The Cybersecurity Maturity Model Certification (CMMC) in Practice

Background

In the last few years every industry has witnessed a growing number of cyber attacks, and with it, each week a new hacker group has been identified, and carried on with its injurious mission. Every day a new vulnerability is found and being exploited, and every other day news breaks that millions of corporate and private user credentials are leaked on the Dark Web or being sold on illegal markets.

While it has become a natural part of everyday life, the damage caused by cyber attacks is growing rapidly, and the overall sum is enormous: 5 trillion dollars this year alone and it will reach $6 trillion in 2021. But of course the real damage is not always financial loss. It can be data loss as well, and breach of sensitive/strategic data, or in other cases: damaging loss of credibility, market share or clientele.

Some threat actors are for-profit criminals and hacking groups, but – what makes the situation even more distressing – the biggest threat actors are state-sponsored APT (Advanced Persistent Threat) groups, operating under the permission and protection of a foreign regime. Their goal is not money – or not just money – but intelligence gathering, diversion, disinformation and sabotage, and ultimately something political. It has become quite clear, the international pursuit of state interests has given birth to a new theater of war operations, namely cyber warfare. This picture is not exaggerated at all: the security and the defense capabilities of the State are at stake.

This is why the Cybersecurity Maturity Model Certification (CMMC) was born, for cyber warfare not only poses a threat to industrial sector infrastructure. Contractors of the Department of Defense must comply with rigorous cybersecurity requirements in order to protect valuable assets, Controlled Unclassified Information, and military industry technologies belonging to the Government.

Overview

The Cybersecurity Maturity Model Certification (CMMC) is a unified standard for implementing minimum cybersecurity standards in the entire supply chain of the Department of Defense. According to estimates it will be mandatory for over 300,000 suppliers, including the nation's largest manufacturers, small businesses, sub-contractors and foreign suppliers who handle or produce sensitive defense material or information. These contractors will need to complete a CMMC assessment and certification, that has to be renewed every 3 years.

Levels

There are five levels of CMMC certification, each level reflects the maturity of a contractor's cyber security infrastructure to protect sensitive government information. These five levels can be divided into two groups. On the first three levels suppliers need to implement security measures from "basic cyber hygiene" to "good cyber hygiene" using basic security practices, for example antivirus software, changing passwords regularly, and using practices to safeguard CUI (Controlled Unclassified Information). Levels four and five on the other hand require advanced, proactive cybersecurity practices that can defend CUI from Advanced Persistent Threats (APTs) or prevent long-term attacks to mine for sensitive information.

Domains

The CMMC model consists of 17 domains, many of them originated from the Federal Information Processing Standards (FIPS) 200 security-related areas, the NIST SP 800-171 security requirements (Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations), and many additional practices from other standards. Each domain contains a set of processes and capabilities (and in turn, practices) across the five levels.

Domains and Capabilities:

Access Control (AC)

Establish system access requirements

Control internal system access

Control remote system access

Limit data access to authorized users and processes

Asset Management

Identify and document assets

Audit and Accountability (AA)

Define audit requirements

Perform auditing
Identify and protect audit information

Review and manage audit logs

Awareness and Training (AT)

Conduct security awareness activities

Conduct training

Configuration Management (CM)

Establish configuration baselines

Perform configuration and change management

Identification and Authentication (IDA)

Grant access to authenticated entities

Incident Response (IR)

Plan incident response

Detect and report events

Develop and implement a response to a declared incident

Perform post incident reviews
Test incident response

Maintenance (MA)

Manage maintenance

Media Protection (MP)

Identify and mark media

Protect and control media

Sanitize media

Protect media during transport

Personnel Security (PS)

Screen personnel

Protect CUI during personnel actions

Physical Protection (PP)

Limit physical access

Recovery (RE)

Manage back-ups

Risk Management (RM)

Identify and evaluate risk

Manage risk

Security Assessment (SAS)

Develop and manage a system security plan

Define and manage controls

Perform code reviews

System and Communications Protection (SCP)

Define security requirements for systems and communications

Control communications at system boundaries

System and Information Integrity (SII)

Identify and manage information system flaws

Identify malicious content

Perform network and system monitoring

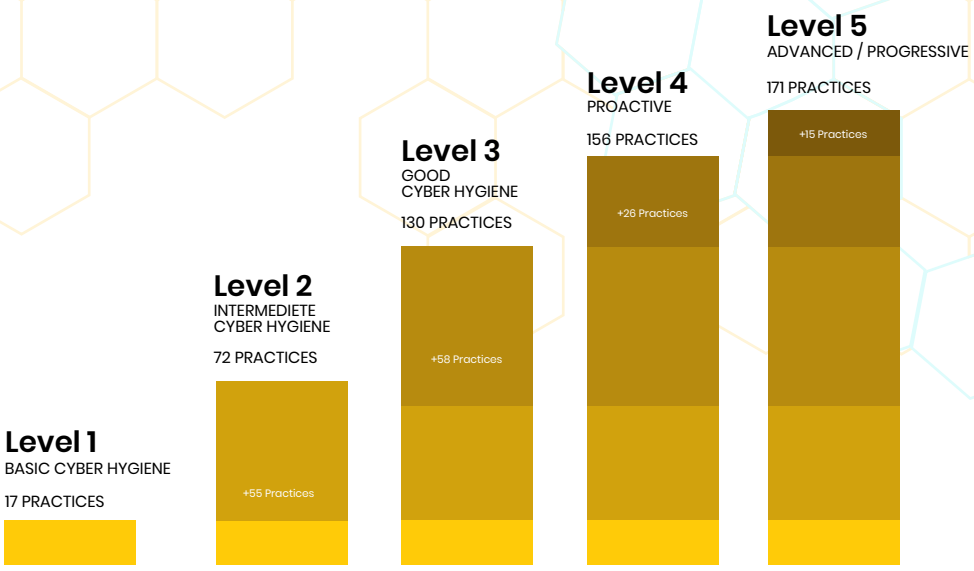
Implement advanced email protections

Situational Awareness (SA)

Implement threat monitoring

Leveled Practices

The CMMC model contains 171 individual practices that are mapped across the five levels for all capabilities and domains. Each level requires the lower level's practices.



Comparing layers of maturity on different levels

Most of the CMMC domains are defined on many different levels and impose several practices or regular tasks in these domains but with different requirements.

Situational awareness (SA) domain, for example, appears only at Level 3, stating that suppliers must receive and respond to cyber threat intelligence from information sharing forums and sources, and communicate to stakeholders. By comparison, in Level 4, a particular emphasis is placed on proactive, advanced techniques: maintaining a cyber threat hunting capability, and detecting, tracking, and disrupting threats that evade existing controls.

In the Security assessment (CA) domain, Level 2 requirements, amongst others, are: periodically assessing the security controls in organizational systems to determine if the controls are effective in their application. One the other hand, by Level 3, the supplier should monitor and test the security controls on an ongoing basis to ensure the continued effectiveness of the controls, and on Level 4 this domain imposes penetration testing and red teaming probes against organizational assets periodically in order to validate defensive capabilities.

Levels 1-3

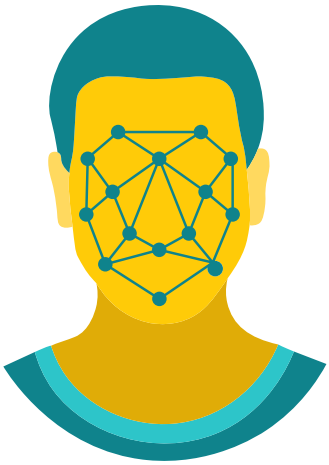
Level 1

Processes (performed): Level 1 requires that an organization perform the specified practices. Because the organization may only be able to perform these practices in an ad-hoc manner and may or may not rely on documentation, process maturity is not assessed for Level 1.

Practices (Basic Cyber Hygiene): In CMMC Level 1 the main objective is to protect Federal Contract Information (FCI). FCI is basically "information, not intended for public release, that is provided by or generated for the Government under a contract to develop or deliver a product or service to the Government." Basic practices should include: using only company assets (printers, computers and laptops, media devices) in the company network, consistent password management for each user and role, limit access to authorized users only, control and limit connections to external networks (including WiFi) and information systems, keep FCI information safe from publicly accessible platforms. In general, these practices are basic, everyday safety measures that need to be performed properly without integrated feedback mechanisms or continuous evaluation.

Key domains and practices in Level 1:

Identification and authentication



Identify information system users, processes acting on behalf of users, or devices

Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems

Physical protection

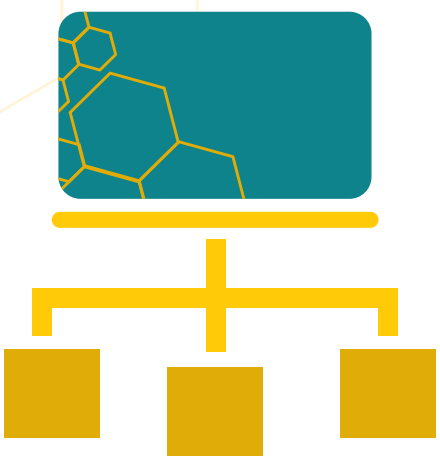
Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals

Escort visitors and monitor visitor activity

Maintain audit logs of physical access

Control and manage physical access devices

System and communications protection



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

Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks

Identify, report, and correct information and information system flaws in a timely manner

Provide protection from malicious code at appropriate locations within organizational information systems

Update malicious code protection mechanisms when new releases are available

Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed

System and information integrity

Interestingly, as early as Level 1, the Media Protection domain has a firm standpoint on data storage media: before reuse or disposal, every media containing Federal Contract Information should be sanitized or destroyed.

Level 2

Level 2 basically describes a transition phase and introduces the importance of documentation and security practices that require system-wide, repeatable drills. In contrast to Level 1, these practices require or are based on process documentation, for example periodically scanning vulnerabilities, and require certain built-in feedback mechanisms.

Processes (documented): In terms of cyber security processes, Level 2 introduces maturity into the CMMC model and also serves as a transitional phase between basic security measures and sound protection of CUI. This level requires that an organization establish and document practices and policies to guide the implementation of their CMMC efforts. The documentation of practices enables individuals to perform them in a repeatable manner. Organizations develop mature capabilities by documenting their processes and then practicing them as documented.

Practices ("Intermediate Cyber Hygiene"): Level 2 is basically building a bridge from Level 1 to Level 3 and consists of a subset of the requirements specified in NIST SP 800-171 as well as practices from other standards and references. It contains 72 cyber security practices, part of them address the protection of CUI.

Some examples from the required practices in Level 2:

Access control

Limit use of portable storage devices on external systems

Limiting unsuccessful logon attempts

Monitoring remote access sessions

Implement the principle of least privilege, including for specific security functions and privileged accounts

Risk management

Periodically assessing risks to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, storage, and transmission of CUI

Periodically scanning vulnerabilities in organizational systems and applications

Remediate vulnerabilities in accordance with risk assessments

Recovery

Regular performance and testing of data back-ups

Protecting the confidentiality of CUI information at storage locations

Security assessment

Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems

Periodically assess the security controls in organizational systems to determine if the controls are effective in their application

Hint: According to the Department of Defense, no contracts will require this level, because it can be described as a transition phase. Nevertheless it may count as a sign of maturity and good cybersecurity hygiene to business partners and investors. But contracts where storage or transmission of CUI information is essential will require Level 3 certification. Note: regardless of public procurement assessment, Level 3 is still built on Level 2 requirements.

Level 3

Generally, Level 3 introduces the concept of a planned, and ongoing security management, the constant reviewing and evaluating of applied policies and practices. This should ensure that security solutions are implemented correctly and are able to be fully effective while being actively monitored.

For a defense contractor, Level 3, as the Level motto phrase "good cyber hygiene" suggests, means that security becomes a priority, the top concern of the organization. Therefore the emphasis is on planning and constantly reevaluating security practices. Continuous logging, log analysis, monitoring and Incident Response is also an important part of Level 3 requirements.

Processes (managed): Level 3 requires that an organization establish and maintain a plan demonstrating the management of activities for practice implementation. The plan may include information on missions, goals, project plans, resourcing, required training, and
involvement of relevant stakeholders.

Practices ("good cyber hygiene"): the practices of this level focus on the protection of CUI and encompass all of the security requirements specified in NIST SP 800-171 as well as additional practices from other standards and references to mitigate threats.

Some examples from the required practices:

Access control

Separate the duties of individuals to reduce the risk of malevolent activity without collusion

Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs

Automatically terminate user sessions after a defined condition

Employ cryptographic mechanisms to protect the confidentiality of remote access sessions

Authorize remote execution of privileged commands and remote access to security-relevant information

Audit and Accountability

Review and update logged events
Alert in the event of an audit logging process failure

Collect audit information (e.g., logs) into one or more central repositories

Protect audit information and audit logging tools from unauthorized access, modification, and deletion

Correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity

Provide audit record reduction and report generation to support on-demand analysis and reporting

Media protection

Mark media with necessary CUI markings and distribution limitations

Prohibit the use of portable storage devices when such devices have no identifiable owner

Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards

Incident response

Track, document, and report incidents to designated officials and/or authorities both internal and external to the organization

Test the organizational incident response capability

Situational awareness

Receive and respond to cyber threat intelligence from information sharing forums and sources and communicate to stakeholders

Event logging and log analysis on CMMC Level 3

A new aspect in this level is the event monitoring and analysis capability that in the most cases will require sophisticated software solutions or third-party providers of Incident Response and Incident Reporting. In most cases it means implementing a Security Operations Center (SOC) for capturing logs and a SIEM (Security Information and Event Management) or MSS (Managed Security Services) solution for analysis and investigative purposes. Outsourcing security management could be a reasonable solution, especially for organizations with limited staff or shortage of security specialists.

Protection against malicious network traffic

With the domains System and Communication Protection (SC) and System and Information Integrity (SI) come another set of active defense capability requirements: protection against malicious traffic, DNS filtering, spam protection, and email sandboxing. Defense contractors can employ many forms of network security software or cloud-based solutions to identify, detect, and block threats like malicious websites, zero-day vulnerabilities, or phishing, malware and ransomware threats. With email sandboxing solutions all suspicious files and URLs attached to an email can be opened and inspected in a safe and isolated environment.

Level 4

Levels 4 and 5 introduce not only completely new criteria but a different perspective. The CMMC model begins to focus more on the proactive practices, like threat detection and threat response. This way an organization can address the changing Tactics, Techniques, and Procedures (TTPs) used by Advanced Persistent Threat groups (APTs).

Key domains and practices in Level 4:

Risk management

Periodically perform risk assessments to identify and prioritize risks according to the defined risk categories, risk sources, and risk measurement criteria

Develop and implement risk mitigation plans

Incident Response

Use knowledge of attacker tactics, techniques, and procedures in incident response planning and execution

Establish and maintain a security operations center (SOC) capability that facilitates a 24/7 response capability

Configuration Management

Employ application whitelisting and an application vetting process for systems identified by the organization

Access control

Control information flows between security domains on connected systems

Periodically review and update CUI program access permissions

Restrict remote network access based on organizationally defined risk factors such as time of day, location of access, physical location, network connection state, and measured properties of the current user and role

Risk Management

Catalog and periodically update threat profiles and adversary TTPs

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

Perform scans for unauthorized ports available across perimeter network boundaries over the organization's Internet network boundaries and other organizationally defined boundaries

Develop and update as required, a plan for managing supply chain risks associated with the IT supply chain

Security Assessment

Create, maintain, and leverage a security strategy and roadmap for organizational cybersecurity improvement

Conduct penetration testing periodically, leveraging automated scanning tools and ad hoc tests using human experts

Periodically perform red teaming against organizational assets in order to validate defensive capabilities

Audit and Accountability

Automate analysis of audit logs to identify and act on critical indicators (TTPs) and/or organizationally defined suspicious activity

Review audit information for broad activity in addition to per-machine activity

New technical and procedural practices to implement

The SOC-SIEM-MSSP-CASB solutions

The Audit and Accountability domain of Level 3 and Level 4 suggests that implementing SOC (Security Operation Center) is required for scanning, monitoring and forensics capabilities.
Also, employing a SIEM solution for centralized log management, log auditing and log analysis is essential.
A Managed Security Services Provider (MSSP) can be useful for ongoing policy and procedure support.

Finally, when an organization heavily leans on cloud-based frameworks, implementing a Cloud Access Security Broker (CASB) solution is required to protect CUI.

Threat Intelligence

Another new security approach at Level 4 is the recommendation to gather and utilize up-to-date intelligence on known attacker TTPs in order to plan and facilitate Incident Response procedures. This can be done by following industry-specific cyber security warnings, the recommendations and alerts of Cybersecurity Agencies, like CISA or NIST.

Know your APTs

Advanced persistent threats mostly operate in a different way in each industrial sector, therefore it is important to know how these groups will try to penetrate your systems and what type of information they are after. Getting warnings and threat reports regularly gives a clear picture on what kind of threats to expect on a sectoral basis. Reports about recent breaches are also useful to be informed on new APT techniques and new vulnerabilities.

Threat hunting

Active APTs usually leave obvious traces when attacking network infrastructure and organization assets, and these data fragments can in many cases identify or warn about a malicious attempt. These traces are called Threat Indicators, and Threat Hunting is a way to collect and identify them. An indicator can be a hostname, an IP address, a hash string, a network request payload or an identified malicious script fragment that could be able to penetrate a supplier organization's network. When an indicator is identified, it always points to an ongoing attack, or at least, a preparation/reconnaissance phase of a future attack, in the best case.

Know your APTs

Advanced persistent threats mostly operate in a different way in each industrial sector, therefore it is important to know how these groups will try to penetrate your systems and what type of information they are after. Getting warnings and threat reports regularly gives a clear picture on what kind of threats to expect on a sectoral basis. Reports about recent breaches are also useful to be informed on new APT techniques and new vulnerabilities.

Threat hunting

Active APTs usually leave obvious traces when attacking network infrastructure and organization assets, and these data fragments can in many cases identify or warn about a malicious attempt. These traces are called Threat Indicators, and Threat Hunting is a way to collect and identify them. An indicator can be a hostname, an IP address, a hash string, a network request payload or an identified malicious script fragment that could be able to penetrate a supplier organization's network. When an indicator is identified, it always points to an ongoing attack, or at least, a preparation/reconnaissance phase of a future attack, in the best case.

Level 5

Level 5 is the highest achievable CMMC Level, where all 171 security controls must be implemented. The general vision of Level 5 is a proactive organization with advanced intelligence and defense techniques, and it will be required by suppliers focused on critical technologies and more sensitive programs. A company at this level must have standardized and optimized practices and many advanced techniques to provide a more effective threat detection and threat response capability. According to the Department of Defense, about 1 percent of the defense contractors will need this compliance level.

Processes (optimizing): Level 5 requires an organization to standardize and optimize process implementation across the organization.

Practices (advanced, proactive): Level 5 focuses on the protection of CUI from APTs. The 15 additional practices increase the depth and sophistication of cybersecurity capabilities.

System and communications protection

Employ organizationally defined and tailored boundary protections in addition to commercially available solutions

Risk management

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

Incident Response

In response to cyber incidents, utilize forensic data gathering across impacted systems, ensuring the secure transfer and protection of forensic data

Use a combination of manual and automated, real-time responses to anomalous activities that match incident patterns

Establish and maintain a cyber incident response team that can investigate an issue physically or virtually at any location within 24 hours

Perform unannounced operational exercises to demonstrate technical and procedural responses

System and information integrity

Monitor individuals and system components on an ongoing basis for anomalous or suspicious behavior

Threat Intelligence and Threat hunting

Compared to Level 4, Threat Intelligence and Threat Hunting requirements are defined as a 24/7 practice on Level 5. A response team should be set up and managed, that can detect and mitigate TTPs in real time while being prepared for any kind of security incident. This team should review all systems annually using the latest threat intelligence, while analyzing and detecting every malicious activity.

Forensics capabilities

Suppliers on Level 5 should set up or contract organizations that can scan and analyze malicious files, email attachments, scripts or executables (software or updates) via sandboxing and/or Malware Analysis solutions.

Tailored solutions

CMMC states that suppliers should deploy "organizationally defined and tailored boundary protections in addition to commercially available solutions". This notion means that beyond standard network and asset protection, such as firewalls, IDS-IDPS, NIDS, SIEM solutions, the usual indicators and event metadata should be enriched from Intelligence sources and sector-specific data mining. For example, an identified attacker's IP address and possible identity can be looked up in a Dark Web mining framework, both on Tor and I2P networks. Or, using another aggregated crawling solution, organizations can launch automated search with these identifiers both on Hacking Forums or Pastebin-like sites.

Real life CTI examples

Levels 4 and 5 impose an intelligence-based strategy against APTs and other threat actors. Many of Cyber Intel Matrix's solutions are in line with these requirements, since threat intelligence, Dark Web monitoring, Honeypot Network Operation and Account Takeover Research are the core concepts of the CIM Framework.

Dark Web

On CMMC Level 4, an important requirement is the active monitoring of possible APT activity (with advanced SIEM solutions), but Level 5 goes further: defense contractors must have an intelligence capability to detect all adversary activities and, for example, monitor any discussion about TTP techniques on the available online media platforms. So, if a manufacturer has been hit by a cyber attack, an alert service can be set up on the Dark Web that detects IPs used by APTs, and scripts that are related to known malwares used by APT groups. This approach can reveal the origin of on attack, the actual objective of the attackers, and helps predict the future behavior of the adversary group in question. It is also possible to estimate the potential industrial target sectors and the Tactics, Techniques, and Procedures the attackers might use in the future.

In the unfortunate event that an attacker successfully penetrates security and a data breach is likely to happen, the damage can be mitigated by setting up a monitoring process that searches for the possible leakage (emails, network setup configurations, credentials, employee names) on forums and markets where hackers usually dump or sell these data. If the described alerting confirms the data breach, after evaluating the leaked information all reversible credentials and configurations can be changed to prevent further damage, since in many cases hackers are not using credentials for direct authorization, they are only trying to sell them. It can also verify the fact and the extent of the breach, and gives certain advantage of having adequate solutions at hand before other hacker groups and the general public are informed about the breach.

Hacking forums

On the other hand, Dark Web forums frequently discuss hacking techniques, disassembling know-how: how to hack a corporate network, what are the vulnerabilities and weaknesses of industrial network devices, protocols, PLCs or HMIs. A good example of this is a recent Dark Web finding from the CIM Platform, that showed that a known healthcare manufacturer's popular heart monitoring device has been disassembled by a hacker and finally hacked. The admin credentials were retrieved and leaked on the Dark Web, and the device became vulnerable and probably dangerous to patients, since it could be stopped or reconfigured anytime by an adversary actor.

Another example is the forum activities where the vulnerabilities of automotive industry related protocols were discussed. Hackers and IT enthusiasts are discussing every day how a Modbus protocol or a vehicle media device can be hacked or reprogrammed. Or, how to stop a driving car, or how to start a steady car.

There are also online communities that are specialized in researching and selling undiscovered Zero Day vulnerabilities for Network Security Tools, CMS platforms, common electronic devices, industrial PLCs, and so on. A manufacturer and product oriented alerting can point out what software needs to be updated, changed or monitored closely, and ultimately the organization itself can develop protective measures against vulnerabilities discovered by Dark Web alerts.

Account takeover research

The CIM development team maintains a research mechanism for Account Takeovers that usually come from well hidden dumps by hackers on the dark web, and some user databases (user-password combo lists) can be found on pastebin sites. We have found that a surprisingly big share of data posted on pastebin sites contains corporate information. An everyday story is that a security specialist of a company needs to purchase and install security devices (electronic locks, CCTV cameras, and the like), so he registers on an security vendor online with his company credentials and orders the equipment. A few months later the vendor suffers a data breach and his company credentials end up on the Dark Web. If a hacker wants to target his company, downloads the data breach and logs in with the employee's credentials (and sadly in many cases the company password is the same as the one used for third party registration, which poses further threat to the company), and can see what type of devices the security professional bought, the manufacturer of the equipment, and can easily learn existing and new vulnerabilities of that device, and can practice and experiment with it, just like in the movies.

The data breaches available on the Dark Web also can be used by hackers to prepare phishing and Social Hacking attacks. For example when a user account breach of 50-60 employees belonging to one company appears on illegal markets, a thorough employee profiling can be performed, focusing on personal habits and weaknesses, that can open enormous cracks in the security of the company. A regular Account Takeover check can mitigate these kinds of threats.

Honeypot Network Operation

On CMMC Level 5 suppliers are required to implement "organizationally defined and tailored boundary protections," which means network protection intelligence specific to the sector and the given industry. This requirement can be achieved by utilizing smart feeds from a Honeypot Network that simulates entire industry-specific networks, network protocols, programmable logic controllers and webservers, by imitating real business infrastructures, like financial providers with affiliates, an entire oil refinery, or production lines.

Once online, these simulated infrastructures will be experiencing several types of cyber attacks, and start to provide valuable information on attackers, their possible goals and methods. This data can be enriched with Dark Web Intelligence, and with well known databases for attacker profiling and detection in order to set up adequate APT defense mechanisms. Using AI technologies, new correlations and sector-specific behavioral patterns also can be established from this data, but most importantly it maps the operations of APT groups.