From Indicators to Insight: Operational Validation of Behavior-Based Cyber Detection in a Live Biotechnology SOC

CFP Submission for CyberBio 2026

Charles Frick, Johns Hopkins Applied Physics Laboratory

Session Overview

This presentation provides a first-hand account of an operational pilot that moved Indicators of Behavior (IOB) from research into a live production Security Operations Center (SOC). Conducted on the HudsonAlpha Institute for Biotechnology campus, the pilot evaluated whether behavior-based cyber threat intelligence could improve detection fidelity, reduce analyst workload, and integrate cleanly with existing SOC tools and workflows.

The pilot was executed over approximately three months, with IOB analytics running continuously in production. Unlike laboratory demonstrations or tabletop exercises, this effort intentionally exposed the analytics to real background noise, operational constraints, and mission-critical data flows associated with active genomic research.

Technical Approach

IOBs were implemented as STIX 2.1 bundles containing:

- Explicitly defined adversary behaviors mapped to MITRE ATT&CK
- Detection analytics translated into the partner's SIEM
- BPMN-based correlation and scoring workflows executed via SOAR
- Operator notification thresholds based on behavioral co-occurrence, not individual alerts

Operational Use Cases

Two adversary scenarios structured the evaluation:

1. **Data Theft in a Multi-Tenant Network**

2. **Genomic Data Integrity Compromise**

Across both use cases, alerts were generated within five minutes of the final observed behavior, with zero false positives.

Results and Impact

Key outcomes from the pilot include:

- **Zero false-positive alerts** across ~90 days of continuous operation
- **Complete suppression of alert fatigue**, with operators receiving only validated, high-confidence notifications
- **Earlier detection** compared to manual analysis, which can take weeks to identify similar patterns
- **No disruption** to SOC workflows or research operations during deployment

These results confirm that behavior-based correlation is not only feasible in production, but operationally advantageous—particularly in environments with high data volume, diverse tenants, and limited endpoint visibility.

Audience Takeaways

Attendees will leave with:

- A concrete understanding of how IOBs function in live SOC environments
- Practical insight into integrating behavior-based analytics with existing SIEM and SOAR platforms
- Measured performance data supporting IOB adoption
- Lessons learned for transitioning emerging cyber analytics from research to operations

This session is particularly relevant for SOC leaders, threat intelligence teams, government stakeholders, and organizations seeking scalable, low-noise detection strategies for complex operational environments.