




Whitepaper

ASSESSING OPERATIONAL TECHNOLOGY (OT) CYBERSECURITY MATURITY

AN ANALYSIS OF LEASED DATACENTERS UTILIZING THE
CYBERSECURITY MATURITY MODEL CERTIFICATION (CMMC)

Jim Gilsinn

Principal Industrial Consultant
Dragos, Inc.

 info@dragos.com

 [@DragosInc](https://twitter.com/DragosInc)

INTRODUCTION

In early 2021, Dragos began conducting a series of assessments to evaluate the overall cybersecurity maturity of the operational technology (OT) environment for several leased datacenters (LDCs). During these assessments, Dragos found recurring trends in the vulnerabilities found in the LDCs. This report discusses some of those trends and how Dragos is using the experience gained during these assessments to improve our processes.

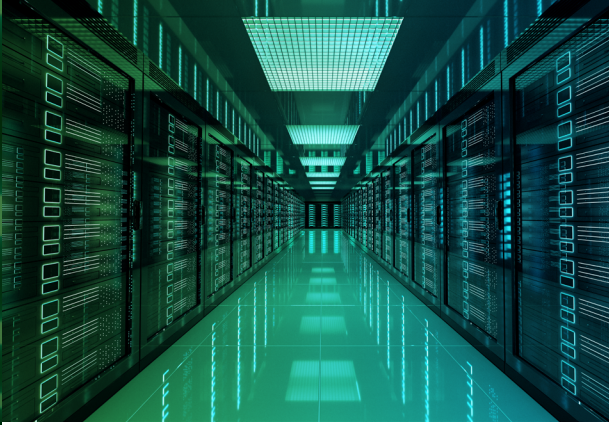
Dragos chose to use the Cybersecurity Maturity Model Certification (CMMC), published in 2020, as a foundation for a series of benchmarking assessments.¹ While CMMC is wide-ranging and covers a broad view of organizational cybersecurity maturity, it does have its drawbacks. The largest and most difficult drawback is related to interpreting the requirements with an eye towards OT. CMMC's focus is protecting the confidentiality of information. Confidentiality, although on the list of cybersecurity priorities for OT, is usually considered a lower priority than safety, integrity, and availability. Dragos reinterpreted many of the requirements in ways that were relevant to OT organizations. This required Dragos to re-imagine the language and purpose around each of the requirements.

Another drawback to using CMMC for these assessments related to it being a certification standard.² Auditors use the requirements as pass/fail criteria. Dragos wanted to develop an assessment that provided a variable scale to show areas for improvement. The variable scale needed to provide enough granularity to show incremental improvements over time applied across the entire security program, domain by domain, and even for individual areas within each domain. This level of granularity allows the organization to better understand how they can choose a target score and develop their roadmap. They could then focus their resources on the domains and areas that would have the greatest return on investment and improvement to their score.

Over the course of 2021 and early 2022, Dragos conducted assessments for 12 different LDCs, covering a total of 16 different regions. Some organizations asked Dragos to evaluate their regions independently due to different organizational structures and recent acquisitions that had not been fully integrated yet.

Because the number of regions included in these assessments is small, Dragos does not purport the information presented here to be a complete and thorough evaluation of all types of datacenters. This report only discusses some broad trends that were visible after looking across the group of LDCs assessed.

UNDERSTANDING THE ENVIRONMENT



When thinking about a datacenter, OT may not be the first thing that comes to mind. Usually, images of rows and rows of pristine computer racks are often what might be pictured. Some customer-facing equipment and spaces in datacenters may appear that way, but there are many areas that look more like traditional OT environments. Devices and systems like programmable logic controllers (PLCs) and energy management systems (EMSs) are common in the OT environment and are necessary to keep the datacenters running at peak efficiency with a minimum of downtime.

LDC & End-User Responsibilities

When trying to understand the relationship between LDCs and their customers, there are three main models depending on the responsibility to operate different parts of the system, as seen in [Figure 1](#) end-user owned & operated, LDC sole tenant, and LDC multi-tenant.

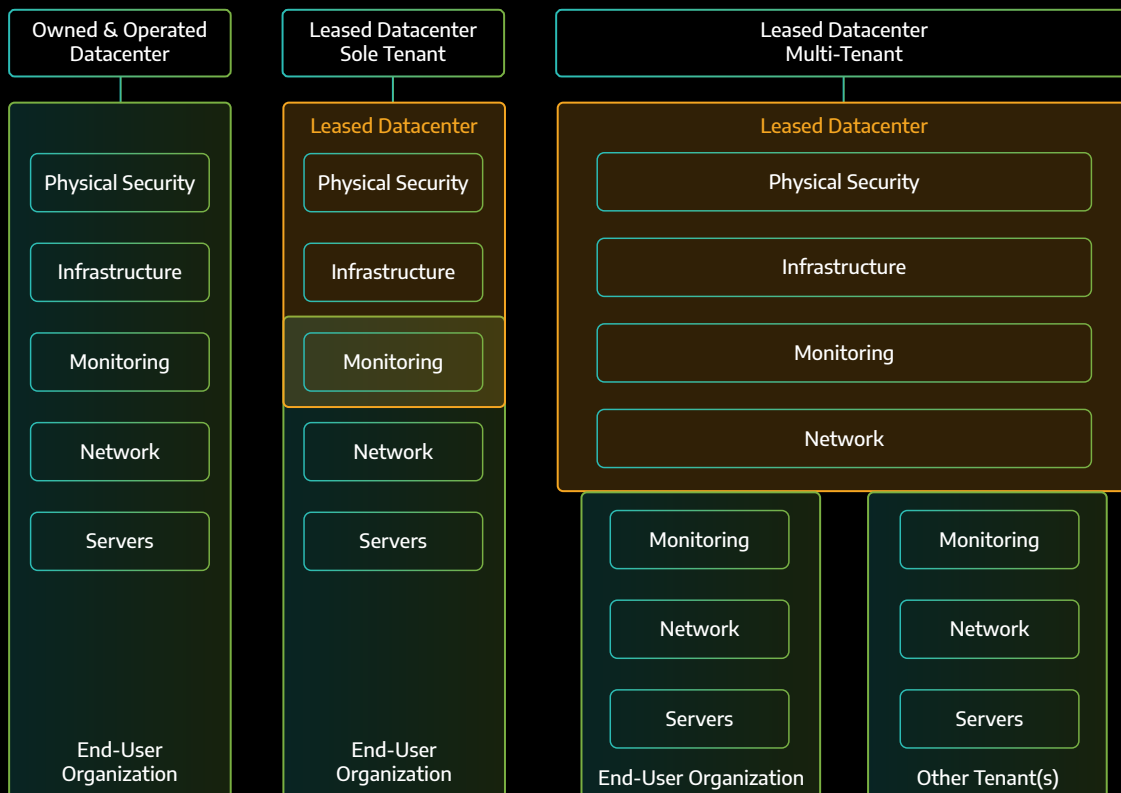


Figure 1: LDC vs. End-User Responsibilities

When an end-user owns and operates their own datacenters, they are responsible for all aspects of running the facility, from the physical security and infrastructure to running the network and servers and monitoring all the systems. In this case, the end-user has total control over all aspects of the facility, including the specific vendors used, the network architecture, and the security measures in place. While this may be desirable from an oversight perspective, it may not be cost effective in all cases. It may be easier and quicker for the end-user to lease space from an already existing datacenter organization.

When an end-user works with a LDC, they may be either the only organization being

hosted at the facility (sole tenant) or one of many organizations being hosted at the facility (multi-tenant). In the case of a sole tenant LDC, the end-user is primarily responsible for the servers and major network infrastructure, the LDC is responsible for the physical security and overall facility infrastructure. Both organizations often share the responsibility for monitoring different systems. In the case of a multi-tenant LDC, the end-user is like any other customer. They are provided equipment rack space, power, and a network connection in a segmented environment. The LDC maintains the overall facility and integrated environment and the end-user maintains their own servers, network connections, and monitoring separate from other tenants.

Description of LDC OT Environments

The LDCs assessed were generally divided into three main environments, as shown in [Figure 2](#) business, customer(s), and OT. The business environment consisted of normal administrative functions, such as human resources, finances, and sales. The customer(s) environment consisted of the services and systems provided to the LDC's customers, such as the dedicated network interfaces, virtual servers, and front-end control panels that customers would use. The OT environment generally consisted of the rest of the systems and services used by the LDC to operate their facility, such as the EMS, building management system (BMS), fire monitoring and suppression, PLCs, generators and heating, ventilation, and air conditioning (HVAC).

When considering the potential impact due to an incident within the OT environment of a datacenter, consequences like health and safety tend to be more localized like those for an electrical substation versus the geographically dispersed effects from an incident in an oil & gas or chemical facility. The time scales for production downtime are much shorter than in those environments, though, often measured in seconds for their EMS and HVAC systems similar to discrete-part manufacturing. If they have a power outage, their backup power generators must start within a few seconds, or the uninterruptible power systems (UPSs) will drain and the servers will shut down. If their HVAC systems stop operating and the customer environments are not cooled properly, they need to start shutting down the customer environments to protect the servers from overheating within a few tens of seconds. These facilities often run at better than 5-9's reliability (99.999%) which equates to approximately 5 minutes of downtime per year.

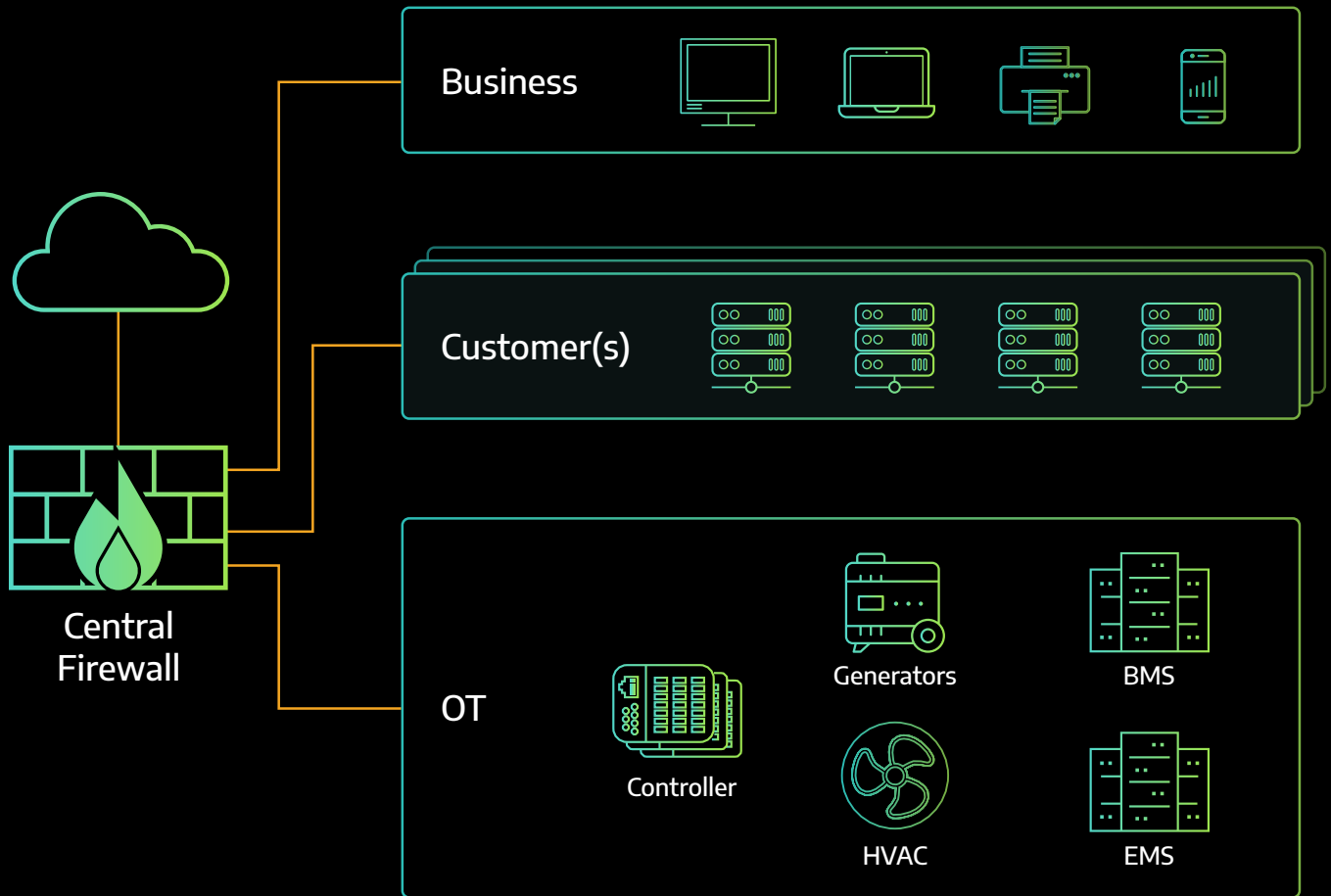


Figure 2: Example LDC Environment

OVERVIEW OF ASSESSMENT METHODOLOGY

The assessment methodology used CMMC version 1.02,³ Level 3 as its base, which encompasses Managed Processes and Good Cyber Hygiene Practices. For CMMC v1.02, Level 3 is seen as the minimum level where the system is protected. CMMC v1.02 also has levels 4 & 5 that are seen as an organizational ability to protect the system from Advanced Persistent Threats (APTs). Since this assessment methodology was trying to evaluate overall cybersecurity maturity for OT organizations, it was capped at Level 3.

CMMC Level 3 consists of 181 individual requirements contained within 17 different cybersecurity domains shown in [Table 1](#). These domains stem from NIST SP 800-171, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*, and are a subset of the ones

developed for NIST SP 800-53, *Security and Privacy Controls for Information Systems and Organizations*. For each requirement, Dragos developed one or more questions, resulting in 339 total questions for the assessment. Each domain had three questions to evaluate the process requirements. The rest of the questions targeted the practices requirements for each of the domains. The questions were phrased so that they could be answered using a small number of discrete, multiple-choice answers. More detailed information about the assessment process and questionnaire is discussed later in [Appendix B – Detailed Description of Methodology](#).

Abbr.	Domain
AC	Access Control
AM	Asset Management
AU	Audit & Accountability
AT	Awareness & Training
CM	Configuration Management
IA	Identification & Authentication
IR	Incident Response
MA	Maintenance
MP	Media Protection
PE	Physical Protection
PS	Personnel Security
RE	Recovery
RM	Risk Management
CA	Security Assessment
SA	Situational Awareness
SC	Systems & Communication Protection
SI	System & Information Integrity

Table 1: CMMC v1.02 Domains

The questions were also evaluated for consistency and implementation. Consistency evaluated how well the organization applied the process or practice across their entire organization. Implementation evaluated how completely the process or practice was implemented. The difference is somewhat subtle. An example of consistency would be having different policies applied to all personnel within one region versus another. An example of implementation would be a process that is currently being instituted across the entire organization but is only 60% complete. The combination of these factors added additional granularity to the responses used during the assessment.

The questions were also assigned a weighting factor based upon their perceived importance to OT. Since the CMMC is focused on protecting the confidentiality of information, there are some requirements that are less relevant to the OT environment. For completeness, Dragos did not remove those requirements from the assessment; however, we did assign a weighting factor to each question that reduced their impact upon the final calculated values of maturity.

Level 0	Incomplete/Unaware
Level 1	Initial/Ad-Hoc
Level 2	Documented/Inconsistent
Level 3	Managed/Practiced
Level 4	Improving/Optimizing

The calculated scores for each question were then tallied to form a fractional score from zero to four for each cybersecurity domain. The scale used loosely follows the one presented in the NIST Cybersecurity Framework (CSF) v1.1. More information on each of these levels can be found in [Appendix B – Detailed Description of Methodology](#).

Overview of Vulnerability Trend Analysis

Over the course of the assessments conducted, several findings and recommendations were identified for each one of the LDCs. When looking across all the individual findings and recommendations, Dragos was able to identify multiple finding categories. These finding categories allowed Dragos to link the findings from the LDCs and start to identify some of the trends. Each of the finding categories was then further grouped into vulnerability trends based on Dragos’s understanding of how they applied to the LDC’s OT environments. The vulnerability trends identified were also found to be like other trends from the 2020 and 2021 Dragos Year in Reviews. This allowed for some comparisons to be made to the cybersecurity posture of other OT organizations. A look at the aggregated vulnerability and trend analysis can be found in [Appendix A – Aggregated Assessment Data](#).

DOMAIN MATURITY

Focusing on the overall maturity assessment, it is natural to first look at the different domains and see where the LDCs had their strengths and weaknesses. [Figure 3](#) shows the minimum, maximum, and average maturity scores for each of the CMMC domains. Four domains scored an average of 2.5 or better: Asset Management (AM), Incident Response (IR), Physical Protection (PE), and Personnel Security (PS). The higher score for these domains is consistent with the business practices for LDCs.

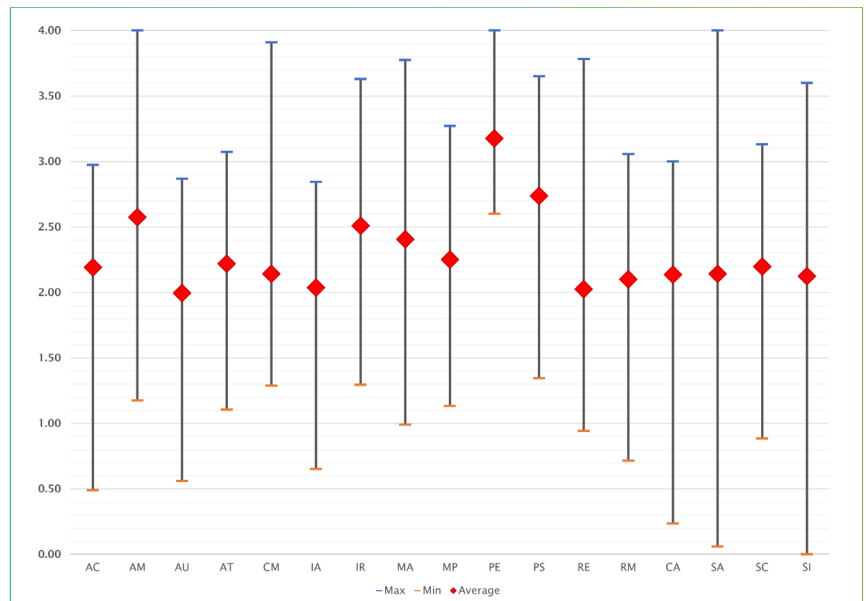


Figure 3: LDC Maturity Levels Per CMMC Domain

Because many of these environments have shared, multi-tenant spaces, they have established very stringent security practices around physical and personnel security, as well as asset management and incident response. The processes they had in place for their customer-facing environments often translated to well managed processes for all their environments, including OT.

While there were no areas where the average LDC performed poorly, there were some domains where they performed lower than others, specifically Audit & Accountability (AU), Identification & Authentication (IA), and Recovery (RE). For AU, the lower score was primarily attributed to lacking monitoring and logging capabilities throughout their OT systems. All the LDCs had well-staffed Network Operations Centers (NOCs) and/or Security Operations Centers (SOCs) to monitor their customer environments and respond to potential network reliability or security events. However, they had not extended their event analysis capabilities to align with the lower levels of the Purdue model.⁴ For IA, the lower score primarily related to the LDCs having less separation from their IT domain than desired, as described in one of the major trends observed in the next section. It was often the case that the LDCs used their IT credentials across both the IT and OT domains.

For RE, the lower score primarily related to conducting recovery tests and having backups of lower-level devices in the OT environment. All the LDCs acknowledged that backups were a necessary part of their cybersecurity program. However, many of them did not regularly test their backups to ensure their processes worked adequately. They may also have conducted restore tests on some systems, but not on all their systems. When looking at their lower-level devices, like PLCs, many of the LDCs believed they would rebuild those configurations from scratch instead of keeping backups of the running program because the configurations and programs were not overly complex.

OVERALL VULNERABILITY TRENDS

As discussed earlier, these assessments were limited to a small sampling of LDCs. Even so, some trends started to emerge by the end of the first year of assessments. This section describes some of the major vulnerability trends observed. A listing of the data is shown later in [Appendix A – Aggregated Assessment Data](#).

Vulnerability Trend	%
Cyber Readiness & Training	25.2%
OT Logging & Monitoring	17.6%
Remote & Vendor Maintenance	16.0%
Separation From IT	24.4%
Other	16.8%

Cyber Readiness & Training

One area regularly observed by Dragos is a weakness in overall cyber readiness and training tailored specific to the OT environment. This was identified as one of the top three vulnerabilities in the 2020 Dragos Year in Review. This is not to say that personnel at these organizations do not receive cybersecurity training or conduct readiness drills. Rather, OT-specific cyber readiness and training

accounts for how those activities have been tailored to the organization's policies, procedures, operating environment, and corporate culture within their OT environments and related to their OT-specific risks.

The topic of cyber readiness and training is broad and covers several individual finding categories, consisting of approximately 25% of the total findings:

- OT-Specific Training,
- OT Threat Intelligence,
- OT-Specific Policies & Procedures,
- OT-Specific Recovery Plan,
- Tabletop Exercises (TTXs), and
- Incident Response.

As stated above, more general topics around each of these individual items were covered by the LDCs; however, they were not specifically tailored to the OT environment. An example of this is the cybersecurity training for personnel. The training was relatively generic and primarily targeted at IT/business-related concepts, such as not opening email attachments from unknown sources and not entering their private information into untrusted websites. While necessary, this training does not relate to the potential risks and cybersecurity-related activities that personnel would face within the OT environment where email and web browsing are usually not allowed.

Separation From IT

Another area that Dragos regularly observed in OT customers is their lack of separation from IT networks and services, identified as two of the top four key findings in the 2021 Dragos Year in Review. Separation from IT is more than separating the networks themselves, although that is one part. The topic of separation from IT covered approximately 24% of the total findings and consisted of the following:

- Network Segmentation,
- Domain Authentication,
- Unsafe Engineering Workstation Practices,
- Hardening, and
- External DNS.

Somewhat different from most OT-focused organizations, LDCs seemed more comfortable utilizing their organization's IT services to operate and maintain their OT environment. In more traditional OT organizations, there can be a clear separation between the OT and IT organizations, sometimes leading to adversarial relationships. The LDCs tended to exhibit a much more collaborative environment, often incorporating many of the common IT services, like networks and domain authentication.

Having organizations leverage integrated services has concrete business advantages and cost savings. The issue with OT and IT sharing resources comes about with the different risks to the business related to the cybersecurity countermeasures applied to those systems. This is not to say that some organizations have not made use of the same network infrastructure, access control systems, and maintenance equipment. Those examples are usually for extremely mature organizations that have well thought out policies and procedures with a very good understanding of all their systems.

The decision to have consolidated and integrated systems needs to be a conscious, risk-based decision for OT organizations. They need to consider the impacts to the organization in the event of

a loss or manipulation of visibility or control of their OT systems and how that translates to overall business risks. During discussions with the LDCs, many had not considered some of the cybersecurity implications of fully integrated systems. In combination with lacking cyber readiness TTXs, they were unaware of the impact from this level of integration.

OT Logging & Monitoring

The number one key finding from the Dragos 2021 Year in Review report relates to visibility inside the OT environment. This project also identified it as a finding and recommendation for the LDCs. This finding combined both OT-specific logging and monitoring as well as the development of a Collection Management Framework (CMF). This finding and recommendation was identified in every LDC, in nearly every region, and constituted 18% of all assessment findings.

It could be interpreted as self-serving to identify this finding and recommendation, given the products and services provided by Dragos. However, at its core, this finding stems from an “assume breach” mentality. Assuming that the system will be breached at some point, whether intentionally or not, is a mindset that has been an important shift in cybersecurity over the past decade or so, especially in OT. No longer are organizations asking, “why would someone attack us?” They are now asking, “what do we do when something happens?” Without having visibility into the environment, organizations have difficulty in detecting, responding, and recovering.

The LDCs all had very well defined and managed NOCs and/or SOCs. This was seen as a core business function, as it was directly related to uptime and reliability of their environments. However, the primary focus of their NOCs and/or SOCs was on their customer environment. When there was integration into the OT environment, it was often only to the network infrastructure equipment and server-style hardware. Workstations and more OT-specific devices, like PLCs, EMS, and BMS, were not often incorporated into this logging and monitoring ecosystem. In some cases, the devices did not have the capability, while in others, they were not configured to send logs and events to a centralized monitoring system.

Remote & Vendor Maintenance

Maintenance, whether it is performed by employees or vendors, is a necessary part of any OT system. The systems, devices, networks, and related equipment may need to be reconfigured or maintained to keep the entire system running at peak efficiency or respond to an event. Included in remote and vendor maintenance are all the ancillary processes that need to be in place to enable personnel to perform these activities. For the LDCs assessed, the finding categories related to remote and vendor maintenance consisted of approximately 16% of the total findings, including:

- Removable Media,
- Vendor Management,
- Multifactor Authentication,
- Remote Maintenance, and
- Physical Security.

Many of the LDCs did not consider remote and vendor maintenance to be an issue until after the discussions with Dragos. They trusted employees and vendors would conduct themselves securely. One of the common philosophies with cybersecurity is “trust, but verify.” It is still very important to implement policies, procedures, and practices to reduce the overall risks to the business that could be caused by the inadvertent or malicious subversion of cybersecurity countermeasures.

Similarly, organizations should implement cybersecurity policies, procedures, and practices that allow personnel to continue to perform their day-to-day activities without inserting too many roadblocks or onerous tasks. Cybersecurity countermeasures should be balanced to reduce risk to the organization, while still allowing personnel to conduct their daily activities with a minimum of overhead. Some situations can be improved with personnel training, while others may require more creative technical solutions.

As an example, removable media is a well-known attack vector into protected systems that may have network-based segregation in place. Personnel will often need to move files into and out of a protected environment. If an organization has policies to disallow removable media, then it needs to also implement a secure file transfer system that is easy for personnel to use such that employees can perform their daily tasks without circumventing cybersecurity countermeasures.

LESSONS LEARNED

While the assessments conducted during this project in 2021 and early 2022 were seen as successful, there were some lessons learned.

Update and Improve the Model

The CMMC model was updated in December 2021. While not fundamentally different, there were some significant changes that would affect its usage moving forward. The most important of these changes was the removal of three domains: Asset Management (AM), Recovery (RE), and Situational Awareness (SA).

For the early 2022 assessments, Dragos spent time updating the questionnaire by decoupling it from being directly related to each requirement in CMMC. The domains that were used by CMMC v1.02 were all kept, since these are a subset of the domains in NIST SP 800-53, and the questions were reorganized to make them flow better during the assessment. We often got questions from the LDCs that we were asking the same or similar questions multiple times because they related to requirements at Levels 1, 2, and 3.

As the team conducting these assessments has expanded, Dragos has found that we need to conduct periodic reviews of the questionnaire to improve the overall coverage and phrasing to assist our assessors and the LDCs.

CMMC and Its Application to OT

One of the recurring issues that Dragos dealt with during these assessments was the need to explain how CMMC applied to the organizations, especially if they had no involvement with the US government. It usually required time to explain that CMMC was only being used as a framework to allow Dragos to build an overall organizational maturity assessment. The questionnaire developed tried to re-imagine the purpose that was behind the requirement, moving past the strict letter of the requirement itself. This included the way Dragos rephrased some of the requirements to look at sensitive information or critical systems for the OT environment.

The process to decouple the questionnaire from being directly related to each of the CMMC requirements was a first step for this activity. Dragos also conducted a cross-mapping effort for each of the questions to a variety of OT standards and guideline documents. This allows us to show how each of the questions is relevant to these industry documents.

The expanding team has also provided Dragos with an opportunity to improve the assessor's context provided along with each of the questions. As we have brought on new team members, they have taken a fresh look at the questions, and we have had an opportunity to tailor the wording of both the questions themselves and the accompanying text with each question to help guide both the assessors and LDCs. Dragos found that these assessments worked better as facilitated self-assessments for the LDCs, which meant that the LDCs were filling in the questionnaires without all the commentary that Dragos personnel normally provided during the interviews. Improving the text that accompanies each question will help Dragos to better work with the LDCs.

NEXT STEPS

After each project that Dragos conducts, an internal retrospective is conducted to review the lessons learned during the project and plan for what needs to be done to improve our processes in the future. In this case, a focus is the need to generalize the model we are using for these assessments and the questionnaire itself.

Multiple models exist to measure overall organizational maturity. CMMC is just one. There are also the Department of Energy (DoE) Cybersecurity Capability Maturity Model (C2M2), the US National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF), and the Capability Maturity Model Integration (CMMI) to name a few. The need for this type of assessment will far exceed the

ability for Dragos to generate independent assessments for each of these frameworks very quickly. Considering that much of the content is consistent between many of these frameworks, it is also unnecessary.

A methodology that can be applied to whatever requirement or maturity framework customers require is needed. Dragos plans to build upon our experience with the CMMC, C2M2, and other assessments to develop a common methodology that can be mapped to the frameworks. This mapping will allow Dragos to tailor the interview questionnaire for the customer with greater ease, reducing the time required to prepare for assessments. Having a more general questionnaire will also allow Dragos to integrate

new frameworks more easily, since the bulk of the material will be consistent with only a small fraction of questions needing to be newly generated.

APPENDIX A – AGGREGATED ASSESSMENT DATA

This appendix presents more information about the data collected during the assessments.

Aggregated Maturity Data

Table 2 shows the aggregated minimum, maximum, and average values displayed in Figure 3.

Domain	Max.	Min.	Avg.
AC	2.97	0.49	2.19
AM	4.00	1.17	2.58
AU	2.87	0.56	2.00
AT	3.07	1.10	2.22
CM	3.91	1.29	2.14
IA	2.84	0.65	2.04
IR	3.63	1.29	2.51
MA	3.78	0.99	2.41
MP	3.27	1.13	2.25
PE	4.00	2.60	3.18
PS	3.65	1.34	2.74
RE	3.78	0.94	2.02
RM	3.06	0.71	2.10
CA	3.00	0.24	2.14
SA	4.00	0.06	2.14
SC	3.13	0.88	2.20
SI	3.60	0.00	2.12

Table 2: Maturity Data Statistics Per CMMC Domain

Findings and Vulnerability Trends

Table 3 shows the finding categories, the corresponding vulnerability trend, and a relative distribution of how many times each category was identified in the LDCs.

Finding Category	Vulnerability Trend	Distribution
OT Logging & Monitoring	OT Logging & Monitoring	High
Network Segmentation	Separation from IT	High
OT-Specific Training	Cyber Readiness & Training	High
Domain Authentication	Separation from IT	High
OT Threat Intel	Cyber Readiness & Training	Moderate
Removable Media	Remote & Vendor Maintenance	Moderate
OT-Specific Policies & Procedures	Cyber Readiness & Training	Moderate
Asset Inventory	Other	Moderate
CMF	OT Logging & Monitoring	Moderate
Insecure Protocols	Other	Moderate
Unsafe Engineering Workstation	Separation from IT	Moderate
Documentation	Other	Moderate
Hardening	Separation from IT	Low
Vendor Management	Remote & Vendor Maintenance	Low
MFA	Remote & Vendor Maintenance	Low
Configuration Management	Other	Low
OT-Specific Recovery Plan	Cyber Readiness & Training	Low
Tabletop Exercises	Cyber Readiness & Training	Low
Remote Maintenance	Remote & Vendor Maintenance	Low
Physical Security	Remote & Vendor Maintenance	Low
External DNS	Separation from IT	Low
Vulnerability Management	Other	Low
Password Policy	Other	Low
Incident Response	Cyber Readiness & Training	Low

Table 3: Finding Category Counts

Table 4 shows the consolidated vulnerability trends and the percentage of total findings.

Vulnerability Trend	%
Cyber Readiness & Training	25.2%
OT Logging & Monitoring	17.6%
Remote & Vendor Maintenance	16.0%
Separation From IT	24.4%
Other	16.8%

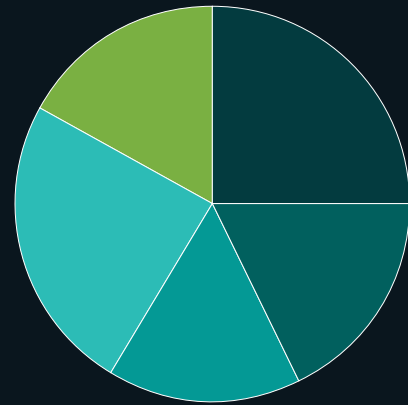


Table 4: Vulnerability Trend Summary



APPENDIX B – DETAILED DESCRIPTION OF METHODOLOGY

A questionnaire was developed that covered each of the requirements in the CMMC. Each requirement had one or more questions associated with it to solicit more information from the LDCs about their OT cybersecurity. [Table 5](#) shows the number of requirements and questions developed for each domain.

Abbr.	Domain	Req.	Ques.
AC	Access Control	25	44
AM	Asset Management	4	5
AU	Audit & Accountability	14	26
AT	Awareness & Training	6	10
CM	Configuration Management	12	24
IA	Identification & Authentication	14	27
IR	Incident Response	10	15
MA	Maintenance	9	11
MP	Media Protection	11	19
PE	Physical Protection	9	17
PS	Personnel Security	5	10
RE	Recovery	6	13
RM	Risk Management	9	21
CA	Security Assessment	8	19
SA	Situational Awareness	4	10
SC	System & Communication Protection	22	44
SI	System & Information Integrity	13	24
Totals		181	339

Table 5: Number of Requirements and Questions for Assessment

The questions were each written so they could be answered using a small number of discrete, multiple-choice answers. This allowed the analysis and reporting to be simplified by associating numeric scores with each of the answers. It also allowed calculations to be made to determine the overall maturity for each domain.

There were four sets of multiple-choice answers:

1	2	3	4
<input type="radio"/> Yes <input type="radio"/> No	<input type="radio"/> All <input type="radio"/> Some <input type="radio"/> None	<input type="radio"/> Fully <input type="radio"/> Largely <input type="radio"/> Partially <input type="radio"/> Not Implemented	<input type="radio"/> Maturity Level 0 <input type="radio"/> Maturity Level 1 <input type="radio"/> Maturity Level 2 <input type="radio"/> Maturity Level 3 <input type="radio"/> Maturity Level 4

The maturity levels discussed earlier were loosely based upon the NIST CSF. Depending on how the questions were worded and their intent, the maturity levels were determined by looking at a combination of people, process, and technology. General descriptions of how each of the maturity levels were determined is shown below.

- Level 0 – Incomplete/Unaware**
 The organization has not demonstrated that they have any executed any processes or have any processes in place to respond to or manage cybersecurity in this area. The organization may or may not be aware that this area applied.
- Level 1 – Initial/Ad-Hoc**
 The organization has demonstrated that they are performing some actions and have some procedures in place related to this area of cybersecurity. The processes are performed ad-hoc and are either undocumented or not fully documented. There is an over reliance on the heroics of personnel to perform these actions or procedures. The organization may have implemented technical solutions; however, they are either not implemented consistently or not implemented in an industry accepted or recommended way.
- Level 2 – Documented/Inconsistent**
 The organization has demonstrated that they are documenting and performing most of their policies, procedures, and technical solutions consistently under normal circumstances. There will be technical solutions in place that generally follow industry recommended practices. There may be inconsistencies in how the organization applies its policies, procedures, and technical solutions across the organization, such as for different facilities or divisions.
- Level 3 – Managed/Practiced**
 The organization has demonstrated that they are documenting and performing all their policies, procedures, and technical solutions consistently across the entire organization under both normal and adverse conditions.
- Level 4 – Improving/Optimizing**
 The organization has demonstrated that they are not just documenting and performing, but also evaluating and improving all their policies, procedures, and technical solutions under both normal and adverse conditions.

In addition to each individual question's specific answer, two other aspects were also included for each question: Consistency and Implementation. Consistency was intended to evaluate how well they applied their policies, procedures, and chosen technical solution across the entire organization. It helped determine if there were organizational units that used different policies, procedures, or technical solutions and was evaluated using the maturity level scale shown above. Implementation was used to measure how completely the policies, procedures, and chosen technical solutions had been implemented throughout the organization. This helped determine if there were different systems that may have been excluded from a particular mitigation. Implementation was evaluated using the scale presented in DoE's C2M2 version 2.0.

- **Fully Implemented** = Complete
- **Largely Implemented** = Complete, but with a recognized opportunity for improvement
- **Partially Implemented** = Incomplete; there are multiple opportunities for improvement
- **Not Implemented** = Absent; the practice is not performed by the organization

The difference between consistency and implementation might seem subtle. An example of consistency would be an organization that acquires a new division. During the transition period when the new division is being integrated, the policies, procedures, and technical solutions may be inconsistent with the parent organization. An example of implementation would be logging and monitoring. An organization may require logging and monitoring for all their servers, workstations, and network infrastructure equipment, but not for their PLCs. They may have mature and consistent policies across their entire organization, but some devices may be exempt.

Dragos also provided a weighting factor for each question. Since the original purpose of the CMMC framework was to protect information, there are some requirements that are more relevant to the OT domain than others. While developing the questions, Dragos determined that there was a need to weight certain questions higher or lower depending on their perceived relevance to the OT environment.

As each of the questions was answered, the weighting factor was multiplied by the combined numeric score to determine the calculated score for that question. Once each of the questions in a particular CMMC domain were answered, the sum of the question responses was divided by the maximum possible score for that domain resulting in the calculated domain score.

REFERENCES

- 1 CMMC was originally developed by the US Department of Defense (DoD) to evaluate the overall cybersecurity posture of contractors in the Defense Industrial Base (DIB) and the way they manage Controlled Unclassified Information (CUI) and Federal Contracting Information (FCI). CMMC was an extension of the self-assessment contracting organizations were already required to perform based upon the NIST Special Publication (SP) 800-171, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*
- 2 For a description of standards, certification, and accreditation, see section 3 of the 2003 paper, titled Environmental and Social Standards, Certification and Labelling for Cash Crops from the Food and Agriculture Organization of the United Nations. <https://www.fao.org/3/y5136e/y5136e07.htm>
- 3 CMMC released version 2.0 in December 2021 after many of the assessments were complete.
- 4 Purdue Enterprise Reference Architecture (PERA), <http://pera.net/>

ABOUT DRAGOS, INC.

Dragos has a global mission: to safeguard civilization from those trying to disrupt the industrial infrastructure we depend on every day. The practitioners who founded Dragos were drawn to this mission through decades of government and private sector experience.

Dragos codifies the knowledge of our cybersecurity experts into an integrated software platform that provides customers critical visibility into ICS and OT networks so that threats and vulnerabilities are identified and can be addressed before they become significant events. Our solutions protect organizations across a range of industries, including power and water utilities, energy, and manufacturing, and are optimized for emerging applications like the Industrial Internet of Things (IIoT).

Dragos is privately held and headquartered in the Washington, DC area with regional presence around the world, including Canada, Australia, New Zealand, Europe, and the Middle East.

**TO LEARN MORE ABOUT DRAGOS
AND OUR TECHNOLOGY, SERVICES,
AND THREAT INTELLIGENCE FOR
THE INDUSTRIAL COMMUNITY,
PLEASE VISIT WWW.DRAGOS.COM.**



THANK YOU