

Thank you for signing in early

The webinar will begin promptly at
12:00 pm ET, 9:00 am PT



SERDP and ESTCP Webinar Series

- The webinar will begin promptly at 12:00 pm ET, 9:00 am PT
- Options for accessing the webinar audio
 - Listen to the broadcast audio if your computer is equipped with speakers
 - Call into the conference line
 - (669) 900-6833 or (929) 205-6099
 - Required webinar ID: 708-683-274
 - YouTube live stream
 - <https://www.youtube.com/user/SERDPESTCP>
- For questions or technical issues, please email serdp-estcp@noblis.org or call 571-372-6565

Securing DoD Control Systems and Infrastructure from Cyber Threats

July 9, 2020



Welcome and Introductions

Rula A. Deeb, Ph.D.
Webinar Coordinator



Webinar Agenda

- **Webinar logistics** (5 minutes)
Dr. Rula Deeb, Geosyntec Consultants
- **Overview of SERDP and ESTCP** (5 minutes)
Mr. Timothy Tetreault, SERDP and ESTCP
- **Securing Military Installations Against Cyber Attacks** (25 minutes + Q&A)
Dr. Jonathan Butts and Mr. Billy Rios, QED Secure Solutions
- **Physical Cybersecurity: Low-Cost Data Diodes for DoD Facility Equipment Monitoring** (25 minutes + Q&A)
Mr. Colin Dunn, Fend Incorporated
- **Final Q&A session**

Zoom Instructions

- Download Zoom
 - <https://zoom.us/download>
- If you cannot download Zoom, you can view the slides using an internet browser
 - Create a free Zoom account (<https://zoom.us/signup>)
 - Use a compatible browser (Firefox, IE or Edge)
 - View the webinar at <https://success.zoom.us/wc/708683274/join>
- If the material is not showing on your screen or if screen freezes
 - Key in Ctrl + F5 to do a hard refresh of your browser

Zoom Instructions (Cont'd)

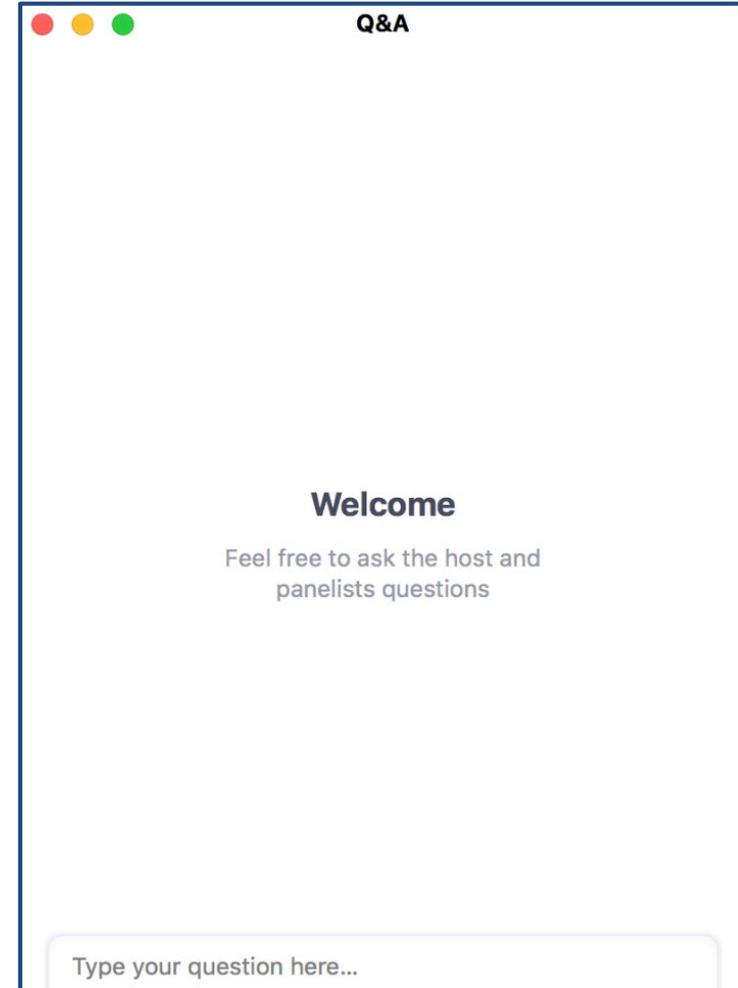
- If you are connecting to computer audio
 - Click the arrow next to the “Join Audio” button
 - Select test “Speaker and Microphone”
 - Follow prompts
- If you experience difficulties with the audio, call into the conference line
 - (669) 900-6833 or (929) 205-6099
 - Required webinar ID: 708-683-274

In Case of Continued Technical Difficulties

- Download a PDF of the slides at <https://serdp-estcp.org/Tools-and-Training/Webinar-Series/07-09-2020> and call into the conference line
 - (669) 900-6833 or (929) 205-6099
 - Required webinar ID: 708-683-274
- We will also be live streaming the webinar on the SERDP and ESTCP YouTube channel
 - <https://www.youtube.com/user/SERDPESTCP>

How to Ask Questions

- Find the Q&A button on your control bar and type in your question(s)
- Make sure to add your organization name at the end of your question so that we can identify you during the Q&A sessions



SERDP and ESTCP Overview

Timothy Tetreault
SERDP and ESTCP



SERDP

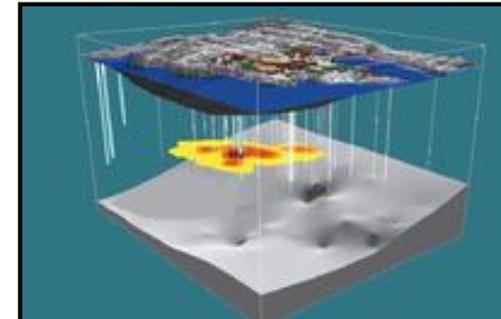
- Strategic Environmental Research and Development Program
- Established by Congress in FY 1991
 - DoD, DOE and EPA partnership
- SERDP is a requirements driven program which identifies high-priority environmental science and technology investment opportunities that address DoD requirements
 - Advanced technology development to address near term needs
 - Fundamental research to impact real world environmental management

ESTCP

- Environmental Security Technology Certification Program
- Demonstrate innovative cost-effective environmental and energy technologies
 - Capitalize on past investments
 - Transition technology out of the lab
- Promote implementation
 - Facilitate regulatory acceptance

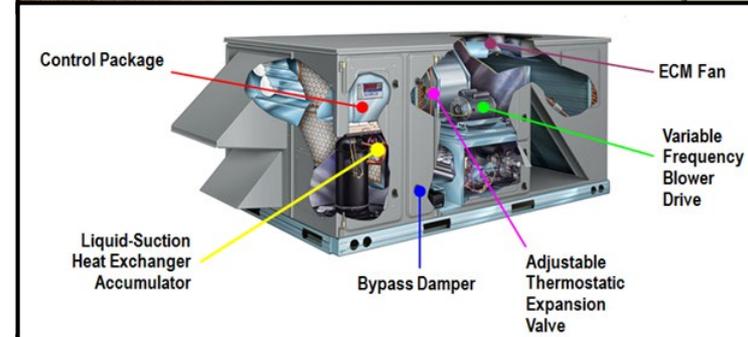
Program Areas

- Environmental Restoration
- Installation Energy and Water
- Munitions Response
- Resource Conservation and Resiliency
- Weapons Systems and Platforms



Installation Energy and Water

- Smart and secure installation energy management
 - Microgrids
 - Energy storage
 - Ancillary service markets
- Efficient integrated buildings and components
 - Design, retrofit, operate
 - Enterprise optimized investment
 - Advanced components
 - Intelligent building management
 - Non-invasive energy audits
- Distributed generation
 - Cost effective
 - On-site
 - Emphasis on renewables



SERDP and ESTCP Webinar Series

Date	Topic
July 23, 2020	Predicting PFAS Fate and Transport in Subsurface Environments, and Treatment
August 20, 2020	Addressing Threatened and Endangered Species on DoD Lands
September 10, 2020	Advances in Cold Spray Repair Technologies and Application of Waterjet to Large and Medium Caliber Gun Barrel Refurbishment
September 24, 2020	Munitions Distribution, Mobility and Burial in the Underwater Environment
October 8, 2020	Managing AFFF Impacts to Subsurface Environments and Assessment of Commercially Available Fluorine-Free Foams (Part 1)
October 22, 2020	Managing AFFF Impacts to Subsurface Environments and Assessment of Commercially Available Fluorine-Free Foams (Part 2)

For upcoming webinars, please visit

<http://serdp-estcp.org/Tools-and-Training/Webinar-Series>



Save the Date

SERDP • ESTCP SYMPOSIUM

A three-day symposium showcasing the latest technologies that enhance DoD's mission through improved environmental and energy performance

December 1-3, 2020
Washington, DC

Poster abstracts due August 14
Registration is open!

Securing Military Installations Against Cyber Attacks



Jonathan Butts, Ph.D.
QED Secure Solutions

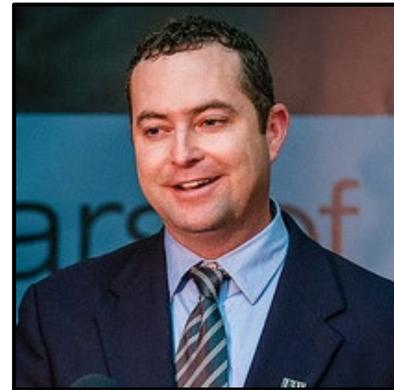


Billy Rios
QED Secure Solutions



Project Motivation and Goals

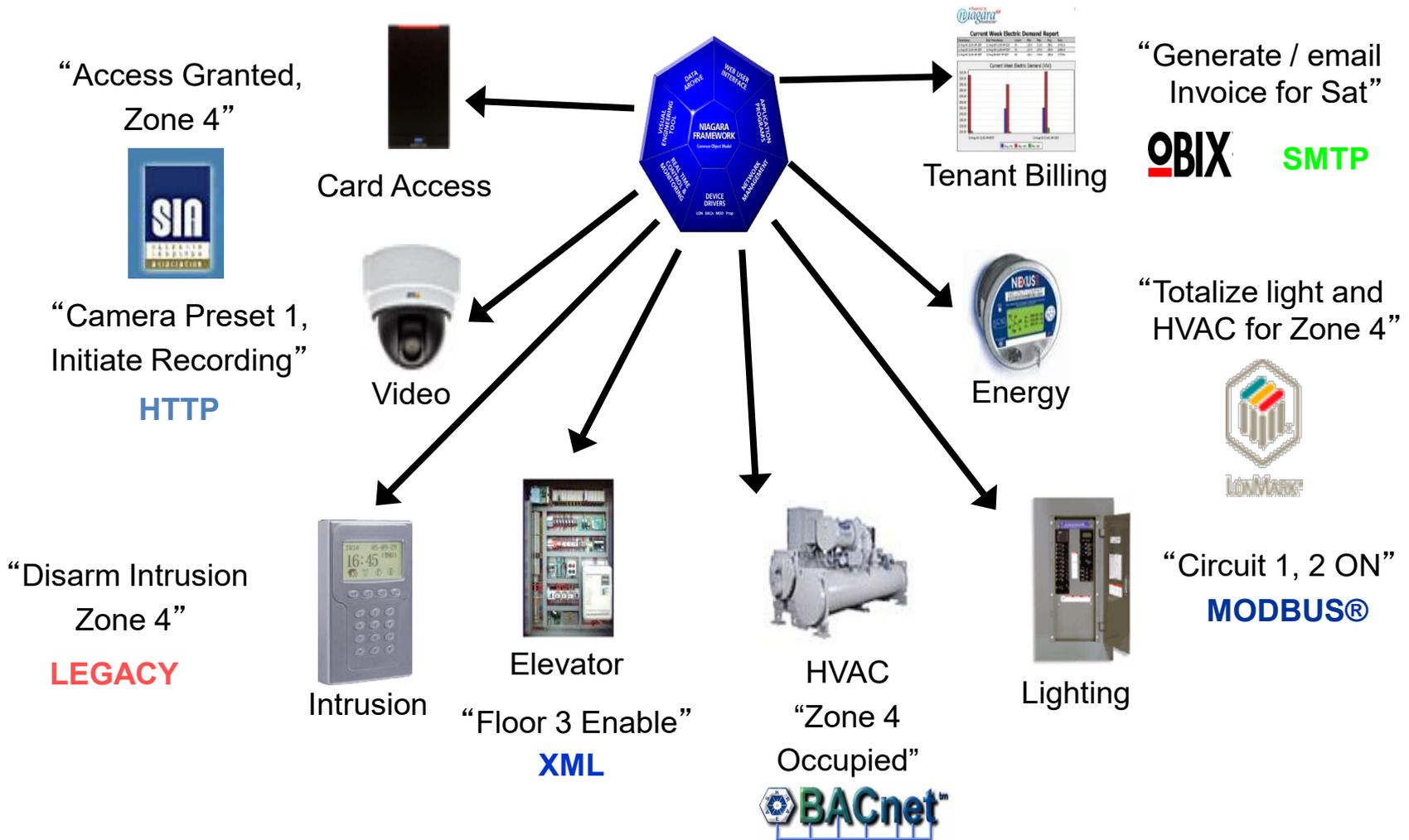
Jonathan Butts, Ph.D.
QED Secure Solutions



Agenda

- Building automation systems
- Military installation cybersecurity challenges
- Baseline Automated Security Enumeration and Configuration (BASEC) configuration analysis
- Observations and findings
- Conclusions

Building Automation Systems



Threats

- Hackers breached New Jersey industrial HVAC system
- Ransomware disguised as Allen-Bradley control system update
- Building control system at Google Australia office hacked
- Building control systems can be pathway to target-like attack
- DHS report: Building automation systems vulnerable to attack

Risks to Military Installations

- **Safety/security**
 - Impede building safety functions
 - Impact environmental conditions
 - Alter building access
- **Access to network data**
 - Ability to gain access to protected data
 - Pivot point for executing attacks
 - Potential for exfiltration while avoiding Defense Information Systems Agency safeguards
- **Operations impact**
 - Mission assurance
 - Potential to degrade military objectives
 - Direct impact to core installation functions

Current State of Affairs

- **Auditing**
 - Vast majority of devices are configured insecurely
 - Lack of common configuration/implementation standards
 - Use of commercial network infrastructure
 - Lack of capability to identify, monitor or track systems
 - Test and reporting takes weeks
- **Analysis**
 - Expensive for extensive site evaluation
 - Assessment teams do not readily scale
 - One-time snapshot of current security posture
 - Difficult to obtain meaningful metrics for comparative analysis
 - Enterprise solution needed to assist management and auditing

BASEC Configuration Analysis

Billy Rios
QED Secure Solutions

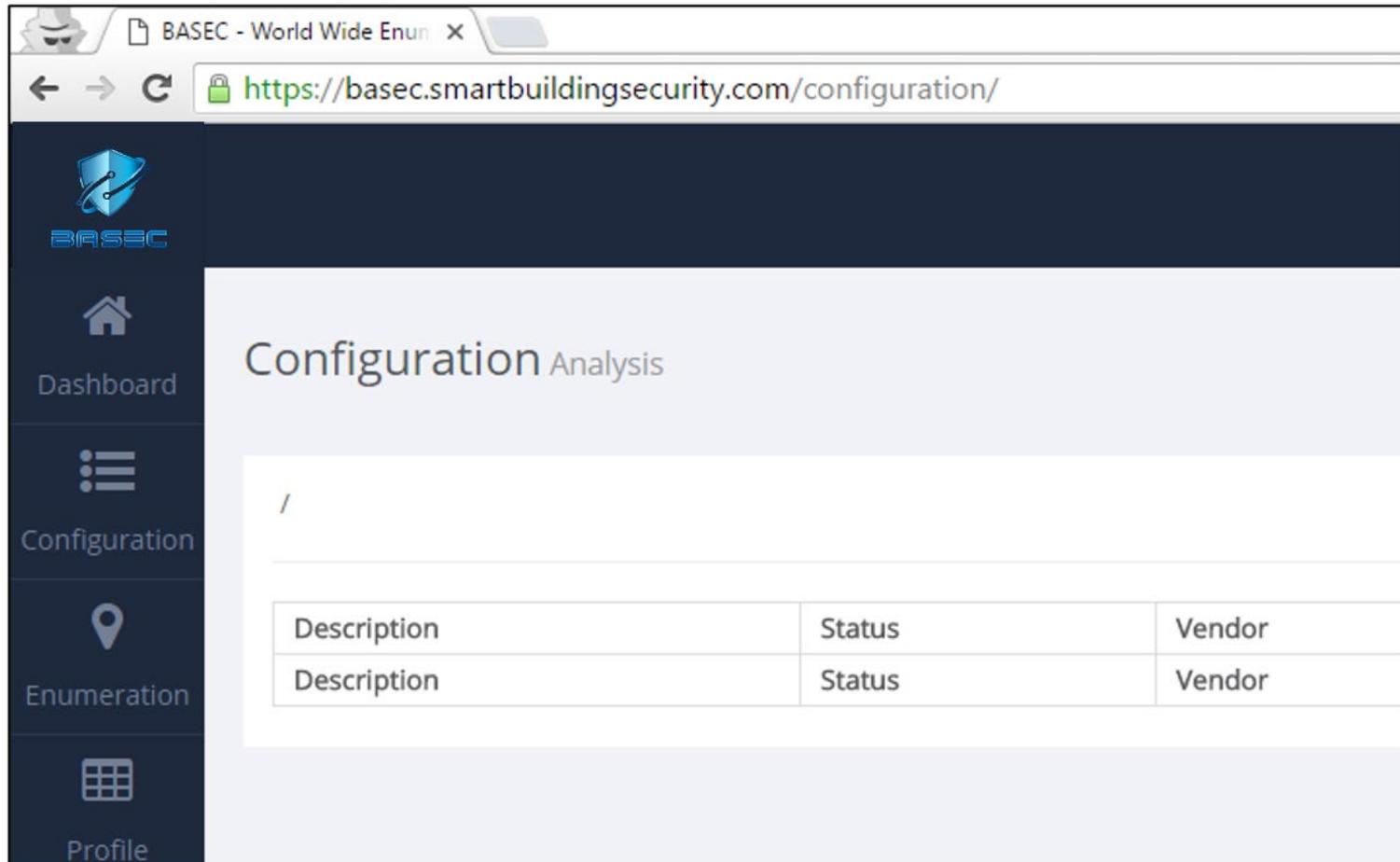


ESTCP Project Goals

- Demonstrate ability to automate and track Risk Management Framework (RMF) compliance
- Incorporate BASEC with current DoD network solutions
- Implement with no architecture changes required
- Provide enterprise solution that ensures system compliance
- Integrate BASEC with authority to operate procedures
- Generate automated reports that identify compliant/non-compliant security configuration details

Is your building automation system installed and configured securely?

Configuration Analysis



BASEC - World Wide Enum x

← → ↻ <https://basec.smartbuildingsecurity.com/configuration/>

BASEC

Dashboard

Configuration

Enumeration

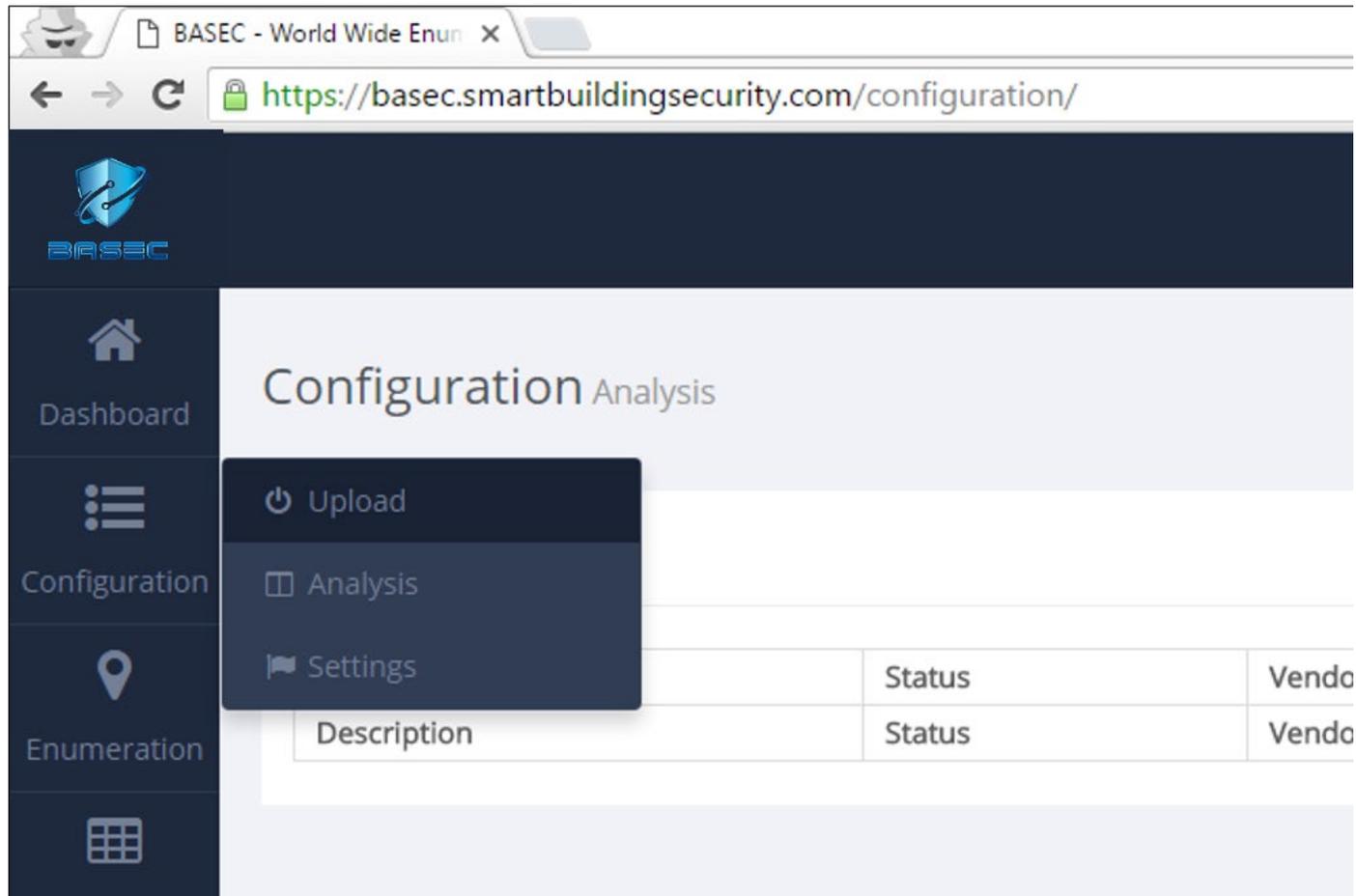
Profile

Configuration Analysis

Description	Status	Vendor
Description	Status	Vendor

BASEC provides automated means to upload and analyze configuration files

Configuration Analysis

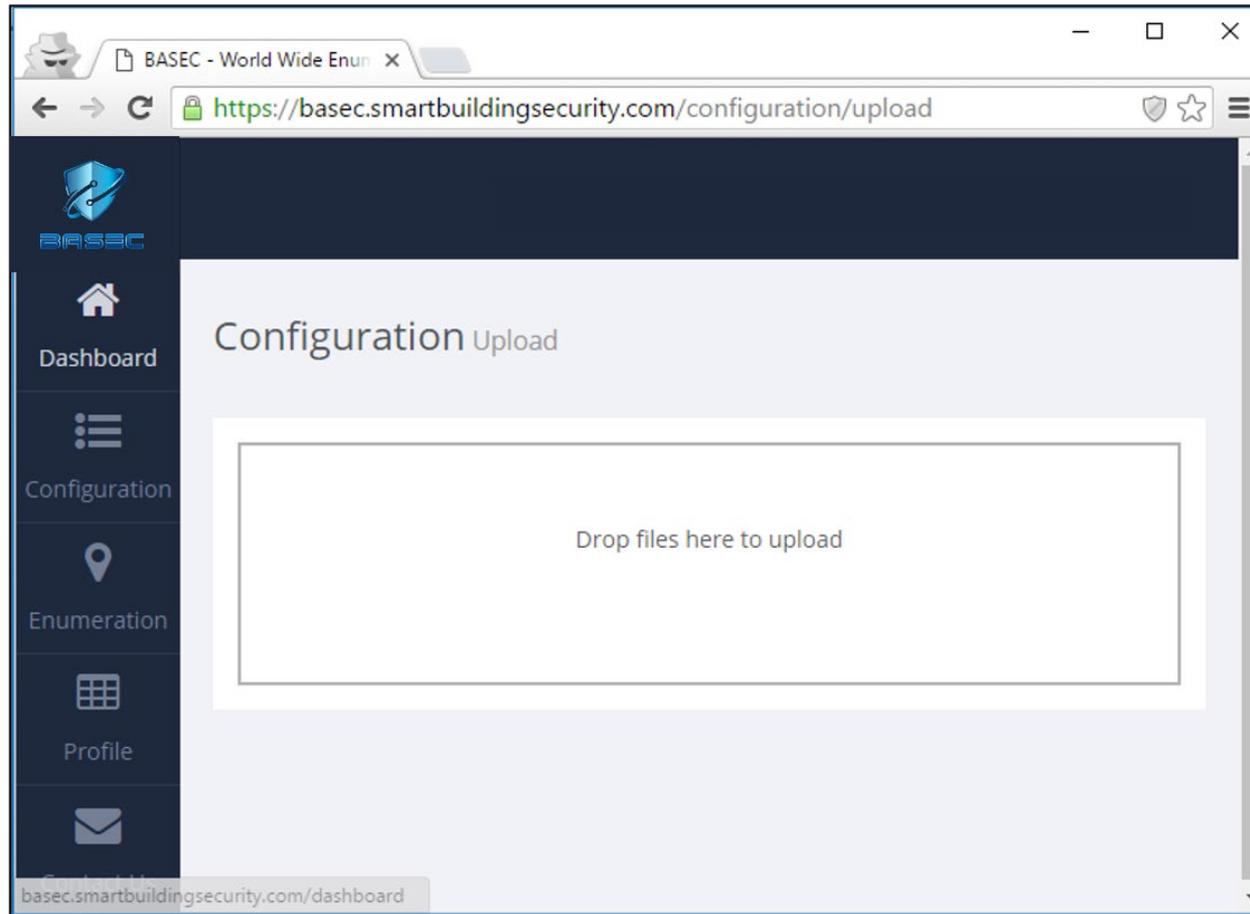


The screenshot shows a web browser window with the URL <https://basec.smartbuildingsecurity.com/configuration/>. The page title is "Configuration Analysis". On the left, there is a dark sidebar with navigation options: "Dashboard", "Configuration", and "Enumeration". The "Configuration" menu is open, showing sub-options: "Upload", "Analysis", and "Settings". The main content area contains a table with the following structure:

Description	Status	Vendo

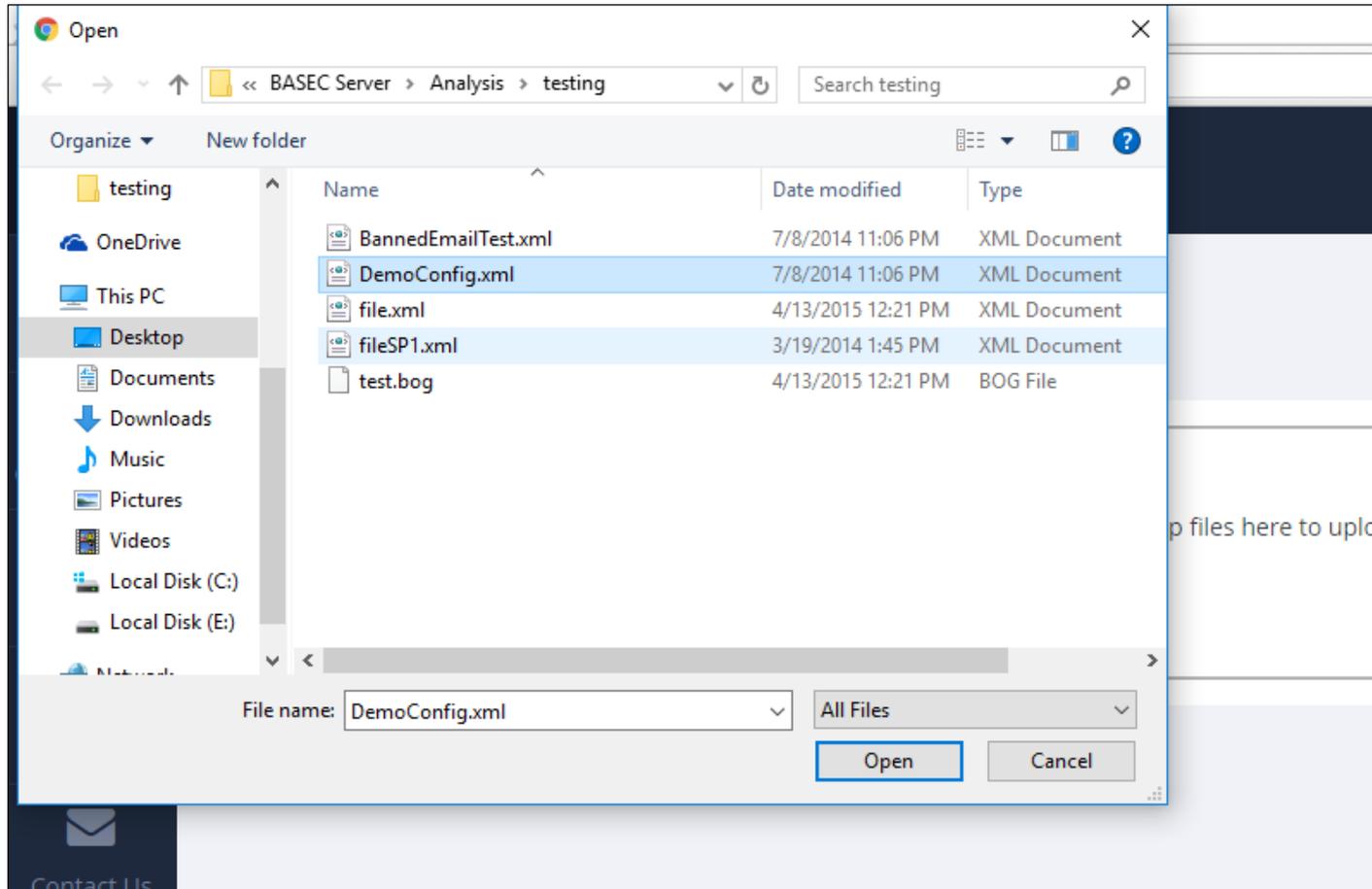
BASEC provides automated means to upload and analyze configuration files

Configuration Analysis



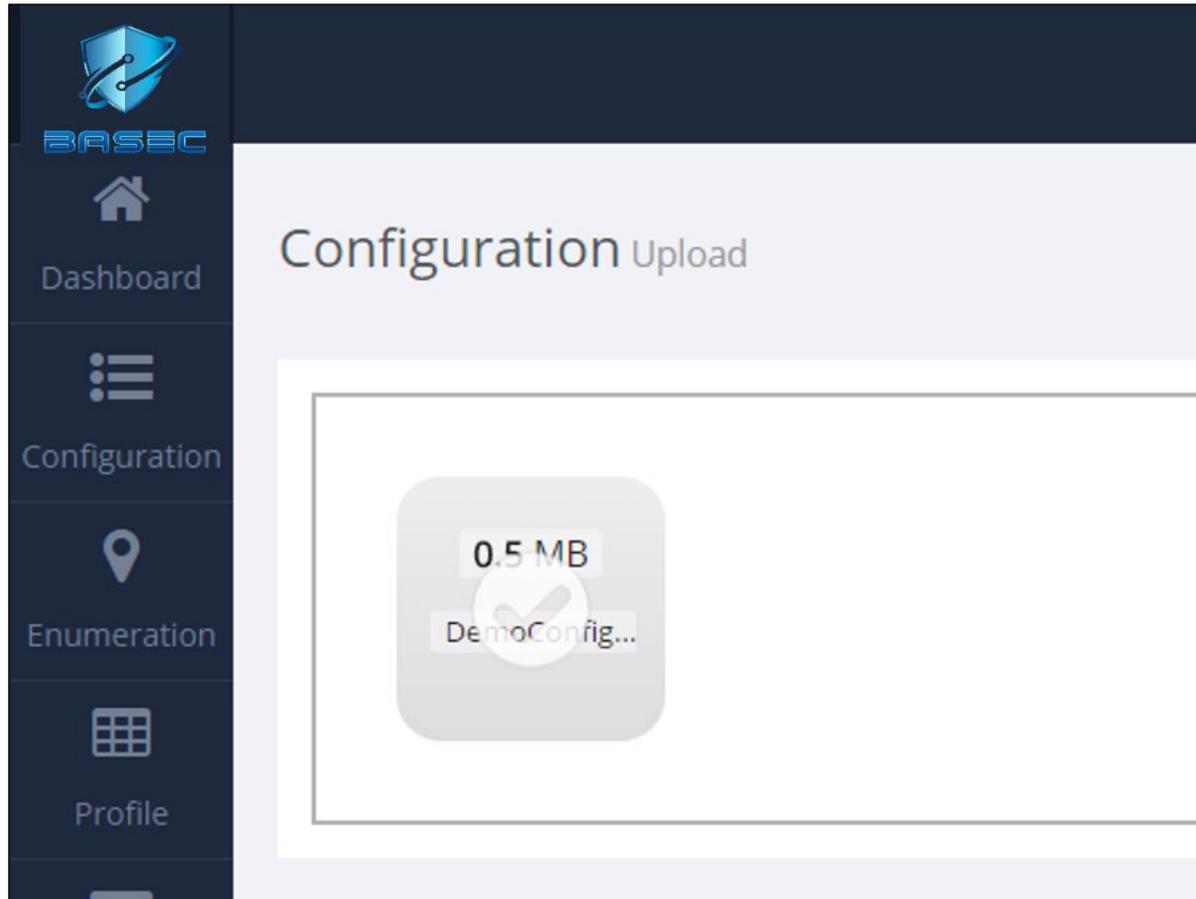
BASEC provides automated means to upload and analyze configuration files

Configuration Analysis



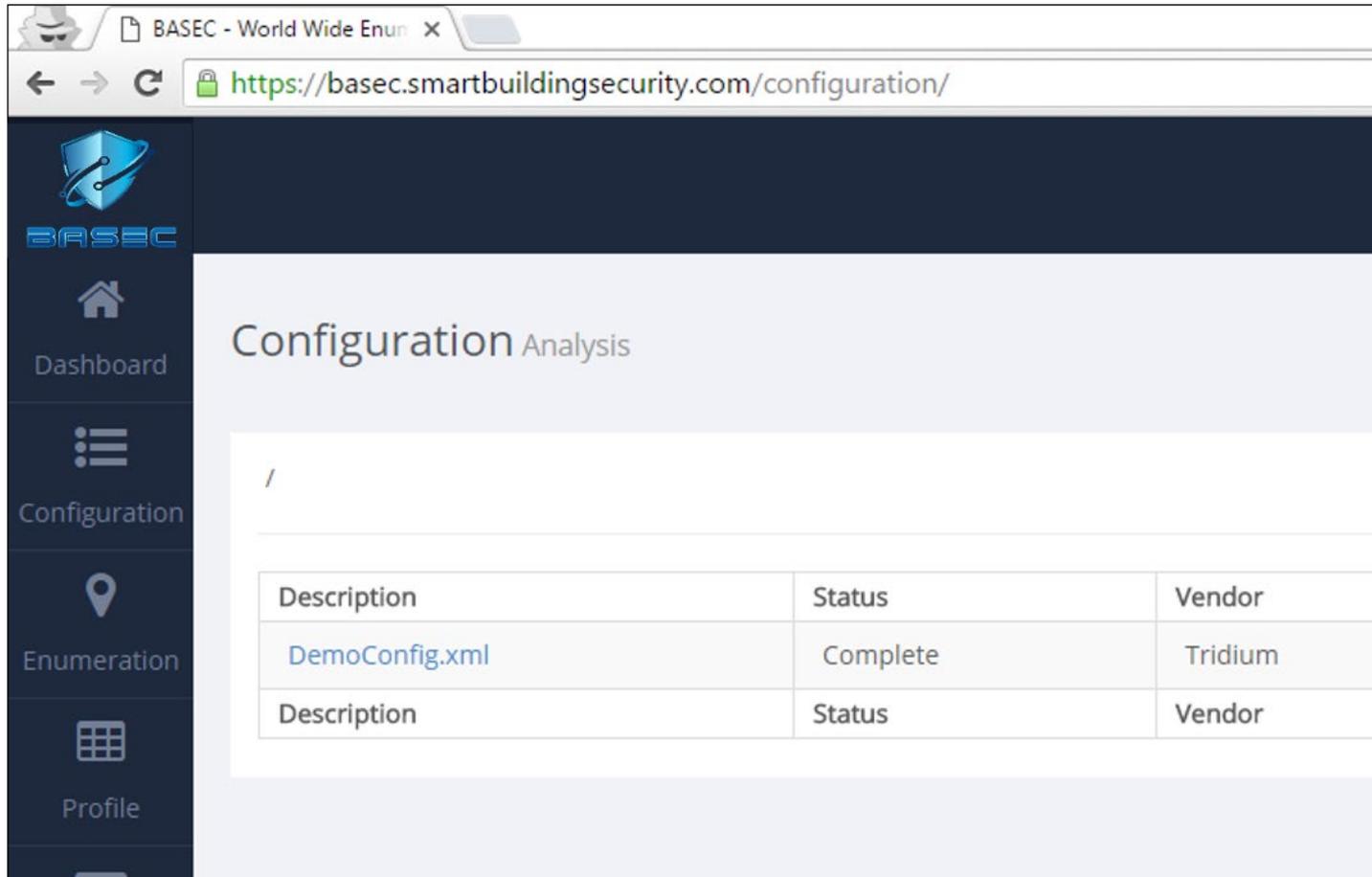
BASEC provides automated means to upload and analyze configuration files

Configuration Analysis



BASEC provides automated means to upload and analyze configuration files

Configuration Analysis

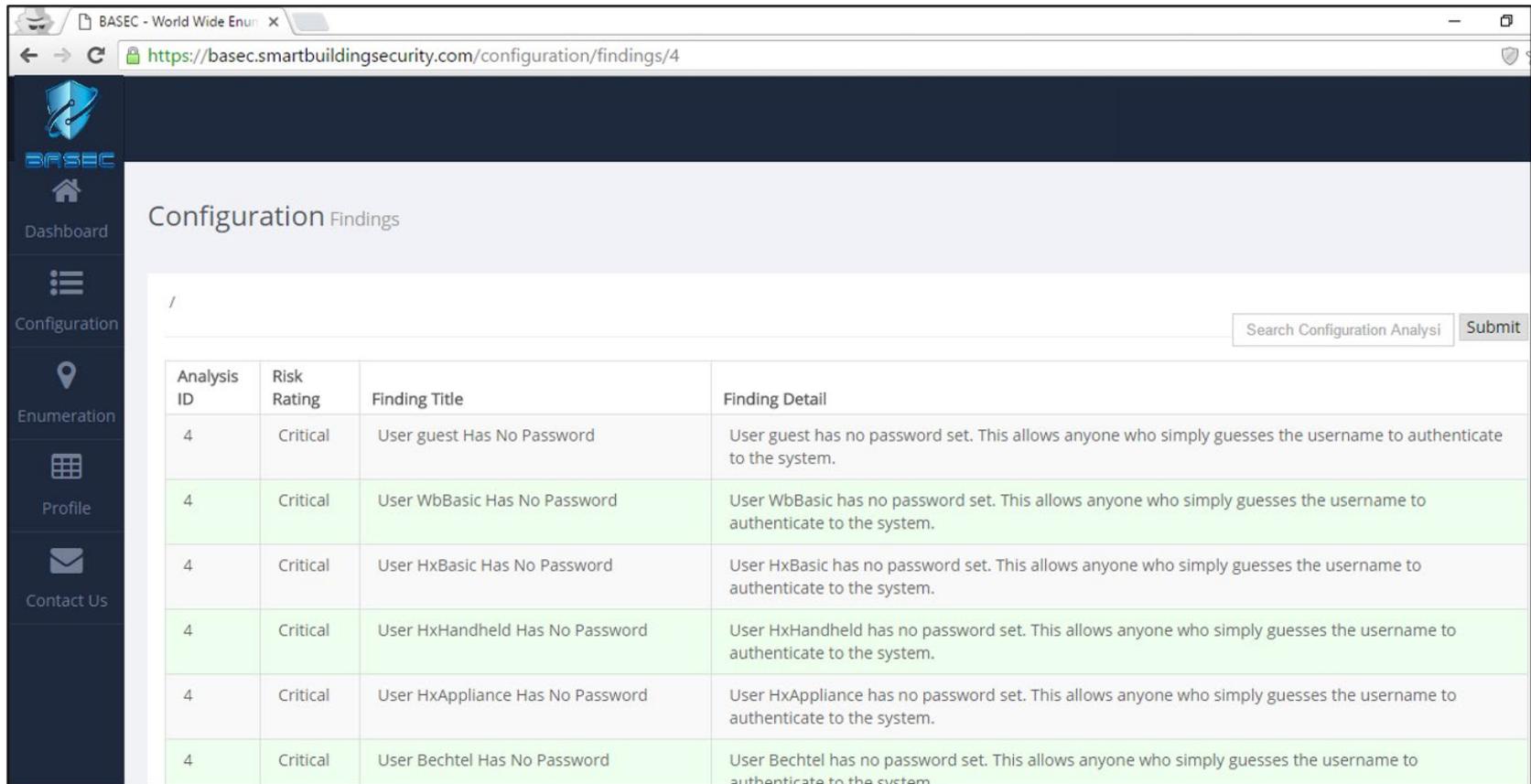


Configuration Analysis

Description	Status	Vendor
DemoConfig.xml	Complete	Tridium
Description	Status	Vendor

BASEC provides automated means to upload and analyze configuration files

Configuration Analysis



The screenshot shows a web browser window with the URL <https://basec.smartbuildingsecurity.com/configuration/findings/4>. The page title is "Configuration Findings". On the left is a dark sidebar with navigation icons and labels: "Dashboard", "Configuration", "Enumeration", "Profile", and "Contact Us". The main content area features a search bar with the text "Search Configuration Analysis" and a "Submit" button. Below the search bar is a table with the following data:

Analysis ID	Risk Rating	Finding Title	Finding Detail
4	Critical	User guest Has No Password	User guest has no password set. This allows anyone who simply guesses the username to authenticate to the system.
4	Critical	User WbBasic Has No Password	User WbBasic has no password set. This allows anyone who simply guesses the username to authenticate to the system.
4	Critical	User HxBasic Has No Password	User HxBasic has no password set. This allows anyone who simply guesses the username to authenticate to the system.
4	Critical	User HxHandheld Has No Password	User HxHandheld has no password set. This allows anyone who simply guesses the username to authenticate to the system.
4	Critical	User HxAppliance Has No Password	User HxAppliance has no password set. This allows anyone who simply guesses the username to authenticate to the system.
4	Critical	User Bechtel Has No Password	User Bechtel has no password set. This allows anyone who simply guesses the username to authenticate to the system.

BASEC provides automated means to upload and analyze configuration files

Configuration Analysis



Severity	Name
Critical	The Tridium instance is outdated and vulnerable to publically known vulnerabilites
Critical	The BACnet user account does not have a password
Critical	The Guest user account does not have a password
Critical	The WbBasic user account does not have a password
Critical	The HxBasic user account does not have a password
Critical	The HxHandheld user account does not have a password
Critical	The HxAppliance user account does not have a password
Critical	The Bechtel user account does not have a password
High	The Guest Account is Enabled
High	Banned Email Domain Used For Alerting (EmailRecipient)
High	Banned Email Domain Used For Alerting (EmailRecipient1)
High	User demo Has Weak Password (Length)
High	User tbs Has Weak Password (Length)
High	User ofacility Has Weak Password (Length)

BASEC provides automated means to upload and analyze configuration files

New User Interface

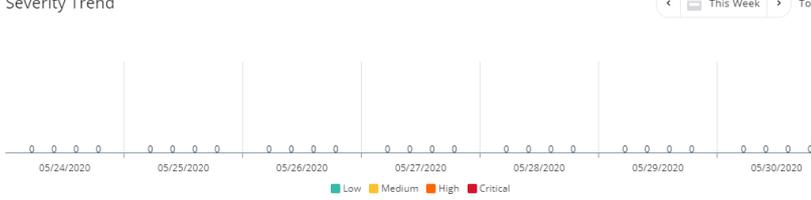
Dashboard

- Dashboard
- Configuration
- Enumeration
- IdM Settings

Dashboard

Severity Trend

< This Week > Total



Drop file here to upload

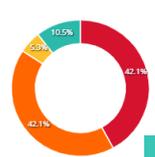
3
Completed Lifetime Scans & Reports

57
Total Lifetime Vulnerabilities

6
Low

24
High

3
Medium



14
Total Users

No users were

Configuration / Analysis

DESCRIPTION	STATUS	VENDOR	SUBMITTED	RISK RATING
1. DemoConfig (1).bog	Complete	Tridium	Jan 22, 2020, 10:24 p.m.	●
2. ESTCP_DEMO.xml	Complete	Tridium	Jan 17, 2020, 7:26 p.m.	●
3. BannedEmailTest.xml	Complete	Tridium	Jan 17, 2020, 3:33 p.m.	●

Overall Risk Distribution



Overall Vendor Finding Distribution



ESTCP Supported Efforts

- Core military installation assessments
 - Evaluated at six military installations
 - Four major vendors
 - Identified hundreds of misconfiguration vulnerabilities
- Training
 - Six training events in partnership with Idaho National Labs
 - 150 active duty, guard and civilians trained
 - Students from Army, Air Force, Navy, Space Force, Army Corps of Engineers
- Directives
 - Congressional Mandate National Defense Authorization Act 1650
 - RMF compliance

Observations

- **Trends**
 - Default configurations (78%)
 - Weak/default passwords (85%)
 - Unpatched systems (92%)
 - Internet exposure (12%)
 - Improper permissions/users (100%)
 - Common configuration used across installation (80%)
 - Fail to implement RMF controls (100%)
- **Implications**
 - Ability to remotely control systems
 - If one system compromised, all are compromised
 - No standard policy requirements
 - Reliance on third-party integrators
 - Active intrusion sets

ESTCP Project Updates

- **Assessment criteria**
 - Time required to evaluate configurations
 - Evaluation in seconds vs. hours
 - Effective across multiple sites/vendors
 - Multiple installations and vendors
 - Consistency in findings and reporting
 - Ability to incorporate with current DoD solutions
 - DoD DISA cloud-based solution
 - Trained users implementing during actual assessments
- **Enhance DoD capabilities**
 - Increase situational awareness
 - Incorporate standards
 - Automate RMF Capabilities
 - DoD scalable enterprise solution

Conclusions

- BASEC provides scalable means to identify, baseline, and certify cyber security configurations against RMF
- BASEC demonstrated the ability to rapidly identify vulnerable and misconfigured systems for DoD building and energy infrastructure
- Service components have been able to leverage BASEC for Congressionally mandated requirements
- BASEC provides solution that establishes and enforces cyber security standards for military installations at a significant cost reduction over current manual practices

SERDP & ESTCP Webinar Series

For additional information, please visit
<https://serdp-estcp.org/Program-Areas/Installation-Energy-and-Water/Energy/Conservation-and-Efficiency/EW18-5333>

Speaker Contact Information

j.butts@QEDsecure.com; billy.rios@QEDsecure.com
214-489-7767



Q&A Session 1



Physical Cybersecurity: Low-Cost Data Diodes for DoD Facility Equipment Monitoring

Colin Dunn, PE, CEM
Fend Incorporated

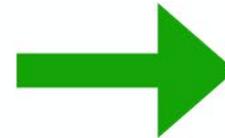


Agenda

- Connected infrastructure
 - Risks and benefits
- Data diodes
 - Tool for facility managers
- ESTCP project description
- Benefits to DoD

Connected Infrastructure: Real-Time Operational Awareness

Equipment Assets



Remote Monitoring



Efficiency



Business Interruption



Productivity

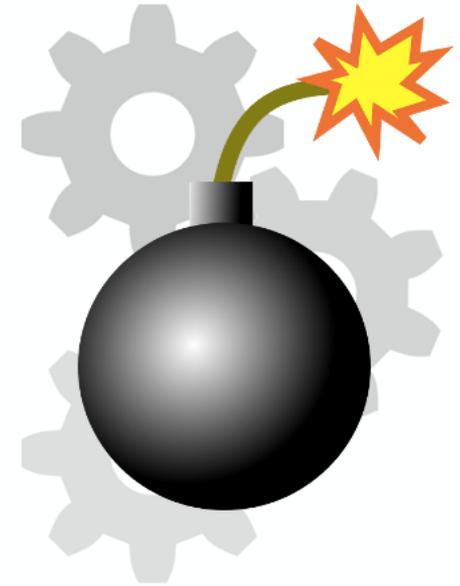
Connectivity Invites Attack



Steal Data



**Inject
Ransomware**



**Modify or Destroy
Equipment**

Cybersecurity Suite of Tools and Techniques



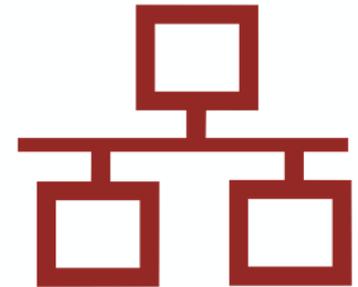
Policies and Training



Cyber Insurance



Air Gap



Dedicated Fiber



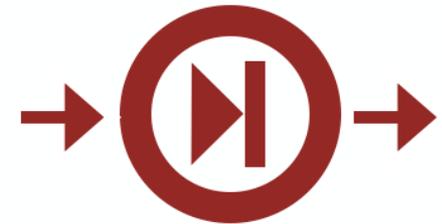
Firewalls



Software



Cloud-Based Threat Detection



Data Diodes

Data Diodes: Tomorrow's Go-To Solution for DoD Facility Managers



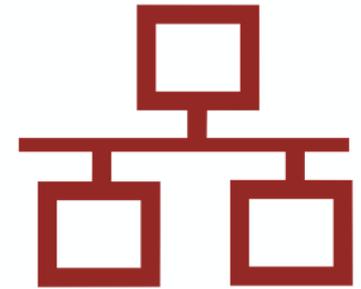
Policies and Training



Cyber Insurance



Air Gap



Dedicated Fiber



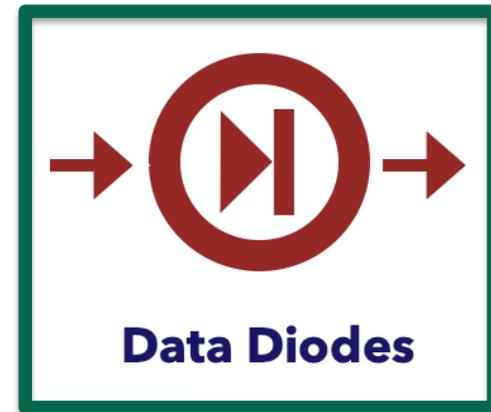
Firewalls



Software

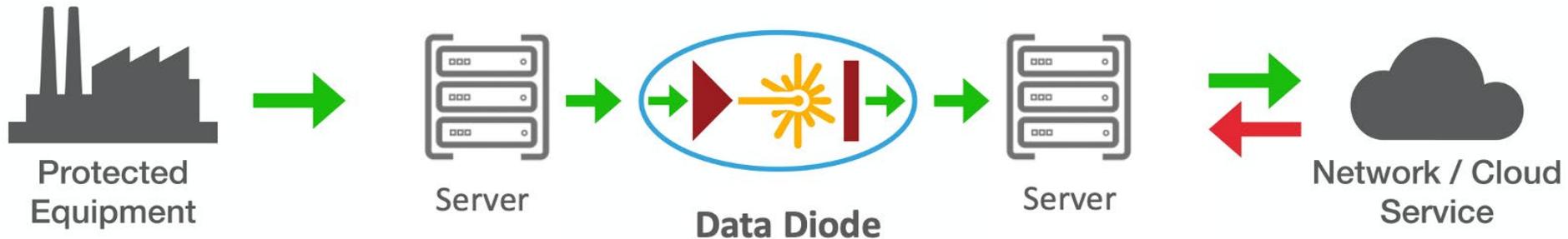


Cloud-Based Threat Detection



Data Diodes

Data Diodes Stop All Inbound Traffic



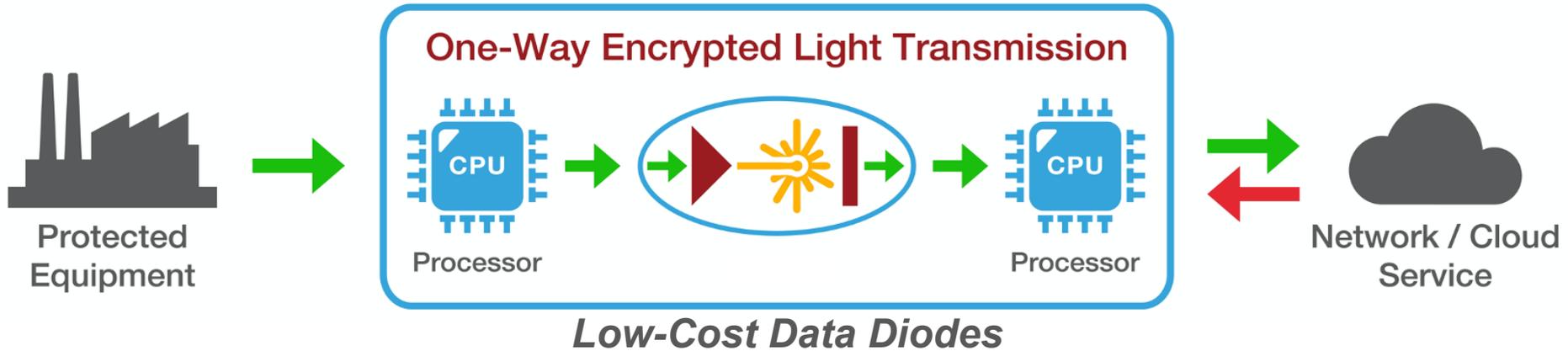
Benefits

- Physically enforced one-way data flow
- Cannot hack through network connection
- Used by nuclear facilities, water treatment plants, refineries and governments

Challenges for Widespread DoD Adoption

- Oversized for equipment monitoring
 - Data throughput up to 10 Gigabits per second
- Requires configuration of on-site servers by network engineers
- High costs
 - Typically \$30K to over \$100K per connection
- Limited domestic producers

New Industrial Diodes Provide Improved Usability and Costs

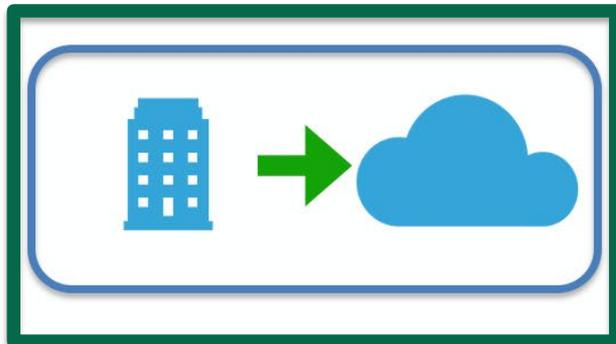


- Next generation
 - Low cost, no maintenance, onboard processors
- Ideal for Industrial Internet of Things equipment monitoring
- Serial or ethernet connections for new and legacy systems
- Straightforward installation
- Can bring legacy equipment safely into remote monitoring environments or the cloud



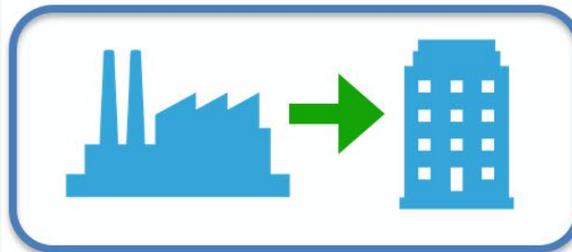
ESTCP Test Design and Objectives

- Overall goals are to demonstrate
 - Complete isolation of protected equipment
 - Interoperability with various equipment types
 - Ease of installation
 - Cost performance

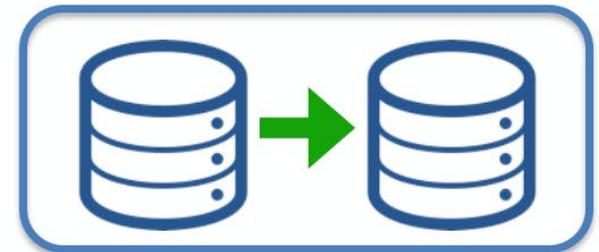


Remote Monitoring

Focus of this ESTCP Project

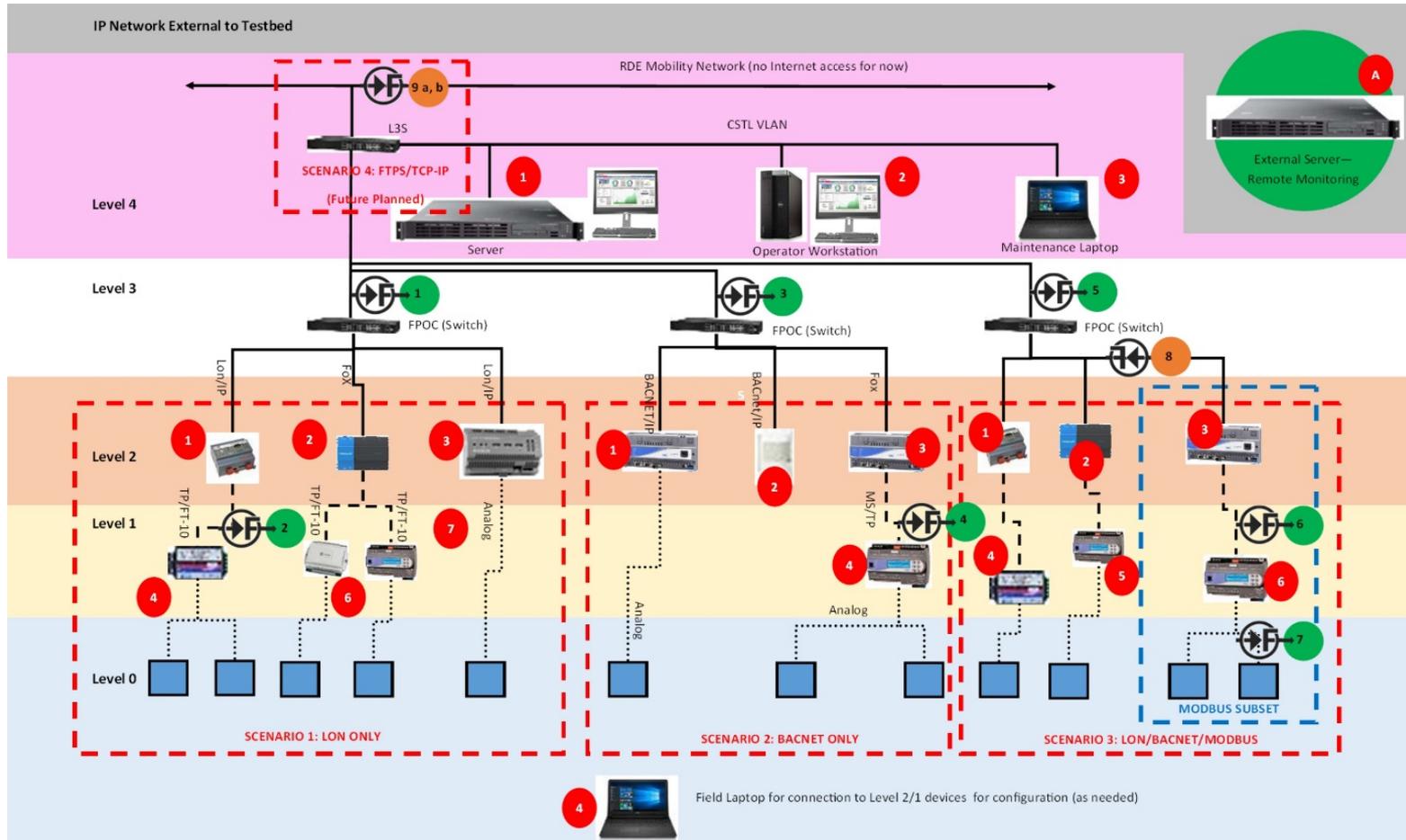


Operational Technology/
Informational Technology
Data Historian



Secure Database
Replication/ Backup

Compatibility Tests

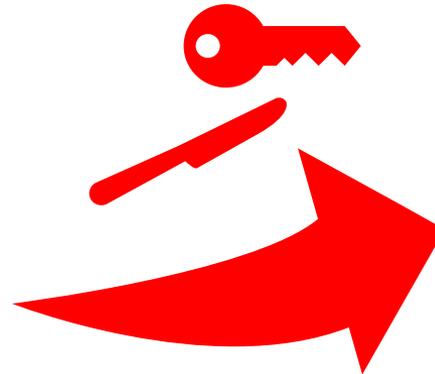


Confirm compatibility with the most commonly used machine communication protocols across DoD

Penetration Tests



Penetrate
Disrupt
Disable



Determine whether an attacker could disable or hack through the diode

Field Tests

- Facilities at Construction Engineering Research Laboratory (CERL)
- Additional sites
 - Navy
 - Air Force



Test building at CERL

Benefits to DoD

- Increased access to building performance data
- Compliance with cybersecurity requirements
- Integration of data from multiple disparate sources
- Improved operational efficiency
 - Energy and manpower

Conclusions

- Remote monitoring
 - Powerful tool when deployed securely
- Data diodes
 - Physical cybersecurity
 - Now a practical alternative to traditional defenses
- Benefits
 - Increased operational resilience and energy efficiency

SERDP & ESTCP Webinar Series

For additional information, please visit
[https://www.serdp-estcp.org/Program-Areas/
Installation-Energy-and-Water/Energy/
Conservation-and-Efficiency/EW19-5156](https://www.serdp-estcp.org/Program-Areas/Installation-Energy-and-Water/Energy/Conservation-and-Efficiency/EW19-5156)

Speaker Contact Information

cdunn@fend.tech; 571-970-1382 x700



Q&A Session 2



The next webinar is on
July 23, 2020

*Predicting PFAS Fate and
Transport in Subsurface
Environments, and Treatment*



Survey Reminder

Please take a moment to complete the survey that will pop up on your screen when the webinar ends

