CMMC 2.0

Cybersecurity Maturity Model Certification 2.0

The Cybersecurity Maturity Model Certification 2.0 (CMMC 2.0) is a framework used to assess the cybersecurity posture of contractors and subcontractors working with the US Department of Defense (DoD). It maps specific controls and processes associated with various cybersecurity standards to three maturity models, ranging from basic cyber hygiene to advanced.

The initial version of CMMC (CMMC 1.0) was published by the DoD in September 2020. In November 2021, the DoD announced CMMC 2.0 which included a streamlined model, reliable assessments, and flexible implementation. Specific changes in CMMC 2.0 include the following: reducing the model from 5 to 3 compliance levels; allowing companies at Level 1 and Level 2 to demonstrate compliance through self-assessment; and allowing companies to make Plans of Action & Milestones (POA&Ms) to achieve certification or waive CMMC requirements, both under certain limited circumstances.

CMMC 2.0 has largely been put in place to verify organizational compliance with NIST 800-171 standards and ensures the security of Controlled Unclassified Information (CUI) that resides on DOD industry partners' networks. It will be incorporated into the Defense Federal Acquisition Regulation Supplement (DFARS) and used as a requirement for awarding contracts.

The framework is designed to allow smaller businesses to implement the controls associated with lower levels of maturity in a cost-effective and affordable way, while organizations with more resources can build to advanced maturity. Each DOD contract specifies a required level of CMMC 2.0 certification.

It will be critical for all organizations that may affect the security of CUI to have some level of CMMC 2.0 compliance at every level of the contractor supply chain. This requires visibility and cyber defense of CUI across the entire lifecycle of the data and anywhere it may be stored, transmitted, and processed.

Achieving CMMC 2.0 With Self-Learning AI Defense

Darktrace delivers AI-powered threat detection, investigation, and response that can support organizations in their journey towards cyber maturity as defined by the CMMC 2.0 framework. Through a unified platform approach, Darktrace provides autonomous cyber defense across the entire enterprise, from cloud, SaaS, and email environments, to corporate networks, remote endpoints, and cyber-physical systems.

With Self-Learning AI, the Darktrace learns what normal behavior looks like across the business in order to spot the subtle deviations that signal an attack, from novel ransomware to stealthy insiders.

The technology spots emerging threats in real time with the Enterprise Immune System, performs automatic investigations with Cyber AI Analyst, and autonomously contains threats with Darktrace Antigena – all without relying on any rules, signatures, or prior assumptions.

Darktrace and CMMC: Framework Applicability

Presented below is a guide showing how Darktrace can assist organizations in working towards CMMC 2.0 practices and associated maturity levels.

For more information on how Darktrace capabilities map to the NIST framework, please see our white paper on Darktrace and NIST.

CMMC 2.0 Framework Applicability					CMMC Level Requirement		
Domain	Capacity	Number	Description	Darktrace Capability	1	2	3
Access Control	Authorized Access Control	AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	Darktrace Antigena can enforce access restrictions to tagged systems. This would provide a backstop for access controls that are not performing.	✓	N/A	N/A
	External Connections	AC.1.003	Verify and control/limit connections to and use of external information systems.	Darktrace can be configured in such a way as to interrupt and prevent data transfer to unauthorized devices.	✓	N/A	N/A
	Control CUI Flow	AC.2.016	Control the flow of CUI in accordance with approved authorizations.	Darktrace can be used to detect misconfiguration and perodically review system configurations.	N/A	✓	N/A
	Separation of Duties	AC.3.017	Separate the duties of individuals to reduce the risk of malevolent activity without collusion.	Darktrace can be configured in such a way as to interrupt and prevent access to un-authorized devices. This would complement proper SoD access control management within the application layer.	N/A	✓	N/A
	Privileged Functions	AC.3.018	Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.	Darktrace can monitor and identify anomalous user activity. This would include anomalous logins from low privelaged users.	N/A	✓	N/A
	Mobile Device Connection	AC.3.020	Control connection of mobile devices.	Darktrace can be used to detect and interrupt anomalous and unauthorized use, regardless of the device.	N/A	✓	N/A

Domain	Capacity	Number	Description	Darktrace Capability	1	2	3
	Privileged Remote Access	AC.3.021	Authorize remote execution of privileged commands and remote access to security-relevant information.	Darktrace can be used to detect and interrupt anomalous and unauthorized use.	N/A	✓	N/A
Audit and Accountability	Event Review	AU.3.045	Review and update logged events.	Darktrace provides real-time, AI-driven investigation of anomalous events occuring within the organization.	N/A	✓	N/A
	Audit Protection	AU.3.049	Protect audit information and audit logging tools from unauthorized access, modification, and deletion.	Darktrace monitors for anomalous data transfer and anomalous identity usage and can act in real-time to disrupt malicious activity.	N/A	✓	N/A
	Audit Correlation	AU.3.051	Correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity.	Darktrace can serve as a centralized collection point for collection and correlation of logs and network traffic to provide situational awareness of anomalous activity.	N/A	✓	N/A
	Reduction & Reporting	AU.3.052	Provide audit record reduction and report generation to support on-demand analysis and reporting.	Darktrace AI can support investigation of anomalous events including full automation for a subset of event criteria.	N/A	✓	N/A
Configuration Management	Access Restrictions for Change	CM.3.067	Define, document, approve, and enforce physical and logical access restrictions associated with changes to organizational systems.	Darktrace can be configured in such a way as to interrupt data transfer and file writes to un-authorized devices.	N/A	✓	N/A
Identification and Authentication	Multifactor Authentication	IA.3.083	Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.	The Darktrace appliance can be configured to require Multi-Factor Authentication (MFA) for remote access.	N/A	✓	N/A

Domain	Capacity	Number	Description	Darktrace Capability	1	2	3
Incident Response	Incident Reporting	IR.3.098	Track, document, and report incidents to designated officials and/or authorities both internal and external to the organization.	Darktrace conducts an AI-based investigation and triage of all alerts in the platform. This information is timelined and summarized for human consumption. Darktrace has several hundred models alerting to anomalous behavior related to incidents which will automatically trigger an alert in real time.	N/A	✓	N/A
Maintenance	System Maintenance Control	MA.2.112	Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance.	Darktrace can be used to autonomously detect and interrupt anomalous and unauthorized use, including for system maintenance.	N/A	✓	N/A
Media Protection	Removable Media	MP.2.121	Control the use of removable media on system components.	Darktrace can be configured in such a way as to interrupt and prevent data transfer to un-authorized devices.	N/A	✓	N/A
Personnel Security	Personnel Actions	PS.2.128	Ensure that organizational systems containing CUI are protected during and after personnel actions such as terminations and transfers.	Darktrace can used to tag users to put them on a watch-list. Darktrace has the ability to fine-tune existing models to give greater emphasis to the behavior of users or devices deemed to be «high-risk». Many organizations use this to provide additional assurance for leavers.	N/A	✓	N/A
Physical Protection	Monitor Facility	PE.2.135	Protect and monitor the physical facility and support infrastructure for organizational systems.	Darktrace can support the monitoring and reporting on physical protection control programs.	N/A	✓	N/A
System and Communications Protection	Boundary Protection	SC.1.175	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	Darktrace can be used to detect and interrupt anomalous and unauthorized use.	✓	N/A	N/A

Domain	Capacity	Number	Description	Darktrace Capability	1	2	3
	Public-Access System Separation	SC.1.176	Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.	Darktrace can be used to detect and interrupt anomalous and unauthorized use.	✓	N/A	N/A
	Network Communication by Exception	SC.3.183	Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception).	Darktrace can be used to prohibit anomalous traffic and perodically review system configurations.	N/A	✓	N/A
	Connections Termination	SC.3.186	Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity.	Darktrace uses unsupervised machine learning algortihms to determine the rarity of a given connection based on behavior patterns.	N/A	✓	N/A
	Voice Over Internet Protocol	SC.3.189	Control and monitor the use of Voice over Internet Protocol (VoIP) technologies	Darktrace can be used to detect and take action on anomalous files and email messages.	N/A	✓	N/A
	Data at Rest	SC.3.191	Protect the confidentiality of CUI at rest.	Darktrace provides robust protection of the endpoint by monitoring data transfer to and from the endpoint to determine and interrupt anomalous data transfer.	N/A	✓	N/A
System and Information Integrity	Malicious Code Protection	SI.1.211	Provide protection from malicious code at appropriate locations within organizational information systems.	Darktrace detects and can be configured to prevent any amonalous activity and any potential malicious software within the network.	✓	N/A	N/A
	Security Alerts & Advisories	SI.2.214	Monitor system security alerts and advisories and take action in response.	Darktrace provides real-time, AI-driven investigation of anomalous events occuring within the organization.	N/A	✓	N/A

Domain	Capacity	Number	Description	Darktrace Capability	1	2	3
	Monitor Communications for Attacks	SI.2.216	Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.	Darktrace provides real-time, AI-driven investigation of all communications traffic occuring within the organization.	N/A	✓	N/A
	Identify Unauthorized Use	SI.2.217	Identify unauthorized use of organizational systems.	Darktrace can serve as a centralized collection point for collection and correlation of logs and network traffic to provide situational awareness of anomalous activity.	N/A	✓	N/A

About Darktrace

Darktrace (DARK:L), a global leader in cyber security AI, delivers world-class technology that protects over 6,500 customers worldwide from advanced threats, including ransomware and cloud and SaaS attacks. Darktrace's fundamentally different approach applies Self-Learning AI to enable machines to understand the business in order to autonomously defend it. Headquartered in Cambridge, UK, the company has 1,700 employees and over 30 offices worldwide. Darktrace was named one of TIME magazine's 'Most Influential Companies' for 2021.

For more information

- Visit darktrace.com
- Book a demo
- Visit our YouTube channel
- Follow us on Twitter
- Follow us on LinkedIn