网络空间威胁对抗与防御技术研讨会
暨 第九届安天网络安全冬训营

亂雲飛渡

资源代价与安全算力

威胁框架的新进展

安天 | 研究院

CONTENTS
目 录

01 新内容

版本	时间	内容/结构主要变化
V3	2018.10.23 2019.04.29	分类：Enterprise (All, Linux, macOS, Windows), Pre-, Mobile 企业版战术/技术：战术11 + 技术223 . V1 & V2 已不在MITRE网站 (github)
V4	2019.04.30 2019.07.30	分类：Enterprise (All, Linux, macOS, Windows), Pre-, Mobile 企业版战术/技术：战术12 + 技术244 . 增加了战术“Impact”
V5	2019.07.31 2019.10.23	分类：Enterprise (All, Linux, macOS, Windows), Pre-, Mobile 企业版战术/技术：战术12 + 技术244 . 引入了“缓解”
V6	2019.10.24 2020.03.30	分类：Enterprise (Windows, macOS, Linux, Cloud <AWS, GCP, Azure, Office365, Azure AD, SaaS>), Pre-, Mobile (Android, iOS), ICS 企业版战术/技术：战术12 + 技术266 . 增加了类型“云，工控”， 丰富了技术内容
V7 beta	2020.03.31 2020.07.07	分类：Enterprise (Windows, macOS, Linux, Cloud <AWS, GCP, Azure, Office365, Azure AD, SaaS>), Pre-, Mobile (Android, iOS), ICS . 企业版战术/技术：战术12 + 技术156 + 子技术260 . 技术 细化为“子技术”
V7	2020.07.08 2020.10.26	分类：Enterprise (Windows, macOS, Linux, Cloud <AWS, GCP, Azure, Office365, Azure AD, SaaS>), Pre-, Mobile (Android, iOS), ICS . 企业版战术/技术：战术12 +技术156 + 子技术272 . 形成“子技术”正式版
V8	2020.10.27 2021.04.28	分类：Enterprise (Pre-, Windows, macOS, Linux, Cloud <AWS, GCP, Azure, Office365, Azure AD, SaaS>, Network), Mobile (Android, iOS), ICS . 企业版战术/技术：战术14 +技术178 + 子技术352 统一“Pre-”与“Enterprise”，扩展了战术“侦察，资源开发”，技术内容继续丰富
V9	2021.04.29 2021.10.20	分类：Enterprise (Pre-, Windows, macOS, Linux, Cloud <Office365, Azure AD, Google Workspace, SaaS, IaaS>, Network, Containers), Mobile (Android, iOS), ICS 企业版战术/技术：战术14 +技术185 + 子技术367 . 数据源描述-I，调整云，增加容器，技术内容继续丰富
V10	2021.10.21 n/a	分类：Enterprise (Pre-, Windows, macOS, Linux, Cloud <Office365, Azure AD, Google Workspace, SaaS, IaaS>, Network, Containers), Mobile (Android, iOS), ICS 企业版战术/技术：战术14 +技术188 + 子技术379 . 数据源描述-II，技术内容继续丰富

更新概要

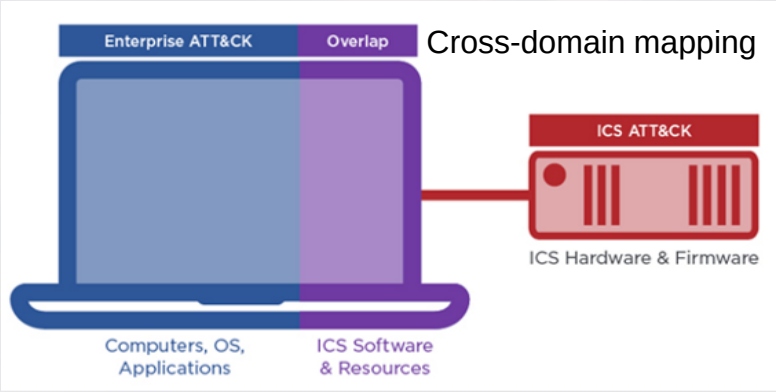
- 总体来看，各个重要更新及其意义
  - 攻击技术分解为攻击子技术（v7，2020）
    将“技术”分解为“子技术”，构建对威胁更为精准的刻画
  - 合并 Pre- 形成企业版战术统一 （v8，2020）
    前摄以识别“潜在的威胁”，并形成对“网空杀伤链”的分析闭环
  - 面向新兴场景 （云.v6 工控.v6 Network.v8 容器.v9 云调整v.9）
    引入云、容器、工控等模型，扩展框架威胁分析的适用范围
  - 重构数据源描述 （v.9 & v.10，2021）
    优化威胁检测的关键环节，推动框架实用易用
  - **子技术 Sub-Technique，数据源/数据组件 DataSource/DataComponent**

更新概要

- V9 更新情况
  - 数据源描述 – 阶段 I
  - 引入 Container 与 Google Workspace
  - 合并 AWS/GCP/Azure 为单一 IaaS
  - 增加了若干新的 技术/子技术，例如
    - Credentials from Password Stores
    - o Password Managers
    - o Windows Credential Manager
  - 修改了若干 技术/子技术，例如
    - Account Discovery
    - o Cloud Account
    - o Email Account
    - o Local Account

更新概要

- V10 更新情况
  - 数据源描述 – 阶段 II
  - 其它模型方面的调整优化
    - 如 ICS 引入“跨越映射”分析
  - 增加了若干新的 技术/子技术，例如
    - 隐藏工件 Hide Artifacts
    - o Hidden Files and Directories
    - o Hidden Users
  - 修改了若干 技术/子技术，例如
    - Compromise Infrastructure
    - o DNS Server
    - o Domains
    - o Server
    - o Virtual Private Server
    - o Web Services

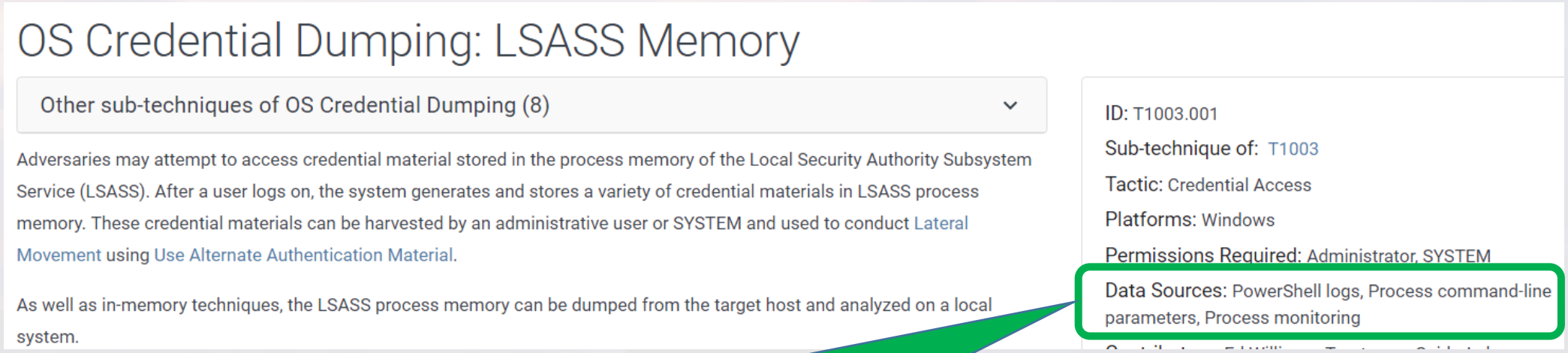


对数据源描述的改进

- 数据源描述的重要性

对数据源描述的改进

- 数据源描述存在的问题（V8，举例）

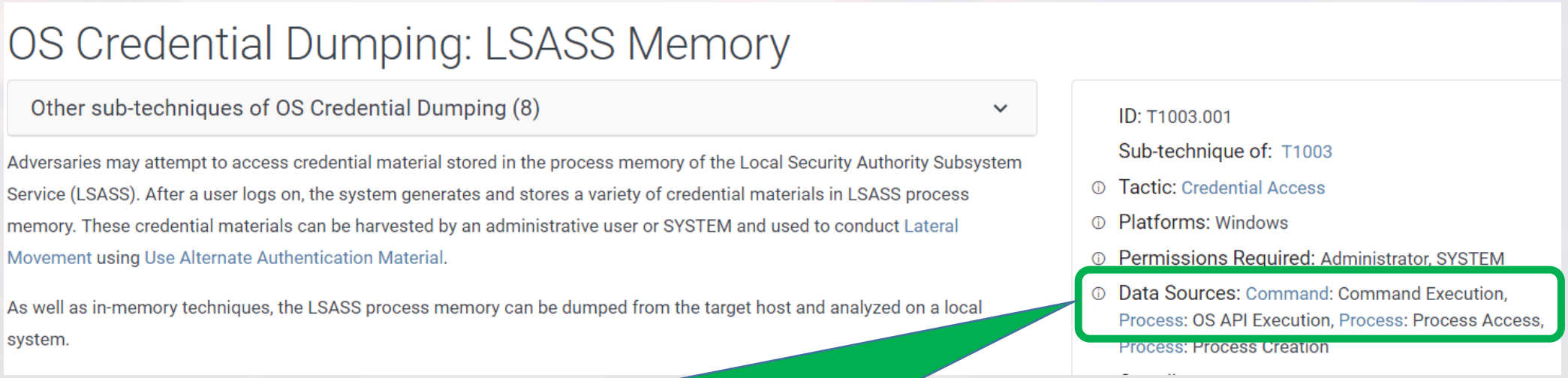


Data Source: PowerShell logs, Process command-line parameters, Process monitoring

从哪里收集数据

对数据源描述的改进

- 数据源描述的改进 - I（V9，举例）



Data Source: Command: Command Execution, Process: OS API Execution, Process: Process Access

“数据源:数据源组件”配对

从哪里收集数据 + 收集哪些数据值

对数据源描述的改进

```yaml
name: Command
definition: A directive given to a computer program, acting as an interpreter of some kind, in order to perform a specific task
collection_layers:
  - Host
  - Container
platforms:
  - Windows
  - Linux
  - macOS
  - Network
  - Containers
contributors:
  - Austin Clark
  - ATT&CK
  - Center for Threat-Informed Defense (CTID)
data_components:
  - name: Command Execution
    type: activity
    description: "Invoking a computer program directive to perform a specific task (ex: Windows EID 4688 of cmd.exe showing command-l
    relationships:
      - source_data_element: user
        relationship: executed
        target_data_element: command
      - source_data_element: process
        relationship: executed
        target_data_element: command
references:
  - https://confluence.atlassian.com/confkb/how-to-enable-command-line-audit-logging-in-linux-956166545.html
  - https://www.scip.ch/en/?labs.20150108
```

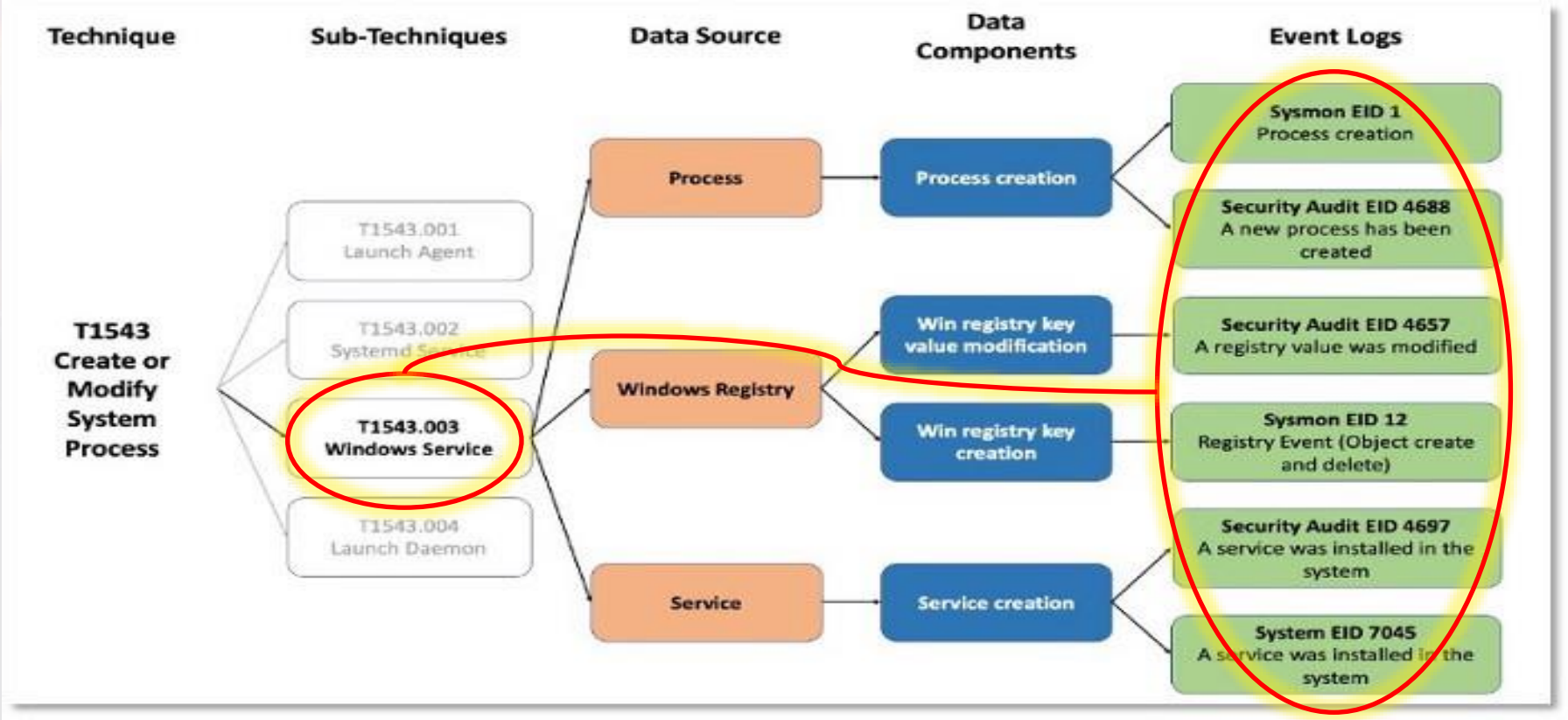
Data Source

Data Component

最终来源所在

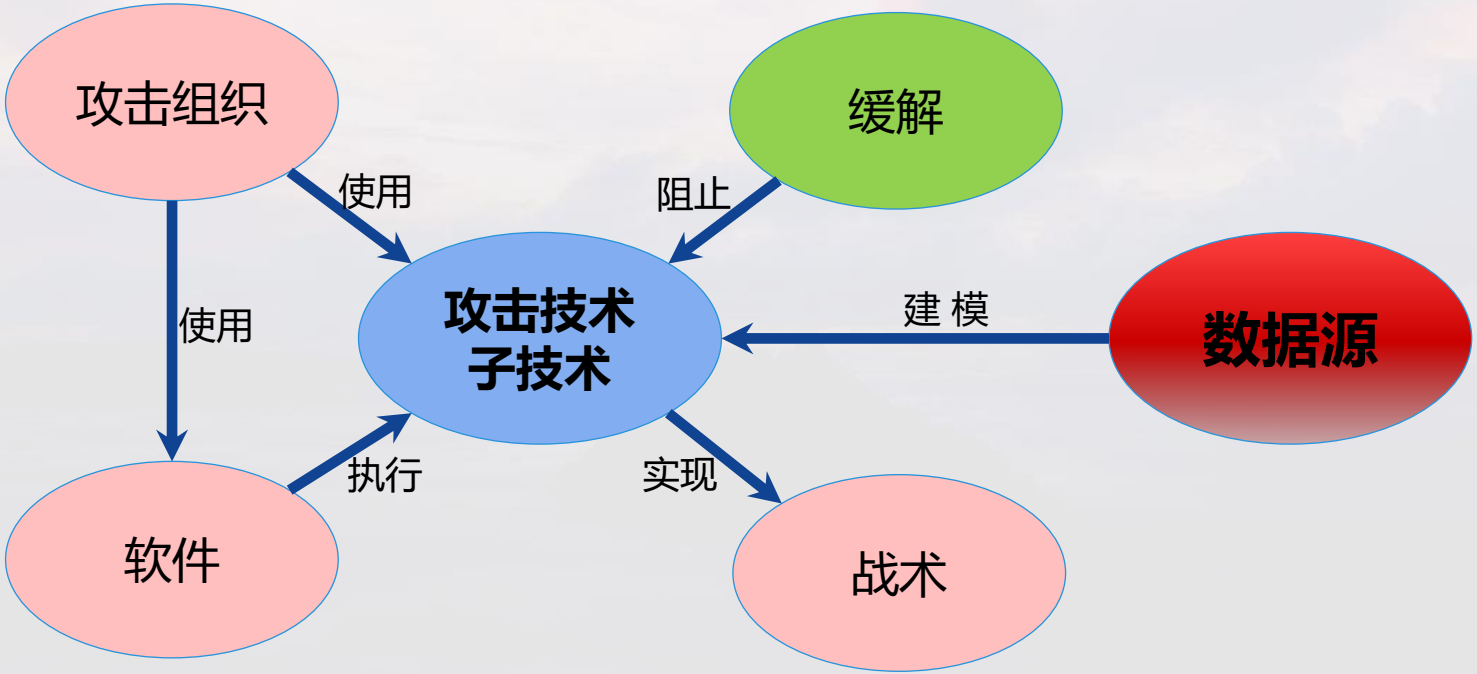
对数据源描述的改进

- 清晰建立“攻击技术检测”与“检测所需最终数据”间的关联



对数据源描述的改进

- 数据源描述的改进 - II（V10）



对数据源描述的改进

Network Traffic

Data transmitted across a network (ex: Web, DNS, Mail, File, etc.), that is either summarized (ex: Netflow) and/or captured as raw data in an analyzable format (ex: PCAP)

ID: DS0029
Platforms: IaaS, Linux, Windows, macOS
Collection Layers: Cloud Control Plane, Host, Network
Contributors: Center for Threat-Informed Defense (CTID); ExtraHop
Version: 1.0
Created: 20 October 2021
Last Modified: 10 November 2021

Live Version

Data Components

Network Traffic: Network Connection Creation

Initial construction of a network connection, such as capturing socket information with a source/destination IP and port(s) (ex: Windows EID 5156, Sysmon EID 3, or Zeek conn.log)

Domain	ID	Name
Enterprise	T1020	Automated Exfiltration
	.001	Traffic Duplication
Enterprise	T1197	BITS Jobs
Enterprise	T1176	Browser Extensions

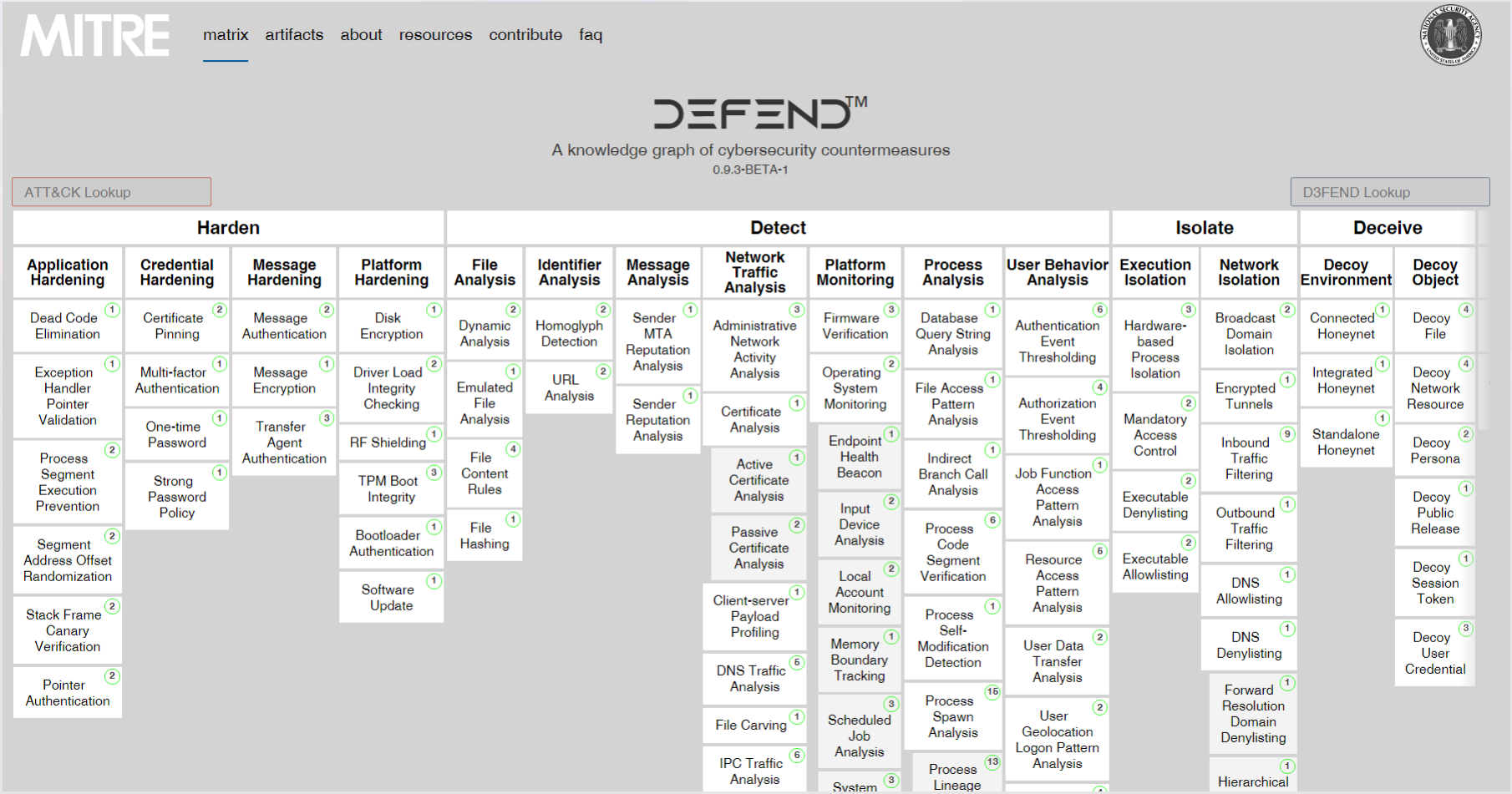
02 新方向

从威胁分析转向防御分析

- 以ATT&CK为基础，进一步构建“防御视角”的分析框架
- 包括：
  - SHIELD，　2020年度
  - **D3FEND，　2021年度**
  - **ENGAGE，　2021年度**

D3FEND

网络安全对策技术的知识图谱，它是防御性网络安全技术以及其与进攻技术关系知识的目录



D3FEND

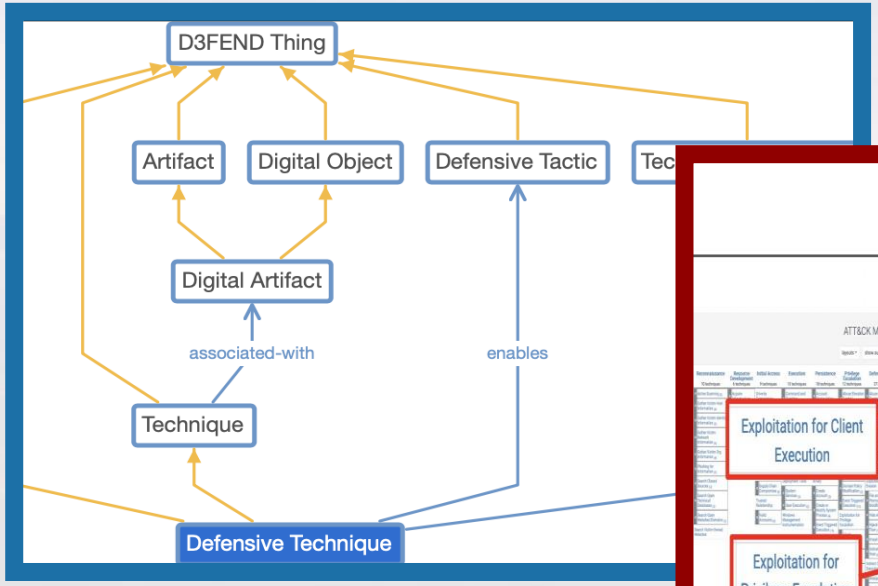
防御战术：Defensive Tactic；防御战术是防御者对对手采取的策略位于知识图谱的第一行

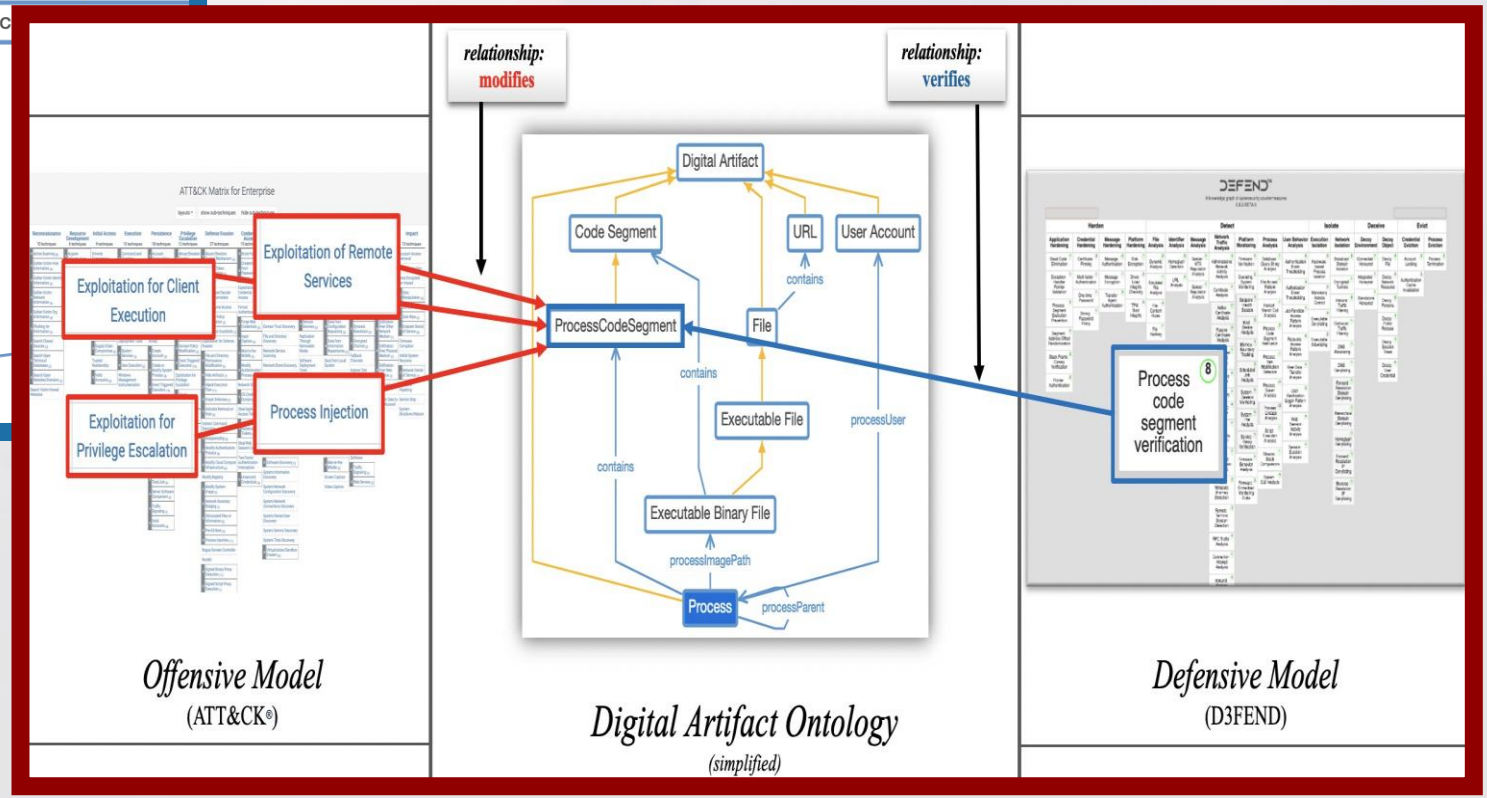
基础技术：Base Techniques；技术是实现战术策略的方法，基础技术位于知识图谱的第二行

防御技术：Defensive Techniques；防御技术是由基础技术派生而来的，是基础技术的具体体现，防御技术位于知识图谱基础技术下面的列中

硬化（Harden）							
应用强化	Application Hardening	凭证强化	Credential Hardening	消息强化	Message Hardening	平台强化	Platform Hardening
死代码消除	Dead Code Elimination	证书固定	Certificate Pinning	消息认证	Message Authentication	磁盘加密	Disk Encryption
异常处理程序指针验证	Exception Handler Pointer Validation	多重身份验证	Multi-factor Authentication	消息加密	Message Encryption	驱动程序负载完整性检查	Driver Load Integrity Checking
流程段执行保护	Process Segment Execution Prevention	一次性密码	One-time Password	传输代理身份验证	Transfer Agent Authenticati	射频屏蔽	RF Shielding
段地址偏移随机化	Segment Address Offset Randomization	强密码策略	Strong Password Policy			TPM引导完整性	TPM Boot Integrity
堆栈帧金丝雀验证	Stack Frame Canary Verification					引导加载程序身份验证	Bootloader Authentication
指针认证	Pointer Authentication					软件更新	Software Update

D3FEND


D3FEND Thing
Artifact
Digital Object
Defensive Tactic
Tec
Digital Artifact
associated-with
enables
Technique
Defensive Technique


relationship:
modifies
relationship:
verifies
ATT&CK Matrix for Enterprise
Exploitation of Remote Services
Exploitation for Client Execution
Process Injection
Exploitation for Privilege Escalation
Digital Artifact
Code Segment
URL
User Account
contains
ProcessCodeSegment
File
contains
Executable File
processUser
contains
Executable Binary File
processImagePath
Process
processParent
DEFEND
Process code segment verification
8
Offensive Model
(ATT&CK®)
Digital Artifact Ontology
(simplified)
Defensive Model
(D3FEND)

Multi-factor Authentication

Definition

ID: D3-MFA (Multi-factor Authentication)

Requiring proof of two or more pieces of evidence in order to authenticate a user.

How it works

When logging into an account users present two or more credentials that fall into different categories: something you know (password or PIN), something you have (smart card or phone), or something you are (fingerprint).

Considerations

MFA configuration steps may vary across accounts and in some cases left up to users to activate and implement.

Digital Artifact Relationships:

This countermeasure technique is related to specific digital artifacts. Click the artifact node for more information.

Multi-factor Authentication authenticates User Account

Related ATT&CK Techniques:

Download ATT&CK Navigator Layer

These mappings are inferred, experimental, and will improve as the knowledge graph grows.

These offensive techniques are determined related because of the way this defensive technique, d3f:Multi-factorAuthentication , authenticates User Account .

Defense Evasion	Initial Access	Persistence	Privilege Escalation
Valid Accounts	Valid Accounts	Valid Accounts	Valid Accounts
Default Accounts	Default Accounts	Default Accounts	Default Accounts
Domain Accounts	Domain Accounts	Domain Accounts	Domain Accounts
Local Accounts	Local Accounts	Local Accounts	Local Accounts
Cloud Accounts	Cloud Accounts	Cloud Accounts	Cloud Accounts
		Account Manipulation	Create Account
		Additional Azure Service Principal Credentials	Local Account

ENGAGE

- 讨论和规划对手交战、欺骗和拒绝活动的框架；目标是挑战控制对手并开始影响时间、地点与交战方式，然后尽可能最大化自己的学习，并拒绝对手的学习；要在防御范围内进一步控制对手，主动在内部网络环境与之互动及抗衡
- **对手交战**（Adversary Engagement）：交战是拒绝和欺骗的结合，以增加对手的网络行动的成本和降低其价值；对手交战的目标是暴露对手及其弱点，了解其能力和意图，并对其施加代价
- **网空拒绝**（Cyber Denial）：拒绝是指防止或损害对手收集情报的能力和努力；拒绝还支持防止或破坏对手实现效果的企图
- **网空欺骗**（Cyber Deception）：开发欺骗性的事实和虚构以误导对手，同时隐瞒关键事实和虚构以防止对手形成正确的估计或采取适当的行动

ENGAGE

Prepare	Expose		Affect			Elicit		Understand
Planning	Collection	Detection	Prevention	Direction	Disruption	Reassurance	Motivation	Analysis
Define Exit Criteria	API Monitoring	Decoy Artifacts and Systems	Baseline	Decoy Artifacts and Systems	Decoy Artifacts and Systems	Application Diversity	Application Diversity	Distill Intelligence
Develop Threat Model	Network Monitoring	Detonate Malware	Hardware Manipulation	Detonate Malware	Isolation	Artifact Diversity	Artifact Diversity	Hotwash
Persona Creation	Software Manipulation	Network Analysis	Isolation	Email Manipulation	Network Manipulation	Burn-In	Detonate Malware	Inform Threat Model
Strategic Goal	System Activity Monitoring		Network Manipulation	Migrate Attack Vector	Software Manipulation	Email Manipulation	Information Manipulation	Refine Operation Activities
Storyboarding			Security Controls	Network Manipulation		Information Manipulation	Personas	
				Peripheral Management		Network Diversity	Network Diversity	
				Security Controls		Peripheral Management		
				Software Manipulation		Pocket Litter		

API Monitoring

Monitor local APIs that might be used by adversary tools and activity.

API Monitoring involves capturing an internal OS function for its usage, accompanying arguments, and result. When a defender captures this information, the data gathered can be analyzed to gain insights into the activity of an adversary at a level deeper than normal system activity monitoring. This type of monitoring can also be used to produce high-fidelity detections. For example, the defender can trace activity through WinSock TCP API functions to view potentially malicious network events or trace usage of the Win32 DeleteFile() function to log all attempts at deleting a given file.

Details

ID: EAC0001
Type: Engagement
Goals: Expose
Approaches: Collection

Whenever an adversary interacts with the environment, their actions reveal vulnerabilities. Defenders can utilize engagement activities to take advantage of such weaknesses.

The following table lists the adversary tactics on the left and the revealed vulnerability on the right that can be exploited by the defender using **API Monitoring**.

ATT&CK® Tactics	Adversary Vulnerability Presented
Discovery	When adversaries interact with the environment or personas, they are vulnerable when they collect, observe, or manipulate system artifacts or information. Manipulated data may cause them to reveal behaviors, use additional or more advanced capabilities against the target, and/or impact their dwell time.
Discovery, Defense Evasion, Execution, Command and Control, Privilege Escalation, Impact, Persistence	When adversaries utilize or abuse system features, software, or other resources, they may be vulnerable to monitoring or Man-in-the-Middle manipulation.
Initial Access, Impact	When adversaries interact with network or system resources, they are vulnerable to triggering tripwires or engaging in easily detectable, anomalous behavior.

Mapping To Initial Access

When an adversary engages in a specific behavior, they are vulnerable to expose an unintended weakness. By looking at each ATT&CK activity, we can examine the weaknesses revealed and identify an engagement activity or activities to exploit this weakness. The following table outlines the Adversary Vulnerabilities and Engagement Activities that are available to the defender when the adversary engages in Initial Access behaviors.

Details

ATT&CK ID: TA0001

ATT&CK® Technique	Adversary Vulnerability	Engagement Activity	Engagement Activity Description
Valid Accounts	When adversaries interact with the environment or personas, they are vulnerable when they collect, observe, or manipulate system artifacts or information. Manipulated data may cause them to reveal behaviors, use additional or more advanced capabilities against the target, and/or impact their dwell time.	Decoy Artifacts and Systems	Introduce impersonations to expand the scope of a deceptive story.
Valid Accounts	When adversaries interact with the environment or personas, they are vulnerable to collecting, or in some way interacting with, manipulated or decoy data. In those cases the data may increase their tolerance for imperfections in the environment and improve the overall believability of the ruse.	Pocket Litter	Place data on a system to reinforce the legitimacy of the system or user.
Valid Accounts	When adversaries interact with the environment or personas, they are vulnerable to collecting, or in some way interacting with, manipulated or decoy data. In those cases the data may increase their tolerance for imperfections in the environment and improve the overall believability of the ruse.	Personas	Create fictitious human user(s) through a combination of planted data and revealed behavior patterns.
Valid Accounts	When adversaries interact with the environment or personas, they are vulnerable to collecting, or in some way interacting with, manipulated or decoy data. In those cases the data may increase their tolerance for imperfections in the environment and improve the overall believability of the ruse.	Burn-In	Exercise a target system in a manner where it will generate desirable system artifacts.

威胁对抗，知攻知防

- **ATT&CK**，支撑对威胁的全面深入分析，以指导攻击者行为描述、检测机制开发以及防御效果测试

知敌方能制敌

- **D3FEND**，提供可用以加固和保护其信息资产的对策信息，探讨了组织应实施的防御性最佳实践

不可胜在己，可胜在敌

- **ENGAGE**，精简了SHIELD，重点放在拒绝、欺骗和对手交战等领域；并着意于交战的战略规划

赋予防御主动性

03 新力量

NIST

- National Institute of Standards and Technology
- 开发网络弹性：一种系统安全工程方法
  SP 800-160 Vol.2 Rev.1 (Draft)，2021/12/09
- 该版本对 ATT&CK 运用的理念
  - 随着关键基础设施的网络攻击态势的愈发严重性，业务弹性和任务弹性才是工业网络安全追求的终极目标
  - 网络弹性在于将弹性措施部署于网络安全防御体系中，以保持最重要业务的持续运营
  - 分析了ATT&CK-TTP (包括ICS) 攻击 OT情况下，对于网络弹性的潜在影响与应对措施
- 基本方法
  - 构建标准化的单一的威胁分类法，基于 ATT&CK 框架
  - 将网络弹性的分析方法与支持措施，映射于ATT&CK 框架的技术与缓解

ATT&CK Technique	Mitigation or Candidate Mitigation	Cyber Resiliency Implementation Approaches	Potential Effects	Cyber Resiliency Controls
Active Scanning (T1595)	Present Deceptive Information (CM1101)	Disinformation	Deceive	SC-30(4)
		Tainting	Detect	SI-20
	Passive Decoys (CM1104)	Misdirection	Di…	SC-26
		Architectural Diver…		SC-30
	Conc… Disc…			…6)
		Obfuscation	Degrade, Exert	SC-28(1), SC-30, SC-30(5)
	Inspect and Analyze Network Traffic (CM2002)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2), SI-4(4)
Gather Victim Host Information (T1592)	Present Deceptive Information (CM1101)	Disinformation	Deceive	SC-30(4)
	Passive Decoys (CM1104)	Misdirection	Divert, Deceive	SC-26
		Architectural Diversity	Divert, Exert	SC-29

Concealment and Misdirection | Misleading Informaton
SC-30隐藏与误导 | (4)误导性信息

CISA

- Cybersecurity and Infrastructure Security Agency
- Best Practices for MITRE ATT&CK® Mapping， June 2021
- 帮助分析师准确、一致地将对手行为映射到相关的ATT&CK 技术——无论分析师是希望将 ATT&CK 纳入网络安全出版物还是对原始数据的分析
- 包括
  - 将 MITRE ATT&CK 映射到报告中
  - 将 MITRE ATT&CK 映射到原始数据

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

映射于CTI报告

1. 找出行为
2. 研究行为
3. 确定策略
4. 识别技术
5. 识别子技术
6. 与其他分析结果对照

映射于原始数据

1. 从数据源开始确定技术和过程
2. 从特定工具或属性开始并扩大范围
3. 从分析开始

小结

- 回顾了2021年度 ATT&CK 框架的内容更新，尤其是数据源描述方面的改进
- 介绍了2021年度新提出 D3FEND和ENGAGE 框架，分析了二者在防御构建中的作用意义
- 简介了 NIST和CISA 权威官方机构对 ATT&CK框架的指导应用

谢谢大家

安天冬训营 wtc.antiy.cn