| REPORT DOCUMENTATION PAGE | *Form Approved*<br>*OMB No. 0704-0188* |
|---|---|

| | | |
|---|---|---|
| **1. REPORT DATE** *(DD-MM-YYYY)*<br>July 22, 2022 | **2. REPORT TYPE**<br>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** | **19a. NAME OF RESPONSIBLE PERSON** |
|---|---|---|---|---|---|
| **a. REPORT** | **b. ABSTRACT** | **c. THIS PAGE** | | | Susan Carpenito |
| | | | | 31 | **19b. TELEPHONE NUMBER** *(Include area code)*<br>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**

**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 threat[1] (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

# List of Figures

# 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 threat[2] (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.

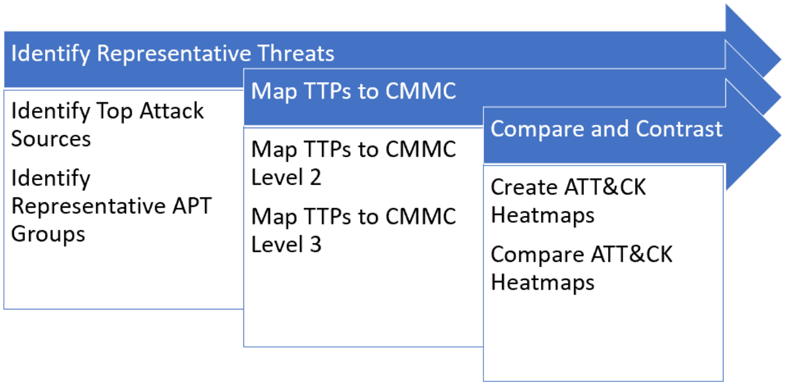


**Figure 1. Process for Developing C-ACT Worked Examples**

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 maps[3] 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

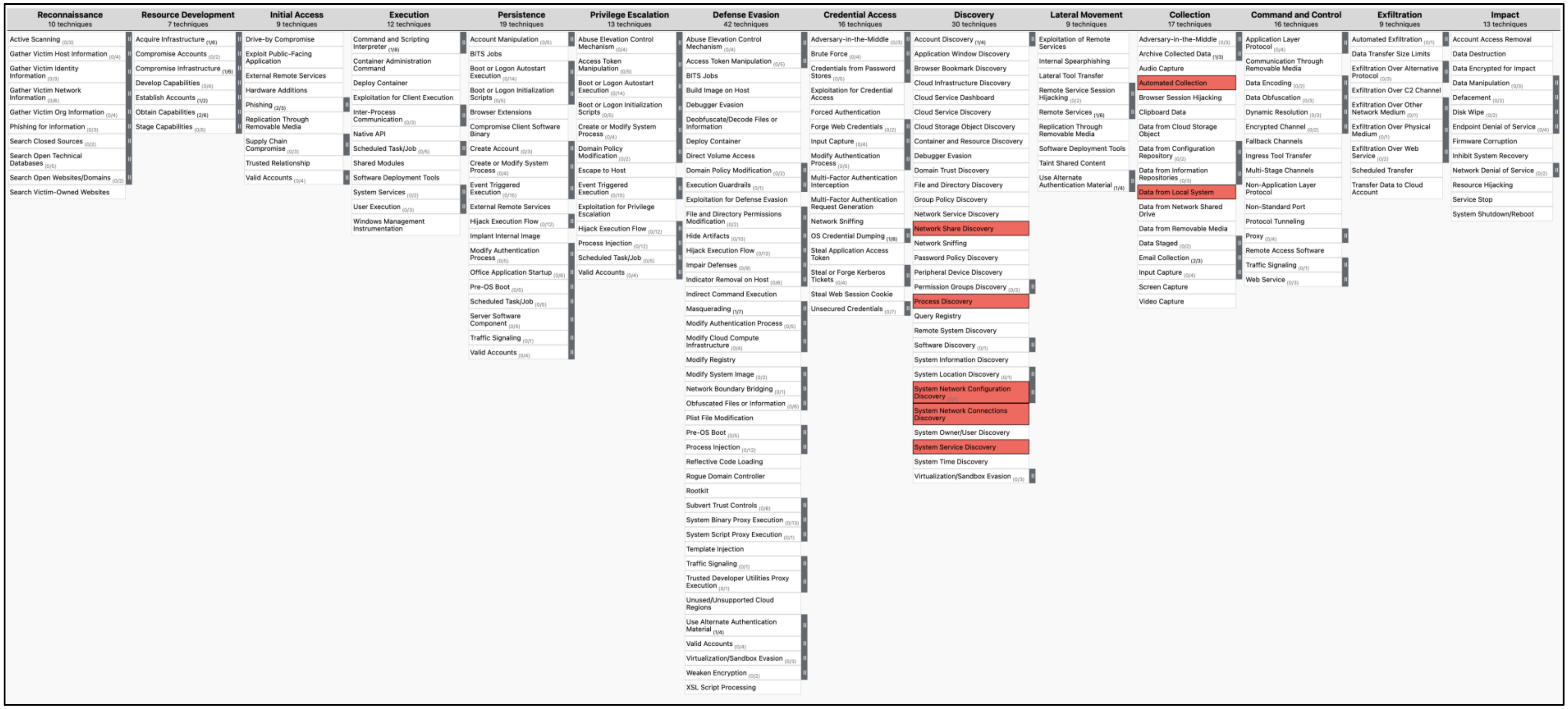
A high-level result of the TTPs APT1 commonly uses against targets is shown below in Figure 2. APT1 uses 23 observed tactics, techniques, and procedures to exploit targets. Based on the AFRL mappings, these TTPs are mitigated by 62 identified NIST controls with enhancements.

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

- Active Scanning (0/3)
- Gather Victim Host Information (0/4)
- Gather Victim Identity Information (0/3)
- Gather Victim Network Information (0/6)
- Gather Victim Org Information (0/4)
- Phishing for Information (0/3)
- Search Closed Sources (0/2)
- Search Open Technical Databases (0/5)
- Search Open Websites/Domains (0/2)
- Search Victim-Owned Websites

**Resource Development**
7 techniques

- Acquire Infrastructure (1/6)
- Compromise Accounts (0/2)
- Compromise Infrastructure (1/6)
- Develop Capabilities (0/4)
- Establish Accounts (1/2)
- Obtain Capabilities (2/6)
- Stage Capabilities (0/5)

**Initial Access**
9 techniques

- Drive-by Compromise
- Exploit Public-Facing Application
- External Remote Services
- Hardware Additions
- Phishing (2/3)
- Replication Through Removable Media
- Supply Chain Compromise (0/3)
- Trusted Relationship
- Valid Accounts (0/4)

**Execution**
12 techniques

- Command and Scripting Interpreter (1/8)
- Container Administration Command
- Deploy Container
- Exploitation for Client Execution
- Inter-Process Communication (0/3)
- Native API
- Scheduled Task/Job (0/5)
- Shared Modules
- Software Deployment Tools
- System Services (0/2)
- User Execution (0/3)
- Windows Management Instrumentation

**Persistence**
19 techniques

- Account Manipulation (0/5)
- BITS Jobs
- Boot or Logon Autostart Execution (0/14)
- Boot or Logon Initialization Scripts (0/5)
- Browser Extensions
- Compromise Client Software Binary
- Create Account (0/3)
- Create or Modify System Process (0/4)
- Event Triggered Execution (0/15)
- External Remote Services
- Hijack Execution Flow (0/12)
- Implant Internal Image
- Modify Authentication Process (0/5)
- Office Application Startup (0/6)
- Pre-OS Boot (0/5)
- Scheduled Task/Job (0/5)
- Server Software Component (0/5)
- Traffic Signaling (0/1)
- Valid Accounts (0/4)

**Privilege Escalation**
13 techniques

- Abuse Elevation Control Mechanism (0/4)
- Access Token Manipulation (0/5)
- Boot or Logon Autostart Execution (0/14)
- Boot or Logon Initialization Scripts (0/5)
- Create or Modify System Process (0/4)
- Domain Policy Modification (0/2)
- Escape to Host
- Event Triggered Execution (0/15)
- Exploitation for Privilege Escalation
- Hijack Execution Flow (0/12)
- Process Injection (0/12)
- Scheduled Task/Job (0/5)
- Valid Accounts (0/4)

**Defense Evasion**
42 techniques

- Abuse Elevation Control Mechanism (0/4)
- Access Token Manipulation (0/5)
- BITS Jobs
- Build Image on Host
- Debugger Evasion
- Deobfuscate/Decode Files or Information
- Deploy Container
- Direct Volume Access
- Domain Policy Modification (0/2)
- Execution Guardrails (0/1)
- Exploitation for Defense Evasion
- File and Directory Permissions Modification (0/2)
- Hide Artifacts (0/10)
- Hijack Execution Flow (0/12)
- Impair Defenses (0/9)
- Indicator Removal on Host (0/6)
- Indirect Command Execution
- Masquerading (1/7)
- Modify Authentication Process (0/5)
- Modify Cloud Compute Infrastructure (0/4)
- Modify Registry
- Modify System Image (0/2)
- Network Boundary Bridging (0/1)
- Obfuscated Files or Information (0/6)
- Plist File Modification
- Pre-OS Boot (0/5)
- Process Injection (0/12)
- Reflective Code Loading
- Rogue Domain Controller
- Rootkit
- Subvert Trust Controls (0/6)
- System Binary Proxy Execution (0/13)
- System Script Proxy Execution (0/1)
- Template Injection
- Traffic Signaling (0/1)
- Trusted Developer Utilities Proxy Execution (0/1)
- Unused/Unsupported Cloud Regions
- Use Alternate Authentication Material (1/4)
- Valid Accounts (0/4)
- Virtualization/Sandbox Evasion (0/3)
- Weaken Encryption (0/2)
- XSL Script Processing

**Credential Access**
16 techniques

- Adversary-in-the-Middle (0/3)
- Brute Force (0/4)
- Credentials from Password Stores (0/5)
- Exploitation for Credential Access
- Forced Authentication
- Forge Web Credentials (0/2)
- Input Capture (0/4)
- Modify Authentication Process (0/5)
- Multi-Factor Authentication Interception
- Multi-Factor Authentication Request Generation
- Network Sniffing
- OS Credential Dumping (1/8)
- Steal Application Access Token
- Steal or Forge Kerberos Tickets (0/4)
- Steal Web Session Cookie
- Unsecured Credentials (0/7)

**Discovery**
30 techniques

- Account Discovery (1/4)
- Application Window Discovery
- Browser Bookmark Discovery
- Cloud Infrastructure Discovery
- Cloud Service Dashboard
- Cloud Service Discovery
- Cloud Storage Object Discovery
- Container and Resource Discovery
- Debugger Evasion
- Domain Trust Discovery
- File and Directory Discovery
- Group Policy Discovery
- Network Service Discovery
- 🟥 Network Share Discovery
- Network Sniffing
- Password Policy Discovery
- Peripheral Device Discovery
- Permission Groups Discovery (0/3)
- 🟥 Process Discovery
- Query Registry
- Remote System Discovery
- Software Discovery (0/1)
- System Information Discovery
- System Location Discovery (0/1)
- 🟥 System Network Configuration Discovery (0/1)
- 🟥 System Network Connections Discovery
- System Owner/User Discovery
- 🟥 System Service Discovery
- System Time Discovery
- Virtualization/Sandbox Evasion (0/3)

**Lateral Movement**
9 techniques

- Exploitation of Remote Services
- Internal Spearphishing
- Lateral Tool Transfer
- Remote Service Session Hijacking (0/2)
- Remote Services (1/6)
- Replication Through Removable Media
- Software Deployment Tools
- Taint Shared Content
- Use Alternate Authentication Material (1/4)

**Collection**
17 techniques

- Adversary-in-the-Middle (0/3)
- Archive Collected Data (1/3)
- Audio Capture
- 🟥 Automated Collection
- Browser Session Hijacking
- Clipboard Data
- Data from Cloud Storage Object
- Data from Configuration Repository (0/2)
- Data from Information Repositories (0/3)
- 🟥 Data from Local System
- Data from Network Shared Drive
- Data from Removable Media
- Data Staged (0/2)
- Email Collection (2/3)
- Input Capture (0/4)
- Screen Capture
- Video Capture

**Command and Control**
16 techniques

- Application Layer Protocol (0/4)
- Communication Through Removable Media
- Data Encoding (0/2)
- Data Obfuscation (0/3)
- Dynamic Resolution (0/3)
- Encrypted Channel (0/2)
- Fallback Channels
- Ingress Tool Transfer
- Multi-Stage Channels
- Non-Application Layer Protocol
- Non-Standard Port
- Protocol Tunneling
- Proxy (0/4)
- Remote Access Software
- Traffic Signaling (0/1)
- Web Service (0/3)

**Exfiltration**
9 techniques

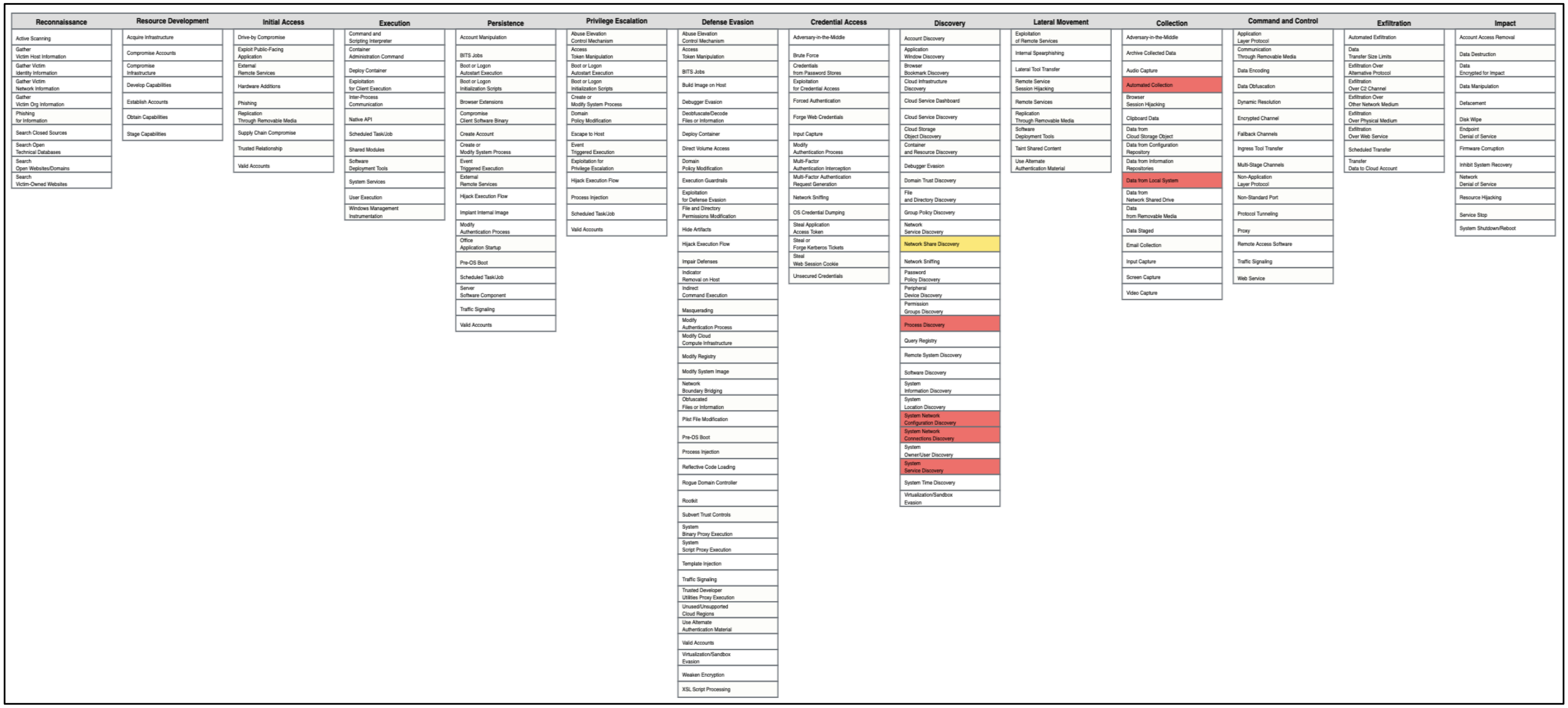
- Automated Exfiltration (0/1)
- Data Transfer Size Limits
- Exfiltration Over Alternative Protocol (0/3)
- Exfiltration Over C2 Channel
- Exfiltration Over Other Network Medium (0/1)
- Exfiltration Over Physical Medium (0/1)
- Exfiltration Over Web Service (0/2)
- Scheduled Transfer
- Transfer Data to Cloud Account

**Impact**
13 techniques

- Account Access Removal
- Data Destruction
- Data Encrypted for Impact
- Data Manipulation (0/3)
- Defacement (0/2)
- Disk Wipe (0/2)
- Endpoint Denial of Service (0/4)
- Firmware Corruption
- Inhibit System Recovery
- Network Denial of Service (0/2)
- Resource Hijacking
- Service Stop
- System Shutdown/Reboot

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

**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.

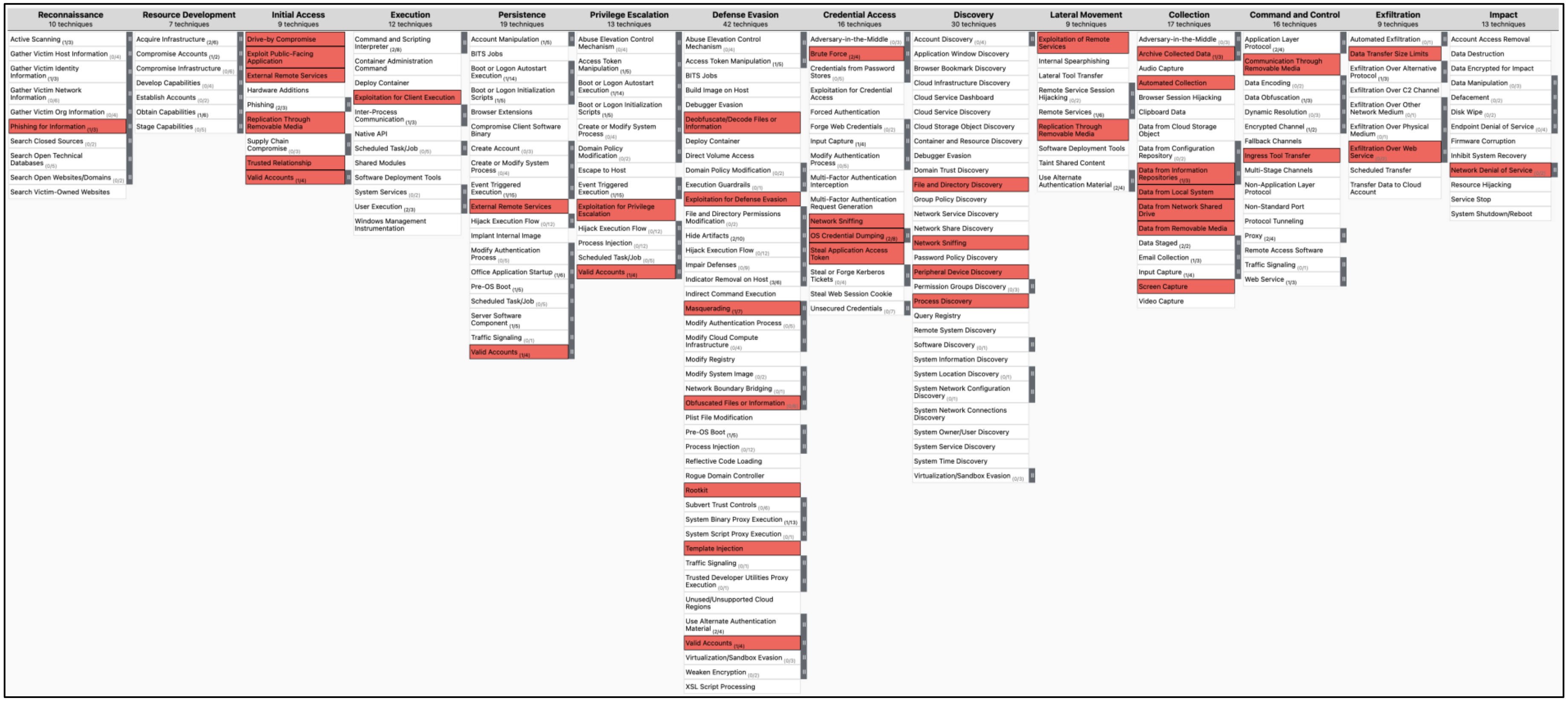
## 3.2 APT28 Results

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

- Active Scanning (1/3)
- Gather Victim Host Information (0/4)
- Gather Victim Identity Information (1/3)
- Gather Victim Network Information (0/6)
- Gather Victim Org Information (0/4)
- 🟥 Phishing for Information (1/3)
- Search Closed Sources (0/2)
- Search Open Technical Databases (0/5)
- Search Open Websites/Domains (0/2)
- Search Victim-Owned Websites

**Resource Development**
7 techniques

- Acquire Infrastructure (2/6)
- Compromise Accounts (1/2)
- Compromise Infrastructure (0/6)
- Develop Capabilities (0/4)
- Establish Accounts (0/2)
- Obtain Capabilities (1/6)
- Stage Capabilities (0/5)

**Initial Access**
9 techniques

- 🟥 Drive-by Compromise
- 🟥 Exploit Public-Facing Application
- 🟥 External Remote Services
- Hardware Additions
- Phishing (2/3)
- 🟥 Replication Through Removable Media
- Supply Chain Compromise (0/3)
- 🟥 Trusted Relationship
- 🟥 Valid Accounts (1/4)

**Execution**
12 techniques

- Command and Scripting Interpreter (2/8)
- Container Administration Command
- Deploy Container
- 🟥 Exploitation for Client Execution
- Inter-Process Communication (1/3)
- Native API
- Scheduled Task/Job (0/5)
- Shared Modules
- Software Deployment Tools
- System Services (0/2)
- User Execution (2/3)
- Windows Management Instrumentation

**Persistence**
19 techniques

- Account Manipulation (1/5)
- BITS Jobs
- Boot or Logon Autostart Execution (1/14)
- Boot or Logon Initialization Scripts (1/5)
- Browser Extensions
- Compromise Client Software Binary
- Create Account (0/3)
- Create or Modify System Process (0/4)
- Event Triggered Execution (1/15)
- 🟥 External Remote Services
- Hijack Execution Flow (0/12)
- Implant Internal Image
- Modify Authentication Process (0/5)
- Office Application Startup (1/6)
- Pre-OS Boot (1/5)
- Scheduled Task/Job (0/5)
- Server Software Component (1/5)
- Traffic Signaling (0/1)
- 🟥 Valid Accounts (1/4)

**Privilege Escalation**
13 techniques

- Abuse Elevation Control Mechanism (0/4)
- Access Token Manipulation (1/5)
- Boot or Logon Autostart Execution (1/14)
- Boot or Logon Initialization Scripts (1/5)
- Create or Modify System Process (0/4)
- Domain Policy Modification (0/2)
- Escape to Host
- Event Triggered Execution (1/15)
- 🟥 Exploitation for Privilege Escalation
- Hijack Execution Flow (0/12)
- Process Injection (0/12)
- Scheduled Task/Job (0/5)
- 🟥 Valid Accounts (1/4)

**Defense Evasion**
42 techniques

- Abuse Elevation Control Mechanism (0/4)
- Access Token Manipulation (1/5)
- BITS Jobs
- Build Image on Host
- Debugger Evasion
- 🟥 Deobfuscate/Decode Files or Information
- Deploy Container
- Direct Volume Access
- Domain Policy Modification (0/2)
- Execution Guardrails (0/1)
- 🟥 Exploitation for Defense Evasion
- File and Directory Permissions Modification (0/2)
- Hide Artifacts (2/10)
- Hijack Execution Flow (0/12)
- Impair Defenses (0/9)
- Indicator Removal on Host (3/6)
- Indirect Command Execution
- 🟥 Masquerading (1/7)
- Modify Authentication Process (0/5)
- Modify Cloud Compute Infrastructure (0/4)
- Modify Registry
- Modify System Image (0/2)
- Network Boundary Bridging (0/1)
- 🟥 Obfuscated Files or Information (0/6)
- Plist File Modification
- Pre-OS Boot (1/5)
- Process Injection (0/12)
- Reflective Code Loading
- Rogue Domain Controller
- 🟥 Rootkit
- Subvert Trust Controls (0/6)
- System Binary Proxy Execution (1/13)
- System Script Proxy Execution (0/1)
- 🟥 Template Injection
- Traffic Signaling (0/1)
- Trusted Developer Utilities Proxy Execution (0/1)
- Unused/Unsupported Cloud Regions
- Use Alternate Authentication Material (2/4)
- 🟥 Valid Accounts (1/4)
- Virtualization/Sandbox Evasion (0/3)
- Weaken Encryption (0/2)
- XSL Script Processing

**Credential Access**
16 techniques

- Adversary-in-the-Middle (0/3)
- 🟥 Brute Force (2/4)
- Credentials from Password Stores (0/5)
- Exploitation for Credential Access
- Forced Authentication
- Forge Web Credentials (0/2)
- Input Capture (1/4)
- Modify Authentication Process (0/5)
- Multi-Factor Authentication Interception
- Multi-Factor Authentication Request Generation
- 🟥 Network Sniffing
- 🟥 OS Credential Dumping (2/8)
- 🟥 Steal Application Access Token
- Steal or Forge Kerberos Tickets (0/4)
- Steal Web Session Cookie
- Unsecured Credentials (0/7)

**Discovery**
30 techniques

- Account Discovery (0/4)
- Application Window Discovery
- Browser Bookmark Discovery
- Cloud Infrastructure Discovery
- Cloud Service Dashboard
- Cloud Service Discovery
- Cloud Storage Object Discovery
- Container and Resource Discovery
- Debugger Evasion
- Domain Trust Discovery
- 🟥 File and Directory Discovery
- Group Policy Discovery
- Network Service Discovery
- Network Share Discovery
- 🟥 Network Sniffing
- Password Policy Discovery
- 🟥 Peripheral Device Discovery
- Permission Groups Discovery (0/3)
- 🟥 Process Discovery
- Query Registry
- Remote System Discovery
- Software Discovery (0/1)
- System Information Discovery
- System Location Discovery (0/1)
- System Network Configuration Discovery (0/1)
- System Network Connections Discovery
- System Owner/User Discovery
- System Service Discovery
- System Time Discovery
- Virtualization/Sandbox Evasion (0/3)

**Lateral Movement**
9 techniques

- 🟥 Exploitation of Remote Services
- Internal Spearphishing
- Lateral Tool Transfer
- Remote Service Session Hijacking (0/2)
- Remote Services (1/6)
- 🟥 Replication Through Removable Media
- Software Deployment Tools
- Taint Shared Content
- Use Alternate Authentication Material (2/4)

**Collection**
17 techniques

- Adversary-in-the-Middle (0/3)
- 🟥 Archive Collected Data (1/3)
- Audio Capture
- 🟥 Automated Collection
- Browser Session Hijacking
- Clipboard Data
- Data from Cloud Storage Object
- Data from Configuration Repository (0/2)
- 🟥 Data from Information Repositories (1/3)
- 🟥 Data from Local System
- 🟥 Data from Network Shared Drive
- 🟥 Data from Removable Media
- Data Staged (2/2)
- Email Collection (1/3)
- Input Capture (1/4)
- 🟥 Screen Capture
- Video Capture

**Command and Control**
16 techniques

- Application Layer Protocol (2/4)
- 🟥 Communication Through Removable Media
- Data Encoding (0/2)
- Data Obfuscation (1/3)
- Dynamic Resolution (0/3)
- Encrypted Channel (1/2)
- Fallback Channels
- 🟥 Ingress Tool Transfer
- Multi-Stage Channels
- Non-Application Layer Protocol
- Non-Standard Port
- Protocol Tunneling
- Proxy (2/4)
- Remote Access Software
- Traffic Signaling (0/1)
- Web Service (1/3)

**Exfiltration**
9 techniques

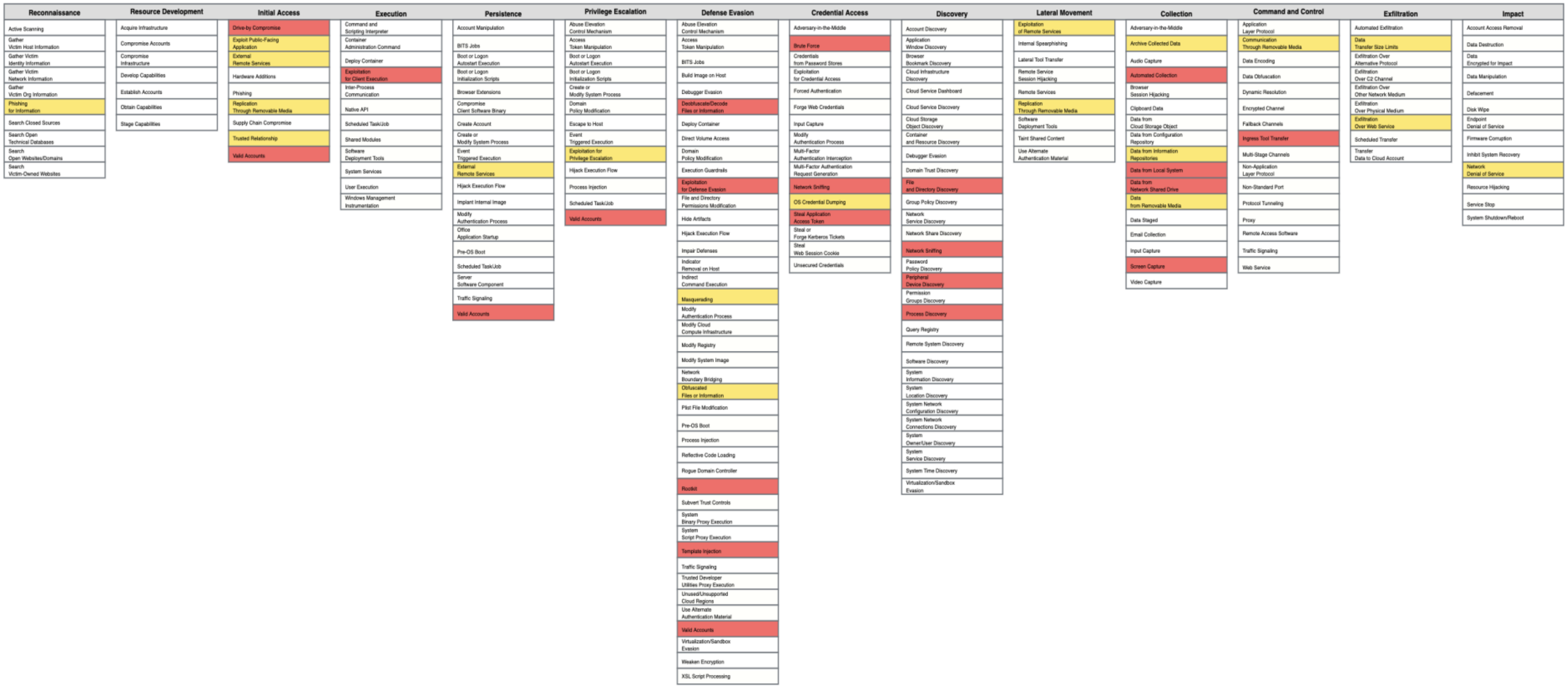
- Automated Exfiltration (0/1)
- 🟥 Data Transfer Size Limits
- Exfiltration Over Alternative Protocol (1/3)
- Exfiltration Over C2 Channel
- Exfiltration Over Other Network Medium (0/1)
- Exfiltration Over Physical Medium (0/1)
- 🟥 Exfiltration Over Web Service (0/2)
- Scheduled Transfer
- Transfer Data to Cloud Account

**Impact**
13 techniques

- Account Access Removal
- Data Destruction
- Data Encrypted for Impact
- Data Manipulation (0/3)
- Defacement (0/2)
- Disk Wipe (0/2)
- Endpoint Denial of Service (0/4)
- Firmware Corruption
- Inhibit System Recovery
- 🟥 Network Denial of Service (0/2)
- Resource Hijacking
- Service Stop
- System Shutdown/Reboot

**Figure 4. APT28 Coverage map**

TTPs used by APT28 shown as red.



**Reconnaissance**

- Active Scanning
- Gather Victim Host Information
- Gather Victim Identity Information
- Gather Victim Network Information
- Gather Victim Org Information
- 🟨 Phishing for Information
- Search Closed Sources
- Search Open Technical Databases
- Search Open Websites/Domains
- Search Victim-Owned Websites

**Resource Development**

- Acquire Infrastructure
- Compromise Accounts
- Compromise Infrastructure
- Develop Capabilities
- Establish Accounts
- Obtain Capabilities
- Stage Capabilities

**Initial Access**

- 🟥 Drive-by Compromise
- 🟨 Exploit Public-Facing Application
- 🟨 External Remote Services
- Hardware Additions
- Phishing
- 🟨 Replication Through Removable Media
- Supply Chain Compromise
- 🟨 Trusted Relationship
- 🟥 Valid Accounts

**Execution**

- Command and Scripting Interpreter
- Container Administration Command
- Deploy Container
- 🟥 Exploitation for Client Execution
- Inter-Process Communication
- Native API
- Scheduled Task/Job
- Shared Modules
- Software Deployment Tools
- System Services
- User Execution
- Windows Management Instrumentation

**Persistence**

- Account Manipulation
- BITS Jobs
- Boot or Logon Autostart Execution
- Boot or Logon Initialization Scripts
- Browser Extensions
- Compromise Client Software Binary
- Create Account
- Create or Modify System Process
- Event Triggered Execution
- 🟨 External Remote Services
- Hijack Execution Flow
- Implant Internal Image
- Modify Authentication Process
- Office Application Startup
- Pre-OS Boot
- Scheduled Task/Job
- Server Software Component
- Traffic Signaling
- 🟥 Valid Accounts

**Privilege Escalation**

- Abuse Elevation Control Mechanism
- Access Token Manipulation
- Boot or Logon Autostart Execution
- Boot or Logon Initialization Scripts
- Create or Modify System Process
- Domain Policy Modification
- Escape to Host
- Event Triggered Execution
- 🟨 Exploitation for Privilege Escalation
- Hijack Execution Flow
- Process Injection
- Scheduled Task/Job
- 🟥 Valid Accounts

**Defense Evasion**

- Abuse Elevation Control Mechanism
- Access Token Manipulation
- BITS Jobs
- Build Image on Host
- Debugger Evasion
- 🟥 Deobfuscate/Decode Files or Information
- Deploy Container
- Direct Volume Access
- Domain Policy Modification
- Execution Guardrails
- 🟥 Exploitation for Defense Evasion
- File and Directory Permissions Modification
- Hide Artifacts
- Hijack Execution Flow
- Impair Defenses
- Indicator Removal on Host
- Indirect Command Execution
- 🟨 Masquerading
- Modify Authentication Process
- Modify Cloud Compute Infrastructure
- Modify Registry
- Modify System Image
- Network Boundary Bridging
- 🟨 Obfuscated Files or Information
- Plist File Modification
- Pre-OS Boot
- Process Injection
- Reflective Code Loading
- Rogue Domain Controller
- 🟥 Rootkit
- Subvert Trust Controls
- System Binary Proxy Execution
- System Script Proxy Execution
- 🟥 Template Injection
- Traffic Signaling
- Trusted Developer Utilities Proxy Execution
- Unused/Unsupported Cloud Regions
- Use Alternate Authentication Material
- 🟥 Valid Accounts
- Virtualization/Sandbox Evasion
- Weaken Encryption
- XSL Script Processing

**Credential Access**

- Adversary-in-the-Middle
- 🟥 Brute Force
- Credentials from Password Stores
- Exploitation for Credential Access
- Forced Authentication
- Forge Web Credentials
- Input Capture
- Modify Authentication Process
- Multi-Factor Authentication Interception
- Multi-Factor Authentication Request Generation
- 🟥 Network Sniffing
- 🟨 OS Credential Dumping
- 🟥 Steal Application Access Token
- Steal or Forge Kerberos Tickets
- Steal Web Session Cookie
- Unsecured Credentials

**Discovery**

- Account Discovery
- Application Window Discovery
- Browser Bookmark Discovery
- Cloud Infrastructure Discovery
- Cloud Service Dashboard
- Cloud Service Discovery
- Cloud Storage Object Discovery
- Container and Resource Discovery
- Debugger Evasion
- Domain Trust Discovery
- 🟥 File and Directory Discovery
- Group Policy Discovery
- Network Service Discovery
- Network Share Discovery
- 🟥 Network Sniffing
- Password Policy Discovery
- 🟥 Peripheral Device Discovery
- Permission Groups Discovery
- 🟥 Process Discovery
- Query Registry
- Remote System Discovery
- Software Discovery
- System Information Discovery
- System Location Discovery
- System Network Configuration Discovery
- System Network Connections Discovery
- System Owner/User Discovery
- System Service Discovery
- System Time Discovery
- Virtualization/Sandbox Evasion

**Lateral Movement**

- 🟨 Exploitation of Remote Services
- Internal Spearphishing
- Lateral Tool Transfer
- Remote Service Session Hijacking
- Remote Services
- 🟨 Replication Through Removable Media
- Software Deployment Tools
- Taint Shared Content
- Use Alternate Authentication Material

**Collection**

- Adversary-in-the-Middle
- 🟨 Archive Collected Data
- Audio Capture
- 🟥 Automated Collection
- Browser Session Hijacking
- Clipboard Data
- Data from Cloud Storage Object
- Data from Configuration Repository
- 🟨 Data from Information Repositories
- 🟥 Data from Local System
- 🟥 Data from Network Shared Drive
- 🟨 Data from Removable Media
- Data Staged
- Email Collection
- Input Capture
- 🟥 Screen Capture
- Video Capture

**Command and Control**

- Application Layer Protocol
- 🟨 Communication Through Removable Media
- Data Encoding
- Data Obfuscation
- Dynamic Resolution
- Encrypted Channel
- Fallback Channels
- 🟥 Ingress Tool Transfer
- Multi-Stage Channels
- Non-Application Layer Protocol
- Non-Standard Port
- Protocol Tunneling
- Proxy
- Remote Access Software
- Traffic Signaling
- Web Service

**Exfiltration**

- Automated Exfiltration
- 🟨 Data Transfer Size Limits
- Exfiltration Over Alternative Protocol
- Exfiltration Over C2 Channel
- Exfiltration Over Other Network Medium
- Exfiltration Over Physical Medium
- 🟨 Exfiltration Over Web Service
- Scheduled Transfer
- Transfer Data to Cloud Account

**Impact**

- Account Access Removal
- Data Destruction
- Data Encrypted for Impact
- Data Manipulation
- Defacement
- Disk Wipe
- Endpoint Denial of Service
- Firmware Corruption
- Inhibit System Recovery
- 🟨 Network Denial of Service
- Resource Hijacking
- Service Stop
- System Shutdown/Reboot

**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.

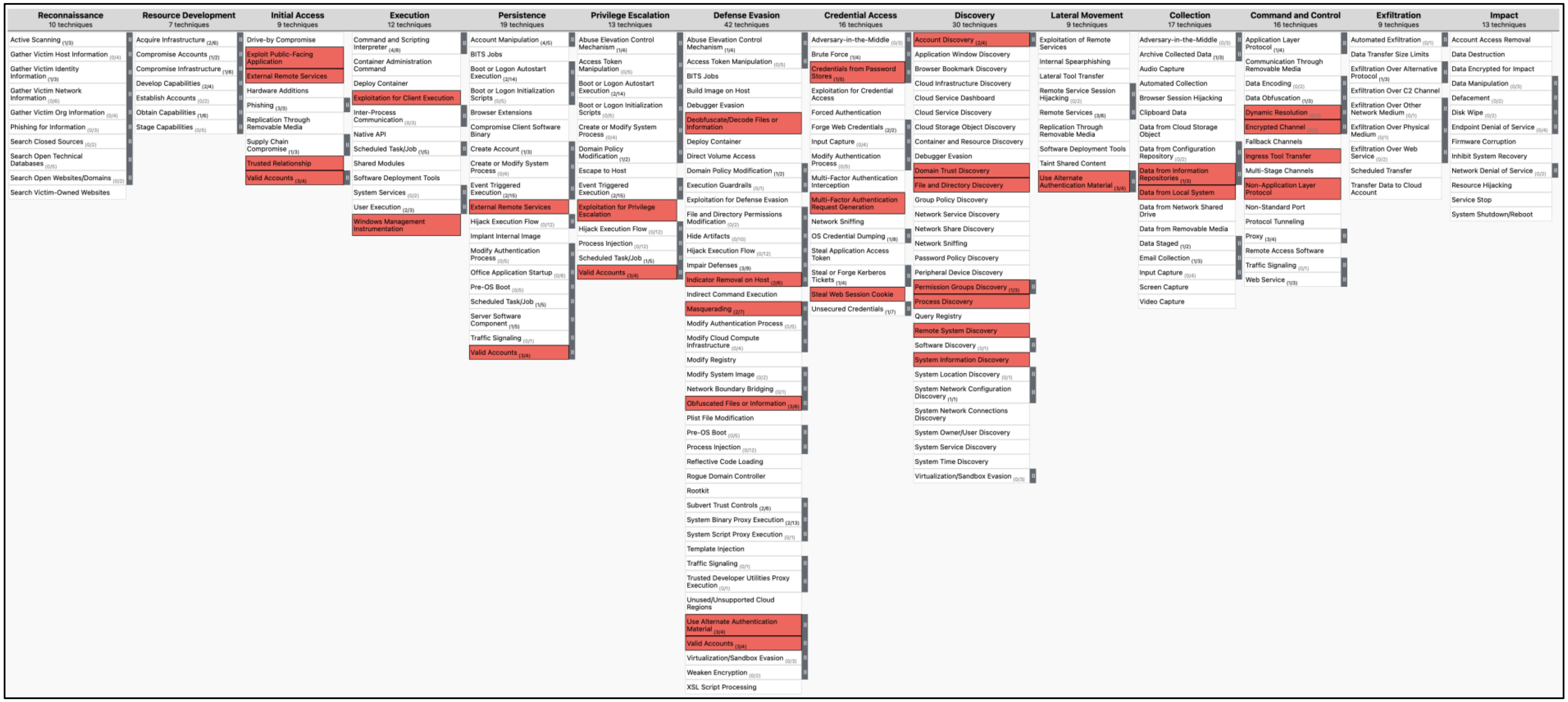
## 3.3 APT29 Results

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.



Reconnaissance
10 techniques

- Active Scanning (1/3)
- Gather Victim Host Information (0/4)
- Gather Victim Identity Information (1/3)
- Gather Victim Network Information (0/6)
- Gather Victim Org Information (0/4)
- Phishing for Information (0/3)
- Search Closed Sources (0/2)
- Search Open Technical Databases (0/5)
- Search Open Websites/Domains (0/2)
- Search Victim-Owned Websites

Resource Development
7 techniques

- Acquire Infrastructure (2/6)
- Compromise Accounts (1/2)
- Compromise Infrastructure (1/6)
- Develop Capabilities (2/4)
- Establish Accounts (0/2)
- Obtain Capabilities (1/6)
- Stage Capabilities (0/5)

Initial Access
9 techniques

- Drive-by Compromise
- 🟥 Exploit Public-Facing Application
- 🟥 External Remote Services
- Hardware Additions
- Phishing (3/3)
- Replication Through Removable Media
- Supply Chain Compromise (1/3)
- 🟥 Trusted Relationship
- 🟥 Valid Accounts (3/4)

Execution
12 techniques

- Command and Scripting Interpreter (4/8)
- Container Administration Command
- Deploy Container
- 🟥 Exploitation for Client Execution
- Inter-Process Communication (0/3)
- Native API
- Scheduled Task/Job (1/5)
- Shared Modules
- Software Deployment Tools
- System Services (0/2)
- User Execution (2/3)
- 🟥 Windows Management Instrumentation

Persistence
19 techniques

- Account Manipulation (4/5)
- BITS Jobs
- Boot or Logon Autostart Execution (2/14)
- Boot or Logon Initialization Scripts (0/5)
- Browser Extensions
- Compromise Client Software Binary
- Create Account (1/3)
- Create or Modify System Process (0/4)
- Event Triggered Execution (2/15)
- 🟥 External Remote Services
- Hijack Execution Flow (0/12)
- Implant Internal Image
- Modify Authentication Process (0/5)
- Office Application Startup (0/6)
- Pre-OS Boot (0/5)
- Scheduled Task/Job (1/5)
- Server Software Component (1/5)
- Traffic Signaling (0/1)
- 🟥 Valid Accounts (3/4)

Privilege Escalation
13 techniques

- Abuse Elevation Control Mechanism (1/4)
- Access Token Manipulation (0/5)
- Boot or Logon Autostart Execution (2/14)
- Boot or Logon Initialization Scripts (0/5)
- Create or Modify System Process (0/4)
- Domain Policy Modification (1/2)
- Escape to Host
- Event Triggered Execution (2/15)
- 🟥 Exploitation for Privilege Escalation
- Hijack Execution Flow (0/12)
- Process Injection (0/12)
- Scheduled Task/Job (1/5)
- 🟥 Valid Accounts (3/4)

Defense Evasion
42 techniques

- Abuse Elevation Control Mechanism (1/4)
- Access Token Manipulation (0/5)
- BITS Jobs
- Build Image on Host
- Debugger Evasion
- 🟥 Deobfuscate/Decode Files or Information
- Deploy Container
- Direct Volume Access
- Domain Policy Modification (1/2)
- Execution Guardrails (0/1)
- Exploitation for Defense Evasion
- File and Directory Permissions Modification (0/2)
- Hide Artifacts (0/10)
- Hijack Execution Flow (0/12)
- Impair Defenses (3/9)
- 🟥 Indicator Removal on Host (2/6)
- Indirect Command Execution
- 🟥 Masquerading (2/7)
- Modify Authentication Process (0/5)
- Modify Cloud Compute Infrastructure (0/4)
- Modify Registry
- Modify System Image (0/2)
- Network Boundary Bridging (0/1)
- 🟥 Obfuscated Files or Information (3/6)
- Plist File Modification
- Pre-OS Boot (0/5)
- Process Injection (0/12)
- Reflective Code Loading
- Rogue Domain Controller
- Rootkit
- Subvert Trust Controls (2/6)
- System Binary Proxy Execution (2/13)
- System Script Proxy Execution (0/1)
- Template Injection
- Traffic Signaling (0/1)
- Trusted Developer Utilities Proxy Execution (0/1)
- Unused/Unsupported Cloud Regions
- 🟥 Use Alternate Authentication Material (3/4)
- 🟥 Valid Accounts (3/4)
- Virtualization/Sandbox Evasion (0/3)
- Weaken Encryption (0/2)
- XSL Script Processing

Credential Access
16 techniques

- Adversary-in-the-Middle (0/3)
- Brute Force (1/4)
- 🟥 Credentials from Password Stores (1/5)
- Exploitation for Credential Access
- Forced Authentication
- Forge Web Credentials (2/2)
- Input Capture (0/4)
- Modify Authentication Process (0/5)
- Multi-Factor Authentication Interception
- 🟥 Multi-Factor Authentication Request Generation
- Network Sniffing
- OS Credential Dumping (1/8)
- Steal Application Access Token
- Steal or Forge Kerberos Tickets (1/4)
- 🟥 Steal Web Session Cookie
- Unsecured Credentials (1/7)

Discovery
30 techniques

- 🟥 Account Discovery (2/4)
- Application Window Discovery
- Browser Bookmark Discovery
- Cloud Infrastructure Discovery
- Cloud Service Dashboard
- Cloud Service Discovery
- Cloud Storage Object Discovery
- Container and Resource Discovery
- Debugger Evasion
- 🟥 Domain Trust Discovery
- 🟥 File and Directory Discovery
- Group Policy Discovery
- Network Service Discovery
- Network Share Discovery
- Network Sniffing
- Password Policy Discovery
- Peripheral Device Discovery
- 🟥 Permission Groups Discovery (1/3)
- 🟥 Process Discovery
- Query Registry
- 🟥 Remote System Discovery
- Software Discovery (0/1)
- 🟥 System Information Discovery
- System Location Discovery (0/1)
- System Network Configuration Discovery (1/1)
- System Network Connections Discovery
- System Owner/User Discovery
- System Service Discovery
- System Time Discovery
- Virtualization/Sandbox Evasion (0/3)

Lateral Movement
9 techniques

- Exploitation of Remote Services
- Internal Spearphishing
- Lateral Tool Transfer
- Remote Service Session Hijacking (0/2)
- Remote Services (3/6)
- Replication Through Removable Media
- Software Deployment Tools
- Taint Shared Content
- 🟥 Use Alternate Authentication Material (3/4)

Collection
17 techniques

- Adversary-in-the-Middle (0/3)
- Archive Collected Data (1/3)
- Audio Capture
- Automated Collection
- Browser Session Hijacking
- Clipboard Data
- Data from Cloud Storage Object
- Data from Configuration Repository (0/2)
- 🟥 Data from Information Repositories (1/3)
- 🟥 Data from Local System
- Data from Network Shared Drive
- Data from Removable Media
- Data Staged (1/2)
- Email Collection (1/3)
- Input Capture (0/4)
- Screen Capture
- Video Capture

Command and Control
16 techniques

- Application Layer Protocol (1/4)
- Communication Through Removable Media
- Data Encoding (0/2)
- Data Obfuscation (1/3)
- 🟥 Dynamic Resolution (0/3)
- 🟥 Encrypted Channel (0/2)
- Fallback Channels
- 🟥 Ingress Tool Transfer
- Multi-Stage Channels
- 🟥 Non-Application Layer Protocol
- Non-Standard Port
- Protocol Tunneling
- Proxy (3/4)
- Remote Access Software
- Traffic Signaling (0/1)
- Web Service (1/3)

Exfiltration
9 techniques

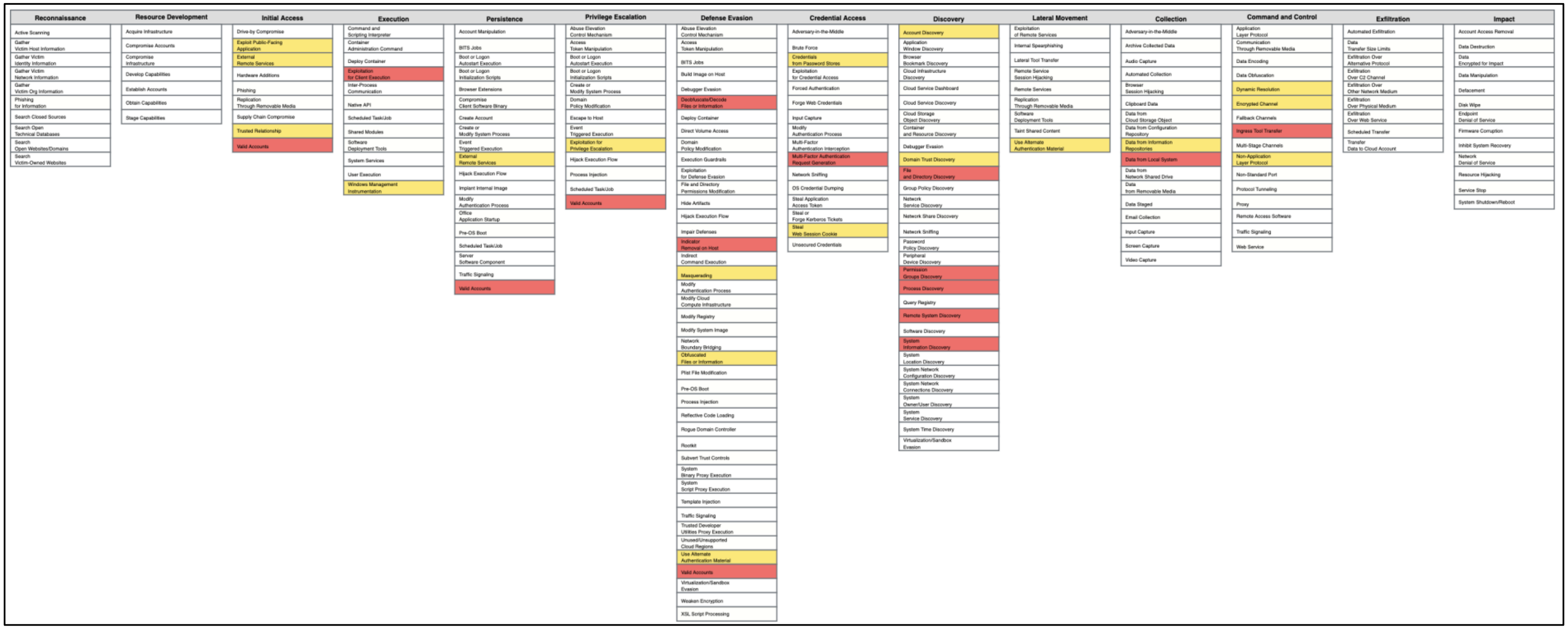
- Automated Exfiltration (0/1)
- Data Transfer Size Limits
- Exfiltration Over Alternative Protocol (1/3)
- Exfiltration Over C2 Channel
- Exfiltration Over Other Network Medium (0/1)
- Exfiltration Over Physical Medium (0/1)
- Exfiltration Over Web Service (0/2)
- Scheduled Transfer
- Transfer Data to Cloud Account

Impact
13 techniques

- Account Access Removal
- Data Destruction
- Data Encrypted for Impact
- Data Manipulation (0/3)
- Defacement (0/2)
- Disk Wipe (0/2)
- Endpoint Denial of Service (0/4)
- Firmware Corruption
- Inhibit System Recovery
- Network Denial of Service (0/2)
- Resource Hijacking
- Service Stop
- System Shutdown/Reboot

**Figure 6. APT29 Coverage map**

TTPs used by APT29 shown as red.



**Reconnaissance**
- Active Scanning
- Gather Victim Host Information
- Gather Victim Identity Information
- Gather Victim Network Information
- Gather Victim Org Information
- Phishing for Information
- Search Closed Sources
- Search Open Technical Databases
- Search Open Websites/Domains
- Search Victim-Owned Websites

**Resource Development**
- Acquire Infrastructure
- Compromise Accounts
- Compromise Infrastructure
- Develop Capabilities
- Establish Accounts
- Obtain Capabilities
- Stage Capabilities

**Initial Access**
- Drive-by Compromise
- 🟨 Exploit Public-Facing Application
- 🟨 External Remote Services
- Hardware Additions
- Phishing
- Replication Through Removable Media
- Supply Chain Compromise
- 🟨 Trusted Relationship
- 🟥 Valid Accounts

**Execution**
- Command and Scripting Interpreter
- Container Administration Command
- Deploy Container
- 🟥 Exploitation for Client Execution
- Inter-Process Communication
- Native API
- Scheduled Task/Job
- Shared Modules
- Software Deployment Tools
- System Services
- User Execution
- 🟨 Windows Management Instrumentation

**Persistence**
- Account Manipulation
- BITS Jobs
- Boot or Logon Autostart Execution
- Boot or Logon Initialization Scripts
- Browser Extensions
- Compromise Client Software Binary
- Create Account
- Create or Modify System Process
- Event Triggered Execution
- 🟨 External Remote Services
- Hijack Execution Flow
- Implant Internal Image
- Modify Authentication Process
- Office Application Startup
- Pre-OS Boot
- Scheduled Task/Job
- Server Software Component
- Traffic Signaling
- 🟥 Valid Accounts

**Privilege Escalation**
- Abuse Elevation Control Mechanism
- Access Token Manipulation
- Boot or Logon Autostart Execution
- Boot or Logon Initialization Scripts
- Create or Modify System Process
- Domain Policy Modification
- Escape to Host
- Event Triggered Execution
- 🟨 Exploitation for Privilege Escalation
- Hijack Execution Flow
- Process Injection
- Scheduled Task/Job
- 🟥 Valid Accounts

**Defense Evasion**
- Abuse Elevation Control Mechanism
- Access Token Manipulation
- BITS Jobs
- Build Image on Host
- Debugger Evasion
- 🟥 Deobfuscate/Decode Files or Information
- Deploy Container
- Direct Volume Access
- Domain Policy Modification
- Execution Guardrails
- Exploitation for Defense Evasion
- File and Directory Permissions Modification
- Hide Artifacts
- Hijack Execution Flow
- Impair Defenses
- 🟥 Indicator Removal on Host
- Indirect Command Execution
- 🟨 Masquerading
- Modify Authentication Process
- Modify Cloud Compute Infrastructure
- Modify Registry
- Modify System Image
- Network Boundary Bridging
- 🟨 Obfuscated Files or Information
- Plist File Modification
- Pre-OS Boot
- Process Injection
- Reflective Code Loading
- Rogue Domain Controller
- Rootkit
- Subvert Trust Controls
- System Binary Proxy Execution
- System Script Proxy Execution
- Template Injection
- Traffic Signaling
- Trusted Developer Utilities Proxy Execution
- Unused/Unsupported Cloud Regions
- 🟨 Use Alternate Authentication Material
- 🟥 Valid Accounts
- Virtualization/Sandbox Evasion
- Weaken Encryption
- XSL Script Processing

**Credential Access**
- Adversary-in-the-Middle
- Brute Force
- 🟨 Credentials from Password Stores
- Exploitation for Credential Access
- Forced Authentication
- Forge Web Credentials
- Input Capture
- Modify Authentication Process
- Multi-Factor Authentication Interception
- 🟥 Multi-Factor Authentication Request Generation
- Network Sniffing
- OS Credential Dumping
- Steal Application Access Token
- Steal or Forge Kerberos Tickets
- 🟨 Steal Web Session Cookie
- Unsecured Credentials

**Discovery**
- 🟨 Account Discovery
- Application Window Discovery
- Browser Bookmark Discovery
- Cloud Infrastructure Discovery
- Cloud Service Dashboard
- Cloud Service Discovery
- Cloud Storage Object Discovery
- Container and Resource Discovery
- Debugger Evasion
- 🟨 Domain Trust Discovery
- 🟥 File and Directory Discovery
- Group Policy Discovery
- Network Service Discovery
- Network Share Discovery
- Network Sniffing
- Password Policy Discovery
- Peripheral Device Discovery
- 🟥 Permission Groups Discovery
- 🟥 Process Discovery
- Query Registry
- 🟥 Remote System Discovery
- Software Discovery
- 🟥 System Information Discovery
- System Location Discovery
- System Network Configuration Discovery
- System Network Connections Discovery
- System Owner/User Discovery
- System Service Discovery
- System Time Discovery
- Virtualization/Sandbox Evasion

**Lateral Movement**
- Exploitation of Remote Services
- Internal Spearphishing
- Lateral Tool Transfer
- Remote Service Session Hijacking
- Remote Services
- Replication Through Removable Media
- Software Deployment Tools
- Taint Shared Content
- 🟨 Use Alternate Authentication Material

**Collection**
- Adversary-in-the-Middle
- Archive Collected Data
- Audio Capture
- Automated Collection
- Browser Session Hijacking
- Clipboard Data
- Data from Cloud Storage Object
- Data from Configuration Repository
- 🟨 Data from Information Repositories
- 🟥 Data from Local System
- Data from Network Shared Drive
- Data from Removable Media
- Data Staged
- Email Collection
- Input Capture
- Screen Capture
- Video Capture

**Command and Control**
- Application Layer Protocol
- Communication Through Removable Media
- Data Encoding
- Data Obfuscation
- 🟨 Dynamic Resolution
- 🟨 Encrypted Channel
- Fallback Channels
- 🟥 Ingress Tool Transfer
- Multi-Stage Channels
- 🟨 Non-Application Layer Protocol
- Non-Standard Port
- Protocol Tunneling
- Proxy
- Remote Access Software
- Traffic Signaling
- Web Service

**Exfiltration**
- Automated Exfiltration
- Data Transfer Size Limits
- Exfiltration Over Alternative Protocol
- Exfiltration Over C2 Channel
- Exfiltration Over Other Network Medium
- Exfiltration Over Physical Medium
- Exfiltration Over Web Service
- Scheduled Transfer
- Transfer Data to Cloud Account

**Impact**
- Account Access Removal
- Data Destruction
- Data Encrypted for Impact
- Data Manipulation
- Defacement
- Disk Wipe
- Endpoint Denial of Service
- Firmware Corruption
- Inhibit System Recovery
- Network Denial of Service
- Resource Hijacking
- Service Stop
- System Shutdown/Reboot

**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.

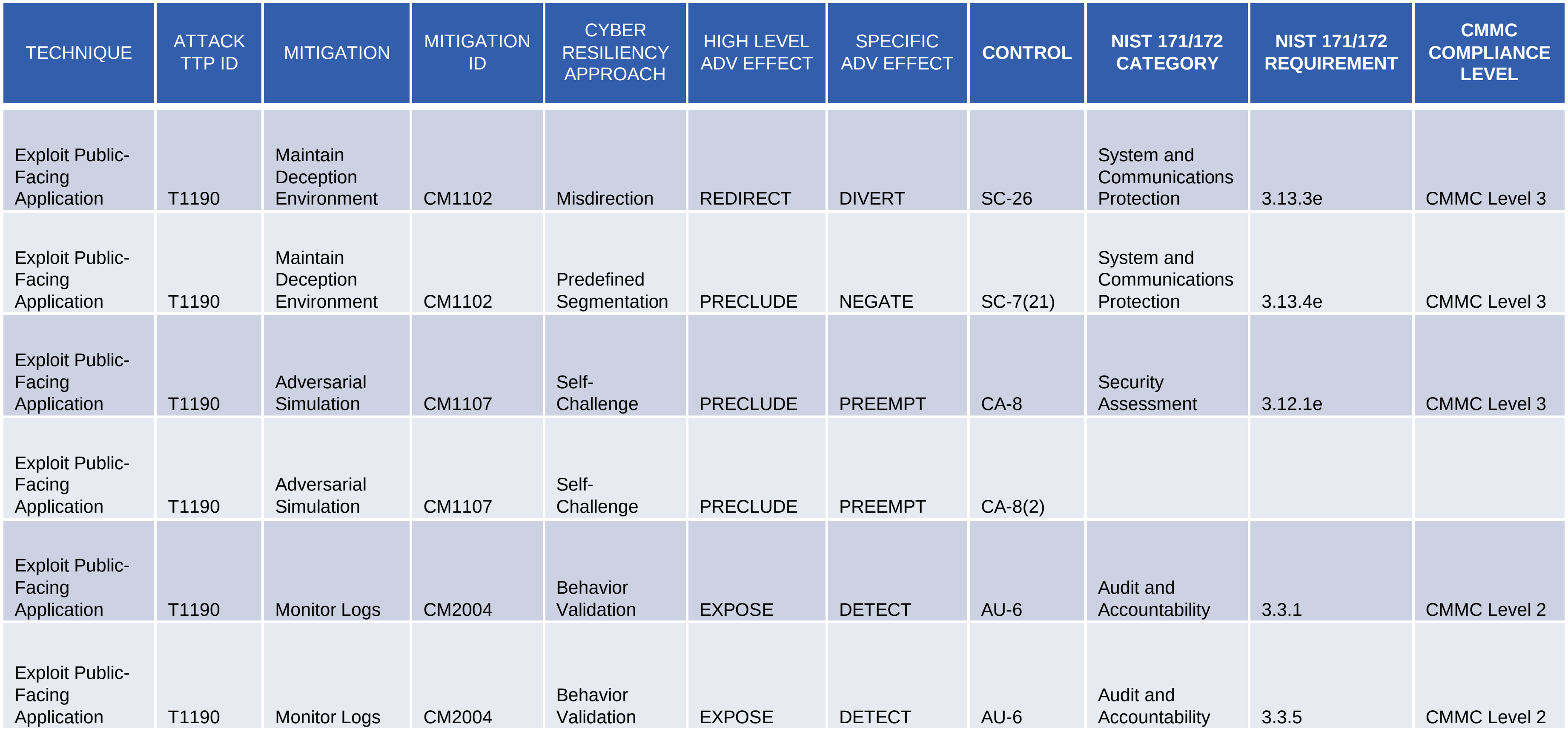
### A.1.1 Mapping Files

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 controls[10]. 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.



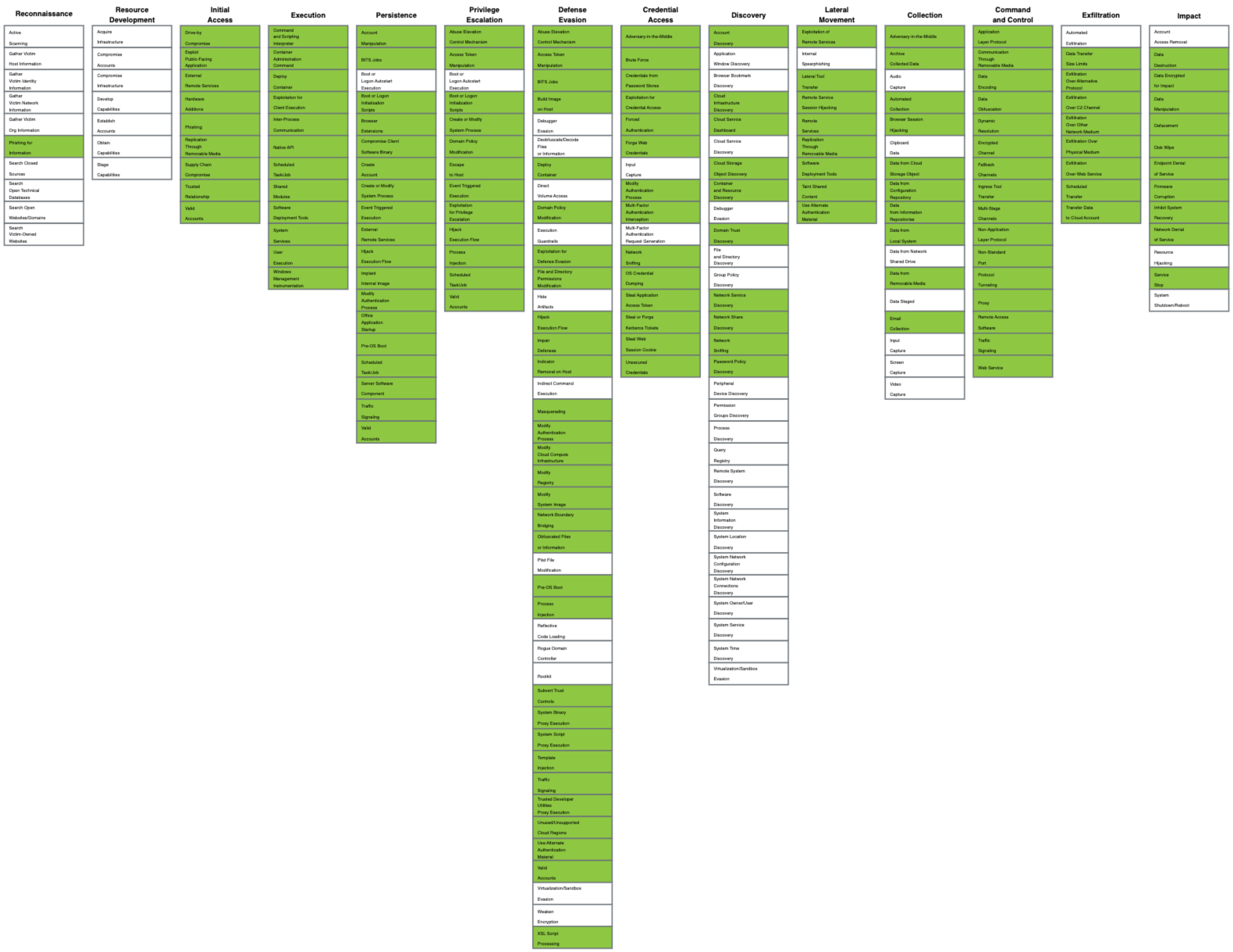
| TECHNIQUE | ATTACK TTP ID | MITIGATION | MITIGATION ID | CYBER RESILIENCY APPROACH | HIGH LEVEL ADV EFFECT | SPECIFIC ADV EFFECT | CONTROL | NIST 171/172 CATEGORY | NIST 171/172 REQUIREMENT | CMMC COMPLIANCE LEVEL |
|---|---|---|---|---|---|---|---|---|---|---|
| Exploit Public-Facing Application | 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.xlx – 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.



Reconnaissance
- ⬜ Active Scanning
- ⬜ Gather Victim Host Information
- ⬜ Gather Victim Identity Information
- ⬜ Gather Victim Network Information
- ⬜ Gather Victim Org Information
- 🟩 Phishing for Information
- ⬜ Search Closed Sources
- ⬜ Search Open Technical Databases
- ⬜ Search Open Websites/Domains
- ⬜ Search Victim-Owned Websites

Resource Development
- ⬜ Acquire Infrastructure
- ⬜ Compromise Accounts
- ⬜ Compromise Infrastructure
- ⬜ Develop Capabilities
- ⬜ Establish Accounts
- ⬜ Obtain Capabilities
- ⬜ Stage Capabilities

Initial Access
- 🟩 Drive-by Compromise
- 🟩 Exploit Public-Facing Application
- 🟩 External Remote Services
- 🟩 Hardware Additions
- 🟩 Phishing
- 🟩 Replication Through Removable Media
- 🟩 Supply Chain Compromise
- 🟩 Trusted Relationship
- 🟩 Valid Accounts

Execution
- 🟩 Command and Scripting Interpreter
- 🟩 Container Administration Command
- 🟩 Deploy Container
- 🟩 Exploitation for Client Execution
- 🟩 Inter-Process Communication
- 🟩 Native API
- 🟩 Scheduled Task/Job
- 🟩 Shared Modules
- 🟩 Software Deployment Tools
- 🟩 System Services
- 🟩 User Execution
- 🟩 Windows Management Instrumentation

Persistence
- 🟩 Account Manipulation
- 🟩 BITS Jobs
- ⬜ Boot or Logon Autostart Execution
- 🟩 Boot or Logon Initialization Scripts
- 🟩 Browser Extensions
- 🟩 Compromise Client Software Binary
- 🟩 Create Account
- 🟩 Create or Modify System Process
- 🟩 Event Triggered Execution
- 🟩 External Remote Services
- 🟩 Hijack Execution Flow
- 🟩 Implant Internal Image
- 🟩 Modify Authentication Process
- 🟩 Office Application Startup
- 🟩 Pre-OS Boot
- 🟩 Scheduled Task/Job
- 🟩 Server Software Component
- 🟩 Traffic Signaling
- 🟩 Valid Accounts

Privilege Escalation
- 🟩 Abuse Elevation Control Mechanism
- 🟩 Access Token Manipulation
- ⬜ Boot or Logon Autostart Execution
- 🟩 Boot or Logon Initialization Scripts
- 🟩 Create or Modify System Process
- 🟩 Domain Policy Modification
- 🟩 Escape to Host
- 🟩 Event Triggered Execution
- 🟩 Exploitation for Privilege Escalation
- 🟩 Hijack Execution Flow
- 🟩 Process Injection
- 🟩 Scheduled Task/Job
- 🟩 Valid Accounts

Defense Evasion
- 🟩 Abuse Elevation Control Mechanism
- 🟩 Access Token Manipulation
- 🟩 BITS Jobs
- 🟩 Build Image on Host
- ⬜ Debugger Evasion
- ⬜ Deobfuscate/Decode Files or Information
- 🟩 Deploy Container
- ⬜ Direct Volume Access
- 🟩 Domain Policy Modification
- ⬜ Execution Guardrails
- 🟩 Exploitation for Defense Evasion
- 🟩 File and Directory Permissions Modification
- ⬜ Hide Artifacts
- 🟩 Hijack Execution Flow
- 🟩 Impair Defenses
- 🟩 Indicator Removal on Host
- ⬜ Indirect Command Execution
- 🟩 Masquerading
- 🟩 Modify Authentication Process
- 🟩 Modify Cloud Compute Infrastructure
- 🟩 Modify Registry
- 🟩 Modify System Image
- 🟩 Network Boundary Bridging
- 🟩 Obfuscated Files or Information
- ⬜ Plist File Modification
- 🟩 Pre-OS Boot
- 🟩 Process Injection
- ⬜ Reflective Code Loading
- ⬜ Rogue Domain Controller
- ⬜ Rootkit
- 🟩 Subvert Trust Controls
- 🟩 System Binary Proxy Execution
- 🟩 System Script Proxy Execution
- 🟩 Template Injection
- 🟩 Traffic Signaling
- 🟩 Trusted Developer Utilities Proxy Execution
- 🟩 Unused/Unsupported Cloud Regions
- 🟩 Use Alternate Authentication Material
- 🟩 Valid Accounts
- ⬜ Virtualization/Sandbox Evasion
- ⬜ Weaken Encryption
- 🟩 XSL Script Processing

Credential Access
- 🟩 Adversary-in-the-Middle
- 🟩 Brute Force
- 🟩 Credentials from Password Stores
- 🟩 Exploitation for Credential Access
- 🟩 Forced Authentication
- 🟩 Forge Web Credentials
- ⬜ Input Capture
- 🟩 Modify Authentication Process
- 🟩 Multi-Factor Authentication Interception
- ⬜ Multi-Factor Authentication Request Generation
- 🟩 Network Sniffing
- 🟩 OS Credential Dumping
- 🟩 Steal Application Access Token
- 🟩 Steal or Forge Kerberos Tickets
- 🟩 Steal Web Session Cookie
- 🟩 Unsecured Credentials

Discovery
- 🟩 Account Discovery
- ⬜ Application Window Discovery
- ⬜ Browser Bookmark Discovery
- 🟩 Cloud Infrastructure Discovery
- 🟩 Cloud Service Dashboard
- ⬜ Cloud Service Discovery
- 🟩 Cloud Storage Object Discovery
- 🟩 Container and Resource Discovery
- ⬜ Debugger Evasion
- 🟩 Domain Trust Discovery
- ⬜ File and Directory Discovery
- ⬜ Group Policy Discovery
- 🟩 Network Service Discovery
- 🟩 Network Share Discovery
- 🟩 Network Sniffing
- 🟩 Password Policy Discovery
- ⬜ Peripheral Device Discovery
- ⬜ Permission Groups Discovery
- ⬜ Process Discovery
- ⬜ Query Registry
- ⬜ Remote System Discovery
- ⬜ Software Discovery
- ⬜ System Information Discovery
- ⬜ System Location Discovery
- ⬜ System Network Configuration Discovery
- ⬜ System Network Connections Discovery
- ⬜ System Owner/User Discovery
- ⬜ System Service Discovery
- ⬜ System Time Discovery
- ⬜ Virtualization/Sandbox Evasion

Lateral Movement
- 🟩 Exploitation of Remote Services
- ⬜ Internal Spearphishing
- 🟩 Lateral Tool Transfer
- 🟩 Remote Service Session Hijacking
- 🟩 Remote Services
- 🟩 Replication Through Removable Media
- 🟩 Software Deployment Tools
- 🟩 Taint Shared Content
- 🟩 Use Alternate Authentication Material

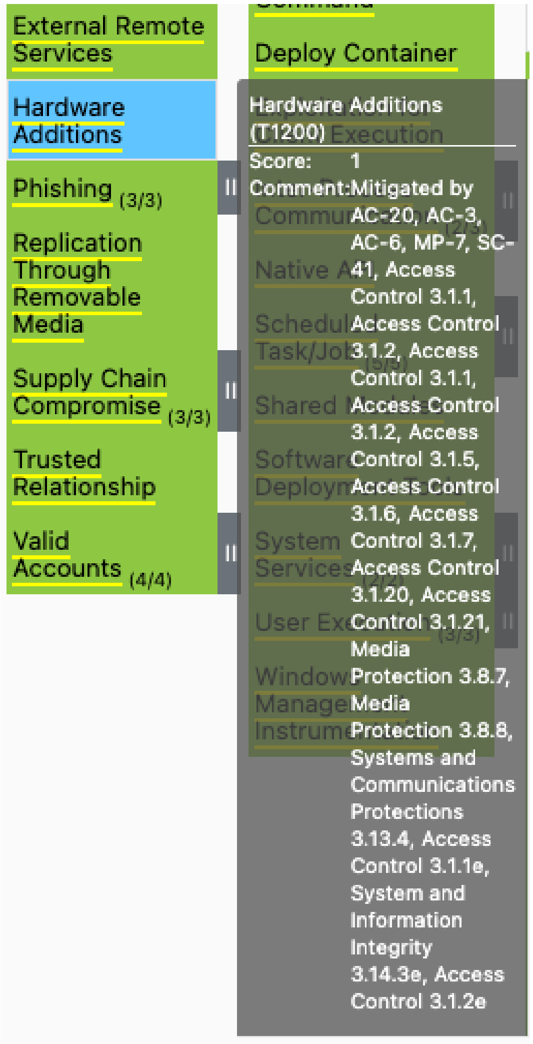
Collection
- 🟩 Adversary-in-the-Middle
- 🟩 Archive Collected Data
- ⬜ Audio Capture
- 🟩 Automated Collection
- 🟩 Browser Session Hijacking
- ⬜ Clipboard Data
- 🟩 Data from Cloud Storage Object
- 🟩 Data from Configuration Repository
- 🟩 Data from Information Repositories
- 🟩 Data from Local System
- ⬜ Data from Network Shared Drive
- 🟩 Data from Removable Media
- ⬜ Data Staged
- 🟩 Email Collection
- ⬜ Input Capture
- ⬜ Screen Capture
- ⬜ Video Capture

Command and Control
- 🟩 Application Layer Protocol
- 🟩 Communication Through Removable Media
- 🟩 Data Encoding
- 🟩 Data Obfuscation
- 🟩 Dynamic Resolution
- 🟩 Encrypted Channel
- 🟩 Fallback Channels
- 🟩 Ingress Tool Transfer
- 🟩 Multi-Stage Channels
- 🟩 Non-Application Layer Protocol
- 🟩 Non-Standard Port
- 🟩 Protocol Tunneling
- 🟩 Proxy
- 🟩 Remote Access Software
- 🟩 Traffic Signaling
- 🟩 Web Service

Exfiltration
- ⬜ Automated Exfiltration
- 🟩 Data Transfer Size Limits
- 🟩 Exfiltration Over Alternative Protocol
- 🟩 Exfiltration Over C2 Channel
- 🟩 Exfiltration Over Other Network Medium
- 🟩 Exfiltration Over Physical Medium
- 🟩 Exfiltration Over Web Service
- 🟩 Scheduled Transfer
- 🟩 Transfer Data to Cloud Account

Impact
- ⬜ Account Access Removal
- 🟩 Data Destruction
- 🟩 Data Encrypted for Impact
- 🟩 Data Manipulation
- 🟩 Defacement
- 🟩 Disk Wipe
- 🟩 Endpoint Denial of Service
- 🟩 Firmware Corruption
- 🟩 Inhibit System Recovery
- 🟩 Network Denial of Service
- ⬜ Resource Hijacking
- 🟩 Service Stop
- ⬜ System Shutdown/Reboot

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



Hardware Additions (T1200)

Score: 1

Comment: Mitigated by AC-20, AC-3, AC-6, MP-7, SC-41, Access Control 3.1.1, Access Control 3.1.2, Access Control 3.1.1, Access Control 3.1.2, Access Control 3.1.5, Access Control 3.1.6, Access Control 3.1.7, Access Control 3.1.20, Access Control 3.1.21, Media Protection 3.8.7, Media Protection 3.8.8, Systems and Communications Protections 3.13.4, Access Control 3.1.1e, System and Information Integrity 3.14.3e, Access Control 3.1.2e

**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.

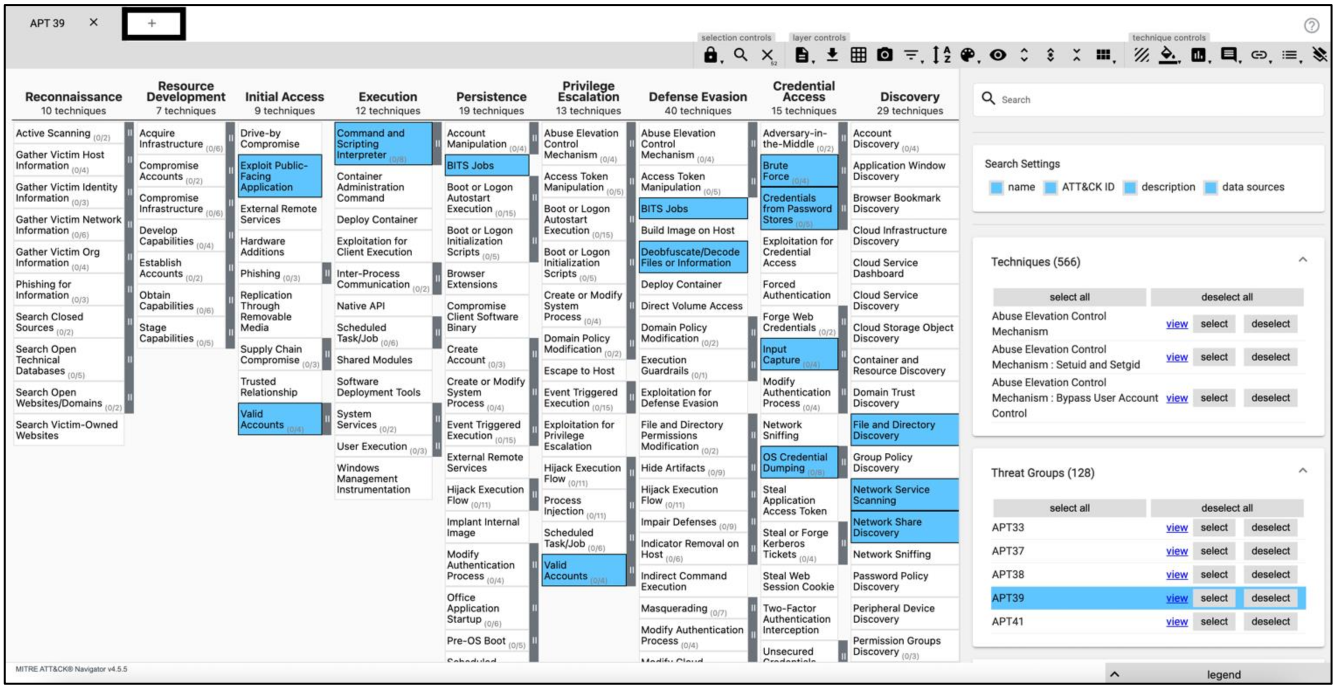
7. Identify ATT&CK TTPs used by the chosen APT on the MITRE ATT&CK website.
8. Open the mapping matrix created by this project.
9. Filter the ATT&CK TTP column, selecting all the ATT&CK TTPs identified in step 1.
10. Record the number of unique controls in the CONTROL ID column in the filtered list*; 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.



| Reconnaissance<br>10 techniques | Resource Development<br>7 techniques | Initial Access<br>9 techniques | Execution<br>12 techniques | Persistence<br>19 techniques | Privilege Escalation<br>13 techniques | Defense Evasion<br>40 techniques | Credential Access<br>15 techniques | Discovery<br>29 techniques |
|---|---|---|---|---|---|---|---|---|
| Active Scanning (0/2) | Acquire Infrastructure (0/6) | Drive-by Compromise | Command and Scripting Interpreter (0/8) | Account Manipulation (0/4) | Abuse Elevation Control Mechanism (0/4) | Abuse Elevation Control Mechanism (0/4) | Adversary-in-the-Middle (0/2) | Account Discovery (0/4) |
| Gather Victim Host Information (0/4) | Compromise Accounts (0/2) | Exploit Public-Facing Application | Container Administration Command | BITS Jobs | Access Token Manipulation (0/5) | Access Token Manipulation (0/5) | Brute Force (0/4) | Application Window Discovery |
| Gather Victim Identity Information (0/3) | Compromise Infrastructure (0/6) | External Remote Services | Deploy Container | Boot or Logon Autostart Execution (0/15) | Boot or Logon Autostart Execution (0/15) | BITS Jobs | Credentials from Password Stores (0/5) | Browser Bookmark Discovery |
| Gather Victim Network Information (0/6) | Develop Capabilities (0/4) | Hardware Additions | Exploitation for Client Execution | Boot or Logon Initialization Scripts (0/5) | Boot or Logon Initialization Scripts (0/5) | Build Image on Host | Exploitation for Credential Access | Cloud Infrastructure Discovery |
| Gather Victim Org Information (0/4) | Establish Accounts (0/2) | Phishing (0/3) | Inter-Process Communication (0/2) | Browser Extensions | Create or Modify System Process (0/4) | Deobfuscate/Decode Files or Information | Forced Authentication | Cloud Service Dashboard |
| Phishing for Information (0/3) | Obtain Capabilities (0/6) | Replication Through Removable Media | Native API | Compromise Client Software Binary | Domain Policy Modification (0/2) | Deploy Container | Forge Web Credentials (0/2) | Cloud Service Discovery |
| Search Closed Sources (0/2) | Stage Capabilities (0/5) | Supply Chain Compromise (0/3) | Scheduled Task/Job (0/6) | Create Account (0/3) | Escape to Host | Direct Volume Access | Input Capture (0/4) | Cloud Storage Object Discovery |
| Search Open Technical Databases (0/5) | | Trusted Relationship | Shared Modules | Create or Modify System Process (0/4) | Event Triggered Execution (0/15) | Domain Policy Modification (0/2) | Modify Authentication Process (0/4) | Container and Resource Discovery |
| Search Open Websites/Domains (0/2) | | Valid Accounts (0/4) | Software Deployment Tools | Event Triggered Execution (0/15) | Exploitation for Privilege Escalation | Execution Guardrails (0/1) | Network Sniffing | Domain Trust Discovery |
| Search Victim-Owned Websites | | | System Services (0/2) | External Remote Services | Hijack Execution Flow (0/11) | Exploitation for Defense Evasion | OS Credential Dumping (0/8) | File and Directory Discovery |
| | | | User Execution (0/3) | Hijack Execution Flow (0/11) | Process Injection (0/11) | File and Directory Permissions Modification (0/2) | Steal Application Access Token | Group Policy Discovery |
| | | | Windows Management Instrumentation | Implant Internal Image | Scheduled Task/Job (0/6) | Hide Artifacts (0/9) | Steal or Forge Kerberos Tickets (0/4) | Network Service Scanning |
| | | | | Modify Authentication Process (0/4) | Valid Accounts (0/4) | Hijack Execution Flow (0/11) | Steal Web Session Cookie | Network Share Discovery |
| | | | | Office Application Startup (0/6) | | Impair Defenses (0/9) | Two-Factor Authentication Interception | Network Sniffing |
| | | | | Pre-OS Boot (0/5) | | Indicator Removal on Host (0/6) | Unsecured | Password Policy Discovery |
| | | | | Scheduled | | Indirect Command Execution | | Peripheral Device Discovery |
| | | | | | | Masquerading (0/7) | | Permission Groups Discovery (0/3) |
| | | | | | | Modify Authentication Process (0/4) | | |
| | | | | | | Modify Cloud | | |

Search Settings

■ name ■ ATT&CK ID ■ description ■ data sources

Techniques (566)

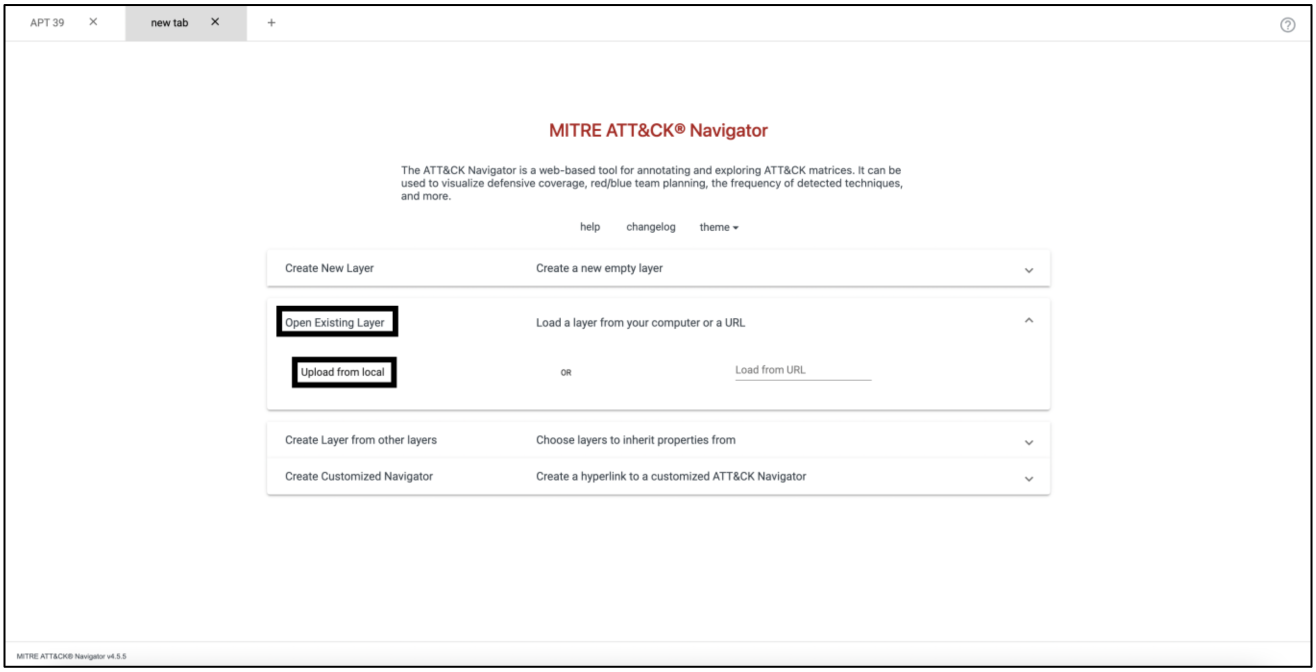
| select all | deselect all | | |
|---|---|---|---|
| Abuse Elevation Control Mechanism | view | select | deselect |
| Abuse Elevation Control Mechanism : Setuid and Setgid | view | select | deselect |
| Abuse Elevation Control Mechanism : Bypass User Account Control | view | select | deselect |

Threat Groups (128)

| select all | deselect all | | |
|---|---|---|---|
| APT33 | view | select | deselect |
| APT37 | view | select | deselect |
| APT38 | view | select | deselect |
| APT39 | view | select | deselect |
| APT41 | view | select | deselect |

**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.



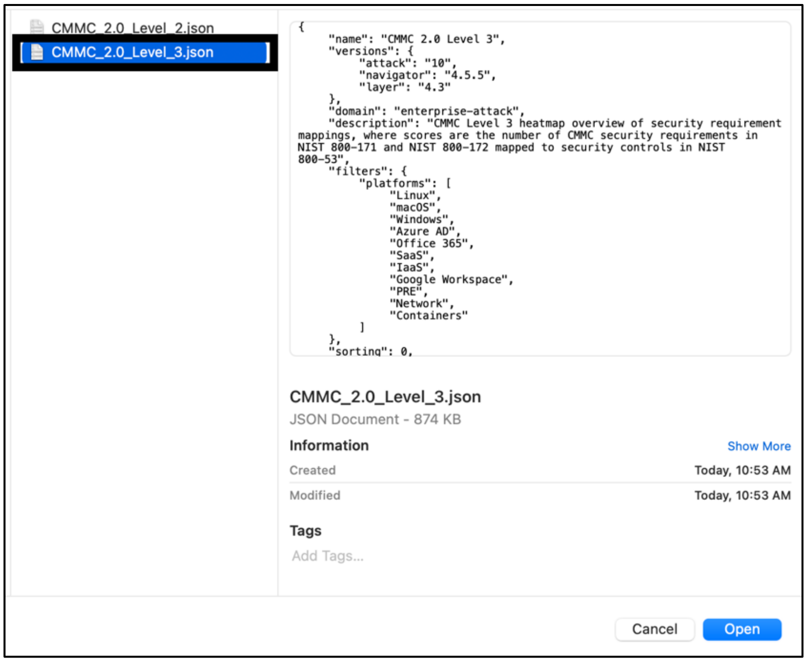
MITRE ATT&CK® Navigator

The ATT&CK Navigator is a web-based tool for annotating and exploring ATT&CK matrices. It can be used to visualize defensive coverage, red/blue team planning, the frequency of detected techniques, and more.

| | |
|---|---|
| Create New Layer | Create a new empty layer |
| Open Existing Layer | Load a layer from your computer or a URL |
| Upload from local | OR Load from URL |
| Create Layer from other layers | Choose layers to inherit properties from |
| Create Customized Navigator | Create a hyperlink to a customized ATT&CK Navigator |

**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.



```
{
     "name": "CMMC 2.0 Level 3",
     "versions": {
          "attack": "10",
          "navigator": "4.5.5",
          "layer": "4.3"
     },
     "domain": "enterprise-attack",
     "description": "CMMC Level 3 heatmap overview of security requirement
mappings, where scores are the number of CMMC security requirements in
NIST 800-171 and NIST 800-172 mapped to security controls in NIST
800-53",
     "filters": {
          "platforms": [
               "Linux",
               "macOS",
               "Windows",
               "Azure AD",
               "Office 365",
               "SaaS",
               "IaaS",
               "Google Workspace",
               "PRE",
               "Network",
               "Containers"
          ]
     },
     "sorting": 0,
```

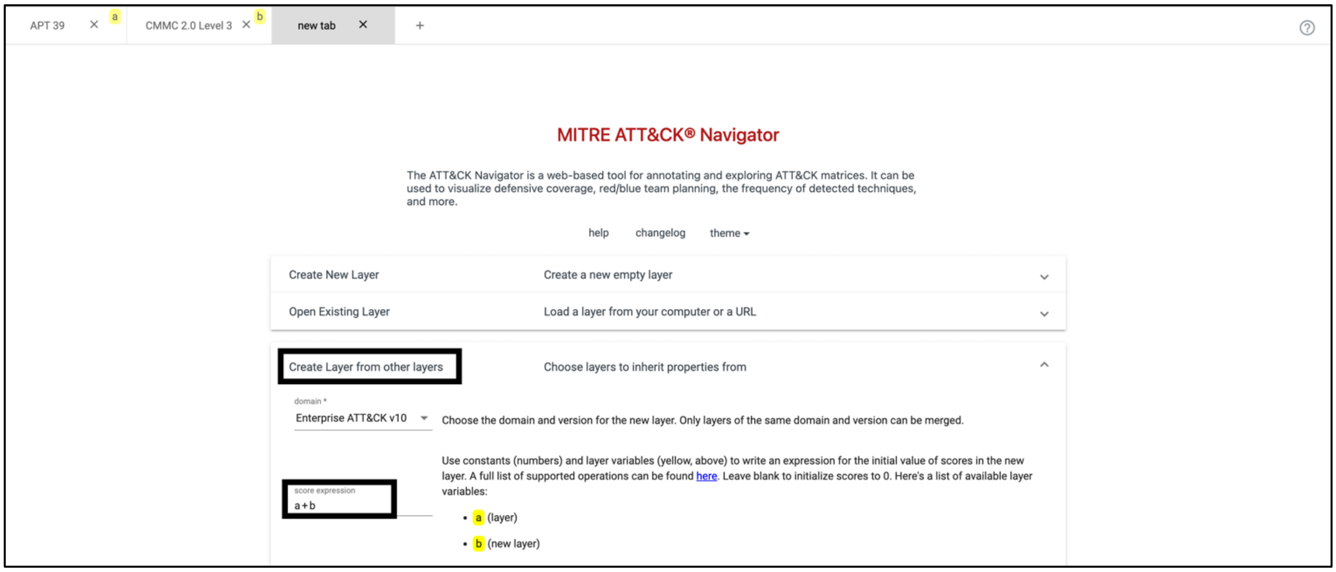
CMMC_2.0_Level_3.json
JSON Document - 874 KB

Information

| | |
|---|---|
| Created | Today, 10:53 AM |
| Modified | Today, 10:53 AM |

**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.



The ATT&CK Navigator is a web-based tool for annotating and exploring ATT&CK matrices. It can be used to visualize defensive coverage, red/blue team planning, the frequency of detected techniques, and more.

Create New Layer — Create a new empty layer

Open Existing Layer — Load a layer from your computer or a URL

Create Layer from other layers — Choose layers to inherit properties from

domain *: Enterprise ATT&CK v10

Choose the domain and version for the new layer. Only layers of the same domain and version can be merged.

score expression: a+b

Use constants (numbers) and layer variables (yellow, above) to write an expression for the initial value of scores in the new layer. A full list of supported operations can be found here. Leave blank to initialize scores to 0. Here's a list of available layer variables:

- a (layer)
- b (new layer)

**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 Enginuity
- 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 |