Capability	Practices					COMODO Offerings	
	Level 1 (L1)	Level 2 (L2)	Level 3 (L3)	Level 4 (L4)	Level 5 (L5)	COMODO Product/Service	How COMODO assist?
Domain: Access Control (AC)							
C001 Establish system access requirements	P1001	P1005				MDR Detect COMODO SOC	MDR allows the organization to enable or disable portable storage devices via its ITSM profile settings. (P1006) It is also possible to manage mobile devices via ITSM once it is enrolled. (P1020) All the audit logs including execution of functions are recorded through our ITSM audit logs and they are analyzed by SOC team to be validated. (P1002, P1018) In addition to ITSM audit logs, Comodo SOC is collecting and analyzing logs from multiple log sources to perform their operations. Such events can also be used to support multiple number of capabilities for CMMC (P1001, P1007, P1008, P1009, P1021, P1032) Comodo SOC also has the capability to detect and label different network segments and perform its processes considering different networks such as LAN, WAN, DMZ etc. This allows to define separate rules for the direction of traffic throughout different networks. Having such events supports organizations to validate some capabilities in CMMC. (P1011, P1013) Additionally, customer specific correlation rules can be defined to validate specific security requirements of the organization. (P1003)
		P1006					
C002 Control internal system access	P1002	P1007	P1017	P1023	P1024		
		P1008	P1018	P1025			
		P1009	P1019				
		P1010	P1012				
		P1011	P1020				
C003 Control remote system access		P1013	P1014	P1032			
		P1015	P1021				
C004 Limit data access to authorized users and processes	P1003	P1016	P1022				
	P1004						
Domain: Asset Management (AM)							
C005 Identify and document assets			P1035			MDR Detect	MDR combines all the asset related data from AD, network traffic and customer itself; and creates an asset model for the organization. This model is used by SOC operations such as Incident Handling and Response, Reporting and/or Threat Hunting. Additionally, this model can be enhanced and enriched to satisfy some compliance capabilities. (P1126, P1035)
			P1036				
C006 Manage asset inventory				P1226			
Domain: Audit and Accountability (AA)							
C007 Define audit requirements		P1041	P1045			MDR Detect	Our MDR solution comes with a powerful network sensor that is installed on customer infrastructure. In addition to collecting and analyzing raw network traffic via mirror port configuration, or using hub/ TAP devices, Network Sensor also provides log forwarder functionality which allows customers to forward audit (or any other) logs to MDR using our common event model. (P1048) These collected events are reviewed and analyzed by our SOC team and any kind of suspicious activities are reported to customer immediately by some automatic and manual escalation processes. (P1044, P1045, P1049, P1051, P1053, P1054) Our SOC also provides regular audit reports for our customers compliant with PCI-DSS and HIPAA regulations. (P1052) We can also create asset repository by collecting required data from the organization and identify assets not reporting audit logs properly if requested. (P1055)
			P1046				
C008 Perform auditing		P1042	P1048		P1055		
		P1043					
C009 Identify and protect audit information			P1049				
			P1050				
C010 Review and manage audit logs		P1044	P1051	P1053			
			P1052	P1054			
Domain: Awareness and Training (AT)							
C011 Conduct security awareness activities		P1056	P1058	P1059		N/A	N/A
				P1060			
C012 Conduct training		P1057					
Domain: Configuration Management (CM)							
C013 Establish configuration baselines		P1061				MDR Detect	MDR allows organization to fetch all user installed software list per device and monitor it through ITSM. (P1063) This knowledge combined with action logs can be used to validate software related security policies. P(1069, P1073) It is also possible to apply customized security configurations to each device through security profiles. (P1064) All the configuration changes from authorized users and attempts from unauthorized users are logged. (P1065) MDR stores all the network traffic logs which allows the organization to follow all actions over ports, protocols or services when necessary. P(1068)
		P1062					
		P1063					
C014 Perform configuration and change management		P1064	P1067	P1073	P1074		
		P1065	P1068				
		P1066	P1069				
Domain: Identification and Authentication (IDA)							
C015 Grant access to authenticated entities	P1076	P1078	P1083			N/A	N/A
	P1077	P1079	P1084				
		P1080	P1085				
		P1081	P1086				
		P1082					
Domain: Incident Response (IR)							
C016 Plan incident response		P1092		P1100	P1106	COMODO SOC	Our SOC team provides 24/7 IHR service by combining audit logs, network events and the other events that are generated by our security solutions such as AEP, EDR or DLP. (P1107, P1094, P1096) SOC service covers all four steps of IHR that is defined by NIST as Preparation; Detection and Analysis; Containment, Eradication and Recovery; Post-Incident Activity; (P1092) and we also follow MITRE ATT&CK vector to determine attacker's TTPs and classify the incidents. (P1100). Our service uses AWS infrastructure to store all short and long time events and provides regular reports to customers such Operational Report, Executive Report, Compliance Reports or Incident Report. (P1093, P1098) We also provide a powerful correlation engine that uses both signature and behavior based approaches to detect anomalous activities and we use automatic and manual approaches to notify the customer in case of a high priority incident. (P1102) In such significant cases, a detailed incident report is provided to customer including the investigation results of root cause of analysis of the incident. (P1097) We apply follow the sun model with our analysts on four geographical locations around the world, therefore our SOC is online 24/7 for not only to analyzing incidents and but also providing quick response to customer. (P1101)
C017 Detect and report events		P1093					
		P1094					
C018 Develop and implement a response to a declared incident		P1096	P1098	P1101	P1102		
					P1107		
					P1108		
C019 Perform post incident reviews		P1097					
C020 Test incident response			P1099		P1110		
Domain: Maintenance (MA)							
C021 Manage maintenance		P1111	P1115			N/A	N/A
		P1112	P1116				
		P1113					
		P1114					
Domain: Media Protection (MP)							
C022 Identify and mark media			P1122			MDR Detect	MDR allwos to control the use of removable media, either allow to access or disable. (P1221)
C023 Protect and control media		P1119	P1123				
		P1120					
		P1121					
C024 Sanitize media	P1118						
C025 Protect media during transport			P1124				
			P1125				
Domain: Personnel Security (PS)							

C026 Screen personnel		P1127				N/A	N/A
C027 Protect federal contract information during personnel actions		P1128					
Domain: Physical Protection (PP)							
C028 Limit physical access	P1131	P1135	P1136			N/A	N/A
	P1132						
	P1133						
	P1134						
Domain: Revocery (RE)							
C029 Manage back-ups		P1137	P1139			N/A	N/A
		P1138					
C030 Manage information security continuity					P1140		
Domain: Risk Management (RM)							
C031 Identify and evaluate risk		P1141	P1144	P1149		MDR Detect	Vulnerability assessment is one of the core functionalities in MDR. Network sensor can be scheduled to perform a vulnerability scan on predefined networks with predefined scan period. MDR offers regular vulnerability assessment report to customer. (P1142) This reports play a crucial role for customer when remediating the devices with detected vulnerabilities. (P1143) MDR get benefits from multiple threat intelligence resources to analyze network traffic. SOC team also perform regular threat intelligence improvements in order to adapt the latest updates in cyber security threats. (P1150) Regular MDR reports (i.e Operational Report, Executive Report) and MDR metrics presents how SOC is performing and what kind of threats has been detected and reported to customers. Such information could be useful when analyzing the effectiveness of security solutions in the organization. (P1155)
		P1142		P1150			
				P1151			
C032 Manage risk		P1143	P1146		P1152		
			P1147		P1155		
C033 Manage supply chain risk				P1148			
Domain: Security Assessment (SAS)							
C034 Develop and manage a system security plan		P1157		P1163		N/A	N/A
C035 Define and manage controls		P1158	P1161	P1164			
		P1159		P1165			
C036 Perform code reviews			P1162				
Domain: Situational Awareness (SA)							
C037 Implement threat monitoring			P1169	P1171		COMODO SOC	Our SOC team contains multiple components, one of which is Threat Hunting (P1171). In this scope, our Tier-3 analyst team is collecting hign amount of IoCs from our customer organizations, information sharing platforms (i.e MISP), and varied threat sources. (P1169, P1173)
				P1173			
Domain: System and Communications Protection (SCP)							
C039 Define security requirements for systems and communications		P1178	P1177	P1197	P1198	MDR Detect	Network Monitoring is the core functionalitiy of MDR. Network Sensor captures network communications of the customer. (P1198) This data allows the SOC to provide reports about internal and external network communication, therefore that helps the customer to validate network related security policies. (P1183, P1184, P1186)
		P1179	P1180	P1228	P1230		
			P1181				
			P1182				
			P1183				
			P1184				
			P1185				
			P1186				
			P1187				
			P1188				
			P1189				
			P1190				
			P1191				
C040 Control communications at system boundaries	P1175		P1192	P1199	P1208	MDR Protect	ITSM allows customers to implemet a policy restriction to publicly accessible websites. (P1193) Moreoever, it is possible to manually utilize devices with CSS settings to enforce URL filtering on them to block access to websites that are not approved by the organization. (P1129) MDR provides sandboxing functionality in terms of endpoint protection with ITSM. Once an executable or script has been detected, the file is analyzed and it is contained to run in containment if it is determined to be suspicious.(P1202) Comodo Dome covers domain name filtering, which is not inbuild with MDR. This solution allows customers to block custom selected domains, moreover it allows to utilize threat intelligence to proactively block DNS requests from malicious domains. (P1192, P1199)
	P1176		P1193	P1202			
				P1229			
Domain: System and Informational Integrity (SII)							
C041 Identify and manage information system flaws	P1210	P1214		P1221		MDR Detect COMODO SOC	Our SOC team monitors system security alerts and advisories and take action in response. (P1214) SOC works together with Comodo threat lab and it uses other third party threat intelligence in order to perform advance analysis and threat hunting processes. (P1221) MDR provide protection from malicious code by containment -sandboxing- service. (P1211) Additionally, it performs periodic scans on all available devices in order to detect any kind of malicious files. (P1213) MDR also performs behavioral analysis to detect suspicious behaviors on the organizational devices. (P1122) MDR provides protection for malicious emails as well, once an email is opened with any malicious code or attachment, it is contained in our containment.(P1220, P1218) Patch management service of MDR is responsible to keep the product up-to date after each release. (P1212) Network Monitoring is the core functionality of MDR. Network Sensor captures all internal and external communications of the organization and analyzes them both automatic and manual processes to detect possible attacks. (P1216, P1217) In addition to signature based detection, our MDR provides behavior based analysis to detect anomalous or suspicious behaviors, as well. (P1222)
C042 Identify malicious content	P1211				P1222		
	P1212						
	P1213						
C043 Perform network and system monitoring		P1216	P1218		P1223		
		P1217					
C044 Implement advanced email protections			P1219				
			P1220				