

2025

seceon

From Risk to Resilience:

DoD Cybersecurity Protecting $400B+ in Contracts

Explore how defense contractors can close critical cyber gaps, achieve CMMC 2.0 compliance, and safeguard sensitive data against ransomware, nation-state attacks, and insider threats.

Executive Summary

The U.S. Defense Industrial Base (DIB), comprising more than 300,000 contractors and subcontractors, is the backbone of American military strength. This ecosystem provides critical technologies, supply chains, logistics, and services that power national defense. Yet, it has become a primary target of nation-state adversaries, ransomware groups, and insider threats, making it one of the most at-risk industries in the world.

With CMMC 2.0 enforcement underway, over 75% of contractors remain unprepared, risking exclusion from $400+ billion in Department of Defense (DoD) contracts. Fragmented tools, compliance confusion, and escalating cyberattacks create a perfect storm of risk.

Seceon's AI-driven Open Threat Management (OTM) platform offers a unified solution to meet CMMC 2.0 requirements, stop advanced persistent threats (APTs), and consolidate fragmented defenses, achieving full compliance in just five months.

The Industry: The Defense Industrial Base at a Critical Juncture

The Defense Industrial Base represents a vast and diverse network, from major aerospace and defense companies to niche subcontractors providing components, logistics, and services. Its importance to national security makes it a prime target for foreign adversaries.

- **Size and Scope:** Over 300,000 contractors participate in the DoD supply chain.
- **Economic Value:** Annual DoD contract value exceeds $400 billion.
- **Mission Criticality:** Contractors safeguard Controlled Unclassified Information (CUI), prototypes, and supply chain integrity vital for military readiness.

The sector is undergoing digital transformation by embracing cloud adoption, IoT, OT integration, and remote work, but this has widened the attack surface. Every contractor, no matter their size, is now part of a global battlefield in cyberspace.

Current Threat Landscape: Escalating Attacks on DoD Contractors

The DIB faces a multi-vector, coordinated threat environment:

- **Ransomware Epidemic:** 300% increase (2020–2024) in ransomware attacks against defense contractors. High-profile attacks disrupted operations and threatened supply chain continuity.
- **Nation-State Espionage:** Chinese APT groups targeting naval and aerospace contractors for IP theft. Russian operations are probing supply chains and defense communications. Campaigns often persist undetected for months, exfiltrating sensitive defense data.
- **Supply Chain Compromise:** The SolarWinds breach (2020) demonstrated how attackers can infiltrate multiple contractors at once. Vendors and third-party suppliers remain the weakest link in compliance and monitoring.
- **Critical Infrastructure Overlap:** Attacks like the Colonial Pipeline ransomware exposed the dependence of defense operations on energy and logistics providers.

- **Insider Threats:** Employee sabotage, accidental misconfigurations, and credential misuse account for 22% of breaches in the sector.
- **Compliance Pressure:** 75% of contractors are not ready for CMMC 2.0 Level 2 certification. Failure means contract exclusion, fines, and reputational damage.



Critical Vulnerabilities in the Defense Ecosystem

- **Fragmented Security Tools:** Most contractors run 8–15 separate tools, creating gaps and integration challenges.
- **Lack of Continuous Monitoring:** 45% cannot demonstrate real-time compliance reporting.
- **Insufficient APT Defense:** 85% lack advanced capabilities to detect stealthy nation-state attacks.
- **OT and ICS Risks:** Defense production plants and logistics systems are increasingly targeted.
- **Supply Chain Blind Spots:** Third-party vendor risks create cascading breaches across multiple contractors.

Traditional Security Failures

The current security model across many DoD contractors has proven inadequate:

- **Tool Proliferation Crisis:** Teams juggle dozens of unintegrated tools, creating alert fatigue and blind spots.
- **Compliance Gaps:** Contractors struggle to generate audit-ready documentation for CMMC, NIST, or ITAR.
- **Slow Incident Response:** Average detection time is 190 days, leaving attackers undisturbed.
- **High Costs, Low ROI:** Redundant tools and overlapping services consume budgets but fail to prevent breaches.

Seceon’s Unified Solution: CMMC Compliance and Cyber Resilience in Five Months

Seceon’s Open Threat Management (OTM) Platform addresses these failures with a cloud-native, AI-driven solution:

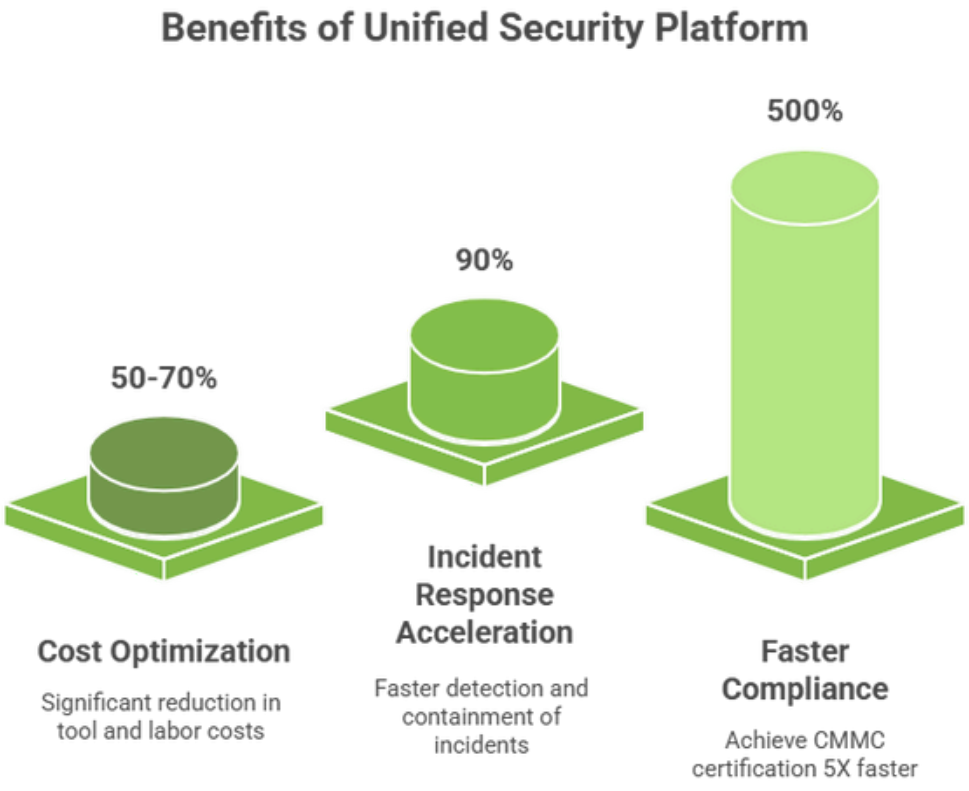
- **aiSIEM**: AI-powered SIEM processing 150M+ events/sec, enriched with threat intelligence.
- **aiXDR**: Extended Detection and Response mapped to MITRE ATT&CK for APT defense.

- **SOAR**: Automated orchestration delivering sub-minute incident containment.
- **aiSecurityScore360**: Continuous posture scoring and compliance monitoring.
- **aiBAS360**: Breach and attack simulation to validate resilience.

Compliance Alignment: Automates all 110 CMMC Level 2 controls across 17 practice families such as Access Control, Audit, Incident Response, and System Integrity.

Business Case and ROI Analysis

- **Tool Consolidation:** Reduce from 15+ security tools to 1 unified platform.
- **Cost Optimization:** 50–70% reduction in tool and labor costs.
- **Incident Response Acceleration:** 90% faster detection and containment.
- **Faster Compliance:** Achieve CMMC certification 5X faster than traditional methods.
- **Contract Protection:** Safeguards $400B+ DoD contracts from compliance-based exclusion.



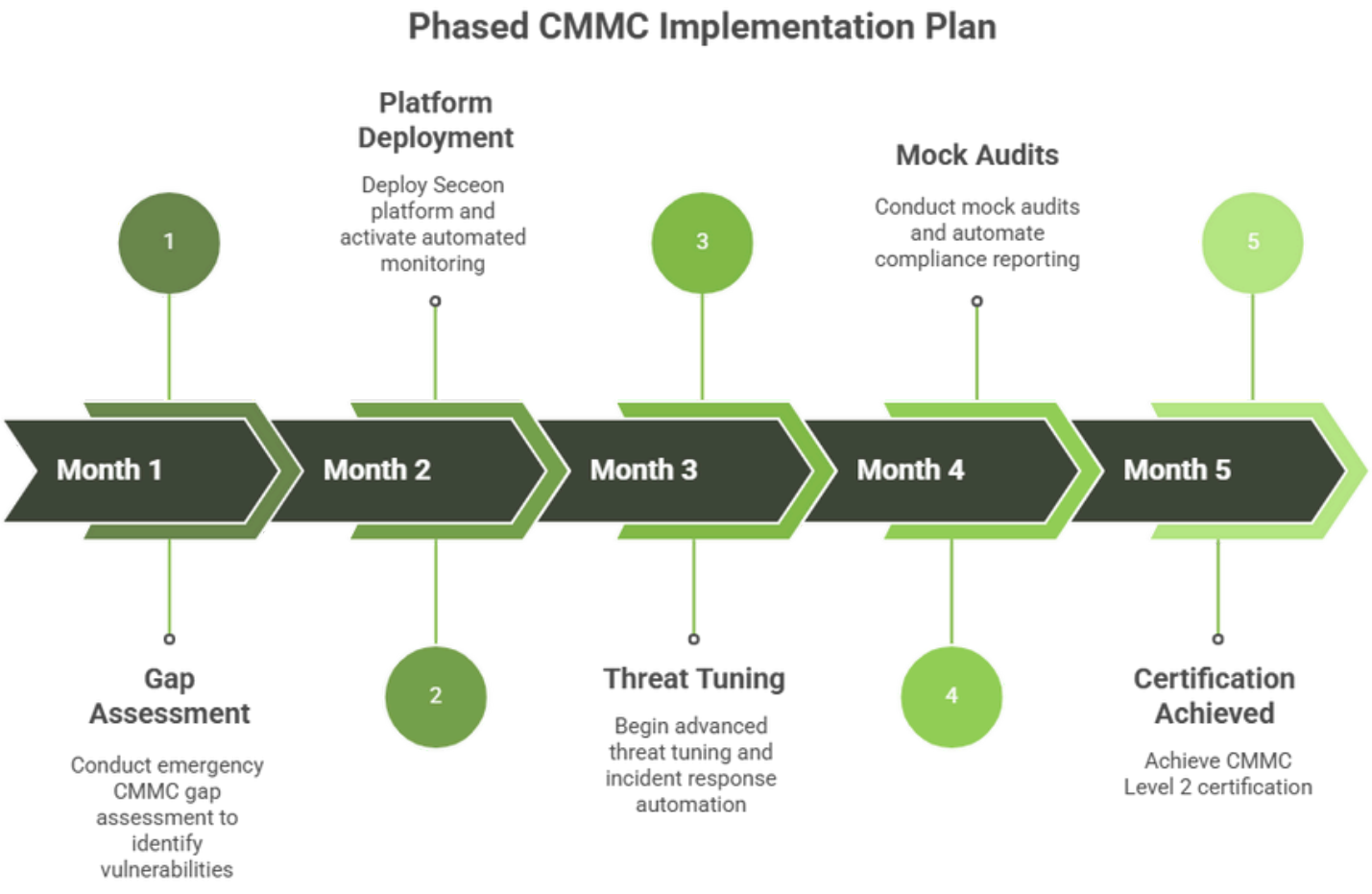
Implementation Strategy: Phased Five-Month Plan

Phase 1: Foundation (Months 1–2)

- Emergency CMMC gap assessment.
- Deploy the Seceon platform, activate all controls, and begin automated monitoring.

Phase 2: Optimization and Certification (Months 3–5)

- Advanced threat tuning and incident response automation.
- Mock audits, real-time compliance reporting, and documentation automation.
- CMMC Level 2 certification achieved.



CYBER SIEGE
Defense Industrial Base Under Attack

DIB
Defense Industrial Base

CMMC
Compliance Mandates

APT
Nation-State Threats

Current Threat Level: Critical

300%
Increase in ransomware attacks since 2020 (Disrupting operations)

75%
Contractors not ready for CMMC 2.0 (Compliance crisis)

$400B+
DoD contracts at risk without certification (Economic impact)

190 days
Average detection time for breaches (Slow response)

Current Problems

- Multiple security tools
- Fragmented defenses
- Slow response times
- Alert fatigue
- Compliance challenges

Seceon Solution

- Unified AI-driven platform
- Rapid CMMC compliance
- Automated response
- Fewer false positives
- Continuous monitoring

Transform Your Cybersecurity

15 → 1
Tools Consolidated

90%
Faster Detection

24/7
AI, ML & DTM Protection

Don't wait for the next attack.
Secure your DoD contracts with Seceon's unified AI, ML & DTM platform today.

Conclusion: Securing America's Defense Supply Chain

The Defense Industrial Base is under siege. Nation-state adversaries, ransomware groups, and insider threats have created a cyber battleground where every contractor, large or small, must prove resilience and compliance.

Traditional tools and fragmented defenses have failed. Seceon's AI-driven OTM platform enables DoD contractors to:

- Consolidate tools into a unified system.
- Achieve compliance in five months.
- Defend against APTs and ransomware with proactive automation.
- Protect national security and safeguard contracts.

Next Step: Secure your future with Seceon. Request a demo today at www.seceon.com/contact-us.

About Seceon

Seceon enables MSPs, MSSPs, and Enterprises to reduce cyber threat risks and their security stack complexity while greatly improving their ability to detect and block threats, and breaches at scale. Seceon's Open Threat Management (OTM) platform augments and automates MSP and MSSP security services with our AI and ML-powered aiSIEM, aiXDR, and aiMSSP platforms. The platform delivers gapless coverage by collecting telemetry from logs, identity management, network logs and flows, endpoints, clouds, and applications. It's all enriched and analyzed in real-time by applying threat intelligence, AI and ML models built on behavioral analysis, and correlation engines to create reliable, transparent detections and alerts. Over 680 partners are reselling and/or running the industry's lowest TCO, efficient security services with automated cyber threat remediation and continuous compliance for over 9,000 clients.

References and Citations:

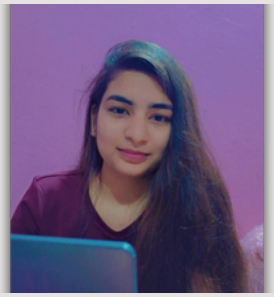
This whitepaper is based on research and data from:

- U.S. Department of Defense (DoD). *Cybersecurity Maturity Model Certification (CMMC) 2.0 Overview*. 2024.
- IBM Security. *Cost of a Data Breach Report 2024*. IBM & Ponemon Institute, 2024.
- Verizon. *2024 Data Breach Investigations Report (DBIR)*. Verizon Enterprise, 2024.
- Federal Bureau of Investigation (FBI). *IC3 Annual Internet Crime Report 2023*. U.S. Department of Justice, 2024.
- Cybersecurity and Infrastructure Security Agency (CISA). *Ransomware Trends and Defense Guidance for Critical Infrastructure*. U.S. DHS, 2024.
- International Institute for Strategic Studies (IISS). *Cyber Capabilities and National Power: A Net Assessment – 2023 Update*. London: IISS, 2023.

About the Author

Khyati Vishwakarma

AI/ML Cybersecurity Engineer, Seceon Inc.



Khyati brings deep expertise in applying artificial intelligence and machine learning to safeguard IT, OT, IoT, and cloud ecosystems against advanced and evolving cyber threats. At Seceon, she plays a key role in strengthening enterprise security resilience, ensuring alignment with global compliance frameworks, and delivering measurable ROI through the company's next-generation aiSIEM and OTM platforms.

About the Author



Aditya Kumar

AI/ML Cybersecurity Engineer, Seceon Inc.

Aditya brings deep expertise in applying artificial intelligence and machine learning to safeguard IT, OT, IoT, and cloud ecosystems against advanced and evolving cyber threats. At Seceon, he plays a key role in strengthening enterprise security resilience, ensuring alignment with global compliance frameworks, and delivering measurable ROI through the company's next generation aiSIEM and OTM platforms.

© 2025 Seceon Inc. All rights reserved. aiSIEM, aiXDR, are trademarks and registered trademarks of Seceon Inc. in the United States and other countries. All other brand names, product names, or trademarks belong to their respective owners.