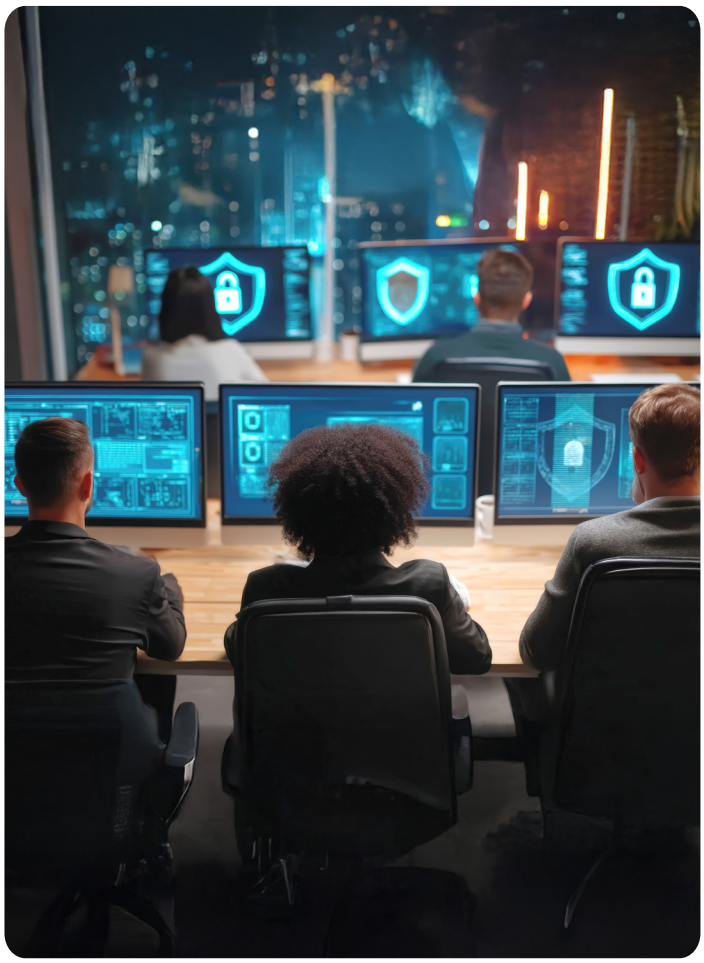
MANTECH™
ALWAYS ADVANCING

MANTECH's Cell-Based SOC

The Next-Generation Security Operations Center

The Evolving Federal Cyber Landscape

The cybersecurity landscape is in a state of constant, rapid evolution. Federal agencies face the challenge of building scalable, resilient and secure digital environments that can support their critical missions while withstanding persistent and sophisticated cyber threats.



For 57 years, MANTECH has served as a trusted advisor to government clients across the Defense, Intelligence and Federal Civilian sectors. We are an elite cyber provider focused on driving mission outcomes through:

- Cyber Engineering
- Cyber Operations (Offensive and Defensive)
- Cyber Analytics

We deliver efficiency and excellence on both the offensive and defensive sides of the cyber fence, fundamentally advancing our federal clients' missions. Understanding how to take advantage of vulnerabilities makes MANTECH well positioned to defend against those same vulnerabilities. At MANTECH, we are ***ALWAYS ADVANCING***.

The Traditional Security Operations Center

A Security Operations Center (SOC) is an organization responsible for the continuous monitoring of critical networks to thwart in-process cyberattacks and provide high-end analysis, forensics and threat-hunting services. The bedrock of any SOC is built on three key characteristics:

- **People:** Dedicated teams of security professionals, including analysts, incident responders and threat hunters, who use their expertise and critical thinking to monitor, investigate and respond to threats.
- **Processes:** A well-defined set of procedures and workflows, such as incident response playbooks and forensic analysis procedures, that ensure consistency and effectiveness from detection to resolution.
- **Technology:** A robust suite of security tools, including Security Information and Event Management (SIEM), Endpoint Detection and Response (EDR) and Security Orchestration, Automation and Response (SOAR) and AI platforms.

MANTECH International Corporation. All Rights Reserved.

Challenges of the Traditional Model

Traditional SOCs are often structured as a tiered system (Tier I, II and III). This model creates significant inefficiencies and risks:

- **Hand-off Delays:** Critical time is lost as incidents are passed from one tier to the next.
- **Case Backlogs:** The tiered structure often results in bottlenecks, leading to significant backlogs of unaddressed issues.
- **Inexperienced Decision Makers:** Tier 1 personnel—the least experienced—are often responsible for making the initial, critical decisions.
- **High Turnover:** The repetitive and often unfulfilling work of the lower tiers contributes to high employee turnover and burnout.

The MANTECH Cell-Based SOC: A New Approach

To overcome the inefficiencies of the traditional model, MANTECH has developed and successfully deployed a new, next-generation approach: the Cell-Based SOC. Instead of organizing by experience in tiers, this first-of-its-kind model for the federal government aligns personnel into functionally-aligned cells that are enabled and empowered to deliver value-added outcomes.

For example, instead of passing an incident from one person to the next, a single detection cell is responsible for a complete outcome—seeing a ticket through its entire lifecycle to resolution. This model creates a cohesive and more efficient workflow, giving a team full responsibility and accountability for an outcome of measurable value.

Transformational Advantages

The Cell-Based SOC is designed to unlock the full potential of human capital and drive dramatic improvements in security outcomes.

- **Faster Resolution Times: The median time to resolve a security incident has been reduced by 75%, with more than 95% of cybersecurity incidents resolved in less than 15 minutes**, averaging six minutes per response. This approach has also **reduced ticket backlogs by over 70% for our federal clients**.
- **Increased Analyst Time on Target:** Our cell-based model achieved **90% reduction in false positives** through alert refinement, new rules, advanced analysis techniques and integrating threat intelligence. Advanced tagging and correlation strategies help us identify the real threats and better prioritize employees' valuable time.
- **Enhanced Career Development:** By empowering individuals to see incidents through to resolution, the Cell-Based SOC provides on-the-job training, accelerating career development and significantly improving staff retention and morale.

Driving Financial and Mission Value

In today's resource-constrained environment, financial efficiency and a focus on FinOps are crucial. The Cell-Based SOC is radically more efficient than the tiered model, delivering better security outcomes while driving down costs. Importantly, the Cell-Based SOC model provides value to the taxpayer by focusing on quick resolution and reducing hand-off delays.

This model is a prime example of how MANTECH is ***Always Advancing*** our clients' missions. By increasing the nation's security posture with more efficient and reliable cybersecurity, we enable federal employees to focus on their core missions, maximize business value and lower long-term operational costs.

In business more than 57 years, MANTECH excels in cognitive cyber, AI, data collection & analytics, enterprise IT, systems engineering and software application development solutions that support national and homeland security.

LEARN MORE

Tim Schaad, Federal Civilian Sector Technical Director | timothy.schaad@MANTECH.com