SENTINELBLUE
OVERWATCH

SOLUTION BRIEF

365 Security Monitoring, Threat Detection, & Incident Response with SOC-as-a-Service

SENTINEL BLUE OVERWATCH

Small and mid-sized defense contractors need to monitor, detect, and respond to cybersecurity threats with all the speed and decisiveness of a well-resourced enterprise, but without the overhead of building an in-house SOC. Overwatch can help.

Stay Aware With Overwatch

Purpose-built for the Defense Industrial Base and CMMC environments, Overwatch delivers continuous AI-assisted security monitoring and response through fully compliant SOC-as-a-Service. With Overwatch, Sentinel Blue operates as your dedicated blue team and MSSP, providing visibility into your environment and taking action when suspicious activity or threats are identified.

Your Personal Threat Hunters

Sentinel Blue brings a deep roster of expertise in cybersecurity and the defense industry. Hunting hackers, identifying supply chain threats, and helping DIB contractors strengthen their cyber resilience is our bread and butter. With an extensive team of SMEs who care deeply about providing affordable, enterprise-grade cybersecurity solutions, we work around the clock to keep your operations secure and compliant.

OVERWATCH at a Glance

365
COVERAGE

≥95-100%
SLAs

LED BY INDUSTRY EXPERTISE

CompTIA CySA+ CERTIFIED Plus Series

GIAC CERTIFIED GCIH INCIDENT HANDLER

ADVISOR BLUE TEAM LEVEL 1

Keeping Federal Contractors Compliant

Overwatch is tailored to support the defense industry and other highly regulated environments. With security monitoring solutions that align closely with regulatory requirements including CMMC Level 2, Overwatch delivers the robust security posture that federal and DIB compliance demands.

OVERWATCH: ENTERPRISE-GRADE CAPABILITIES & MANAGED SOC/SIEM SERVICES

- **Continuous Security Monitoring:** Continuous human + machine surveillance across your environment, including weekends and holidays when attackers are most active.
- **Managed Detection and Response (MDR):** Real-time threat protection paired with hands-on response actions: isolating endpoints, killing malicious processes, and containing incidents before they escalate.
- **SIEM Management and Tuning:** Full lifecycle ownership of the System and Information Event Management (SIEM) platform, including log ingestion, parsing, correlation rules, and ongoing tuning to reduce false positives.
- **Endpoint Detection and Response (EDR/XDR):** Deployment, monitoring, and management with a world-class, leading platform (Defender for Endpoint) with active investigation of every meaningful alert.
- **Proactive Threat Hunting:** Hypothesis and intelligence-driven hunts in your environment using the latest Tactics, Techniques, and Procedures (TTPs) from MITRE ATT&CK, surfacing threats that bypass automated detections.
- **Threat Intelligence Integration:** Curated, contextualized intel from commercial, open-source, and ISAC feeds, targeting your environment and the DIB
- **Incident Response and Containment:** Defined runbooks, SLA-bound response times, and direct escalation paths to senior responders for critical-severity events, including containment and digital forensics for evidence preservation and collection.
- **Digital Forensics and Root Cause Analysis:** Post-incident investigation including timeline reconstruction, malware analysis, and an incident report.
- **Vulnerability Management:** Continuous scanning and risk/exploit-based analysis, prioritizing efforts where it matters most.
- **Identity Threat Detection (ITDR):** Monitoring for credential abuse, impossible travel, privilege escalation, MFA bypass, and lateral movement across cloud identity providers.
- **Email Security and Phishing Response:** Active analysis of user-reported phishing, BEC investigation, and rapid remediation.
- **Compliance and Audit Reporting:** Evidence collection and reporting aligned to CMMC.

About Sentinel Blue

Sentinel Blue is a CMMC leader and managed security service provider bringing the power of enterprise cybersecurity tools to federal contractors of all sizes. Specializing in emerging technologies and digital transformation, Sentinel Blue offers comprehensive, scalable, end-to-end cybersecurity solutions for clients and partners within the defense industrial base (DIB) and other highly regulated industries. **Learn more here.**