REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

The public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden, to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.
PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
06/16/2023	Conference Briefing	

4. TITLE AND SUBTITLE

MITRE FiGHT: Ensuring a Secure & Resilient 5G

5a. CONTRACT NUMBER

W56KGU-18-D-0004

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Michaela Vanderveen

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

The MITRE Corporation
7515 Colshire Drive
McLean, VA 22102

8. PERFORMING ORGANIZATION REPORT NUMBER

PRS-23-1945

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Under Secretary of Defense for Research and Engineering

10. SPONSOR/MONITOR'S ACRONYM(S)

USD(R&E)

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

By applying a comprehensive 5G Threat Framework to specific use cases and architectures, we can quantify risks and prioritize mitigations to ensure 5G can revolutionize with minimum compromise. Five-G Hierarchy of Threats (FiGHT) Philosophy:

§ A threat model that documents adversary behaviors relevant to 5G

§ Leverages concepts from ATT&CK but is a separate framework

15. SUBJECT TERMS

Modeling and Simulation; Computer Security, 5G; resilience; cybersecurity; FiGHT; adversary behavior

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE		16	Susan Carpenito
					19b. TELEPHONE NUMBER *(Include area code)* 781-271-7646

MITRE FiGHT™
Ensuring a Secure & Resilient 5G

June 16, 2023

Contact: Michaela Vanderveen
mvanderveen@mitre.org

Approved for Public Release. Case Number 23-1945

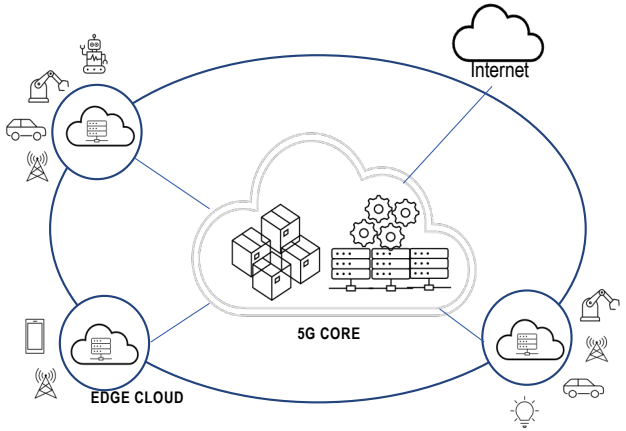
MITRE | SOLVING PROBLEMS FOR A SAFER WORLD™

©2023 THE MITRE CORPORATION. ALL RIGHTS RESERVED. APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED. PUBLIC RELEASE CASE NUMBER 23-1945

5G Security: Perspective and Needs

5G is the most secure cellular system to date. However, security vulnerabilities remain.

- Decoupling of software and hardware/platform requires new and additional security measures
- Auxiliary technologies from the Internet are brought into 5G and their threats inherited
- Complexity of deployments (cloud, physical, hybrid) poses a configuration/responsibility challenge
- Supply Chain risk is increasing. Use of COTS* and Open-source s/w is ubiquitous
- Standards (e.g. 3GPP) leave some controls optional



By applying a comprehensive 5G Threat Framework to specific use cases and architectures, we can quantify risks and prioritize mitigations to ensure 5G can revolutionize with minimum compromise

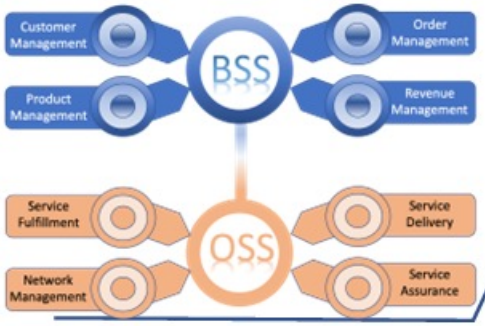
MITRE

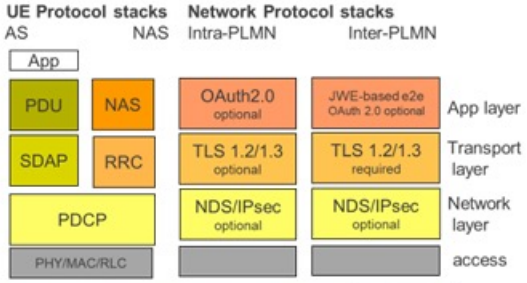
©2023 THE MITRE CORPORATION. ALL RIGHTS RESERVED. APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED. PUBLIC RELEASE CASE NUMBER 23-1949

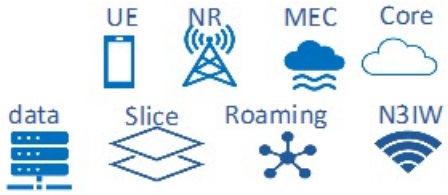
©2023 THE MITRE CORPORATION. ALL RIGHTS RESERVED. FOR INTERNAL and GOV'T USE ONLY.

*Commercial off the Shelf, including hardware, software, Operating Systems, Infrastructure, etc.

5G Complexity: A system of many systems







Complexity is the enemy of security

©2023 THE MITRE CORPORATION. ALL RIGHTS RESERVED. APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED. PUBLIC RELEASE CASE NUMBER 23-1945

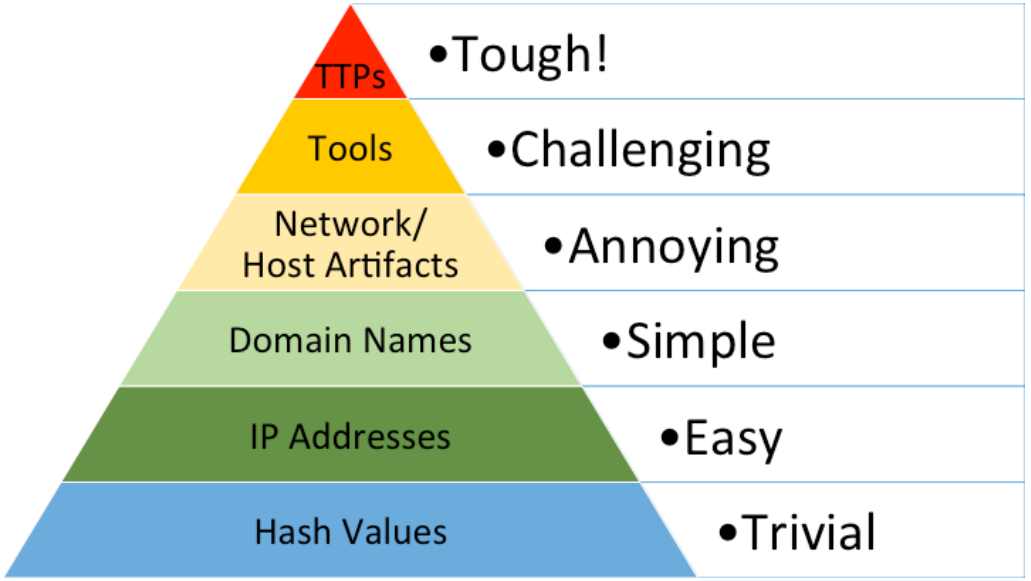
Motivations for a 5G Threat Based Framework

What can the adversary do against your critical assets?

- 5G system well defined: environment bounds adversary operations
- Understanding resulting adversary behavior can inform cyber defense

What can you do against the adversary?

- Reduce the attack surface through various mitigations
- Techniques for hunting and removing adversaries from the network



The Pyramid of Pain by David J Bianco

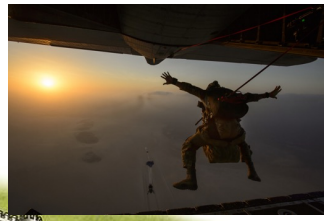
MITRE

©2023 THE MITRE CORPORATION. ALL RIGHTS RESERVED. APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED. PUBLIC RELEASE CASE NUMBER 23-1945

Cybersecurity should be *threat-informed*

Knowledge of my adversary can help me answer…

What do I know about my own strengths and weaknesses?
What do I know about my adversary's capabilities and intent?



Reference: [Engineering-as-a-Moat]

MITRE

©2023 THE MITRE CORPORATION. ALL RIGHTS RESERVED. APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED. PUBLIC RELEASE CASE NUMBER 23-1945

MITRE | Five-G Hierarchy of Threats

FiGHT™ is a threat-based framework to assess the confidentiality, integrity, and availability of our 5G networks, as well as the systems and applications using them.

FiGHT™ leverages concepts from existing security frameworks and builds upon them, incorporating predictive and lab-proven threats to critical 5G assets.

Risk Management

Identification

Assessments
Analysis & Prioritization

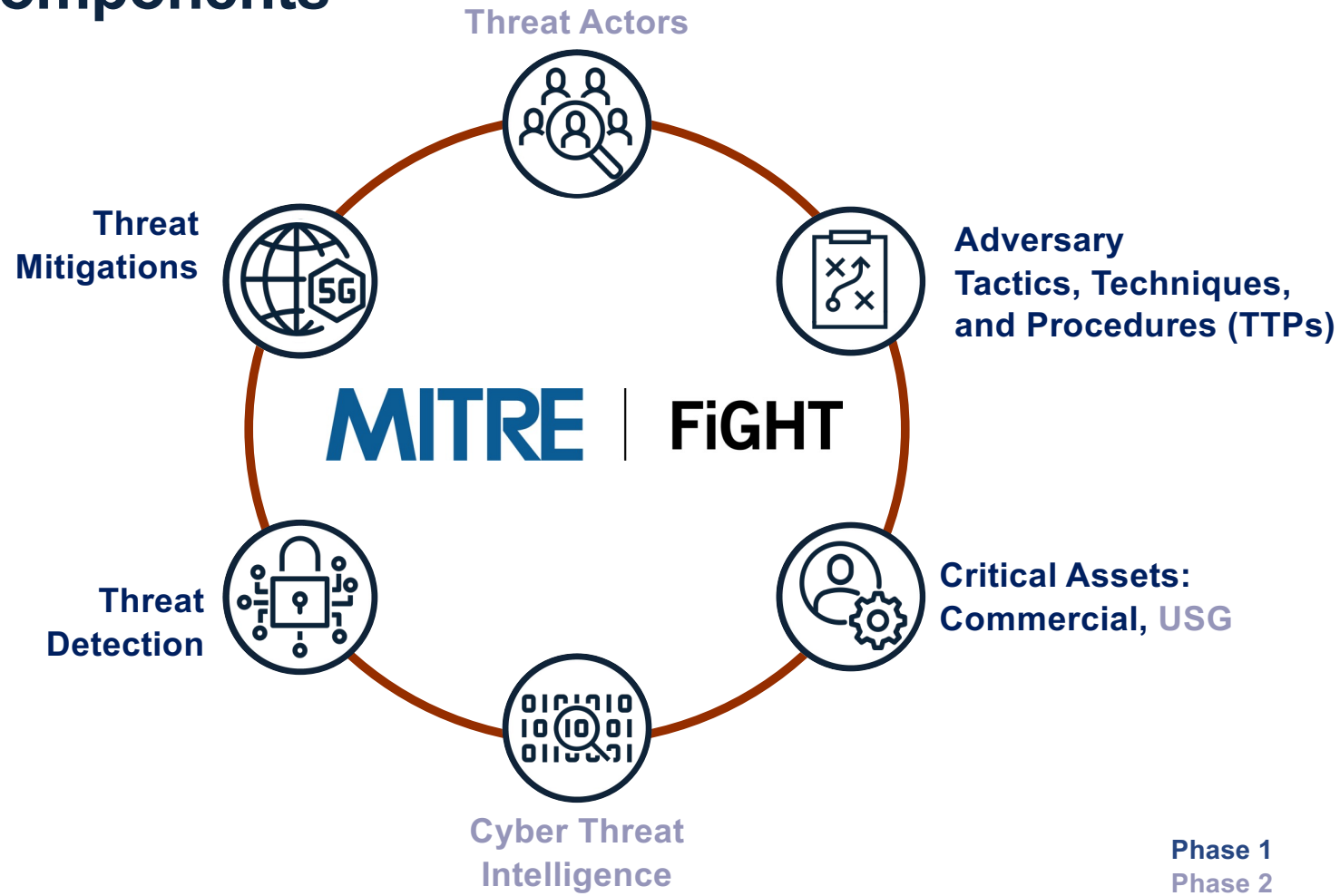
Acquisition planning

Security automation

MITRE

©2023 THE MITRE CORPORATION. ALL RIGHTS RESERVED. APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED. PUBLIC RELEASE CASE NUMBER 23-1945

FiGHT™ Components



Phase 1
Phase 2

MITRE

©2023 THE MITRE CORPORATION. ALL RIGHTS RESERVED. APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED. PUBLIC RELEASE CASE NUMBER 23-1945

FiGHT™ Philosophy

- **A threat model that documents adversary behaviors relevant to 5G**
- **Leverages concepts from ATT&CK but is a separate framework**
- **Sources:**
  - Empirical Observation - adversary behaviors from contributed threat intel.
  - Proof of Concept - adversary behaviors successfully demonstrated in a laboratory setting
  - Predictive - conceptual adversary behaviors not yet demonstrated in a laboratory setting or in the wild
- **Fitting behaviors into a threat model is iterative journey/subject to discussion**

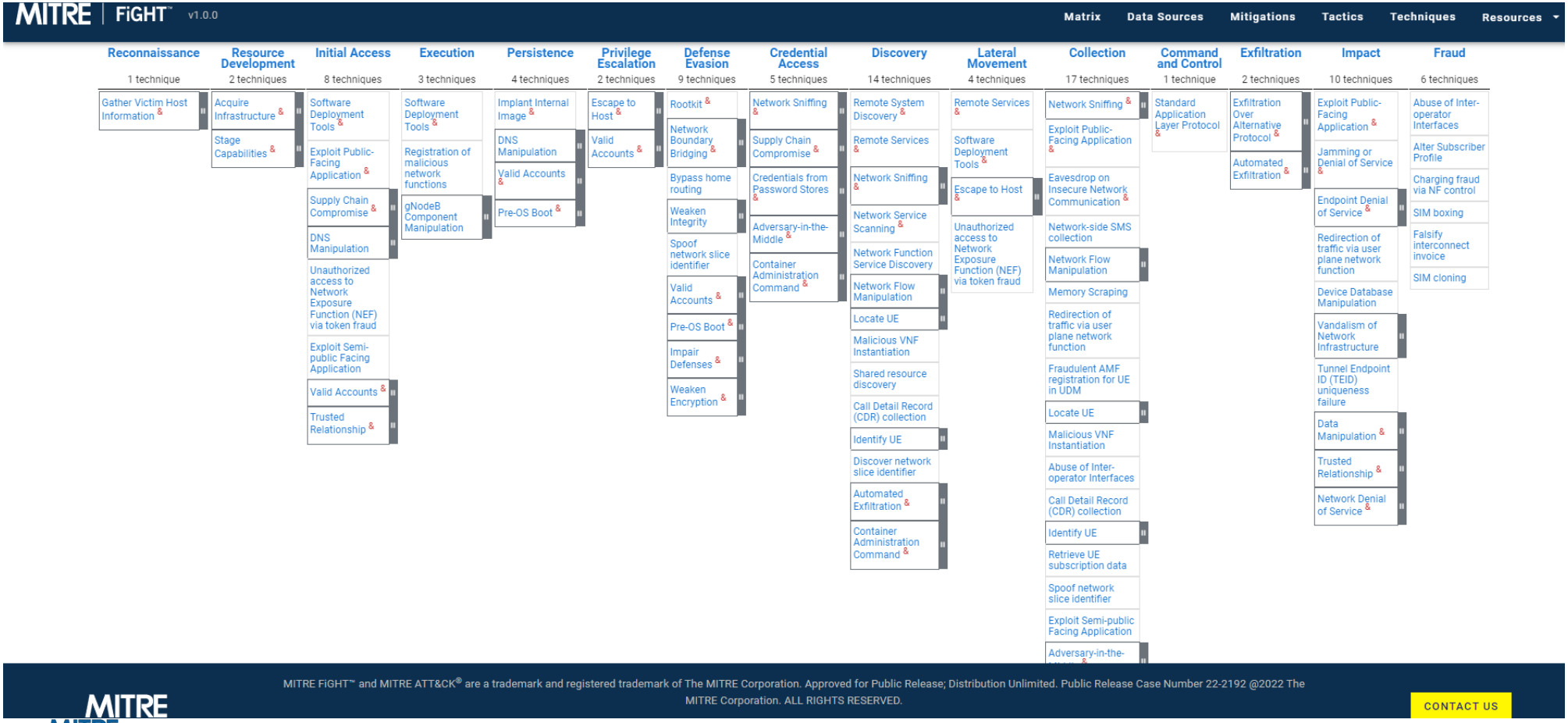
MITRE

©2023 THE MITRE CORPORATION. ALL RIGHTS RESERVED. APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED. PUBLIC RELEASE CASE NUMBER 23-1945

FiGHT™ Matrix

Launched Sept. 2022

https://fight.mitre.org

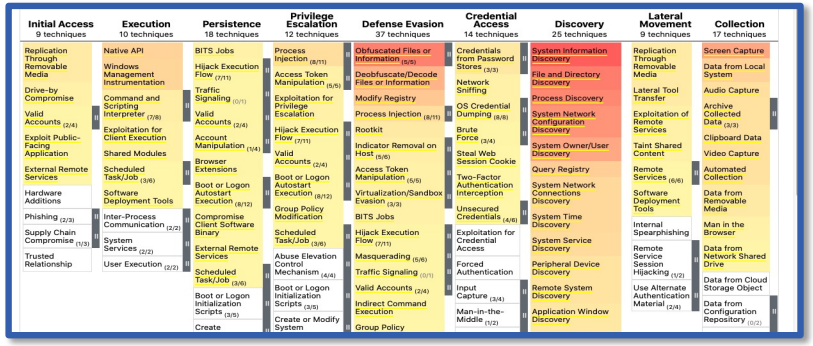


MITRE

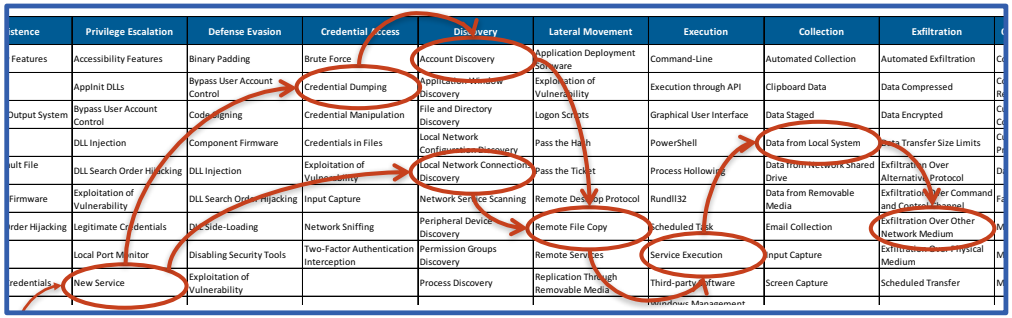
©2023 THE MITRE CORPORATION. ALL RIGHTS RESERVED. APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED. PUBLIC RELEASE CASE NUMBER 23-1945

FiGHT™ can be operationalized

See The Threat



Emulate Adversaries



Develop Analytics

```
#Parse log file for failed login attempts
   failed_attempts=$(grep "authentication failure"
/var/log/auth.log)
# Write failed attempts to log file
  if [ -n "$failed_attempts" ]; then
        echo "$failed_attempts" >> "$log_file"
  fi
```

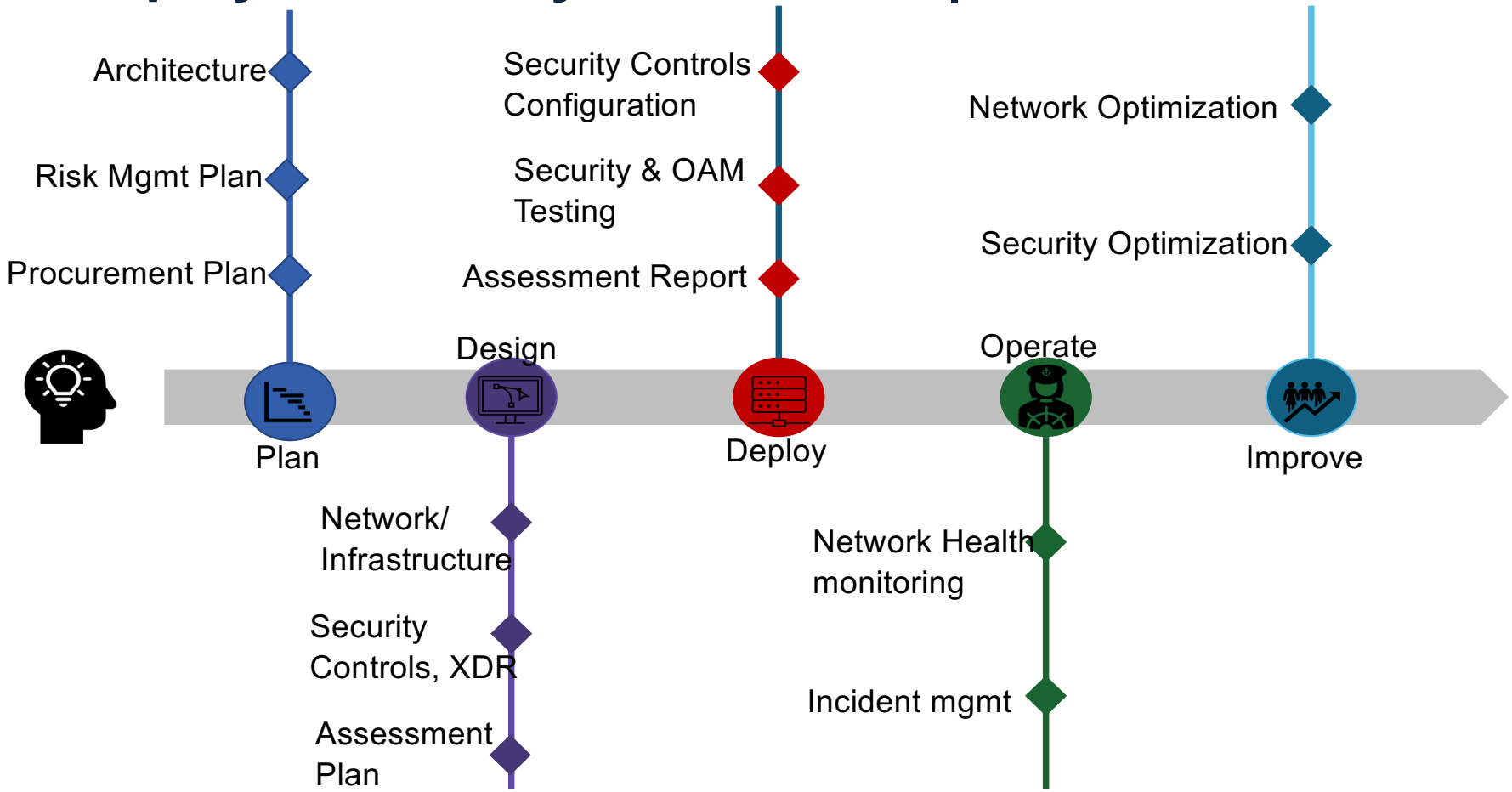
Assess Your Defenses

FiGHT™ can be used to perform threat-informed defense in risk management and operations.

MITRE

©2023 THE MITRE CORPORATION. ALL RIGHTS RESERVED. APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED. PUBLIC RELEASE CASE NUMBER 23-1945

5G Deployment life cycle: FiGHT™ | ATT&CK® informed

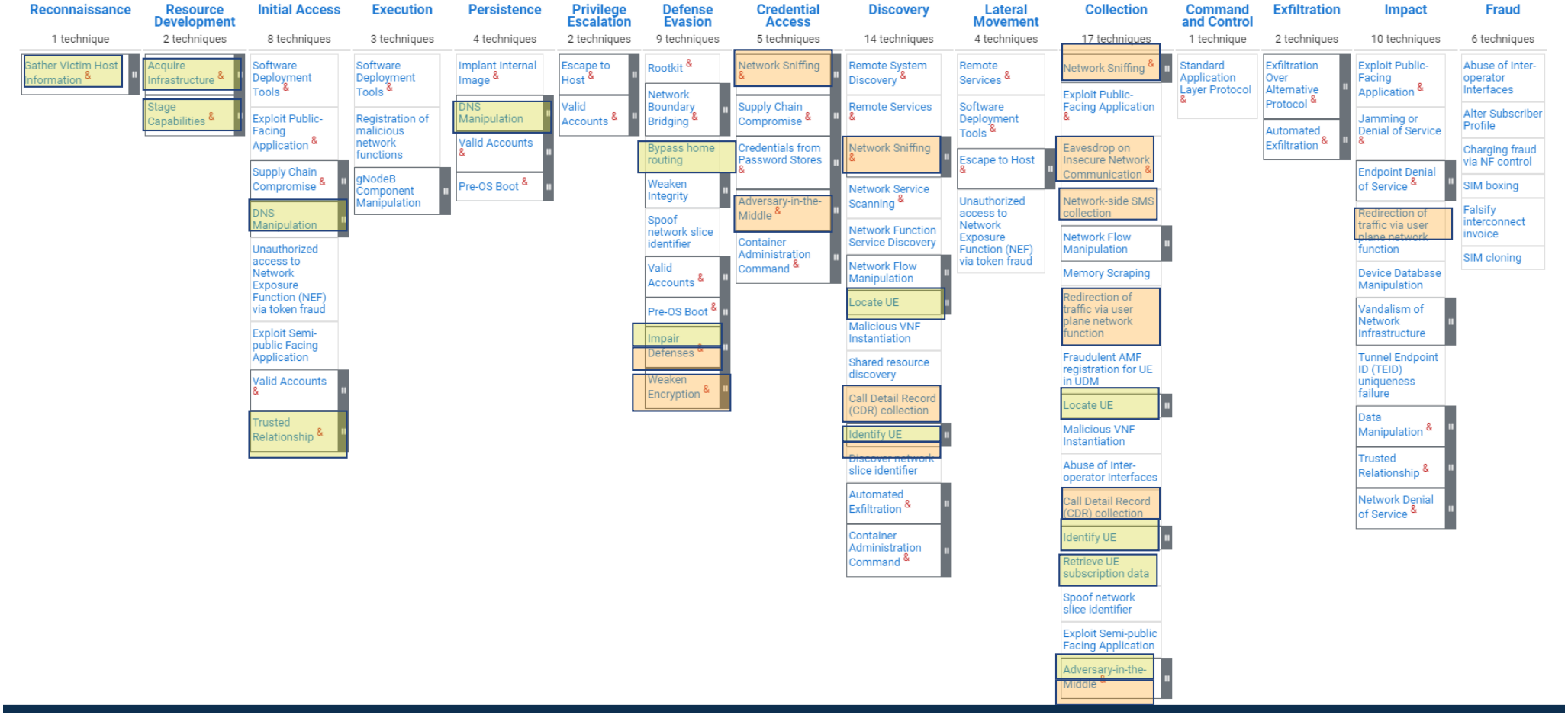


MITRE

©2023 THE MITRE CORPORATION. ALL RIGHTS RESERVED. APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED. PUBLIC RELEASE CASE NUMBER 23-1945

Threats relevant to untrusted commercial deployments
Adversary Goal 1: identify and locate UE; Goal 2: intercept UE communications

Example

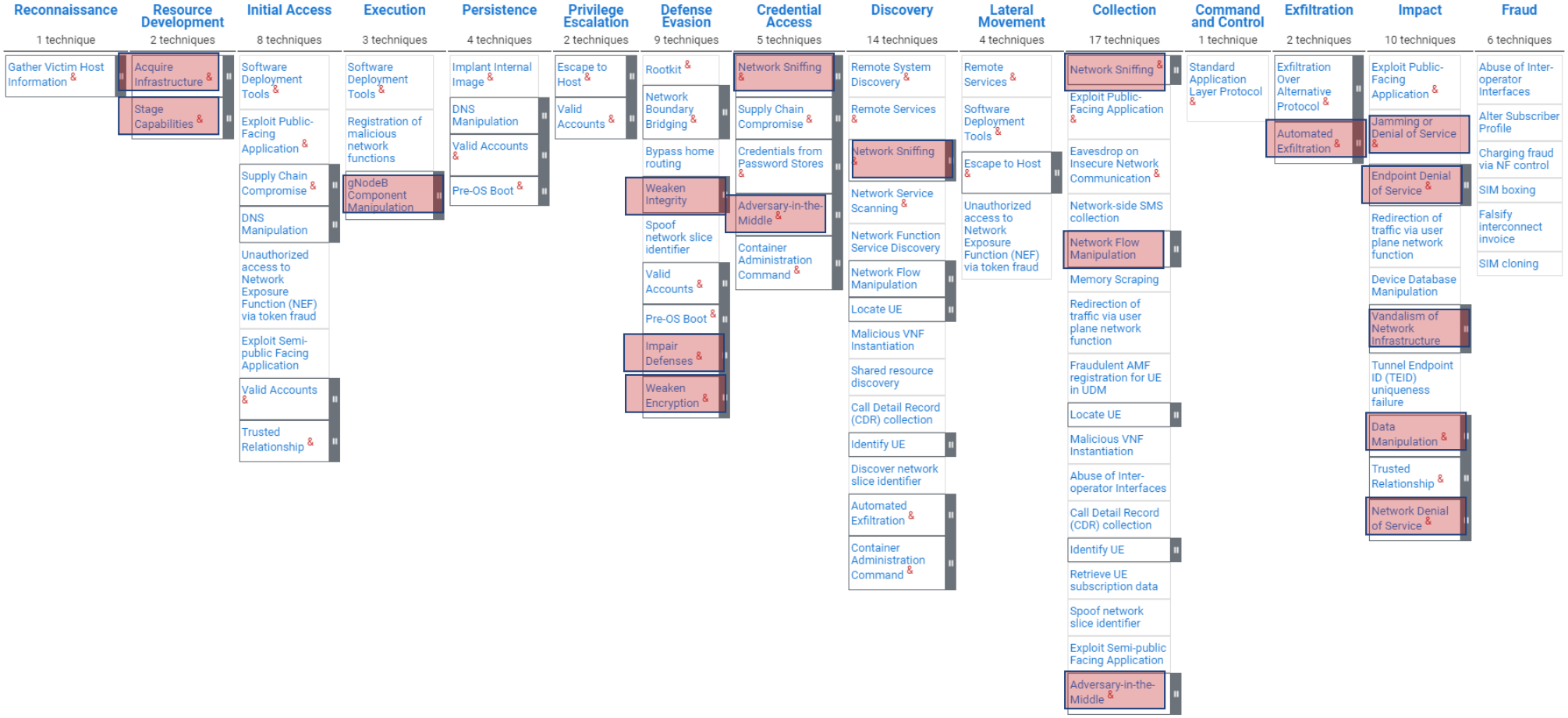


©2023 THE MITRE CORPORATION. ALL RIGHTS RESERVED. APPROVED FOR PUBLIC RELEASE. DISTRIBUTION UNLIMITED. PUBLIC RELEASE CASE NUMBER 23-1945
© 2023 THE MITRE CORPORATION. ALL RIGHTS RESERVED. FOR INTERNAL and GOVT USE ONLY.

Threats relevant tactical deployments

Adversary goal: intercept or disrupt communications

Example



©2023 THE MITRE CORPORATION. ALL RIGHTS RESERVED. APPROVED FOR PUBLIC RELEASE. DISTRIBUTION UNLIMITED. PUBLIC RELEASE CASE NUMBER 23-1945
© 2023 THE MITRE CORPORATION. ALL RIGHTS RESERVED. FOR INTERNAL and GOV'T USE ONLY.

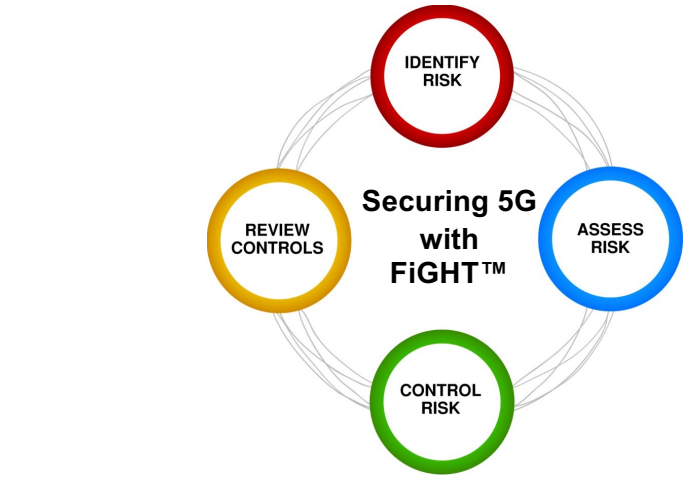
FiGHT Tooling

Tools	Tool Use	Status
FiGHT Pipeline	Creation and editing of the threat model	90% complete
FiGHT Navigator	Visual application of the threat model for scenarios building	80% complete
STIX & TAXII	Intelligence sharing STIX – model TAXII – communication method	70% complete Not started
FiGHT Workbench	User-side editing of the threat model	Not started
FiGHT Flow	Visual modeling of adversary emulation over time	Not started
CALDERA	Automated adversary emulation for red team assessment	Not started

©2023 THE MITRE CORPORATION. ALL RIGHTS RESERVED. APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED. PUBLIC RELEASE CASE NUMBER 23-1945

FiGHT summary - DOD

Ensure that the DOD can design, deploy and manage secure tactical networks, and operate through commercial 5G networks whenever and wherever



Achievements:

- Developed and published threat-based framework https://fight.mitre.org
- Continually modernize/extend capability
- Collaborate with vendors, community (e.g., GSMA)

Goals:

- Lab testing of techniques
- Support/collaborate with government sponsors and operators

Impact:

- Enables to operationalize security hardening detection and mitigation techniques --- to protect DOD assets and communication from adversary activity

Tactical

Untrusted

DOD Enterprise

MITRE

©2023 THE MITRE CORPORATION. ALL RIGHTS RESERVED. APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED. PUBLIC RELEASE CASE NUMBER 23-1949.

©2023 THE MITRE CORPORATION. ALL RIGHTS RESERVED. FOR INTERNAL and GOV'T USE ONLY.

MITRE | FiGHT

fight@mitre.org

https://fight.mitre.org

MITRE | SOLVING PROBLEMS FOR A SAFER WORLD™

©2023 THE MITRE CORPORATION. ALL RIGHTS RESERVED. APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED. PUBLIC RELEASE CASE NUMBER 23-1945