

REPORT DOCUMENTATION PAGE					Form Approved OMB No. 0704-0188	
The public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden, to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.						
1. REPORT DATE (DD-MM-YYYY) July 22, 2022		2. REPORT TYPE Technical Paper			3. DATES COVERED (From - To)	
4. TITLE AND SUBTITLE C-ACT (CMMC v2.0-ATT&CK Compliance Tool) v1.0 Report				5a. CONTRACT NUMBER W56KGU-18-D-0004		
				5b. GRANT NUMBER		
				5c. PROGRAM ELEMENT NUMBER		
6. AUTHOR(S) Lorraine M. DeBlasio; Ted Farnsworth; Phu-Gui Feng; Daniel C. McLeod;				5d. PROJECT NUMBER 100927.10.100.D33J.AA0		
				5e. TASK NUMBER		
				5f. WORK UNIT NUMBER		
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) The MITRE Corporation 202 Burlington Road Bedford, MA 01730				8. PERFORMING ORGANIZATION REPORT NUMBER PRS-22-2454; MTR220108		
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) DoD CIO CMMC PMO				10. SPONSOR/MONITOR'S ACRONYM(S) DoD CIO CMMC PMO		
				11. SPONSOR/MONITOR'S REPORT NUMBER(S)		
12. DISTRIBUTION/AVAILABILITY STATEMENT DISTRIBUTION STATEMENT A. Approved for public release: distribution unlimited.						
13. SUPPLEMENTARY NOTES						
14. ABSTRACT The Cybersecurity Maturity Model Certification (CMMC)-ATT&CK Compliance Tool (C-ACT) is a capability developed by MITRE's CMMC project team. This report presents a worked example of how the C-ACT can be used to provide insight into the potential benefits (in terms of potential effects on adversary activities) of CMMC requirements.						
15. SUBJECT TERMS Network Security; Computer Security; ATT&CK; cybersecurity; maturity model;						
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES 31	19a. NAME OF RESPONSIBLE PERSON Susan Carpenito	
a. REPORT	b. ABSTRACT	c. THIS PAGE			19b. TELEPHONE NUMBER (Include area code) 781-271-7646	



MTR220108
MITRE TECHNICAL REPORT

C-ACT (CMMC v2.0-ATT&CK Compliance Tool) v1.0 Report

Sponsor: DoD CIO CMMC PMO
Contract No.: W56KGU-18-D-0004
Project No.: 100927.10.100.D33J.AA0

The views, opinions and/or findings contained in this report are those of The MITRE Corporation and should not be construed as an official government position, policy, or decision, unless designated by other documentation.

**Approved for Public Release;
Distribution Unlimited. Public
Release Case Number 22-2454**

**©2022 The MITRE
Corporation. All Rights
Reserved.**

Authors:
Lorraine M. DeBlasio
Ted Farnsworth
Phu-Gui Feng
Daniel C. McLeod

July 22, 2022

Contact:
c-act-list@mitre.org

Acknowledgements

The team wants to thank the tech editor Claudette H Bishop, who provided extensive technical editorial changes.

We want to acknowledge MITRE Subject Matter Experts (SMEs) Richard D Graubart, Deb Bodeau, John R Woodill Jr., Rob Brown, and Cristina Padro for their guidance and advice.

Executive Summary

The Cybersecurity Maturity Model Certification (CMMC)-ATT&CK Compliance Tool (C-ACT) is a capability developed by MITRE's CMMC project team. This report presents a worked example of how the C-ACT can be used to provide insight into the potential benefits (in terms of potential effects on adversary activities) of CMMC requirements.

The CMMC program is intended to protect the Defense Industrial Base (DIB) and the Department of Defense (DoD) supply chain against increasingly frequent and complex cyberattacks, by providing DIB members with requirements for systems handling sensitive information. The CMMC 2.0 framework defines three levels of requirements intended to enhance the protection of unclassified information within the DoD supply chain:

- CMMC Level 1 provides basic safeguarding of Federal Contracting Information as specified in Federal Acquisition Regulation clause 52.204-21.
- CMMC Level 2 encompasses the security requirements for Controlled Unclassified Information (CUI) as specified in NIST SP 800-171.
- CMMC Level 3 consists of the Level 2 practices and a subset of requirements from NIST SP 800-172.

The C-ACT is intended to illustrate and provide understanding of how CMMC requirements could potentially mitigate attacks from different advanced persistent threat¹ (APT) actors. The C-ACT was designed to assess and visualize CMMC potential effectiveness, at both Level 2 and Level 3, against a specific cyber-attack or scenario.

The C-ACT draws from multiple sources, including:

- Information published on adversarial threat actors that seek to exfiltrate information from target organizations such as DIB companies drawn from MITRE's Adversary Tactics, Techniques and Common Knowledge (ATT&CK)[®] knowledge base [2]. Using ATT&CK, the activities of a specific threat actors can be decomposed into tactics, techniques, and procedures (TTPs).
- Analysis by ATT&CK of common intrusion activity by APT actors, that are tracked by a common name in the security community, articulating which ATT&CK TTPs the activities employed.
- The controls in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 [3] [4] that protect against those TTPs are identified, and mappings provided in NIST SP 800-171 between its requirements (CMMC Level 2 practices) and NIST SP 800-53 controls and mappings provided in NIST SP 800-172 and its requirements (superset of CMMC Level 3 practices).
- Mappings published by MITRE Engenuity between MITRE ATT&CK for Enterprise TTPs to the NIST SP 800-53 controls that mitigate the specific TTPs.

¹ NIST SP 800-171 Rev. 2 [5] and NIST SP 800-172 [6] define the APT as "an adversary that possesses sophisticated levels of expertise and significant resources which allow it to create opportunities to achieve its objectives by using multiple attack vectors including, for example, cyber, physical, and deception. These objectives typically include establishing and extending footholds within the IT infrastructure of the targeted organizations for purposes of exfiltrating information, undermining or impeding critical aspects of a mission, program, or organization; or positioning itself to carry out these objectives in the future. The advanced persistent threat pursues its objectives repeatedly over an extended period; adapts to defenders' efforts to resist it; and is determined to maintain the level of interaction needed to execute its objectives."

- Mappings by MITRE and the Air Force Research Laboratory (AFRL) between ATT&CK for Enterprise TTP to NIST 800-53 control *and enhancements* levels. The MITRE/AFRL mapping also identifies the potential effect controls or enhancements have on the ATT&CK TTP (e.g., delay, divert, contain, detect).

The C-ACT utilizes the above mappings, and the coverage map capability of the ATT&CK Navigator to provide insight, analysis, and a visualization of the potential mitigating effects the CMMC practices have on adversary threat actors. This report illustrates the use of the C-ACT for three APT actors (APT1, APT28 and APT29). Potentially this capability can help identify the adequacy of the CMMC model and can provide a basis for changes in future versions.

The current findings of this activity indicated that compared to CMMC Level 2, CMMC Level 3 covers a significantly higher percentage of controls with enhancements, regardless of the APT being observed. This result was anticipated during research, as CMMC Level 3 consists of a subset of the requirements defined in NIST SP 800-172, which is meant to address advanced persistent threats.

Table of Contents

1 Introduction 1

1.1 Background 2

1.2 Assumptions 3

2 Identify Representative Threats..... 4

3 Threat Comparison 6

3.1 APT1 Results..... 6

3.2 APT28 Results..... 9

3.3 APT29 Results..... 12

4 Summary 15

5 References..... 16

Appendix A C-ACT Users Guide 17

A.1 Tool Description..... 17

A.1.1 Mapping Files..... 17

A.1.2 ATT&CK Coverage Maps 19

A.2 C-ACT Instructions 22

A.3 ATT&CK Navigator Instructions..... 22

A.4 C-ACT Files 25

Appendix B Abbreviations and Acronyms..... 25

List of Figures

Figure 1. Process for Developing C-ACT Worked Examples 1

Figure 2. APT1 Coverage map 7

Figure 3. APT1 and CMMC Level 3 Overlay 8

Figure 4. APT28 Coverage map 10

Figure 5. APT28 and CMMC Level 3 Overlay 11

Figure 6. APT29 Coverage map 13

Figure 7. APT29 and CMMC Level 3 Overlay 14

Figure 8. Section of C-ACTv2.xlsx – the MITRE/AFRL ATT&CK to CMMC Matrix..... 18

Figure 9. CMMC Level 3 ATT&CK Navigator Layer render 20

Figure 10. CMMC Level 3 ATT&CK Navigator Layer showing notes on Hardware Additions TTP
..... 21

Figure 11. APT 39 Coverage map..... 23

Figure 12. ATT&CK Navigator Add Layer Page – Open Existing Layer..... 23

Figure 13. Local Dialog box..... 24

Figure 14. ATT&CK Navigator Add Layer Page – Create Layer from other layers 24

1 Introduction

The Cybersecurity Maturity Model Certification (CMMC) [1] is intended to protect the Defense Industrial Base (DIB) and the Department of Defense (DoD) supply chain against increasingly frequent and complex cyberattacks, by providing DIB members with requirements for systems handling sensitive information. The CMMC-ATT&CK Compliance Tool (C-ACT) is a capability developed by MITRE's CMMC project team. The C-ACT is intended to illustrate and provide understanding of how CMMC requirements could mitigate attacks from different advanced persistent threat² (APT) actors.

This document provides a worked example of how the C-ACT can be used to provide insight into the potential benefits (in terms of potential effects on adversary activities) of CMMC requirements. This worked example uses information published on adversarial attacks and actors that seek to exfiltrate information from target organizations such as DIB companies drawn from MITRE's Adversary Tactics, Techniques and Common Knowledge (ATT&CK)[®] knowledge base [2]. The process used in this worked example is illustrated in Figure 1. The first step, described in Section 2, is to identify the representative threats, first by sponsor nation and then by APT group. This study focuses on three exemplar APTs, one of which is responsible for the SolarWinds attack, to understand the extent to which CMMC Levels 2 and 3 protect against APT TTPs.

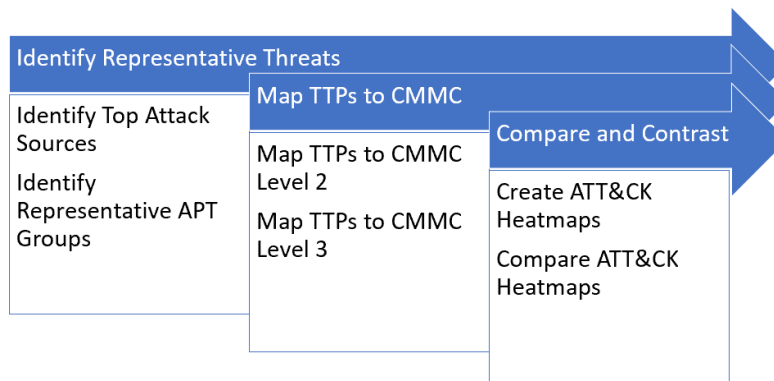


Figure 1. Process for Developing C-ACT Worked Examples

Using ATT&CK, the activities of a specific attacker group are decomposed into tactics, techniques, and procedures (TTPs). In the second step, the controls in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 [3] [4] that protect against those TTPs are identified, and a mapping matrix is created between the NIST SP 800-53 controls and the CMMC 2.0 Level 2 and Level 3 practices. In the third step, the results of the mappings are represented as ATT&CK coverage maps, enabling visual comparison between the potential mitigation offered by CMMC Level 2 and Level 3. The results of the second and third steps, represented as a C-ACT matrix-based comparison and ATT&CK coverage map visualization, are presented in Section 3. These results leverage the full C-ACT matrix mappings of ATT&CK TTPs to CMMC

² NIST SP 800-171 Rev. 2 [5] and NIST SP 800-172 [6] define the APT as “an adversary that possesses sophisticated levels of expertise and significant resources which allow it to create opportunities to achieve its objectives by using multiple attack vectors including, for example, cyber, physical, and deception. These objectives typically include establishing and extending footholds within the IT infrastructure of the targeted organizations for purposes of exfiltrating information, undermining or impeding critical aspects of a mission, program, or organization; or positioning itself to carry out these objectives in the future. The advanced persistent threat pursues its objectives repeatedly over an extended period; adapts to defenders’ efforts to resist it; and is determined to maintain the level of interaction needed to execute its objectives.”

controls and the corresponding visualizations created using the ATT&CK Navigator (see Appendix A for details).

The rest of this Introduction provides background and identifies assumptions for the C-ACT and the worked example. Appendix A provides a user's guide to the C-ACT.

1.1 Background

The following paragraphs provide background on the CMMC and on ATT&CK-related resources.

The CMMC 2.0 framework defines three levels of requirements intended to enhance the protection of unclassified information within the DoD supply chain:

- CMMC Level 1 provides basic safeguarding of Federal Contracting Information as specified in Federal Acquisition Regulation clause 52.204-21. CMMC Level 1 can be viewed as basic cyber hygiene, to mitigate common or simple threats (e.g., human error).
- CMMC Level 2 encompasses the security requirements for Controlled Unclassified Information (CUI) as specified in NIST SP 800-171 [5], which are intended to address known and anticipated threats against the confidentiality of CUI (see below). These specifically include insider threats.
- CMMC Level 3 consists of the Level 2 practices and a subset of requirements from NIST SP 800-172. [6] NIST SP 800-172 is intended to address the APT.

Confidentiality, integrity, and availability are three fundamental tenets of information security, and are colloquially known as the "CIA Triad." Confidentiality refers to preserving authorized restrictions on information access and disclosure, including protecting proprietary information. Integrity involves guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. Availability refers to ensuring timely and reliable access to and use of information. NIST SP 800-171 [5] requirements, and therefore CMMC Level 2, are focused on the confidentiality of CUI on non-federal systems. NIST SP 800-172 [6], and CMMC Level 3, are focused on the confidentiality, integrity, and availability of CUI.

While this study focuses on Levels 2 and 3, only CMMC Level 3 is intended to provide some protection against APTs. The C-ACT was designed to assess and visualize CMMC effectiveness, at both Level 2 and Level 3, against a specific cyber-attack or scenario.

MITRE ATT&CK® is a publicly available knowledge base of observed cyber adversary techniques, tactics, and procedures, with their corresponding mitigations. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community. This data includes APTs and the TTPs used by those APTs. The MITRE ATT&CK Navigator [7] is a tool MITRE created to visually organize and display the MITRE ATT&CK TTPs according to their respective Tactics, Techniques, and Sub-Techniques. The Navigator includes ATT&CK technique layers for APTs identified on the MITRE ATT&CK website. The tool also contains tools for shading, scoring, adding comments, and combining layers.

MITRE Engenuity recently completed and published the NIST 800-53 Controls to ATT&CK Mappings project [8]. This project maps MITRE ATT&CK TTPs to the NIST SP 800-53 controls that mitigate the specific TTP. This mapping was done at the TTP and TTP sub-technique levels to the 800-53 control level, but not to the control enhancement level. Henceforth in this report, this mapping will be referred to as the Engenuity mapping.

MITRE and the Air Force Research Laboratory (AFRL) collaborated on a separate effort to map the MITRE ATT&CK TTPs to NIST SP 800-53 controls [9]. This effort produced mapping at the ATT&CK TTP, but not sub-technique, to NIST 800-53 control and control enhancements levels. The MITRE/AFRL mapping also identifies the potential effect controls or enhancements have on the ATT&CK TTP (e.g., delay, divert, contain, detect). Because it has been incorporated into the AFRL Cyber Survivability Attributes (CSA) Tool, this mapping will be referred to as the AFRL mapping.

1.2 Assumptions

The following assumptions apply to this study and development of the tool:

1. The implementation and configurations of CMMC security practices, NIST SP 800-171 security requirements, NIST SP 800-172 security requirements, and NIST SP 800-53 security and privacy controls must be done correctly to be effective.
2. The assessments in this report assume a best-case scenario and ideal protections from implemented controls. Correctly implemented controls must be used correctly, with uses integrated into standard operating procedures (SOPs), to be effective.
3. The assessment also assumes all controls that mitigate a given technique are equally effective and complementary at doing so. That is, if three controls mitigate a given technique, each is responsible for one third of the mitigation and there is no overlap. In reality, the effectiveness of any control is highly dependent on its implementation, and controls can overlap or interact.
4. The public threat information used in the study is assumed to be applicable to attacks on the DoD supply chain/DIB.
5. The exemplar threats used in the study, which are based on subject matter experts' (SMEs') expectation of likely attacks to DIB companies, are assumed to be accurate characterizations of said threats.
6. It is assumed that past cyber-attacks are accurate predictors for present and future cyber threats.

2 Identify Representative Threats

Representative threats against the Defense Industrial Base (DIB) were identified to support the subsequent analysis. This involved looking at nation-state sponsors of attacks, and then selecting three representative APT groups from the top two sponsors.

We first looked at incident counts by attack sponsors to identify the top attacking sponsors. This is motivated by the assumption that higher incident counts by attack sponsors are known to be of high impact, that sponsoring attack nations become the research targets to focus on for this task. We used three data sources: Kaggle, ATT&CK, and the General Services Administration (GSA).

Kaggle, a subsidiary of Google LLC, is an open-source online community repository for data machine learning practitioners to find datasets, which we used to find data for this effort. We used more than 480 attacker-sponsored incidents in the downloaded public dataset for our analysis.

The Kaggle dataset (<https://www.kaggle.com>) revealed the following findings:

- There are attack sponsor nations inside the dataset: 36
- The number of sponsored cyber incidents is: 440
- The total global cyber incidents, including the sponsored ones, are: 481
- The dataset covers the years: 2005–2020
- From the dataset, the top sponsors who are attributed with the cyber incident counts are:
 1. China
 2. Russian Federation
 3. Iran (Islamic Republic of)
 4. Korea (Democratic People's Republic of)
 5. United States
 6. Israel
 7. Saudi Arabia
 8. Vietnam
 9. Pakistan
 10. United Arab Emirates

The MITRE ATT&CK knowledge base [2] contains information on 134 cyber-attack groups. A similar analysis was conducted on this dataset, specifically identifying groups with a history of targeting confidentiality, integrity and or availability of data of U.S. victims. This analysis yielded similar results as the Kaggle analysis, with APTs attributed to China and Russia constituting the greatest number of cyber-attack groups meeting our criteria. Based on these findings and SME inputs, we determined APT1 attributed to China and APT28 attributed to Russia would serve as useful examples for our analysis.

The General Services Administration (GSA) has also published guidance on several key considerations for the APT products, solutions, and services marketplace, including information on APT lifecycles [10]. In that guidance, APT29 is listed as one of the well-known attackers.

Based on the findings from the Kaggle, MITRE ATT&CK, and GSA guidance, APT1, APT28, and APT29 were chosen as the example threats for analysis by the CMMC-ATT&CK Compliance Tool. APT1 uses 23 TTPs; APT28 uses 84 TTPs; and APT29 uses 32 TTPs.

3 Threat Comparison

The potential effects of controls associated with CMMC Levels 2 and 3 on the three identified APT groups were analyzed, using the C-ACT mapping matrix (Excel workbooks) and ATT&CK Navigator coverage maps. This provides a rough estimate of potential protection based upon the CMMC Level:

- APT1 uses 23 TTPs that are mitigated by 62 controls and enhancements. Of those 62 controls and enhancements, CMMC Level 2 implements 2 and CMMC Level 3 implements 10.
- APT28 uses 84 TTPs that are mitigated by 130 controls and enhancements. Of those 130 controls and enhancements, CMMC Level 2 implements 6 and CMMC Level 3 implements 19.
- APT29 uses 32 TTPs that are mitigated by 127 controls and enhancements. Of those 127 controls and enhancements, CMMC Level 2 implements 6 and CMMC Level 3 implements 22.

The coverage maps for CMMC Levels 2 and 3 were overlaid with the ATT&CK coverage maps³ specific to these three APTs. Overlaying these two visual layers gave the team clear indicators of which techniques used by an APT were mitigated by NIST controls covered in a CMMC Level, and which were not. Unmitigated TTPs are shown as red, TTPs potentially mitigated to some extent as yellow, and all other TTPs as white. The C-ACT matrix was used to produce the threat comparison results in the following sections. (See Appendix A for detailed instructions.)

The results of this analysis demonstrate that compared to CMMC Level 2, CMMC Level 3 covers a significantly higher percentage of controls with enhancements, regardless of the APT being observed. This result was anticipated, as CMMC Level 3 adheres to NIST 800-172 and is meant to address advanced persistent threats. The following sections present a breakdown of these results based upon the APTs observed.

3.1 APT1 Results

A high-level result of the TTPs APT1 commonly uses against targets is shown below in Figure 2. APT1 uses 23 observed tactics, techniques, and procedures to exploit targets. Based on the AFRL mappings, these TTPs are mitigated by 62 identified NIST controls with enhancements.

Taking this information and overlaying it with the CMMC Level 3 navigation layers produces the image shown in Figure 3. The C-ACT matrix provides the result that CMMC Level 3 covers 10 of the 62 controls with enhancements that were previously identified to mitigate APT1. Thus, CMMC Level 3 currently covers approximately 16% of threats posed by APT1^{4 5}.

³ Because these coverage maps are produced as layers by the ATT&CK Navigator, they are referred to as navigation layers.

⁴ CMMC Level 2 covers 2 of the 62 NIST controls previously identified to mitigate APT1, or approximately >2%. CMMC Level 2 adheres to NIST 800-171, which is not designed to convey approximate APT mitigations.

⁵ The CMMC Level 2 APT1 coverage map is not shown, as there is no difference from Figure 2.

Reconnaissance 10 techniques	Resource Development 7 techniques	Initial Access 9 techniques	Execution 12 techniques	Persistence 19 techniques	Privilege Escalation 13 techniques	Defense Evasion 42 techniques	Credential Access 16 techniques	Discovery 30 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 16 techniques	Exfiltration 9 techniques	Impact 13 techniques
Active Scanning (013)	Acquire Infrastructure (016)	Drive-by Compromise (018)	Command and Scripting Interpreter (019)	Account Manipulation (015)	Abuse Elevation Control Mechanism (014)	Abuse Elevation Control Mechanism (014)	Adversary-in-the-Middle (015)	Account Discovery (014)	Exploitation of Remote Services (017)	Adversary-in-the-Middle (015)	Application Layer Protocol (014)	Automated Exfiltration (017)	Account Access Removal (017)
Gather Victim Host Information (016)	Compromise Accounts (011)	Exploit Public-Facing Application (018)	Container Administration Command (019)	BITS Jobs (015)	Access Token Manipulation (015)	Access Token Manipulation (015)	Brute Force (016)	Application Window Discovery (014)	Internal Spearphishing (017)	Archive Collected Data (013)	Communication Through Removable Media (017)	Data Transfer Size Limits (017)	Data Destruction (017)
Gather Victim Identity Information (016)	Compromise Infrastructure (016)	External Remote Services (018)	Deploy Container (019)	Boot or Logon Autostart Execution (014)	Boot or Logon Autostart Execution (014)	Boot or Logon Autostart Execution (014)	Credentials from Password Stores (016)	Browser Bookmark Discovery (017)	Lateral Tool Transfer (017)	Audio Capture (013)	Data Encoding (017)	Exfiltration Over Alternative Protocol (017)	Data Encrypted for Impact (017)
Gather Victim Network Information (018)	Develop Capabilities (014)	Hardware Additions (018)	Exploitation for Client Execution (019)	Boot or Logon Initialization Scripts (015)	Debugger Evasion (015)	Debugger Evasion (015)	Exploitation for Credential Access (016)	Cloud Infrastructure Discovery (014)	Remote Service Session Hijacking (017)	Automated Collection (013)	Data Obfuscation (017)	Exfiltration Over C2 Channel (017)	Data Manipulation (013)
Gather Victim Org Information (014)	Establish Accounts (013)	Phishing (017)	Inter-Process Communication (019)	Browser Extensions (015)	Deobfuscate/Decode Files or Information (015)	Deobfuscate/Decode Files or Information (015)	Forced Authentication (016)	Cloud Service Dashboard (017)	Remote Services (016)	Clipboard Data (013)	Dynamic Resolution (017)	Exfiltration Over Other Network Medium (017)	Defacement (017)
Phishing for Information (013)	Obtain Capabilities (018)	Replication Through Removable Media (018)	Native API (019)	Compromise Client Software Binary (015)	Create or Modify System Process (014)	Create or Modify System Process (014)	Forge Web Credentials (016)	Cloud Storage Object Discovery (017)	Replication Through Removable Media (018)	Data from Cloud Storage Object (013)	Encrypted Channel (017)	Exfiltration Over Physical Medium (017)	Disk Wipe (017)
Search Closed Sources (011)	Stage Capabilities (015)	Supply Chain Compromise (013)	Scheduled Task/Job (015)	Create Account (013)	Domain Policy Modification (015)	Domain Policy Modification (015)	Input Capture (016)	Container and Resource Discovery (017)	Software Deployment Tools (017)	Data from Configuration Repository (013)	Fallback Channels (017)	Exfiltration Over Web Service (017)	Endpoint Denial of Service (011)
Search Open Technical Databases (015)		Trusted Relationship (014)	Shared Modules (019)	Create or Modify System Process (014)	Escape to Host (015)	Escape to Host (015)	Modify Authentication Process (015)	Debugger Evasion (017)	Taint Shared Content (017)	Data from Information Repositories (013)	Ingress Tool Transfer (017)	Exfiltration Over Web Service (017)	Firmware Corruption (017)
Search Open Websites/Domains (013)		Valid Accounts (014)	Software Deployment Tools (019)	Event Triggered Execution (015)	Event Triggered Execution (015)	Event Triggered Execution (015)	Multi-Factor Authentication Interception (016)	Domain Trust Discovery (017)	Use Alternate Authentication Material (014)	Data from Local System (013)	Multi-Stage Channels (017)	Scheduled Transfer (017)	Inhibit System Recovery (017)
			System Services (017)	External Remote Services (015)	Exploitation for Privilege Escalation (015)	Exploitation for Privilege Escalation (015)	Multi-Factor Authentication Request Generation (016)	File and Directory Permissions Modification (017)	Group Policy Discovery (017)	Data from Network Shared Drive (013)	Non-Application Layer Protocol (017)	Transfer Data to Cloud Account (017)	Network Denial of Service (013)
			User Execution (013)	Hijack Execution Flow (017)	Hijack Execution Flow (017)	Hijack Execution Flow (017)	Network Sniffing (016)	Network Service Discovery (017)	Network Service Discovery (017)	Data from Removable Media (013)	Non-Standard Port (017)	Resource Hijacking (013)	Service Stop (017)
			Windows Management Instrumentation (019)	Implant Internal Image (017)	Process Injection (017)	Process Injection (017)	OS Credential Dumping (016)	Network Share Discovery (017)	Network Sniffing (017)	Proxy (014)	Protocol Tunneling (017)	System Shutdown/Reboot (017)	
				Modify Authentication Process (015)	Scheduled Task/Job (015)	Scheduled Task/Job (015)	Steal Application Access Token (016)	Password Policy Discovery (017)	Password Policy Discovery (017)	Data Staged (017)	Remote Access Software (017)		
				Office Application Startup (015)	Valid Accounts (014)	Valid Accounts (014)	Tickets (016)	Peripheral Device Discovery (017)	Peripheral Device Discovery (017)	Email Collection (017)	Traffic Signaling (017)		
				Pre-OS Boot (015)	Indirect Command Execution (015)	Indirect Command Execution (015)	Steal Web Session Cookie (016)	Permission Groups Discovery (016)	Permission Groups Discovery (016)	Input Capture (014)	Web Service (017)		
				Scheduled Task/Job (015)	Masquerading (017)	Masquerading (017)	Unsecured Credentials (017)	Process Discovery (017)	Process Discovery (017)	Screen Capture (017)			
				Server Software Component (015)	Modify Authentication Process (015)	Modify Authentication Process (015)		Query Registry (017)	Query Registry (017)	Video Capture (017)			
				Traffic Signaling (017)	Modify Cloud Compute Infrastructure (014)	Modify Cloud Compute Infrastructure (014)		Remote System Discovery (017)	Remote System Discovery (017)				
				Valid Accounts (014)	Modify Registry (017)	Modify Registry (017)		Software Discovery (017)	Software Discovery (017)				
					Network Boundary Bridging (017)	Network Boundary Bridging (017)		System Information Discovery (017)	System Information Discovery (017)				
					Obfuscated Files or Information (015)	Obfuscated Files or Information (015)		System Location Discovery (017)	System Location Discovery (017)				
					Plist File Modification (017)	Plist File Modification (017)		System Network Configuration Discovery (017)	System Network Configuration Discovery (017)				
					Pre-OS Boot (015)	Pre-OS Boot (015)		System Network Connections Discovery (017)	System Network Connections Discovery (017)				
					Process Injection (017)	Process Injection (017)		System Owner/User Discovery (017)	System Owner/User Discovery (017)				
					Reflective Code Loading (017)	Reflective Code Loading (017)		System Service Discovery (017)	System Service Discovery (017)				
					Rogue Domain Controller (017)	Rogue Domain Controller (017)		System Time Discovery (017)	System Time Discovery (017)				
					Rootkit (017)	Rootkit (017)		Virtualization/Sandbox Evasion (017)	Virtualization/Sandbox Evasion (017)				
					Subvert Trust Controls (016)	Subvert Trust Controls (016)							
					System Binary Proxy Execution (013)	System Binary Proxy Execution (013)							
					System Script Proxy Execution (017)	System Script Proxy Execution (017)							
					Template Injection (017)	Template Injection (017)							
					Traffic Signaling (017)	Traffic Signaling (017)							
					Trusted Developer Utilities Proxy Execution (017)	Trusted Developer Utilities Proxy Execution (017)							
					Unused/Unsupported Cloud Regions (017)	Unused/Unsupported Cloud Regions (017)							
					Use Alternate Authentication Material (014)	Use Alternate Authentication Material (014)							
					Valid Accounts (014)	Valid Accounts (014)							
					Virtualization/Sandbox Evasion (013)	Virtualization/Sandbox Evasion (013)							
					Weaken Encryption (017)	Weaken Encryption (017)							
					XSL Script Processing (017)	XSL Script Processing (017)							

Figure 2. APT1 Coverage map

TTPs used by APT1 shown as red.

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Active Scanning	Acquire Infrastructure	Drive-by Compromise	Command and Control Interpreter	Account Manipulation	Abuse Elevation Control Mechanism	Abuse Elevation Control Mechanism	Adversary-in-the-Middle	Account Discovery	Exploitation of Remote Services	Adversary-in-the-Middle	Application Layer Protocol	Automated Exfiltration	Account Access Removal
Gather Victim Host Information	Compromise Accounts	Exploit Public-Facing Application	Console Administration Command	BITS Jobs	Access Token Manipulation	Access Token Manipulation	Brute Force	Application Windows Discovery	Internal Spearphishing	Archives Collected Data	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Gather Victim Infrastructure	Compromise Infrastructure	External Remote Services	Deploy Container	Boot or Login Automation Execution	Boot or Login Automation Execution	Boot or Login Automation Execution	Credentials from Password Stores	Browser	Lateral Tool Transfer	Audio Capture	Data Encoding	Exfiltration Over Alternative Protocol	Data Exfiltration
Gather Victim Network Information	Develop Capabilities	Hardware Additions	Exploitation for Client Execution	Browser Extensions	Build Image in Host	Build Image in Host	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking	Automated Collection	Data Obfuscation	Exfiltration Over CD Channel	Data Manipulation
Gather Victim Org Information	Establish Accounts	Phishing	High Process Communication	Browser Extensions	Create or Modify System Process	Create or Modify System Process	Forceful Authentication	Cloud Service Dashboard	Remote Services	Browser Session Hijacking	Dynamic Resolution	Exfiltration Over Other Network Medium	Deactivation
Phishing for Information	Obtain Capabilities	Replication Through Removable Media	Native API	Compromise Client Software Binary	Domain Policy Manipulation	Domain Policy Manipulation	Forge Web Credentials	Cloud Service Discovery	Replication Through Removable Media	Clipboard Data	Encrypted Channel	Exfiltration Over Physical Medium	Data Wipe
Search Closed Sources	Stage Capabilities	Supply Chain Compromise	Scheduled Task/Job	Create Account	Escape to Host	Escape to Host	Input Capture	Cloud Storage Object Discovery	Software Deployment Tests	Data from Configuration Repository	Fallback Channels	Exfiltration Over Web Service	Endpoint Denial of Service
Search Open Technical Databases		Trusted Relationship	Shared Modules	Create or Modify System Process	Event Triggered Execution	Event Triggered Execution	Modify Authentication Process	Container and Resource Discovery	Use Shared Content	Data from Information Repository	Ingress Tool Transfer	Multi-Stage Channels	Firmware Corruption
Search Open Websites/Domains		Valid Accounts	Software Deployment Tools	External Remote Services	Exploitation for Privilege Escalation	Exploitation for Privilege Escalation	Multi-Factor Authentication Interception	Debugger Evasion	Network Sniffing	Data from Network Shared Drive	Non-Application Layer Protocol	Scheduled Transfer	Incident System Recovery
Search Victim-Owned Websites			System Services	Hijack Execution Flow	Hijack Execution Flow	Hijack Execution Flow	Network Sniffing	Domain Trust Discovery	Domain Trust Discovery	Data from Removable Media	Non-Standard Port	Transfer Data to Cloud Account	Resource Hijacking
			User Execution	Implement Internal Image	Process Injection	Process Injection	OS Credential Dumping	File and Directory Discovery	File and Directory Discovery		Protocol Tunneling		Service Stop
			Windows Management Instrumentation	Scheduled Task/Job	Scheduled Task/Job	Scheduled Task/Job	OS Credential Dumping	Group Policy Discovery	Group Policy Discovery		Proxy		System Shutdown/Restart
				Modify Authentication Process	Valid Accounts	Valid Accounts	Steal Application Access Token	Network Service Discovery	Network Service Discovery	Data Staged	Reverse Access Software		
				Office Application Startup			Steal or Forge Kerberos Tickets	Network Sniffing	Network Sniffing	Email Collection	Traffic Signaling		
				Pre-OS Boot			Unsecured Credentials	Payment Policy Discovery	Payment Policy Discovery	Input Capture	Web Service		
				Scheduled Task/Job				Peripheral Device Discovery	Peripheral Device Discovery	Screen Capture			
				Server Software Component				Permission	Permission	Video Capture			
				Traffic Signaling				Single Discovery	Single Discovery				
				Valid Accounts				Process Discovery	Process Discovery				
								Query Registry	Query Registry				
								Remote System Discovery	Remote System Discovery				
								Software Discovery	Software Discovery				
								System Information Discovery	System Information Discovery				
								System Location Discovery	System Location Discovery				
								System Network Configuration Discovery	System Network Configuration Discovery				
								System Network Connections Discovery	System Network Connections Discovery				
								System Owner/User Discovery	System Owner/User Discovery				
								System Service Discovery	System Service Discovery				
								System Time Discovery	System Time Discovery				
								Virtualization/Sandbox Evasion	Virtualization/Sandbox Evasion				

Figure 3. APT1 and CMMC Level 3 Overlay

Unmitigated TTPs are shown as red, TTPs potentially mitigated to some extent as yellow, and all other TTPs as white.

3.2 APT28 Results

A high-level result of the TTPs APT28 commonly uses against targets is shown below in Figure 4. APT28 uses 84 observed tactics, techniques, and procedures to exploit targets. Based on the AFRL mapping, these TTPs are mitigated by 130 identified NIST controls with enhancements.

Taking this information and overlaying it with the CMMC Level 3 navigation layers produces the image shown in Figure 5. The C-ACT matrix provides the result that CMMC Level 3 covers 19 of the 130 controls with enhancements that were previously identified to mitigate APT28. Thus, CMMC Level 3 currently covers approximately 14% of threats posed by APT28.^{6 7}

⁶ There is no difference between the CMMC Level 2 map and Figure 4.

⁷ CMMC Level 2 covers 6 of the 130 NIST controls previously identified to mitigate APT28, or approximately >2%. CMMC Level 2 adheres to NIST 800-171, which is not intended to address the APT.

Reconnaissance 10 techniques	Resource Development 7 techniques	Initial Access 9 techniques	Execution 12 techniques	Persistence 19 techniques	Privilege Escalation 13 techniques	Defense Evasion 42 techniques	Credential Access 16 techniques	Discovery 30 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 16 techniques	Exfiltration 9 techniques	Impact 13 techniques
Active Scanning (V3)	Acquire Infrastructure (V6)	Drive-by Compromise (V6)	Command and Scripting Interpreter (V6)	Account Manipulation (V6)	Abuse Elevation Control Mechanism (V6)	Abuse Elevation Control Mechanism (V6)	Adversary-in-the-Middle (V6)	Account Discovery (V6)	Exploitation of Remote Services (V6)	Adversary-in-the-Middle (V6)	Application Layer Protocol (V6)	Automated Exfiltration (V6)	Account Access Removal (V6)
Gather Victim Host Information (V6)	Compromise Accounts (V6)	Exploit Public-Facing Application (V6)	Container Administration Command (V6)	BITS Jobs (V6)	Access Token Manipulation (V6)	Access Token Manipulation (V6)	Brute Force (V6)	Application Window Discovery (V6)	Internal Spearphishing (V6)	Archive Collected Data (V6)	Communication Through Removable Media (V6)	Data Transfer Size Limits (V6)	Data Destruction (V6)
Gather Victim Identity Information (V6)	Compromise Infrastructure (V6)	External Remote Services (V6)	Deploy Container (V6)	Boot or Logon Autostart Execution (V6)	Boot or Logon Autostart Execution (V6)	Boot or Logon Autostart Execution (V6)	Credentials from Password Stores (V6)	Browser Bookmark Discovery (V6)	Lateral Tool Transfer (V6)	Audio Capture (V6)	Data Encoding (V6)	Exfiltration Over Alternative Protocol (V6)	Data Encrypted for Impact (V6)
Gather Victim Network Information (V6)	Develop Capabilities (V6)	Hardware Additions (V6)	Exploitation for Client Execution (V6)	Boot or Logon Initialization Scripts (V6)	Boot or Logon Initialization Scripts (V6)	Build Image on Host (V6)	Exploitation for Credential Access (V6)	Cloud Infrastructure Discovery (V6)	Remote Service Session Hijacking (V6)	Automated Collection (V6)	Data Obfuscation (V6)	Exfiltration Over C2 Channel (V6)	Data Manipulation (V6)
Gather Victim Org Information (V6)	Establish Accounts (V6)	Phishing (V6)	Inter-Process Communication (V6)	Browser Extensions (V6)	Create or Modify System Process (V6)	Debugger Evasion (V6)	Forced Authentication (V6)	Cloud Service Dashboard (V6)	Remote Services (V6)	Clipboard Data (V6)	Dynamic Resolution (V6)	Exfiltration Over Other Network Medium (V6)	Defacement (V6)
Phishing for Information (V6)	Obtain Capabilities (V6)	Replication Through Removable Media (V6)	Native API (V6)	Compromise Client Software Binary (V6)	Create or Modify System Process (V6)	Desktop/Screen/Decode Files or Information (V6)	Forge Web Credentials (V6)	Cloud Storage Object Discovery (V6)	Replication Through Removable Media (V6)	Data from Cloud Storage Object (V6)	Encrypted Channel (V6)	Exfiltration Over Physical Medium (V6)	Disk Wipe (V6)
Search Closed Sources (V6)	Stage Capabilities (V6)	Supply Chain Compromise (V6)	Scheduled Task/Job (V6)	Create Account (V6)	Domain Policy Modification (V6)	Deploy Container (V6)	Input Capture (V6)	Container and Resource Discovery (V6)	Software Deployment Tools (V6)	Data from Configuration Repository (V6)	Fallback Channels (V6)	Exfiltration Over Web Service (V6)	Firmware Corruption (V6)
Search Open Technical Databases (V6)	Trusted Relationship (V6)	Trusted Relationship (V6)	Shared Modules (V6)	Create or Modify System Process (V6)	Domain Policy Modification (V6)	Direct Volume Access (V6)	Multi-Factor Authentication Interception (V6)	Debugger Evasion (V6)	Use Alternate Authentication Material (V6)	Data from Information Repositories (V6)	Ingress Tool Transfer (V6)	Scheduled Transfer (V6)	Inhibit System Recovery (V6)
Search Open Websites/Domains (V6)	Valid Accounts (V6)	Valid Accounts (V6)	Software Deployment Tools (V6)	Event Triggered Execution (V6)	Event Triggered Execution (V6)	Domain Policy Modification (V6)	Multi-Factor Authentication Interception (V6)	Domain Trust Discovery (V6)	File and Directory Discovery (V6)	Data from Local System (V6)	Non-Application Layer Protocol (V6)	Transfer Data to Cloud Account (V6)	Resource Hijacking (V6)
Search Victim-Owned Websites (V6)			System Services (V6)	External Remote Services (V6)	Exploitation for Privilege Escalation (V6)	Exploitation for Defense Evasion (V6)	Multi-Factor Authentication Request Generation (V6)	File and Directory Discovery (V6)	Group Policy Discovery (V6)	Data from Network Shared Drive (V6)	Non-Standard Port (V6)		Service Stop (V6)
			User Execution (V6)	Hijack Execution Flow (V6)	Hijack Execution Flow (V6)	File and Directory Permissions Modification (V6)	Network Sniffing (V6)	Network Service Discovery (V6)	Network Share Discovery (V6)	Data from Removable Media (V6)	Protocol Tunneling (V6)		System Shutdown/Reboot (V6)
			Windows Management Instrumentation (V6)	Implant Internal Image (V6)	Process Injection (V6)	Hide Artifacts (V6)	OS Credential Dumping (V6)	Network Sniffing (V6)	Password Policy Discovery (V6)	Data Staged (V6)	Proxy (V6)		
				Modify Authentication Process (V6)	Scheduled Task/Job (V6)	Hijack Execution Flow (V6)	Steal Application Access Token (V6)	Peripheral Device Discovery (V6)	Screen Capture (V6)	Email Collection (V6)	Remote Access Software (V6)		
				Office Application Startup (V6)	Valid Accounts (V6)	Indicator Removal on Host (V6)	Steal or Forge Kerberos Tickets (V6)	Permission Groups Discovery (V6)	Screen Capture (V6)	Input Capture (V6)	Traffic Signaling (V6)		
				Pre-OS Boot (V6)		Indirect Command Execution (V6)	Steal Web Session Cookie (V6)	Process Discovery (V6)		Screen Capture (V6)	Web Service (V6)		
				Scheduled Task/Job (V6)		Masking (V6)	Unsecured Credentials (V6)	Query Registry (V6)		Video Capture (V6)			
				Server Software Component (V6)		Modify Authentication Process (V6)		Remote System Discovery (V6)					
				Traffic Signaling (V6)		Modify Cloud Compute Infrastructure (V6)		Software Discovery (V6)					
				Valid Accounts (V6)		Modify Registry (V6)		System Information Discovery (V6)					
						Modify System Image (V6)		System Location Discovery (V6)					
						Network Boundary Bridging (V6)		System Network Configuration Discovery (V6)					
						Obfuscated Files or Information (V6)		System Network Connections Discovery (V6)					
						Plist File Modification (V6)		System Owner/User Discovery (V6)					
						Pre-OS Boot (V6)		System Service Discovery (V6)					
						Process Injection (V6)		System Time Discovery (V6)					
						Reflective Code Loading (V6)		Virtualization/Sandbox Evasion (V6)					
						Rogue Domain Controller (V6)							
						Rootkit (V6)							
						Subvert Trust Controls (V6)							
						System Binary Proxy Execution (V6)							
						System Script Proxy Execution (V6)							
						Template Injection (V6)							
						Traffic Signaling (V6)							
						Trusted Developer Utilities Proxy Execution (V6)							
						Unused/Unsupported Cloud Regions (V6)							
						Use Alternate Authentication Material (V6)							
						Valid Accounts (V6)							
						Virtualization/Sandbox Evasion (V6)							
						Weaken Encryption (V6)							
						XSL Script Processing (V6)							

Figure 4. APT28 Coverage map

TTPs used by APT28 shown as red.

[illegible]

Figure 5. APT28 and CMMC Level 3 Overlay

Unmitigated TTPs are shown as red, TTPs potentially mitigated to some extent as yellow, and all other TTPs as white.

3.3 APT29 Results

A high-level result of the TTPs APT29 commonly uses against targets is shown below in Figure 6. APT29 uses 32 observed tactics, techniques, and procedures to exploit targets. Based on the AFRL mappings, these TTPs are mitigated by 127 identified NIST controls with enhancements.

Taking this information and overlaying it with the CMMC Level 3 navigation layers produces the image shown in Figure 7. The C-ACT matrix provides the result that CMMC Level 3 covers 22 of the 127 controls with enhancements that were previously identified to mitigate APT29. At the time of this study, this data produces the result that CMMC Level 3 currently covers approximately 17% of threats posed by APT29.^{8 9}

⁸ CMMC Level 2 covers 6 of the 127 NIST controls with enhancements previously identified to mitigate APT29, or approximately 4%.

⁹ There is no difference between the CMMC Level 2 map and Figure 6.

[illegible]

Figure 6. APT29 Coverage map

TTPs used by APT29 shown as red.

[illegible]

Figure 7. APT29 and CMMC Level 3 Overlay

Unmitigated TTPs are shown as red, TTPs potentially mitigated to some extent as yellow, and all other TTPs as white.

4 Summary

This paper presents the CMMC-ATT&CK Compliance Tool (C-ACT) capability that illustrates and provides understanding of cybersecurity attacks against the Defense Industrial Base and the Department of Defense supply chain. The capability is demonstrated through analysis of three representative attackers (APT1, APT28, and APT29), to understand the extent to which CMMC Levels 2 and 3 protect against TTPs. The details of the analysis could change, as the set of requirements in CMMC Level 3 has not been finalized; however, the C-ACT enables analysis to be repeated in a consistent way with reduced effort.

As part of the tool, a set of reusable deliverables was produced, including the C-ACT mapping matrices and the CMMC Level 2 and Level 3 ATT&CK Navigator coverage maps. These are described in Appendix A. Output from the tools – analysis of specific threat events – can provide insight to identify the mitigating effects the CMMC practices have on adversary threat events. Analyses can help identify the adequacy of the CMMC model and can provide a basis for changes in future versions.

In addition, the work done with the CMMC model is being integrated into the AFRL CSA tool, for use by a broader community.

5 References

- [1] OUSD(A&S), "Securing the Defense Industrial Base: CMMC 2.0," 2022. [Online]. Available: <https://www.acq.osd.mil/cmmc/index.html>.
- [2] The MITRE Corporation, "Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK™)," The MITRE Corporation, 2022. [Online]. Available: <https://attack.mitre.org/>.
- [3] NIST, "NIST SP 800-53 R4, Security and Privacy Controls for Federal Information Systems and Organizations," April 2013. [Online]. Available: <http://dx.doi.org/10.6028/NIST.SP.800-53r4>.
- [4] Joint Task Force, "NIST SP 800-53R5, Security and Privacy Controls for Information Systems and Organizations," 10 December 2020. [Online]. Available: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf>.
- [5] NIST, "NIST SP 800-171 Rev. 2, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations," 28 January 2021. [Online]. Available: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r2.pdf>.
- [6] NIST, "NIST SP 800-172, Enhanced Security Requirements for Protecting Controlled Unclassified Information: A Supplement to NIST Special Publication 800-171," 2 February 2021. [Online]. Available: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-172.pdf>.
- [7] The MITRE Corporation, "MITRE ATT&CK Navigator," January 2022. [Online]. Available: <https://mitre-attack.github.io/attack-navigator/>.
- [8] MITRE Engenuity, "Mapping Methodology," Center for Threat-Informed Defense ATT&CK Control Framework Mappings, 14 December 2020. [Online]. Available: https://github.com/center-for-threat-informed-defense/attack-control-framework-mappings/blob/master/docs/mapping_methodology.md.
- [9] D. J. Bodeau, R. D. Graubart, E. Laderman, L. K. Jones and D. Black, "Cyber Resiliency Approaches and Controls to Mitigate Adversary Tactics, Techniques, and Procedures (TTPs): Mapping Cyber Resiliency to the ATT&CK® Framework – Revision 2, MTR200286R2, PR 21-3123," The MITRE Corporation, Bedford, MA, 2021.
- [10] GSA, "Advanced Persistent Threat (APT) Buyer's Guide, Version 1.1," 2021 January. [Online]. Available: https://interact.gsa.gov/sites/default/files/APT_Buyers_Guide_v1.1_20210121.pdf.

Appendix A C-ACT Users Guide

A.1 Tool Description

The CMMC-ATT&CK Compliance Tool, in its current form, comprises two Excel mapping matrix files and the CMMC Level 2 and 3 json ATT&CK Navigator layers. The two Excel mapping matrix files are used to identify and compare ATT&CK TTP mitigations between APTs and CMMC requirements. The two ATT&CK Navigator layers are used to visualize coverage provided by CMMC.

A.1.1 Mapping Files

CMMC Level 2 practices are equivalent to NIST SP 800-171 Rev2 security requirements. CMMC Level 3 practices are a subset of NIST SP 800-172 security requirements. Both NIST SP 800-171 Rev2 and NIST SP 800-172 include glossaries that map their respective security requirements to NIST SP 800-53 security and privacy controls¹⁰. The team identified two mappings between NIST SP 800-53 security and privacy controls and MITRE ATT&CK TTPs. The first mapping from MITRE Engenuity relates the ATT&CK techniques and sub-techniques to NIST SP 800-53 security and privacy controls but does not include control enhancements. The second mapping is from a MITRE/AFRL effort that relates the ATT&CK techniques, but not sub-techniques, to NIST SP 800-53 security and privacy controls and their enhancements.

The team developed a Python script to merge the NIST SP 800-171 and NIST SP 800-172 mappings with the Engenuity mapping. The team modified the Python script to similarly merge the NIST SP 800-171 and NIST SP 800-172 mappings with the MITRE/AFRL ATT&CK control and enhancement mapping.

This effort produced two Excel spreadsheet deliverables. Both relate MITRE ATT&CK TTPs, NIST SP 800-53 security and privacy controls, NIST SP 800-171 and 800-172 security requirements, and CMMC Level 2 and Level 3. The first is named “C-ACTv1.xlsx” and uses the MITRE Engenuity mapping. The second is named “C-ACTv2.xlsx” and uses the MITRE/AFRL mapping. The figure below is a subset of the C-ACTv2 mapping showing relationships between ATT&CK TTP ID, mitigating controls, NIST SP 171/172 security requirements, and CMMC compliance level.

¹⁰ NIST SP 800-171 Rev 2 maps its requirements to the controls and enhancements in NIST SP 800-53 R4. An updated version of NIST SP 800-171 is expected to be produced sometime in 2022, and that will contain mappings to 800-53 R5. NIST SP 800-172 maps its requirements to controls and enhancements in NIST SP 800-53 R5.

TECHNIQUE	ATTACK TTP ID	MITIGATION	MITIGATION ID	CYBER RESILIENCY APPROACH	HIGH LEVEL ADV EFFECT	SPECIFIC ADV EFFECT	CONTROL	NIST 171/172 CATEGORY	NIST 171/172 REQUIREMENT	CMMC COMPLIANCE LEVEL
Exploit Public-Facing Application	T1190	Maintain Deception Environment	CM1102	Misdirection	REDIRECT	DIVERT	SC-26	System and Communications Protection	3.13.3e	CMMC Level 3
Exploit Public-Facing Application	T1190	Maintain Deception Environment	CM1102	Predefined Segmentation	PRECLUDE	NEGATE	SC-7(21)	System and Communications Protection	3.13.4e	CMMC Level 3
Exploit Public-Facing Application	T1190	Adversarial Simulation	CM1107	Self-Challenge	PRECLUDE	PREEMPT	CA-8	Security Assessment	3.12.1e	CMMC Level 3
Exploit Public-Facing Application	T1190	Adversarial Simulation	CM1107	Self-Challenge	PRECLUDE	PREEMPT	CA-8(2)			
Exploit Public-Facing Application	T1190	Monitor Logs	CM2004	Behavior Validation	EXPOSE	DETECT	AU-6	Audit and Accountability	3.3.1	CMMC Level 2
Exploit Public-Facing Application	T1190	Monitor Logs	CM2004	Behavior Validation	EXPOSE	DETECT	AU-6	Audit and Accountability	3.3.5	CMMC Level 2

Figure 8. Section of C-ACTv2.xlsx – the MITRE/AFRL ATT&CK to CMMC Matrix

A.1.2 ATT&CK Coverage Maps

The team used an ATT&CK layer (json) created by the MITRE Engenuity team and modified the Python script used to create the mapping matrices described above. Each ATT&CK TTP has a comment in the tool listing mitigating NIST SP 800-53 security and privacy controls and associated NIST SP 800-171 and NIST SP 800-172 security requirements.

The outcome of this research focus is two .json files, one for CMMC Level 2 and one for CMMC Level 3, which can be imported into the MITRE ATT&CK Navigator. These layers create a visual representation of the mitigations put in place by CMMC. Figure 9 below is the visual output of this deliverable. The figure shows CMMC Level 3 mitigations for each MITRE ATT&CK TTP where the TTP is colored green if mitigated by some CMMC Level 3 practices. Figure 10 shows the Hardware Additions TTP as an example TTP and comment within the tool.

CMMC-ATT&CK Compliance Tool

DoD CIO CMMC PMO

[illegible]

Figure 9. CMMC Level 3 ATT&CK Navigator Layer render

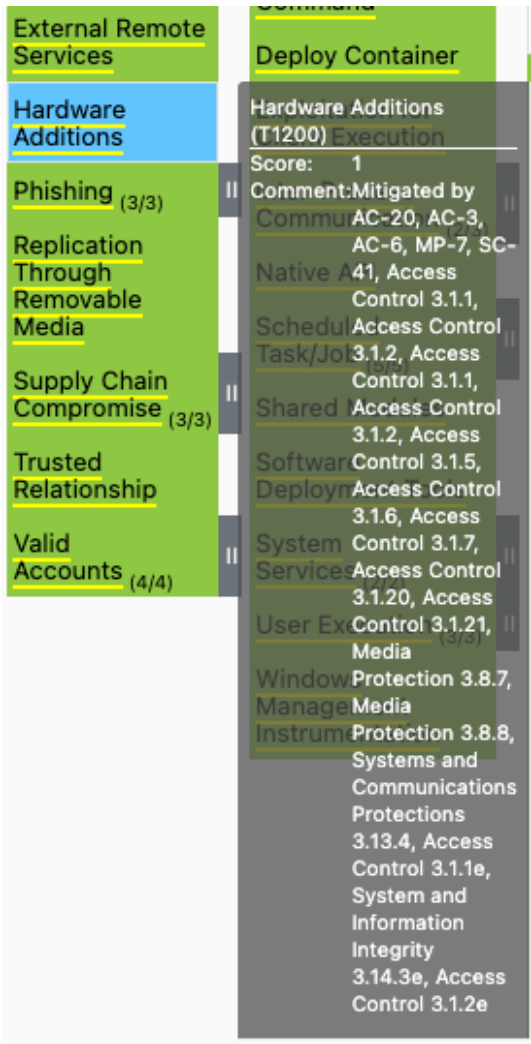


Figure 10. CMMC Level 3 ATT&CK Navigator Layer showing notes on Hardware Additions TTP

A.2 C-ACT Instructions

For analysts, the following steps are provided as instructions to use the tool.

7. Identify ATT&CK TTPs used by the chosen APT on the MITRE ATT&CK website.
8. Open the mapping matrix created by this project.
9. Filter the ATT&CK TTP column, selecting all the ATT&CK TTPs identified in step 1.
10. Record the number of unique controls in the CONTROL ID column in the filtered list*; this is the list of controls needed to mitigate the APT.
11. Filter the CMMC COMPLIANCE Level column on CMMC Level 2, and identify the unique number of controls in the CONTROL ID column.* This is the number of controls implemented by CMMC Level 2 to mitigate the threat.
12. Filter the CMMC COMPLIANCE Level column on CMMC Level 2 and CMMC Level 3, and identify the unique number of controls in the CONTROL ID column.* This is the number of controls implemented by CMMC Level 3 to mitigate the threat.
 - a. As stated in the assumptions, the CMMC Level 3 results are based on a preliminary list of included NIST SP 800-172 security requirements. The Excel sheet used has all NIST SP 800-172 requirements included. Requirements may be deselected in the filter menu of the NIST SP 800-171/172 Security Requirements column as desired before counting the unique number of controls in step 6.
13. Use the results in step 4, 5, and 6 to analyze the overlap.

* One method is to copy the controls column to another sheet or workbook and use the Excel “remove duplicates” function.

A.3 ATT&CK Navigator Instructions

The overlay was accomplished by using the ATT&CK Navigator layer combination feature, taking the color-coded information, and scoring of one layer and combining it with another to produce a visual comparison. Figure 10 through 7 demonstrate high-level images of how to accomplish this task.

For the purposes of this explanation, Figure 11 already has a layer created: *APT 39*, an advanced persistent threat group within the MITRE ATT&CK Framework. This is done using the multi-select selection control.

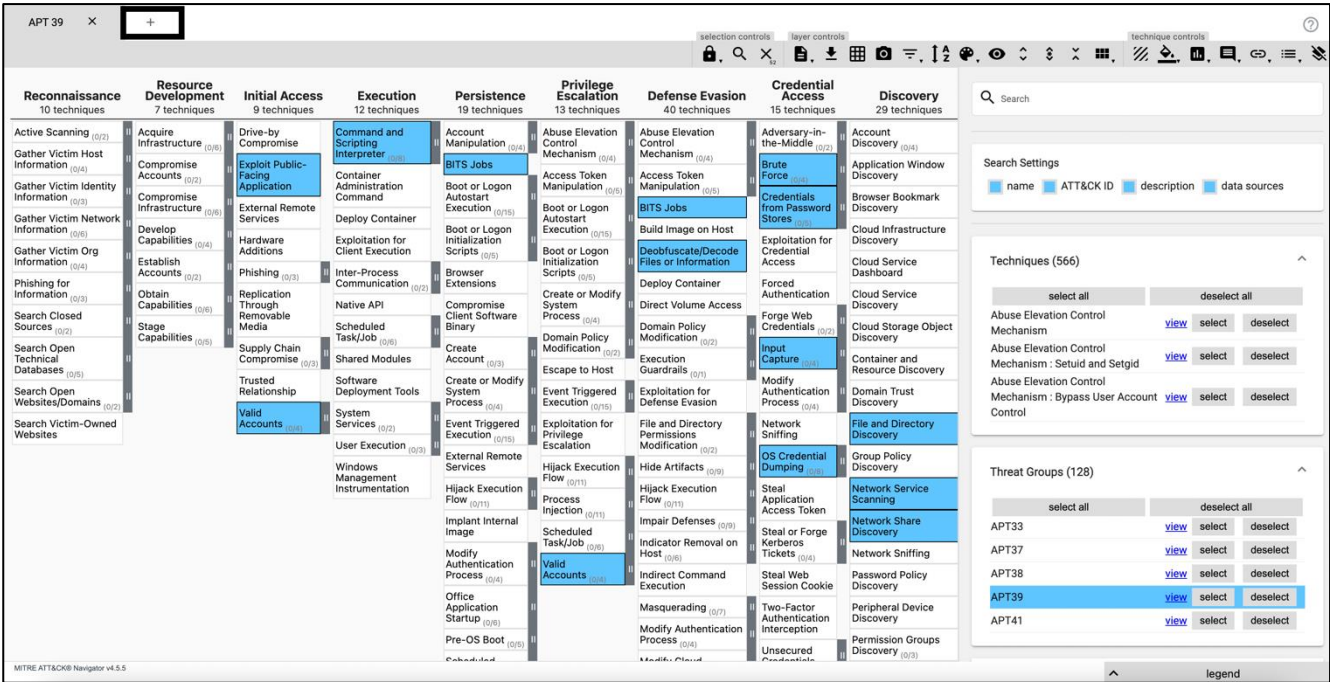


Figure 11. APT 39 Coverage map

Selecting the “+” symbol in the top left corner brings up Figure 12, allowing the user to upload the .json layer of the desired CMMC Level layer.



Figure 12. ATT&CK Navigator Add Layer Page – Open Existing Layer

Uploading from local gives the following dialog box, shown in Figure 13, from the user’s local machine.

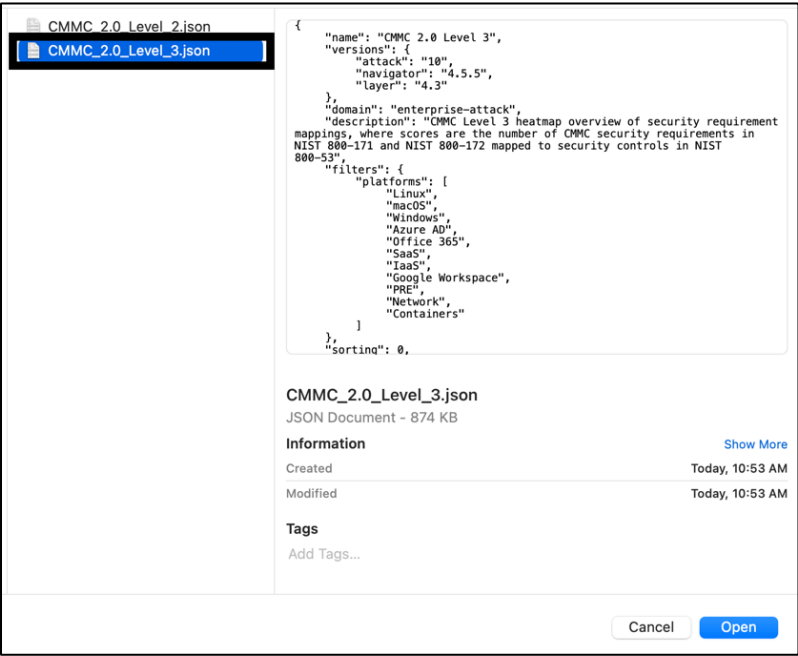


Figure 13. Local Dialog box

Once the desired CMMC layer is uploaded into the Navigator, the two layers are combined, as demonstrated in Figure 14. Choosing *Create layer from other layers* allows an individual to overlay two layers and analyze similarities and differences. To achieve the scoring color scheme used in the Section 3, select the color setup layer control. Set the low value to –2 and the high value to 0. In the same menu, set the colors, from low to high, as red, yellow, and white.

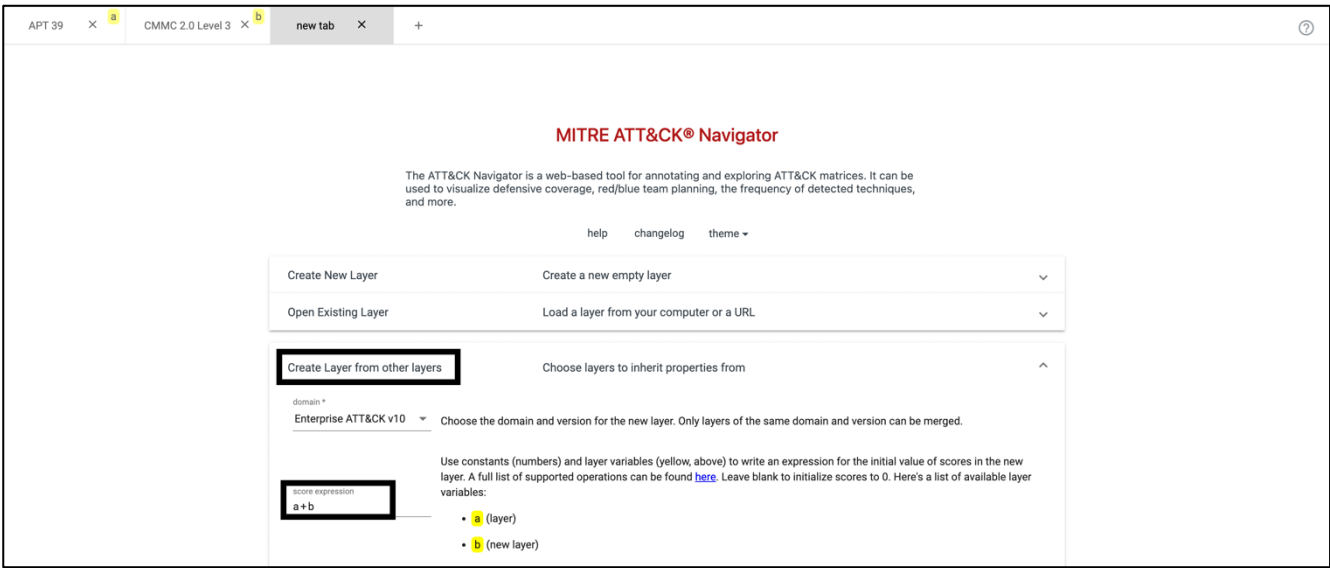


Figure 14. ATT&CK Navigator Add Layer Page – Create Layer from other layers

A.4 C-ACT Files

The C-ACT tool consists of 4 files:

- C-ACT Mapping Matrix based on MITRE/AFRL Collaboration
- C-ACT Mapping Matrix based on MITRE Engenuity
- CMMC Level 2 Coverage map ATT&CK Navigator Layer
- CMMC Level 3 Coverage map ATT&CK Navigator Layer

Please contact the C-ACT team: c-act-list@mitre.org for the newest C-ACT tool versions.

Appendix B Abbreviations and Acronyms

Term	Definition
AFRL	Air Force Research Laboratory
APT	Advanced Persistent Threat
ATT&CK	Adversarial Tactics, Techniques, and Common Knowledge
C-ACT	CMMC-ATT&CK Compliance Tool
CMMC	Cybersecurity Maturity Model Certification
CSA	Cyber Survivability Attribute(s)
CUI	Controlled Unclassified Information
DIB	Defense Industrial Base
DoD	Department of Defense
NIST	National Institute of Standards and Technology
SP	(NIST) Special Publication
TTPs	Tactics, Techniques, and Procedures