# ANTISOC™

New from BHIS, the ANTISOC™ is just what it sounds like – a red team operations center. Based on customer and tester feedback, we created this offering to expand upon the traditional point-in-time penetration test.

## ANTISOC™ Benefits

### Follow the Threats

Attacker techniques are constantly evolving. ANTISOC™ operators work to emulate recently disclosed attacks against our customers, reporting their success or failure.

### Expanded Timelines

More time means we can pursue attacks that are not feasible during traditional short-term engagements, and lay low when identified by defenders.

### Tailored Fit

ANTISOC™ is built with open scoping in mind, but rules of engagement are defined on a per-customer basis.

### Reworked Reporting

Reports are delivered in real-time via a ticketing system, combined with quarterly debrief presentations detailing overall risk, findings, and detection metrics.

# One Year of ANTISOC™

## Initial Access Attempts

- Reconnaissance
- Password Guessing
- Web Application Exploitation
- Phishing
- N-day Exploits

## Assumed Compromise

- Valid Accounts
- Trusted Agent Execution
- Deploy Drop Device/ Implant VM
- Cloud Attacks (i.e key disclosure, illicit consent grants)

## Post Exploitation

- Information Gathering
- Lateral Movement
- Privilege Elevation
- Pursue Pre-defined Goals

## Purple Team

- Collaborative Meetings
- Overt Testing
- Build Detections
- Re-execute Previous Attacks

## Continuous Activities:

- Vulnerability Scanning
- Tool Development
- Data Breach Analysis
- Training
- Your ideas here, we take requests!