility, located in Fairfax County Virginia. DEVCOM C5ISR's NVESD (Night Vision and Electronic Sensors Directorate) also called Area 300.

The site consists of the Fort Belvoir NVESD 300 area campus, building 361 for Network CRN 2.0. Each building is (or will be) expected to be equipped with multiple PIT devices as part of a phased project that is currently underway.

PIT devices expected to be available within the site include:

- SEL-2740s, Software Defined Network (SDN) Switches
- SEL-2488, Satellite Clock Server
- Tridium J-8100 Controllers
- EasyIO FC-20 BMS Controllers
- Workstations (TBD)
- Servers (TBD)

Other IP-enabled devices may be added to the monitoring scope as they are installed.

Each building is connected via fiber optic media to a central location. This location will be used for centralized monitoring and reporting of all PIT systems. The SEL-2740s SDN switches will facilitate communication between buildings, PIT systems, and PIT devices.

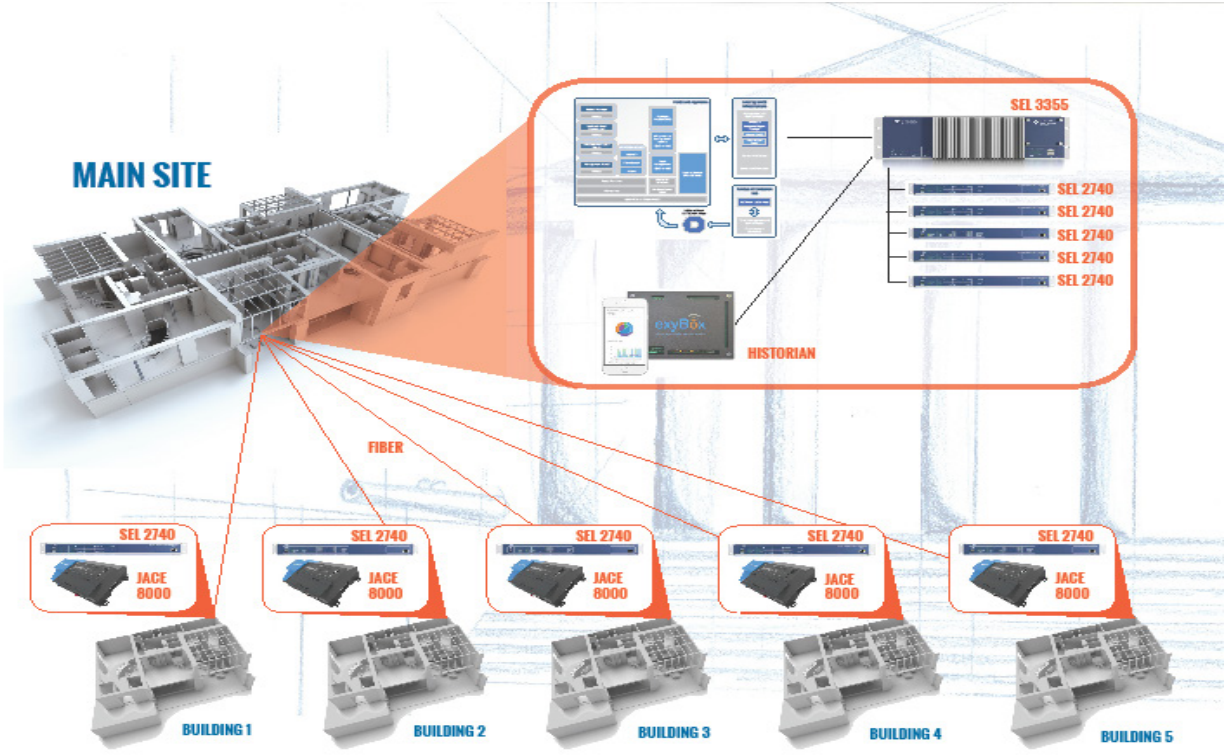


Figure 3. Facility Site Location and Operation

4.1 FACILITY/SITE LOCATION AND OPERATIONS

C5ISR Center's Night Vision and Electronic Sensors Directorate is "The Army's Sensor Developer," conducting research and development that provides U.S. Soldiers with advanced sensor technology to dominate the 21st-century digital battlefield.

NVESD exploits sensor and sensor suite technologies to:

- See, acquire, and target opposing forces, day, or night, under adverse battlefield environments
- Deny the enemy the same capability through electro-optic means and/or camouflage, concealment, and deception
- Provide capabilities for night driving and pilotage
- Detect, neutralize, clear and mark explosive hazards including minefields and unexploded ordnance
- Protect forward troops, fixed installations, and rear echelons from enemy intrusion

C5ISR Center NVESD leverages its explosive hazard expertise in support of the critical U.S. Humanitarian Demining R&D Program.

4.2 FACILITY/SITE CONDITIONS

EMCS, which are designed to enable communications between electrical, mechanical, and Information Technology (IT) systems, allow for maximized energy efficiencies through intelligent management of electrical demand. Because these systems are classified as PIT systems by the DoD, they have been installed at DoD installations for decades with very little or no coordination with DoD's more general Information Assurance (IA) strategies. Existing EMCS deployments frequently cannot reach their full potential for energy savings because of their lack of compliance with DoD IA strategies.

Devices are added and removed from the overall EMCS network on a regular basis (monthly at some installations), presenting complex baselining challenges and preventing easy application of security controls. The lack of an accurate and continuously updated catalog of IP addresses, MAC addresses, and other key identifying information of devices attached to the EMCS network inhibits effective change management, putting these networks at risk of active Intelligence, Surveillance, and Reconnaissance (ISR) activities by advanced persistent adversaries. Furthermore, standard IT scanning and enumeration techniques are not designed for these networks and are unable to speak their native EMCS protocols like BACnet, and Modbus.

Historically, the mitigations for this risk are to "air-gap" the EMCS network (or to isolate the EMCS into a VLAN serviced by the installing EMCS integrator or OEM provider), which decreases its functionality and prevents it from delivering its full energy savings potential. Unfortunately, outsourcing this effort to outside Subject Matter Experts (SMEs) creates large gaps in maintenance and security when contracts expire, or integrators move on. An IT nightmare ensues, as knowledge of these systems and implementation of the system's security typically leaves with the SMEs. Without accurate knowledge of what devices are part of the EMCS system or how they communicate, IT personnel are unable to maintain the EMCS effectively, and the increasingly out-of-date system becomes an attack vector for the adversaries.

It is important that any EMCS defense in depth strategy includes a detailed and continuously maintained asset list. Without a rigorous asset management solution, it will be extremely hard to detect new malicious devices or provide any form of configuration and change management system to maintain a healthy and secure network. Accurate asset management will also have operational and energy benefits by illuminating prioritized End of Support (EOS) EMCS assets for upgrade through capital and life cycle planning for operators of EMCS systems. Conventional IT asset management solutions do not recognize the protocols that EMCS systems speak and cannot offer continuous updating and change detection.

Effective system patching is a key element of an effective defense in depth strategy but is rare for EMCS deployments. Patching processes, if done at all, can create problems with the EMCS. If the EMCS is run by firmware-based devices, then applying a firmware update at minimum requires a reboot to apply the firmware after uploading it to the device. In some instances, firmware-based devices must be taken offline and put into a different operational mode in order to upload the firmware, which requires additional downtime. In addition, the devices may require re-configuration after the update, as certain devices do not retain all settings after applying a firmware update. Even minimal downtime can negate months of energy savings. Software patches can fix bugs, plug recently discovered vulnerabilities, or add new functionality or features. Because of this, IA professionals push to have all released patches deployed rapidly in their enclaves. The expectation of rapid patching for Microsoft Operating Systems (OSes), Java Virtual Machines (JVMs), and other components of an EMCS that are common to an IT environment is considered important because the risk of applying these patches may cause system failures and downtime, IT staff are often compelled to rely on the Original Equipment Manufacturer (OEM) to validate a successful patch and the vendor to perform the actual patching. This high bar means that in most cases EMCS patching never happens at all.

Operationally, the process of researching available and validated patches from OEMs can be a challenge. Patches often reside behind credentialed web portals run by the OEM. The process of finding, validating, and checking hashes for patches creates added labor. Most EMCS vendors use technicians in the field to do one-off patch deployments, which creates variability in patching processes and an inability to generalize techniques and procedures. This increases the risk of operational problems during the patching process and the resulting increased energy consumption when the EMCS are taken offline for remedial maintenance or do not take advantage of additional operational OEM feature updates over time.

Best practices for designing defense in depth strategies for IT systems include Continual Diagnostics and Monitoring (CDM), but these systems are rarely found in EMCS environments. This leaves the system vulnerable to malware without Intrusion Detection System (IDS) and Security Information and Event Management (SIEM) to alert system owners to attacks or vulnerabilities on the system.

5.0 TEST DESIGN

FoxGuard Solutions performed integration testing in a laboratory environment at a FoxGuard Solutions facility. SSI built and delivered a test bed (Figure 4) that mimicked the CRN test environment FoxGuard Solutions. The equipment consisted of:

- Dell PowerEdge R730: Virtual environment hosting Active Directory, McAfee ePO HBSS, Syslog server, and applications for accessing/managing the OT devices
- Two SEL-2740S Software-defined Networking Switches
- JACE-8000 controller
- EasyIO FC-20 controller
- eGauge Meter

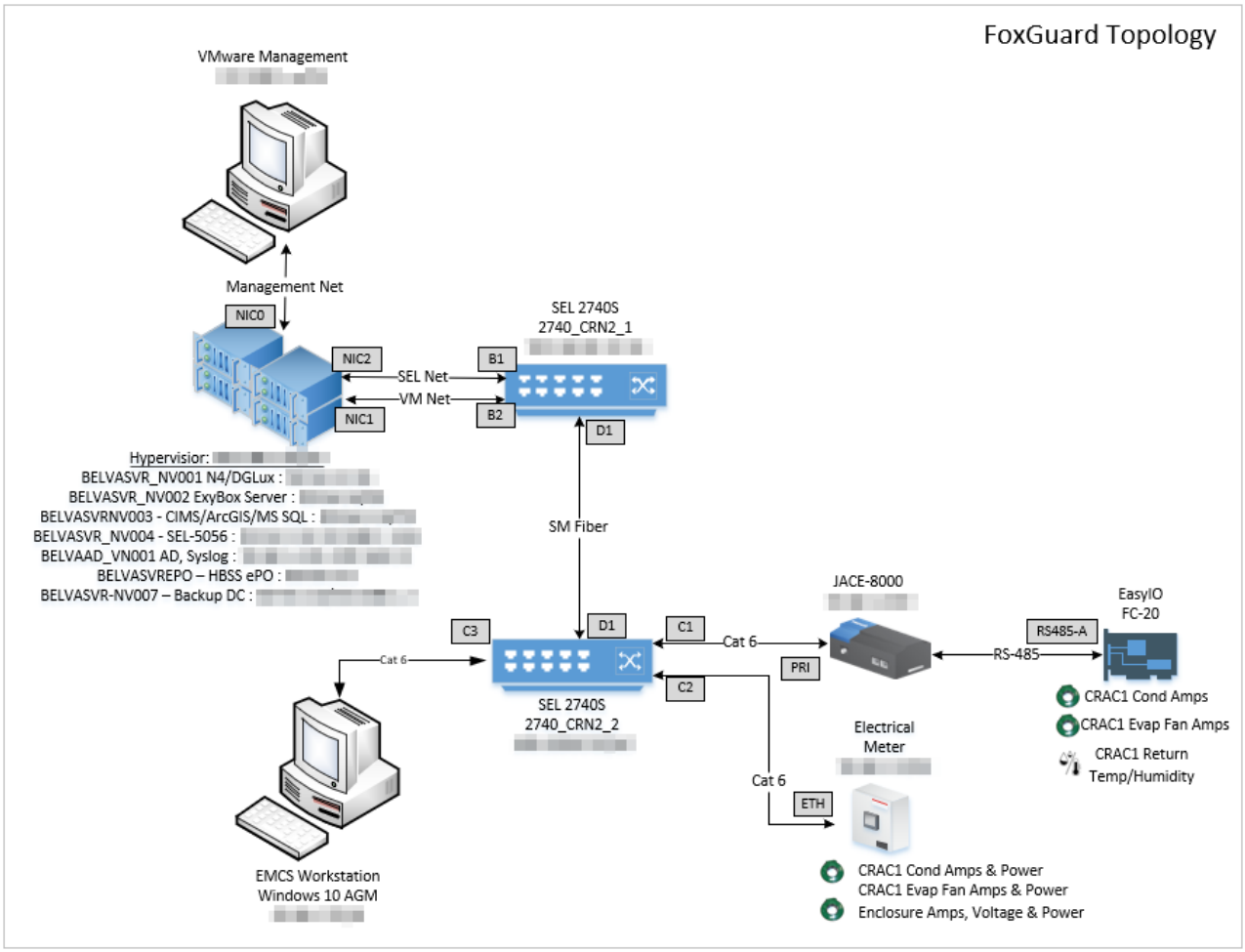


Figure 4. Test Environment Diagram

Once the equipment was received and hooked up in a test rack, FoxGuard engineers worked with SSI to confirm that all components were operational and ran through validation procedures provided by SSI to confirm functionality. The Sentrigard solution was then integrated with the test equipment.

Several configuration changes were made on the provided test equipment to properly integrate Sentrigard modules with the environment. Once all Sentrigard functions were verified as working, the validation tests were run again to ensure the equipment still functioned as intended.

The tests were functional in nature and did not generate any data or outputs other than confirmation between FoxGuard Solutions and SSI that the Sentrigard product was successfully integrated with the test equipment without adversely affecting functionality. These tests included the following:

- Verified that the baseline management module could communicate with all virtual machines
- Verified that the log collection agents installed on each virtual machine were sending logs to the Sentrigard log collection module as well as the existing Syslog server
- Verified that traffic flows were being mirrored to the network anomaly detection module
- Verified that the patch management module was able to scan all virtual machines and deploy the latest security patches
- Ran through SSI-provided validation checklist to ensure all devices/applications were still communicating with each other properly

SSI did not do any additional testing. FoxGuard changed the baseline configuration to include a SPAN port for Nozomi.

5.1 CONCEPTUAL EXPERIMENT DESIGN

The test design followed a standard test pattern that is used with FoxGuard Solutions' existing customers to validate patches against vendor-specific hardware/software. The test pattern is:

- Verify normal functionality is present prior to the start of the test
- Perform required changes, such as software updates, configuration changes, etc.
- Verify normal functionality is present after changes are complete
- Note any changes to the system baseline after changes are complete

5.2 BASELINE CHARACTERIZATION

FoxGuard Solutions used guidance from SSI to identify "normal" functionality for the provided test equipment as the baseline for demonstration success The validation instructions provided by SSI were tested prior to implementation of the Sentrigard Enterprise technology solution, as well as after deployment. No abnormalities were discovered in the functionality of the test equipment after deployment of Sentrigard Enterprise in the FoxGuard Solutions test lab.

5.3 DESIGN AND LAYOUT OF TECHNOLOGY COMPONENTS

The Sentrigard Enterprise technology solution is described at a high level in section 2.1 of this report. The following sections describe each component of the solution in more detail:

NGINX Reverse Proxy

NGINX is a free open-source HTTP server and reverse proxy that uses an event-driven architecture rather than relying on threads to handle requests. This runs as a Docker container on the Linux Application Host virtual machine and is bound to an external network adapter. Within the Sentrigard Enterprise solution, the NGINX reverse proxy provides a landing page for users to access the web-based applications within Sentrigard Enterprise. An example of the landing page can be seen in figure 5 below:

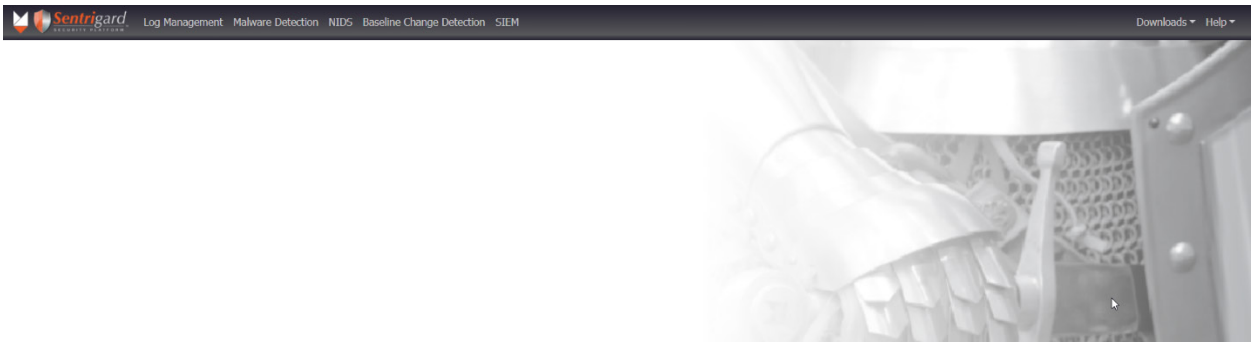
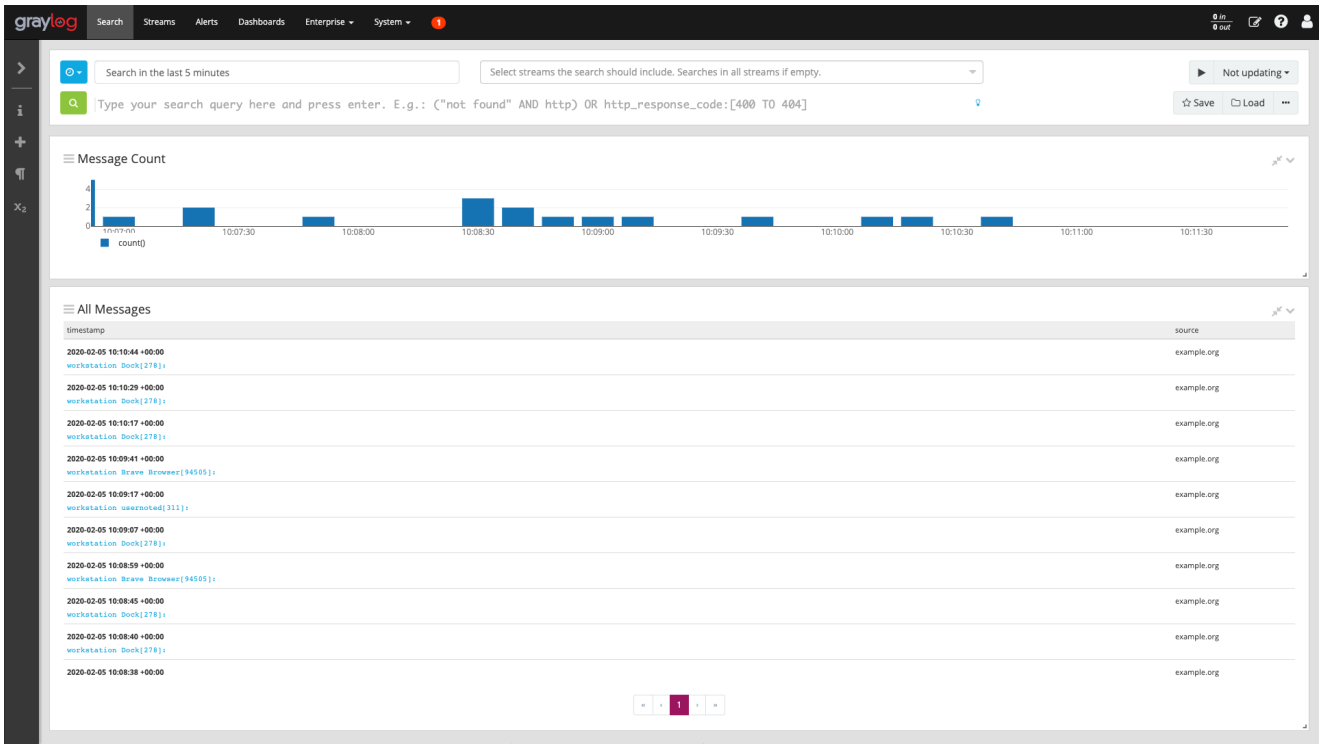


Figure 5. The Sentrigard Enterprise Landing Page

The reverse proxy also routes requests for each web-based application to the correct internal service. For example, Graylog runs as a Docker container and does not expose the web-based management port to external systems. Instead, requests are sent to a URL such as **https://sentrigard-enterprise/graylog**, and are then routed by the proxy to the container. Additionally, the proxy can modify cookies for specific application requests where a cookie from another application the user is logged into may cause issues with another application. This allows the application with the offending cookie to still function as required but disables that cookie for requests to other applications.

Graylog

Graylog is the primary centralized log collection point that runs as a Docker container on the Linux Application Host virtual machine. It is referred to as the Log Management Module with the Sentrigard Enterprise solution. Graylog is an open-source application that shares technology components with the widely used ELK stack. The ELK stack consists of Elasticsearch, Logstash, and Kibana, all of which are open source. Elastic is a search and analytics engine that is responsible for indexing log data. Logstash is a data processing pipeline that ships log messages from various sources and can transform data on the fly. Kibana is a frontend application that allows users to query data stored in Elasticsearch, as well as providing robust data visualization capabilities. Graylog uses Elasticsearch to store data, Beats (which are lightweight log shippers forked from Logstash), and its own graphical frontend that provides similar capabilities to Kibana. An example of this graphical frontend can be seen below:



On Windows and Linux-based endpoints, the Sidecar application is installed to assist with log collection. Sidecar allows for centralized management of log shipping tools, including Beats. Winlogbeat (collects Windows event logs) and Filebeat (collects log files) applications are used within Sentrigard Enterprise. Sidecar allows an administrator to define configurations for each log shipper from the Graylog web interface and assign it to individual Sidecars. For all other devices, Graylog is configured to accept Syslog over TCP and UDP.

Graylog is configured with default dashboards and alerts to help users visualize data and receive alerts for specific events. Alerts were not used for this demonstration because the CRN test environment does not have email servers. For more advanced analytics and event management, Graylog is configured to forward logs to Splunk Enterprise.

Splunk Enterprise

Splunk Enterprise is a commercial product that allows users to search, analyze, and visualize data gathered from various sources within a network. It is referred to as the SIEM (Security Information and Event Management) Module in the Sentrigard Enterprise solution. Splunk provides more advanced search and analytics capabilities than Graylog's open-source product. A default dashboard application is included that provides high-level information about the security state of the network and network assets. An example can be seen in figure 6.

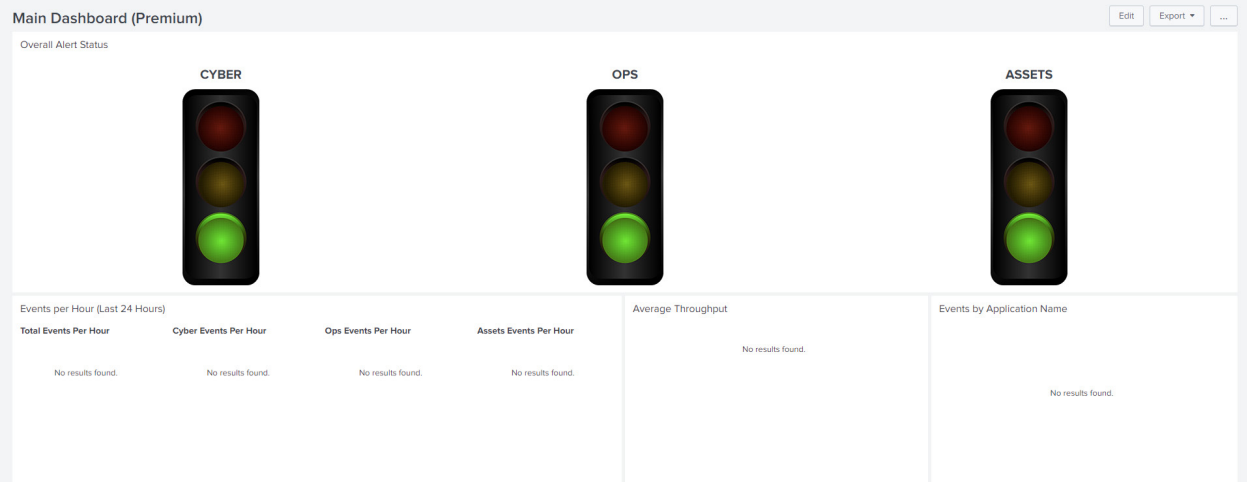


Figure 6. The Sentrigard Enterprise Dashboard Application

As used within Sentrigard Enterprise, data flowed into Splunk Enterprise solely from Graylog. Splunk Enterprise can also accept Syslog messages and log data sent by the Splunk Universal Forwarder.

OSSEC

OSSEC is an open-source Host-based Intrusion Detection System (HIDS) that provides additional security features often lacking in Host Based Security System (HBSS)products. Within the Sentrigard Enterprise product, OSSEC is used to provide rootkit detection, file integrity checking, and Windows registry monitoring.

The OSSEC agent runs seamlessly in the background on Windows and Linux-based endpoints and reports all events to the OSSEC server. The OSSEC server runs in a Docker container on the Linux Application Host virtual machine. All messages from OSSEC are forwarded to Graylog for analysis. There are defined alerts and dashboards in Graylog to show detections by the OSSEC agent.

TDi ConsoleWorks

TDi ConsoleWorks is a commercial product that can provide secure remote access, configuration and baseline monitoring for assets, logging, and endpoint password management. The ConsoleWorks server resides on a CentOS-based virtual machine within the Sentrigard Enterprise solution.

The primary features utilized in this solution are the configuration and baseline monitoring. This product is referred to as the Baseline Change Detection Module within Sentrigard Enterprise. ConsoleWorks is configured with multiple “consoles”, where each “console” is a connection to a unique device. Baseline processors, which are scripts written within the ConsoleWorks application, connect to each console and periodically retrieve configuration information and compare it to a known baseline configuration. This baseline configuration is created by retrieving the configuration from a device that is configured with the desired configuration and marking it as the master baseline.

If differences are detected, a diff report is generated within ConsoleWorks and a message is sent to Graylog to inform users that a change was detected and should be investigated. In figure 7 an example of a baseline change detected in the status of Windows services on a server, presented as a side-by-side diff:

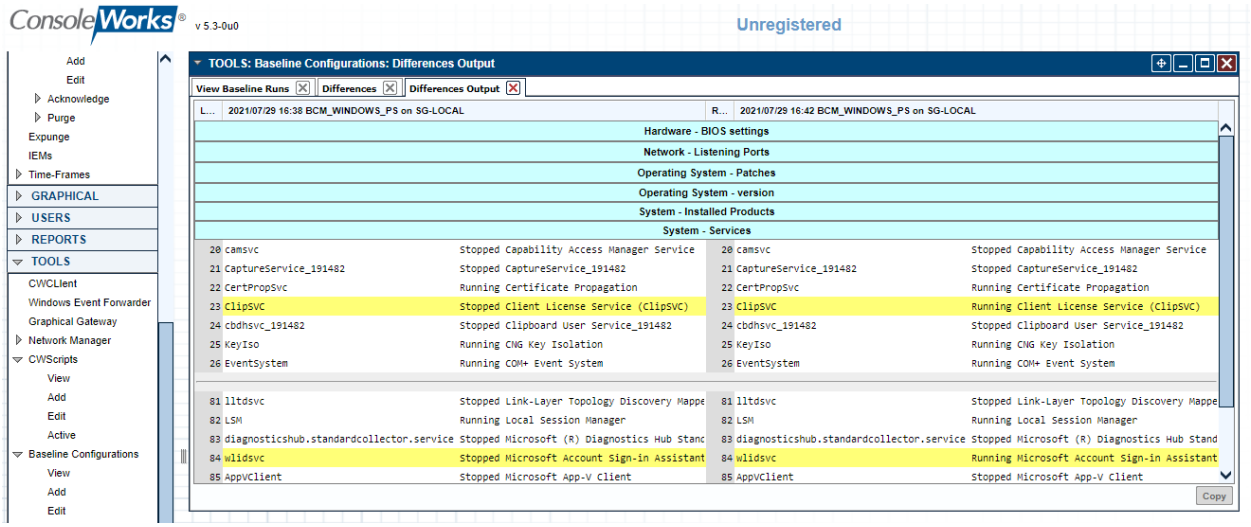


Figure 7. ConsoleWorks Baseline Change

Ivanti Security Controls

Ivanti Security Controls is the Patch Management Module of the Sentrigard Enterprise solution. Ivanti is a commercial product that allows an administrator to scan Windows and Red Hat Linux-based endpoints for missing patches and deploy them remotely. The patch data and patches can be downloaded directly from the vendor's website or provided by FoxGuard Solutions as part of the PBA subscription program. FoxGuard Solutions has integrated this product into multiple OT locations worldwide, and it has been well received by customers in multiple industries.

In addition to the operating system patches, Ivanti Security Controls supports a wide range of third-party applications found in many IT environments. Examples of supported third-party products that FoxGuard Solutions commonly sees in OT environments include:

- 7-Zip
- Adobe Reader DC
- Google Chrome
- Microsoft Office
- Microsoft SQL Server
- Mozilla Firefox
- Notepad++
- PuTTY
- WinSCP

As shown in figure 8, administrators can see a overview of the status of the patches in their environment, and quickly deployed by selected or all missing patches. Relevant information includes the version of the patched software, how the patch was detected missing, and any associated CVEs for each patch.

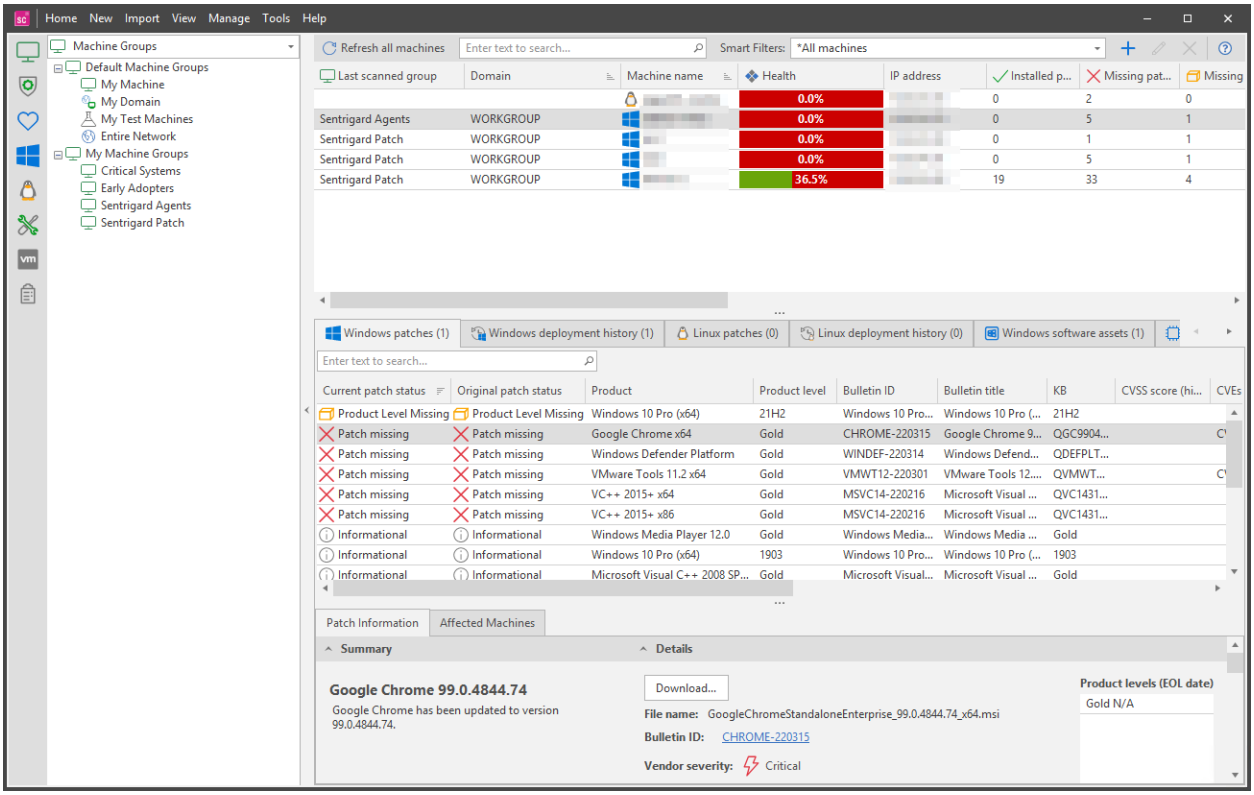


Figure 8. Sentrigard Enterprise Patch Status View

Nozomi Guardian

Nozomi Guardian is an advanced threat detection platform used for ICS, OT, IoT, and IT networks. This product is referred to as the Network Anomaly Detection Module within the Sentrigard Enterprise solution. An overview of the main dashboard of the Nozomi Guardian web-based interface can be seen in figure 9.

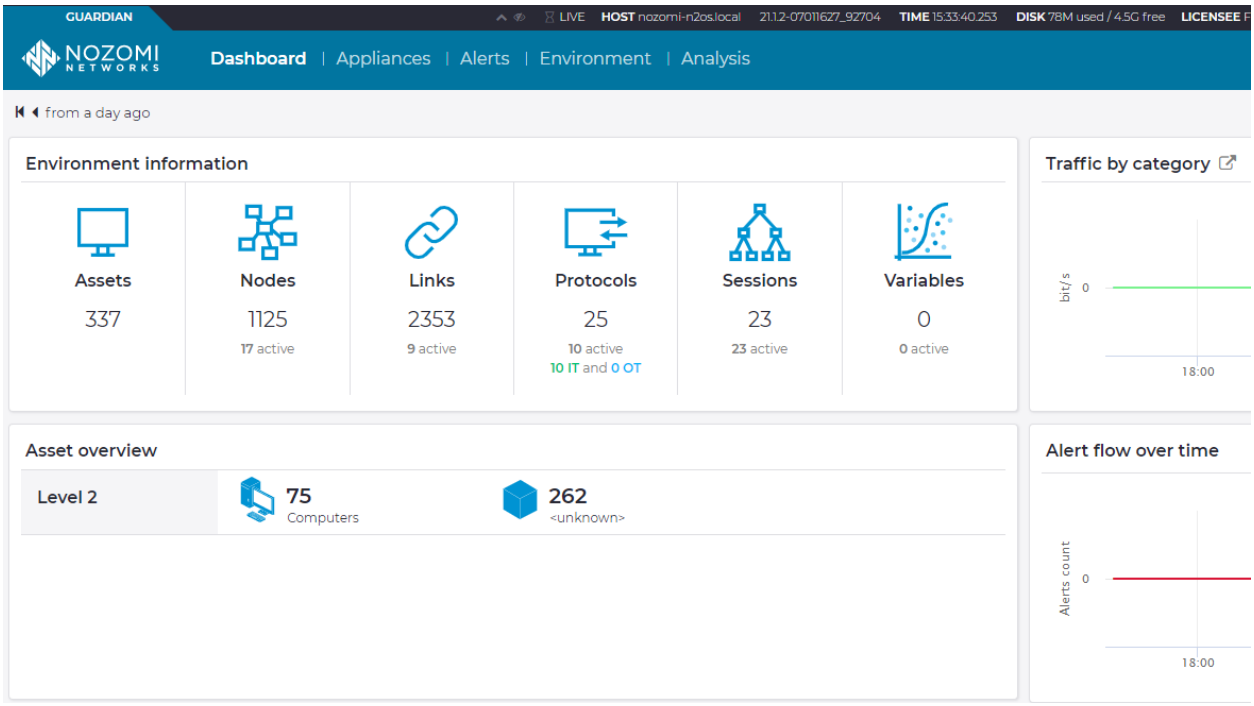


Figure 9. Nozomi Guardian Web-based Interface

Nozomi Guardian monitors network traffic via one or more promiscuous network ports. Traditionally this is achieved using mirrored ports (sometimes referred to as SPAN ports) or network taps. Within the CRN test environment, Nozomi Guardian receives forwarded traffic flows as configured on the SDN switches.

Nozomi Guardian can be used to generate a baseline of known good network traffic within an environment, and alert users whenever new devices appear, new connections between devices occur, new protocols appear, and more. With the Threat Intelligence feed (which can be updated without an active Internet connection), various threats can be detected using a combination of packet-based signatures (as used in most NIDS products) and Yara rules. These detection rules include a wide variety of IT and OT threats, including Stuxnet, Havex, BlackEnergy.

5.4 OPERATIONAL TESTING

Testing in the FoxGuard Solutions lab environment validated the introduction of the Sentrigard Enterprise solution into the CRN test environment would not hinder existing functionality. Validation was performed prior to the integration to confirm everything was functioning normally, and after the integration to confirm the introduction of the Sentrigard Enterprise solution did not cause any key functions or communication paths to stop working. Validation testing was conducted between April 2021 and August 2021.

Validation tests consisted of:

- Verify connectivity to the domain on each domain-joined virtual machine,
- Verify syslog messages are being sent to the syslog server on each virtual machine,

- Verify connection to the HBSS server on each virtual machine,
- Verify replication between the domain controllers
- Verify Fox connection to remote JACE on the N4Tridium virtual machine,
- On the SEL5056 virtual machine, verify the SEL-5056 service is running and check for offline devices
- On the CIMS_ArGIS_SQL virtual machine:
  - Verify the CIMS service is running and functioning correct
  - Verify connection to SQL database
  - Verify connection to ArcGIS
  - Verify connection to Niagara
- On the Exybox virtual machine:
  - Verify the Exybox service is running and functioning correctly
  - Verify connection to SQL database
  - Verify BACnet connections to remote JACE

No issues were found with any of the above validation checks in the FoxGuard Solutions lab environment.

6.0 PERFORMANCE ASSESSMENT

With the Sentrigard in place the CRN 2.0 is subset of OT and IT components found on the FB-FRCS production network. CRN 2.0 consists of a ESXI server that contains the same virtual machines that are part of the production network. A single SDN switch provides network connectivity between devices. A JACE 8100 building automation controller gets data from a single EasyIO which is monitoring an air conditioning system in building 361. These devices provide the same network protocols found on the production network. One electric meter is also part of the CRN 2.0 network that represents the electric meters and protocols. The components and data from a previous ESTCP microgrid project have been integrated into the network. All these systems provide users with real data from actual hardware in a controlled environment for OT training, cybersecurity testing, and software/firmware testing. Using the Sentrigard system administrators must apply any software or firmware patches to the CRN 2.0 components before any changes are made to the production network. New hardware and software can be added to the system for integration testing, product comparisons, and vulnerability analysis. The network is designed to scale up or down to meet user requirements. CRN 2.0 can be accessed remotely to allow users to conduct testing at a significant cost savings. CRN 2.0 was recently used by a DoE project focused on OT cybersecurity. The stakeholders remotely connected to the CRN 2.0 network and conducted all required testing, experiments, and analysis. Future efforts for CRN 2.0 include extending the software defined network to a contractor facility allowing for software sustainment activities (updates and patches) to be conducted remotely. This will significantly reduce the amount of costs required to maintain a system's authority to operate. Another future effort will be to push the building automation system data to a DOD approved cloud for analysis.

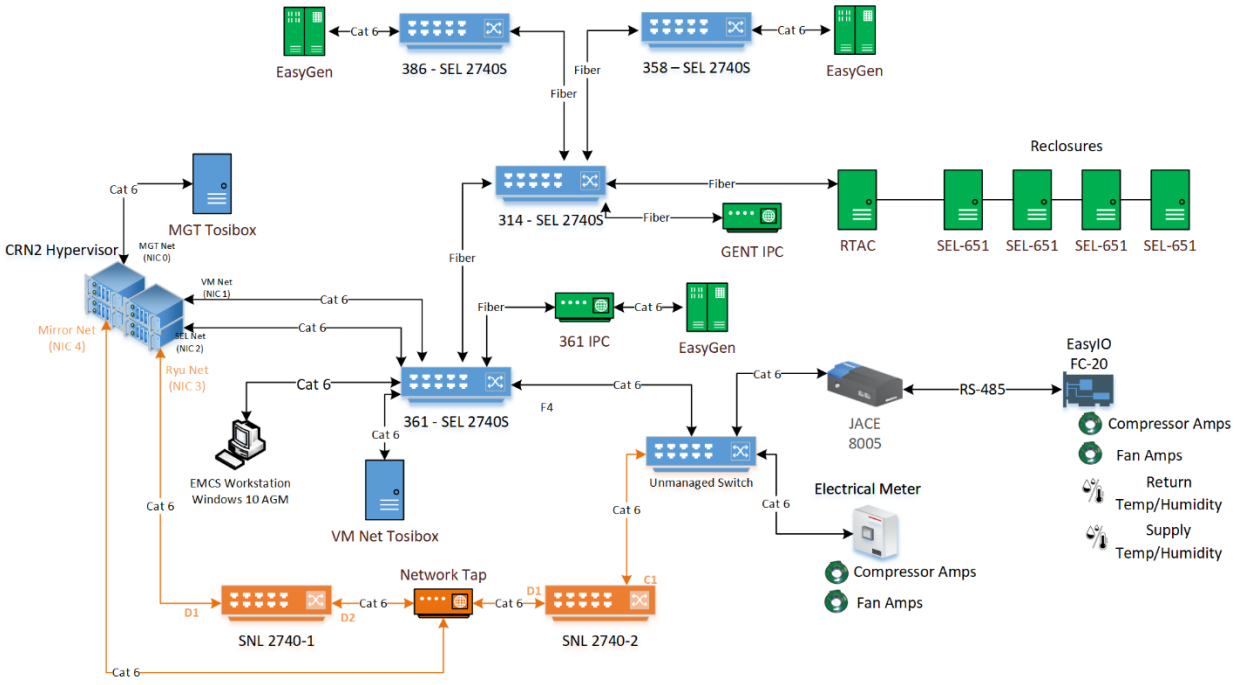


Figure 10. CRN 2.0

7.0 COST ASSESSMENT

Costs for implementation at a given site are provided in 7.3. In addition, the cost benefit of the technology is explained below table 2 in 7.1.

7.1 COST MODEL

An estimated cost model for the technology is provided in the below table.

Table 2. Cost Model of Technology

Cost Element	Data Tracked During the Demonstration	Estimated Costs
Hardware capital costs	Estimates made based on component costs for demonstration	$290,115.00
Installation costs	Labor and material required to install	$60,000.00
Maintenance	Frequency of required maintenance Labor and material per maintenance action	Frequency is low to none Expense: $12,500.00/ year
Hardware lifetime	Estimate based on components degradation during demonstration	5 years
Operator training	Estimate of training costs	$5,000.00

[1] Detailed list of materials and analytical costs provided in Final Report

For each cost element relevant to the technology, a provided subsection is below:

Hardware Costs:

- The cost of the initial investment in the hardware is comparative to the amount of labor needed to effectively research and patch existing appliances within the network. Initially, deployments would require a form of custom work to support the specific devices installed at different sites.
- Through DoD voice of the customer processes, FoxGuard found between 1 and 3 full-time employees are budgeted to deploy patches and other EMCS security controls at DoD installations (reference upon request).

Maintenance:

- FoxGuard provides the licensing for the software used under the contract agreement and the terms of licensing length are confirmed based on the customers' needs or requests. The physical hardware of this system requires limited maintenance action or labor. The estimated labor costs and training costs presented in Table 2 are the outsourced support from contractors a site may be using to manage their OT/IT environments, install patch updates quarterly and report

Hardware Lifetime

- FoxGuard estimates the lifetime of the hardware is expected to be 5 years based on standard use of service equipment in a controlled environment setting.

Operator Training

- The estimated time to train an operator to successfully use the Sentrigard Patch System is 3 business days. This can be reduced if training can be completed remotely.

7.2 COST DRIVERS

Site-specific cost drivers on this project were all managed within the budget of the contract. Cost reduction drivers within the overall scope of this project are identified below.

Funding

- Determination of where the appliance needs to be installed has potential to have an impact on the cost if a new space must be built on site.
- The efforts taken in this specific site and project to provide an RMF A&A were ineffective due to the additional funding required for a sponsorship of the RMF and the A&A RFM process requirements.

Schedule

- The impact of a global Pandemic. Though this is something that can never be anticipated it is suggested that future projects consider the impacts on delays in installation and sitework due to these types of challenges. There is work such as prep and testing on the appliance that can be done during a time like this to help reduce some delay.

Cost Reduction Drivers

- Scaling this solution to an enterprise level would produce great economies of scale for the DoD because most of the functionality of the EMCS security platform is generally applicable to EMCS networks built on supported devices. Initially, deployments would require custom work to support the specific devices installed at different sites, but each new deployment would be able to re-use the technology developed and lessons learned at previous sites.
- Rapid scaling of patch deployments across multiple installations will decrease operating costs by harmonizing patch research and aggregation across multiple EMCS deployments. Additional cost saving opportunities exist by centralizing the lab-based validation efforts and patching services across the whole DoD deployment into a single validation lab. This will centralize and simplify the costs of validating and documenting patching for an EMCS at one location instead of across hundreds of individual deployment sites and personnel.

7.3 COST ANALYSIS

We have provided realistic estimates for the costs of the technology when implemented operationally. This is estimated based on current pricing as of 2022. The price is estimated, every site can be different and if installed on multiple sites there could be additional savings. A narrative of how each applicable cost element can be used to estimate the life-cycle costs for implementing and operating the demonstrated technology is provided below.

- The requirement of a single site that has a confirmed asset list, which can be broken down into a unique item list. For the purpose of the below cost analysis, we have estimated that a typical single site has up to 100 unique items that require support and monitoring, and dedicated rack space available for the appliance is available.
- Licensing for software should be considered by periods such as one year, three years, or five years licensing terms.

Sentrigard Enterprise Equipment (including Software Licensing for 1 year)	$ 77,889.35
Installation and site support work (Est. 175hrs)	$ 35,000.00
Patch Availability Reporting Subscription (12 months) & Setup fee (Based on 100 UI Service) additional cost savings can be provided if a multiyear subscription is purchased.	$ 64,200.00
Patch Binary Acquisition Subscription (12 months) & Setup fee (Based on 100 UI Service) additional cost savings can be provided if a multiyear subscription is purchased.	$ 40,200.00
Total Estimated Pricing	**$ 217,289.35**

- Replacement costs should be evaluated based on the need for network infrastructure changes and product feature updates or improvements at the time of replacement. Estimated per site replacement costs are shown below. These costs can additionally be reduced if multiple sites are being replaced at the same time.

Sentrigard Enterprise Equipment Upgrade (including Software Licensing for 1 year)	$ 80,226.03
Installation and site support work (Est. 100hrs)	$ 20,000.00
Patch Availability Reporting Subscription renewal 12-month subscription (Based on 100 UI Service)	$ 55,105.00
Patch Binary Acquisition Subscription renewal 12-month subscription (Based on 100 UI Service)	$ 34,505.00
Total Estimated Pricing	**$ 189,836.03**

At the time of the creation of this report FoxGuard Solutions were not aware of any alternative systems to replace what has been implemented at the site.

8.0 IMPLEMENTATION ISSUES

No procurement issues were encountered for implementation of this technology solution. The Sentrigard server uses standard commercial off-the-shelf (COTS) hardware and a combination of readily available open-source and commercial software components. The network anomaly detection module is sourced from a specific vendor and uses hardware provided by that vendor. As of the time of writing this report, global supply chain issues relating to the manufacturing of chips are certainly a procurement concern, but once those issues have been addressed the required hardware should be readily available.

During implementation, issues were discovered with the software-defined networking configuration already present within the demonstration environment and the lack of standard support for mirroring traffic (as compared to traditional switching hardware). For many switch vendors, mirroring traffic is well documented and only takes a handful of commands to implement. The software-defined networking technology in use within the demonstration environment required additional effort to come up with a configuration that provided the same level of traffic visibility required for the network anomaly detection software to function as intended. Prior to the implementation of future instances of this technology, a more thorough review of the networking configuration should be completed to determine the capabilities of the existing network infrastructure to support mirroring traffic. In addition, SMEs for the network infrastructure should be consulted early on to ensure they are ready to assist and test any changes early in the process of implementation.

Existing configurations for the HBSS were preventing the baseline configuration module from functioning as intended. The HBSS configuration had to be adjusted to allow the necessary traffic through the host-based firewall on the Windows-based endpoints. This issue is not a major concern for future implementations of the technology, and simply requires changes to the HBSS configuration to allow the required traffic.

Due to the limitations of time on the contract and additional site funding we were unable to secure a Sponsor within the US Army to complete the RMF submission and approval. We have the completed RMF documentation which can be provided upon request.

APPENDIX A POINTS OF CONTACT

Point of Contact Name	Organization Name Address	Phone Fax Email	Role in Project
Paul Riggins	FoxGuard Solutions	priggins@foxguardsolutions.com	Lead Program Manager
Owen Green	Spectrum Solutions, Inc. (Industry Partner)	ogreen@spectrumsi.com	Systems Engineer
Kevin Brady	Operations Division C5ISR Center, RTI (NVESD) U.S. Army Combat Capabilities Development Command (DEVCOM) Fort Belvoir, VA (Sponsor Site)	kevin.w.brady.civ@army.mil	Action Officer