CYBERSECURITY

# SERVICES OVERVIEW

MorganFranklin Consulting
A Vaco Company

## A Cyber Fusion Center That Optimizes Your Security Solutions

Our Cyber Fusion Center is the culmination of security operations and monitoring resulting from the combination of a Cybersecurity Operations Center (CSOC) with adjacent supporting services including threat intelligence, threat hunting, detection engineering, security engineering and architecture, digital forensic, malware analysis, purple team testing and validation, and incident response.

### Enhance Efficiency and Maximize Results by Aligning CSOC and Its Supplementary Services.

Each service consumes inputs from CSOC and produces outputs to CSOC that enhance monitoring and response with timely information about emerging threats, linear analysis of Indicators of Compromise (IOC) and observable threat actor activity, support for retrospective analysis of security telemetry, enhancements and maturity in existing detection capabilities, gap analysis of detection and response tooling, deep-dive analysis of artifacts collected by CSOC, and support for complex incidents and incident response.

A Cyber Fusion Center enables an evolving security capability that matures overall monitoring, detection, and response continuously over time. At MorganFranklin, **we believe that Cyber Fusion Center is the next generation of CSOC offering,** providing demonstrable value over the traditional CSOC approach.

## Why MorganFranklin?

We secure a comprehensive understanding of your enterprise level needs, recognizing that cybersecurity incidents can have a direct and immediate impact on revenue and reputation.

- **Dedicated experts and tailored service.** We provide a named team of highly experienced and certified security professionals who have built robust CSOC monitoring and SIEM engineering functions for global organizations.
- **Tierless model.** Our analysts operate across all traditional tiers (initial investigation and triage, suspected true positive, incident handling and remediation), owning incidents and all alerts from investigation to resolution.
- **Your tools, our people.** We operate in your environment (e.g., SIEM, ticketing system, tech stack) and with your preferred tools.
- **Extension of your team.** Our analysts are credentialed in your organization and operate as an extension of your security team to augment your capabilities.
- **Ongoing transparency.** We will provide weekly metrics and Quarterly Business Reviews (QBR) to measure and demonstrate improvement over time.
- **Experience across technology stacks.** Our teams have experience, certification and training across several security and technology solutions, tools and processes.

How Business
MOVES FORWARD

www.morganfranklin.com/cybersecurity

## Our CSOC Services

More Than Just Monitoring

**Our Cybersecurity Operations Center (CSOC) is continuously monitoring and responding**. We are always on duty, watching for threats, responding to alerts and improving the environment by updating documentation, researching new trends or tuning your tools.

### Threat Intelligence

Respond to analysts requests for intelligence (RFI) and provide expert research to enhance Indicators of Compromise (IOC) or adversary tactics/tools, techniques or procedures (TTP); generate new content for detection engineering, threat hunting, and continuous monitoring.

### Threat Hunting

Provide hypothesis-driven retrospective searches to ensure that nothing has "slipped through the net" over time and evaded detections. Work in tandem with our CSOC, Threat Intelligence and Incident Response teams to provide ongoing validation for current and emerging threats and vulnerabilities.

### Testing & Validation

Perform quarterly adversary simulations (purple team tests) mapped to MITRE ATT&CK to ensure that the CSOC has the visibility to find intrusions and to map ability to prevent attacks.

### Engineering & Architecture

Evaluate an organization's security controls, recommend improvements and assist with onboarding to ensure maximum visibility and value from an organization's security stack.

### Incident Response

Provide at-the-ready trained digital forensic investigators and incident responders (DFIR) to assist with complex, large-scale incidents. From identification to remediation and containment, our DFIR team is prepared to supplement a client's security team's ability to respond to incidents.

## We Provide Deep Professional Experience

### TEAM QUALIFICATIONS

- Our professionals bring deep expertise and various credentials including:
- Industry recognized certifications such as CompTIA Security+ and CySA+ or are scheduled to sit for those exams
- Certifications in vendor solutions such as Microsoft SA-200 (Microsoft Security Operations Analyst), Splunk Fundamentals or other tool specific training
- Academic degrees from global institutions including bachelor's and master's degrees
- Former members of military, government intelligence, and law enforcement

### ONGOING DEVELOPMENT

Our people are our strongest asset, and MorganFranklin is committed to the ongoing growth and professional development of everyone on our team. Each analyst on our team has a personalized training and development roadmap.

### 24x7x365 FOLLOW-THE-SUN MODEL

**We operate with shifts distributed across geographies** for redundancy. Each shift is aligned to local daytime. Our analysts are distributed across telecom providers for resiliency and operate via VPN or encrypted remote connections.