

Compliance vs Security

*Exploring the Real-World Security Value of
CMMC*

Jacob Horne, Summit 7

April 4th, 2024



Agenda

- Understand NIST SP 800-53
- Understand Advanced Persistent Threats (APTs)
- Understand NIST SP 800-171 Tailoring
- Understand the MITRE ATT&CK Framework
- Map NIST SP 800-53 to MITRE ATT&CK
- Key Takeaways for industry, NIST, and DoD



Understanding NIST SP 800-53



NIST SP 800-53 is a catalog of controls is designed to be used in a larger risk management context (“RMF”)

NIST Special Publication 800-53
Revision 4

Security and Privacy Controls for Federal Information Systems and Organizations

JOINT TASK FORCE
TRANSFORMATION INITIATIVE

This publication is available free of charge from:
<http://dx.doi.org/10.6028/NIST.SP.800-53r4>

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

“The purpose of this publication is to provide guidelines for selecting and specifying security to meet the requirements of FIPS Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*.”

“The catalog of security controls can be effectively used to:

- Protect information and information systems from **traditional and advanced persistent threats** in varied operational, environmental, and technical scenarios
- Demonstrate compliance with a variety of governmental, organizational, or institutional security requirements”



NIST controls come in two forms: “base controls” which can be supplemented by “control enhancements”

“Base Control”

SI-4 INFORMATION SYSTEM MONITORING

Control: The organization:

- a. Monitors the information system to detect:
 1. Attacks and indicators of potential attacks in accordance with [*Assignment: organization-defined monitoring objectives*]; and
 2. Unauthorized local, network, and remote connections;
- b. Identifies unauthorized use of the information system through [*Assignment: organization-defined techniques and methods*];
- c. Deploys monitoring devices:
 1. Strategically within the information system to collect organization-determined essential information; and
 2. At ad hoc locations within the system to track specific types of transactions of interest to the organization;
- d. Protects information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion;
- e. Heightens the level of information system monitoring activity whenever there is an indication of increased risk to organizational operations and assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information;
- f. Obtains legal opinion with regard to information system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations; and
- g. Provides [*Assignment: organization-defined information system monitoring information*] to [*Assignment: organization-defined personnel or roles*] [*Selection (one or more): as needed; [Assignment: organization-defined frequency]*].

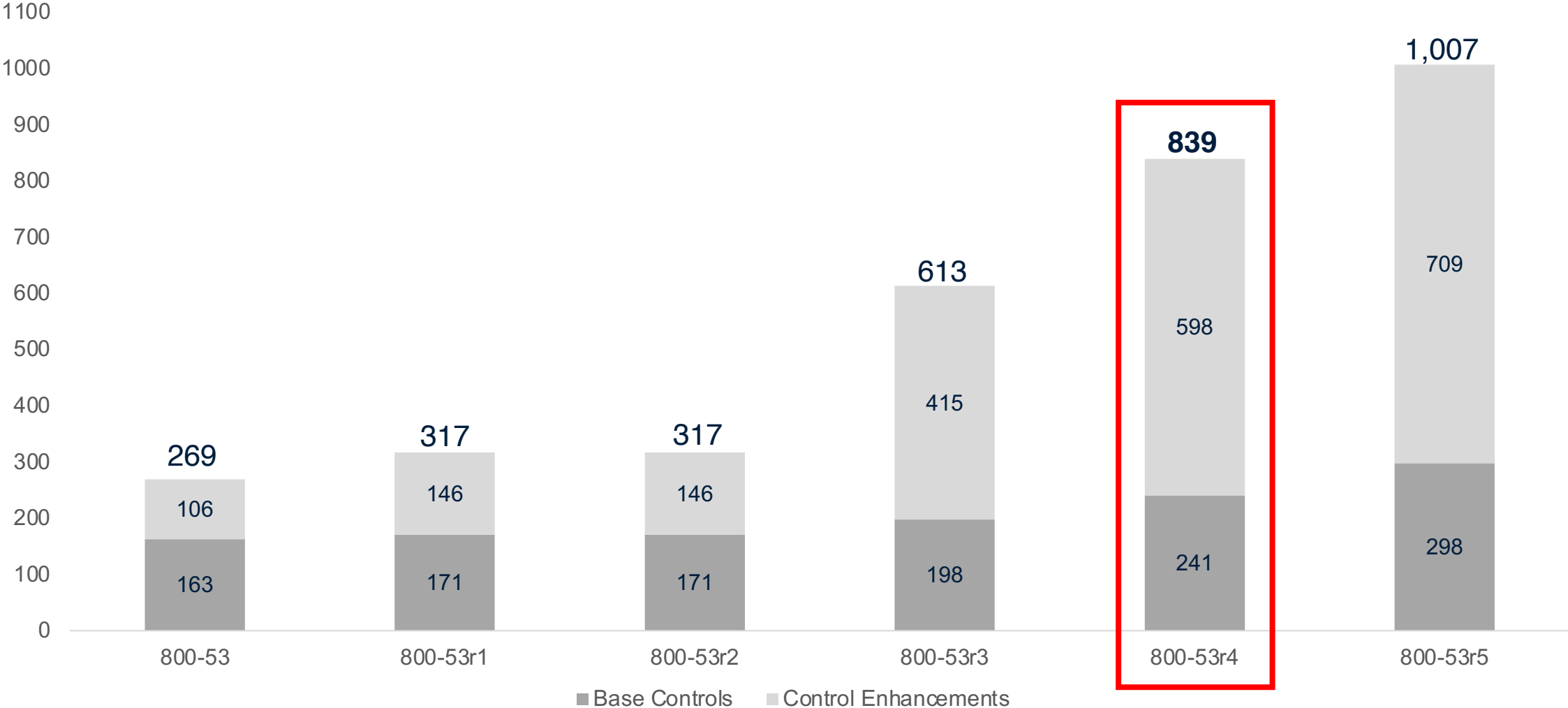
“Control Enhancement”

- (4) *INFORMATION SYSTEM MONITORING | INBOUND AND OUTBOUND COMMUNICATIONS TRAFFIC*
The information system monitors inbound and outbound communications traffic [*Assignment: organization-defined frequency*] for unusual or unauthorized activities or conditions.



Think of SP 800-53 like a dictionary or a toolbox that you select from; the size of the dictionary has grown over the last 20 years

of Controls in NIST SP 800-53 Over Time



800-53 is divided into low, moderate, and high “baselines” that act as starting points for “tailoring” controls to an organizational system

NIST Special Publication 800-53
Revision 4

Security and Privacy Controls for Federal Information Systems and Organizations

JOINT TASK FORCE
TRANSFORMATION INITIATIVE

This publication is available free of charge from:
<http://dx.doi.org/10.6028/NIST.SP.800-53r4>

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

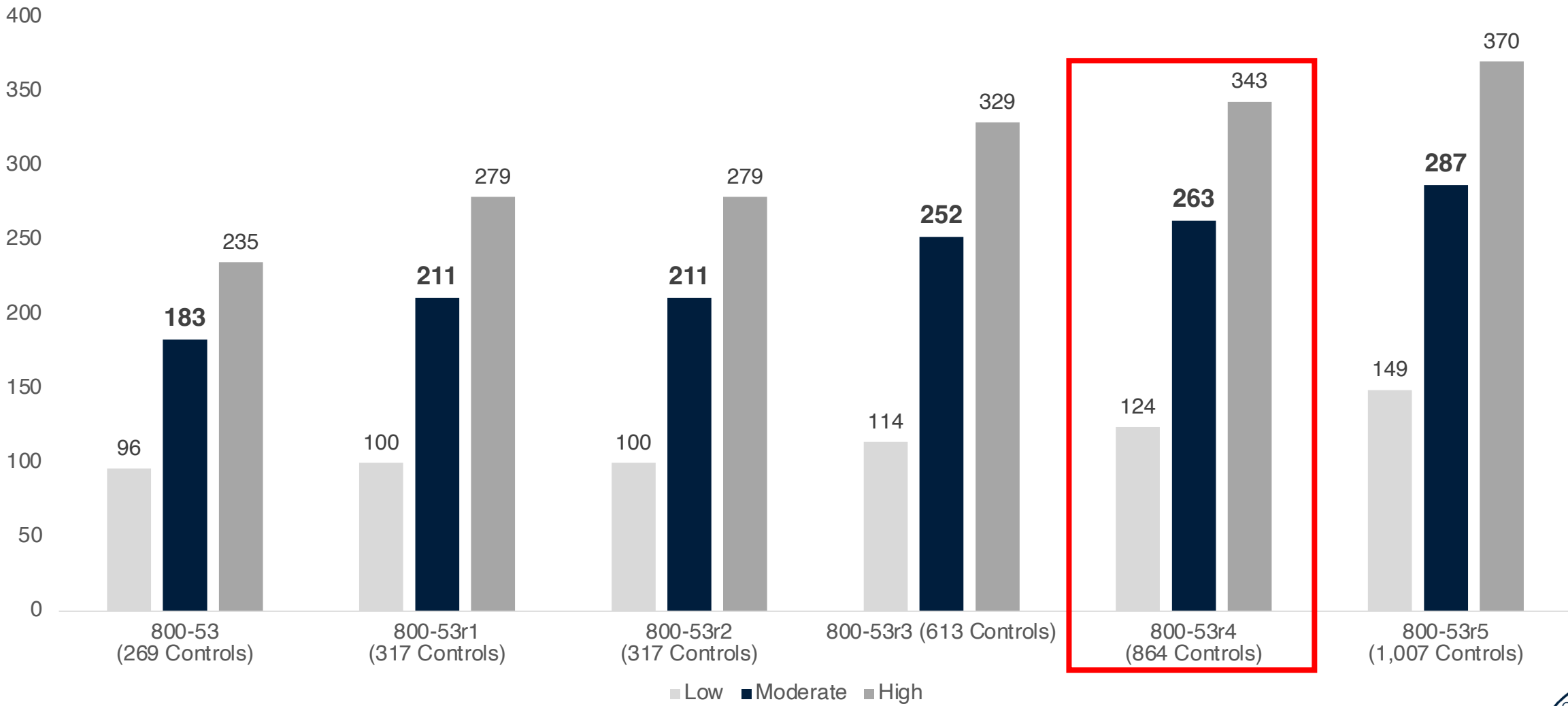
“The first step in selecting and specifying security controls for the information system is to choose the appropriate security control baseline.

The security controls and enhancements in the baselines **are a starting point** from which controls/enhancements may be removed, added, or specialized based on the tailoring guidance.”



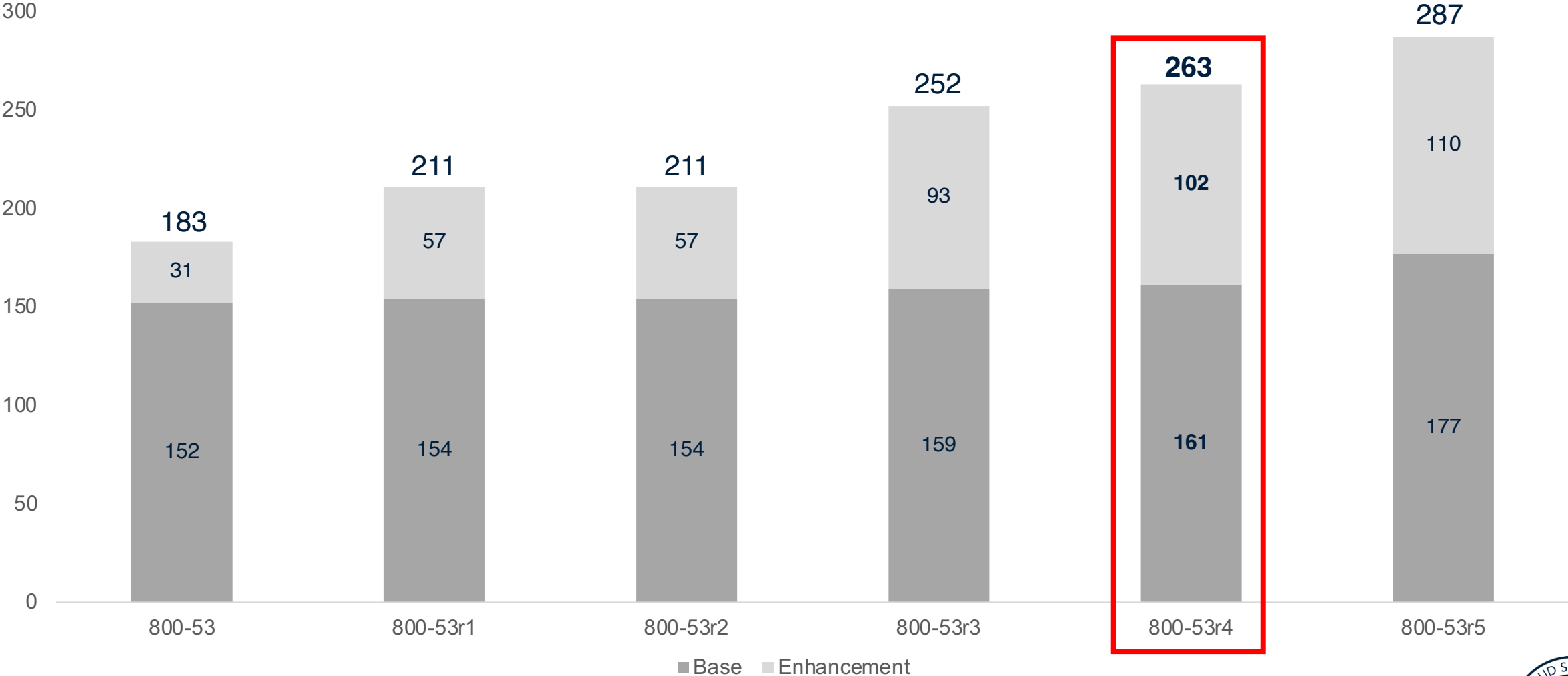
Since revision 3 the majority of controls in NIST SP 800-53 are not assigned to any baseline

Low, Moderate, & High Baselines Over Time



Over time the revisions have increased the number of control enhancements in the various baselines

NIST SP 800-53 Moderate Baseline Size Over Time

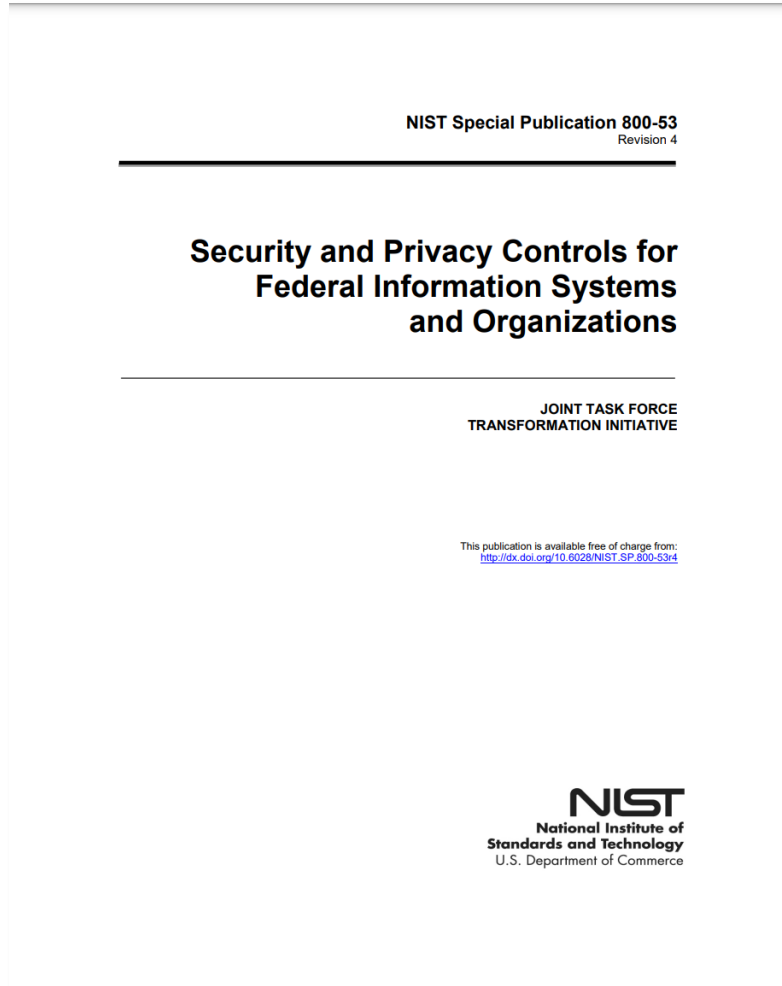


The SP 800-53r4 moderate baseline represents just 31% of the entire SP 800-53r4 catalog of controls and enhancements

Family	AC	AT	AU	CA	CM	CP	IA	IR	MA	MP	PE	PL	PS	RA	SA	SC	SI
C o n t r o l s	AC-1	AT-1	AU-1	CA-1	CM-1	CP-1	IA-1	IR-1	MA-1	MP-1	PE-1	PL-1	PS-1	RA-1	SA-1	SC-1	SI-1
	AC-2	AT-2	AU-2	CA-2	CM-2	CP-2	IA-2	IR-2	MA-2	MP-2	PE-2	PL-2	PS-2	RA-2	SA-2	SC-2	SI-2
	AC-2(1)	AT-2(2)	AU-2(3)	CA-2(1)	CM-2(1)	CP-2(1)	IA-2(1)	IR-3	MA-3	MP-3	PE-3	PL-2(3)	PS-3	RA-3	SA-3	SC-4	SI-2(2)
	AC-2(2)	AT-3	AU-3	CA-3	CM-2(3)	CP-2(3)	IA-2(2)	IR-3(2)	MA-3(1)	MP-4	PE-4	PL-4	PS-4	RA-5	SA-4	SC-5	SI-3
	AC-2(3)	AT-4	AU-3(1)	CA-3(5)	CM-2(7)	CP-2(8)	IA-2(3)	IR-4	MA-3(2)	MP-5	PE-5	PL-4(1)	PS-5	RA-5(1)	SA-4(1)	SC-7	SI-3(1)
	AC-2(4)		AU-4	CA-5	CM-3	CP-3	IA-2(8)	IR-4(1)	MA-4	MP-5(4)	PE-6	PL-8	PS-6	RA-5(2)	SA-4(2)	SC-7(3)	SI-3(2)
	AC-3		AU-5	CA-6	CM-3(2)	CP-4	IA-2(9)	IR-5	MA-4(2)	MP-6	PE-6(1)		PS-7	RA-5(5)	SA-4(9)	SC-7(4)	SI-4
	AC-4		AU-6	CA-7	CM-4	CP-4(1)	IA-2(11)	IR-6	MA-5	MP-7	PE-8		PS-8		SA-4(10)	SC-7(5)	SI-4(2)
	AC-5		AU-6(1)	CA-7(1)	CM-5	CP-6	IA-2(12)	IR-6(1)	MA-6	MP-7(1)	PE-9				SA-5	SC-7(7)	SI-4(4)
	AC-6		AU-6(3)	CA-9	CM-6	CP-6(1)	IA-3	IR-7			PE-10				SA-8	SC-8	SI-4(5)
	AC-6(1)		AU-7		CM-7	CP-6(3)	IA-4	IR-7(1)			PE-11				SA-9	SC-8(1)	SI-5
	AC-6(2)		AU-7(1)		CM-7(1)	CP-7	IA-5	IR-8			PE-12				SA-9(2)	SC-10	SI-7
	AC-6(5)		AU-8		CM-7(2)	CP-7(1)	IA-5(1)				PE-13				SA-10	SC-12	SI-7(1)
	AC-6(9)		AU-8(1)		CM-7(4)*	CP-7(2)	IA-5(2)				PE-13(3)				SA-11	SC-13	SI-7(7)
	AC-6(10)		AU-9		CM-7(5)*	CP-7(3)	IA-5(3)				PE-14					SC-15	SI-8
	AC-7		AU-9(4)		CM-8	CP-8	IA-5(11)				PE-15					SC-17	SI-8(1)
	AC-8		AU-11		CM-8(1)	CP-8(1)	IA-6				PE-16					SC-18	SI-8(2)
	AC-11		AU-12		CM-8(3)	CP-8(2)	IA-7				PE-17					SC-19	SI-10
	AC-11(1)				CM-8(5)	CP-9	IA-8									SC-20	SI-11
	AC-12				CM-9	CP-9(1)	IA-8(1)									SC-21	SI-12
	AC-14				CM-10	CP-10	IA-8(2)									SC-22	SI-16
	AC-17				CM-11	CP-10(2)	IA-8(3)									SC-23	
	AC-17(1)						IA-8(4)									SC-28	
	AC-17(2)															SC-39	
	AC-17(3)																
	AC-17(4)																
	AC-18																
	AC-18(1)																
	AC-19																
	AC-19(5)																
	AC-20																
	AC-20(1)																
	AC-20(2)																
	AC-21																
	AC-22																
Count	35	5	18	10	22	22	23	12	9	9	18	6	8	7	14	24	21



The baselines are intended to be well-rounded, general purpose starting points; baselines have limits and may need to be supplemented based on specific threats or system/organizational requirements



There are also some possible situations that are specifically not addressed in the baselines:

- Insider threats exist within organizations
- Classified data/information is processed, stored, or transmitted by information systems
- **Advanced persistent threats (APTs) exist within organizations**
- Selected data/information requires specialized protection based on federal legislation, directives, regulations, or policies
- Information systems need to communicate with other systems across different security domains

“If any of the above assumptions apply, then **additional security controls would likely be needed** to ensure adequate protection”



The baselines are intended to be well-rounded, general purpose starting points; baselines have limits and may need to be supplemented based on specific threats or system/organizational requirements

NIST Special Publication 800-53
Revision 4

**Security and Privacy Controls for
Federal Information Systems
and Organizations**

JOINT TASK FORCE
TRANSFORMATION INITIATIVE

This publication is available free of charge from:
<http://dx.doi.org/10.6028/NIST.SP.800-53r4>

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

Situations requiring potential baseline supplementation

Advanced Persistent Threat

Security control baselines do not assume that the current threat environment is one where adversaries have achieved a significant foothold and presence within organizations and organizational information systems—that is, organizations are dealing with an **advanced persistent threat (APT)**.



Understanding Advanced Persistent Threats (APTs)



Advanced Persistent Threats are much more than just access to “zero-day” exploits

“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 (e.g., cyber, physical, and deception). These objectives typically include establishing and extending footholds within the information technology 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.” – NIST Glossary



Pursues its objectives repeatedly over an extended period of time



Adapts to defenders' efforts to resist it



Is determined to maintain the level of interaction needed to execute its objectives



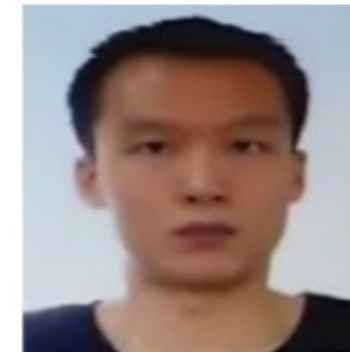
Advanced Persistent Threats are much more than just access to “zero-day” exploits

APT 31



The screenshot shows the top portion of a press release page. At the top left is the Department of Justice seal and the text "Office of Public Affairs, U.S. Department of Justice". To the right are links for "Our Offices", "Find Help", and "Contact Us", along with a search bar. Below this is a navigation menu with items: "About", "News", "Documents", "Internships", "FOIA", "Contact", and "Information for Journalists". The main content area features a breadcrumb trail: "Justice.gov > Office of Public Affairs > News > Press Releases > Seven Hackers Associated With Chinese Government Charged With Computer Intrusions Targeting Perceived Critics of China and U.S. Businesses and Politicians". On the left is a "News" sidebar with links for "All News", "Blogs", "Photo Galleries", "Podcasts", and "Press Releases" (which is highlighted). The main headline reads "Seven Hackers Associated with Chinese Government Charged with Computer Intrusions Targeting Perceived Critics of China and U.S. Businesses and Politicians". Below the headline, it says "Monday, March 25, 2024" and "For Immediate Release".

<https://www.justice.gov/opa/pr/seven-hackers-associated-chinese-government-charged-computer-intrusions-targeting-perceived>



Advanced Persistent Threats are much more than just access to “zero-day” exploits



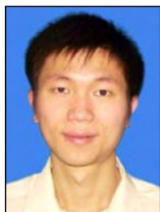
FBI FEDERAL BUREAU OF INVESTIGATION



WANTED BY THE FBI

APT 40 CYBER ESPIONAGE ACTIVITIES

Conspiracy to Damage Protected Computers and Commit Economic Espionage; Criminal Forfeiture



Zhu Yunmin



Wu Shurong



Ding Xiaoyang



Cheng Qingmin

CAUTION

On May 28, 2021, a federal grand jury in the United States District Court for the Southern District of California returned an indictment against four People's Republic of China (PRC) citizens for their alleged roles in a long running campaign of computer network operations targeting trade secrets, intellectual property, and other high value information from companies, universities, research institutes, and governmental entities in the United States and abroad, as well as multiple foreign governments. The indictment alleges that Zhu Yunmin, Wu Shurong, Ding Xiaoyang, and Cheng Qingmin targeted the following sectors: aerospace/aviation, biomedical, defense industrial base, healthcare, manufacturing, maritime, research institutes, transportation (rail and shipping), and virus research from 2012 to 2018, on behalf of the PRC Ministry of State Security. Additionally, the indictment alleges the use of front companies by the PRC Ministry of State Security to conduct cyber espionage.

The four individuals are identified as:

ZHU Yunmin 朱允敏 (STC Codes: 2612/0336/2404) Alias: Zhu Rong

WU Shurong 吴淑荣 (STC Codes: 0702/3219/2837) Aliases: goodperson, ha0r3n, Shi Lei

DING Xiaoyang 丁晓阳 (STC Codes: 0002/2556/7122) Aliases: Ding Hao, Manager Chen

CHENG Qingmin 程庆民 (STC Codes: 4453/1987/3046) Alias: Manager Cheng

If you have any information concerning these individuals, please contact your local FBI office, or the nearest American Embassy or Consulate.

Field Office: San Diego

www.fbi.gov



WANTED BY THE FBI

APT 41 GROUP



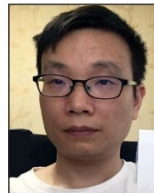
ZHANG Haoran



TAN Dailin



QIAN Chuan



FU Qiang



JIANG Lizhi

CAUTION

ZHANG Haoran, TAN Dailin, QIAN Chuan, FU Qiang, and JIANG Lizhi are all part of a Chinese hacking group known as APT 41 and BARIUM.

On August 15, 2019, a Grand Jury in the District of Columbia returned an indictment against Chinese nationals ZHANG Haoran and TAN Dailin on charges including Unauthorized Access to Protected Computers, Aggravated Identity Theft, Money Laundering, and Wire Fraud. These charges primarily stemmed from alleged activity targeting high technology and video gaming companies, and a United Kingdom citizen.

On August 11, 2020, a Grand Jury in the District of Columbia returned an indictment against Chinese nationals QIAN Chuan, FU Qiang, and JIANG Lizhi on charges including Racketeering, Money Laundering, Fraud, Identity Theft, and Access Device Fraud. These charges stem from their alleged unauthorized computer intrusions while employed by Chengdu 404 Network Technology Company. The defendants allegedly conducted supply chain attacks to gain unauthorized access to networks throughout the world, targeting hundreds of companies representing a broad array of industries to include: social media, telecommunications, government, defense, education, and manufacturing. These victims included companies in Australia, Brazil, Germany, India, Japan and Sweden. The defendants allegedly targeted telecommunications providers in the United States, Australia, China (Tibet), Chile, India, Indonesia, Malaysia, Pakistan, Singapore, South Korea, Taiwan, and Thailand. The defendants allegedly deployed ransomware attacks and demanded payments from victims.

If you have any information concerning these individuals, please contact your local FBI office, or the nearest American Embassy or Consulate.

Field Office: Washington D.C.

www.fbi.gov



WANTED BY THE FBI

IRGC CYBER ACTORS

Conspiracy to Commit Computer Intrusions; Obtaining Information by Unauthorized Access to Protected Computers; Intentional Damage to Protected Computers; Aggravated Identity Theft; Conspiracy to Commit Wire Fraud



Said Pourkarim Arabi



Mohammad Reza Espargham



Mohammad Bayati

CAUTION

Said Pourkarim Arabi, Mohammad Reza Espargham, and Mohammad Bayati are wanted for their alleged involvement in criminal activities including computer intrusions, identity theft, and wire fraud. These Iranian hackers allegedly conspired to commit computer intrusions targeting American companies in the aerospace and satellite industries. They allegedly engaged in a coordinated campaign of social engineering that resulted in the theft of United States citizens' identities, which they then used to steal critical information related to American aerospace and satellite technology and resources, including sensitive commercial information, intellectual property, and personal data. The men allegedly conducted this activity at the direction of Iran's Islamic Revolutionary Guard Corps (IRGC). On September 15, 2020, a federal grand jury in the United States District Court for the Eastern District of Virginia, in Alexandria, Virginia, indicted the men on charges of Conspiracy to Commit Computer Intrusions, Obtaining Information by Unauthorized Access to Protected Computers, Intentional Damage to Protected Computers, Aggravated Identity Theft, and Conspiracy to Commit Wire Fraud, and federal arrest warrants were issued.

If you have any information concerning these individuals, please contact your local FBI office, or the nearest American Embassy or Consulate.

Field Office: Washington D.C.

www.fbi.gov

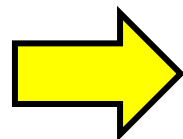
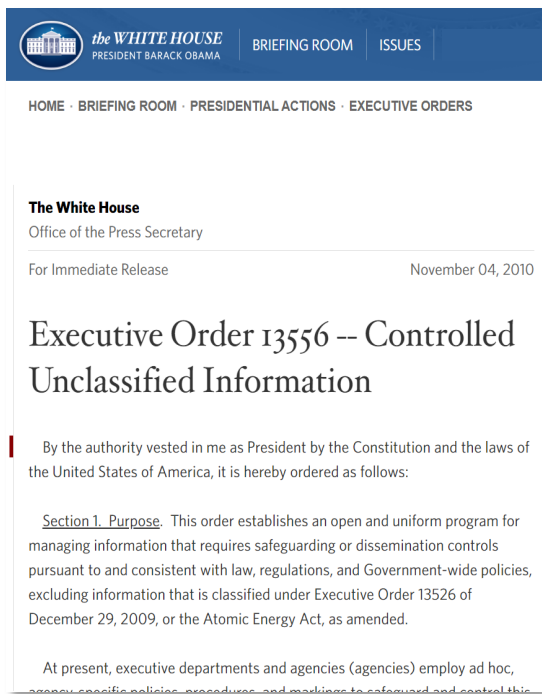


Understanding SP 800-171 Tailoring

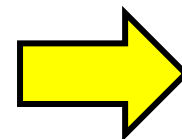


The cascade of federal guidance since the CUI Executive Order has constrained the tailoring of NIST SP 800-171 to the moderate baseline of NIST SP 800-53 with a focus on data confidentiality

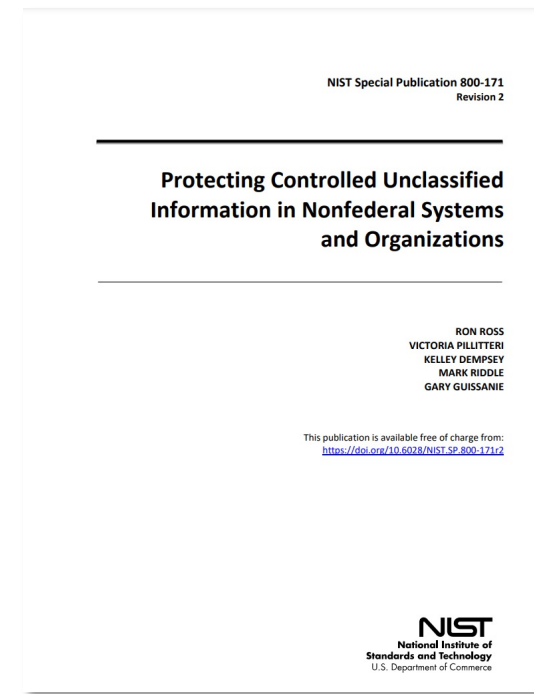
EO 13556 (2010)



32 CFR 2002 (2016)



NIST SP 800-171 (2015*)



§ 2(c) "The National Archives and Records Administration [NARA] shall serve as the Executive Agent to implement this order and oversee agency actions to ensure compliance with this order."

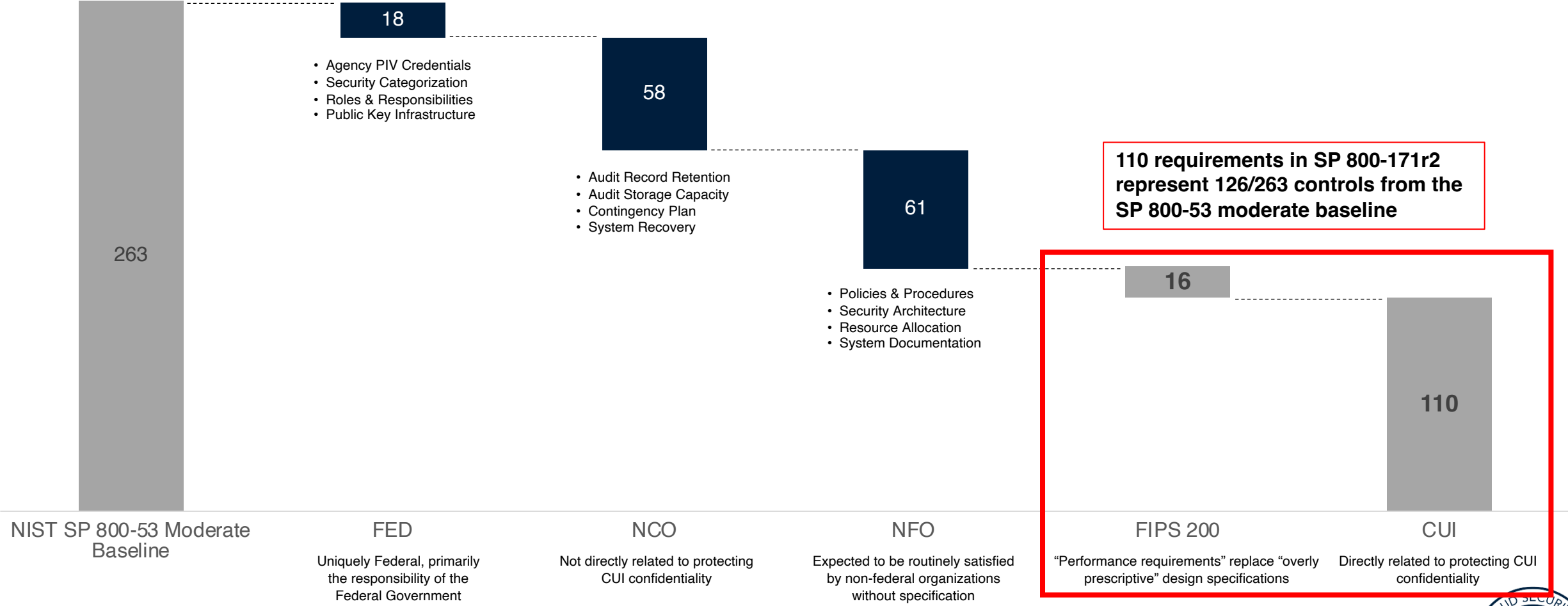
§ 2002.14(g) "In accordance with FIPS PUB 199, CUI Basic is categorized at no less than the moderate confidentiality impact level."

2.1 Basic Assumptions "In accordance with 32 CFR 2002, CUI is categorized at no less than the moderate confidentiality impact value."

*For an explanation of out-of-sequence dates see: <https://youtu.be/jbY2irZ1ePg?si=fqstgVIR9WFVPBfm>



Instead of adding additional security controls the moderate baseline to address APTs, controls were removed from the baseline due to interpretations of federal policy guidance



Only 126 controls from the NIST SP 800-53r4 moderate baseline are considered “directly related to protecting CUI confidentiality”

Family	AC	AT	AU	CA	CM	CP	IA	IR	MA	MP	PE	PL	PS	RA	SA	SC	SI
C o n t r o l s	AC-1	AT-1	AU-1	CA-1	CM-1	CP-1	IA-1	IR-1	MA-1	MP-1	PE-1	PL-1	PS-1	RA-1	SA-1	SC-1	SI-1
	★ AC-2	AT-2	AU-2	CA-2	CM-2	CP-2	★ IA-2	IR-2	MA-2	MP-2	★ PE-2	PL-2	PS-2	RA-2	SA-2	SC-2	★ SI-2
	AC-2(1)	AT-2(2)	AU-2(3)	CA-2(1)	CM-2(1)	CP-2(1)	IA-2(1)	IR-3	MA-3	MP-3	★ PE-3	PL-2(3)	PS-3	RA-3	SA-3	SC-4	SI-2(2)
	AC-2(2)	AT-3	AU-3	CA-3	CM-2(3)	CP-2(3)	IA-2(2)	IR-3(2)	MA-3(1)	MP-4	PE-4	PL-4	PS-4	RA-5	SA-4	SC-5	★ SI-3
	AC-2(3)	AT-4	AU-3(1)	CA-3(5)	CM-2(7)	CP-2(8)	IA-2(3)	IR-4	MA-3(2)	MP-5	PE-5	PL-4(1)	PS-5	RA-5(1)	SA-4(1)	★ SC-7	SI-3(1)
	AC-2(4)		AU-4	CA-5	CM-3	CP-3	IA-2(8)	IR-4(1)	MA-4	MP-5(4)	PE-6	PL-8	PS-6	RA-5(2)	SA-4(2)	SC-7(3)	SI-3(2)
	★ AC-3		AU-5	CA-6	CM-3(2)	CP-4	IA-2(9)	IR-5	MA-4(2)	★ MP-6	PE-6(1)		PS-7	RA-5(5)	SA-4(9)	SC-7(4)	SI-4
	AC-4		AU-6	CA-7	CM-4	CP-4(1)	IA-2(11)	IR-6	MA-5	MP-7	PE-8		PS-8		SA-4(10)	SC-7(5)	SI-4(2)
	AC-5		AU-6(1)	CA-7(1)	CM-5	CP-6	IA-2(12)	IR-6(1)	MA-6	MP-7(1)	PE-9				SA-5	SC-7(7)	SI-4(4)
	AC-6		AU-6(3)	CA-9	CM-6	CP-6(1)	★ IA-3	IR-7			PE-10				SA-8	SC-8	SI-4(5)
	AC-6(1)		AU-7		CM-7	CP-6(3)	IA-4	IR-7(1)			PE-11				SA-9	SC-8(1)	SI-5
	AC-6(2)		AU-7(1)		CM-7(1)	CP-7	★ IA-5	IR-8			PE-12				SA-9(2)	SC-10	SI-7
	AC-6(5)		AU-8		CM-7(2)	CP-7(1)	IA-5(1)				PE-13				SA-10	SC-12	SI-7(1)
	AC-6(9)		AU-8(1)		CM-7(4)*	CP-7(2)	IA-5(2)				PE-13(3)				SA-11	SC-13	SI-7(7)
	AC-6(10)		AU-9		CM-7(5)*	CP-7(3)	IA-5(3)				PE-14					SC-15	SI-8
	AC-7		AU-9(4)		CM-8	CP-8	IA-5(11)				PE-15					SC-17	SI-8(1)
	AC-8		AU-11		CM-8(1)	CP-8(1)	IA-6				PE-16					SC-18	SI-8(2)
	AC-11		AU-12		CM-8(3)	CP-8(2)	IA-7				PE-17					SC-19	SI-10
	AC-11(1)				CM-8(5)	CP-9	IA-8									SC-20	SI-11
	AC-12				CM-9	CP-9(1)	IA-8(1)									SC-21	SI-12
	AC-14				CM-10	CP-10	IA-8(2)									SC-22	SI-16
	★ AC-17				CM-11	CP-10(2)	IA-8(3)									SC-23	
AC-17(1)						IA-8(4)									SC-28		
AC-17(2)															SC-39		
AC-17(3)																	
AC-17(4)																	
AC-18																	
AC-18(1)																	
AC-19																	
AC-19(5)																	
★ AC-20																	
★ AC-20(1)																	
AC-20(2)																	
AC-21																	
★ AC-22																	
Count	28	3	13	3	13	1	11	6	6	8	6	1	3	3	1	15	5

■ SP 800-171

★ CMMC Level 1



To make matters worse, most NIST SP 800-171 requirements are only partial versions of their source controls in SP 800-53

SP 800-53r4

SP 800-171r2

SI-4 INFORMATION SYSTEM MONITORING

Control: The organization:

- a. Monitors the information system to detect:
 - 1. Attacks and indicators of potential attacks in accordance with [Assignment: organization-defined monitoring objectives]; and
 - 2. Unauthorized local, network, and remote connections;
- b. Identifies unauthorized use of the information system through [Assignment: organization-defined techniques and methods];
- c. Deploys monitoring devices:
 - 1. Strategically within the information system to collect organization-determined essential information; and
 - 2. At ad hoc locations within the system to track specific types of transactions of interest to the organization;
- d. Protects information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion;
- e. Heightens the level of information system monitoring activity whenever there is an indication of increased risk to organizational operations and assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information;
- f. Obtains legal opinion with regard to information system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations; and
- g. Provides [Assignment: organization-defined information system monitoring information] to [Assignment: organization-defined personnel or roles] [Selection (one or more): as needed; [Assignment: organization-defined frequency]].

3.14.6	SECURITY REQUIREMENT
Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.	
ASSESSMENT OBJECTIVE	
Determine if:	
3.14.6[a]	the system is monitored to detect attacks and indicators of potential attacks.
3.14.6[b]	inbound communications traffic is monitored to detect attacks and indicators of potential attacks.
3.14.6[c]	outbound communications traffic is monitored to detect attacks and indicators of potential attacks.

“NCO”
 Not directly related to protecting CUI confidentiality
 • See SP 800-171 Appendix E

(4) INFORMATION SYSTEM MONITORING | INBOUND AND OUTBOUND COMMUNICATIONS TRAFFIC
 The information system monitors inbound and outbound communications traffic [Assignment: organization-defined frequency] for unusual or unauthorized activities or conditions.

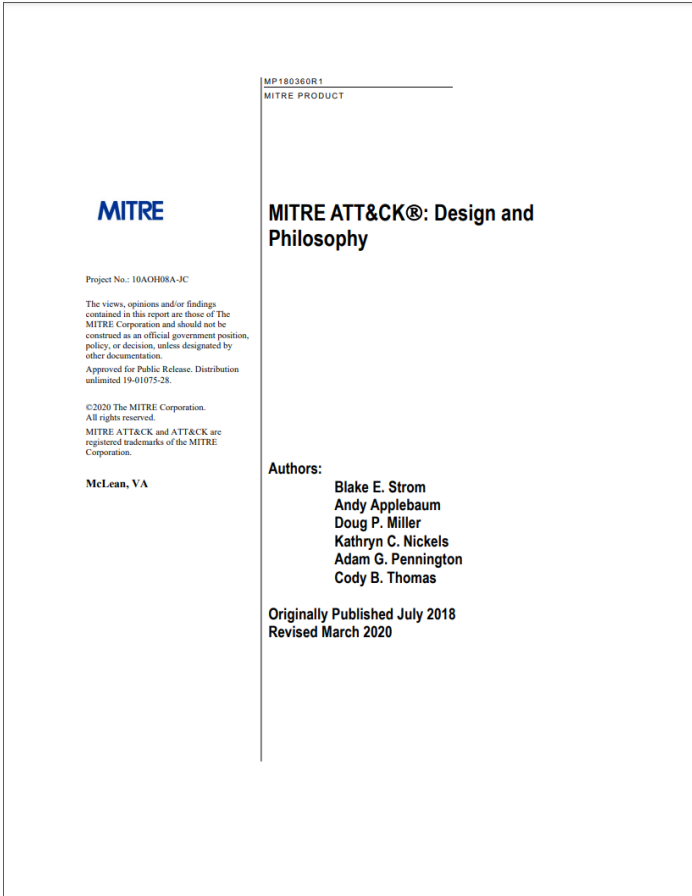


Understanding MITRE ATT&CK



MITRE ATT&CK: Adversarial Tactics, Techniques, & Common Knowledge

A knowledge base of cyber adversary behavior that organizes adversary tactics and techniques



Three conceptual ideas that are core to the philosophy behind ATT&CK:



Maintains the adversary's perspective

- Provides a more accurate frame of reference for how to approach assessing defensive coverage
- Conveys the relationships and dependencies between adversarial actions
- Agnostic of any particular defensive tool or method of collecting data.



Follows real-world activity through empirical examples

- Drawn from publicly reported incidents of suspected advanced persistent threat group behavior
 - Sources: CTI reports, research (con presentations, webinars, blogs, social media), malware samples, etc.
- Grounded to real-world threats that are likely to be encountered rather than theoretical techniques that **are unlikely to be seen due** to difficulty of use or low utility



Has an appropriate level of abstraction to bridge offensive with defense

- A taxonomy for adversarial actions across their lifecycle
- Categorization related to adversary actions and way of defending against it



The basis of the ATT&CK model is the set of techniques and sub-techniques that represent actions that adversaries can perform to accomplish objectives

Core Components of the MITRE ATT&CK Model

Groups

Groups are defined as named intrusion sets, threat groups, actor groups, or campaigns that typically represent targeted, persistent threat activity.

ATT&CK primarily focuses on APT groups though it may also include other advanced groups such as financially motivated actors.

Software

Tools used by defenders, pen testers, and adversaries.

Malware used for malicious purposes by adversaries



Figure 3. ATT&CK Model Relationships

Tactics

The highest-level expression of adversary activity

The “why”; the reason for performing an action

Short-term, tactical adversary goals during an attack

Things adversaries do during an operation, such as persist, discover information, move laterally, execute files, and exfiltrate data

Remain relatively static over time because adversary goals are unlikely to change

<https://www.mitre.org/news-insights/publication/mitre-attck-design-and-philosophy>



The basis of the ATT&CK model is the set of techniques and sub-techniques that represent actions that adversaries can perform to accomplish objectives

Core Components of the MITRE ATT&CK Model

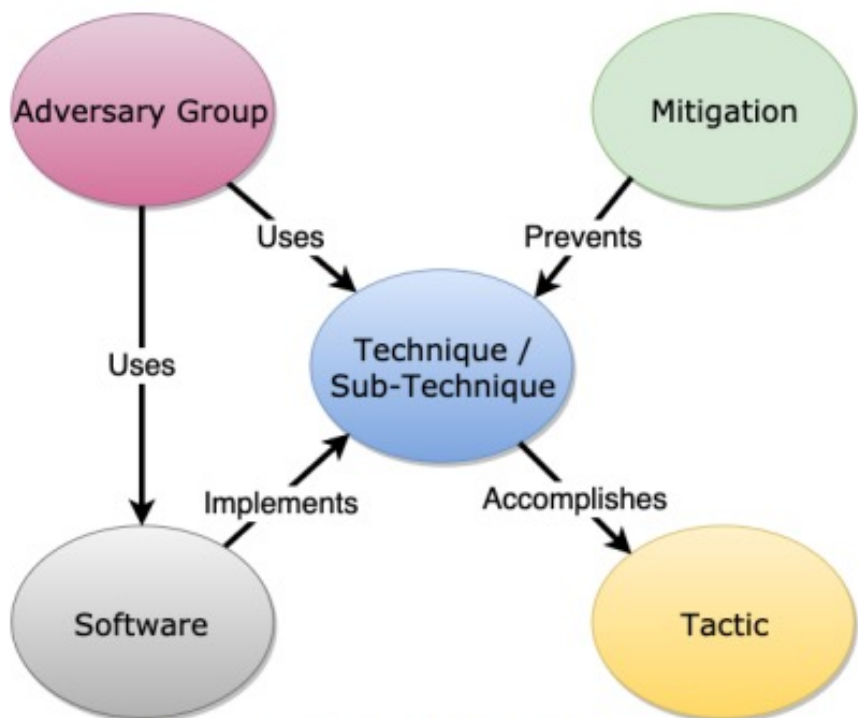


Figure 3. ATT&CK Model Relationships

Techniques & Sub-Techniques

Techniques represent “how” an adversary achieves a tactical objective by performing an action.

- Ex: dump credentials from an operating system to gain access to useful credentials within a network.

Represent the individual actions adversaries make or pieces of information the adversary learns by performing an action

Sub-techniques describe the ways techniques are applied to specific technologies, operating systems, etc.

- Ex: phishing is subdivided to differentiate the vector of delivery—attachment, link, or service

The basis of the ATT&CK model is the set of techniques and sub-techniques that represent actions that adversaries can perform to accomplish objectives

Core Components of the MITRE ATT&CK Model

Mitigations

Mitigations in ATT&CK represent security concepts and classes of technologies that can be used to **prevent a technique or sub-technique from being successfully executed**.

Mitigations are vendor product agnostic and only describe categories or classes of technologies, not specific solutions.

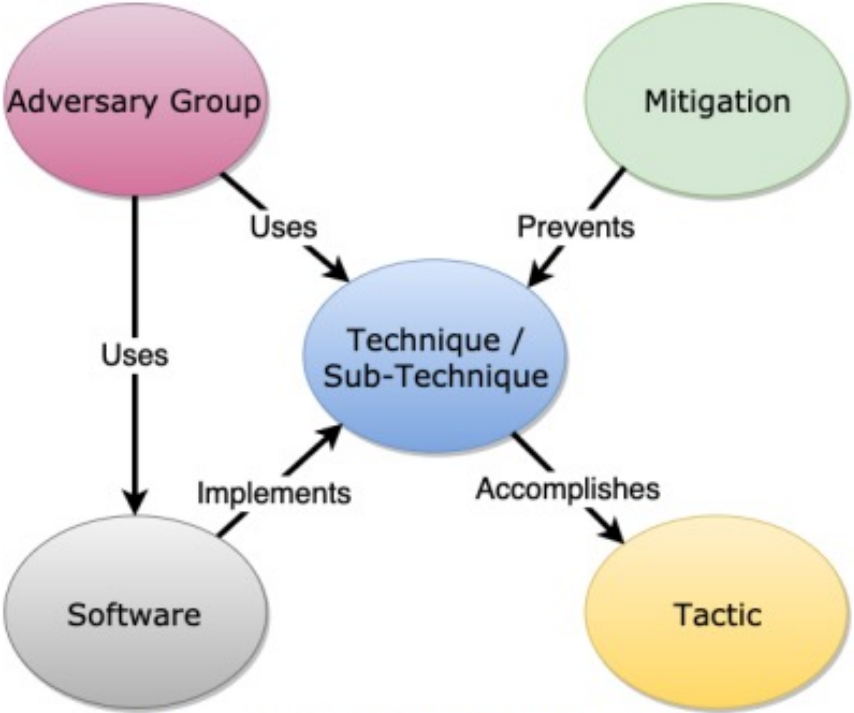


Figure 3. ATT&CK Model Relationships



The basis of the ATT&CK model is the set of techniques and sub-techniques that represent actions that adversaries can perform to accomplish objectives

Core Components of the MITRE ATT&CK Model

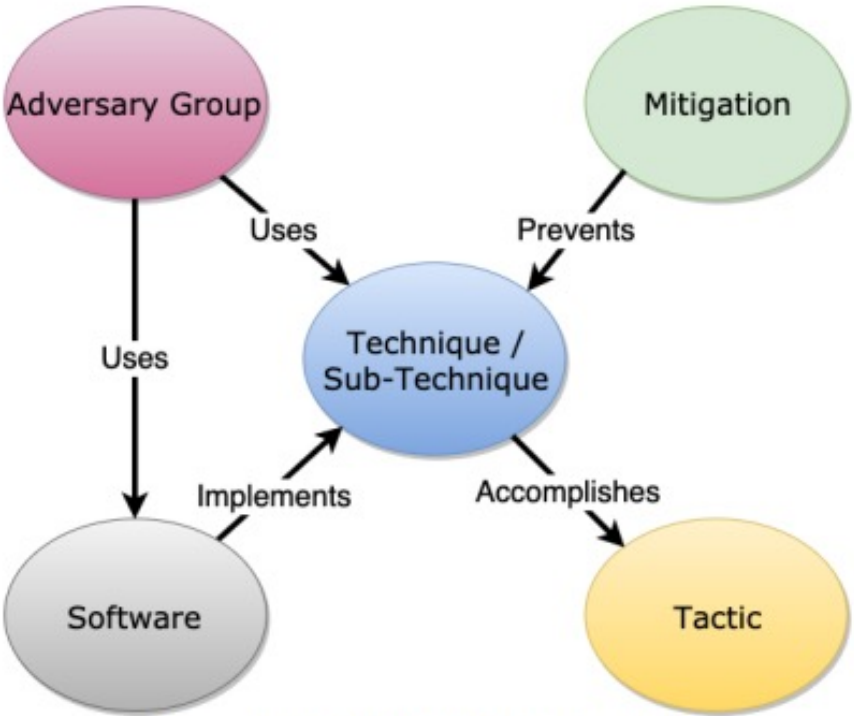


Figure 3. ATT&CK Model Relationships

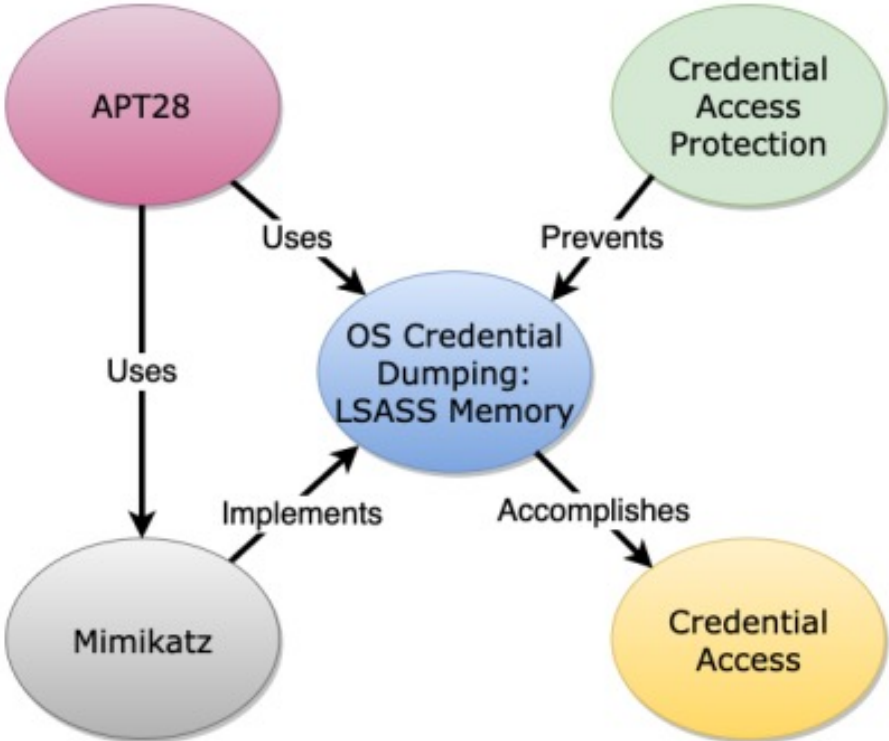


Figure 4. ATT&CK Model Relationships Example

An example as applied to a specific persistent threat group where APT28 uses Mimikatz for credential dumping against Windows LSASS process memory:

<https://www.mitre.org/news-insights/publication/mitre-attck-design-and-philosophy>



The relationship between tactics, techniques, and sub-techniques in the model can be visualized in the ATT&CK “Matrix”

Thank you to Tidal Cyber and SOC Prime for becoming ATT&CK's first Benefactors. To join the cohort, or learn more about this program visit our [Benefactors page](#).

MATRICES

- Enterprise ^
- PRE
- Windows
- macOS
- Linux
- Cloud v
- Network
- Containers
- Mobile v
- ICS

Home > Matrices > Enterprise

Enterprise Matrix

Below are the tactics and techniques representing the MITRE ATT&CK® Matrix for Enterprise. The Matrix contains information for the following platforms: [Windows](#), [macOS](#), [Linux](#), [PRE](#), [Azure AD](#), [Office 365](#), [Google Workspace](#), [SaaS](#), [IaaS](#), [Network](#), [Containers](#).

[View on the ATT&CK® Navigator](#)
↗

[Version Permalink](#)

layout: side ▾ show sub-techniques hide sub-techniques

help

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access
10 techniques	8 techniques	10 techniques	14 techniques	20 techniques	14 techniques	43 techniques	17 techniques
Active Scanning (3)	Acquire Access	Content Injection	Cloud Administration Command	Account Manipulation (6)	Abuse Elevation Control Mechanism (5)	Abuse Elevation Control Mechanism (5)	Adversary-in-the-Middle (3)
Gather Victim Host Information (4)	Acquire Infrastructure (8)	Drive-by Compromise	Command and Scripting Interpreter (9)	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Brute Force (4)
Gather Victim Identity Information (3)	Compromise Accounts (3)	Exploit Public-Facing Application	Container Administration Command	Boot or Logon Autostart Execution (14)	Account Manipulation (6)	BITS Jobs	Credentials from Password Stores (6)
Gather Victim Network Information (6)	Compromise Infrastructure (7)	External Remote Services	Deploy Container	Boot or Logon Initialization Scripts (5)	Boot or Logon Execution (14)	Build Image on Host	Exploitation for Credential Access
Gather Victim Org Information (4)	Develop Capabilities (4)	Hardware Additions	Exploitation for Client Execution	Browser Extensions	Boot or Logon Initialization Scripts (5)	Debugger Evasion	Forced Authentication
Phishing for Information (4)	Establish Accounts (3)	Phishing (4)	Inter-Process Communication (3)	Compromise Client Software Binary	Create or Modify System Process (4)	Deobfuscate/Decode Files or Information	Forge Web Credentials (2)
Search Closed Sources (2)	Obtain Capabilities (6)	Replication Through Removable	Native API	Create Account (3)		Deploy Container	Input Capture (4)
Search Open	Stage Capabilities (6)					Direct Volume Access	
						Domain Policy Modification (2)	



ATT&CK V12 contains 14 Tactics, 193 Techniques, 401 Sub-techniques, 135 Groups, 14 Campaigns, and 718 Pieces of Software

Reconnaissance 10 techniques	Resource Development 8 techniques	Initial Access 10 techniques	Execution 14 techniques	Persistence 20 techniques	Privilege Escalation 14 techniques	Defense Evasion 43 techniques	Credential Access 17 techniques	Discovery 32 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 17 techniques	Exfiltration 9 techniques	Impact 14 techniques
Active Scanning (0/3)	Acquire Access	Content Injection	Cloud Administration Command	Account Manipulation (0/6)	Abuse Elevation Control Mechanism (0/5)	Abuse Elevation Control Mechanism (0/5)	Adversary-in-the-Middle (0/3)	Account Discovery (0/4)	Exploitation of Remote Services	Adversary-in-the-Middle (0/3)	Application Layer Protocol (0/4)	Automated Exfiltration (0/1)	Account Access Removal
Gather Victim Host Information (0/4)	Acquire Infrastructure (0/6)	Drive-by Compromise	Command and Scripting Interpreter (0/7)	BITS Jobs	Access Token Manipulation (0/5)	Access Token Manipulation (0/5)	Brute Force (0/4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (0/3)	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Gather Victim Identity Information (0/3)	Compromise Accounts (0/2)	Exploit Public-Facing Application	Container Administration Command	Boot or Logon Autostart Execution (0/14)	Account Manipulation (0/6)	Account Manipulation (0/5)	Credentials from Password Stores (0/6)	Browser Information Discovery	Lateral Tool Transfer	Audio Capture	Exfiltration Over Alternative Protocol (0/3)	Exfiltration Over Alternative Protocol (0/3)	Data Encrypted for Impact
Gather Victim Network Information (0/6)	Compromise Infrastructure (0/7)	External Remote Services	Deploy Container	Boot or Logon Initialization Scripts (0/5)	Boot or Logon Autostart Execution (0/14)	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (0/2)	Automated Collection	Content Injection	Exfiltration Over C2 Channel	Data Manipulation (0/3)
Gather Victim Org Information (0/4)	Develop Capabilities (0/4)	Hardware Additions	Exploitation for Client Execution	Browser Extensions	Boot or Logon Initialization Scripts (0/5)	Debugger Evasion	Forced Authentication	Cloud Service Dashboard	Remote Services (0/8)	Clipboard Data	Data Encoding (0/2)	Exfiltration Over Other Network Medium (0/1)	Defacement (0/2)
Phishing for Information (0/4)	Establish Accounts (0/3)	Phishing (0/4)	Inter-Process Communication (0/3)	Compromise Client Software Binary	Boot or Logon Initialization Scripts (0/5)	Deobfuscate/Decode Files or Information	Forge Web Credentials (0/2)	Cloud Storage Object Discovery	Replication Through Removable Media	Data from Cloud Storage	Data Obfuscation (0/3)	Exfiltration Over Physical Medium (0/1)	Disk Wipe (0/2)
Search Closed Sources (0/2)	Obtain Capabilities (0/6)	Replication Through Removable Media	Native API	Create Account (0/5)	Create or Modify System Process (0/4)	Deploy Container	Input Capture (0/4)	Container and Resource Discovery	Software Deployment Tools	Data from Configuration Repository (0/2)	Dynamic Resolution (0/3)	Exfiltration Over Web Service (0/4)	Endpoint Denial of Service (0/4)
Search Open Technical Databases (0/5)	Stage Capabilities (0/6)	Supply Chain Compromise (0/3)	Scheduled Task/Job (0/5)	Create or Modify System Process (0/4)	Domain Policy Modification (0/2)	Direct Volume Access	Modify Authentication Process (0/8)	Debugger Evasion	Taint Shared Content	Data from Information Repositories (0/3)	Encrypted Channel (0/2)	Exfiltration Over Web Service (0/4)	Financial Theft
Search Open Websites/Domains (0/3)		Trusted Relationship	Serverless Execution	Event Triggered Execution (0/16)	Escape to Host (0/7)	Domain Policy Modification (0/2)	Multi-Factor Authentication Interception (0/8)	Device Driver Discovery	Use Alternate Authentication Material (0/4)	Data from Network Shared Drive	Fallback Channels	Scheduled Transfer	Firmware Corruption
Search Victim-Owned Websites		Valid Accounts (0/4)	Shared Modules	External Remote Services (0/16)	Event Triggered Execution (0/16)	Exploitation for Defense Evasion	Multi-Factor Authentication Request Generation	Domain Trust Discovery		Data from Removable Media	Ingress Tool Transfer	Transfer Data to Cloud Account	Inhibit System Recovery
			Software Deployment Tools	Hijack Execution Flow (0/12)	Exploitation for Privilege Escalation	File and Directory Permissions Modification (0/2)	Network Sniffing	File and Directory Discovery		Data from Network Shared Drive	Multi-Stage Channels		Network Denial of Service (0/2)
			System Services (0/2)	Implant Internal Image (0/8)	Hijack Execution Flow (0/12)	Hide Artifacts (0/11)	OS Credential Dumping (0/8)	Group Policy Discovery		Data from Network Shared Drive	Non-Application Layer Protocol		Resource Hijacking
			User Execution (0/3)	Modify Authentication Process (0/6)	Process Injection (0/12)	Hijack Execution Flow (0/12)	Steal Application Access Token	Log Enumeration		Data from Network Shared Drive	Non-Standard Port		Service Stop
			Windows Management Instrumentation	Office Application Startup (0/16)	Scheduled Task/Job (0/5)	Impair Defenses (0/11)	Steal or Forge Authentication Certificates	Network Service Discovery		Data from Network Shared Drive	Protocol Tunneling		System Shutdown/Reboot
				Power Settings	Valid Accounts (0/4)	Impersonation	Steal or Forge Kerberos Tickets (0/4)	Network Sniffing		Data from Network Shared Drive	Proxy (0/4)		
				Pre-OS Boot (0/5)		Indicator Removal (0/5)	Steal Web Session Cookie	Log Enumeration		Data from Network Shared Drive	Remote Access Software		
				Scheduled Task/Job (0/5)		Indirect Command Execution	Unsecured Credentials (0/8)	Network Service Discovery		Data from Network Shared Drive	Traffic Signaling (0/2)		
				Server Software Component (0/5)		Masquerading (0/7)		Network Share Discovery		Data from Network Shared Drive	Web Service (0/3)		
				Traffic Signaling (0/2)		Modify Authentication Process (0/8)		Network Sniffing		Data from Network Shared Drive			
				Valid Accounts (0/4)		Modify Cloud Compute Infrastructure (0/5)		Password Policy Discovery		Data from Network Shared Drive			
						Modify Registry		Peripheral Device Discovery		Data from Network Shared Drive			
						Modify System Image (0/2)		Permission Groups Discovery (0/3)		Data from Network Shared Drive			
						Network Boundary Bridging (0/1)		Process Discovery		Data from Network Shared Drive			
						Obfuscated Files or Information (0/12)		Query Registry		Data from Network Shared Drive			
						Plist File Modification		Remote System Discovery		Data from Network Shared Drive			
						Pre-OS Boot (0/5)		Software Discovery (0/7)		Data from Network Shared Drive			
						Process Injection (0/12)		System Information Discovery		Data from Network Shared Drive			
						Reflective Code Loading		System Location Discovery (0/7)		Data from Network Shared Drive			
						Rogue Domain Controller		System Network Configuration Discovery (0/2)		Data from Network Shared Drive			
						Rootkit		System Network Connections Discovery		Data from Network Shared Drive			
						Subvert Trust Controls (0/6)		System Owner/User Discovery		Data from Network Shared Drive			
						System Binary Proxy Execution (0/13)		System Service Discovery		Data from Network Shared Drive			
						System Script Proxy Execution (0/1)		System Time Discovery		Data from Network Shared Drive			
						Template Injection		Virtualization/Sandbox Evasion (0/3)		Data from Network Shared Drive			
						Traffic Signaling (0/2)				Data from Network Shared Drive			
						Trusted Developer Utilities Proxy Execution (0/1)				Data from Network Shared Drive			
						Unused/Unsupported Cloud Regions				Data from Network Shared Drive			
						Use Alternate Authentication Material (0/4)				Data from Network Shared Drive			
						Valid Accounts (0/4)				Data from Network Shared Drive			
						Virtualization/Sandbox Evasion (0/3)				Data from Network Shared Drive			
						Weaken Encryption (0/2)				Data from Network Shared Drive			
						XSL Script Processing				Data from Network Shared Drive			



ATT&CK V12 contains 14 Tactics, 193 Techniques, 401 Sub-techniques, 135 Groups, 14 Campaigns, and 718 Pieces of Software

Credential Access 17 techniques	Discovery 32 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 17 techniques	Exfiltration 9 techniques	Impact 14 techniques
Adversary-in-the-Middle (0/3)	Account Discovery (0/4)	Exploitation of Remote Services	Adversary-in-the-Middle (0/3)	Application Layer Protocol (0/4)	Automated Exfiltration (0/1)	Account Access Removal
Brute Force (0/4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (0/3)	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Credentials from Password Stores (0/6)	Browser Information Discovery	Lateral Tool Transfer	Audio Capture	Content Injection	Exfiltration Over Alternative Protocol (0/3)	Data Encrypted for Impact
Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (0/2)	Automated Collection	Data Encoding (0/2)	Exfiltration Over C2 Channel	Data Manipulation (0/3)
Forced Authentication	Cloud Service Dashboard	Remote Services (0/8)	Browser Session Hijacking	Data Obfuscation (0/3)	Exfiltration Over Other Network Medium (0/1)	Defacement (0/2)
Forge Web Credentials (0/2)	Cloud Service Discovery	Replication Through Removable Media	Clipboard Data	Dynamic Resolution (0/3)	Exfiltration Over Physical Medium (0/1)	Disk Wipe (0/2)
Input Capture (0/4)	Cloud Storage Object Discovery	Software Deployment Tools	Data from Cloud Storage	Encrypted Channel (0/2)	Exfiltration Over Web Service (0/4)	Endpoint Denial of Service (0/4)
Modify Authentication Process (0/8)	Container and Resource Discovery	Taint Shared Content	Data from Configuration Repository (0/2)	Fallback Channels	Scheduled Transfer	Financial Theft
Multi-Factor Authentication Interception	Debugger Evasion	Use Alternate Authentication Material (0/4)	Data from Information Repositories (0/3)	Ingress Tool Transfer	Transfer Data to Cloud Account	Firmware Corruption
Multi-Factor Authentication Request Generation	Device Driver Discovery		Data from Local System	Multi-Stage Channels		Inhibit System Recovery
Network Sniffing	Domain Trust Discovery		Data from Network Shared Drive	Non-Application Layer Protocol		Network Denial of Service (0/2)
OS Credential Dumping (0/8)	File and Directory Discovery		Data from Removable Media	Non-Standard Port		Resource Hijacking
Steal Application Access Token	Group Policy Discovery		Data Staged (0/2)	Protocol Tunneling		Service Stop
Steal or Forge Authentication Certificates	Log Enumeration		Email Collection (0/3)	Proxy (0/4)		System Shutdown/Reboot
Steal or Forge Kerberos Tickets (0/4)	Network Service Discovery		Input Capture (0/4)	Remote Access Software		
Steal Web Session Cookie	Network Share Discovery		Screen Capture	Traffic Signaling (0/2)		
Unsecured Credentials (0/8)	Network Sniffing		Video Capture	Web Service (0/3)		
	Password Policy Discovery					
	Peripheral Device Discovery					
	Permission Groups Discovery (0/3)					
	Process Discovery					
	Query Registry					
	Remote System Discovery					

You can explore the MITRE ATT&CK Model in detail via the MITRE ATT&CK Matrix – even if you have no technical training

OS Credential Dumping (0/8)

- /etc/passwd and /etc/shadow
- Cached Domain Credentials
- DCSync
- LSA Secrets
- LSASS Memory ←
- NTDS
- Proc Filesystem
- Security Account Manager

MITRE | ATT&CK®

Thank you to Tidal Cyber and SOC Prime for becoming ATT&CK's first Benefactors. To join the cohort, or learn more about this program visit our [Benefactors page](#).

Home > Techniques > Enterprise > OS Credential Dumping

OS Credential Dumping

Sub-techniques (8)

ID	Name
T1003.001	LSASS Memory
T1003.002	Security Account Manager
T1003.003	NTDS
T1003.004	LSA Secrets
T1003.005	Cached Domain Credentials
T1003.006	DCSync
T1003.007	Proc Filesystem
T1003.008	/etc/passwd and /etc/shadow

Adversaries may attempt to dump credentials to obtain account login and credential material, normally in the form of a hash or a clear text password, from the operating system and software. Credentials can then be used to perform [Lateral Movement](#) and access restricted information.

Several of the tools mentioned in associated sub-techniques may be used by both adversaries and professional security testers. Additional custom tools likely exist as well.

ID: T1003
 Sub-techniques: T1003.001, T1003.002, T1003.003, T1003.004, T1003.005, T1003.006, T1003.007, T1003.008
 ① **Tactic:** Credential Access
 ① **Platforms:** Linux, Windows, macOS
 ① **Permissions Required:** Administrator, SYSTEM, root
 Contributors: Ed Williams, Trustwave, SpiderLabs; Vincent Le Toux
 Version: 2.1
 Created: 31 May 2017
 Last Modified: 08 March 2022

[Version Permalink](#)

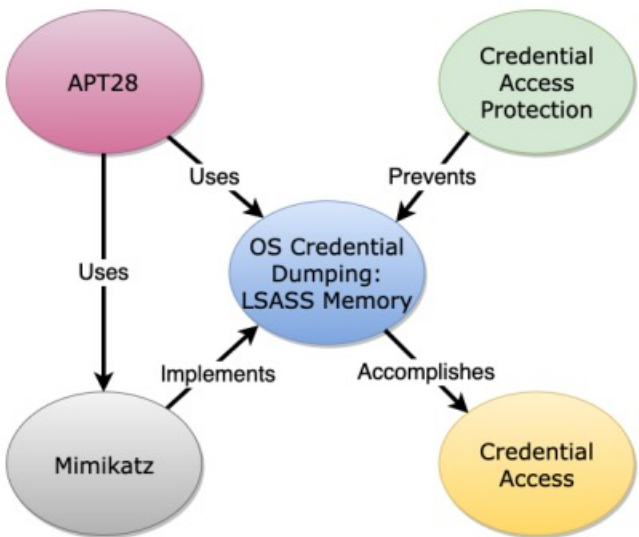


Figure 4. ATT&CK Model Relationships Example



You can explore the MITRE ATT&CK Model in detail via the MITRE ATT&CK Matrix – even if you have no technical training

OS Credential Dumping (0/8)

- /etc/passwd and /etc/shadow
- Cached Domain Credentials
- DCSync
- LSA Secrets
- LSASS Memory** ←
- NTDS
- Proc Filesystem
- Security Account Manager

MITRE | ATT&CK

Matrices | Tactics | Techniques | Defenses | CTI | Resources | Benefactors

Thank you to Tidal Cyber and SOC Prime for becoming ATT&CK's first Benefactors. To join the cohort, or learn more about this program visit our [Benefactors page](#).

Home > Techniques > Enterprise > OS Credential Dumping > LSASS Memory

OS Credential Dumping: LSASS Memory

Other sub-techniques of OS Credential Dumping (8)

ID	Name
T1003.001	LSASS Memory
T1003.002	Security Account Manager
T1003.003	NTDS
T1003.004	LSA Secrets
T1003.005	Cached Domain Credentials
T1003.006	DCSync
T1003.007	Proc Filesystem
T1003.008	/etc/passwd and /etc/shadow

Adversaries may attempt to access credential material stored in the process memory of the Local Security Authority Subsystem Service (LSASS). After a user logs on, the system generates and stores a variety of credential materials in LSASS process memory. These credential materials can be harvested by an administrative user or SYSTEM and used to conduct Lateral Movement using Use Alternate Authentication Material.

As well as in-memory techniques, the LSASS process memory can be dumped from the target host and analyzed on a local system.

ID: T1003.001
 Sub-technique of: T1003
 Tactic: Credential Access
 Platforms: Windows
 Contributors: Ed Williams, Trustwave, SpiderLabs; Edward Millington; Olaf Hartong, Falcon Force
 Version: 1.3
 Created: 11 February 2020
 Last Modified: 24 July 2023
[Version Permalink](#)

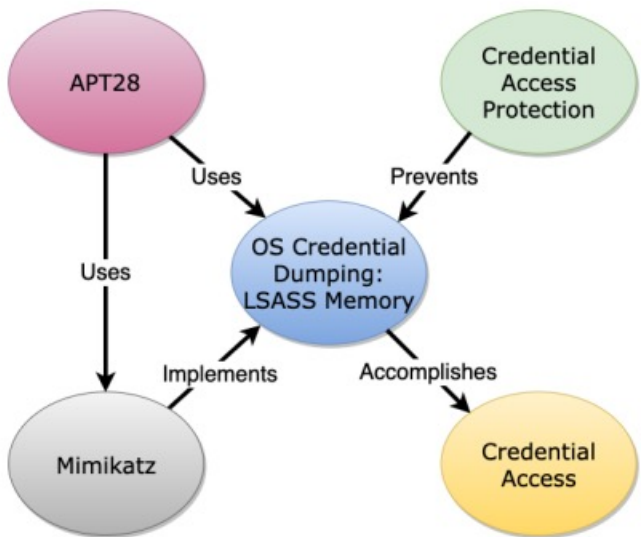


Figure 4. ATT&CK Model Relationships Example



You can explore the MITRE ATT&CK Model in detail via the MITRE ATT&CK Matrix – even if you have no technical training



**WANTED
BY THE FBI**

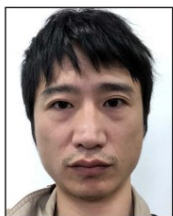
APT 41 GROUP



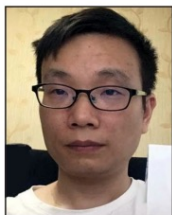
ZHANG Haoran



TAN Dailin



QIAN Chuan



FU Qiang



JIANG Lizhi

CAUTION

ZHANG Haoran, TAN Dailin, QIAN Chuan, FU Qiang, and JIANG Lizhi are all part of a Chinese hacking group known as APT 41 and BARIUM.

On August 15, 2019, a Grand Jury in the District of Columbia returned an indictment against Chinese nationals ZHANG Haoran and TAN Dailin on charges including Unauthorized Access to Protected Computers, Aggravated Identity Theft, Money Laundering, and Wire Fraud. These charges primarily stemmed from alleged activity targeting high technology and video gaming companies, and a United Kingdom citizen.

On August 11, 2020, a Grand Jury in the District of Columbia returned an indictment against Chinese nationals QIAN Chuan, FU Qiang, and JIANG Lizhi on charges including Racketeering, Money Laundering, Fraud, Identity Theft, and Access Device Fraud. These charges stem from their alleged unauthorized computer intrusions while employed by Chengdu 404 Network Technology Company. The defendants allegedly conducted supply chain attacks to gain unauthorized access to networks throughout the world, targeting hundreds of companies representing a broad array of industries to include: social media, telecommunications, government, defense, education, and manufacturing. These victims included companies in Australia, Brazil, Germany, India, Japan and Sweden. The defendants allegedly targeted telecommunications providers in the United States, Australia, China (Tibet), Chile, India, Indonesia, Malaysia, Pakistan, Singapore, South Korea, Taiwan, and Thailand. The defendants allegedly deployed ransomware attacks and demanded payments from victims.

If you have any information concerning these individuals, please contact your local FBI office, or the nearest American Embassy or Consulate.

Field Office: Washington D.C.

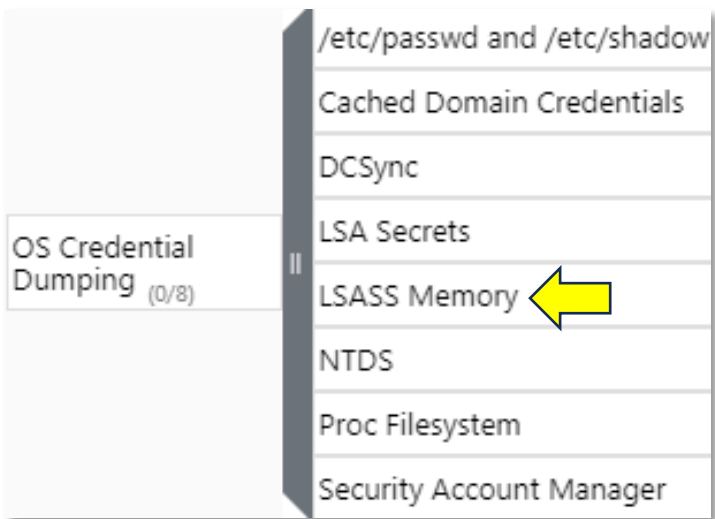
www.fbi.gov

Procedure Examples

ID	Name	Description
C0025	2016 Ukraine Electric Power Attack	During the 2016 Ukraine Electric Power Attack, Sandworm Team used Mimikatz to capture and use legitimate credentials. ^[5]
G0006	APT1	APT1 has been known to use credential dumping using Mimikatz. ^[6]
G0007	APT28	APT28 regularly deploys both publicly available (ex: Mimikatz) and custom password retrieval tools on victims. ^{[7][8]} They have also dumped the LSASS process memory using the MiniDump function. ^[9]
G0022	APT3	APT3 has used a tool to dump credentials by injecting itself into lsass.exe and triggering with the argument "dig." ^[10]
G0050	APT32	APT32 used Mimikatz and customized versions of Windows Credential Dumper to harvest credentials. ^{[11][12]}
G0064	APT33	APT33 has used a variety of publicly available tools like LaZagne, Mimikatz, and ProcDump to dump credentials. ^{[13][14]}
G0087	APT39	APT39 has used Mimikatz, Windows Credential Editor and ProcDump to dump credentials. ^[15]
G0096	APT41	APT41 has used hashdump, Mimikatz, and the Windows Credential Editor to dump password hashes from memory and authenticate to other user accounts. ^{[16][17]}
G0143	Aquatic Panda	Aquatic Panda has attempted to harvest credentials through LSASS memory dumping. ^[18]
S0606	Bad Rabbit	Bad Rabbit has used Mimikatz to harvest credentials from the victim's machine. ^[19]
G0108	Blue Mockingbird	Blue Mockingbird has used Mimikatz to retrieve credentials from LSASS memory. ^[20]
G0060	BRONZE BUTLER	BRONZE BUTLER has used various tools (such as Mimikatz and WCE) to perform credential dumping. ^[21]
G0003	Cleaver	Cleaver has been known to dump credentials using Mimikatz and Windows Credential Editor. ^[22]
S0154	Cobalt Strike	Cobalt Strike can spawn a job to inject into LSASS memory and dump password hashes. ^[23]



You can explore the MITRE ATT&CK Model in detail via the MITRE ATT&CK Matrix – even if you have no technical training



Mitigations

ID	Mitigation	Description
M1040	Behavior Prevention on Endpoint	On Windows 10, enable Attack Surface Reduction (ASR) rules to secure LSASS and prevent credential stealing. ^[92]
M1043	Credential Access Protection	With Windows 10, Microsoft implemented new protections called Credential Guard to protect the LSA secrets that can be used to obtain credentials through forms of credential dumping. It is not configured by default and has hardware and firmware system requirements. It also does not protect against all forms of credential dumping. ^{[93][94]}
M1028	Operating System Configuration	Consider disabling or restricting NTLM. ^[95] Consider disabling WDigest authentication. ^[96]
M1027	Password Policies	Ensure that local administrator accounts have complex, unique passwords across all systems on the network.
M1026	Privileged Account Management	Do not put user or admin domain accounts in the local administrator groups across systems unless they are tightly controlled, as this is often equivalent to having a local administrator account with the same password on all systems. Follow best practices for design and administration of an enterprise network to limit privileged account use across administrative tiers.
M1025	Privileged Process Integrity	On Windows 8.1 and Windows Server 2012 R2, enable Protected Process Light for LSA. ^[97]
M1017	User Training	Limit credential overlap across accounts and systems by training users and administrators not to use the same password for multiple accounts.

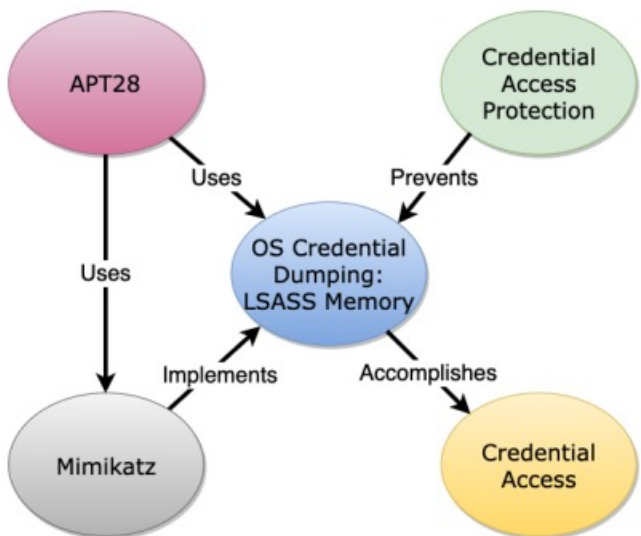


Figure 4. ATT&CK Model Relationships Example



You can explore the MITRE ATT&CK Model in detail via the MITRE ATT&CK Matrix – even if you have no technical training

OS Credential Dumping (0/8)	/etc/passwd and /etc/shadow
	Cached Domain Credentials
	DCSync
	LSA Secrets
	LSASS Memory ←
	NTDS
	Proc Filesystem
	Security Account Manager

Detection

ID	Data Source	Data Component	Detects
DS0017	Command	Command Execution	<p>Monitor executed commands and arguments that may attempt to access credential material stored in the process memory of the Local Security Authority Subsystem Service (LSASS). Remote access tools may contain built-in features or incorporate existing tools like Mimikatz. PowerShell scripts also exist that contain credential dumping functionality, such as PowerSploit's Invoke-Mimikatz module,^[98] which may require additional logging features to be configured in the operating system to collect necessary information for analysis.</p> <p>Note: Event ID 4104 from the "Microsoft-Windows-PowerShell/Operational" log captures Powershell script blocks, whose contents can be further analyzed to determine if they're performing LSASS dumping.</p>
DS0028	Logon Session	Logon Session Creation	<p>Monitor for newly constructed logon behavior from credentials being accessed by process memory of the LSASS. For example, detect behaviors of Secretsdump against a system, not being a Domain Controller.</p>
DS0009	Process	OS API Execution	<p>Monitor for API calls that may attempt to access credential material stored in the process memory of the Local Security Authority Subsystem Service (LSASS). OS API calls associated with LSASS process dumping include <code>OpenProcess</code> and <code>MiniDumpWriteDump</code>. Execution of these functions might trigger security log ids such as 4663 (Microsoft Security Auditing) and 10 (Microsoft Sysmon)</p> <p>Note: Most EDR tools do not support direct monitoring of API calls due to the sheer volume of calls produced by an endpoint but may have alerts or events that are based on abstractions of OS API calls. Dynamic malware analysis tools (i.e., sandboxes) can be used to trace the execution, including OS API calls, for a single PE binary.</p>

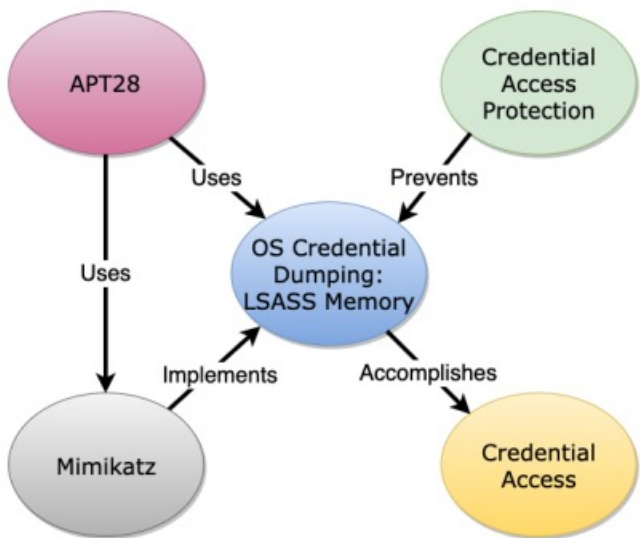
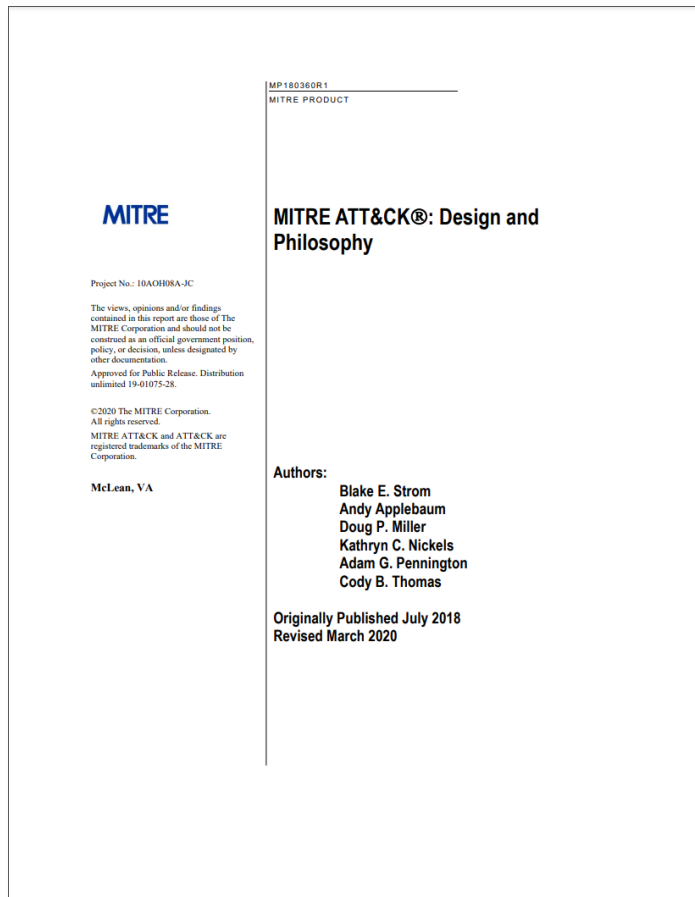


Figure 4. ATT&CK Model Relationships Example



MITRE ATT&CK and NIST SP 800-171 bring two different perspectives to data confidentiality that must be compared to determine coverage of threats



“The types of tactics in ATT&CK have historically aligned to covering adversaries primarily focused on breaching **the confidentiality of information**.

Goals such as initial access, discovery, and credential access are commonly used to gain and expand access within an environment with an ultimate objective of stealing information through collection and exfiltration.”


In 2019, the Impact tactic was added to ATT&CK to address the lack of coverage for disruptive and/or destructive attacks:

- Targeted ransomware, disk wiper incidents, manipulation of financial transactions, and large-scale distributed denial of service attacks
- The Impact tactic specifically involve only attacks impacting **the integrity or availability of information or systems**.



Mapping NIST SP 800-53 to MITRE ATT&CK




 MITRE
ENGUINITY.
A Foundation for Public Good

WHO WE ARE ▾ **CYBERSECURITY** ▾ TELECOM ▾ GROWING IMPACT ▾ NEWS & INSIGHTS ▾ SEARCH ▾

CYBERSECURITY: CENTER FOR THREAT-INFORMED DEFENSE

[CHECK OUT OUR WORK](#) →

IN THIS SECTION **CENTER FOR THREAT-INFORMED DEFENSE** GET INVOLVED ABOUT US ▾ OUR WORK RESOURCES ▾ [BLOG](#) [PARTICIPANT LOGIN](#)



Security Control Mappings: A Bridge to Threat-Informed Defense



Jon Baker · [Follow](#)

Published in MITRE-Engenuity · 7 min read · Dec 15, 2020



112



1





PROBLEM

Defenders lack a single resource to view defensive capabilities mapped to the adversarial attack techniques in ATT&CK.



SOLUTION

Create a central hub that provides access to all mappings, and offer standard tools and processes for developing mappings to ATT&CK.



IMPACT

Defenders can easily access and explore mapped security controls from the perspective of the ATT&CK techniques they mitigate.

<https://mitre-engenuity.org/cybersecurity/center-for-threat-informed-defense/our-work/nist-800-53-control-mappings/>





MAPPINGS EXPLORER

Mappings Explorer enables cyber defenders to understand how security controls and capabilities map onto the adversary behaviors catalogued in the [MITRE ATT&CK](#) knowledge base. These mappings form a bridge between the threat-informed approach to cybersecurity and the traditional security controls perspective.

Learn More



<https://center-for-threat-informed-defense.github.io/mappings-explorer/>



MAPPING METHODOLOGY

ATT&CK Mitigation Review

- Select an ATT&CK mitigation and study it.
- What is the mitigation preventing?
- What techniques has it been applied to?



ATT&CK Technique Review

- Examine each referenced technique in the context of the selected mitigation.
- What is the adversary's goal (tactic) and how are they achieving that goal (technique)?
- How does the mitigation prevent that behavior?



Security Control Review

- Examine each security control in the context of the mitigation.
- Is the control in scope?
- Does the control align with the intent of the ATT&CK mitigation?
- Is the control relevant to the specific technique under review?



Create a Mapping

- If the control is deemed relevant, create a mapping.
- Document the new mapping for the single technique in the context of the mitigation that is under review.

<https://center-for-threat-informed-defense.github.io/mappings-explorer/about/methodology/>

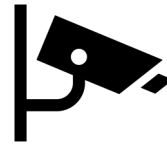


NIST 800-53 MAPPING SCOPE



Operational Controls vs Policy & Procedures

Does not account for the management elements in policy & procedures



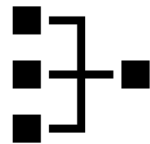
Mitigation vs Monitoring

Controls that may only monitor adversary behaviors are out of scope.



Controls vs Control Enhancements

Only maps to the control level



Network Infrastructure Devices

Techniques for adversary behavior on switches, routers, etc.



Pre-compromise Mitigation

Reconnaissance and Resource Development techniques are out of scope

<https://center-for-threat-informed-defense.github.io/mappings-explorer/about/methodology/nist-scope/>



Only 88 controls from in-scope families are tailored as directly related to protecting the confidentiality of CUI in NIST SP 800-171

• Total in-scope controls in the moderate baseline: 187 (ONLY 41% of direct operational controls are considered directly relevant in SP 800-171)

Family	AC	AT	AU	CA	CM	CP	IA	IR	MA	MP	PE	PL	PS	RA	SA	SC	SI
	AC-1	AT-1	AU-1	CA-1	CM-1	CP-1	IA-1	IR-1	MA-1	MP-1	PE-1	PL-1	PS-1	RA-1	SA-1	SC-1	SI-1
★	AC-2	AT-2	AU-2	CA-2	CM-2	CP-2	★ IA-2	IR-2	MA-2	MP-2	★ PE-2	PL-2	PS-2	RA-2	SA-2	SC-2	★ SI-2
	AC-2(1)	AT-2(2)	AU-2(3)	CA-2(1)	CM-2(1)	CP-2(1)	IA-2(1)	IR-3	MA-3	MP-3	★ PE-3	PL-2(3)	PS-3	RA-3	SA-3	SC-4	SI-2(2)
	AC-2(2)	AT-3	AU-3	CA-3	CM-2(3)	CP-2(3)	IA-2(2)	IR-3(2)	MA-3(1)	MP-4	PE-4	PL-4	PS-4	RA-5	SA-4	SC-5	★ SI-3
	AC-2(3)	AT-4	AU-3(1)	CA-3(5)	CM-2(7)	CP-2(8)	IA-2(3)	IR-4	MA-3(2)	MP-5	PE-5	PL-4(1)	PS-5	RA-5(1)	SA-4(1)	★ SC-7	SI-3(1)
	AC-2(4)		AU-4	CA-5	CM-3	CP-3	IA-2(8)	IR-4(1)	MA-4	MP-5(4)	PE-6	PL-8	PS-6	RA-5(2)	SA-4(2)	★ SC-7(3)	SI-3(2)
★	AC-3		AU-5	CA-6	CM-3(2)	CP-4	IA-2(9)	IR-5	MA-4(2)	★ MP-6	PE-6(1)		PS-7	RA-5(5)	SA-4(9)	SC-7(4)	SI-4
	AC-4		AU-6	CA-7	CM-4	CP-4(1)	IA-2(11)	IR-6	MA-5	MP-7	PE-8		PS-8		SA-4(10)	SC-7(5)	SI-4(2)
	AC-5		AU-6(1)	CA-7(1)	CM-5	CP-6	IA-2(12)	IR-6(1)	MA-6	MP-7(1)	PE-9				SA-5	SC-7(7)	SI-4(4)
	AC-6		AU-6(3)	CA-9	CM-6	CP-6(1)	★ IA-3	IR-7			PE-10				SA-8	SC-8	SI-4(5)
	AC-6(1)		AU-7		CM-7	CP-6(3)	IA-4	IR-7(1)			PE-11				SA-9	SC-8(1)	SI-5
	AC-6(2)		AU-7(1)		CM-7(1)	CP-7	★ IA-5	IR-8			PE-12				SA-9(2)	SC-10	SI-7
	AC-6(5)		AU-8		CM-7(2)	CP-7(1)	IA-5(1)				PE-13				SA-10	SC-12	SI-7(1)
	AC-6(9)		AU-8(1)		CM-7(4)*	CP-7(2)	IA-5(2)				PE-13(3)				SA-11	SC-13	SI-7(7)
	AC-6(10)		AU-9		CM-7(5)*	CP-7(3)	IA-5(3)				PE-14					SC-15	SI-8
	AC-7		AU-9(4)		CM-8	CP-8	IA-5(11)				PE-15					SC-17	SI-8(1)
	AC-8		AU-11		CM-8(1)	CP-8(1)	IA-6				PE-16					SC-18	SI-8(2)
	AC-11		AU-12		CM-8(3)	CP-8(2)	IA-7				PE-17					SC-19	SI-10
	AC-11(1)				CM-8(5)	CP-9	IA-8									SC-20	SI-11
	AC-12				CM-9	CP-9(1)	IA-8(1)									SC-21	SI-12
	AC-14				CM-10	CP-10	IA-8(2)									SC-22	SI-16
★	AC-17				CM-11	CP-10(2)	IA-8(3)									SC-23	
	AC-17(1)						IA-8(4)									SC-28	
	AC-17(2)															SC-39	
	AC-17(3)																
	AC-17(4)																
	AC-18																
	AC-18(1)																
	AC-19																
	AC-19(5)																
★	AC-20																
★	AC-20(1)																
	AC-20(2)																
	AC-21																
★	AC-22																
Count	28	3	13	3	13	1	11	6	6	8	6	1	3	3	1	15	5

- In-Scope (MITRE)
- Not In-Scope
- SP 800-171
- CMMC Level 1



68% of MITRE's mappings stem from just 16 controls in NIST SP 800-53r4

NIST SP 800-53r4 controls with at least 100 ATT&CK v12.1 technique mappings

Control	Techniques	Total	SP 800-53 Moderate	SP 800-171	CMMC L1
SI-4	350	7.19%	✓	✓	✗
CM-6	326	6.70%	✓	✓	✗
CM-2	259	5.32%	✓	✓	✗
AC-3	251	5.16%	✓	✓	✓
AC-6	240	4.93%	✓	✓	✗
SI-3	208	4.28%	✓	✓	✓
CM-7	207	4.25%	✓	✓	✗
CA-7	202	4.15%	✓	✓	✗
AC-2	194	3.99%	✓	✓	✓
SI-7	190	3.91%	✓	✗	✗
IA-2	166	3.41%	✓	✓	✓
AC-5	162	3.33%	✓	✓	✗
SC-7	148	3.04%	✓	✓	✓
CM-5	147	3.02%	✓	✓	✗
AC-4	145	2.98%	✓	✓	✗
RA-5	106	2.18%	✓	✓	✗
	3,301	68%			



About NIST SP 800-172 and CMMC Level 3...



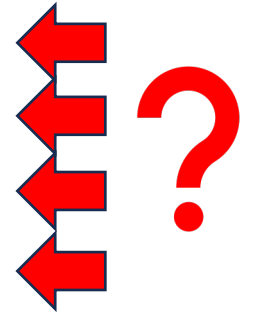
NIST SP 800-172: 66 "enhancements" representing 75 new controls

CMMC Level 3: 24 requirements representing 46/75 of those new controls

Family	AC	AT	AU	CA	CM	CP	IA	IR	MA	MP	PE	PL	PS	RA	SA	SC	SI
	AC-1	AT-1	AU-1	CA-1	CM-1	CP-1	IA-1	IR-1	MA-1	MP-1	PE-1	PL-1	PS-1	RA-1	SA-1	SC-1	SI-1
	★ AC-2	AT-2	AU-2	CA-2	CM-2	CP-2	★ IA-2	IR-2	MA-2	MP-2	★ PE-2	PL-2	PS-2	RA-2	SA-2	SC-2	★ SI-2
	AC-2(1)	AT-2(2)	AU-2(3)	CA-2(1)	CM-2(1)	CP-2(1)	IA-2(1)	IR-3	MA-3	MP-3	★ PE-3	PL-2(3)	PS-3	RA-3	SA-3	★ SC-3	SI-2(2)
	AC-2(2)	★ AT-2(1)	AU-3	★ CA-3	★ CM-2(2)	CP-2(3)	IA-2(2)	IR-3(2)	MA-3(1)	MP-4	PE-4	PL-4	PS-4	★ RA-3(1)	SA-4	SC-4	★ SI-3
	AC-2(3)	★ AT-2(3)	AU-3(1)	CA-3(5)	CM-2(3)	CP-2(8)	IA-2(3)	IR-4	MA-3(2)	MP-5	PE-5	PL-4(1)	PS-5	★ RA-3(3)	SA-4(1)	SC-5	★ SI-3(1)
	AC-2(4)	★ AT-2(4)	AU-4	CA-5	CM-2(7)	CP-3	IA-2(8)	IR-4(1)	MA-4	MP-5(4)	PE-6	★ PL-8	PS-6	★ RA-3(4)	SA-4(2)	★ SC-7	SI-3(2)
	★ AC-3	★ AT-2(5)	AU-5	CA-6	CM-3	CP-4	IA-2(9)	★ IR-4(11)	MA-4(2)	★ MP-6	PE-6(1)		PS-7	RA-5	SA-4(9)	SC-7(3)	SI-4
	★ AC-3(2)	★ AT-2(6)	AU-6	CA-7	CM-3(2)	CP-4(1)	IA-2(11)	★ IR-4(14)	MA-5	★ MP-6(7)	PE-8		PS-8	RA-5(1)	SA-4(10)	SC-7(4)	SI-4(2)
	AC-4	AT-3	AU-6(1)	CA-7(1)	★ CM-3(5)	CP-6	IA-2(12)	IR-5	MA-6	MP-7	PE-9			RA-5(2)	SA-5	SC-7(5)	SI-4(4)
	★ AC-4(1)	AT-4	AU-6(3)	★ CA-8	★ CM-3(8)	CP-6(1)	★ IA-3	IR-6		MP-7(1)	PE-10			RA-5(5)	SA-8	SC-7(7)	SI-4(5)
	★ AC-4(6)	★ AT-6	AU-6(6)	CA-9	CM-4	CP-6(3)	★ IA-3(1)	IR-6(1)			PE-11			★ RA-10	SA-9	★ SC-7(13)	SI-4(7)
	★ AC-4(8)		AU-7		CM-5	CP-7	★ IA-3(4)	IR-7			PE-12				SA-9(2)	★ SC-7(21)	SI-4(11)
	★ AC-4(12)		AU-7(1)		CM-5(4)	CP-7(1)	IA-4	IR-7(1)			PE-13				SA-10	★ SC-7(22)	SI-4(13)
	★ AC-4(13)		AU-8		CM-6	CP-7(2)	★ IA-5	IR-8			PE-13(3)				SA-11	SC-8	SI-4(18)
	★ AC-4(15)		AU-8(1)		CM-7	CP-7(3)	IA-5(1)				PE-14				SA-17	SC-8(1)	SI-4(19)
	AC-5		AU-9		CM-7(1)	CP-8	IA-5(2)				PE-15				SA-17(9)	SC-8(4)	SI-4(20)
	AC-6		AU-9(4)		CM-7(2)	CP-8(1)	IA-5(3)				PE-16			★ SA-21	SC-10	SC-10	★ SI-4(22)
	AC-6(1)		AU-9(5)		CM-7(4)*	CP-8(2)	IA-5(11)				PE-17					SC-12	★ SI-4(24)
	AC-6(2)		AU-11		CM-7(5)*	CP-9	IA-5(18)									SC-13	SI-5
	AC-6(5)		AU-12		CM-8	CP-9(1)	IA-6									SC-15	SI-7
	AC-6(9)				CM-8(1)	CP-9(7)	IA-7									SC-17	★ SI-7(6)
	AC-6(10)				★ CM-8(2)	CP-10	IA-8									SC-18	SI-7(1)
	AC-7				★ CM-8(3)	CP-10(2)	IA-8(1)									SC-19	SI-7(7)
	AC-8				CM-8(5)		IA-8(2)									SC-20	★ SI-7(9)
	AC-11				CM-9		IA-8(3)									SC-21	★ SI-7(10)
	AC-11(1)				CM-10		IA-8(4)									SC-22	SI-8
	AC-12				CM-11											SC-23	SI-8(1)
	AC-14															★ SC-25	SI-8(2)
	★ AC-17															SC-26	SI-10
	AC-17(1)															SC-27	SI-11
	AC-17(2)															SC-28	SI-12
	AC-17(3)															SC-28(2)	SI-14
	AC-17(4)															SC-29	★ SI-14(1)
	AC-18															SC-29(1)	SI-14(2)
	AC-18(1)															SC-30	SI-14(3)
	AC-19															SC-30(2)	SI-16
	AC-19(5)															SC-30(3)	SI-20
	★ AC-20															SC-39	
	★ AC-20(1)															SC-47	
	AC-20(2)															★ SC-49	
	★ AC-20(3)																
	AC-21																
	★ AC-22																
Count	8	6	2	2	6	1	3	2	0	1	0	1	0	4	3	16	16

- ★ PM-16
- ★ PM-16(1)
- ★ SR-2
- ★ SR-6(1)

- ★ CMMC Level 1
- ★ CMMC Level 3
- SP 800-171
- SP 800-172



Key Takeaways



Key Takeaways

- Industry:
 - Cross-reference NIST SP 800-53 – important elements have been tailored out
 - Leverage the details in MITRE ATT&CK to tune your control implementations
 - Participate in the SP 800-172 revision process (ETA: 2H 2024)
 - Should security requirements be tailored based on their mapping to MITRE ATT&CK?



Key Takeaways

- NIST:
 - Is it time to overhaul the SP 800-53 baselines to create more effective starting points?
 - MITRE's analysis appears to fundamentally disagree with the nature of data confidentiality threat mitigation - SP 800-171r4 needs to expand to match the threat
 - SP 800-171 contains the “federal perspective” and the “nonfederal perspective” - it's time to include the adversary perspective



Key Takeaways

- DoD:
 - Will CMMC Level 3 ever match the rhetoric about APTs?
 - DC3/DCISE: quarterly DIB CS advisories need to contain the top MITRE ATT&CK techniques and their relevant mitigating controls (please make these public)
 - Industry: You absolutely need to participate in the DIB CS program in order to make the security control baselines more effective over time

