CLAROTY

WHITE PAPER

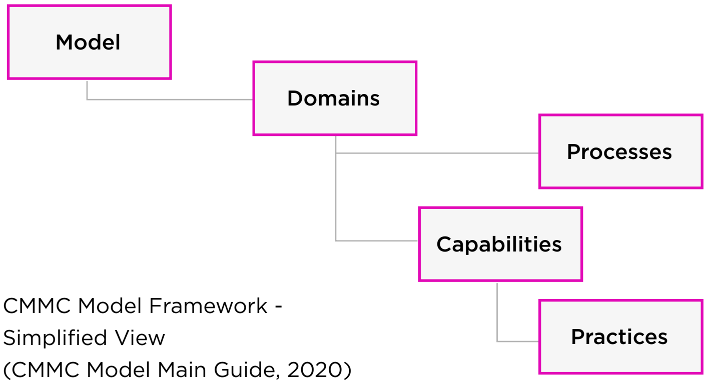
SUPPORTING CMMC COMPLIANCE

How The Claroty Platform supports CMMC Compliance

Introduction

The U.S. Government is taking steps to improve the cybersecurity posture of the Defense Industrial Base (DIB) sector. As such, the Department of Defense created the CMMC framework (similar to other regulatory guidelines) to audit defense contractors' compliance to NIST 800-171. CMMC assesses the maturity and competency in core areas of cybersecurity.

Companies will need to implement these protocols in order to protect Federal Contract Information (FCI) and Controlled Unclassified Information (CUI), and to be considered for RFPs and RFIs. As a leader in industrial cybersecurity, Claroty solutions and services can help you stay within CMMC Compliance.



CMMC Model Framework -
Simplified View
(CMMC Model Main Guide, 2020)

- The model encompasses multiple domains
- For each domain, there are processes that span a subset of the 5 levels
- For each domain, there are capabilities that span a subset of the 5 levels
- For each capability, there are practices that span a subset of the 5 levels

Claroty Solution Overview

Claroty offers a comprehensive set of industrial cybersecurity solutions, including Claroty xDome, Continuous Threat Detection (CTD), and Secure Remote Access (SRA). Claroty's industrial solutions integrate seamlessly with any industrial environment, regardless of its scale, architecture, or maturity of existing cybersecurity programs. Highly flexible and rapid deployment options enable Claroty to reveal and protect all OT and other cyber-physical systems within the network while automatically detecting the earliest indicators of threats to those assets via proprietary detection technologies.

Further extending the value of these controls, Claroty maintains a vast integration ecosystem, robust API, and employs the industry's only solution for integrated remote incident management capabilities that span the entire incident lifecycle.

How Claroty Supports CMMC Compliance

The following tables document how Claroty enables enterprises to directly or indirectly achieve CMMC compliance. Complete process and practice descriptions can be found at the website for the Office of the Under Secretary of Defense.

DOMAIN: ACCESS CONTROL (AC)

Claroty utilizes multiple techniques and capabilities to control network access as well as regulate/monitor the flow of information across the network. This includes tiered user access, multi-factor authentication, strict password rules, virtual network segmentation, and network traffic monitoring, and secure-by-design remote network access, which work together to support the capabilities and practices below.

Capability	Supported Practice
C001: Establish system access requirements	AC.1.001 - Limit information system access to authorized users, processes acting on behalf of authorized users, or devices.
	AC.2.005 - Provide privacy and security notices consistent with applicable CUI rules.
	AC.2.006 - Limit use of portable storage devices on external systems.
C002: Control internal system access	AC.1.002 - Limit information system access to the types of transactions and functions that authorized users are permitted to execute.
	AC.2.007 - Employ the principle of least privilege, including for specific security functions and privileged accounts.
	AC.2.008 - Use non-privileged accounts for roles when accessing nonsecurity functions.
	AC.2.009 - Limit unsuccessful log-on attempts.
	AC.2.011 - Authorize wireless access prior to allowing such actions.
	AC.3.018 - Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs
	AC.4.023 - Control information flows between security domains on connected systems.
	AC.5.024 - Identify and mitigate risk associated with unidentified wireless access points.
C003: Control remote system access	AC.2.013 - Monitor and control remote access sessions
	AC.2.015 - Route remote access via managed access control points
	AC.3.014 - Employ cryptographic mechanisms to protect the confidentiality of remote sessions.
	AC.3.021 - Authorized remote execution of privileged commands and remote access.
	AC.4.032 - Restrict remote network access based on defined risk factors such as time of day, location, network connection state, and measured properties of the current user and role.
C004: Limit data access to authorized users and processes	AC.1.003 - Verify and control/limit connections to and use of external information systems.
	AC.2.016 - Control the flow of CUI in accordance with approved authorizations.

DOMAIN: ASSET MANAGEMENT (AM)

Claroty leverages the broadest and deepest industrial protocol coverage in the industry to enable its unmatched Passive, Active, and AppDB continuous scanning capabilities.

The Claroty Edge data collector is capable of providing a full inventory of all OT, IoT, and IT assets and their accompanying risks and vulnerabilities, within minutes, without the need for additional hardware or network changes.

With these methods Claroty is capable of providing the most comprehensive industrial visibility and asset management controls in the industry, resulting in a highly detailed, centralized inventory of all OT, IoT, and IIoT assets, processes, and connections.

Capability	Supported Practice
C005: Identify and document assets	AM.3.036 Define procedures for the handling of CUI data.
C006: Manage asset inventory	AM.4.226 Employ automated capability to discover and identify systems with specific component attributes (e.g., firmware level, OS type) within your inventory.

DOMAIN: AUDIT AND ACCOUNTABILITY (AU)

Claroty solutions allow for tiered credential access to system information, including centralized data management and analytics, administrative controls, and reports. In addition, SRA enables users to gain full, real-time visibility into user activity with detailed logs of all actions taken during remote network sessions.

Capability	Supported Practice
C007: Define audit requirements	AU.2.041 Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions.
	AU.3.045 Review and update logged events.
C008: Perform auditing	AU.2.042 Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.
	AU.3.048 Collect audit information (e.g., logs) into one or more central repositories.
C009: Identify and protect audit information	AU.3.049 Protect audit information and audit logging tools from unauthorized access, modification, and deletion.
	AU.5.050 Identify assets not reporting audit logs and assure appropriate organizationally defined systems are logging.
C010: Review and manage audit logs	AU.3.052 Provide audit record reduction and report generation to support on-demand analysis and reporting.
	AU.4.053 Automate analysis of audit logs to identify and act on critical indicators (TTPs) and/or organizationally-defined suspicious activity.
	AU.4.054 Review audit information for broad activity in addition to per-machine activity.

DOMAIN: AWARENESS AND TRAINING (AT)

Claroty is your trusted advisor for industrial cybersecurity, continually keeping you customers up-to-date on the latest industry best practices. Claroty solutions are driven by the award-winning Team82 Research Team--an acclaimed group of experts that discover and disclose ICS vulnerabilities.

Claroty is backed and adopted by the top three industrial automation vendors including Rockwell Automation, Schneider Electric, and Siemens. We frequently work with these partners (and others) to provide webinars and other valuable content to the community.

Capability	Supported Practice
C011: Conduct security awareness activities	AT.4.059 Provide awareness training focused on recognizing and responding to threats from social engineering, advanced persistent threat actors, breaches, and suspicious behaviors; update the training at least annually or when there are significant changes to the threat.

DOMAIN: CONFIGURATION MANAGEMENT (CM)

Claroty's superior network discovery and continuous visibility provides a complete picture of all network assets, processes, and sessions. This level of visibility provides the foundation for network administrators to maintain control over device access and configurations, allowing for strict policy enforcement and log management.

Capability	Supported Practice
C013: Establish configuration baselines	CM.2.061 Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.
	CM.2.063 Control and monitor user-installed software.
C014: Perform configuration and change management	CM.2.064 Establish and enforce security configuration settings for information technology products employed in organizational systems.
	CM.2.065 Track, review, approve, or disapprove, and log changes to organizational systems.
	CM.3.067 Track, review, approve, or disapprove, and log changes to organizational systems.
	CM.3.068 Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services.
	CM.3.069 Apply deny-by-exception (blacklisting) policy to prevent the use of unauthorized software or deny-all, permit-by-exception (whitelisting) policy to allow the execution of authorized software.

DOMAIN: IDENTIFICATION AND AUTHENTICATION (IA)

Cybersecurity controls are only as strong as their ability to determine who and what has access to a network. Claroty's industrial solutions contain multiple levels where network administrators can, either manually or automatically, create strict controls over network identification and authentication per user, group, device, or group policy.

Capability	Supported Practice
C015: Grant access to authenticated entities	IA.1.076 Identify information system users, processes acting on behalf of users, or devices.
	IA.1.077 Authenticate (or verify) the identities of those users, processes, or devices as a prerequisite to allowing access to organizational information systems.
	IA.2.078 Enforce a minimum password complexity and change of characters when new passwords are created.
	IA.2.079 Prohibit password reuse for a specified number of generations.
	IA.2.080 Allow temporary password use for system logons with an immediate change to a permanent password.
	IA.2.081 Store and transmit only cryptographically-protected passwords.
	IA.2.082 Store and transmit only cryptographically-protected passwords.
	IA.3.083 Use multi-factor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.
	IA.3.084 Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts.

DOMAIN: INCIDENT RESPONSE (IR)

As part of a holistic approach to industrial cybersecurity, Claroty offers the industry's first industrial cybersecurity solution to offer fully integrated incident management capabilities. These capabilities span the entire incident lifecycle, enabling users to detect, investigate, and respond to industrial cybersecurity incidents across the broadest possible attack surface from any location. As a result, organizations can easily evolve and adapt their overall security posture and workflows for a remote, distributed, and/or highly variable work environment.

Capability	Supported Practice
C016: Plan incident response	IR.2.092 Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.
	IR.4.100 Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.

	IR.5.106 In response to cyber incidents, utilize forensic data gathering across impacted systems, ensuring the secure transfer and protection of forensic data.
C017: Detect and report events	IR.2.093 Detect and report events.
	IR.2.094 Analyze and triage events to support event resolution and incident declaration.
C018: Develop and implement a response to a declared incident	IR.5.102 Use a combination of manual and automated, real-time responses to anomalous activities that matches incident patterns.
C019: Perform post incident reviews	IR.2.097 Perform root cause analysis on incidents to determine underlying causes.

DOMAIN: MAINTENANCE (MA)

Claroty industrial solutions’ network discovery and vulnerability assessment capabilities are an ideal solution for creating and maintaining a preventative maintenance schedule for network assets. SRA enables maintenance staff to quickly and easily connect to the desired asset while giving network administrators full control over remote network sessions. This control includes the ability to provision protocol-level access to specific assets, define session duration, monitor-live all actions taken during remote sessions, and immediately terminate remote sessions if required. SRA reduces mean time-to-repair (MTTR) and boosts uptime by making it faster and easier to connect to and repair OT, IoT, and IIoT assets any time, anywhere.

Capability	**Supported Practice**
C021: Manage maintenance	MA.2.112 Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance.
	MA.2.113 Require multi-factor authentication to establish non-local maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete.
	MA.2.114 Supervise the maintenance activities of personnel without required access authorization.

DOMAIN: RECOVERY (RE)

Claroty solutions enable users to regularly back up network information to secure locations or export logs for reporting and analysis. Additionally, network backup information can be used to enhance visibility into parts of the network that are otherwise difficult to reach via CTD’s App DB parsing..

Capability	**Supported Practice**
C029: Manage backups	RE3.139 Regularly perform complete, comprehensive, and resilient data backups, as organizationally defined.

DOMAIN: RISK MANAGEMENT (RM)

Claroty industrial solutions’ in-depth network discovery and vulnerability assessment capabilities excel at providing a comprehensive view of network risk. All sites , segments, and assets are assessed with risk scoring methodologies These three layers are interdependent and are calculated dynamically to ensure the most up-to-date score is available. These scores are aggregated into a single score when deployed in multi-site environments.

With its vast integrations ecosystem, robust API, and flexible deployment options, Claroty equips you to seamlessly connect your industrial cybersecurity program to your IT security program and, even more importantly, to your organization’s governance, risk, and compliance programs and enterprise-wide risk management strategy.

Capability	Supported Practice
C031: Identify and evaluate risk	RM.2.141 Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI.
	RM.2.142 Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.
	RM.3.144 Periodically perform risk assessments to identify and prioritize risks according to the defined risk categories, risk sources, and risk measurement criteria.
	RM.4.149 Catalog and periodically update threat profiles and adversary TTPs.
	RM.4.150 Employ threat intelligence to inform the development of the system and security architectures, selection of security solutions, monitoring, threat hunting, and response and recovery activities.
	RM.4.151 Perform scans for unauthorized ports available across perimeter network boundaries over the organization’s Internet network boundaries and other organizational-defined boundaries.
	RM.2.143 Remediate vulnerabilities in accordance with risk assessments.
	RM.3.146 Develop and implement risk mitigation plans.
C032: Manage risk	RM.5.155 Analyze the effectiveness of security solutions at least annually to address anticipated risk to the system and the organization based on current and accumulated threat intelligence.

DOMAIN: SECURITY ASSESSMENT (CA)

Insights provided by Claroty solutions enable users to create, maintain, and execute risk reduction programs using key prioritization metrics provided by Claroty, such as asset risk scoring, attack vector mapping, and zone risk analysis.

Capability	Supported Practice
C034: Develop and manage a system security plan	CA.4.163 - Create, maintain, and leverage a security strategy and roadmap for organizational cybersecurity improvement.
C035: Define and manage controls	CA.2.159 - Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.

DOMAIN: SITUATIONAL AWARENESS (SA)

Claroty's threat detection engines are built to monitor the network for both known and unknown threats, behavioral indicators of compromise, and allows network administrators to create custom alerting rules to fit their unique industrial environment. This information is backed up with proprietary research from Claroty's Team82 research team, the latest CVEs from the National Vulnerability Database, and the ongoing collaboration with our industrial automation partners.

By continually monitoring your network for both known and unknown emerging threats, automatically weeding out false positives, and giving you clear direction on how to take action, The Claroty Platform equips you to mitigate threats before they impact your business—regardless of where you are on your industrial cybersecurity journey.

Capability	Supported Practice
C037: Implement threat monitoring	SA.3.169 - Receive and respond to cyber threat intelligence from information sharing forums and sources and communicate to stakeholders.
	SA.4.171 - Establish and maintain a cyber threat hunting capability to search for indicators of compromise in organizational systems and detect, track, and disrupt threats that evade existing controls.
	SA.4.173 - Design network and system security capabilities to leverage, integrate, and share indicators of compromise.

DOMAIN: SYSTEM AND COMMUNICATIONS PROTECTION (SC)

Network segmentation and secure remote access are zero trust controls deemed highly effective at improving industrial cybersecurity posture. Distinguishing legitimate communication across business processes and applications requires a clear picture of how and why these assets are communicating and frequently, ineffective or completely nonexistent segmentation between assets is the root cause of many aspects of network risk.

Claroty jumpstarts network segmentation programs by automatically creating and deploying communication policies that can be enforced through existing infrastructure. Additionally, Claroty streamlines remote access through an OT-specific solution offering RBAC, an industrial-aware secure architecture, and simple administration.

Our secure remote access solution utilizes advanced tunneling to remote direct connection to critical assets, is designed with features securing data at rest, and preserves the Purdue Model method of network communications extending only one layer up or down.

Capability	Supported Practice
C038: Define security requirements for systems and communications	SC.2.179 - Use encrypted sessions for the management of network devices.
	SC.3.180 - Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.
	SC.3.186 - Terminate network connections associated with communications sessions at the end of the session or after a defined period of time.
	SC.3.190 - Protect the authenticity of communications sessions.
	SC.3.191 - Protect the confidentiality of CUI at rest.
C039: Control communications at system boundaries	SC.1.175 - Monitor, control, and protect organizational communications at the external boundaries and key internal boundaries of the information systems.
	SC.1.176 - Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.
	SC.4.199 - Utilize threat intelligence to proactively block DNS requests from reaching malicious domains.
	SC.4.202 - Employ mechanisms to analyze executable code and scripts traversing internet network boundaries or other organizationally defined boundaries.
	SC.5.208 - Employ organizationally defined and tailored boundary protections in addition to commercially available solutions.

DOMAIN: SYSTEM AND INFORMATION INTEGRITY (SI)

SRA integrates seamlessly with ICAP-based antivirus solutions. This capability helps protect the OT environment from malware by increasing the safety of uploaded files necessary for carrying out remote maintenance and related tasks on OT assets. In the event that a file is malicious, SRA users are immediately notified and prevented from uploading it to the asset.

Capability	Supported Practice
C040: Identify and manage information system flaws	SI.1.210 - Identify, report, and correct information and information system flaws in a timely manner.
	SI.2.214 - Monitor system security alerts and advisories and take action in response.
	SI.4.221 - Use threat indicator information relevant to the information and systems being protected and effective mitigations obtained from external organizations to inform intrusion detection and threat hunting.
C041: Identify malicious content	SI.1.212 - Update malicious code protection mechanisms when new releases are available.
	SI.1.213 - Perform periodic scans of the information system and real-time scans of files from external sources.

C042: Perform network and system monitoring	SI.5.222 - Analyze system behavior to detect and mitigate execution of normal system commands and scripts that indicate malicious content.
	SI.2.216 - Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.
	SI.2.217 - Identify unauthorized use of organizational systems.
	SI.5.223 - Monitor individuals and system components on an ongoing basis for anomalous or suspicious behavior.

About Claroty

Claroty empowers organizations to secure cyber-physical systems across industrial (OT), healthcare (IoMT), and enterprise (IoT) environments: the Extended Internet of Things (XIoT). The company's unified platform integrates with customers' existing infrastructure to provide a full range of controls for visibility, risk and vulnerability management, threat detection, and secure remote access.

Backed by the world's largest investment firms and industrial automation vendors, Claroty is deployed by hundreds of organizations at thousands of sites globally. The company is headquartered in New York City and has a presence in Europe, Asia-Pacific, and Latin America.

For more information, visit claroty.com or email contact@claroty.com.

CLAROTY