PERCH

CMMC + Perch Product Mapping

Work towards CMMC compliance with Perch at your back

What's this guide for?

As part of an initiative to protect the United States defense supply chain from cyber threats, the Department of Defense issued a new standard of cybersecurity verification controls for private contractors: the Cybersecurity Maturity Model Certification, or CMMC.

With this product mapping guide, you can see how Perch helps your organization achieve various CMMC compliance requirements.

The big picture

In addition to outlining 5 levels, from "Basic Cyber Hygiene" to "Advanced," CMMC maps seventeen "Capability Domains," each with outlined processes and practices you must meet in order to level up. Perch helps meet requirements in these 6 domains:

- Access Control (AC)
- Incident Response (IR)
- Risk Management (RM)
- Asset Management (AM)
- Maintenance (MA)
- Security Assessment (CA)
- Awareness and Training (AT)
- Media Protection (MP)
- Situational Awareness (SA)
- Audit and Accountability (AU)
- Personnel Security (PS)
- System and Communications Protection (SC)
- Configuration Management (CM)
- Physical Protection (PE)
- System and Information Integrity (SI)
- Identitfication and Authentication (IA)
- Recovery (RE)

The close-up

Perch helps meet these controls:

Capability Domain	CMMC Practice Reference
Access Control	Monitor and control remote access sessions AC.2.013
	Capture the execution of privileged functions in audit logs AC.3.018
Audit & Accountability	Ensure that the actions of users can be uniquely traced so that the proper users can be held accountable AU.2.041
	Create and retain system audit logs to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity AU.2.042
	Collect audit information into one or more central repositories AU.3.048
	Protect audit information and audit logging tools from unauthorized access, modification, and deletion AU.3.049
	Provide audit record reduction and report generation to support on-demand analysis and reporting AU.3.052
	Automate analysis of audit logs to identify and act on critical indicators and/or organizationally defined suspicious activity AU.4.053

Capability Domain	CMMC Practice Reference
Incident Response	Detect and report events IR.2.093
	Analyze and triage events to support event resolution and incident response IR.2.094
	Establish and maintain a security operations center capability that facilitates a 24/7 response capability IR.4.101
Situational Awareness	Receive and respond to cyber threat intelligence from information sharing sources SA.3.169
	Establish and maintain cyber threat hunting capability to search for indicators of compromise in organizational systems SA.4.171
System & Communications Protection	Monitor organization communications at key internal boundaries of the information systems SC.1.175
System & Information Integrity	Monitor system security alerts SI.2.214
	Monitor organizational systems, including inbound and outbound communication traffic, to detect attacks and indicators of potential attacks SI.2.216
	Use threat indicator information relevant to the information systems being protected to inform intrusion detection and threat hunting SI.4.221