LevelBlue
Public Sector

The LevelBlue Advantage for Secure Government and CMMC Compliance

Partner with the first and only pure-play MDR provider with full FedRAMP authorization for CMMC readiness.

Simplifying CMMC compliance

LevelBlue Public Sector specializes in serving the federal, state, and local agencies, Defense Industrial Base (DIB), and other organizations requiring US data sovereignty. As a vendor-agnostic managed security services provider, LevelBlue provides GCC high services and is the only FedRAMP moderate authorized MDR pure-play with a SOC managed exclusively by cleared personnel.

LevelBlue has a proven history of assisting the DIB with CMMC compliance by delivering full MDR and Co-Managed SIEM/SOC as well as CMMC-focused professional services. As a Cyber-AB accredited Registered Provider Organization (RPO), our team uses the official CMMC Readiness Tool (CRT) to effectively manage compliance gaps and remediation efforts. For clients needing more support, TGS collaborates with MSPs to provide "IT boots on the ground" services, streamlining the CMMC process for members of the DIB seeking to be CMMC compliant.

CMMC core capabilities:

Cyber Advisory:

Digital Forensics and Incident Response

24×7 rapid response to a cybersecurity breach and proactive response to readiness services to strengthen security posture.

Threat Detection and Executive Training

Illuminate threats and vulnerabilities for protection from threat actors. Equip leaders with knowledge and expertise to combat the evolving threat landscape.

Roadmaps and Readiness Assessments

Identify security gaps, deliver tailored risk insights, and outline prioritized actions to meet CMMC requirements.

Security Testing Services:

Pen Testing and Attack Simulations

Conduct testing and real-world attack scenarios across your networks, applications, and databases to reveal vulnerabilities in alignment with CMMC.

Benefits to customer

- Quick ROI: Our vendor-agnostic abilities, world-class offerings, and proven use cases allow LevelBlue to get a client to ROI quicker than others.
- Access a team of LevelBlue consultants with deep subject matter expertise in CMMC to help mitigate risk from threat actors and maintain compliance.
- Our experts will create and/or refine your processes and playbooks.
- Achieve greater visibility into the data assets you are responsible for securing.
- Identify security weaknesses and corrective actions to meet CMMC requirements.
- Proactively protect your security investments from potential vulnerabilities.
- Ensure preparedness for upcoming visits from third-party assessors.
- Receive a pre-assessment security check to remediate any deficiencies.
- Receive a pass or fail from our Cyber-AB accredited team for CMMC readiness.

Supported technologies:

- EDR/XDR: Microsoft Defender, Palo Alto Cortex, CrowdStrike, SentinelOne and Carbon Black.
- SIEM: Microsoft Sentinel, Splunk, LogRhythm and IBM QRadar.

Gap Analysis

Identify key weaknesses or deficiencies in your current security programs vs CMMC requirements.

Managed Security Services:

Managed Threat Detection and Response (MDR)

Eliminate active threats with 24×7 threat detection, investigation, and response.

Co-Managed SIEM/SOC

Maximize your SIEM investment, stop alert fatigue, and enhance your team with hybrid security operations support.

Proactive Threat Hunting

Fortify your security defenses by identifying hidden attackers and open threat vectors that can lead to a breach.

Security Technology Management

Monitor, tune, and update your devices for optimal performance and improved defenses.

Partner success examples: Average deal size $669,010

Defense Contractor

Client Chose LevelBlue because of FedRAMP capabilities

The Challenge

- Company serves as a subcontractor for Department of Defense and other federal agencies.
- To retain their competitive advantage, the company needed to achieve CMMC compliance.
- They sought an MSSP with FedRAMP authorization to ensure they meet CMMC controls.

The Solution

- FedRAMP Compliant Managed Detection and Response (MDR) for Microsoft Defender
- Deal closed in 2 months!
- TCV $178K

Client Feedback: Why LevelBlue Won

- LevelBlue solution provides them with a competitive advantage to bid and increase their ability to win new projects.
- LevelBlue has demonstrated extensive experience in helping clients of all sizes meet CMMC requirements and provides a key differentiator in the FedRAMP marketplace.

Architecture and Construction Client

Client chose LevelBlue because of FedRAMP-related capabilities

The Challenge

- Client is a US-based architecture firm that works with several federal agencies to design federal buildings.
- Company needed to achieve CMMC compliance. They sought a Managed Security Services Provider (MSSP) with FedRAMP authorization to ensure they could meet CMMC requirements.

The Solution

- FedRAMP Compliant Managed Detection and Response (MDR) for Microsoft Defender
- Deal Closed in 1 month!
- TCV $209K

Client Feedback: Why LevelBlue Won

- Client selected LevelBlue as they could help them meet CMMC requirements and do so more quickly than other providers.

Key questions for clients

1. Are you familiar with CMMC and its role for DoD contractors?
2. Have you started preparing for certification? If so, what challenges have you faced?
3. What CMMC level (2 or 3) are you required to comply with?
4. Are you working with a CMMC consultant or handling controls internally?
5. Do you have MDR/Managed SIEM with an MSSP that meets CSP/ ESP requirements under DFARS clause 252.204-7012?
6. Are ITAR requirements applicable to your products? If yes, does your MSSP staff comply with US-only SOC/IR support?
7. Do you have FedRAMP requirements for your service provider?
8. Is your organization using M365 GCC or GCC High? What license tier (E3, E5, G5)? Are you utilizing Defender(s) and Sentinel?
9. Are you using FedRAMP-compliant EDR tools like CrowdStrike, Palo Alto Cortex, or SentinelOne?
10. Are you using FedRAMP-compliant SIEM tools like Splunk instead of Microsoft?

Contact Us

Speak with your LevelBlue account executive, or see our Government Solutions web page at levelblue.com/solutions/government