Our People...Your Edge

EDGEWATER

FEDERAL SOLUTIONS

SOC Monitoring
Seamless SOC Support for Mission-Critical Operations

At Edgewater, we provide expert-level Security Operations Center (SOC) monitoring tailored to protect the Nation's most vital information. With **24x7x365 coverage**, our solutions seamlessly integrate into existing Government operations, delivering **real-time alert triage, in-depth threat analysis, and swift response to emerging cyber threats.**

Key SOC Monitoring Capabilities

24/7 Monitoring and Escalation:
Ensure around-the-clock protection with real-time alert triage and rapid response.

Break Down Silos:
Our analysts are trained to interface with Cyber Threat Intel, Detection Engineering, Threat Hunt, and Offensive Cyber teams.

Reduce Dwell Time:
Improve response time across the board with SOC analysts who are expertly trained in initial detection, triage, and rapid escalation of security events.

Playbook-Driven Alert Triage:
Pre-defined triage and response playbooks are customized to meet federal regulations and the specifics of your enterprise, ensuring rapid and accurate alert handling.

Continuous Up-Skilling:
From purple team engagements to mentorship programs to SANS certification allowances, our Tier-1 SOC analysts stay current with industry and adversary trends.

Use Your Stack or Ours:
Seamless integration with existing tools to avoid disruption and maximize current security investments.

Attack Surface Reduction

Detection Engineering

Incident Response

Cyber Threat Intelligence

Threat Hunting

Malware Analysis

Offensive Cyber Emulation

SOC Monitoring

Forensics

Edgewater offers one-of-a-kind Managed Detection and Response stacks for Federal Agencies.

Full Spectrum Cyber Ops

Experience Defending Against
Advanced Adversaries

Supply Chain Attacks

- Solar Winds
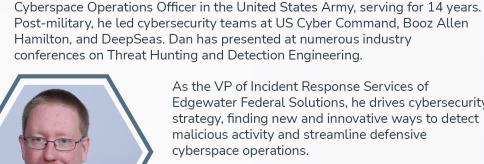- MoveIT
- CyberHeaven Chrome Extensions

Ransomware

- Akira
- Lockbit
- Maze

Zero Days

- Hafnium Exchange (CVE-2021-26855)
- Citrix session Hijacking (CVE-2023-4966)
- Confluence (CVE-2023-22515)

Meet our SOC Monitoring Expert

Dan Rossell is a cybersecurity expert with over twenty years of expertise across the government, military, and private sectors. Dan began his career as a Cyberspace Operations Officer in the United States Army, serving for 14 years. Post-military, he led cybersecurity teams at US Cyber Command, Booz Allen Hamilton, and DeepSeas. Dan has presented at numerous industry conferences on Threat Hunting and Detection Engineering.

As the VP of Incident Response Services of Edgewater Federal Solutions, he drives cybersecurity strategy, finding new and innovative ways to detect malicious activity and streamline defensive cyberspace operations.

Dan Rossell
VP of Incident Response Services

Gartner Alignment ★

Managed Security Services (MSS)
Professional Services

About Edgewater

bsi.

ISO 9001 Quality Management	ISO/IEC 20000-1 Information Technology Service Management	ISO/IEC 27001 Information Security Management
FS 575425	ITMS 667027	IS 667026

CMMI SVC /3 SM
CMMI8V2.0 / Exp. 2025-04-25 / Appraisal #59033

CMMI DEV /3 SM
CMMI8V2.0 / Exp. 2025-04-25 / Appraisal #59033

Secure Your Environment with Edgewater

Trust Edgewater to keep your mission-critical systems secure, so you can focus on driving your mission forward. Connect with our team to unlock SOC monitoring today.

Visit: www.edgewaterit.com
Email: cyber@edgewaterit.com
Call: 301-874-8566