VENARI SECURITY

Whitepaper

Achieving CMMC 2.0 Compliance Through Continuous TLS/SSL Monitoring

Introduction

The Cybersecurity Maturity Model Certification (CMMC) framework establishes a standardized set of cybersecurity requirements for defense contractors and subcontractors. To achieve CMMC compliance, organizations must demonstrate their ability to protect sensitive data and mitigate cybersecurity risks. One critical aspect of CMMC compliance is the proper use of encryption to safeguard sensitive information.

This whitepaper explores the encryption requirements outlined in the CMMC framework and how Venari Security can help organizations meet these standards through continuous TLS/SSL monitoring.

CMMC Encryption Requirements

The CMMC framework outlines specific requirements for encryption based on the desired level of certification:

Level 1

Basic encryption for controlled unclassified information (CUI) at rest and in transit.

Level 2

Advanced encryption techniques, data loss prevention measures, and continuous monitoring.

Level 3

Enhanced encryption practices, key management, and configuration management.

Level 4 and 5

Even more stringent encryption requirements, including advanced techniques like homomorphic encryption and secure multi-party computation.

Venari Security: Enabling CMMC 2.0 Compliance Through Continuous TLS/SSL Monitoring

Venari Security offers a comprehensive platform designed to monitor and manage TLS/SSL certificates and connections. By continuously assessing an organization's TLS/SSL posture, Venari can help identify and address vulnerabilities that could impact CMMC compliance.

Key features of Venari Security include:

Certificate Inventory and Management:	Venari provides a centralized view of all TLS/SSL certificates, enabling organizations to track expiration dates, manage renewals, and identify vulnerabilities.
Configuration Assessment:	Venari can assess the configuration of TLS/SSL settings to ensure compliance with best practices and security standards.
Vulnerability Detection:	Venari monitors for known vulnerabilities in TLS/SSL protocols and libraries, providing timely alerts and remediation guidance.
Compliance Reporting:	Venari generates detailed reports on an organization's TLS/SSL posture, helping to demonstrate compliance with CMMC and other regulatory frameworks.

Benefits of Using Venari Security

Enhanced Security:

Venari Security helps organizations strengthen their security posture by identifying and addressing vulnerabilities in TLS/SSL implementations.

Reduced Risk:

By proactively managing TLS/SSL certificates and mitigating vulnerabilities, organizations can reduce the risk of data breaches and other security incidents.

Simplified Compliance:

Venari's automated monitoring and reporting capabilities can streamline the process of demonstrating CMMC compliance.

Improved Efficiency:

Venari's centralized platform can help organizations streamline their certificate management processes and improve operational efficiency.

Conclusion

Achieving CMMC compliance requires a robust approach to cybersecurity, including effective management of TLS/SSL encryption. Venari Security provides a powerful solution for organizations seeking to meet their CMMC obligations and enhance their overall security posture. By leveraging Venari's platform for continuous TLS/SSL monitoring, organizations can strengthen their encryption practices, reduce risks, and demonstrate their commitment to cybersecurity.

Bridge your knowledge gap.
Visit: www.venarisecurity.com

Venari Security Ltd.

16 Great Queen Street, London,
WC2B 5AH, United Kingdom
+44 (0)20 7294 7749
info@venarisecurity.com

About Venari Security

Venari Security provides organisations with advanced visibility into their encrypted attack surface, ensuring regulatory compliance and privacy adherence through our cryptographic discovery tool.

Our focus is on crypto agility which helps you assess both external and internal cryptographic risks, preparing your business now and for the quantum future.

VENARI SECURITY