NATIONAL CYBER

# OT/ICS SECURITY OPERATIONS CENTER

*An OT SOC built upon threat informed defense reduces organizational risk by detecting attacks early before they impact the organization and system availability.*

Booz Allen's National Cyber Platform understands the challenges an Operation Technology (OT) Cyber Security Operations Center (SOC) faces in their mission to combat today's threat, the value of incorporating threat intelligence to build a threat informed defense, and the necessities of regulatory and compliance requirements. The Cyber-Physical Defense team at Booz Allen takes pride in helping to secure our nation's most critical infrastructures with over 200 credentialed OT cybersecurity professionals and experience across all 16 Critical Infrastructure sectors.

## KEY THREAT DETECTION OBJECTIVES

1. Minimizes Impact to the OT Environment
2. Increases Visibility to the OT Environment
3. Enables Actionable Alerting
4. Ensures Appropriate Personnel are Ready to Respond
5. Facilitates Effective and Collaborative Response

## BOOZ ALLEN'S *PROVEN* DEPLOYABLE SOC CAPABILITY

1. From-the-ground-up SOC builds
2. Maturity assessments to assist organizations with existing SOC modernization.
3. Threat Intelligence integration to assist organizations build a threat informed defense.
4. Tool deployments to improve SOC visibility and achieve faster detection/response capabilities.
5. Tradecraft-focused detection engineering (ATT&CK, ATT&CK for ICS).

**ASSESS**
Integrate threat intel to develop use cases to build threat-informed defense

**DESIGN**
Formulate detection analytics based on threat intelligence use cases following precision and recall principals

**IMPLEMENT**
Turn detection analytic into identified detection tool syntax

**TUNE**
Tune component ruleset and alerting specifications to reduce false positives and focus team on high fidelity alerts

**MONITOR**
Deploy SOC for information sharing, continuous monitoring, detection, and response

## CAVALIER BRINGS IT ALL TOGETHER

Cavalier is a unified stand-alone security platform for SOC analysts, managers, and incident responders to work in a centralized security management console. Cavalier allows users to manage assets, events, and cases across their environment and platforms without having to individually log into each tool. Manage all the data, securely, at scale and mission speed.

- API Handler allows for a lightweight solution preventing duplicate datasets and high-indexing loads.
- Panels display data from all supported tools & platforms ensuring minimal display loading with dashboards.
- Based on a Docker framework for containerized module integration.
- Built in Unity and Go for speed and efficiency.
- Accumulo database enables Role-Based Access Control (RBAC) to store classified data from CUI to TS.
- Fully customizable user workspace.

## WHY BOOZ ALLEN?

Harness decades of experience in uncommon skillsets in weapon systems, automotive systems, ICS/SCADA systems, IoT, medical technologies, and other Cyber-Physical Systems. Booz Allen has deep experience in the federal and commercial markets supporting complex Cybersecurity assessments, risk management, and solutioning to include conducting red, blue, and purple team assessments, Mission-Based Cyber Risk Assessments, and much more.

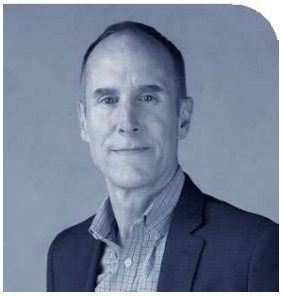
## OUR SERVICES AND APPROACH

Securing critical OT/ICS infrastructure from today's advancing threats requires a cutting-edge and innovative approach. Our approach to establishing an OT monitoring and threat detection program enables broad visibility across the environment while also establishing the processes and personnel training to make it endure.

## ABOUT BOOZ ALLEN

Booz Allen Hamilton has been at the forefront of strategy, technology, and engineering for more than 100 years. Booz Allen partners with private and public sector clients to solve their most pressing problems.

## CONTACT INFORMATION



**DAVID FORBES**
CYBER-PHYSICAL DEFENSE DIRECTOR
FORBES_DAVID@BAH.COM

**BRANDON GRIMES**
LEAD ASSOCIATE
GRIMES_BRANDON@BAH.COM