ESTCP

FINAL REPORT

Energy and Water Projects

Baseline Automated Security Enumeration and Configuration (BASEC)

Jonathan Butts
Billy Rios
QED Secure Solutions

May 2023

ESTCP Project EW20-7198

REPORT DOCUMENTATION PAGE	Form Approved OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)* 31-05-2023	**2. REPORT TYPE** ESTCP Final Report	**3. DATES COVERED** *(From - To)* 8/9/2021 - 8/8/2024

4. TITLE AND SUBTITLE
Baseline Automated Security Enumeration and Configuration

5a. CONTRACT NUMBER
21-C-0053

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
EW20-7198

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
ESTCP Program Office
4800 Mark Center Drive Suite 17D08
Alexandria, VA 22350-3600

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

11. SPONSOR/MONITOR'S REPORT NUMBER(S)
EW20-7198

12. DISTRIBUTION / AVAILABILITY STATEMENT
DISTRIBUTION STATEMENT A. Approved for public release: distribution unlimited

13. SUPPLEMENTARY NOTES

BASEC provides a scalable, enterprise solution intended to integrate specifically with mission assurance efforts and the automation of cyber hygiene assessments. The current method of evaluating installation energy/water control systems cybersecurity relies on manual evaluations and requires assessment teams, follow-on analysis, and specialized skillsets. Unfortunately, such evaluations only show a snapshot in time of the security posture, and the costs for sustaining an effective Service-wide program in this manner are expensive and unrealistic. The BASEC solution automates the analysis of device-level configuration settings for installation energy/water control systems, identifies vulnerabilities in configurations and provides an effective means for maintaining asset inventory at the Service level.

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

16. SECURITY 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)* 214-489-7767

FINAL REPORT
Project: EW20-7198

TABLE OF CONTENTS

Page

LIST OF FIGURES

Page

LIST OF TABLES

Page

ACRONYMS AND ABBREVIATIONS

AFCEC	Air Force Civil Engineer Center
AMC	Army Materiel Command
BASEC	Building Automation System Enumeration and Configuration
CE	Civil Engineer
COINE	Community of Interest Network Enclave
CVE	Common Vulnerabilities and Exposures
DoD	Department of Defense
ESTCP	Environmental Security Technology Certification Program
FRCS	Facility Related Control System
MCICOM	Marine Corps Installations Command
NAVFAC	Naval Facilities Engineering Command
NDAA	National Defense Authorization Act
RMF	Risk Management Framework

ABSTRACT

Energy and water 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 installation energy/water control systems. The primary objective of this Environmental Security Technology Certification Program (ESTCP) effort is to demonstrate and validate the use of the Baseline Automated Security Enumeration and Configuration (BASEC) tool to help strengthen DoD posture against cyber-based attacks targeting military installation critical infrastructure. BASEC provides a scalable, enterprise solution intended to integrate specifically with mission assurance efforts and the automation of cyber hygiene assessments. The current method of evaluating installation energy/water control systems cybersecurity relies on manual evaluations and requires assessment teams, follow-on analysis, and specialized skillsets. Unfortunately, such evaluations only show a snapshot in time of the security posture, and the costs for sustaining an effective Service-wide program in this manner are expensive and unrealistic.

The BASEC solution automates the analysis of device-level configuration settings for installation energy/water control systems, identifies vulnerabilities in configurations and provides an effective means for maintaining asset inventory at the Service level. The automated process reduces the time and cost associated with traditional manual assessments and readily integrates with mission assurance processes. The enterprise solution also includes capabilities that allow analysis of trend data across the entire Service-level infrastructure, as well as “drill down” features for individual systems. The trend data will help provide leadership awareness and oversight for top security issues encountered.

Demonstration and validation of BASEC for enhancing installation energy/water cybersecurity posture includes identifying baseline control system configurations, evaluating BASEC as an enterprise cybersecurity capability, demonstrating scalability to cover all DoD installation energy/water control systems, and ability to deploy BASEC for mission assurance functions and cyber hygiene assessment teams. The ESTCP effort provides critical support in validating BASEC as a viable tool supporting installation energy/water cybersecurity requirements. As a result, the BASEC capability brings a means to enhance DoD mission effectiveness, support risk analysis, and identify gaps in energy and installation cybersecurity that is vital to supporting warfighter efforts.

EXECUTIVE SUMMARY

INTRODUCTION

The 2017 Congressional National Defense Authorization Act (NDAA) line item 1650 mandated the evaluation of cyber vulnerabilities of Department of Defense (DoD) critical infrastructure — (A) to improve the defense of control systems against cyber attacks; (B) to increase the resilience of military installations against cybersecurity threats; (C) to prevent or mitigate the potential for high-consequence cyber attacks; and (D) to inform future requirements for the development of such control systems [1]. Service components completed the required evaluation of installation critical infrastructure; however, the process relied extensively on manual, one-time assessments. Additionally, the execution efforts focused on a small sampling of DoD installations to establish the baseline cybersecurity posture.

Although effective for (and necessary to) identifying the overall cyber security posture of DoD installation critical infrastructure, the NDAA 1650 findings provide a point-in-time snapshot of current cybersecurity defense. Additionally, the associated manual assessments do not scale, are expensive, do not provide consistent results, and do not allow effective analysis of findings across the various installations. The DoD requires an enterprise solution that automates the continual evaluation of critical infrastructure against established cyber hygiene requirements and integrates with mission assurance objectives.

This ESTCP proposal builds on successes from previous work supported under EW18-5333. QED Secure Solutions (QED), with support via ESTCP funding, evaluated the BASEC tool for effectively examining system configuration vulnerabilities in military installation building automation systems. BASEC demonstrated the ability to perform secure evaluations of system configurations against Risk Management Framework (RMF) requirements, track compliance, deploy the capability, and rapidly accomplish auditing tasks. During the previous ESTCP project, QED worked with various Service component representatives for evaluating BASEC in association with RMF compliance. The Service components identified opportunities to extend the BASEC tool to help mitigate gaps in mission assurance capabilities and cyber hygiene. Indeed, the Air Force, Army, Navy and Marine Corps specifically called out BASEC as a tool they believe can help address critical mission assurance and cyber hygiene shortfalls.

All four Service organizations have offered support dedicated to the QED research and development effort funded through the ESTCP proposal to enhance BASEC capabilities that scale and automate installation energy infrastructure cybersecurity. The Air Force Civil Engineer Center (AFCEC), Army Materiel Command (AMC), Naval Facilities Engineering Systems Command (NAVFAC), and Marine Corps Installations Command (MCICOM) all worked with QED to define system requirements, provide access to facilities and configurations, and advise on the ESTCP demonstration efforts.

OBJECTIVES

The primary objective of this ESTCP effort is to demonstrate and validate the use of BASEC as an enterprise solution supporting mission assurance efforts and automation of cyber hygiene capabilities. This demonstration significantly extends the original BASEC capabilities and focuses on an enterprise-wide solution.

The technical objectives are specified by the primary focus areas for the enterprise-level demonstration:

- Ability to scale to DoD-wide coverage
- Provide metrics and trend analysis reporting
- Identify and alert to system modifications and deviations from baseline

The enterprise solution includes demonstration of the BASEC user interface and capabilities that allow analysis of trend data across the entire Service-level infrastructure, as well as "drill down" features for individual systems.

To protect against cyber-based attacks, it is critical that the DoD identify misconfigured and exposed devices that monitor and control energy/water control 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 energy/water control systems. The heart of BASEC is a secure, cloud-based analysis engine that examines and compares submitted configuration and deployment files against established 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 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.

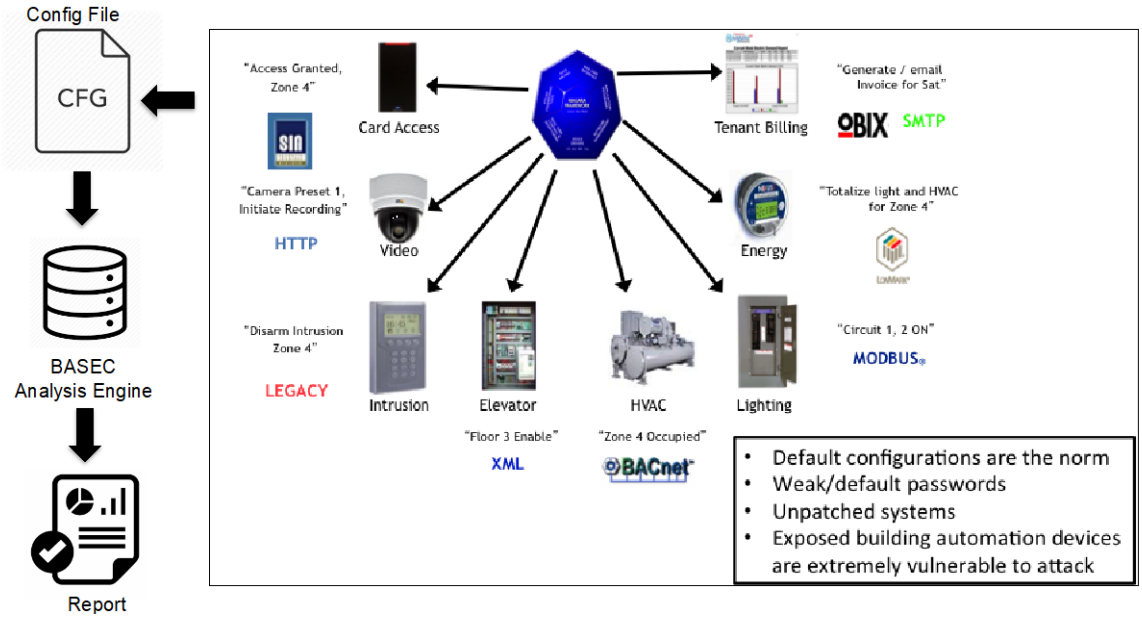

Figure 1. Functional Overview of the BASEC Analysis Process.

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

QED traveled onsite to the installation with AFCEC representatives. Civil Engineer (CE) individuals from the host installation provided copies of the installation configuration files that they store locally on a centrally managed server for each building. QED uploaded the configuration files to the BASEC analysis engine via the user interface. BASEC completed analysis on all 180 configuration files in less than 45 minutes total.

Results of the analysis reveal that the same baseline configuration is deployed to a majority of the controllers. This is not uncommon, as often times CE personnel or system integrators that install the system use a common baseline configuration for all deployments. From a security standpoint, this can be effective if the deployed configuration is hardened. However, the drawback is that if a security weakness exists in one system, then it is present in all systems. As an example, an attacker could probe a relatively innocuous facility to identify weaknesses and develop exploits. The attacker could then leverage that same exploit against a more desirable target on the installation.

From the 180 system evaluated, 34 were found to be in compliance, with no configuration concerns. The remaining 146, or 81% of systems evaluated had one to four identified security concerns rated at a HIGH Critical level.

The first finding in the configuration analysis is that the Guest account has no password. This finding was present on 144 of the 180 systems evaluated. With the Guest account enabled, anyone accessing the controller via a web browser can authenticate using Guest and no password. Once logged in, the Guest account is not restricted in ability to observe and change operating settings. Note that the Tridium Security Guide explicitly recommends disabling Guest accounts.

The second finding in the configuration analysis is that the account BACnet has no password. This finding was present on 37 of the 180 systems evaluated. BACnet is a communications protocol for building automation systems that enables device to device communications. An attacker logging in to the BACnet account has system privileges to observe and modify settings associate with interconnected devices.

The third finding is associated with a created user account. There were 12 systems of the 180 evaluated that had a created user account with no password. Note that the user account was the same username for all twelve systems. An attacker can access the system via a web browser and log in as the user with no password, and assume the authority granted to the user.

The fourth finding in the configuration analysis is that the controllers are running outdated software versions with publicly known vulnerabilities. This finding was present on 145 of the 180 systems evaluated. Published Common Vulnerabilities and Exposures (CVEs) shows that an attacker can bypass intended access restrictions and also allows remote attackers to read sensitive files and consequently execute arbitrary code. Known exploits have been created to execute attacks against these vulnerabilities.

The final finding is associated with the admin user account. One system that was evaluated has an admin user account with no password. An attacker can access the system via a web browser and log in as an administrator with no password and have full control over operations and configuration of the system.

The five findings across 159 of the 180 building control systems that were evaluated had High Critical impact findings. The security concerns are associated with a remote attacker exploiting a weakness that could provide unfettered control of the associated building automation system.

BASEC was able to transform a manual process of evaluating system configurations that traditionally takes weeks to minutes.

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

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 military installations, 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 minimal cyber security management practices or protection mechanisms in place to prevent attacks. Facility 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.

This ESTCP project builds on successes from previous work supported under EW18-5333. QED, with support via ESTCP funding, evaluated the BASEC tool for effectively examining system configuration vulnerabilities in military installation control systems. Through the partnership, QED demonstrated advanced capabilities for the BASEC tool, to include the following goals:

- Demonstrate and validate the use of BASEC to strengthen DoD posture against cyber attacks targeting military installation critical infrastructure
- Identify cybersecurity configuration weaknesses in installation critical infrastructure and support inventory asset tracking compliance
- Implement enterprise solution for Service-level deployment
- Generate automated reporting and metrics to identify compliant/non-compliant security configuration details

AMC, NAVFAC, MCICOM, and AFCEC all dedicated their support to the ESTCP BASEC effort. Indeed, QED hosted monthly sessions with each of the Service representatives to garner valuable insight and feedback to enhance BASEC capabilities. Their support and dedication were invaluable to reaching the level of successes BASEC achieved. Further, AFCEC hosted the onsite demonstration and execution as well as incorporated BAESC into CE professional control system cybersecurity training required for all enlisted 7-level personnel.

1.1 BACKGROUND

Critical infrastructure on military installations are prime targets for adversary attacks. Threats to installation energy/water control systems have been exacerbated by the trend to interconnect management and monitoring capabilities through networking technologies. A cyber-based attack on one of these systems could have potentially devastating consequences—extending from negative impacts on mission effectiveness to safety of personnel. Indeed, the DoD relies on the proper operations of installation critical infrastructure to achieve mission objectives.

To combat threats to military installation, the DoD has defined a strategy through to provide increased visibility and identify trends affecting mission-essential functions across Services and installations. Mission assurance is an integrative framework and a process to protect or ensure the continued function and resilience of military capabilities and assets, to include military installation critical infrastructure (e.g., installation energy/water control systems) [2].

Mission assurance execution has historically been accomplished in an uncoordinated fashion that often resulted in duplicative programs and left critical risks unmitigated [3]. Service components, however, are implementing comprehensive programs and pioneering initiatives to address the threats, to include enforcement of cyber hygiene for military installation critical infrastructure. Such efforts require tools that augment mission assurance efforts, particularly with respect to installation cybersecurity.

This ESTCP effort demonstrates and validates the use of BASEC to help strengthen DoD posture against cyber-based attacks targeting military installation critical infrastructure. BASEC provides a scalable, enterprise solution intended to integrate specifically with Service efforts and the automation of cyber hygiene assessments. The current method of evaluating installation energy/water control systems cybersecurity relies on manual evaluations and requires assessment teams, follow-on analysis, and specialized skill sets. Unfortunately, such evaluations only show a snapshot in time of the security posture, and the costs for sustaining an effective Service-wide program in this manner are expensive and unrealistic. The BASEC solution automates the analysis of device-level configuration settings for installation energy/water control systems and identifies vulnerabilities in configurations. The automated process reduces the time and cost associated with traditional manual assessments and readily integrates with mission assurance processes. The enterprise solution also includes capabilities that allow analysis of trend data across the entire Service-level infrastructure, as well as "drill down" features for individual systems. The trend data will help provide leadership awareness and oversite for top security issues encountered, such as percentage of systems with critical security issues and percentage of systems with insecure configuration settings.

Demonstration and validation of BASEC for enhancing installation energy/water cybersecurity posture includes identifying baseline control system configurations, evaluating BASEC as an enterprise cybersecurity capability, demonstrating scalability to cover all DoD installation energy/water control systems, and ability to deploy BASEC in concert with Service mission assurance efforts. The ESTCP effort provides critical support in validating BASEC as a viable tool supporting installation energy/water cybersecurity requirements. As a result, the BASEC capability brings a means to enhance DoD mission effectiveness, support risk analysis, and identify gaps in energy and installation cybersecurity that is vital to supporting warfighter efforts.

1.2 OBJECTIVE OF THE DEMONSTRATION

The primary objective of this ESTCP effort is to demonstrate and validate the use of BASEC as an enterprise solution supporting mission assurance efforts and automation of cyber hygiene capabilities. This demonstration significantly extends the original BASEC capabilities and focuses on an enterprise-wide solution. Technical objectives are specified by primary focus areas for the enterprise-level demonstration:

- Ability to scale to DoD-wide coverage
- Provide metrics and trend analysis reporting
- Identify and alert to system modifications and deviations from baseline

The enterprise solution includes demonstration of the BASEC user interface and capabilities that allow analysis of trend data across the entire Service-level infrastructure, as well as "drill down" features for individual systems.

1.3 REGULATORY DRIVERS

Government agencies are solidifying efforts to secure national critical infrastructure. Asset management and DoD directives are driving factors for BASEC implementation. Findings from the BASEC analysis align to relevant instructions, guidelines and policies to meet DoD requirements that specify security postures and controls. Considerations for demonstration include:

- 2017 Congressional National Defense Authorization Act, line item 1650
- 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
- UFC 1-300-02

2.0 TECHNOLOGY DESCRIPTION

2.1 TECHNOLOGY OVERVIEW

BASEC provides a scalable means to identify, baseline, and evaluate the cybersecurity configurations for installation energy/water systems. The heart of BASEC is a secure, cloud-based analysis engine that examines and compares submitted configuration and deployment files against established cybersecurity criteria.

Automated facility energy/water systems rely on embedded devices for control and monitoring of system parameters. The system configuration of the devices are stored in configuration files that are set to a default state by vendors and configured during deployment by installation engineer personnel. Typical configuration settings include creation of user accounts, setting of passwords, defining user account roles, specifying account lockout features, implementing security certificates, enabling system services and protocols, establishing audit logs, defining remote connectivity, selecting firmware versions, updating system patches, and setting system-level parameters.

The primary means assessment teams rely on for evaluating device configuration settings is manually intensive. 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. The configuration file contains all possible configuration setting for the destination embedded 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. Note that the actual configuration file is not human readable, and it is not practical to assume an analyst can examine the configuration settings readily by reviewing the configuration file. As such, it is difficult for an analyst to determine the device configuration settings without active system probing or reverse engineering devices settings.

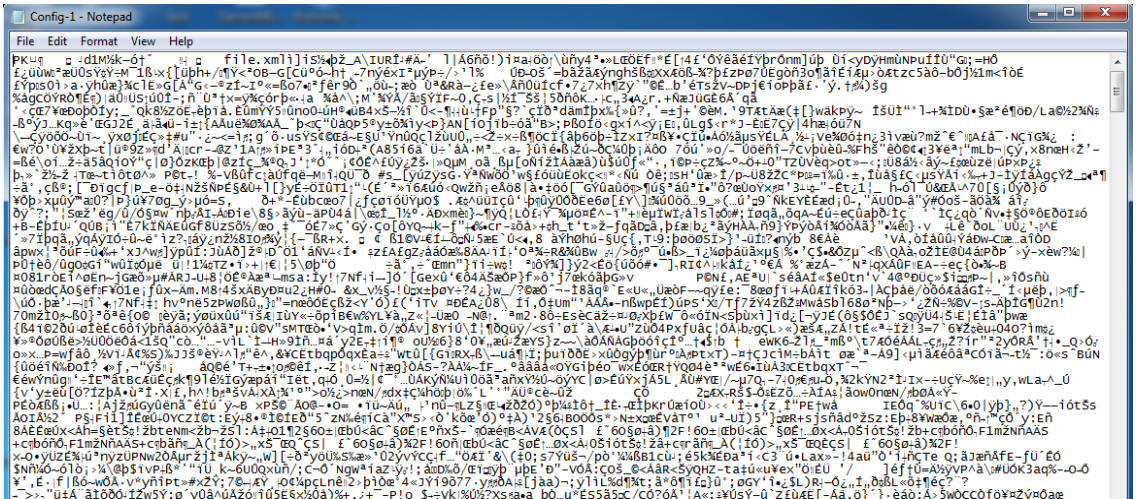

Figure 2. Configuration File from a Tridium Niagara Building Automation Device.

BASEC takes the manually intensive process and automates the analysis to determine device configurations and settings. Figure 3 provides a functional overview of the BASEC analysis process. The installation energy/water device 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.

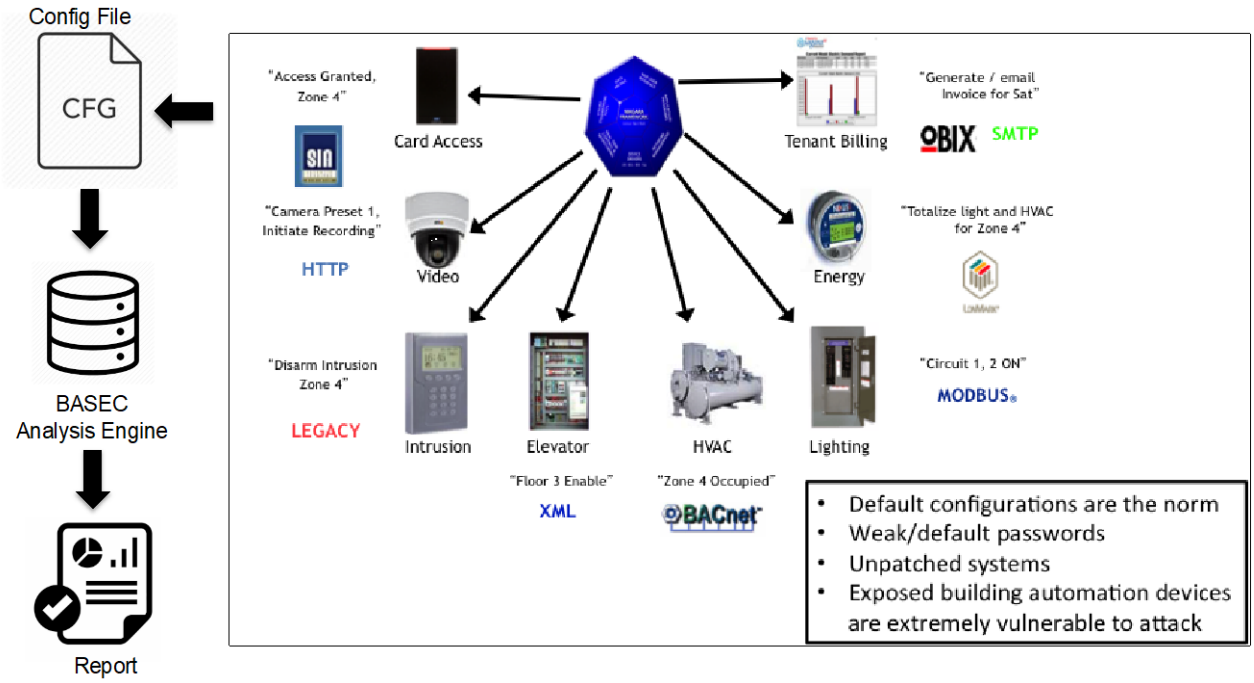

Figure 3. Functional Overview of the BASEC Analysis Process.

The flow diagram in Figure 4 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.

After the analysis engine unpacks the configuration file, the next step is to identify the specific settings. Each vendor has 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.

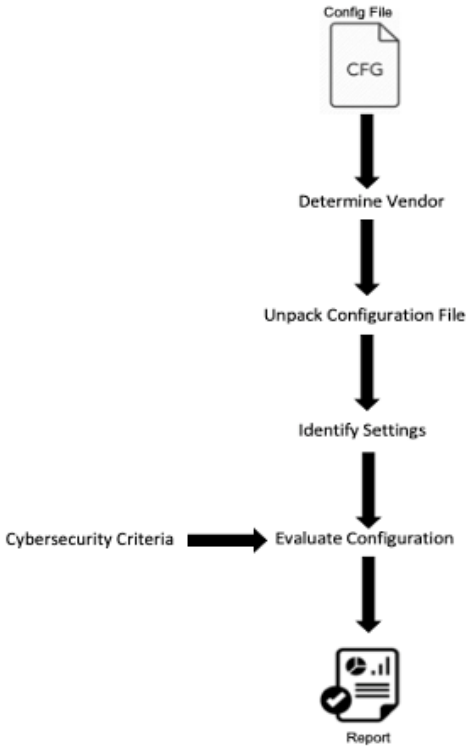

Figure 4. Flow Diagram for BASEC Analysis Engine.

After identifying the set configurations, the analysis engine evaluates the configuration against pre-defined cybersecurity 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. 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.

As shown in Figure 5, BASEC reporting provides the specific weaknesses associated with individual configuration files mapped to the severity rating.

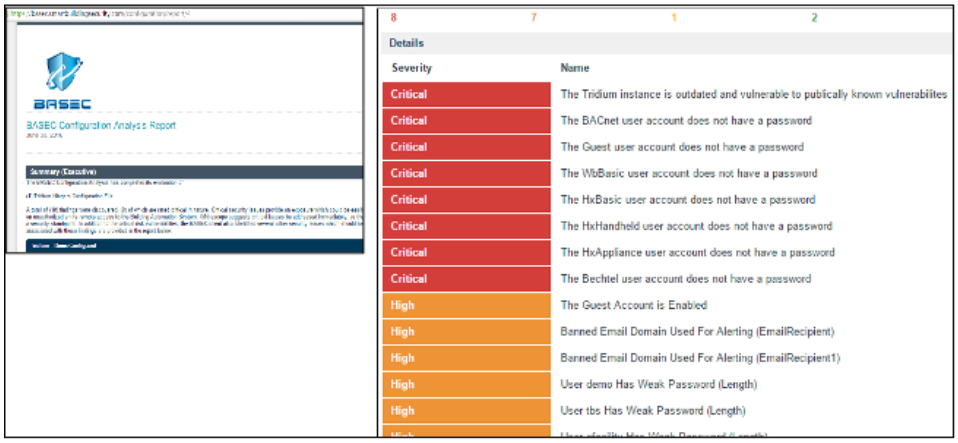

Figure 5. BASEC Reporting Features.

BASEC is currently deployed 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. BASEC currently meets DoD Impact Level 4. QED 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.

2.2 TECHNOLOGY DEVELOPMENT

Technology development for the BASEC demonstration focused on an enterprise solution. Enhancements include user dashboard, hierarchical access control, uploading of device configuration files,

Figure 6 shows a user dashboard after logging in. Each user dashboard displays the associated information based on the varying categories within the span of responsibility for the individual user. The findings severity at the top shows a quick look at the total number of findings based on criticality over the selected time period. A vendor risk scorecard is provided that associates the number of critical findings tied to specific vendors. The POC scorecard provides the same information but tied to designated representatives that are under the user's scope of authority. Top 10 findings area shows the ranked list of deficiencies identified across all evaluated devices. Critical vulnerabilities by base shows the number of identified critical findings by installation. The complaint/non-compliant buildings show a representative in a pie chart for all installations under the span of control for the user. The user can navigate through the various content using the left menu selections. Note that generic information is provided in this report; any specific data related to findings has been redacted.

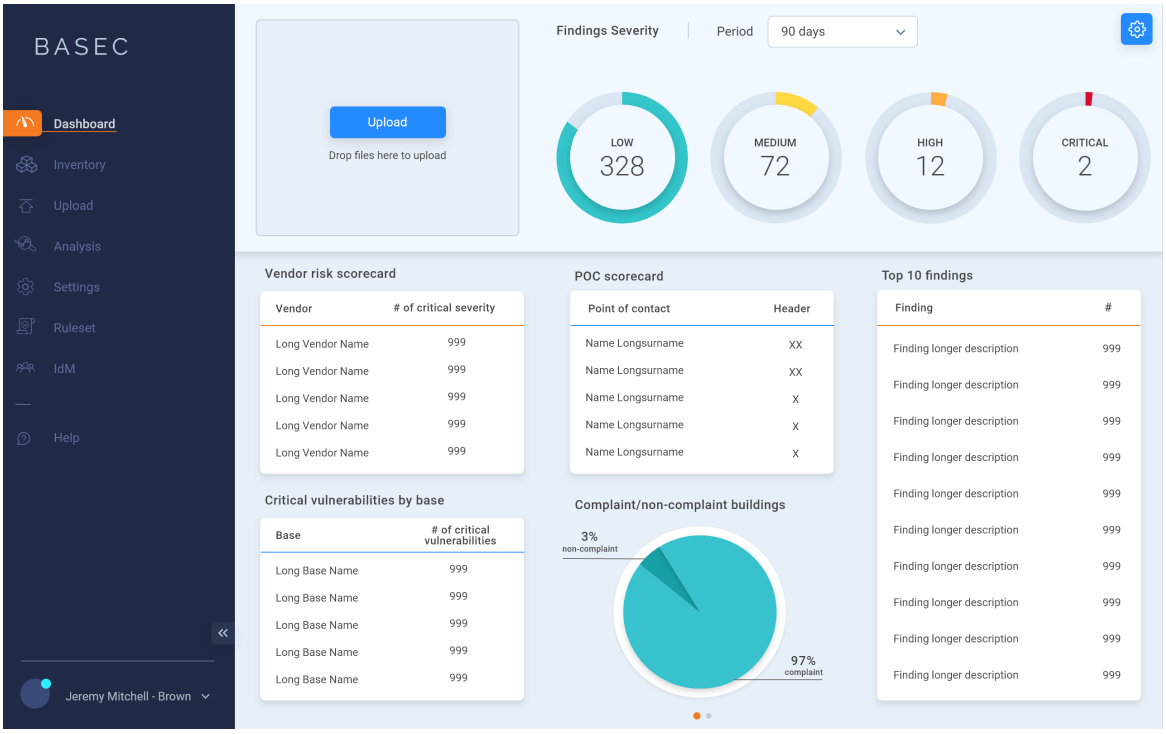

Figure 6. BASEC User Dashboard.

As shown in Figure 7, to upload a new configuration for a device the user can click on the Upload link on the left menu or drag and drop the configuration file to the Upload section on the dashboard.

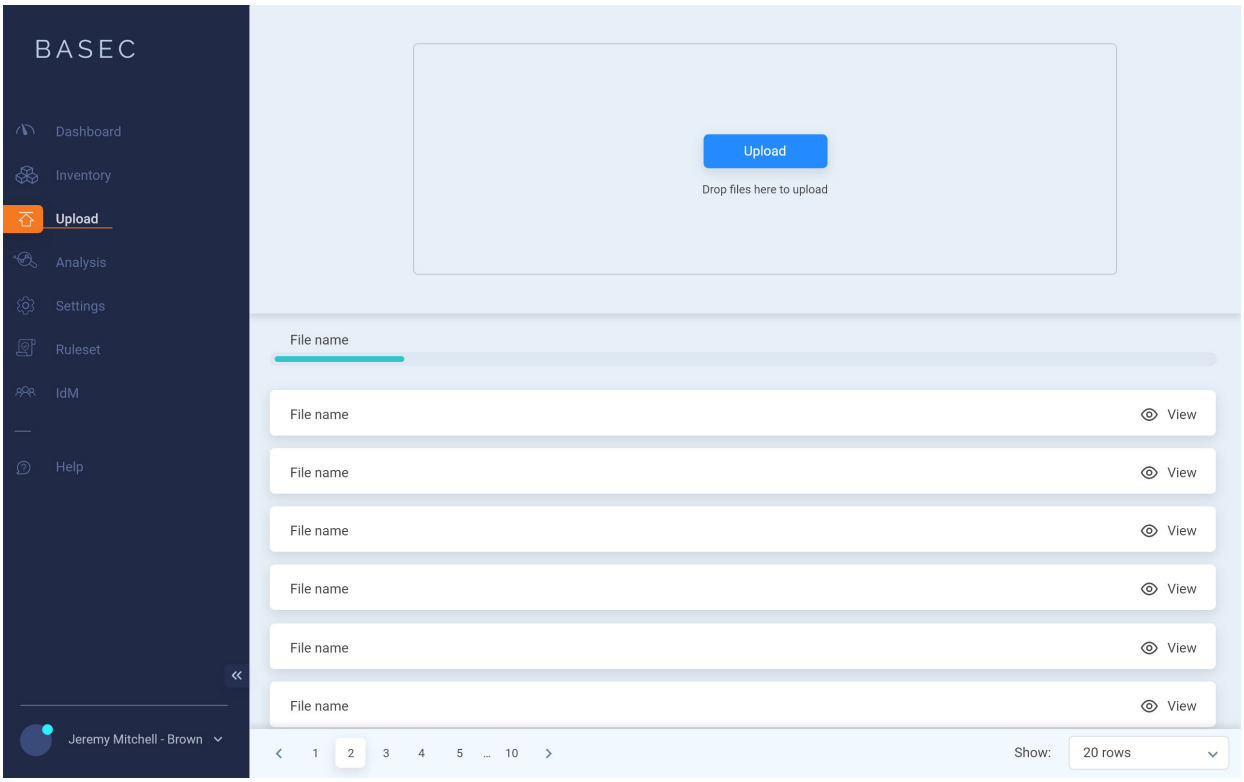

Figure 7. Configuration File Upload.

Once the file is selected or dropped in the Upload field, a menu pop requests details for the specified configuration file, as shown in Figure 8. Details include a device name, Report Date, Building Number, Point of Contact, Facility Related Control System (FRCS) Type, Nomenclature, Region/Major Command, Organization and eMASS ID if one is available. The drop-down fields allow consistency for the fields that aid in inventory management. The specified fields were identified and included at the direction of the Service representatives. Once the information is complete, the automatic analysis initiates to examine the configuration settings.

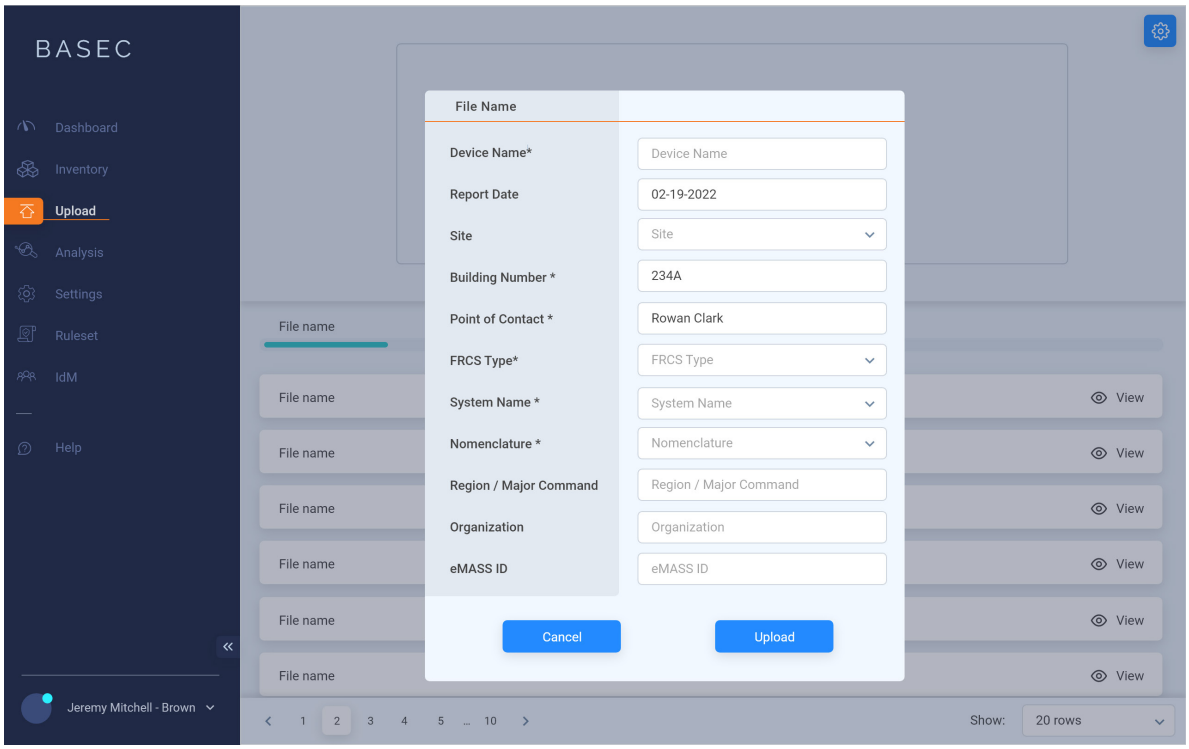

Figure 8. Configuration File Details.

Results can be examined in the Analysis section as shown in Figure 9. The list and details for each uploaded configuration file are presented to the user.

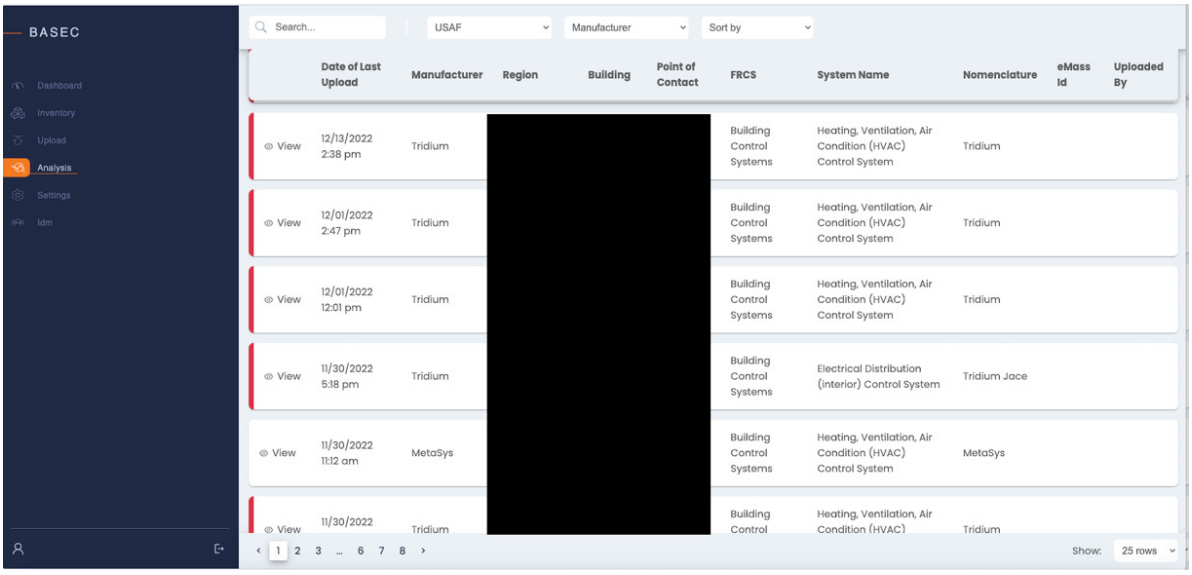

Figure 9. BASEC Analysis Section.

A user can click View for one of the evaluated configuration files to view the detailed findings as shown in Figure 10. If desired, the findings can be exported to a .pdf file.

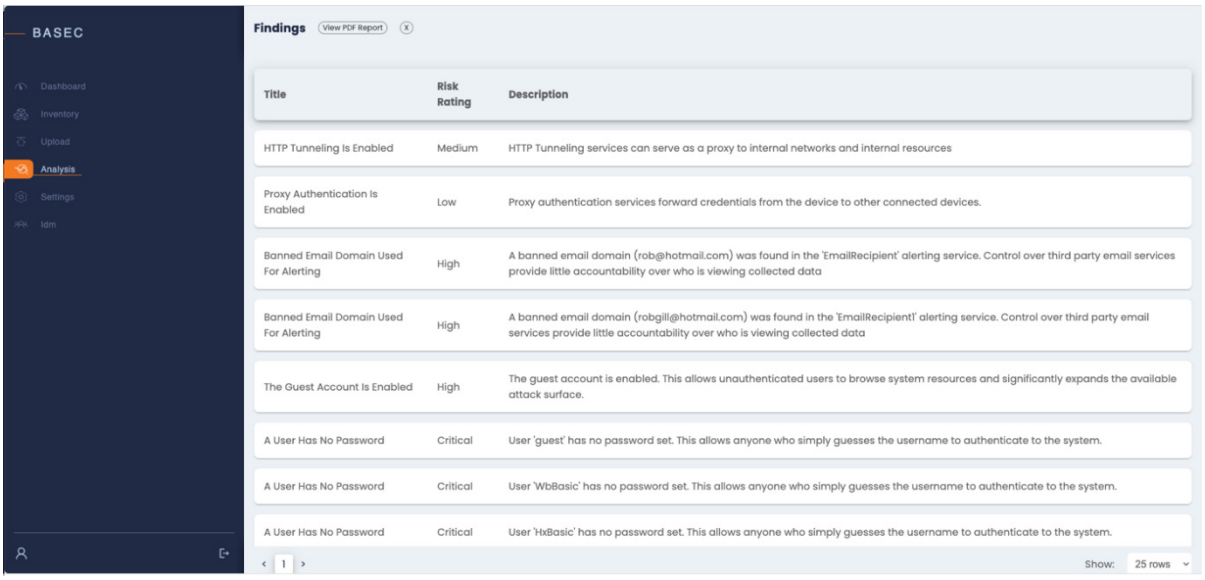

Figure 10. Details of BASEC Analysis.

A top concern voiced by the Service components was the ability for BASEC to aid in asset inventory. QED incorporated the requirement into the BASEC demonstration roll out. Figure 11 shows a capture of the inventory of associated configuration files. The top-level is categorized according to the FRCS type. A user can select the different types of devices and examine just he associated category. The user also has the ability to sort down to the installation level. As an example, a user can select Building Control Systems – HVAC and view only the devices at a specific installation. The details for the device that were entered when the configuration file was uploaded are provided to the user. A search capability provides the ability to search based on desired criteria.

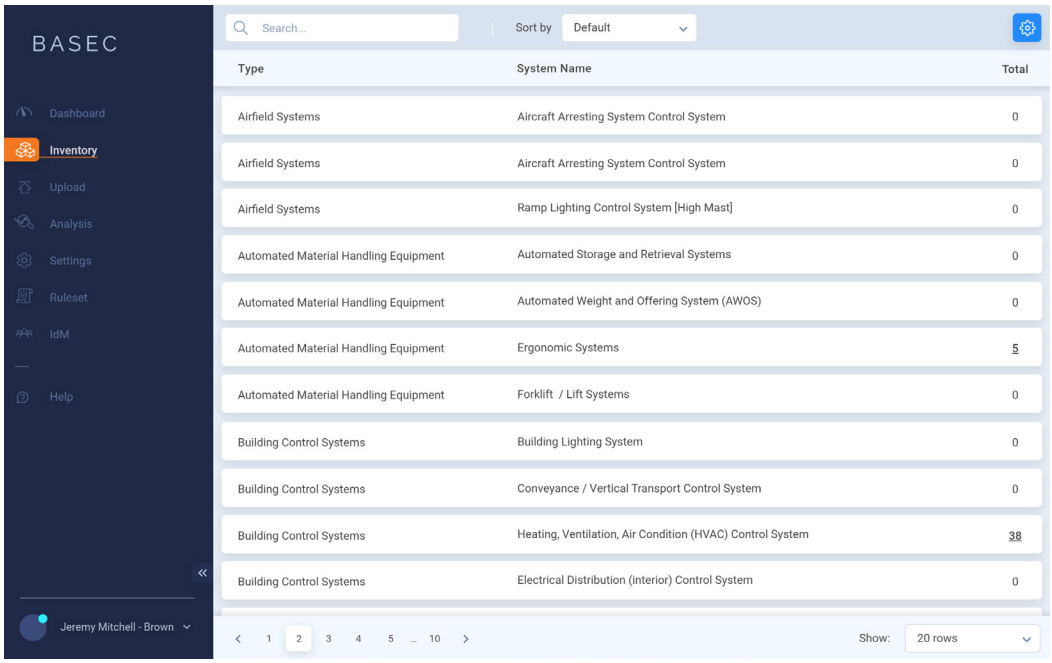

Figure 11. FRCS Inventory of Devices.

Access control for BASEC is configured based on hierarchical structure, such that each designated representative has vision into their span of control. The demonstration is designed with the Service component representative organization as the top level (i.e., AFCEC, NAVFAC, MCICOM and AMC); however, BASEC access control can readily be provisioned to provide a top-level DoD access to examine data trends across all Services together. As shown in Figure 12, the user has the ability to drill down to specific installations or observe findings at a higher level.

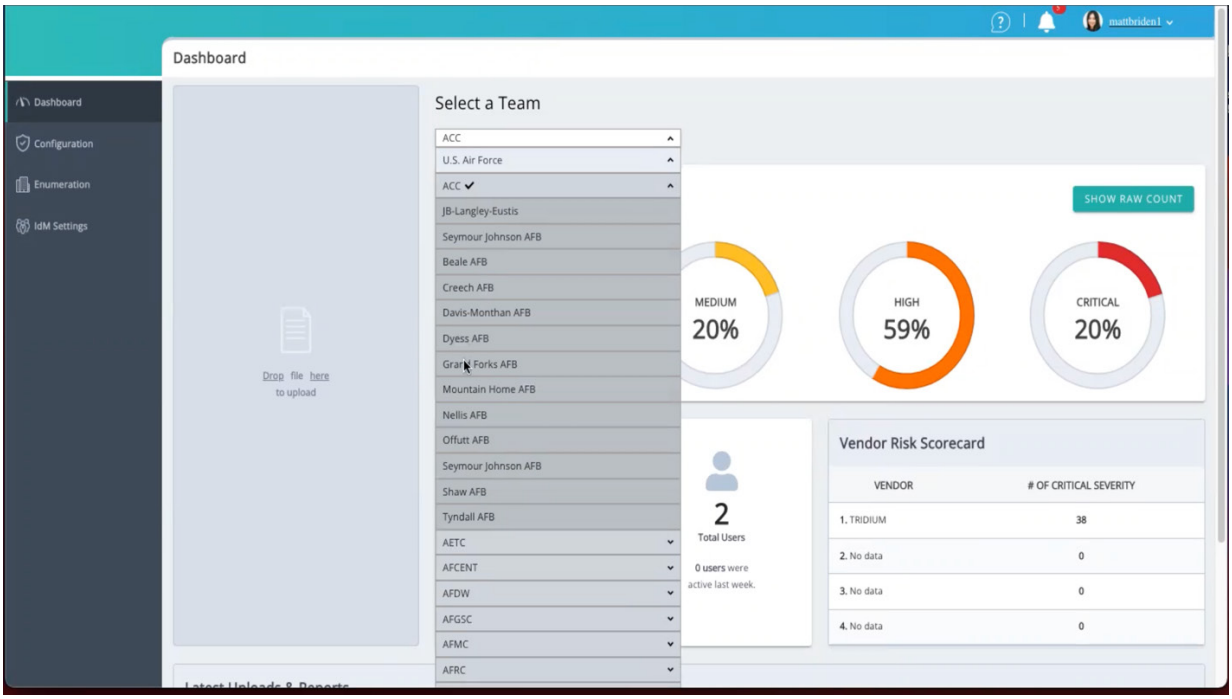

Figure 12. BASEC Drill Down Capabilities.

The BASEC web-based management interface is designed to provide end-users a secure means to upload device configuration files. The user dashboard, shown in Figure 13, allows users to examine findings of individual reports and navigate to historical reports. Access control management has also been built into the BASEC portal, allowing administrative control over who can access specific findings. The BASEC portal enhancements incorporate trend data, refined access controls and "drill down" capabilities supporting Service requirements.

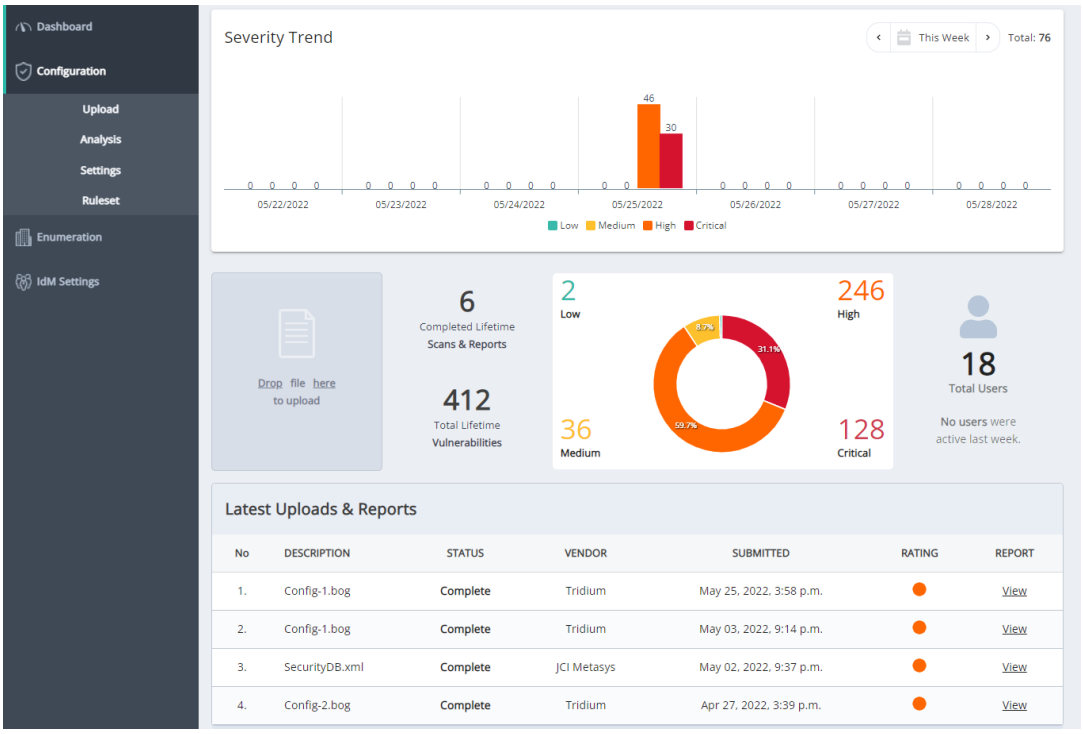

Figure 13. BASEC Historical Perspective and Reporting.

Historical data is be saved and archived for the period of time as specified by the Service components. For analysis, BASEC can incorporate archived data to encompass date intervals as specified by the user. Data trend time intervals can be specified by the end-user to examine user-defined intervals that encompass short-term (e.g., weekly), mid-term (e.g., monthly) and long-term (e.g., yearly) historical records for severity trends as shown in Figure 14.

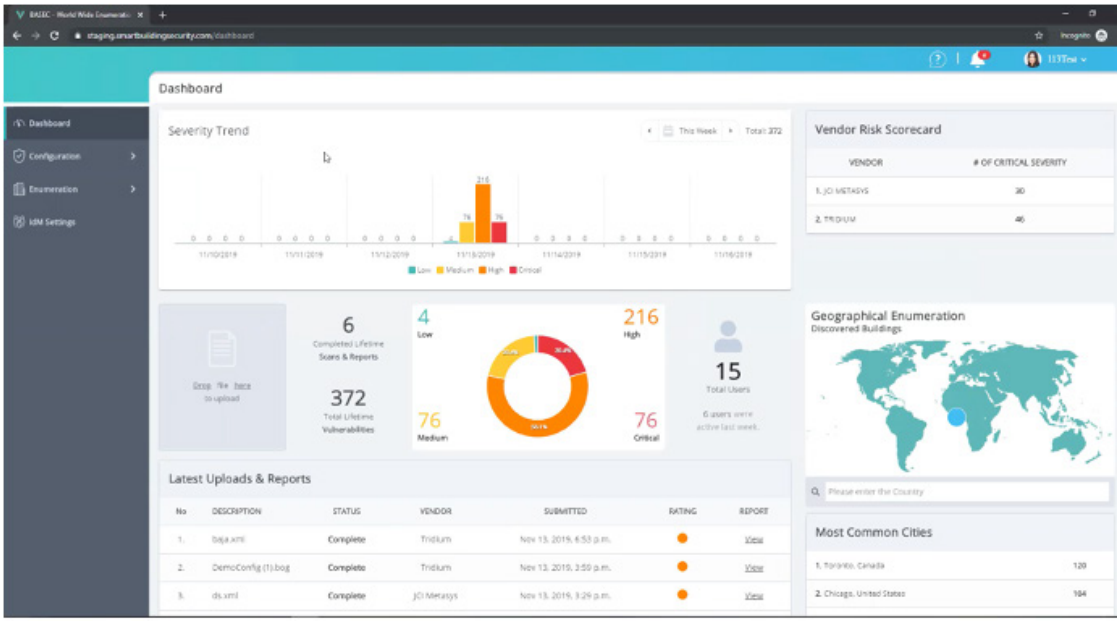

Figure 14. BASEC Presentation of Findings.

As shown in Figure 15, a snapshot can be tailored to show historical views over differing periods. The example shows a 3-month period identifying the severity of findings during that timeframe. This view can be added to the Dashboard for a quick look at numbers for various reporting periods over 30-day increments.

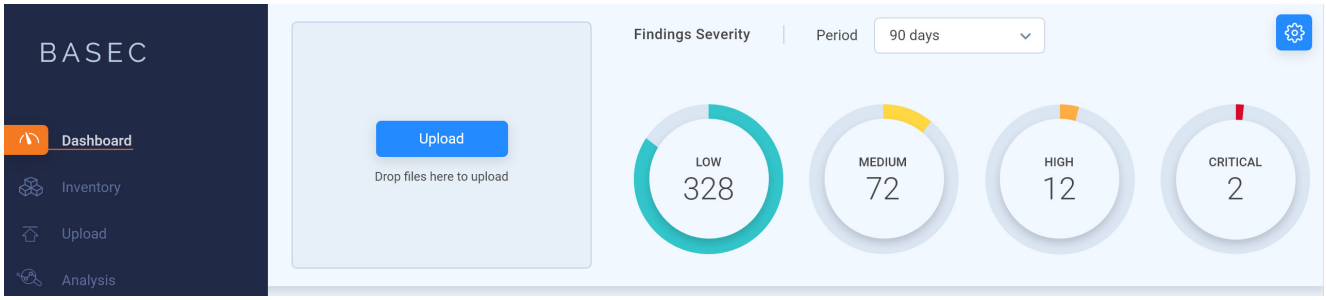

Figure 15. BASEC Historical View of Severity Over Specified Period.

The enhancements incorporated into BASEC help facilitate an enterprise solution that allows fine control and analysis over the cybersecurity posture of installation energy/water control systems.

2.3 ADVANTAGES AND LIMITATIONS OF THE TECHNOLOGY

The DoD needs a cost-effective solution for evaluating the cyber security posture of critical energy/water control systems. The solution should ensure that prior to installation or upgrade, configuration files should be audited to ensure compliance with DoD cyber security guidance and security controls. Annual auditing of installation energy/water system configuration files should be performed to ensure systems remain compliant with DoD cyber security guidance and security controls. Continual monitoring is needed to identify any system-level changes in the configuration that could result in cyber security weaknesses and non-compliance with DoD cyber security guidance and security controls.

The current method of evaluating a DoD installation energy/water systems requires assessment teams, follow-on analysis, and specialized skill sets. Unfortunately, such evaluations only show a snapshot in time of the security posture. Indeed, any adjustment at all to settings requires another evaluation to ensure compliance. The costs for sustaining an effective program in this manner are expensive and unrealistic.

BASEC provides a solution to evaluate the configuration and cyber security standards for military installation energy/water control 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 across multiple integrators and acquisition sources. The DoD will realize cost benefits by requiring third party vendors to conform to configuration standards enforced by BASEC prior to the deployment of new/upgraded systems. By requiring third party vendors to establish a secure configuration prior to deployment, the DoD saves on costs associated with the reconfiguration of devices to meet security objectives.

BASEC implementation provides a new process for engineers to evaluate their security posture. This change management will require incorporation of new workflow and training on how to adequately deploy BASEC to maximize efficiency. It is expected that BASEC will be readily incorporated to meet new guidelines and directives due to the ease of deployment, scalability and workload reduction.

Although the initial focus is evaluating compliance of configuration settings for deployed devices, the BASEC analysis engine collects data points that provide potential for integration with existing or new capabilities. As an example, information from BASEC can be shared with data inventory tools for incorporating configuration data with specific devices. Data correlation and monitoring can facilitate modeling and simulation capabilities as well as integration with Advana or other DoD enterprise databases for data analytics or visualization. These aspects require API integration, which is in the roadmap for future enhancement of BASEC capabilities.

The successes of initial evaluations demonstrate BASEC's utility and potential as a safeguard for DoD critical infrastructure. To prepare for the full deployment, BASEC will need to incorporate DoD secure configuration settings for vendors and apply defined evaluation criteria. Additionally, QED will need to ensure that BASEC reporting mechanisms are consistent with DoD systems and adhere to certification and accreditation requirements. Design work will be required to support the Service wide adoption; however, the technical capabilities exist within the BASEC framework and no advanced technical barriers are expected that will preclude the demonstration of BASEC or limit BASEC's capabilities for DoD implementation.

The final hurdle is the varying device technologies associated with installation energy/water control systems. For each device, an analysis module must be incorporated into the BASEC engine. Examination over the past three years has revealed that BASEC already incorporates a significant number of devices and includes the primary vendors. Minimal changes have been required to include software updates and device enhancements. Finally, once a module is created, it is there for the lifetime of BASEC. Although technologies vary and there is not a set timeline, the average time to create an analysis module is approximately 10 days.

3.0 PERFORMANCE OBJECTIVES

Demonstration of BASEC built on capabilities and lessons from previous installations. As such, the demonstration is cumulative with the fully capable enterprise-level BASEC functionality demonstrated for this effort. Service inputs helped drive the feature requests and determine the end objectives for BASEC technical capabilities. A summary of the measured performance objectives is identified in Table 1.

Table 1. Performance Objectives.

Performance Objective	Metric	Data Requirements	Success Criteria
Scalability	Number of instances that can be concurrently deployed	Evaluation using Cloud Service Metrics	Readily accept over 300,000 instances of BASEC deployment
Trend Data	Statistical Significance	Historical Data	Correlated findings with 95% CI
Coverage of Cyber Hygiene Requirements	Percentage of requirements covered in analysis engine	Configuration files for installation facilities and requirements	95% coverage of requirements
Time to Evaluate System for Compliance	Time	Time for BASEC analysis engine to evaluate	< 15 mins to complete automated analysis
Cost Savings	Dollars	Time and workload	Reduce costs by 70%
User Satisfaction	Degree of Satisfaction	Likert Scale Survey	90% increase in satisfaction

BASEC demonstrated the ability to meet the 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. Findings were verified through manual inspection of the configuration files. BASEC also produced valid reports based on findings incorporating a functional web-based interface management for enterprise deployment.

The following performance metrics demonstrate the effectiveness of deploying BASEC as mapped to the Performance Objectives:

- Scalability. Using the inherent AWS infrastructure, QED tested concurrent loading of up to 500,00 instances without fault. This number far exceeds the expected use case for Service-wide deployment.
- Trend Data. BASEC can track multiple instances of uploaded files mapped to FRCS types. Manual inspection revealed correlated findings for every configuration file evaluated for the duration of the project, consisting of over 500 samples.
- Coverage. BASEC adequately parsed and analyzed 100% of configuration files for the demonstration.

- Time to Evaluate. BASEC completed analysis of individual configuration files at an average of 4 minutes.
- Cost Savings. BASEC evaluated 180 configuration files in less than 45 minutes. A similar manual effort is estimated at approximately over time period of months to perform analysis based on previous assessments (e.g., NDAA 1650). As such, the cost saving in labor hours is readily apparent with efficiencies exceeding 90%. Further, BASEC identified significant findings that have gone previously undetected after years of deployment. This risk reduction is significant. The average time to train personnel to be proficient using BASEC is less than one hour.
- User Satisfaction. The Services have all provided positive feedback on the capabilities of BASEC. Specifically, after the demonstration AFCEC representative claimed *This is most helpful to the base to get on very basic things that they probably had no situational awareness into. Considering how quickly you were able to capture the data, this is quite a win.* The individuals and organizations queried for feedback are provided in Appendix A. The common feedback for successes included the ability to rapidly scale evaluation across multiple installations and correlate the type of findings. Future recommendations included implementation of stand-alone BASEC clients that can be directly integrated in the control system environment.

BASEC was able to transform a manual process of evaluating system configurations that traditionally takes weeks/months to minutes. BASEC also demonstrated effective coverage of the military installation and provided enterprise solution for evaluating system cybersecurity postures.

4.0 FACILITY/SITE DESCRIPTION

Military installations contain myriad building facilities that rely on varying energy/water control systems. QED, in collaboration with AFCEC, selected an installation for the demonstration of BASEC capabilities that contained representative control systems. The installation was a large-size USAF base consisting of multiple buildings and varying operational configurations. The Services chose to focus on one specific vendor for the demonstration so that BASEC enterprise capabilities could be evaluated.

The specific USAF installation is redacted from this report. The discussion on findings to follow describes security concerns for critical energy control systems. Although not classified, AFCEC has requested we redact the specific installation from the report due to associated sensitivities. Interested organizations can coordinate directly with AFCEC if further information is desired.

5.0 TEST DESIGN

For the enterprise demonstration, configuration files for building automation systems were supplied to BASEC, which identifies weak configurations and vulnerable systems. BASEC was evaluated for the ability to provide metrics and analysis for systems across the installation. The types of reporting were driven by Service requirements, and include top security issues encountered, percentage of systems with critical security issues, percentage of systems with insecure configuration settings, and average strength of credentials used by a device. Service representatives had the ability to interact with the BASEC user interface to determine utility of the provided data. User satisfaction and cost savings via workload reduction were evaluated.

5.1 CONCEPTUAL TEST DESIGN

The team evaluated findings from the BASEC analysis engine in a direct comparison against manual observations.

Pretest preparation was used to identify vendor deployments and accessibility to configuration files via coordination with AFCEC representatives. Baseline measurements were performed through manual observation of the configuration files. Configuration files were uploaded to the BASEC portal for automated analysis.

5.2 BASELINE CHARACTERIZATION

QED performed baseline analysis of configuration settings using manual observations. System experts helped determine time for analysis and accuracy of data to form the baseline associated with current manual processes for evaluating the security configuration of devices. The initial baseline sampling occurred at a test facility hosted by AFCEC.

5.3 DESIGN AND LAYOUT OF TECHNOLOGY COMPONENTS

Installation energy/water system devices consist of configuration files that define the specific settings for each specific deployment. QED obtained configuration files from the Service representatives and uploaded them to a server hosted on the DoD cloud. The server contains management roles for BASEC as well as the analytical engine for parsing and evaluating the settings of the configuration files.

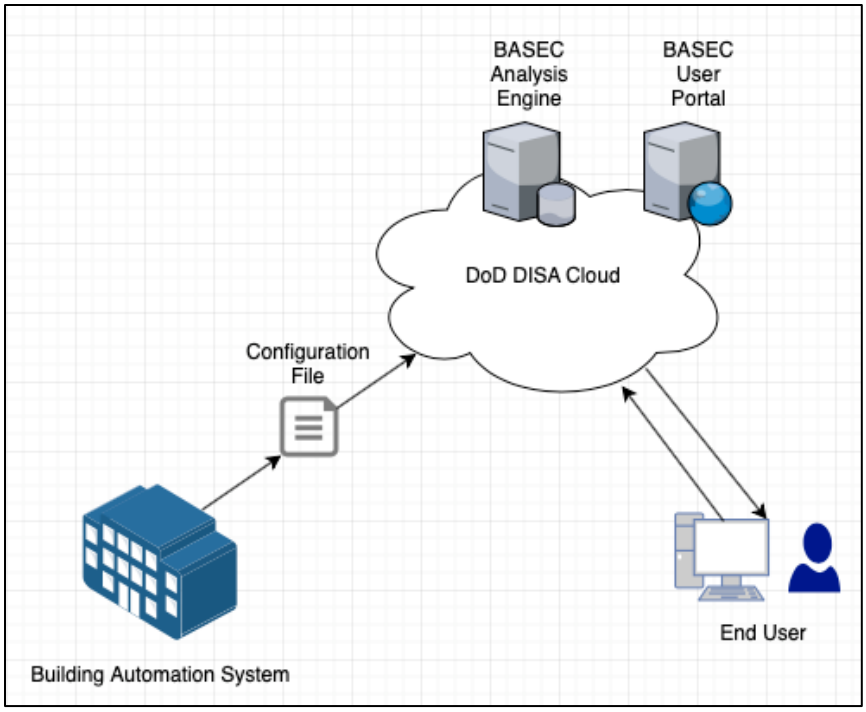

Figure 16. BASEC Test Design.

5.4 OPERATIONAL TESTING

The schedule of completed milestones is outlined in the Gantt chart below, covering the 19-month effort.

TASKS	Months 1-4	Months 5-9	Months 10-14	Months 15-19
1. Data Gathering	Phase 1			
2. Demonstration Planning	Phase 1			
3. Design Work		Phase 1		
4. Field Work		Phase 1		
5. Data Analysis			Phase 1	
6. Reporting	DP			Phase 1 FR

DP – Demonstration Plan
FR – Final Report
TTP – Technology Transition Plan

Data gathering consisted of working with the Service components to identify requirements and metrics desired for the demonstration. Demonstration planning included coordination for the installation and development of execution plans. The design work focused on tailoring BASEC capabilities and reporting to meet Service component needs, to include trend ana analysis identification, device standards for the analysis engine and enterprise features. The field work consisted of baselining BASEC capabilities at a designated AFCEC test facility and deployment to the identified installation. The analysis and reporting concluded the ESTCP effort.

5.5 SAMPLING RESULTS

QED coordinated with AFCEC for sampling of related configuration files at their test facility located at Arnold AFB. QED leveraged the sampling to confirm BASEC capabilities and prepare for the demonstration at the selected AF installation. The sampling results demonstrated the feasibility and revealed a 100% identification of associated findings when compared to manual baseline examination.

6.0 PERFORMANCE ASSESSMENT

QED, in coordination with AFCEC, identified a USAF installation to evaluate the effectiveness of BASEC. The evaluation focused on Tridium JACE controllers deployed across the installation. The controllers provide monitoring and control for the building environmental conditions. For deployment at the installation, one JACE controller is associated with multiple actuators and sensors used to monitor and control environmental conditions within a single building. For larger buildings, multiple controllers may be used within a single building. In total, 180 JACE controllers were evaluated for the installation, associated with 150 different buildings.

A configuration file for each building/zone is created and uploaded to the respective JACE controller that contains operational settings for the system. The configuration file also contains settings for functional parameters (e.g., user accounts, services enabled, software versions, security settings, naming conventions, communication protocols, etc.). Each JACE controller has an associated configuration file containing settings for a respective building/zone. Copies of the configuration files are stored on a local server in the event a backup copy is needed or to use as a baseline to make changes to settings.

QED traveled onsite to the installation with AFCEC representatives. CE individuals from the host installation provided copies of the JACE configuration files that they store locally on a centrally managed server for each building. QED uploaded the configuration files to the BASEC analysis engine via the user interface. BASEC completed analysis on all 180 configuration files in less than 45 minutes total. The results are provided in a hierarchical format via the BASEC user interface, allowing individual examination of the results for each of the associated buildings.

Figure 17. Analysis of Installation Configuration Files.

Results of the analysis reveal that the same baseline configuration is deployed to a majority of the JACE controllers. This is not uncommon, as often times CE personnel or system integrators that install the system use a common baseline configuration for all deployments. From a security standpoint, this can be effective if the deployed configuration is hardened. However, the drawback is that if a security weakness exists in one system, then it is present in all systems. As an example, an attacker could probe a relatively innocuous facility to identify weaknesses and develop exploits. The attacker could then leverage that same exploit against a more desirable target on the installation.

From the 180 systems evaluated, 34 were found to be in compliance, with no configuration concerns. The remaining 146, or 81% of systems evaluated had one to four identified security concerns rated at a HIGH Critical level. A separate Appendix with associated buildings mapped to the findings has been provided to AFCEC.

The first finding in the configuration analysis is that the Guest account has no password. This finding was present on 144 of the 180 systems evaluated. With the Guest account enabled, anyone accessing the controller via a web browser can authenticate using Guest and no password. Once logged in, the Guest account is not restricted in ability to observe and change operating settings. Note that the Tridium Security Guide explicitly recommends disabling Guest accounts.

The second finding in the configuration analysis is that the account BACnet has no password. This finding was present on 37 of the 180 systems evaluated. BACnet is a communications protocol for building automation systems that enables device to device communications. An attacker logging in to the BACnet account has system privileges to observe and modify settings associate with interconnected devices.

The third finding is associated with a created user account. There were 12 systems of the 180 evaluated that had a created user account with no password. Note that the user account was the same username for all twelve systems. An attacker can access the system via a web browser and log in as the user with no password, and assume the authority granted to the user.

The fourth finding in the configuration analysis is that the JACE controllers are running outdated software versions with publicly known vulnerabilities. This finding was present on 145 of the 180 systems evaluated. Published Common Vulnerabilities and Exposures (CVEs) shows that an attacker can bypass intended access restrictions and also allows remote attackers to read sensitive files and consequently execute arbitrary code. Known exploits have been created to execute attacks against these vulnerabilities.

The final finding is associated with the admin user account. One system that was evaluated has an admin user account with no password. An attacker can access the system via a web browser and log in as an administrator with no password and have full control over operations and configuration of the system.

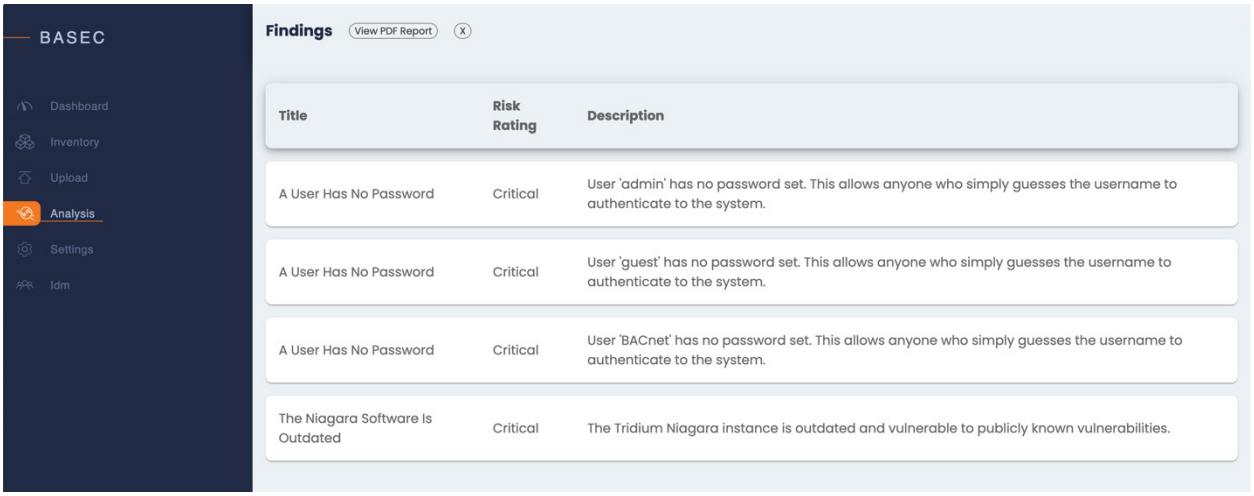

Figure 18. Individual Analysis of System Findings.

The five findings across 159 of the 180 building control systems that were evaluated had High Critical impact findings. The security concerns are associated with a remote attacker exploiting a weakness that could provide unfettered control of the associated building automation system. Figure 18 shows a summary of the findings for the installation.

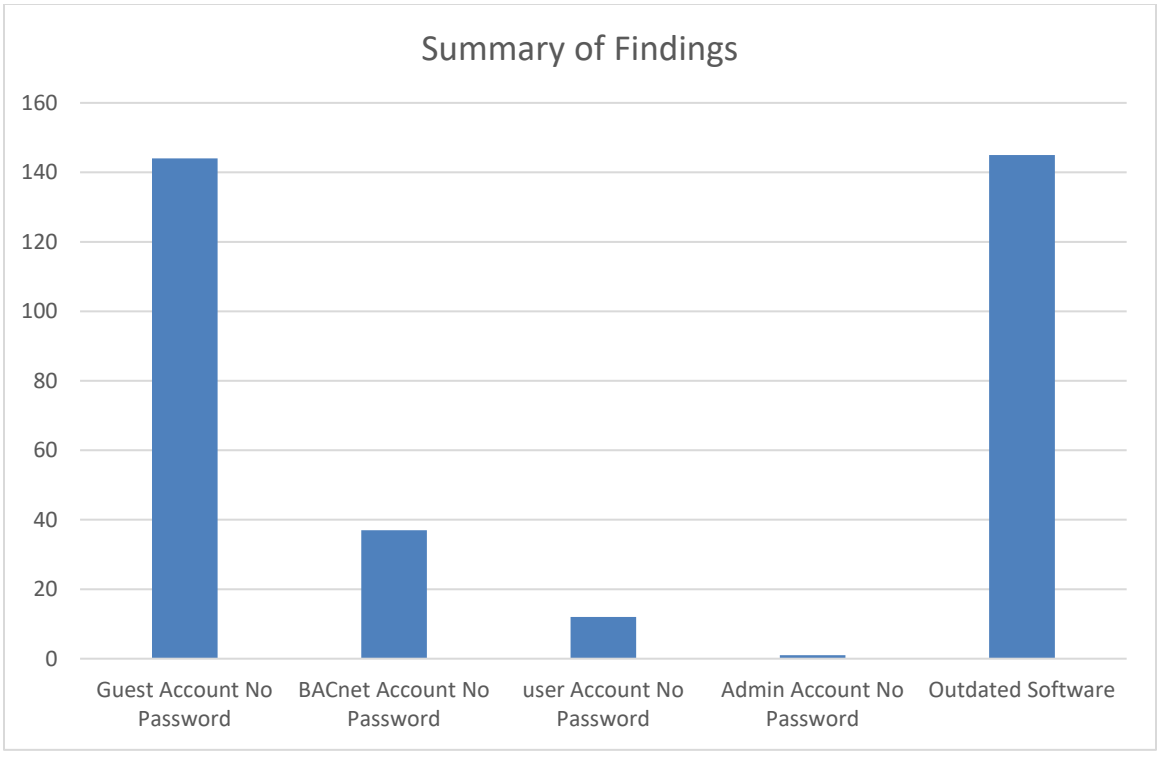

Figure 19. Functional Overview of the BASEC Analysis Process.

The Air Force Community of Interest Network Enclave (COINE) provides separation from the Air Force and DoD networks to protect CE control systems. The COINE provides safeguards and compensating controls to limit access to the JACE controllers, reducing the attack surface.

As such, an attack exploiting the identified configuration vulnerabilities is limited to either traversing through or being initiated on the COINE network. If, however, access is ever obtained to the device, then the deployed systems are exposed to the identified attacks. As a defense-in-depth recommendation, the installation should consider disabling the Guest Account, verifying the requirement for the user created account and setting a password if the account is still needed, setting a BACnet password (or disabling if not required), and updating the software to the most recent version.

The findings for this evaluation are not necessarily unique to this installation or the Air Force. QED has worked with other Service branches, and commonalties of security weaknesses exist across deployments. Common observations include: default configurations, weak/default passwords, unmanaged/outdated user accounts, improper user permissions, unpatched systems, and unnecessary protocols/services.

7.0 COST ASSESSMENT

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. Costs are derived from historical assessments performed by AMC and AFCEC, most notably NDAA1650 studies. 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.

BASEC deployment consists of software engine deployed in the DoD Government cloud. Hardware costs are associated with general computer requirements. Software licensing of BASEC is the core component of the costs, and QED is performing analysis to determine projected licensing structure. The remaining costs are associated with training and personnel. The cost realization, however, should demonstrate significant savings and enhanced security through leveraging BASEC.

8.0 IMPLEMENTATION ISSUES

QED is working closely with AFCEC for full deployment of BASEC to all Air Force installations. Additionally, Air Force CE personnel are being trained on the capabilities and usage of BASEC in concert with a required training course for all 7-leve CE personnel. No specialized equipment is needed for BASEC, and processes readily incorporate into current practices.

BASEC requires sustainment to ensure coverage of newer technologies as well as to incorporate feature enhancements. Maintaining current analysis engine is the most significant aspect of long-term implementation planning. This aspect is expected to be addressed through support agreements and dedicated personnel. AFCEC has offered transition roadmap that includes long-term sustainment and funding. Long-term support and licensing provides necessary coverage to incorporate new technologies in concert with AFCEC requirements. Advancements for inclusion of newer technologies will follow prioritization driven by AFCEC needs.

9.0 REFERENCES

[1] United States Congress, *National Defense Authorization Act for Fiscal Year 2017*, PUBLIC LAW 114–328—DEC. 23, 2016

[2] Deputy Secretary of Defense, *DoD Mission Assurance Strategy,* April 2012.

[3] Chief of Naval Operations, *Navy Mission Assurance Program,* OPNAVINST 3502.8, Nov 2017.

APPENDIX A POINTS OF CONTACT

POINT OF CONTACT	ORGANIZATION	E-mail	Role in Project
Timothy Tetreault	ESTCP	timothy.j.tetreault.civ@mail.mil	Program Manager
Jonathan Butts	QED Secure Solutions	j.butts@qedsecure.com	Primary Investigator
Billy Rios	QED Secure Solutions	billy.rios@qedsecure.com	Technical Lead
Mark McClellan	AFCEC	mark.mcclellan@us.af.mil	USAF AFCEC Rep
James Staton	NAVFAC	james.b.staton2.civ@us.navy.mil	NAVFAC Rep
Nick Spurling	MCICOM	nicholas.spurling@usmc.mil	MCICOM Rep
Wendy Huskey	AMC	wendy.m.huskey.civ@mail.mil	AMC Rep