FINAL REPORT

Building Automation System Enumeration and Configuration (BASEC)

ESTCP Project EW18-5333

JANURAY 2021

Billy Rios
Jonathan Butts
QED Secure Solutions

ESTCP

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
10/01/2021	ESTCP Final Report	<3653645<$$<36636465

4. TITLE AND SUBTITLE
Building Automation System Enumeration and Configuration

5a. CONTRACT NUMBER
W912HQ18C0041

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Billy Rios
Jonathan Butts, PhD

5d. PROJECT NUMBER
EW18-5333

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
QED Secure Solutions
106 N Denton Tap RD
STE 210-132
Coppell, TX 75019

8. PERFORMING ORGANIZATION REPORT NUMBER
EW18-5333

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Environmental Security
4800 Mark Center Drive Suite
Suite 16F16
Alexandria, VA 22350-3600

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

11. SPONSOR/MONITOR'S REPORT NUMBER(S) EW18-5333

12. DISTRIBUTION / AVAILABILITY STATEMENT

Distribution A: Approved for public release; distribution is unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT
The DoD requires a solution that efficiently evaluates system configurations for vulnerabilities and enforces secure configurations across multiple vendors and military installations. To be cost effective, the solution must integrate with existing network security practices and provide the flexibility to support military missions across DoD facilities. The Building Automation System Enumeration and Configuration (BASEC) tool protects organizations by providing a scalable means to identify, baseline, and certify the cyber security configuration for building automation systems. The innovative tool provides a secure means to examine device configurations, audit system settings, define security policies, and obtain reporting from anywhere in the world. BASEC reporting helps identify specific weaknesses associated with individual configuration files (e.g., weak passwords, missing security patches, insecure services, insecure default configurations and weak/insecure protocols in use).

15. SUBJECT TERMS
Cybersecurity, risk management framework, ICS security, critical infrastructure protection, building automation, configuration analysis, cyber vulnerability

16. SECU Y CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c.THIS PAGE**			Jonathan Butts
UNCLASS	UNCLASS	UNCLASS	UNCLASS	33	**19b. TELEPHONE NUMBER** *(include area code)* 210-473-3868

FINAL REPORT
Project: EW18-5333

TABLE OF CONTENTS

Page

LIST OF FIGURES

Page

LIST OF TABLES

Page

ACRONYMS AND ABBREVIATIONS

ARCYBER	Army Cyber
ATO	Authority to Operate
BASEC	Building Automation System Enumeration and Configuration
DoD	Department of Defense
DoDI	Department of Defense Instruction
ESTCP	Environmental Security Technology Certification Program
INL	Idaho National Labs
IT	Information Technology
MCICOM	Marine Corps Installations Command
NAVFAC	Naval Facilities Engineering Command
NDAA	National Defense Authorization Act
NIST	National Institute of Standards and Technology
RMF	Risk Management Framework

ABSTRACT

Energy control systems provide an innovative and cost-effective means to improve efficiency, expand functionality, enhance safety, and increase reliability. The trend, however, to interconnect management and monitoring capabilities through networking technologies has introduced myriad cyber vulnerabilities. For Department of Defense (DoD) installations, the risks are exacerbated due to nonstandard configurations associated with varying implementations across different bases. Indeed, multiple vendor platforms and disparate unpatched systems deployed over varying infrastructures have created an environment with no standard cyber security management practices or protection mechanisms in place to prevent attacks.

Currently, the DoD lacks the capability to efficiently evaluate system configurations of automated building energy control systems. Obtaining authority to operate by satisfying the requirements established in the Department of Defense Instruction (DoDI) 8500.01, Cybersecurity, and DoDI 8510.01, Risk Management Framework (RMF) for DoD Information Technology (IT) is both time consuming and expensive. Additionally, because the process is manual, evaluation results are not always consistent. The primary challenges facing the DoD for evaluating automated building energy control systems include:

- An extensive onsite assessment can cost upwards of $30k
- Testing and reporting takes weeks
- Evaluations are manual and do not readily scale to multiple sites
- Extensive training of skill-sets is required to correctly evaluate systems
- The evaluation is a one-time snapshot of the current security posture

The DoD requires a solution that efficiently evaluates system configurations for vulnerabilities and enforces secure configurations across multiple vendors and military installations. To be cost effective, the solution must integrate with existing network security practices and provide the flexibility to support military missions across DoD facilities.

The Building Automation System Enumeration and Configuration (BASEC) tool protects organizations by providing a scalable means to identify, baseline, and certify the cyber security configuration for building automation systems. The innovative tool provides a secure means to examine device configurations, audit system settings, define security policies, and obtain reporting from anywhere in the world. BASEC reporting helps identify specific weaknesses associated with individual configuration files (e.g., weak passwords, missing security patches, insecure services, insecure default configurations and weak/insecure protocols in use). In addition to individual device configuration settings, BASEC allows analysis of trend data across the entire building and energy infrastructure.

BASEC provides a new technology that can scale cyber security baseline criteria to millions of devices using customizable rule sets mapped to RMF criteria. For ESTCP, QED Secure Solutions demonstrated the ability to perform secure evaluations of system configurations against RMF requirements, track RMF compliance, readily deploy the capability, and accomplish auditing in seconds. The BASEC solution reduced the time and cost of gaining ATO for legacy and new facility energy control systems and has the potential to save the DoD tens of millions of dollars compared against the current state of manual team assessments.

EXECUTIVE SUMMARY

INTRODUCTION

Facility energy control systems provide an innovative and cost-effective means to improve efficiency, expand functionality, enhance safety, and increase reliability. The trend, however, to interconnect management and monitoring capabilities through networking technologies has introduced myriad cyber vulnerabilities. For DoD facilities, the risks are exacerbated due to nonstandard configurations associated with varying implementations across different organizations. Indeed, multiple vendor platforms and disparate unpatched systems deployed over varying infrastructures have created an environment with no standard cyber security management practices or protection mechanisms in place to prevent attacks.

Facility energy control system configurations are not standardized across the DoD, and defense capabilities and tools do not have the ability to monitor and/or evaluate their security posture. A direct cyberattack could result in major impact to mission effectiveness, or jeopardize public safety. Through the ESTCP effort, QED Secure Solutions evaluated the Building Automation System Enumeration and Configuration (BASEC) tool developed to identify misconfigured building automation systems associated with DoD installation infrastructure. The primary objectives associated with the ESTCP effort included:

- Provide automated evaluation of system configurations against RMF requirements
- Show ease of deployment design for use by installation/facility control engineers
- Accomplish compliance auditing in seconds
- Incorporate BASEC with current DoD network solutions with no architecture changes required
- Generate automated reports that identify compliant/non-compliant security configuration details
- Identify savings in cost associated with manual evaluation versus the BASEC automated evaluation capability for obtaining authority to operate (ATO)

BASEC demonstrated a cost-saving solution for evaluating the cyber security posture of military installation building automation systems. QED evaluated BASEC at 35 buildings located on six military installations. Over 150 DoD personnel, including Army, Navy, Air Force, Space Force, and Army Corps of Engineers, were trained and evaluated using BASEC. Additionally, BASEC was incorporated into the 2017 National Defense Authorization Act (NDAA) 1650 efforts with Service component assessment teams to assist in evaluation of installation infrastructure cybersecurity posture. Indeed, BASEC was able to effectively and efficiently audit configuration files to ensure compliance with DoD cyber security guidance and security controls.

OBJECTIVES

Through the ESTCP effort, we demonstrated BASEC's capabilities for identifying vulnerable and misconfigured building energy systems associated with DoD building and energy infrastructure. The primary objectives for the ESTCP effort are as follows:

- Provide secure evaluation of system configurations against RMF requirements
- Demonstrate ability to automate and track RMF compliance
- Show ease of deployment-design for use by installation/facility control engineers
- Accomplish configuration and compliance auditing in seconds…not weeks
- Incorporate BASEC with current DoD network solutions–no architecture changes required
- Generate automated reports to identify compliant/non-compliant configuration details
- Provide an enterprise solution that ensures system compliance against RMF requirements
- Identify savings in cost acquisition by imposing configuration standards prior to deployment of new/upgraded building energy systems
- Identify savings in cost associated with manual evaluation for obtaining authority to operate versus the BASEC automated evaluation capability
- Integrate BASEC with ATO procedures to enhance capabilities and decrease liabilities

To protect against cyber-based attacks, it is critical that the DoD identify misconfigured and exposed devices that monitor and control building energy systems. The BASEC capability provides a solution that establishes and enforces cyber security standards for military installation building and energy systems.

TECHNOLOGY DESCRIPTION

BASEC provides a scalable means to identify, baseline, and certify the cyber security configuration for building automation systems. The heart of BASEC is a secure, cloud-based analysis engine that examines and compares submitted configuration and deployment files against established RMF criteria. QED Secure Solutions has developed algorithms that enumerate configuration parameters and compares them against established acceptance criteria.

Figure ES-1 provides a functional overview of the BASEC analysis process. The building automation system configuration file is uploaded to the BASEC analysis engine. BASEC performs automated analysis on the configuration and provides a report on the selected criteria to identify compliant and noncompliant findings. The resulting process enables rapid, consistent evaluation of systems that readily scales.

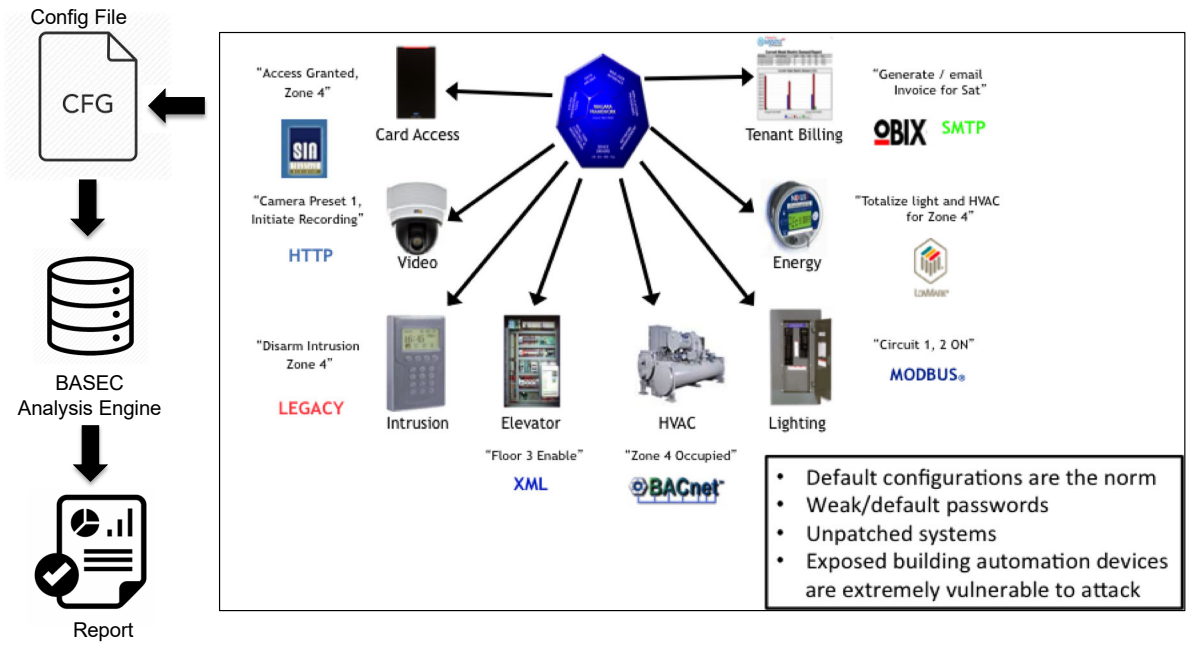

Figure ES-1. Functional Overview of the BASEC Analysis Process.

The BASEC analysis engine is capable of consuming configuration files and enumerating all possible device settings using the BASEC analysis engine. Once uploaded, the file is analyzed by the BASEC analysis engine. When a configuration file is uploaded to BASEC, the analysis engine identifies key indicators within the file to determine the associated vendor. Once the vendor is determined, the analysis engine applies the associated algorithm to unpack the configuration file. Note that each vendor implements their own unique compilation techniques. As such, the reverse engineering required to unpack the configuration files is unique to each specific vendor (and in some instances firmware/software versions). Once a BASEC module is implemented for the file type, however, it is applicable for all future instances of that vendor's same configuration file types. This automated capability to unpack configuration files allows for the rapid evaluation and ability to readily scale.

After identifying the set configurations, the analysis engine evaluates the configuration against pre-defined standards (e.g., DoD RMF criteria). The evaluation determines if each setting is in compliance, is not in compliance, and the severity of the finding if not in compliance. Note that the severity and criteria can be configured to meet individual organizational needs, if desired. For ESTCP demonstrations, the criteria were mapped to common DoD RMF criteria and vendor hardening guides. The BASEC reporting displays the specific weaknesses associated with individual configuration files (e.g., weak passwords, missing security patches, insecure services, insecure default configurations and weak/insecure protocols in use) mapped to the severity rating.

BASEC was designed for ease of use and deployment. For implementation, there are no architecture changes required for the building automation systems. Configuration files are uploaded to the BASEC analysis engine and evaluation is accomplished via BASEC processing. As a result, the system-level configuration can be analyzed without risk to impacting system operations.

PERFORMANCE ASSESSMENT

BASEC was evaluated on six military installations for 35 different building automation systems against four system vendors. The installations consisted of Air Force, Army and Navy facilities. Note that for security considerations, the specific installations are not identified in this report.

The four vendors consisted of Tridium Niagara, Johnson Controls Metasys, Siemens Apogee, and Automated Logic WebCTRL. Four installations implemented one specific vendor, and two installations implemented a mixture of two vendors. The specific facilities examined were associated with core mission/operational functions for the installations.

For evaluation, the team traveled to an installation and met with the designated control system engineer. The control system engineer provided configuration files for the designated facilities. Note that the selection of which facilities to evaluate were determined by the facility engineer and in collaboration with assessment teams. Example building infrastructure included military hospitals, operations control centers, network control centers, military aviation facilities, headquarters facilities, maintenance facilities, and flight simulation facilities. The BASEC reports were provided to the facility engineer upon completion to help them implement more secure configurations in support of hardening the installation infrastructure.

BASEC was evaluated for the ability to identify and examine the configuration of multiple vendor devices that were deployed in multiple building infrastructures and the timeframe required for the evaluation. The type of vendor device or building infrastructure should not impact BASEC's ability to identify configuration deficiencies. At no time should BASEC impact the functional operation of the building automation system. The web-based interface management capability should provide monitoring and reporting of configuration evaluations.

The configuration files of DoD installations were compared against established standards to identify weak configurations and RMF security controls. QED Secure Solutions evaluated BASEC's ability to identify and report deficient system configurations.

BASEC demonstrated the ability to meet the technical and performance objectives for the ESTCP onsite demonstration. For the evaluated buildings, BASEC successfully identified 100% of system device configurations, weak configurations, and changes to configurations. BASEC also produced valid reports based on findings and demonstrated a functional web-based interface management.

The following performance metrics demonstrate the effectiveness of deploying BASEC:

- Average time to perform automated analysis (50 seconds)
- Number of vendors (4)
- Average time to train personnel to be proficient using BASEC (1 hour)
- Coverage of assets (100%)

BASEC was able to transform a manual process of evaluating system configurations that traditionally takes weeks to less than a minute. BASEC also demonstrated effective coverage of the four major building automation vendors that were observed at the six military installations.

COST ASSESSMENT

From a historical perspective, the vast majority of building automation system devices are deployed in their default configuration or configured insecurely. Additionally, recommended controls often lack common configuration and implementation standards. The standards that are recommended typically provide generic guidance that do not readily translate to system specific devices. Organizations often rely on third-party integrators that may rely on commercial network infrastructure or implement configurations that do not comply with DoD security requirements.

Security analysis of DoD building automation systems is expensive for an extensive onsite evaluation. The onsite assessment team approach does not readily scale and provides a one-time snapshot of current security posture. It is also difficult to obtain meaningful metrics for comparative analysis, and there is no current DoD enterprise solution that provides reciprocity for building automation device configuration. As a result, an improperly configured or vulnerable system could result in serious safety concerns, provide access to network data, or negatively impact mission operations. From a safety perspective, an attacker could impede building safety functions, impact environmental conditions or alter building access. Access to network data could result in the ability to obtain protected data, provide a pivot point for executing further attacks or allow exfiltration of data while avoiding DoD network security protections. The operational impact could result in the ability to affect mission assurance, degrade military objectives or provide direct impact to core installation functions.

Findings from the BASEC ESTCP demonstration indicate potential substantial savings to the DoD, while enhancing capabilities. BASEC savings realization include:

- Training. Fully trained on BASEC in one hour vs. assessments requiring cyber operators that must go through extensive training
- Personnel Requirements. Designed for use by installation/facility control engineers
- Time for Assessment. System configuration analyzed in seconds vs. weeks
- Analysis. Consistent findings mapped to defined requirements
- Operational Impacts. Significant potential cost savings with enhanced efficiency and granular results

Manual assessments can cost upwards of $35k and require extensive coordination, allocation of resources and potential disruption to daily operations. The BASEC solution reduces the time and cost of evaluating building automation systems and has the potential for significant cost savings compared against the current state of manual team assessments. Direct cost savings are realized through minimizing the amount of training required to complete compliance auditing, reducing the number of personnel onsite to perform the auditing, greatly reducing the time to complete analysis, providing consistent and timely results, and reducing major impacts to operations.

1.0 INTRODUCTION

1.1 BACKGROUND

Facility energy control systems provide an innovative and cost-effective means to improve efficiency, expand functionality, enhance safety, and increase reliability. The trend, however, to interconnect management and monitoring capabilities through networking technologies has introduced myriad cyber vulnerabilities. For DoD facilities, the risks are exacerbated due to nonstandard configurations associated with varying implementations across different organizations. Indeed, multiple vendor platforms and disparate unpatched systems deployed over varying infrastructures have created an environment with no standard cyber security management practices or protection mechanisms in place to prevent attacks.

Facility energy control system configurations are not standardized across the DoD, and defense capabilities and tools do not have the ability to monitor and/or evaluate their security posture. A direct cyberattack could result in major impact to mission effectiveness, or jeopardize public safety. Through the ESTCP effort, QED Secure Solutions evaluated the Building Automation System Enumeration and Configuration (BASEC) tool developed to identify misconfigured building automation systems associated with DoD installation infrastructure. The primary objectives associated with the ESTCP effort included:

- Provide automated evaluation of system configurations against RMF requirements
- Show ease of deployment design for use by installation/facility control engineers
- Accomplish compliance auditing in seconds
- Incorporate BASEC with current DoD network solutions with no architecture changes required
- Generate automated reports that identify compliant/non-compliant security configuration details
- Identify savings in cost associated with manual evaluation versus the BASEC automated evaluation capability for obtaining authority to operate (ATO)

BASEC demonstrated a cost-saving solution for evaluating the cyber security posture of military installation building automation systems. QED evaluated BASEC at 35 buildings located on six military installations. Over 150 DoD personnel, including Army, Navy, Air Force, Space Force, and Army Corps of Engineers, were trained and evaluated using BASEC. Additionally, BASEC was incorporated into the 2017 National Defense Authorization Act (NDAA) 1650 efforts with Service component assessment teams to assist in evaluation of installation infrastructure cybersecurity posture. Indeed, BASEC was able to effectively and efficiently audit configuration files to ensure compliance with DoD cyber security guidance and security controls.

This report provides results from the ESTCP 24 month effort funded via award EW18-5333. Section 2 discusses the BASEC technology, Section 3 provides the ESTCP demonstration findings, Section 4 identifies the transition efforts and next steps, and Section 5 provides conclusions.

1.2 OBJECTIVE OF THE DEMONSTRATION

Through the ESTCP effort, we demonstrated BASEC's capabilities for identifying vulnerable and misconfigured building energy systems associated with DoD building and energy infrastructure. The primary objectives for the ESTCP effort are as follows:

- Provide secure evaluation of system configurations against RMF requirements
- Demonstrate ability to automate and track RMF compliance
- Show ease of deployment-design for use by installation/facility control engineers
- Accomplish configuration and compliance auditing in seconds…not weeks
- Incorporate BASEC with current DoD network solutions–no architecture changes required
- Generate automated reports to identify compliant/non-compliant configuration details
- Provide an enterprise solution that ensures system compliance against RMF requirements
- Identify savings in cost acquisition by imposing configuration standards prior to deployment of new/upgraded building energy systems
- Identify savings in cost associated with manual evaluation for obtaining authority to operate versus the BASEC automated evaluation capability
- Integrate BASEC with ATO procedures to enhance capabilities and decrease liabilities

To protect against cyber-based attacks, it is critical that the DoD identify misconfigured and exposed devices that monitor and control building energy systems. The BASEC capability provides a solution that establishes and enforces cyber security standards for military installation building and energy systems.

1.3 REGULATORY DRIVERS

Government agencies are solidifying efforts to secure national critical infrastructure. Resulting Risk Management Framework (RMF) and protection strategies are driving factors for BASEC implementation. Findings from the BASEC analysis engine will be mapped to relevant instructions, guidelines and policies that align primarily to RMF requirements that specify security postures and controls. Considerations for demonstration include:

- NIST 800-53
- NIST 800-82
- CNSSI 1253
- DoD Instruction 8100.04
- EO 13806
- UCR 2013
- OSD and DoD Services cybersecurity and control systems regulations and guides
- Industry Best Practices
- DoDIN APL Process Guide
- DISA STIG Questionnaire
- Manufacturer System Description and Component List
- DoDIN APL Product Submittal Form
- UFC 4-010-06

2.0 TECHNOLOGY DESCRIPTION

To protect against cyber-based attacks, it is critical that the DoD identify misconfigured and exposed devices that monitor and control facility energy control systems. BASEC provides a solution that evaluates cyber security standards against established criteria for military installation building automation systems.

2.1 TECHNOLOGY OVERVIEW

2.1.1 Evaluating Security Posture

The primary challenges facing the DoD for evaluating building automation systems include:

- An extensive onsite assessment can cost upwards of $30k
- Testing and reporting takes weeks
- Evaluations are manual and do not readily scale to multiple sites
- Extensive training of skill-sets is required to correctly evaluate systems
- The evaluation is a one-time snapshot of the current security posture

From a historical perspective, the vast majority of building automation system devices are deployed in their default configuration or configured insecurely. Additionally, recommended controls often lack common configuration and implementation standards. The standards that are recommended typically provide generic guidance that do not readily translate to system specific devices. Organizations often rely on third-party integrators that may rely on commercial network infrastructure or implement configurations that do not comply with DoD security requirements.

Security analysis of DoD building automation systems is expensive for an extensive onsite evaluation. The onsite assessment team approach does not readily scale and provides a one-time snapshot of current security posture. It is also difficult to obtain meaningful metrics for comparative analysis, and there is no current DoD enterprise solution that provides reciprocity for building automation device configuration. As a result, an improperly configured or vulnerable system could result in serious safety concerns, provide access to network data, or negatively impact mission operations. From a safety perspective, an attacker could impede building safety functions, impact environmental conditions or alter building access. Access to network data could result in the ability to obtain protected data, provide a pivot point for executing further attacks or allow exfiltration of data while avoiding DoD network security protections. The operational impact could result in the ability to affect mission assurance, degrade military objectives or provide direct impact to core installation functions.

2.1.2 Risk Management Framework

The Risk management framework (RMF) process incorporates standards for securing information systems. The process is based on the National Institute of Standards and Technology (NIST) publications NIST Special Publication 800-37 and NIST Special Publication 800-53. RMF is a six-step process that integrates security and risk management into the system development lifecycle. The six steps are: Categorize information systems; Select security controls; Implement security controls; Assess security controls; Authorize information systems; and Monitor security controls.

BASEC informs the RMF process by evaluating building automation systems to determine if adequate security controls are in place. The BASEC analysis engine has defined controls aligned to NIST guidelines and manufacturer hardening guides. When BASEC evaluates a configuration file for a system, it examines the current configuration and maps the settings to defined security controls. Settings that are not compliant with adequate security controls are identified via the BASEC reporting feature.

2.2 BASEC CAPABILITIES

BASEC evaluates building automation systems for standards compliance and secure configuration. Through the ESTCP project, QED Secure Solutions was able to expand functional capabilities to enhance analysis, incorporate additional device vendors, and refine reporting.

BASEC provides a scalable means to identify, baseline, and certify the cyber security configuration for building automation systems. The heart of BASEC is a secure, cloud-based analysis engine that examines and compares submitted configuration and deployment files against established RMF criteria. QED Secure Solutions has developed algorithms that enumerate configuration parameters and compares them against established acceptance criteria.

Figure 1 provides a functional overview of the BASEC analysis process. The building automation system configuration file is uploaded to the BASEC analysis engine. BASEC performs automated analysis on the configuration and provides a report on the selected criteria to identify compliant and noncompliant findings. The resulting process enables rapid, consistent evaluation of systems that readily scales.

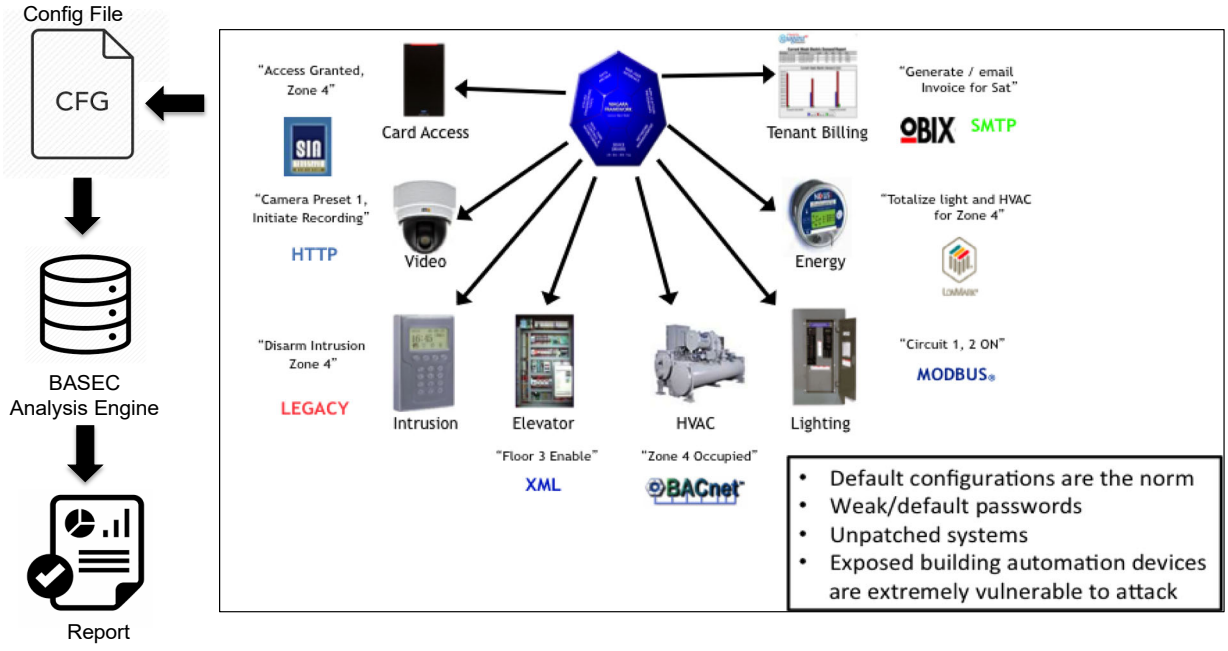

Figure 1. Functional Overview of the BASEC Analysis Process.

As an example, consider the typical configuration file for a facility energy control system shown in Figure 2. Note that this configuration file is from a Tridium Niagara device, which is one of the most widely deployed building automation systems in the DoD. A configuration file, as implied by the name, contains all possible configuration setting for a building automation system device. The configuration file is programmed using device-specific software by an engineer and uploaded to the device. The device accepts the configuration file and modifies the system settings, as specified by the configuration file. As demonstrated, the actual configuration file is not human readable, and it is not practical to assume an analyst can examine the configuration settings by reviewing the configuration file. As such, it is difficult for an analyst to determine the device configuration settings without active system probing or evaluation.

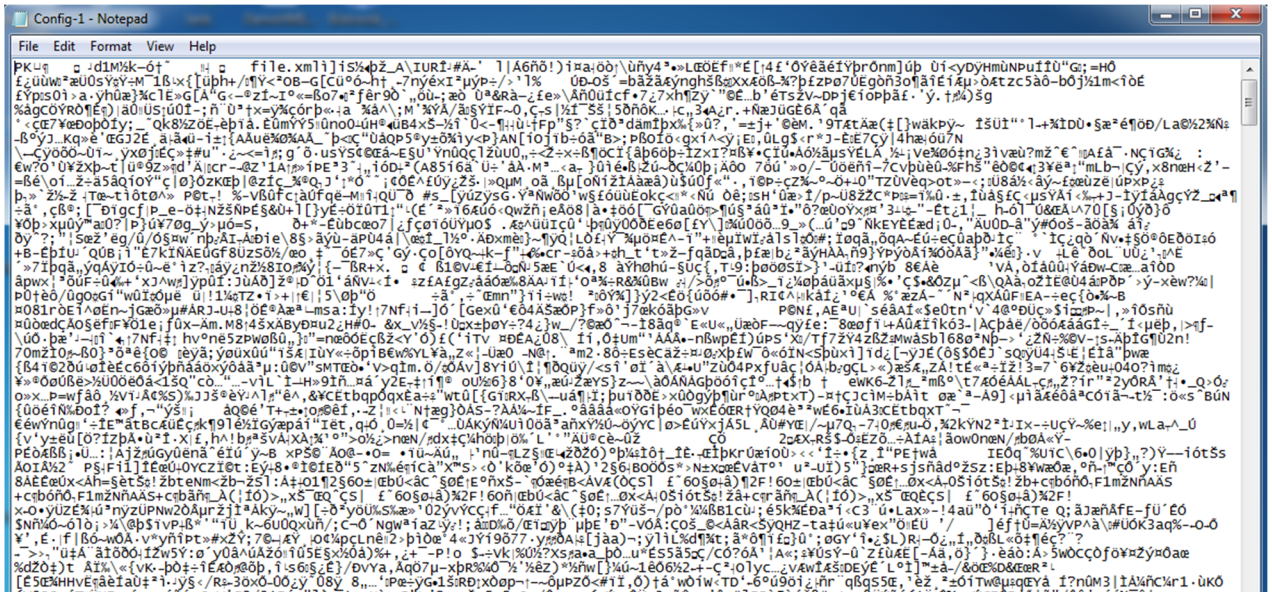

Figure 2. Configuration File from a Tridium Niagara Building Automation Device.

The BASEC analysis engine, however, is capable of consuming the configuration file and enumerating all possible device settings using the BASEC analysis engine. As an example, Figure 3 shows the BASEC portal and main Configuration Analysis page.

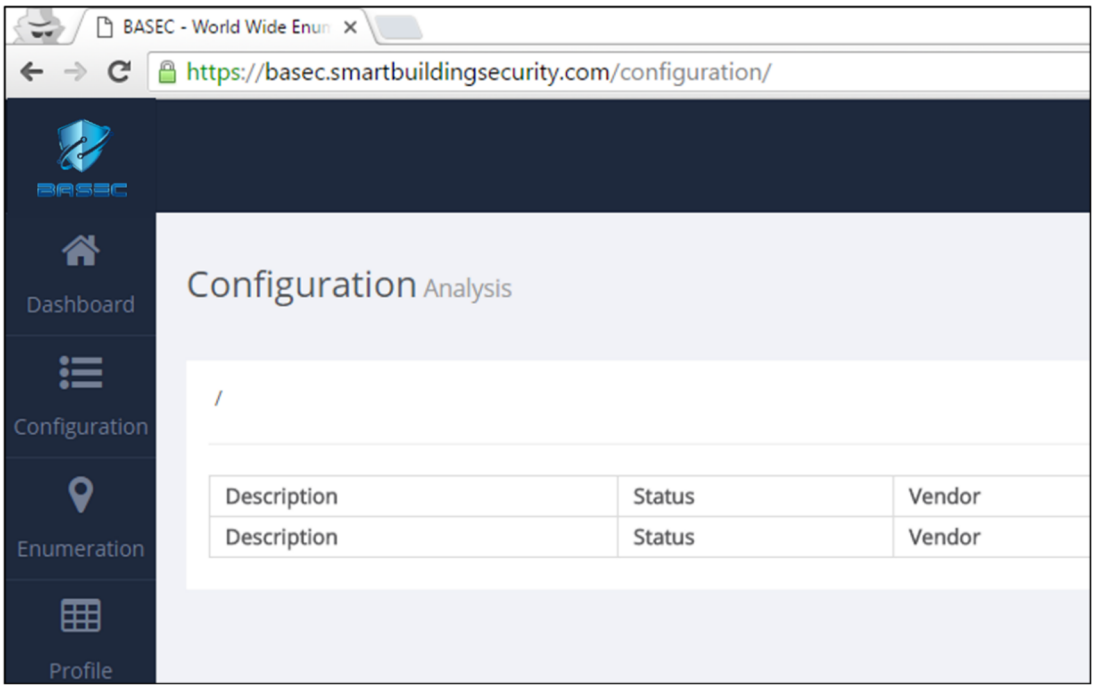

Figure 3. BASEC Portal Landing Page.

A user selects the upload option to load a saved configuration file as shown in Figure 4. Note that configuration files are typically stored by the system integrator/engineer in file share repositories, local system storage, media (e.g., CDs), or can be retrieved directly from the device.

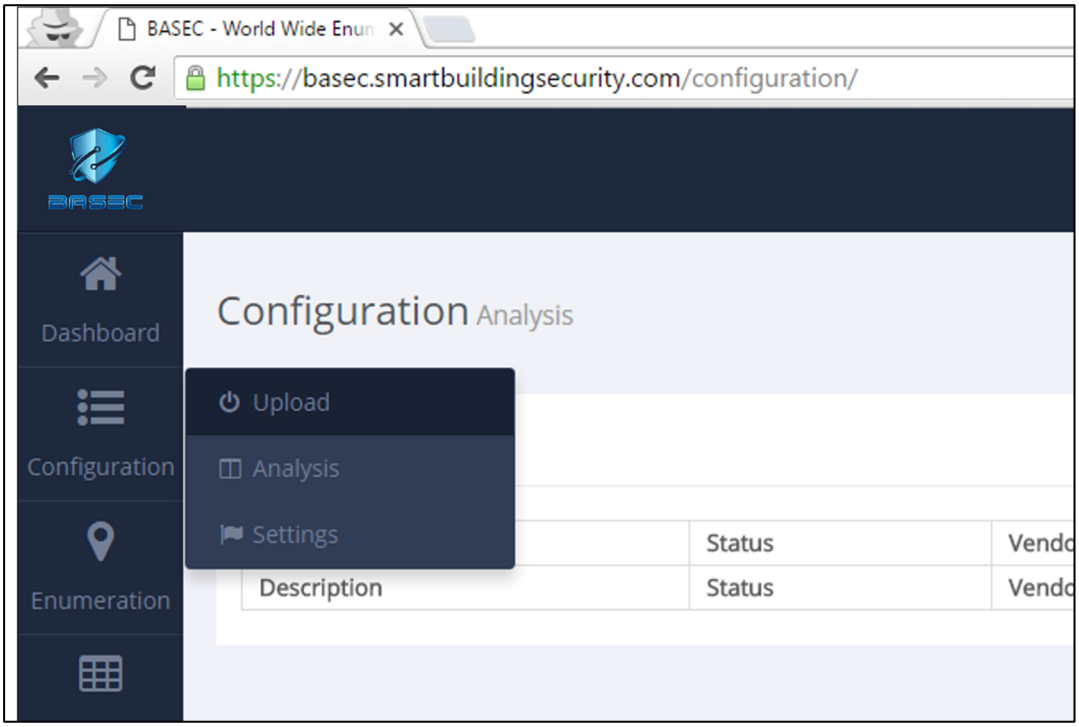

Figure 4. File Upload Option.

The user then selects the configuration file to upload to the BASEC portal as demonstrated in Figure 5.

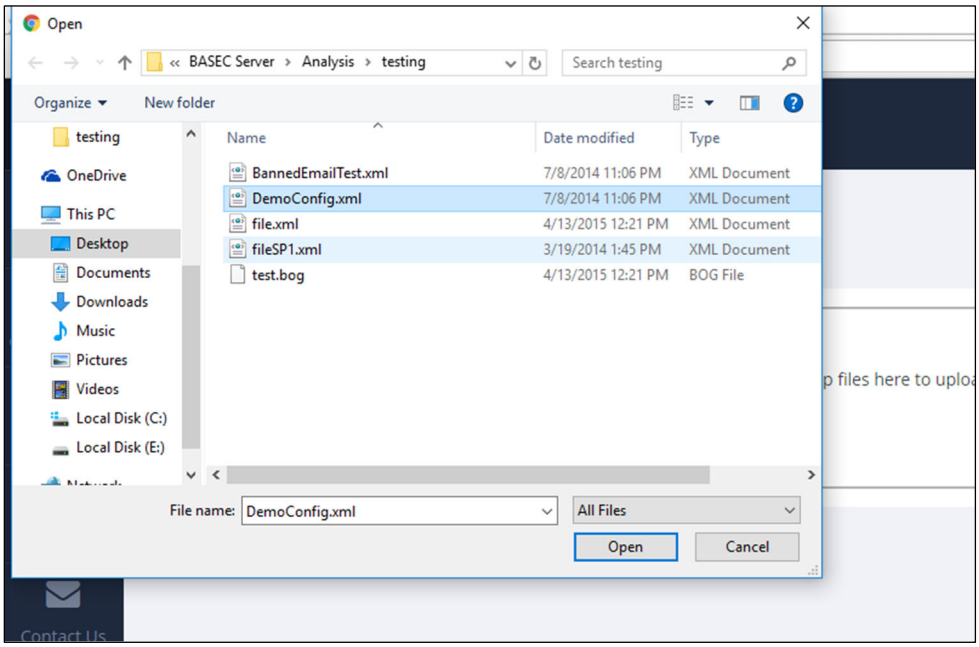

Figure 5. Select configuration File to Be Analyzed.

The user also has the option to drag and drop the configuration file directly to the upload window (Figure 6). Note that implementation of the two upload options was based on user feedback.

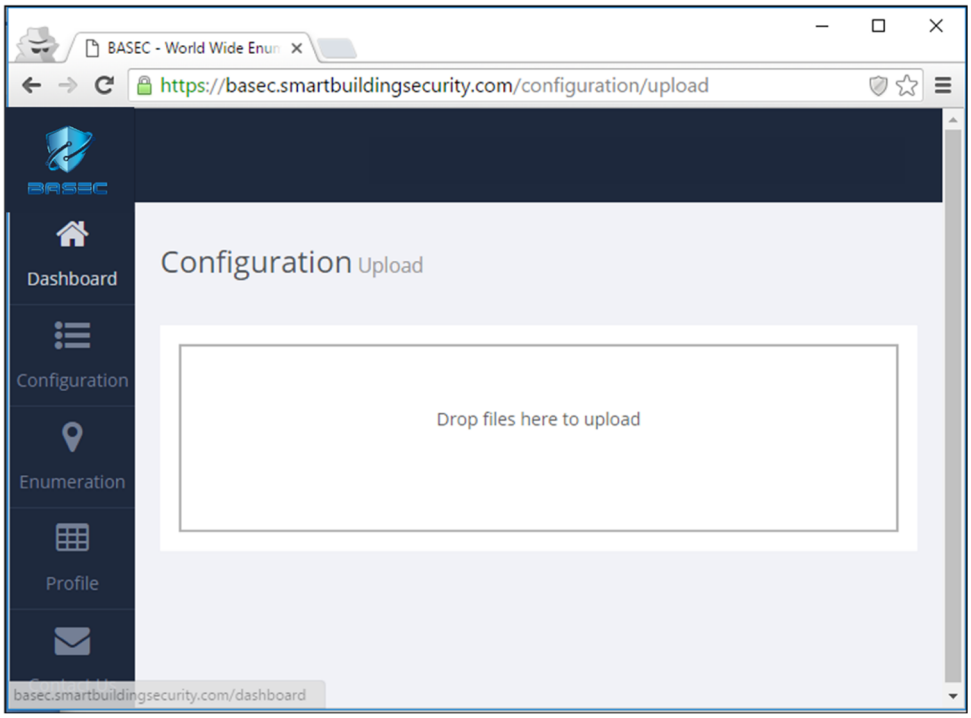

Figure 6. Optional Drag and Drop Feature to Select Configuration File.

Once uploaded, the file is analyzed by the BASEC analysis engine as shown in Figure 7.

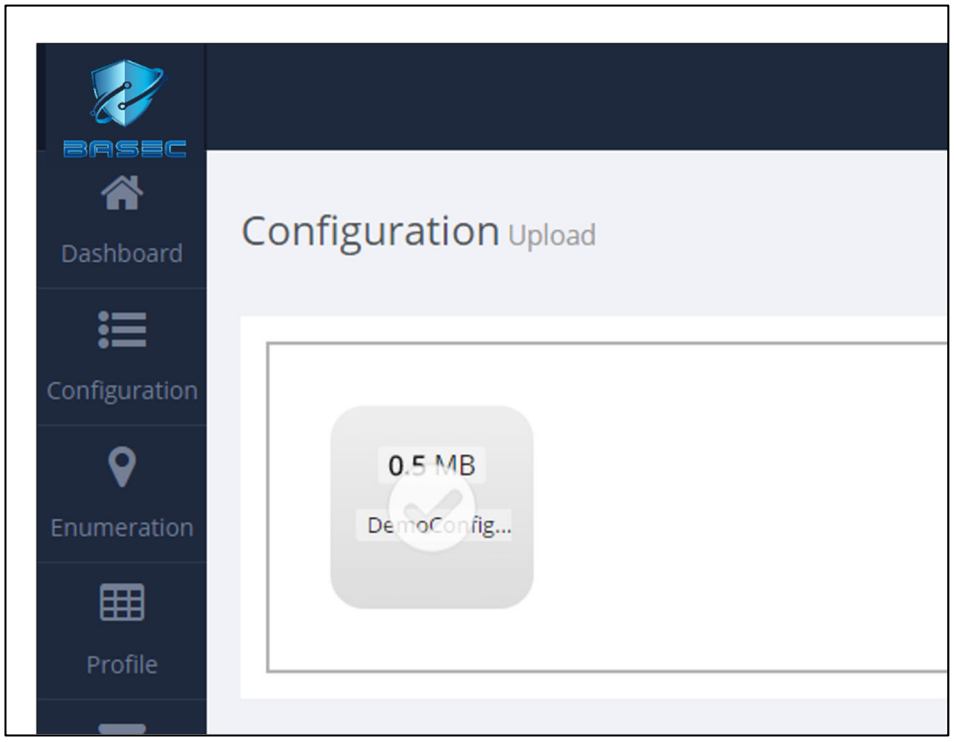

Figure 7. Analysis of Configuration File.

Once complete, the configuration file name is displayed with a hyperlink to the reporting, analysis status, and determined vendor (Figure 8).

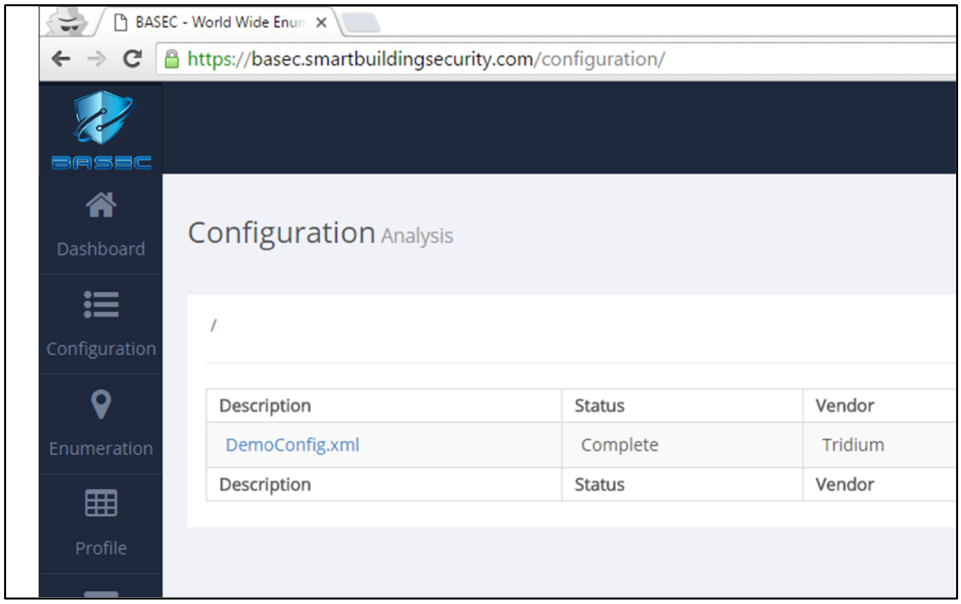

Figure 8. Analysis of Configuration File Complete.

When the hyperlink is clicked, the reporting shows the findings from the analysis. The findings are mapped to selectable criteria and can be updated to reflect desired RMF requirements with an associated risk rating ranging from Critical, High, Medium and Low. The example findings in Figure 9 show identified user names on the system that have no password set.

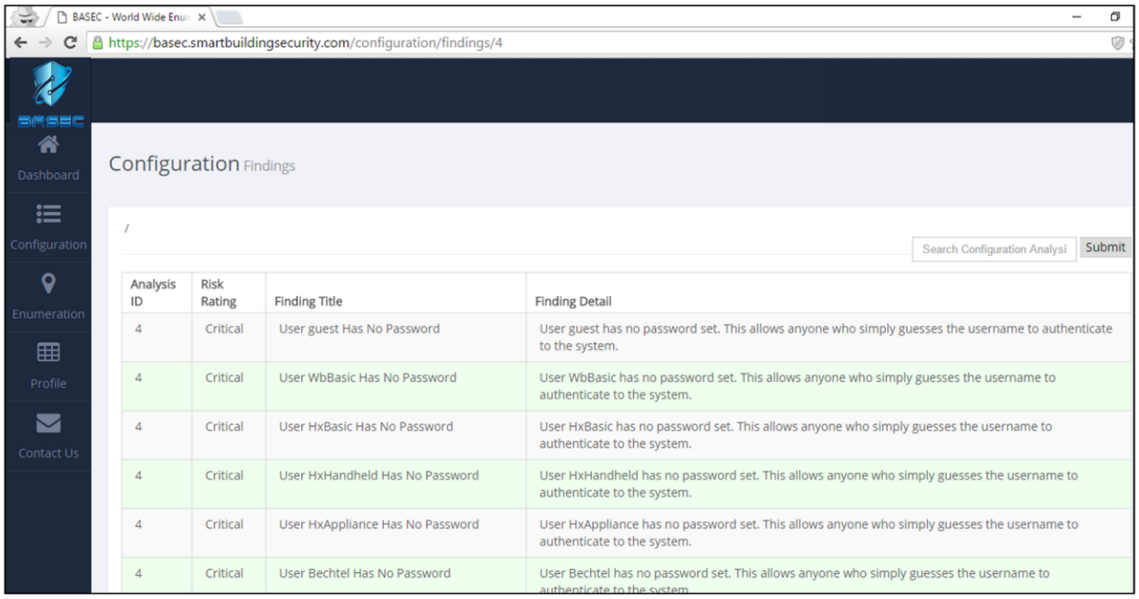

Figure 9. Display of Analysis Results.

BASEC was designed for ease of use and deployment. For implementation, there are no architecture changes required for the building automation systems. Configuration files are uploaded to the BASEC analysis engine and evaluation is accomplished via BASEC processing. As a result, the system-level configuration can be analyzed without risk to impacting system operations.

2.3 ANALYSIS ENGINE

Throughout the ESTCP project, QED Secure Solutions evaluated the analysis engine for the vendors encountered on the DoD installations. When necessary, enhancements to the analysis engine were made to provide coverage for new systems. The BASEC engine now has full analysis support for Tridium Niagara, Johnson Controls Metasys, Siemens Apogee and Automated Logic WebCTRL. Note that these vendors make up the significant majority of facility energy control systems on military installations.

The flow diagram in Figure 10 shows a high-level representation of the analysis engine. When a configuration file is uploaded to BASEC, the analysis engine identifies key indicators within the file to determine the associated vendor. Once the vendor is determined, the analysis engine applies the associated algorithm to unpack the configuration file. Note that each vendor implements their own unique compilation techniques. As such, the reverse engineering required to unpack the configuration files is unique to each specific vendor (and in some instances firmware/software versions). Once a BASEC module is implemented for the file type, however, it is applicable for all future instances of that vendor's same configuration file types. This automated capability to unpack configuration files allows for the rapid evaluation and ability to readily scale.

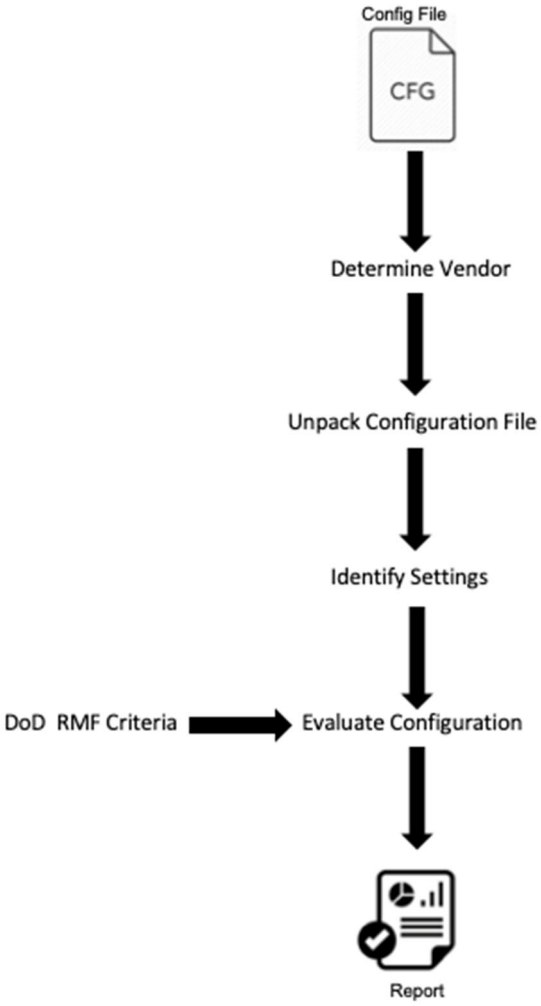

Figure 10. Flow Diagram for BASEC Analysis Engine.

The next step in the analysis is to identify the settings in the unpacked configuration file. Each vendor h*as various settings that users can configure. Example settings include creation of user accounts, setting of passwords, user account roles, account lockout features, security certificates, system services, protocols, audit logs, remote connectivity, version number, patch status, and system management.*

After identifying the set configurations, the analysis engine evaluates the configuration against pre-defined standards (e.g., DoD RMF criteria). The evaluation determines if each setting is in compliance, is not in compliance, and the severity of the finding if not in compliance. Note that the severity and criteria can be configured to meet individual organizational needs, if desired. For ESTCP demonstrations, the criteria were mapped to common DoD RMF criteria and vendor hardening guides. The BASEC reporting displays the specific weaknesses associated with individual configuration files (e.g., weak passwords, missing security patches, insecure services, insecure default configurations and weak/insecure protocols in use) mapped to the severity rating.

2.4 BASEC USABILITY

In addition to functional enhancements, QED Secure Solutions extended the BASEC graphical user interface. The enhanced web-based management interface is designed to provide end-users a secure means to examine device configurations, audit system settings, define security policies, and obtain reporting from anywhere in the world.

Once an individual user authenticates to the BASEC portal, they have a range of options now available for management of services. The user dashboard is shown in Figure 11. From here, the user can examine findings of individual reports, navigate to historical reports, examine ratings for specific facilities and examine overall findings. Access control management has also been built into the enhanced BASEC portal, allowing administrative control over who can access specific findings. Additionally, the Vendor Risk Scorecard maintains a running list of critical findings associated with each vendor.

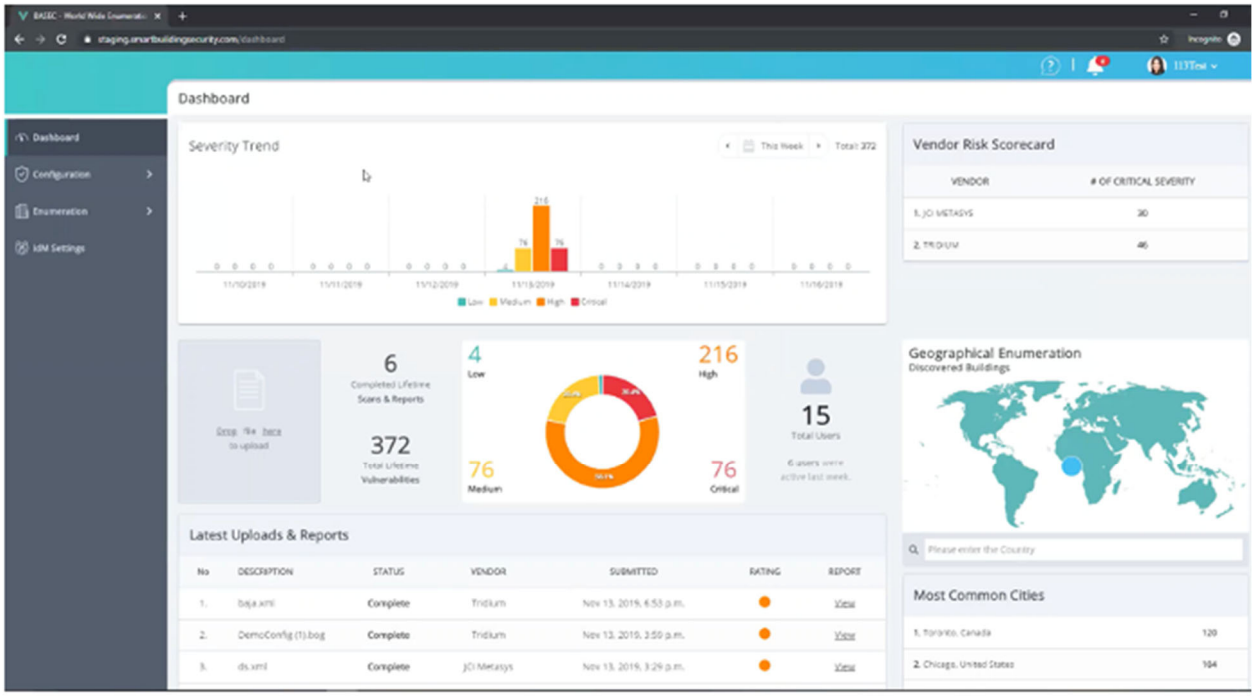

Figure 11. BASEC User Dashboard.

As shown in Figure 12 and Figure 13, the reporting has also been enhanced, to provide more features and easier navigation for the user.

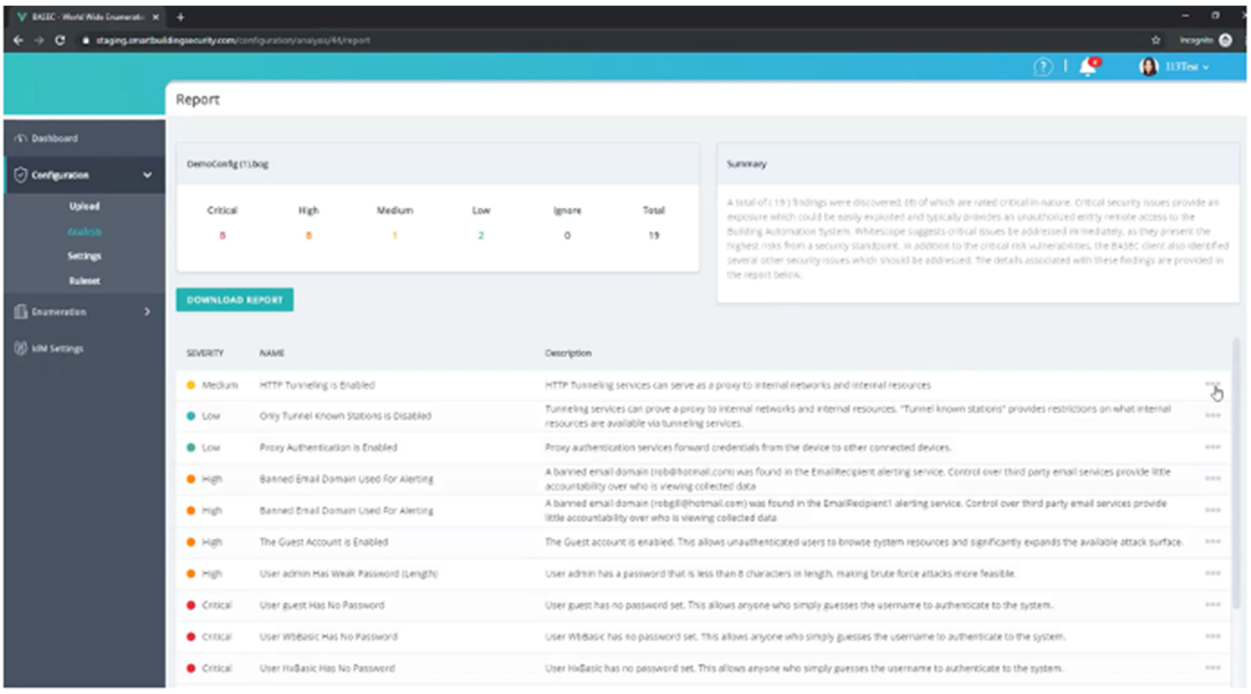

Figure 12. BASEC Reporting Features.

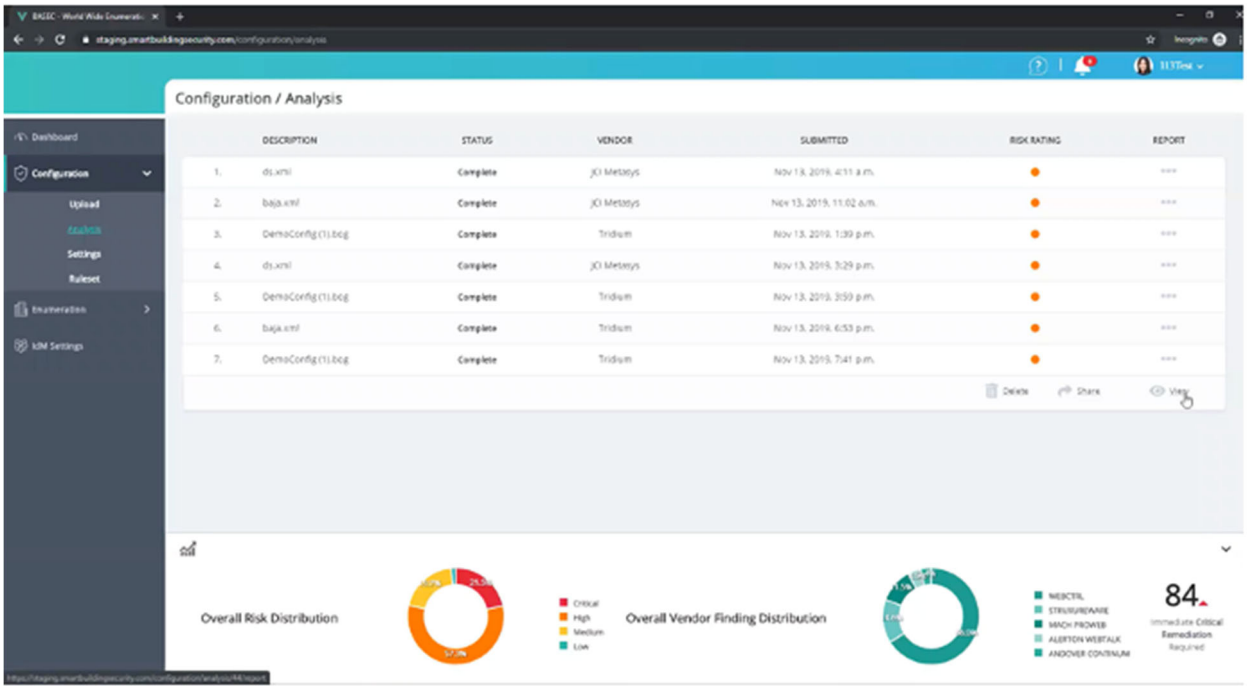

Figure 13. Additional BASEC Reporting Features.

In additional to a web view of the findings, individual reports can be downloaded as a .pdf file, as shown in Figure 14. The BASEC reporting displays the specific weaknesses associated with individual configuration files mapped to the severity rating. Note that the capability of downloading the report to a .pdf was based on user feedback to provide the ability to send reports to third-parties and facilitates inclusion into formal reporting.

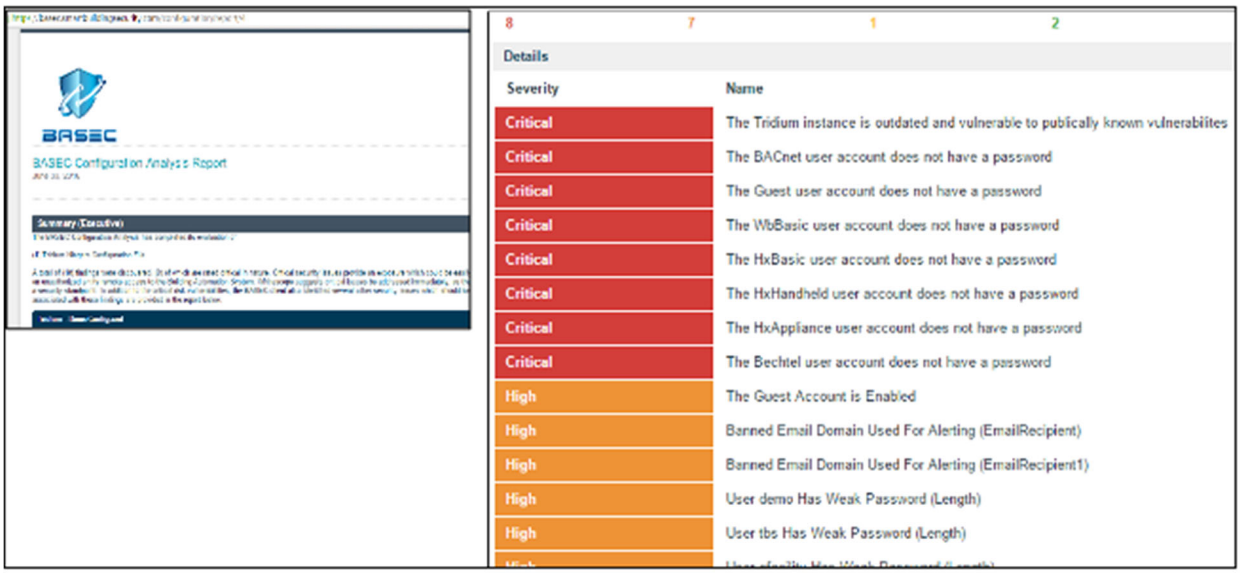

Figure 14. BASEC Standalone Report.

The other major enhancement is the deployment of BASEC entirely in the GovCloud. The current provider is Amazon AWS GovCloud. The Amazon AWS GovCloud (US) provides a platform to implement secure cloud solutions that comply with the DoD Cloud Computing Security Requirements Guide for Impact Levels 2, 4 and 5. Additionally, the AWS GovCloud platform meets the criteria set forth in: the Department of Justice Criminal Justice Information Systems Security Policy; U.S. International Traffic in Arms Regulations; Export Administration Regulations; FIPS 140-2; IRS-1075; and other compliance regimes. BASEC currently meets DoD Impact Level 4. QED Secure Solutions has undergone a series of audits by a qualified third-party auditor to determine whether BASEC meets the technical criteria for ATO and eMass entry. BASEC has met all the technical criteria evaluated by the third party and has implemented numerous defense-in-depth cybersecurity measures to protect the BASEC service.

3.0 ESTCP DEMONSTRATION FINDINGS

For the ESTCP demonstration, QED Secure Solutions deployed BASEC on six military installations during a two-year period, identifying the configuration settings of building automation system devices across multiple vendors and multiple buildings. Findings from the demonstration support BASEC's ability to:

- Automate and track RMF compliance
- Incorporate BASEC with current DoD network solutions
- Implement with no architecture changes required
- Generate automated reports that identify compliant/non-compliant configuration details
- Show ease of deployment design for use by installation/facility control engineers
- Accomplish compliance auditing in seconds
- Identify savings in cost associated with manual evaluation versus the BASEC automated evaluation capability for obtaining ATO

The ESTCP demonstration findings associated with installation evaluations, training, and performance objectives show the effectiveness and utility of leveraging BASEC capabilities for evaluating building automation system configurations.

3.1 INSTALLATION EVALUATION

BASEC was evaluated on six military installations for 35 different building automation systems against four system vendors. The installations consisted of Air Force, Army and Navy facilities. Note that for security considerations, the specific installations are not identified in this report.

The four vendors consisted of Tridium Niagara (40%), Johnson Controls Metasys (25%), Siemens Apogee (20%), and Automated Logic WebCTRL (15%). Four installations implemented one specific vendor, and two installations implemented a mixture of two vendors. The specific facilities examined were associated with core mission/operational functions for the installations.

For evaluation, the team traveled to an installation and met with the designated control system engineer. The control system engineer provided configuration files for the designated facilities. Note that the selection of which facilities to evaluate were determined by the facility engineer and in collaboration with assessment teams. Example building infrastructure included military hospitals, operations control centers, network control centers, military aviation facilities, headquarters facilities, maintenance facilities, and flight simulation facilities. The BASEC reports were provided to the facility engineer upon completion to help them implement more secure configurations in support of hardening the installation infrastructure.

The overall deficiencies in compliance with established RMF security controls included the following:

- Default configurations (78%)
- Weak/default passwords (85%)
- Unmanaged/outdated user accounts (90%)
- Improper user permissions (100%)
- Unpatched systems (92%)
- Internet exposure (12%)
- Unnecessary protocols/services (85%)
- Lack of proper audit logs (92%)

Interestingly, every building automation configuration file examined had at least one deficiency resulting from a failure to implement proper RMF security controls. Default configurations and lack of standard cyber security practices leave DoD facility energy control systems susceptible to cyber-based attacks. Additionally, a trend was identified such that 80% of deployments across the installation used the same baseline configuration.

Summary (Executive)

The BASEC Configuration Analysis has completed its evaluation of:

(1) Tridium Configuration File

A total of (34) findings were discovered, (3) of which are rated critical in nature. Critical security issues provide an exposure which could be easily exploited and typically provides an unauthorized entity remote access to the Building Automation System. Whitescope suggests critical issues be addressed immediately, as they present the highest risks from a security standpoint. In addition to the critical risk vulnerabilities, the BASEC client also identified several other security issues which should be addressed. The details associated with these findings are provided in the report below.

Tridium - config.bog (Anonymous API)

Summary

Critical	High	Medium	Low	Info	Total
3	0	17	14	0	34

Details

Severity	Name
Critical	User Account1 (superuser) Has No Password
Critical	User Account2 Has No Password
Critical	User Account3 Has No Password
Medium	Auto Logoff Is Disabled For Account Account1 (web_WebProfileConfig)
Medium	Auto Logoff Is Disabled For Account Account2 (web_WebProfileConfig)
Medium	Auto Logoff Is Disabled For Account Account3 (web_WebProfileConfig)
Medium	Auto Logoff Is Disabled For Account Account4 (web_WebProfileConfig)
Medium	Auto Logoff Is Disabled For Account Account5 (web_WebProfileConfig)
Medium	Auto Logoff Is Disabled For Account Account6 (web_WebProfileConfig)
Medium	Auto Logoff Is Disabled For Account Account7 (web_WebProfileConfig)
Medium	Auto Logoff Is Disabled For Account Account8 (web_WebProfileConfig)
Medium	Auto Logoff Is Disabled For Account Account9 (web_WebProfileConfig)
Medium	Auto Logoff Is Disabled For Account Account10 (web_WebProfileConfig)
Medium	Auto Logoff Period Is Greater Than 1 Hour For User Account1 (135 Min In WebProfileConfig)
Medium	Auto Logoff Period Is Greater Than 1 Hour For User Account2 (75 Min In WebProfileConfig)
Medium	Auto Logoff Period Is Greater Than 1 Hour For User Account3 (75 Min In WebProfileConfig)
Medium	Auto Logoff Period Is Greater Than 1 Hour For User Account4 (75 Min In MobileWebProfileConfig)
Medium	Auto Logoff Period Is Greater Than 1 Hour For User Account5 (75 Min In WebProfileConfig)
Medium	Auto Logoff Period Is Greater Than 1 Hour For User Account6 (75 Min In WebProfileConfig)
Medium	Auto Logoff Period Is Greater Than 1 Hour For User Account7 (75 Min In WebProfileConfig)
Low	Only Tunnel Known Stations Is Disabled
Low	Auto Logoff Period Is Greater Than 30 Minutes For User Account1 (60 Min In WebProfileConfig)
Low	Auto Logoff Period Is Greater Than 30 Minutes For User Account2 (60 Min In WebProfileConfig)
Low	Auto Logoff Period Is Greater Than 30 Minutes For User Account3 (60 Min In WebProfileConfig)
Low	Auto Logoff Period Is Greater Than 30 Minutes For User Account4 (60 Min In WebProfileConfig)
Low	Auto Logoff Period Is Greater Than 30 Minutes For User Account5 (60 Min In WebProfileConfig)
Low	Auto Logoff Period Is Greater Than 30 Minutes For User Account6 (60 Min In WebProfileConfig)
Low	Auto Logoff Period Is Greater Than 30 Minutes For User Account7 (60 Min In WebProfileConfig)
Low	Auto Logoff Period Is Greater Than 30 Minutes For User Account8 (60 Min In WebProfileConfig)
Low	Auto Logoff Period Is Greater Than 30 Minutes For User Account9 (45mins in MobileWebProfileConfig)
Low	Auto Logoff Period Is Greater Than 30 Minutes For User Account10 (45mins in MobileWebProfileConfig)
Low	Auto Logoff Period Is Greater Than 30 Minutes For User Account11 (45mins in MobileWebProfileConfig)
Low	Auto Logoff Period Is Greater Than 30 Minutes For User Account12 (45mins in MobileWebProfileConfig)
Low	Auto Logoff Period Is Greater Than 30 Minutes For User Account13 (45mins in MobileWebProfileConfig)

Figure 15. Example Report from Building Automation System.

The implications of the findings reveal an overall deficiency in building automation RMF security controls. Additionally, a lack of standard policy enforcement was identified during the demonstration. Consider, for example, the report for one of the building automation systems in Figure 15. The findings reveal a superuser account with no password as well as varying auto-logoff periods for different users. Note that in this example, there were 13 different user accounts identified, with multiple accounts associated with individuals that no longer worked at the installation.

Another identified concern was Internet facing building automation systems. BASEC identified building automation systems that were configured with public IP addresses. As a result, the associated direct interfacing building automation system controller could be accessed from the Internet. Figure 16 shows an example building automation system identified during the demonstration for an Air Force Base that was reachable via the Internet. Note that IP address and specific installation has been redacted. Additionally, these findings were presented to the appropriate organizations, and the exposed facilities have been subsequently removed from Internet access.

Figure 16. Internet Facing Air Force Building Automation System.

BASEC capabilities were lauded by the engineers involved in the ESTCP demonstration. In some instances, the evaluation was the first look into the security posture of the associated building automation systems. In other instances, BASEC was deployed with assessment teams supporting NDAA 1650 efforts. The findings demonstrate the utility of using an automated tool to aid in the evaluation of configurations for RMF security control compliance.

3.2 TRAINING

In cooperation with Army Cyber (ARCYBER) Command and Idaho National Labs (INL), QED Secure Solutions provided facility energy control system assessment training to DoD personnel. During the ESTCP demonstration period, QED Secure Solutions taught seven classes at INL facilities to Army, Navy, Air Force, Space Force, and Army Corps of Engineers personnel with a wide-range of background experience (cyber specialists to program managers).

The course was intended for U.S. military and/or Department of Defense personnel assigned to conduct cyber vulnerability evaluations of DOD critical infrastructure.

During the BASEC training module, QED Secure Solutions demonstrated the manual process of evaluating building automation systems. As noted in the course, such evaluation processes require extensive reverse engineering and system-level knowledge. Alternatively, the students were taught how to use BASEC for automatically obtaining the same results. The training block for teaching how to use BASEC was one hour in duration. Upon completion of the training block, students demonstrated proficiency using BASEC during a capstone exercise. On average, students were able to effectively identify the deficiencies in building automation system configurations in less than five minutes using BASEC.

The training environment demonstrated the ability to rapidly teach end users how to deploy BASEC. Additionally, course critiques identified over 95% of students comfortable using BASEC for evaluating building automation system compliance. Finally, over 90% of students identified specific gaps in current capabilities that BASEC can help address.

3.3 PERFORMANCE OBJECTIVES

3.3.1 Methods for Assessing Performance

BASEC was evaluated for the ability to identify and examine the configuration of multiple vendor devices that were deployed in multiple building infrastructures and the timeframe required for the evaluation. The type of vendor device or building infrastructure should not impact BASEC's ability to identify configuration deficiencies. At no time should BASEC impact the functional operation of the building automation system. The web-based interface management capability should provide monitoring and reporting of configuration evaluations.

The configuration files of DoD installations were compared against established standards to identify weak configurations and RMF security controls. QED Secure Solutions evaluated BASEC's ability to identify and report deficient system configurations. The time required for evaluation was evaluated and compared against standard evaluation techniques.

3.3.2 Technical and Performance Objectives

The technical and performance objectives for the onsite demonstration include:

- Accurate identification of system device configurations
- Accurate identification of weak configurations
- Ability to identify changes to configurations
- Ability to produce reports
- Functionality of the web-based interface management

BASEC demonstrated the ability to meet the technical and performance objectives for the ESTCP onsite demonstration. For the evaluated buildings, BASEC successfully identified 100% of system device configurations, weak configurations, and changes to configurations. BASEC also produced valid reports based on findings and demonstrated a functional web-based interface management.

The following performance metrics demonstrate the effectiveness of deploying BASEC:

- Average time to perform automated analysis (50 seconds)
- Number of vendors (4)
- Average time to train personnel to be proficient using BASEC (1 hour)
- Coverage of assets (100%)

BASEC was able to transform a manual process of evaluating system configurations that traditionally takes weeks to less than a minute. BASEC also demonstrated effective coverage of the four major building automation vendors that were observed at the six military installations.

3.3.3 NDAA 1650 Findings

The 2017 Congressional NDAA 1650 mandate specified the evaluation of cyber vulnerabilities of Department of Defense critical infrastructure. As part of the evaluation, Air Force and Army assessments teams deployed BASEC to examine configurations of installation building automation systems.

In support of the BASEC ESTCP demonstration, QED Secure Solutions extrapolated savings from the deployment of BASEC in support of NDAA 1650. Table 1 shows results of comparison between manual evaluation process and using BASEC. The BASEC evaluation consisted of one installation engineer that was trained on BASEC. The traditional assessment consisted of four cyber operators and one installation engineer.

Table 1. Comparison Between BASEC and Traditional Assessment.

Measurement	BASEC	Traditional Assessment
Total time to complete assessment	4 hours*	300 hours
Total time for Reporting	15 mins	40 hours
Coverage of assets	100%	75%
Findings	24 Specific Findings	4 General Recommendations
Time for follow-up to validate fixes	30 mins	Not Accomplished

*Time included coordination of access to system files

The findings readily show the benefits BASEC provides in support of evaluating building automation system configurations.

3.3.4 Savings Realization

Findings from the BASEC ESTCP demonstration indicate potential substantial savings to the DoD, while enhancing capabilities. BASEC savings realization include:

- Training. Fully trained on BASEC in one hour vs. assessments requiring cyber operators that must go through extensive training
- Personnel Requirements. Designed for use by installation/facility control engineers
- Time for Assessment. System configuration analyzed in seconds vs. weeks
- Analysis. Consistent findings mapped to defined requirements
- Operational Impacts. Significant potential cost savings with enhanced efficiency and granular results

Manual assessments can cost upwards of $35k and require extensive coordination, allocation of resources and potential disruption to daily operations. The BASEC solution reduces the time and cost of evaluating building automation systems and has the potential for significant cost savings compared against the current state of manual team assessments. Direct cost savings are realized through minimizing the amount of training required to complete compliance auditing, reducing the number of personnel onsite to perform the auditing, greatly reducing the time to complete analysis, providing consistent and timely results, and reducing major impacts to operations.

4.0 TRANSITION EFFORTS AND NEXT STEPS

QED Secure Solutions presented BASEC capabilities and findings at multiple venues throughout the ESTCP demonstration. The following list highlights presentations of BASEC:

- 2018 SERDP - ESTCP Symposium, Enhancing DoD's Mission Effectiveness
- 2019 SERDP - ESTCP Symposium, Poster Session
- SERDP & ESTCP Webinar Series, Securing DoD Control Systems and Infrastructure from Cyber Threats
- Mission Assurance, Control System Cyber Mitigations & MOSAICS Workshop (Supporting the Office of the Principal Cyber Advisor to SECDEF)
- Installation Energy and Water Program Area, Technical Session on Control System Cybersecurity Technologies (Scheduled)

The presentations allowed QED Secure Solutions to highlight the advancements afforded through the ESTCP project. Additionally, QED Secure Solutions connected with multiple individuals from various organizations that had interest in the BASEC capabilities. QED Secure Solutions provisioned a multitude of BASEC accounts to help DoD organizations facilitate RMF compliance, to include Naval Facilities Engineering Command (NAVFAC), Marine Corps Installations Command (MCICOM), and ARCYBER.

QED Secure Solutions successfully demonstrated BASEC capabilities for identifying building automation system configuration shortfalls and mapping them to RMF requirements. The Service components QED Secure Solutions worked with during the ESTCP demonstration identified opportunities to extend the BASEC tool. Indeed, NAVFAC and Army Materiel Command specifically called out BASEC as a tool they believe can help address significant gaps in mission assurance and cyber hygiene across installation energy/water cybersecurity requirements. Both organizations have provided support for potential follow-on studies to extend BASEC as an enterprise level solution.

5.0 CONCLUSIONS

Current solutions for examining the configuration posture of building automation systems tend to focus on manual assessment capabilities. Although helpful for examining specific installations, these methods do not scale and are not sufficient for meeting the holistic requirements across DoD installations. BASEC provides an innovative solution that can help standardize, enforce, and secure DoD building energy systems across all potential vendors and installations. The ease of deployment is designed for use by installation/facility control engineers and provides detailed reporting without the requirement for advanced cyber security skill sets.

BASEC was evaluated on six military installations, covering 35 unique buildings, and four different vendors. The ESTCP project demonstrated the ability to automate RMF compliance, incorporate BASEC with current DoD network solutions, generate automated reports, and accomplish auditing within seconds. Additionally, over 150 military and government personnel were trained on implementing BASEC supporting RMF auditing capabilities and congressionally mandated assessment requirements. The BASEC solution demonstrated the potential to reduce the time and cost of achieving compliance and affords the DoD opportunity for significant cost savings compared to the current state of manual team assessments.

BASEC provides a solution to evaluate the configuration and cyber security standards for military installation buildings automation systems. BASEC can be implemented at any point during the building energy system lifecycle, providing a means to evaluate and implement a consistent, scalable process for legacy and new system requirements. BASEC affords significant potential in meeting further deficiencies for supporting cybersecurity of facility building and energy infrastructure. Future research efforts include evaluation of BASEC as an enterprise solution that scales to every DoD installation, incorporating continuous monitoring of system configurations, extending BASEC to cover facility energy/water devices, and automating associated cyber hygiene to help strengthen DoD posture against cyber-based attacks targeting military installation critical infrastructure.