cloud security alliance®

Cloud Adversarial Vectors, Exploits, and Threats (CAVEaT™)

An Emerging Threat Matrix for Industry Collaboration

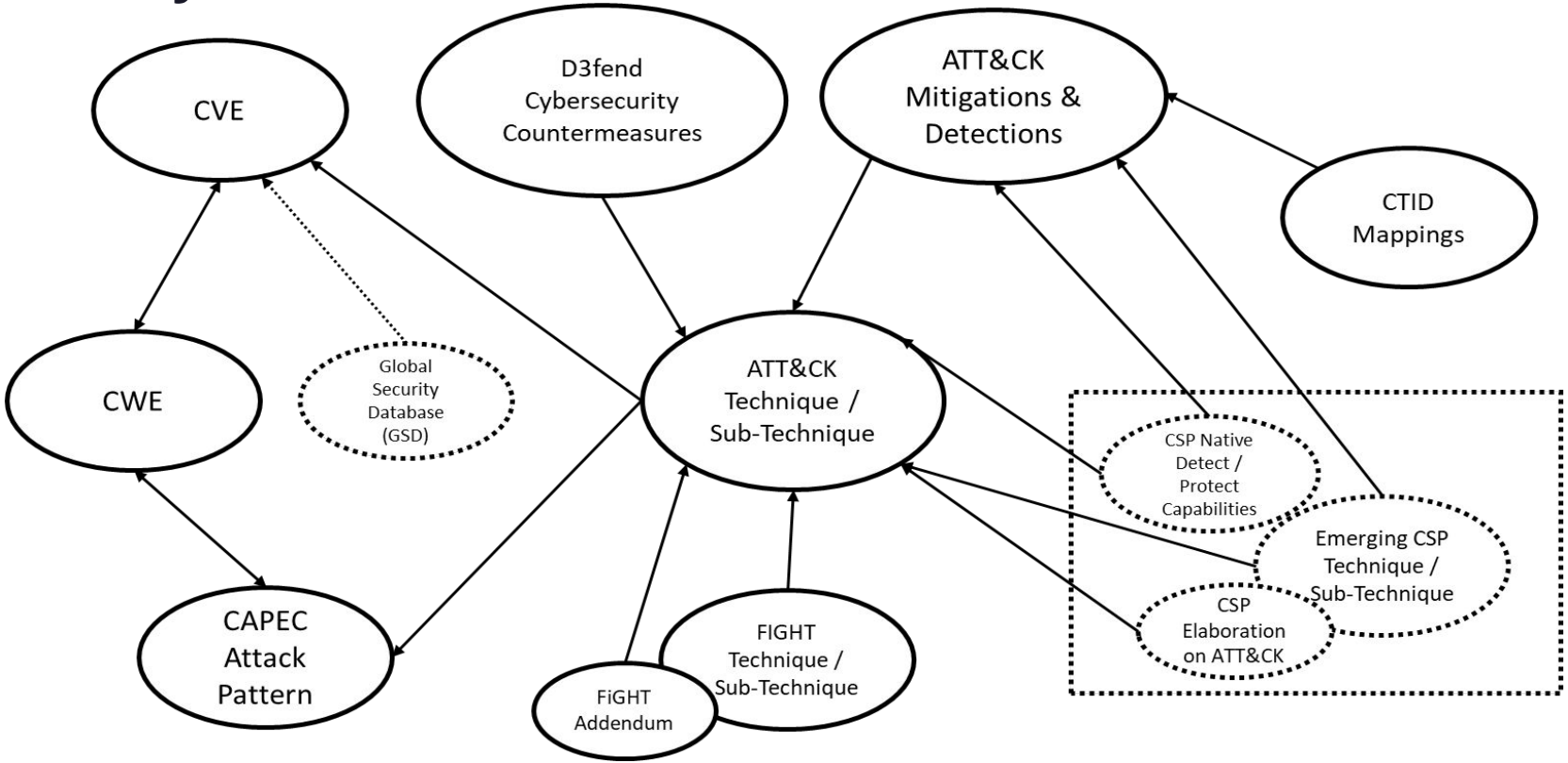
Release Date: 11/21/2023

CAVEaT Working Group

Abstract

Cloud security practitioners agree there's a need for comprehensive threat-informed security guidance to address system assessment, secure design, cyber analytics, and threat mitigation. Due to the rapid development of cloud technologies and service offerings, it is also necessary to develop a forward-looking adversary perspective that identifies emerging cloud service risks along with detailed detections and mitigations for practitioners to implement. The Cloud Security Alliance (CSA) and the MITRE Corporation have established the Cloud Adversarial, Vectors, Exploits, and Threats (CAVEaT™) collaboration to bring relevant content to the cloud security practitioner. This research explores today's available frameworks with relevance to cloud systems and proposes a course of action to advance the state of the art in threat-informed security by collaborating with cloud service providers (CSPs), international security researchers, and key subject matter experts.

Highlights:
Industry Frameworks Available to the CloudSec Practitioner

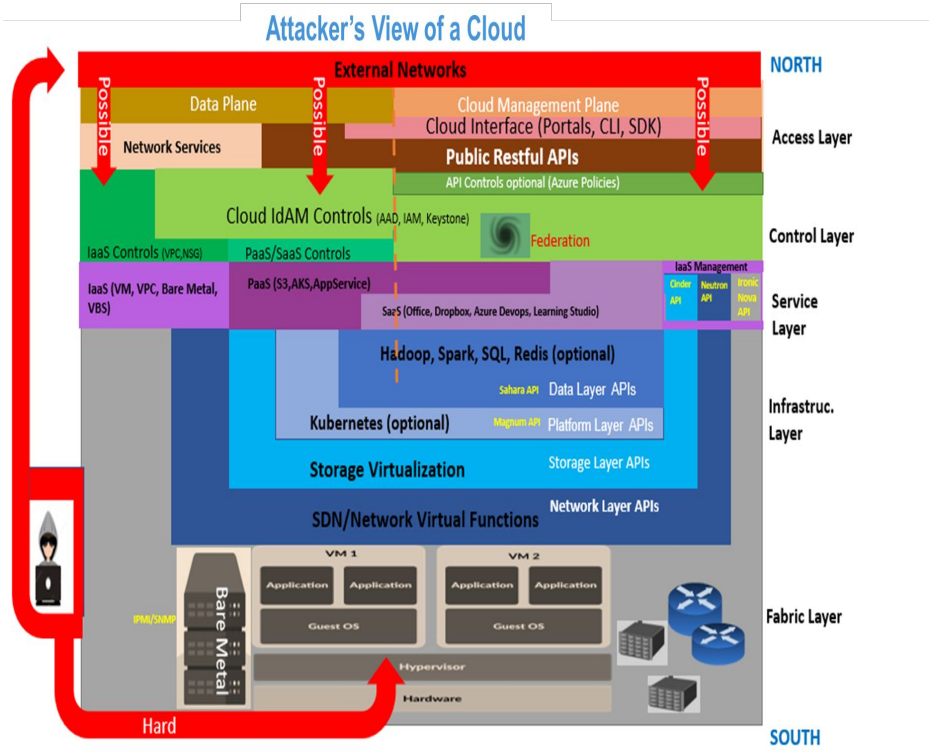


Highlights: Framework Summaries

- **ATT&CK®**: The ATT&CK framework provides the cybersecurity community with an up-to-date knowledge base of adversary behavior based on real-world observations to serve the development of threat models and methodologies.
- **D3FEND™**: Detection, Denial, and Disruption Framework Empowering Network Defense (D3FEND) framework provides the community with an information-dense knowledge graph of cybersecurity countermeasures.
- **CAPEC™**: CAPEC is a method for organizing cyber adversaries' attack patterns to understand how adversaries operate.
- **CVE®**: The Common Vulnerabilities and Exposures (CVE) Program is an international community-based effort that maintains a community-driven, open data registry of publicly known cybersecurity vulnerabilities (CVE List).
- **CWE™**: MITRE's Common Weakness Enumeration (CWE) is a community list of software and hardware weaknesses that identifies the most common and impactful weaknesses.
- **Global Security Database:** The Cloud Security Alliance® (CSA) Global Security Database (GSD) is an emerging framework and knowledgebase for early deep reporting of cloud related and other information technology vulnerabilities.
- **FiGHT™**: The MITRE 5G Hierarchy of Threats (FiGHT) is a curated knowledge base of adversary tactics and techniques that models actual and potential adversary behaviors involved in planning and executing operations against the operators, customers, and suppliers of 5G products, networks, and services.
- **MITRE ATLAS™**: Adversarial Threat Landscape for Artificial-Intelligence (AI) Systems, or ATLAS, is a knowledge base of adversary tactics, techniques, and case studies for machine learning (ML) systems.
- **MITRE Engenuity™ Center for Threat-Informed Defense (CTID) Security Stack Mappings (SSM):** The MITRE CTID SSM repository provides collections of security https://attack.mitre.org/

Cloud Complexity: A system of many systems

- Modern Cloud systems are extremely complex systems of systems built upon multiple layers of technology
- Cloud technology advances much faster than classic enterprise networks
- The complexity and rate of technology advancement is particularly challenging to defenders



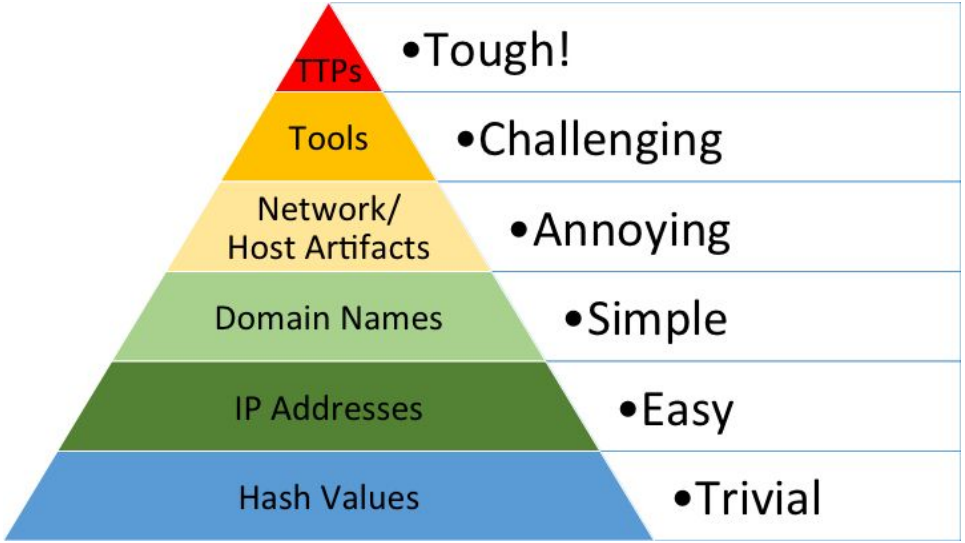
Cybersecurity should be *threat-informed*

What can the adversary do against your critical assets?

- Cloud 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

Forward looking means better planning

- Often, threat frameworks are solely based upon empirical observations of actual adversary behaviors
- Relying upon historical threat data to reduce risk in design and architect their systems is like driving a car while only looking in the rear-view mirror
- Defenders need to be as forward looking as adversaries are, in order to stand a chance in the arms race of cyber security

Forward looking security planning

- Architecting, designing, implementing, testing, and deploying infrastructures take considerable time and effort, even in the cloud

- To be forward looking new threat models are needed that hypothesize what adversaries may do in the future

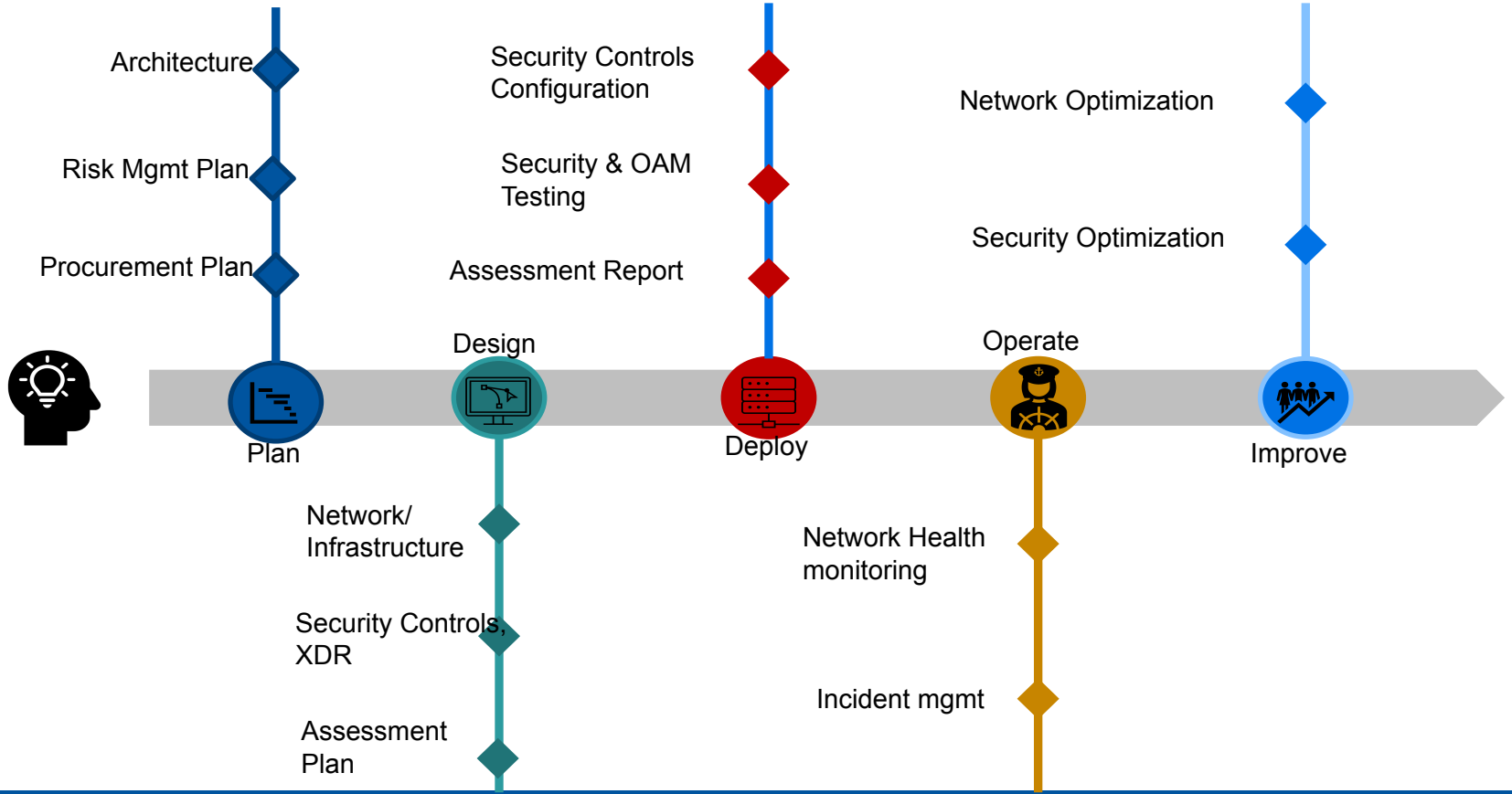
- Based upon prior Cyber Threat Intelligence (CTI) and the latest and greatest technology, we should ask – what might adversaries do here?

CAVEaT – Cloud Adversarial Vectors, Exploits, and Threats

- CAVEaT is a proposed predictive threat model for the cloud that provides robust defensive content for hands-on security practitioners
  - More detailed detections and mitigations that are CSP specific and implementable
  - Built on a MITRE proof of concept

- CAVEaT v1.0 is proposed to be
  - derived from and compatible with MITRE ATT&CK
  - scope adjacent to MITRE ATT&CK
  - CAVEaT is not intended be a substitute for ATT&CK, but rather a compliment and a supplement to it

Cloud life cycle: CAVEAT| ATT&CK® informed



Extending MITRE ATT&CK

MITRE ATT&CK structure

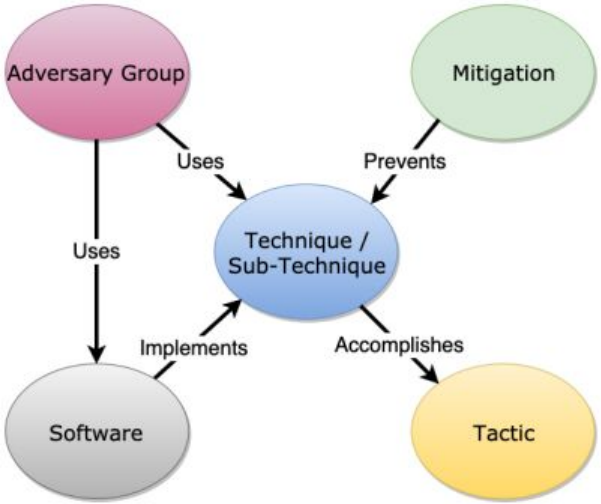
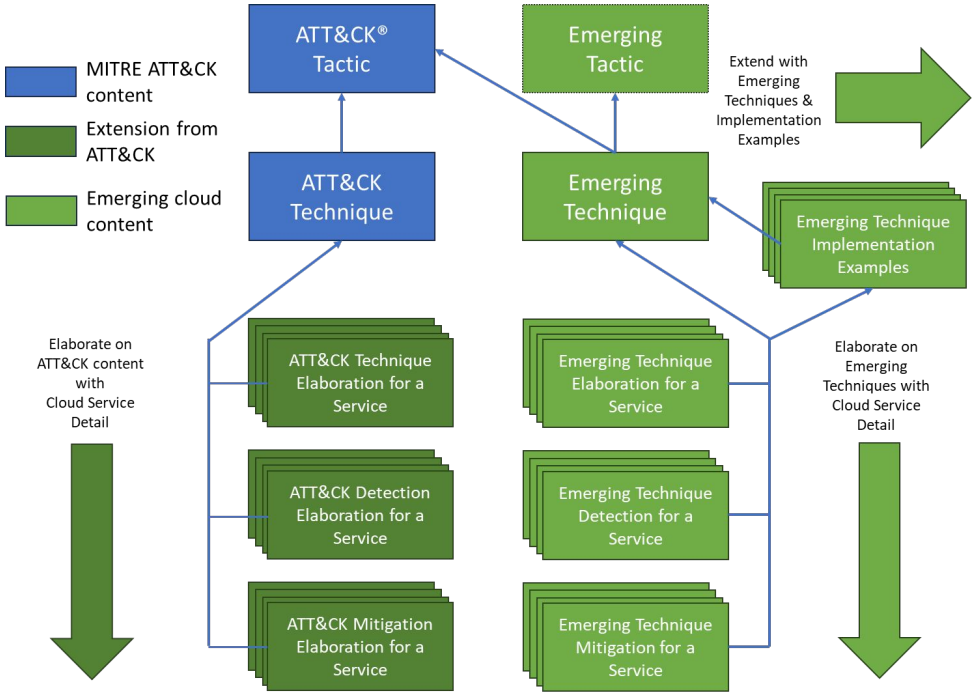


Figure 3. ATT&CK Model Relationships

A proposed CAVEAT structure



Example of an ATT&CK threat model extension

- The MITRE FiGHT Framework is a predictive threat model that is derived from and compatible with ATT&CK
  - https://fight.mitre.org
- The framework has been well received by the 5G and cyber security communities and is being used
  - Several parties have been collaborating with MITRE to improve and expand the model
  - Nokia's 2023 Threat Report used FiGHT to analyze and identify the tactics, techniques and procedures used by LightBasin in the wild
    - https://www.nokia.com/networks/security-portfolio/threat-intelligence-report/
- The FiGHT data formats and software to be released will be fully compatible with the MITRE ATT&CK ecosystem

Recommendations to Improve the Practice of Cloud Security

1. Initiate an industry collaboration promoting open discussion of threats and emerging risks from cloud services.
2. Outline a comprehensive, threat based CSP focused data model to improve mitigation, enhance detection, and improve response.
3. Establish a cloud security industry collaborative content curating body.
4. Establish a rapid/agile program and supporting platform to develop and publish threat-informed cloud security content.

Cloud Adversarial Vectors, Exploits, and Threats (CAVEaT™)

Keywords

ATT&CK, CAPEC, D3FEND, CAVEaT, Threat Modeling, STRIDE, Cyber Kill Chain.

Backstory

This paper is intended to introduce the concept of a emergent cloud technology specific adversarial threat modeling and rapid content acquisition and curation for timely use by cloud security practitioners.

Target Audience

Cloud Security Practitioners
Cloud Service Providers

Sponsors

F5 Inc.,
Vectra AI, Inc.,
The MITRE Corp

The CAVEaT Working Group

- To make CAVEaT happen, the following needs to occur
  - The CAVEaT threat model needs to be finalized
  - New and predictive adversarial behaviors (aka, Techniques) need to be identified and fit to the model
  - For those behaviors, potential detections and mitigations need to be identified
  - Supplement the ATT&CK detections and mitigations with practical procedures
  - Software and data structures need to be developed and released

- After the first release of the model, a sustained and ongoing effort to further develop and curate is necessary
  - Threat frameworks that are not actively developed become useless quickly

Acknowledgements

CSA-DC Chapter Research Committee Chair

- Mari Spina

Contributors

Authors:

- Tim Wade
- Paul Deakin
- Adrian Garcia Gonzalez
- Kerry Long
- Andy Radle
- Eric Arnoth
- Mari Spina

Contributors:

- Robert Marcoux
- Bob Klannukarn
- Rebecca Choynowski
- Oscar Gokce
- Alex Reyes

CSA

- Sean Heide
- Kurt Seifried

Join the CAVEAT Working Group

CSA - Sean Heide
sheide@cloudsecurityalliance.org

Objectives:

- Advance the state and utility CAVEAT
- Peer Supported Curation
- Stakeholder Sharing & Collaboration
- Non-Attribution Reporting
- Confirmed and Hypothetical CloudSec Threats

caveat-leadership@groups.cloudsecurityalliance.org
CAVEAT@cloudsecurityalliance.org