网络空间威胁对抗与防御技术研讨会
暨 第七届安天网络安全冬训营

网空威胁框架的演进

安天解决方案中心

威胁框架：认知与实践

寒夜远征

寒夜远征

CONTENTS

目录

寒夜速记

威胁框架：认知与实践

01 威胁框架的发展历程

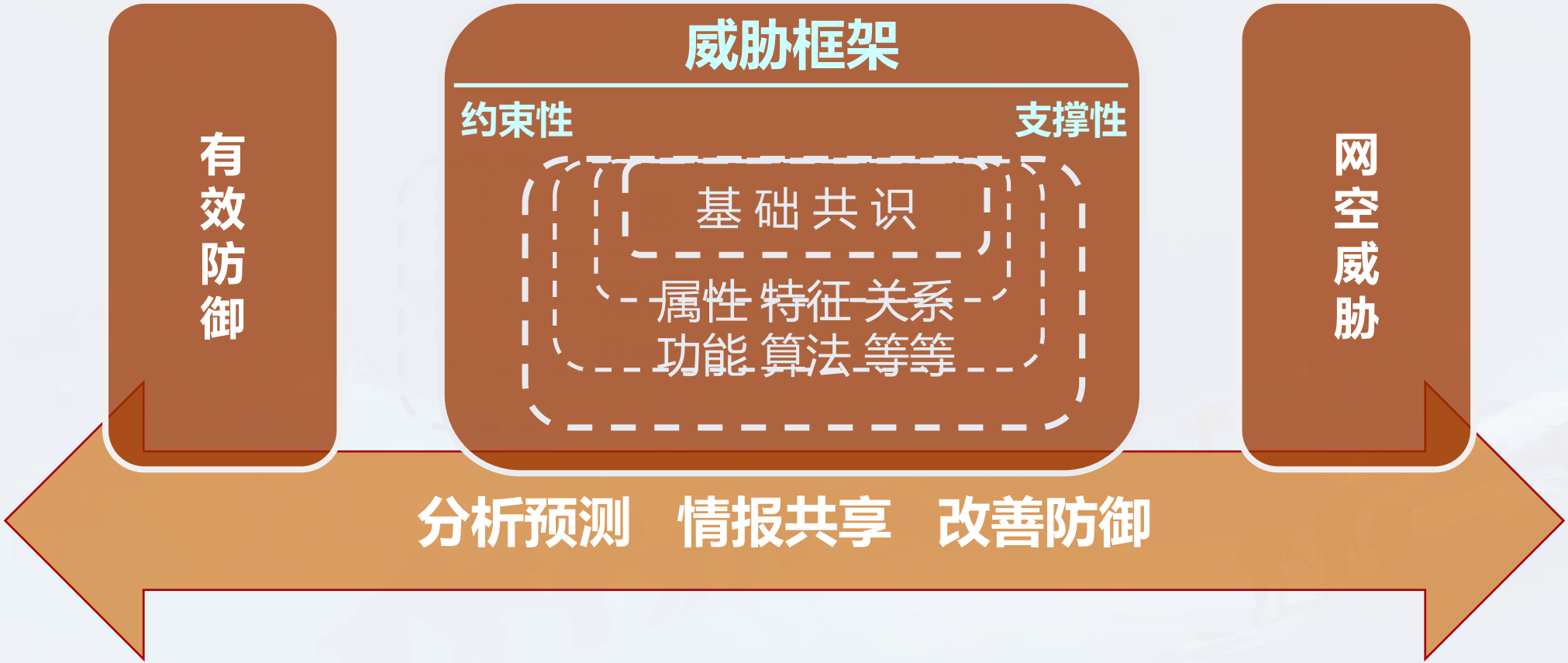
为什么需要威胁框架


蠕虫
后门
木马
病毒
监听
僵尸网络
挖矿木马
灰色软件
勒索软件
黑客工具
社会工程
DDoS
盗号
邮件传输
水坑攻击
脚本病毒
扫描植入
宏病毒
密码破解
提权
格式文档攻击
横向移动
SQL注入
固件植入
身份仿冒

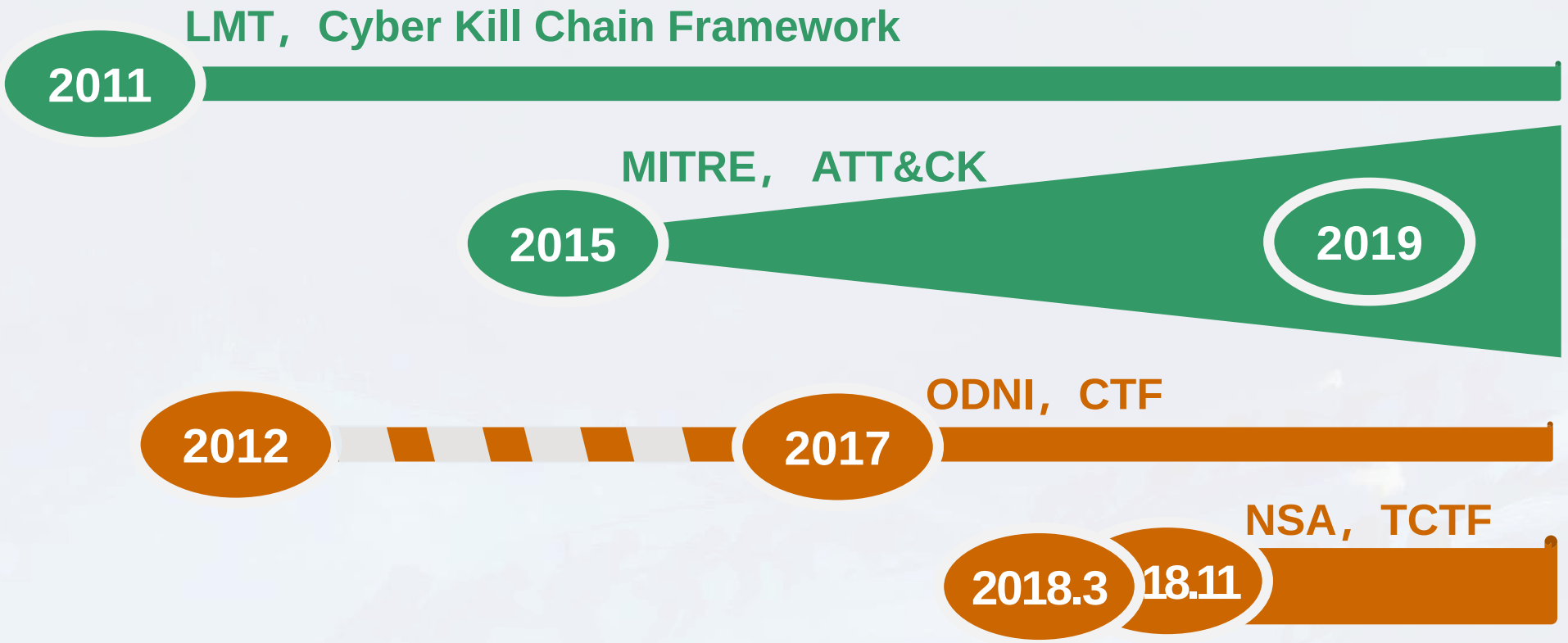
为什么需要威胁框架

Advanced 高级（能力） × **P**ersistent 持续（意图） = **T**hreat 威胁

为什么需要威胁框架



网空威胁框架的构建过程



网空威胁框架的构建过程

- Cyber Kill Chain Framework / 网空杀伤链框架
  - Lockheed Martin，2011

网空威胁框架的构建过程

- 洛克希德·马丁
  - 洛克希德·马丁空间系统公司（Lockheed Martin Space Systems Company，LMT）
  - 全球最大的防务承包商
  - 创建于1912年
  - 航空科技公司，经营航空航天制造、国防工业承包
  - 拥有“臭鼬工厂”等先进研发部门
  - 打造高精尖战机、通讯卫星系统、导弹系统、军用电子装备，等等
  - 战斗机：P38闪电，F16隼，F117夜鹰，F22猛禽，F35闪电II
  - 侦察机：U-2高空间谍侦察机，SR-71黑鸟高空高速战略侦察机
  - 运输机：C-130大力神，C-5，C-141，C5银河重型运输机
  - 火箭与导弹：三叉戟潜射弹道导弹，大力神洲际导弹，AGM-114地狱火
  - 雷　达：宙斯盾系统，远程识别雷达，反隐身雷达
  - 卫　星：DSCS-3，A2100，马丁·玛丽埃塔3000/4000/8000，Tiros-N 气象卫星，GPS III 卫星，获下一代GPS卫星合同

网空威胁框架的构建过程

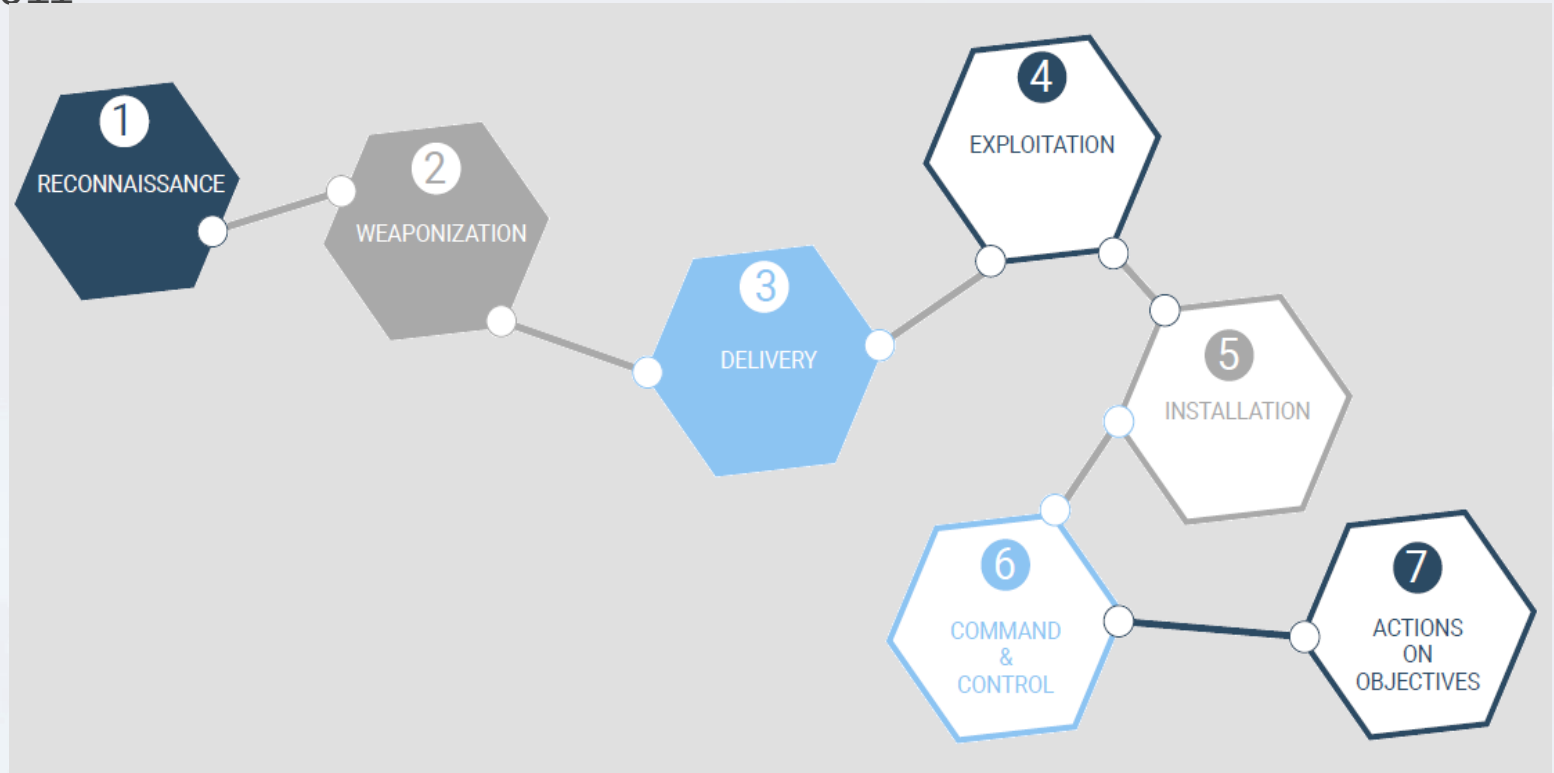
- 洛克希德·马丁

Cyber Full Spectrum Leader

Delivering full-spectrum cyber capabilities and cyber resilient systems to our defense, intelligence community and global security customers

网空威胁框架的构建过程

- Cyber Kill Chain Framework / 网空杀伤链框架
  - Lockheed Martin，2011



网空威胁框架的构建过程

- Cyber Kill Chain Framework / 网空杀伤链框架
  - Lockheed Martin，2011

- **攻击者视角**
- **以“整个攻击过程”而统一离散的威胁事件，形成整体分析**

网空威胁框架的构建过程

- Cyber Kill Chain Framework / 网空杀伤链框架
  - Lockheed Martin，2011
- **ATT&CK** / 对手战术技术公共知识库框架
  - Common Knowledge base of Adversary Tactics and Techniques
  - MITRE，2015 ~ 2019

网空威胁框架的构建过程

- Cyber Kill Chain Framework / 网空杀伤链框架
  - Lockheed Martin，2011
- **ATT&CK** / 对手战术技术公共知识库框架
  - Common Knowledge base of Adversary Tactics and Techniques
  - MITRE，2015 ~ 2019

网空威胁框架的构建过程

- Cyber Kill Chain Framework / 网空杀伤链框架
  - Lockheed Martin，2011
- **ATT&CK** / 对手战术技术公共知识库框架
  - Common Knowledge base of Adversary Tactics and Techniques
  - MITRE，2015 ~ 2019
- Common Cyber Threat Framework / 公共网空威胁框架
  - ODNI，2017

网空威胁框架的构建过程

- 美国情报体系
  - 17个情报机构
  - 以国家情报总监办公室为统领
- ODNI
  - Office of the Director of National Intelligence,国家情报总监办公室
  - 内阁部门
  - 情报总监列席国家安全委员会，任国家安全委员会情报顾问

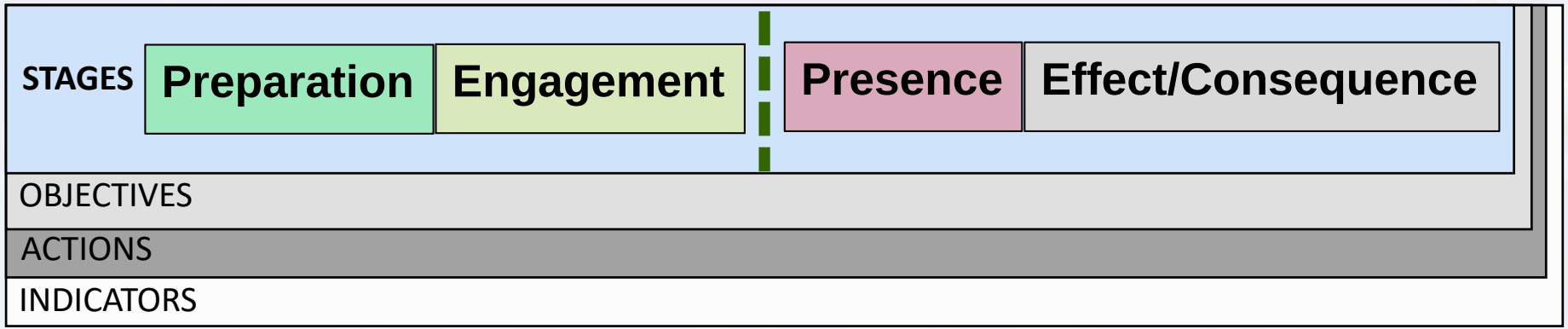
网空威胁框架的构建过程

- ODNI统领
  - CIA, Central Intelligence Agency, 独立
  - NSA, National Security Agency/Central Security Service, 国防部
  - INSCOM, Intelligence and Security Command, 国防部
  - DIA, Defense Intelligence Agency, 国防部
  - I & A, Office of Intelligence and Analysis, 国土安全部
  - AF 25, Twenty-Fifth Air Force, 空军, 国防部
  - Office of Naval Intelligence, 海军, 国防部
  - National Reconnaissance Office, 国防部
  - NGA, National Geospatial-Intelligence Agency, 国防部
  - Bureau of Intelligence and Research, 国务院
  - 等 等
  - 还有各种情报人员协作企业、培训学校，等等

网空威胁框架的构建过程

- *Establish a shared ontology* and *enhance information-sharing* since it is easier to maintain mapping of multiple models to a common reference than directly to each other
- *Characterize and categorize threat activity* in a straightforward way that can support missions ranging from strategic decision-making to analysis and cybersecurity measures and users from generalists to technical experts
- *Support common situational awareness* across organizations

—— "National Intelligence Manager for Cyber, ODNI, 2018"



网空威胁框架的构建过程

- Cyber Kill Chain Framework / 网空杀伤链框架
  - Lockheed Martin，2011
- **ATT&CK** / 对手战术技术公共知识库框架
  - Common Knowledge base of Adversary Tactics and Techniques
  - MITRE，2015 ~ 2019
- Common Cyber Threat Framework / 公共网空威胁框架
  - ODNI，2017
- **Technical Cyber Threat Framework** / 技术性网空威胁框架
  - NSA /CSS，2018

网空威胁框架的构建过程

- Cyber Kill Chain Framework / 网空杀伤链框架
  - Lockheed Martin
- **ATT&CK** / 对手战术技术公共知识库框架
  - Common Knowledge base of Adversary Tactics and Techniques
  - MITRE
- Common Cyber Threat Framework / 公共网空威胁框架
  - ODNI
- **Technical Cyber Threat Framework** / 技术性网空威胁框架
  - NSA/CSS

寒夜速记

威胁框架：认知与实践

02 ATT&CK威胁框架与TCTF威胁框架内容分析

ATT&CK 威胁框架

- MITRE

We Focus on Solving Problems for a Safer World

- 向美国政府提供系统工程、研究开发和信息技术支持
- 是介入政府项目的第三方机构，管理美国联邦政府投资研发中心
- 客户包括美国国防部、联邦航空管理局、国税局、退伍军人事务部、国土安全部等

MITRE Was Established to Serve the Public Interest

ATT&CK 威胁框架

- MITRE
  - **以安全建模而见长！**
    - BLP 经典安全模型
    - 可信计算机系统的建设技术评估标准
    - CVE（Common Vulnerabilities & Exposures, 常见漏洞和暴露）
    - CWE（Common Weakness Enumeration，常见缺陷枚举）
    - CAPEC（Common Attack Pattern Enumeration and Classification，常见攻击模式枚举和分类）
    - CCE（Common Configuration Enumeration，常见配置枚举）
    - STIX（Structured Threat Information eXpression, 结构化威胁信息表达）
    - TAXII（Trusted Automated eXchange of Indicator Information，指标信息的可信自动化交换）
    - 等 等

ATT&CK 威胁框架

- 概 况
  - ATT&CK威胁框架是在洛马杀伤链框架的基础上，构建的一套更细粒度、更易共享的攻击行为模型和知识库，具有更为**丰富的技术性细节**
  - **依据对真实APT攻击进行追踪分析**，提炼出技术点，不断积累知识库，促使该框架基于可能遇到的实际威胁来完善
  - **广泛获得** 安全研究人员与安全厂商的支持

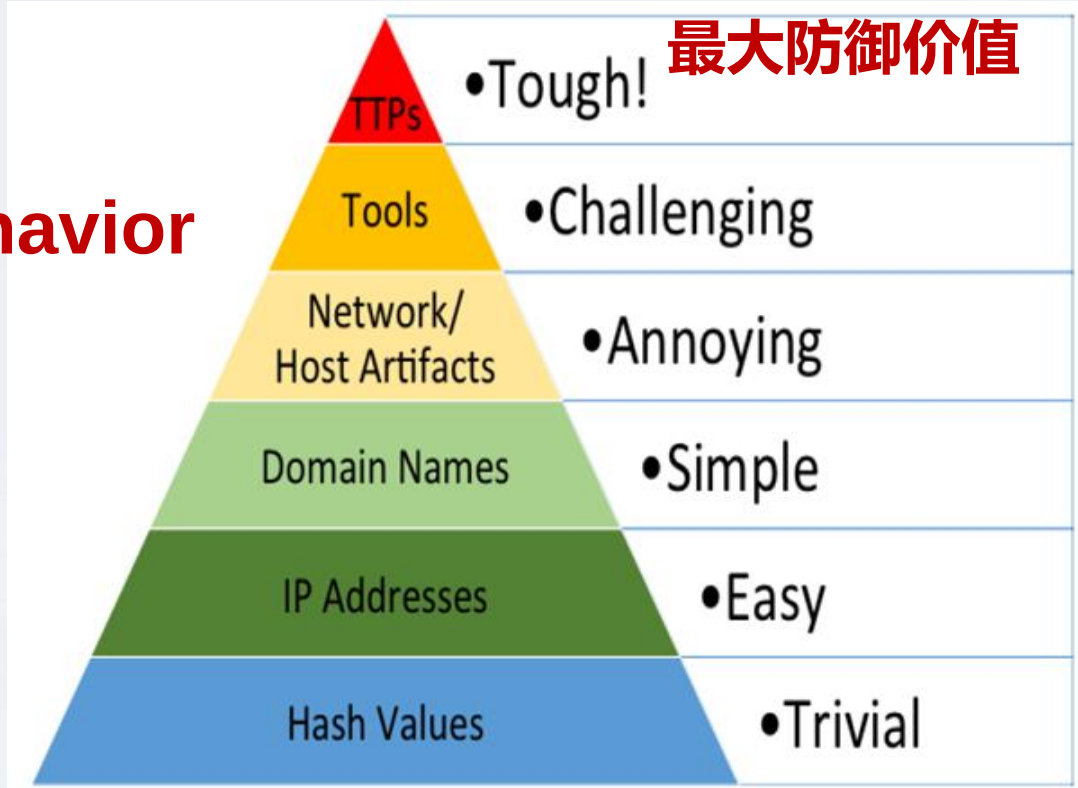
ATT&CK 威胁框架

- **TTP**（Tactics, Techniques and Procedures）
  - 攻击者 “战术技术与过程”
  - 战术Tactics： 目 的
  - 技术Techniques： 动 作
  - 过程Procedures： 具体操作与步骤

ATT&CK 威胁框架

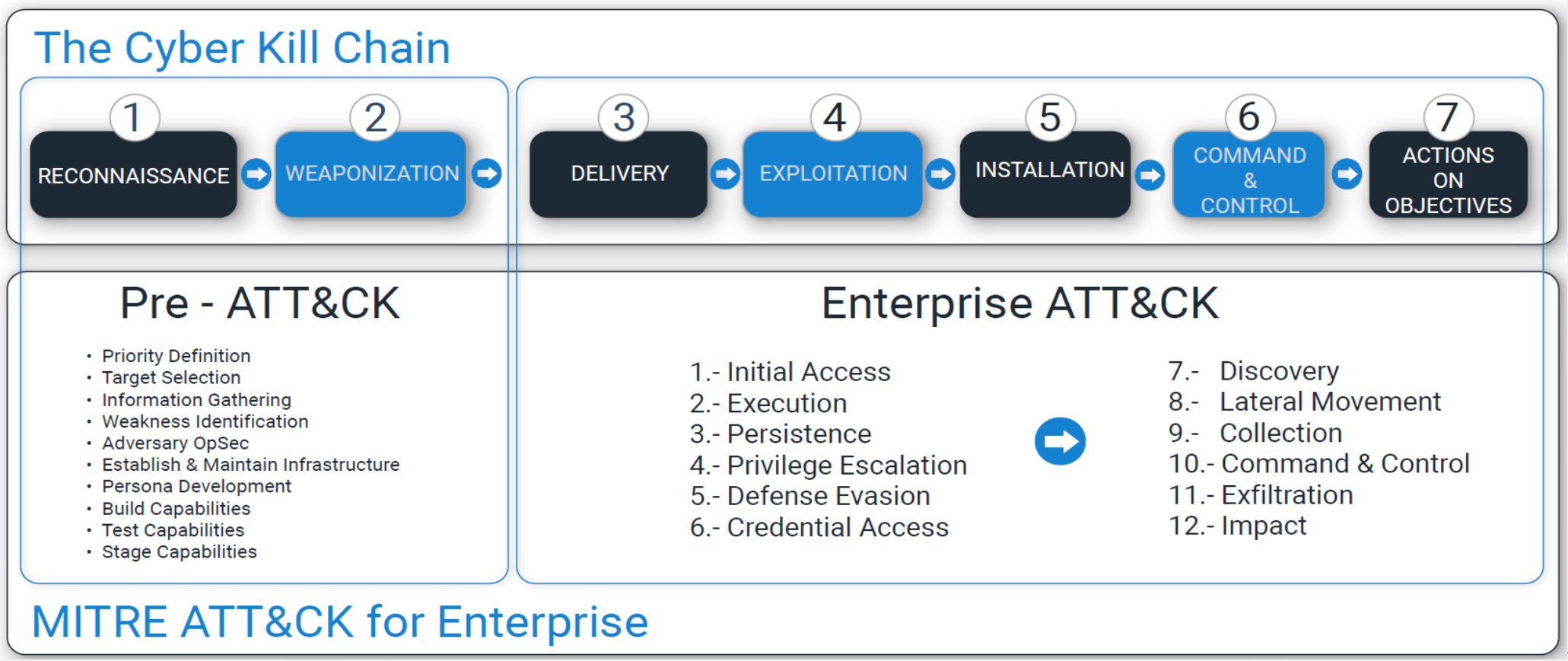
Moving **UP**

from the adversary behavior



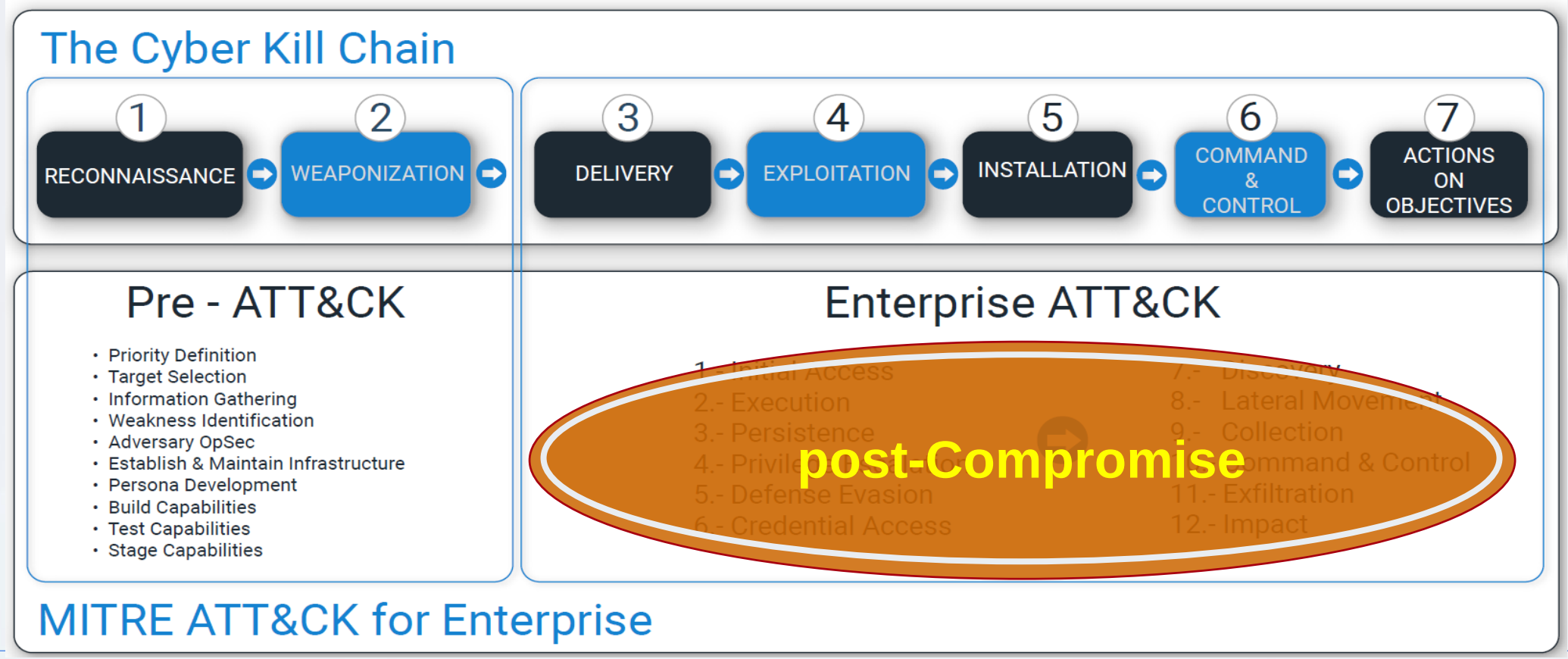
ATT&CK 威胁框架

- 内容概要



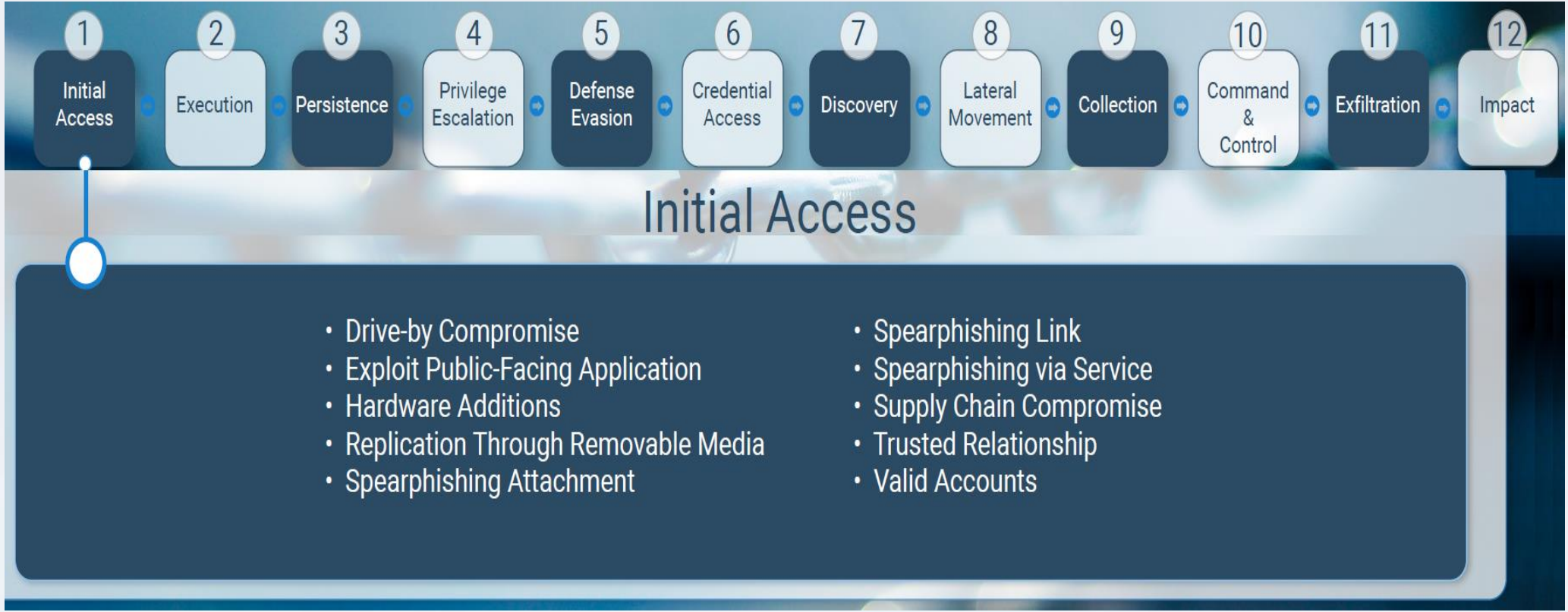
ATT&CK 威胁框架

- 内容概要



ATT&CK 威胁框架

- 内容概要



ATT&CK 威胁框架

初始访问	执行	持久化		提权	防御规避		凭证访问	发现	横向移动	收集	命令与控制	数据渗出	影响
水坑攻击	利用AppleScript	利用.bash_profile和.bashrc	利用LSASS 驱动程序	操纵访问令牌	操纵访问令牌	安装根证书	操纵账户	发现账户	利用AppleScript	捕获音频	利用常用端口	自动渗出数据	删除账户权限
利用面向公众的应用程序	利用CMSTP	利用辅助功能	修改现有服务	借助辅助功能	填充二进制文件	利用InstallUtil	查看Bash历史	发现应用程序窗口	利用应用程序部署软件	自动收集	通过可移动介质通信	压缩数据	损毁数据
利用外部远程服务	利用命令行	操纵账户	Netsh Helper DLL	利用AppCert DLL（注册表项）	利用BITS服务	利用Launchctl	暴力破解	发现浏览器书签	利用组件对象模型（COM）和分布式	收集剪贴板数据	利用连接代理	加密数据	造成恶劣影响的数据加密
添加硬件	利用HTML编译文件	利用AppCert DLL（注册表项）	新建服务	利用AppInit DLL（注册表项）	绕过用户账户控制（UAC）	LC_MAIN劫持	凭证转储	发现域信任	利用远程服务漏洞	收集信息库数据	使用自定义C2协议	限制传输数据大小	网页内容篡换攻击
通过可移动介质复制	利用组件对象模型（COM）和分布式	利用AppInit DLL（注册表项）	启动Office应用程序	利用Windows应用程序兼容性框架	清除命令历史	仿冒	获取Web浏览器凭证	发现文件和目录	执行内部鱼叉式钓鱼攻击	收集本地系统数据	使用自定义加密协议	通过备选协议回传	擦除磁盘内容
使用鱼叉式钓鱼附件	利用控制面板项	利用Windows应用程序兼容性框架	路径拦截	绕过用户账户控制（UAC）	利用CMSTP	修改注册表	获取文件中的凭证	扫描网络服务	利用登录脚本	收集网络共享驱动数据	编码数据	通过C2信道回传	擦除磁盘结构
使用鱼叉式钓鱼链接	使用动态数据交换协议（DDE）	利用认证包	修改属性列表	DLL搜索顺序劫持	代码签名	利用Mshta	获取注册表中的凭证	发现网络共享	利用密码哈希认证	收集可移动介质数据	混淆数据	通过其他网络介质回传	端点侧拒绝服务（DoS）
通过服务执行鱼叉式钓鱼攻击	通过API执行	利用BITS服务	端口敲门	Dylib劫持	投递后编译	删除网络共享连接	利用凭证访问漏洞	网络嗅探	利用Ticket认证	回传数据准备	前置域名	通过物理介质回传	损坏固件
入侵供应链	通过模块加载执行	使用Bootkit	端口监控	提示用户输入合法凭证提权	利用HTML编译文件	利用NTFS交换数据流（ADS）	强制认证	发现密码策略	利用远程桌面协议	收集电子邮件	使用域名生成算法（DGA）	定时传输	禁止系统恢复
利用受信关系	利用主机软件漏洞	添加浏览器扩展插件	利用PowerShell配置文件	利用事件监控守护进程	利用组件固件	混淆文件或信息	利用Hook	发现主机接入设备	拷贝远程文件	输入捕捉	使用备用信道		网络侧拒绝服务（DoS）
利用有效账户	利用图形用户界面（GUI）	更改默认文件关联	利用Rc.common文件	利用漏洞提权	组件对象模型（COM）劫持	伪造父进程	输入捕捉	发现权限组	利用远程服务	浏览器中间人攻击（MitB）	利用多跳代理		资源劫持
	利用InstallUtil	利用组件固件	重启应用程序	额外窗口内存注入（EWMI）	利用连接代理	修改属性列表	欺骗用户输入凭证	发现进程	通过可移动介质复制	获取屏幕截图	创建多级信道		操纵运行时数据
	利用Launchctl	组件对象模型（COM）劫持	冗余访问	利用文件系统权限漏洞	利用控制面板项	端口敲门	使用Kerberoasting技术	查询注册表	共享Webroot目录	捕获视频	使用多协议通信		禁用服务
	利用linux本地任务调度	创建账户	添加注册表运行键/启动文件夹项	利用Hook	使用DCShadow技术	Process Doppelgänging（仿冒合法进	利用Keychain	发现远程系统	SSH劫持		使用多层加密		操纵本地存储数据
	利用LSASS驱动程序	DLL搜索顺序劫持	利用计划任务	映像劫持	反混淆/解码文件或信息	替换进程内存	LLMNR/NBT-NS投毒和中继	发现安全软件	污染共享内容		端口敲门		系统关机/重启
	利用Mshta	Dylib劫持	利用屏幕保护程序	启动守护进程	禁用安全工具	进程注入	网络嗅探	发现软件	利用系统中的第三方软件		利用远程访问工具		操纵传输中的数据
	利用PowerShell	利用事件监控守护进程	利用SSP DLL（注册表项）	新建服务	DLL搜索顺序劫持	冗余访问	利用Password Filter DLL	发现系统信息	利用Windows管理员共享		拷贝远程文件		
	利用Regsvcs/Regasm	利用外部远程服务	利用服务器软件组件	伪造父进程	DLL旁路加载	利用Regsvcs/Regasm	收集私钥	发现系统网络配置	利用Windows远程管理服务		使用标准应用层协议		
	利用Regsvr32	利用文件系统权限漏洞	利用服务注册表权限漏洞	路径拦截	按条件执行	利用Regsvr32	利用Securityd内存	发现系统网络连接			使用标准加密协议		
	利用Rundll32	隐藏文件和目录	利用Setuid和Setgid位	修改属性列表	利用漏洞规避防御	使用Rootkit	窃取Web会话Cookie	发现系统所有者/用户			使用标准非应用层协议		
	利用计划任务	利用Hook	修改快捷方式	端口监控	额外窗口内存注入（EWMI）	利用Rundll32	双因子认证拦截	发现系统服务			利用不常用端口		
	使用脚本	利用Hypervisor	会话发起协议（SIP）和受信提供商劫持	利用PowerShell配置文件	修改文件和目录权限	使用脚本		发现系统时间			利用Web服务		
	利用windows服务	映像劫持	利用启动项	进程注入	删除文件	执行签名的二进制文件代理		虚拟化/沙箱逃逸					
	利用签名的二进制文件代理执行	利用内核模块和扩展	利用系统固件	利用计划任务	文件系统逻辑偏移	执行签名的脚本代理							
	利用签名的脚本代理执行	启动代理	利用Systemd服务	利用服务注册表权限漏洞	绕过Gatekeeper	会话发起协议（SIP）和受信提供商劫持							
	利用Source命令	启动守护进程	利用Windows时间服务	利用Setuid和Setgid位	修改组策略	软件加壳							
	加入空格隐藏扩展名	利用Launchctl	利用Trap命令	SID历史注入	隐藏文件目录	加入空格隐藏扩展名							
	利用系统中的第三方软件	添加LC_LOAD_DYLIB	利用有效账户	利用启动项	隐藏用户	模板注入							
	利用Trap命令	利用linux本地任务调度	使用Web Shell	利用Sudo命令	隐藏窗口	修改文件时间戳							
			利用Windows事件订阅										

ATT&CK 威胁框架

ATT&CK Matrix for Enterprise

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Account Access Removal
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Communication Through Removable Media	Data Compressed	Data Destruction
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery	Component Object Model and Distributed COM	Clipboard Data	Connection Proxy	Data Encrypted	Data Encrypted for Impact
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	Domain Trust Discovery	Exploitation of Remote Services	Data from Information Repositories	Custom Command and Control Protocol	Data Transfer Size Limits	Defacement
Replication Through Removable Media	Component Object Model and Distributed COM	AppInit DLLs	Application Shimming	Clear Command History	Credentials from Web Browsers	File and Directory Discovery	Internal Spearphishing	Data from Local System	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Content Wipe
Spearphishing Attachment	Control Panel Items	Application Shimming	Bypass User Account Control	CMSTP	Credentials in Files	Network Service Scanning	Logon Scripts	Data from Network Shared Drive	Data Encoding	Exfiltration Over Command and Control Channel	Disk Structure Wipe
Spearphishing Link	Dynamic Data Exchange	Authentication Package	DLL Search Order Hijacking	Code Signing	Credentials in Registry	Network Share Discovery	Pass the Hash	Data from Removable Media	Data Obfuscation	Exfiltration Over Other Network Medium	Endpoint Denial of Service
Spearphishing via Service	Execution through API	BITS Jobs	Dylib Hijacking	Compile After Delivery	Exploitation for Credential Access	Network Sniffing	Pass the Ticket	Data Staged	Domain Fronting	Exfiltration Over Physical Medium	Firmware Corruption
Supply Chain	Execution through	Rootkit	Elevated Execution with	Compiled HTML File	Forced	Password Policy	Remote Desktop	Email	Domain Generation	Scheduled	Inhibit System

ATT&CK 威胁框架

- 内容细节（战术举例）

Initial Access

The adversary is trying to get into your network.

ID: TA0001

Created: 17 October 2018

Last Modified: 19 July 2019

Initial Access consists of techniques that use various entry vectors to gain their initial foothold within a network. Techniques used to gain a foothold include targeted spearphishing and exploiting weaknesses on public-facing web servers. Footholds gained through initial access may allow for continued access, like valid accounts and use of external remote services, or may be limited-use due to changing passwords.

Techniques

Techniques: 11

ID	Name	Description
T1189	Drive-by Compromise	A drive-by compromise is when an adversary gains access to a system through a user visiting a website over the normal course of browsing. With this technique, the user's web browser is typically targeted for exploitation, but adversaries may also use compromised websites for non-exploitation behavior such as

ATT&CK 威胁框架

- 内容细节（技术举例）

Spearphishing Attachment

Spearphishing attachment is a specific variant of spearphishing. Spearphishing attachment is different from other forms of spearphishing in that it employs the use of malware attached to an email. All forms of spearphishing are electronically delivered social engineering targeted at a specific individual, company, or industry. In this scenario, adversaries attach a file to the spearphishing email and usually rely upon User Execution to gain execution.

There are many options for the attachment such as Microsoft Office documents, executables, PDFs, or archived files. Upon opening the attachment (and potentially clicking past protections), the adversary's payload exploits a vulnerability or directly executes on the user's system. The text of the spearphishing email usually tries to give a plausible reason why the file should be opened, and may explain how to bypass system protections in order to do so. The email may also contain instructions on how to decrypt an attachment, such as a zip file password, in order to evade email boundary defenses. Adversaries frequently manipulate file extensions and icons in order to make attached executables appear to be document files, or files exploiting one application appear to be a file for a different one.

ID: T1193

Tactic: Initial Access

Platform: Windows, macOS, Linux

Data Sources: File monitoring, Packet capture, Network intrusion detection system, Detonation chamber, Email gateway, Mail server

CAPEC ID: CAPEC-163

Version: 1.0

ATT&CK 威胁框架

- 内容细节（技术举例）

Spearphishing Attachment

Spearphishing attachment is a specific variant of spearphishing. Spearphishing attachment is different from other forms of spearphishing in that it employs the use of malware attached to an email. All forms of spearphishing are electronically delivered social

ID: T1193

Tactic: Initial Access

Procedure Examples

Name	Description
admin@338	admin@338 has sent emails with malicious Microsoft Office documents attached.[92]
APT12	APT12 has sent emails with malicious Microsoft Office documents and PDFs attached.[88][89]
APT19	APT19 sent spearphishing emails with malicious attachments in RTF and XLSM formats to deliver initial exploits.[62]
APT28	APT28 sent spearphishing emails containing malicious Microsoft Office attachments.[22][23][24][25][26][27]
APT29	APT29 has used spearphishing emails with an attachment to deliver files with exploits to initial victims.[33][34]

ATT&CK 威胁框架

- 作用举例：指导如何防御某一具体攻击技术

Example Technique: New Service

–**Description:** When operating systems boot up, they can start programs or applications called services that perform background system functions.

–**(略)**

–**Detection**

- Monitor service creation through changes in the Registry and common utilities using command-line invocation
- Tools such as Sysinternals Autoruns may be used to detect system changes that could be attempts at persistence
- Monitor processes and command-line arguments for actions that could create services

–**Mitigation**

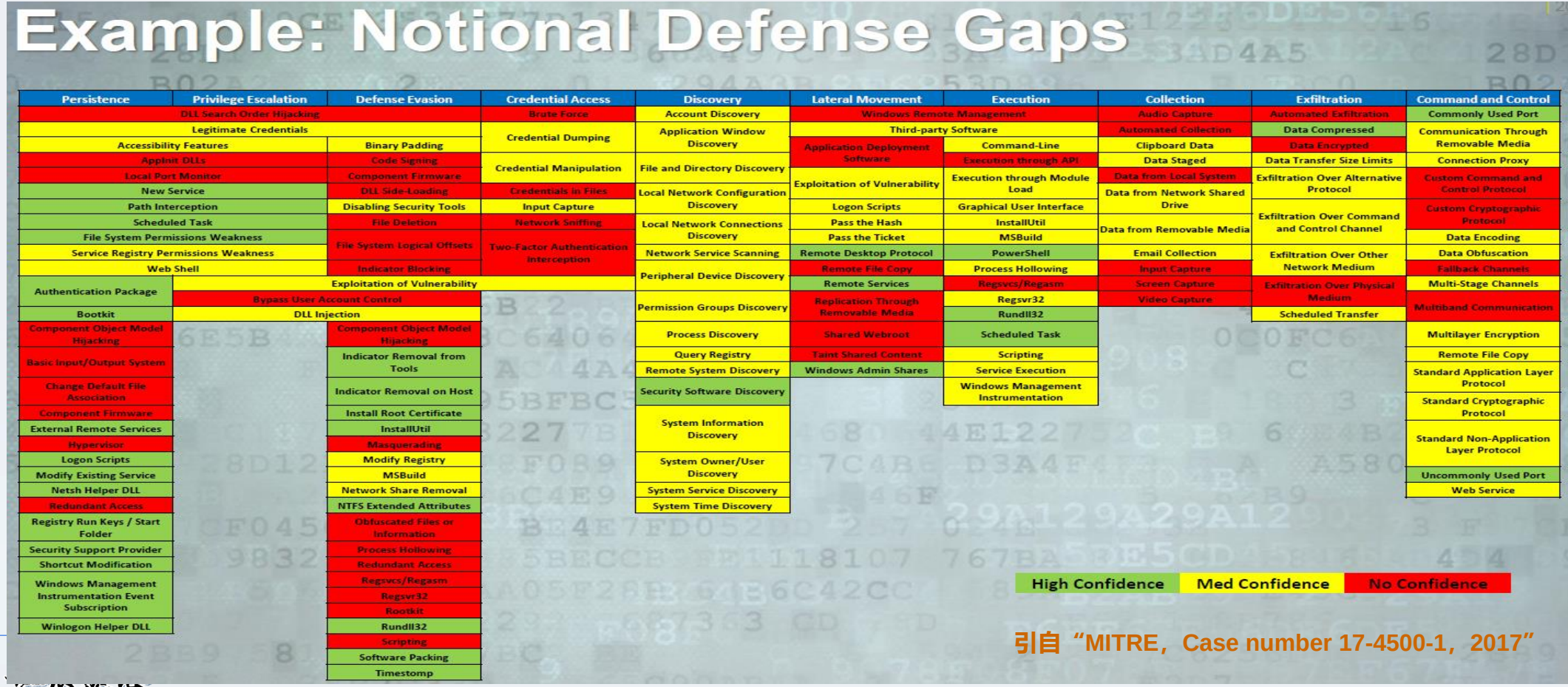
- Limit privileges of user accounts and remediate Privilege Escalation vectors
- Identify and block unnecessary system utilities or potentially malicious software that may be used to create services

–**Data Sources:** Windows Registry, process monitoring, command-line parameters

–**Examples:** *Carbanak*, *Lazarus Group*, TinyZBot, Duqu, CozyCar,CosmicDuke, hcdLoader, …

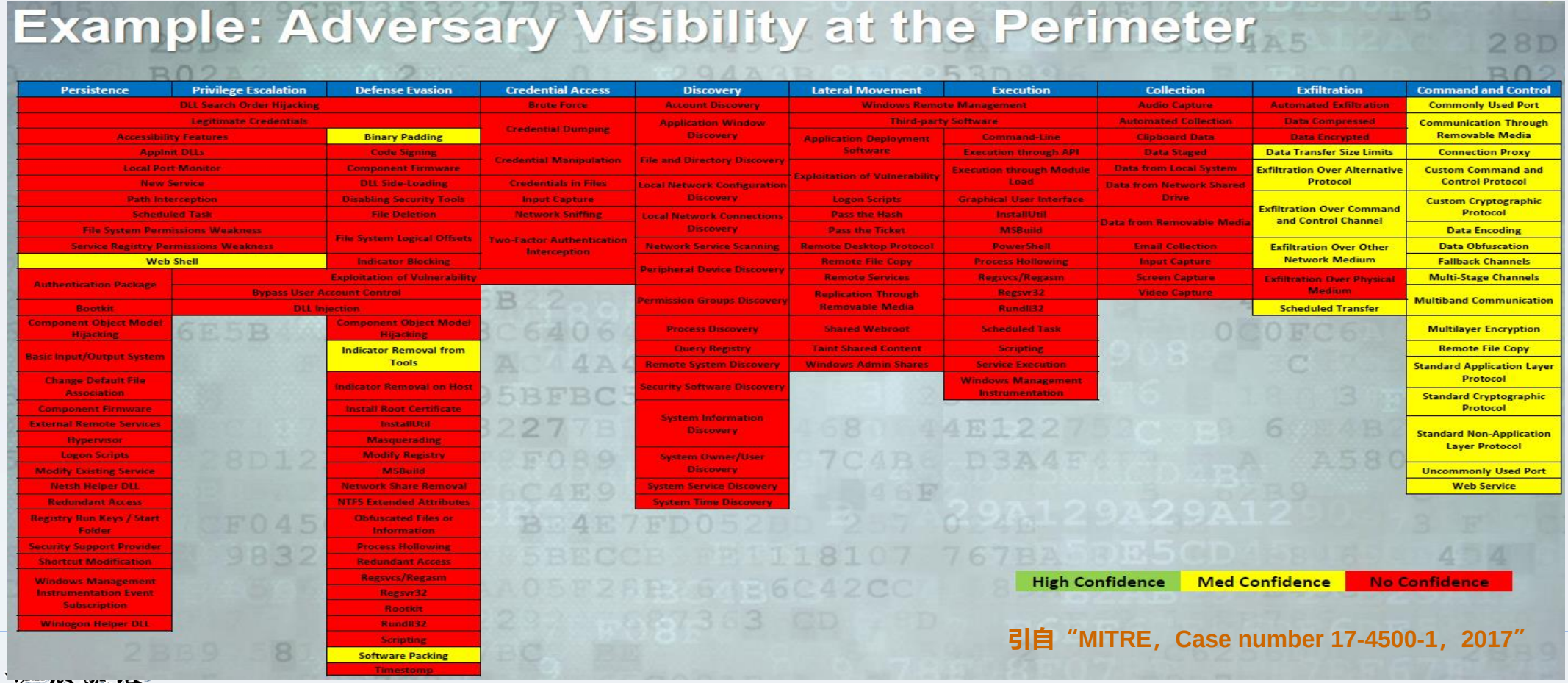
ATT&CK 威胁框架

- 作用举例：指导如何聚焦防御重点



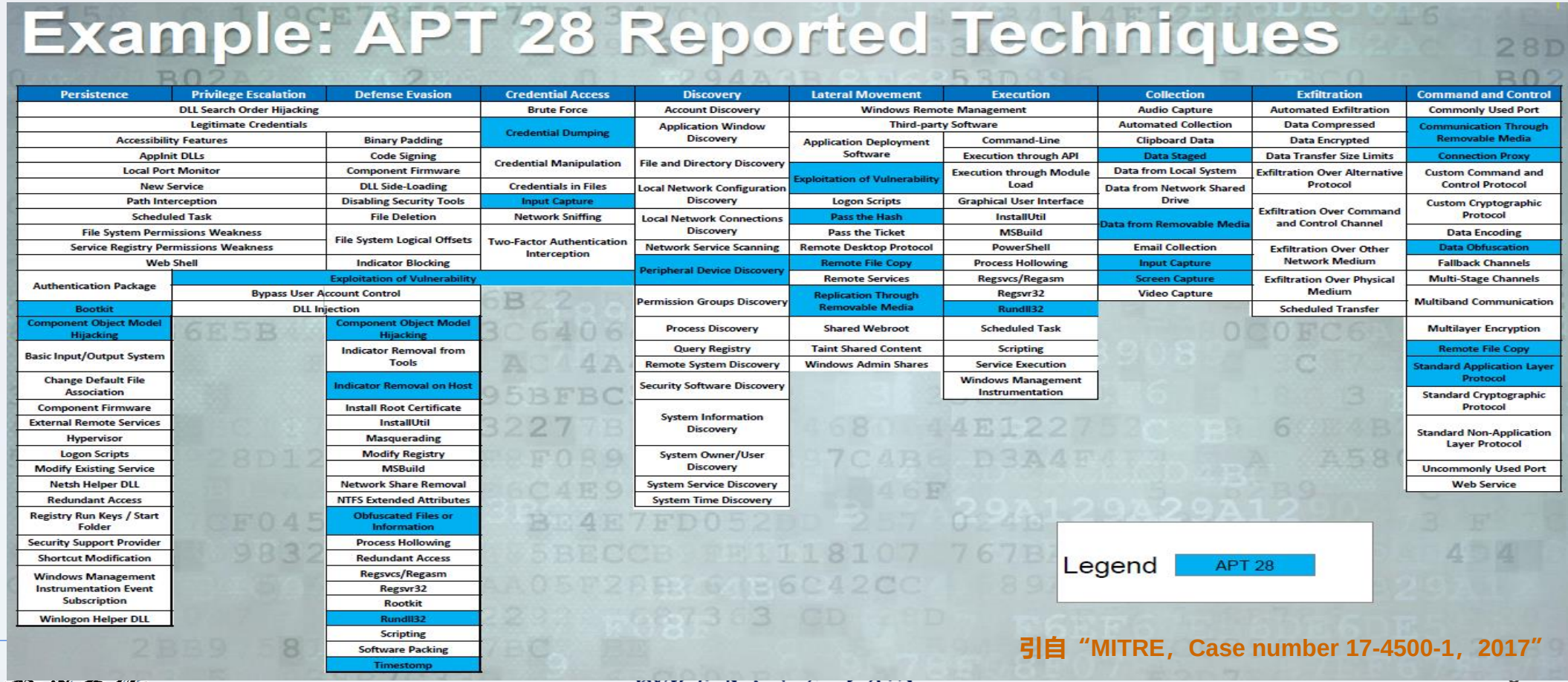
ATT&CK 威胁框架

- 作用举例：指导如何优化防御部署



ATT&CK 威胁框架

- 作用举例：分析特定的APT组织



引自“MITRE，Case number 17-4500-1，2017”

ATT&CK 威胁框架

- 作 用
  - 检测分析
  - 威胁情报
  - 对手仿真
  - 评估与工程

ATT&CK 威胁框架

- 作 用 —— 检测分析
  - 帮助网络防御者开发分析手段，以检测对手使用的技术
  - 可利用网空分析库 (CAR， Cyber Analytics Repository)

MITRE Cyber Analytics Repository　　Analytics　Data Model　Sensors

Analytics 分析方法

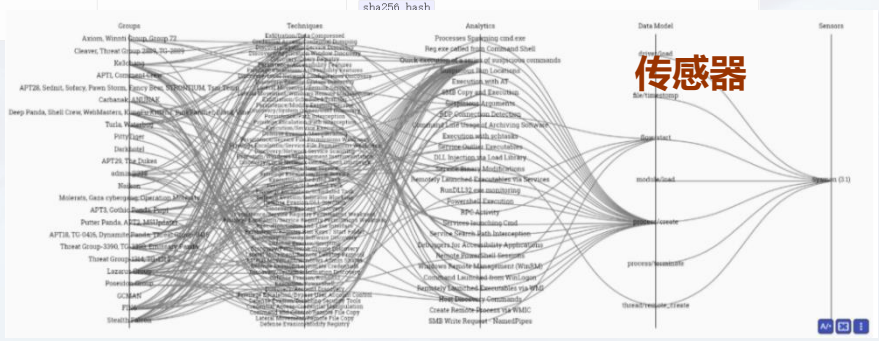
Analytic	ATT&CK Techniques	Implementations
CAR-2013-01-002: Autorun Differences	Modify Existing Service, New Service, Scheduled Task, Port Monitors, Registry Run Keys / Startup Folder, Path Interception, Accessibility Features, Modify Registry, Service Registry Permissions Weakness, Windows Management Instrumentation Event Subscription, File System Permissions Weakness, Change Default File Association, Logon Scripts, Winlogon Helper DLL, AppInit DLLs	
CAR-2013-01-003: SMB Events Monitoring	Data from Network Shared Drive, Windows Admin Shares	Pseudocode
CAR-2013-02-003: Processes Spawning cmd.exe	Command-Line Interface	Dnif, Pseudocode
CAR-2013-02-008: Simultaneous Logins on a Host	Valid Accounts	Pseudocode
CAR-2013-02-012: User Logged in to Multiple Hosts	Valid Accounts	
CAR-2013-03-001: Reg.exe called from Command Shell	Query Registry, Modify Registry, Registry Run Keys / Startup Folder, Service Registry Permissions Weakness	Dnif, Pseudocode

Data Model 数据模型

The Data Model, strongly inspired by CybOX, is an organization of the objects that may be monitored from a host-based or network-based perspective. Each object on can be identified by two dimensions: its actions and fields. When paired together, the three-tuple of `(object, action, field)` acts like a coordinate, and describe what properties and state changes of the object can be captured by a sensor.

Summary

Object	Actions	Fields
driver	load unload	base_address fqdn hostname image_path md5_hash module_name sha1_hash sha256_hash



ATT&CK 威胁框架

- 作 用 —— 威胁情报
  - 了解攻击者行为，并用于改善决策
  - 通过对攻击技术和行为的分析，来辨识攻击组织，以及分析攻击组织的技术变化

APT29 | APT3 | APT29+APT3

selection controls | layer controls | technique controls

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
11 items	34 items	62 items	32 items	69 items	21 items	23 items	18 items	13 items	22 items	9 items	16 items
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Account Access Removal
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Communication Through Removable Media	Data Compressed	Data Destruction
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery	Component Object Model and Distributed COM	Clipboard Data	Connection Proxy	Data Encrypted	Data Encrypted for Impact
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	Domain Trust Discovery	Exploitation of Remote Services	Data from Information Repositories	Custom Command and Control Protocol	Data Transfer Size Limits	Defacement
Replication Through Removable Media	Component Object Model and Distributed COM	AppInit DLLs	Application Shimming	Clear Command History	Credentials from Web Browsers	File and Directory Discovery	Internal Spearphishing	Data from Local System	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Content Wipe
Spearphishing Attachment	Control Panel Items	Application Shimming	Bypass User Account Control	CMSTP	Credentials in Files	Network Service Scanning	Logon Scripts	Data from Network Shared Drive	Data Encoding	Exfiltration Over Command and Control Channel	Disk Structure Wipe
Spearphishing Link	Dynamic Data Exchange	Authentication Package	DLL Search Order Hijacking	Code Signing	Credentials in Registry	Network Share Discovery	Pass the Hash	Data from Removable Media	Data Obfuscation	Exfiltration Over Other Network Medium	Endpoint Denial of Service
Spearphishing via Service	Execution through API	BITS Jobs	Dylib Hijacking	Compile After Delivery	Exploitation for Credential Access	Network Sniffing	Pass the Ticket	Data Staged	Domain Fronting	Exfiltration Over Physical Medium	Firmware Corruption
Supply Chain Compromise	Execution through Module Load	Bootkit	Elevated Execution with Prompt	Compiled HTML File	Forced Authentication	Password Policy Discovery	Remote Desktop Protocol	Email Collection	Domain Generation Algorithms	Scheduled Transfer	Inhibit System Recovery
Trusted Relationship	Exploitation for Client Execution	Browser Extensions	Emond	Component Firmware	Hooking	Peripheral Device Discovery	Remote File Copy	Input Capture	Fallback Channels		Network Denial of Service
Valid Accounts	Graphical User Interface	Change Default File Association	Exploitation for Privilege Escalation	Component Object Model Hijacking	Input Capture	Permission Groups Discovery	Remote Services	Man in the Browser	Multi-hop Proxy		Resource Hijacking
	InstallUtil	Component Firmware	Extra Window Memory Injection	Connection Proxy	Input Prompt	Process Discovery	Replication Through Removable Media	Screen Capture	Multi-Stage Channels		Runtime Data Manipulation
	Launchctl	Component Object Model Hijacking	File System Permissions	Control Panel Items	Kerberoasting	Query Registry	Shared Webroot	Video Capture	Multiband Communication		Service Stop
	Local Job Scheduling	Create Account		DCShadow	Keychain	Remote System Discovery	SSH Hijacking		Multilayer		Stored Data Manipulation
		DLL Search Order		Deobfuscate/Decode Files or Information	LLMNR/NBT-NS Poisoning and	Security Software Discovery					System Shutdown/Reboot
				Disabling Security Tools		Software Discovery					
				DLL Search Order							

ATT&CK Navigator(导航器)

APT3/29 标注（部分显示）

ATT&CK 威胁框架

- 作 用 —— 对手仿真
  - 开展一系列基于威胁的安全测试，模拟真实攻击者的技术，关注技术行为

Atomic Red Team（ART）

是映射到 ATT＆CK框架的小型，高度可移植的检测测试库，每个安全团队都可以执行ART来测试其网络防御

Atomic Test #2 - Network Share Discovery command prompt

Network Share Discovery utilizing the command prompt

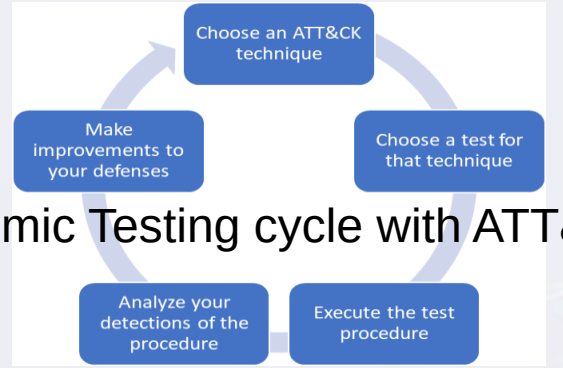
Supported Platforms: Windows

Inputs

Name	Description	Type	Default Value
computer_name	Computer name to find a mount on.	string	computer1

Run it with `command_prompt` **!**

```
net view \\#{computer_name}
```



Atomic Testing cycle with ATT&CK

initial-access	execution	persistence	privilege-escalation	defense-evasion	credential-access
Drive-by Compromise CONTRIBUTE A TEST	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation
Exploit Public-Facing Application CONTRIBUTE A TEST	CMSTP	Accessibility Features	Accessibility Features	Application Access Token CONTRIBUTE A TEST	Bash History
External Remote Services CONTRIBUTE A TEST	Command-Line Interface	Account Manipulation	AppCert DLLs CONTRIBUTE A TEST	BITS Jobs	Brute Force

All Atomic Tests by ATT&CK Tactic & Technique

ATT&CK 威胁框架

- 作 用 —— 评估与工程
  - 基于ATT&CK框架的评估能够为安全工程师和构架师提供有用数据，以证明基于威胁分析的安全改进是合理的
  - 评估组织的能力并推动工程决策，比如应该实现哪些工具或日志
  - 在检测覆盖度上与检测深度上，提供清晰的差距分析，指导加强入侵检测能力

The assessment and engineering process（评估与工程过程）

ATT&CK 威胁框架

- 更多资源；例如 Mitigations (缓解措施)

Enterprise Mitigations

Mitigations: 41

ID	Name	Description
M1036	Account Use Policies	Configure features related to account use like login attempt lockouts, specific login times, etc.
M1015	Active Directory Configuration	Configure Active Directory to prevent use of certain techniques; use SID Filtering, etc.
M1049	A	

Techniques Addressed by Mitigation

Domain	ID	Name	Description
Enterprise	T1110	Brute Force	Set account lockout policies after a certain number of failed login attempts to prevent passwords from being guessed. Too strict a policy may create a denial of service condition and render environments un-usable, with all accounts used in the brute force being locked-out.

Technical Cyber Threat Framework

- NSA
  - 规模最大、技术最复杂的情报机构
  - 专注于“信号情报”（监控、收集、处理通信与其它电子信息，从中破解秘密）
  - 还负责防护外部对美信息系统的渗透
  - 运作棱镜等众多大规模监听项目
  - 大量雇佣数学与技术人员
  - 在美军内部机构是中央安全署（CSS）

Technical Cyber Threat Framework

Administration (行动管理与资源保障)			Preparation (目标勘察与环境整备)		Engagement (接触目标与进攻突防)		Presence (持久化驻留潜伏)						Effect (致效能力运用)					Ongoing Processes (全程持续支撑作业)			
规划	资源开发	研究	侦察	环境预置	投递	利用	执行	内部侦察	提权	凭证访问	横向移动	持久化	监控	渗出	修改	拒绝	破坏	分析、评估、反馈	命令与控制	规避	
分析行动	获取行动所需基础设施	收集信息	执行社会工程学	应用数据文件中添加可利用点	无线接入	滥用协议	创建计划任务	枚举账户和权限	利用应用程序漏洞	添加或修改凭证	利用对等网络	创建新服务	激活记录	收集串扰	修改数据	破坏文件或应用程序	磁盘/操作系统变砖（全部删除）	使用基础设施	向中点发送信标	直接访问磁盘	删除日志数据
确定战略和目标	建立联盟和伙伴关系	确定能力差距	收集凭证	分配行动所需基础设施	改变通信路径	访问虚拟内存	通过服务控制器执行	枚举文件系统	利用固件漏洞	执行社会工程学	远程登录	创建计划任务	被动收集	从本地系统收集	修改进程结果	降低性能	损坏磁盘/操作系统（部分删除）	实施效果评估	建立对等网络	规避数据大小限制	删除toolkit
发布行动指令	创建僵尸网络	确定信息差距	识别串扰	建立跳板	供应链/受信源入侵	执行社会工程学	通过第三方软件执行	枚举本地网络连接	利用操作系统漏洞	破解密码	利用密码哈希认证	编辑boot记录	为其他行动创造条件	从网络资源收集	造成物理影响	中断/拒绝服务	删除数据	优化潜在受害者	中继通信	阻止主机信标上传	为恶意内容签名
制定行动计划	能力开发		测绘可访问网络	建立物理抵近点	可移动介质连接	破解加密	注入进程	枚举本地网络设置	注入进程	转储凭证	利用ticket认证	修改文件类型关联	键盘记录	压缩数据	修改机器间通信	加密数据使其不可用	破坏硬件		发送命令	降级安全产品	将文件存储在非常规的位置
获准执行行动	获得资金		扫描设备	网站植入或预埋	异常网络设备连接	利用固件漏洞	利用授权用户	枚举操作系统和软件	利用辅助功能	劫持活动的凭证	通过可移动介质复制	使用登录脚本	保持访问	泄露数据或信息	更改系统进程的运行状态				利用僵尸网络	延迟活动	根据环境调整行为
选择目标受害者	供应链 预置		爬取网站	预置载荷	通过网站感染	利用本地应用程序漏洞	替换现有二进制文件	枚举进程	利用合法凭证	定位凭证	污染共享内容	利用路径顺序执行	屏幕截屏	将数据存储到指定位置	篡改网站				利用链式协议	采用反取证措施	利用签名内容
	人员和培训资源		选择潜在受害者		注入数据库命令	利用操作系统漏洞	运行shell命令	枚举窗口		键盘记录	利用应用程序部署软件	修改BIOS		运行收集脚本	破解加密				利用对等连接	采用反逆向工程措施	
			调查设备		利用设备交换	利用远程应用程序漏洞	运行无文件载荷	测绘可访问网络			利用远程服务	修改配置用于启动		通过C2信道发送					利用远程shell	使用rootkit	
			利用社交媒体		发送恶意邮件	利用弱访问控制	利用解释脚本	扫描连接的设备			写入远程文件共享	修改现有服务		通过非C2信道发送					利用可移动介质	编码数据	
					借助公共网络基础设施传输	劫持	利用系统接口	嗅探网络			写入共享webroot目录	修改链接		通过其他网络介质发送						加密数据	
					利用CDS或MLS传输	冒充/欺骗用户	利用远程服务					修改服务配置		节流数据						仿冒合法文件	
					利用聊天服务	零日漏洞利用	通过受信应用执行非受信代码					替换服务二进制文件		通过物理方法传输						操纵受信进程	
					利用受感染主机	漏洞利用工具包	写入磁盘					设置为启动时加载		利用CDS或MLS传输						仿冒合法流量	
					利用合法远程访问	利用受信关系						利用库搜索劫持								修改恶意代码以规避检测	
					利用物理网桥	重放攻击														混淆数据	

Technical Cyber Threat Framework

- 对阶段、目标、行为给出了标准定义；例如：
  - **阶段- 接触目标与进攻突防**：在意图获得受害者的物理或虚拟计算机、信息系统、网络和/或数据存储的访问权限之前，威胁行为体对特定目标/目标组执行的攻击活动
  - **目标- 投递**：利用目标在技术、人员或流程中的漏洞，通过技术、认知、物理手段向目标投递恶意载荷。恶意载荷可以像口头传达给目标以获取信息的想法一样简单，也可以像定制恶意软件一样复杂，并可以使用多种方式投递给目标。最常用的远程方法包括鱼叉式网络钓鱼、恶意网站和远程漏洞利用，但也可以通过社会工程或内部威胁进行投递
  - **行为- 发送恶意邮件**：在电子邮件中嵌入恶意附件或链接，发送给目标。打开或执行附件，点击链接或加载电子邮件本身后，用户的计算机可能会受到危害，并可能为恶意行为者提供访问权限

Technical Cyber Threat Framework

- 行为的关键短语

阶 段	目 标	行 动	关键短语
接触目标与进攻突防	投 递	发送恶意邮件	鱼叉式网络钓鱼
接触目标与进攻突防	投 递	发送恶意邮件	网络捕鲸
接触目标与进攻突防	投 递	发送恶意邮件	网络钓鱼
接触目标与进攻突防	投 递	发送恶意邮件	垃圾邮件
接触目标与进攻突防	投 递	发送恶意邮件	恶意附件
接触目标与进攻突防	投 递	发送恶意邮件	恶意链接
接触目标与进攻突防	投 递	发送恶意邮件	网址
接触目标与进攻突防	投 递	发送恶意邮件	嵌入式代码
接触目标与进攻突防	投 递	发送恶意邮件	嵌入式HTML iFrame
接触目标与进攻突防	投 递	发送恶意邮件	iFrame
接触目标与进攻突防	投 递	发送恶意邮件	鱼叉式钓鱼附件
接触目标与进攻突防	投 递	发送恶意邮件	鱼叉式钓鱼链接
接触目标与进攻突防	投 递	发送恶意邮件	通过服务进行鱼叉式网络钓鱼

两个威胁框架的概要对比

寒夜速纪

威胁框架：认知与实践

03 威胁框架的价值

价 值

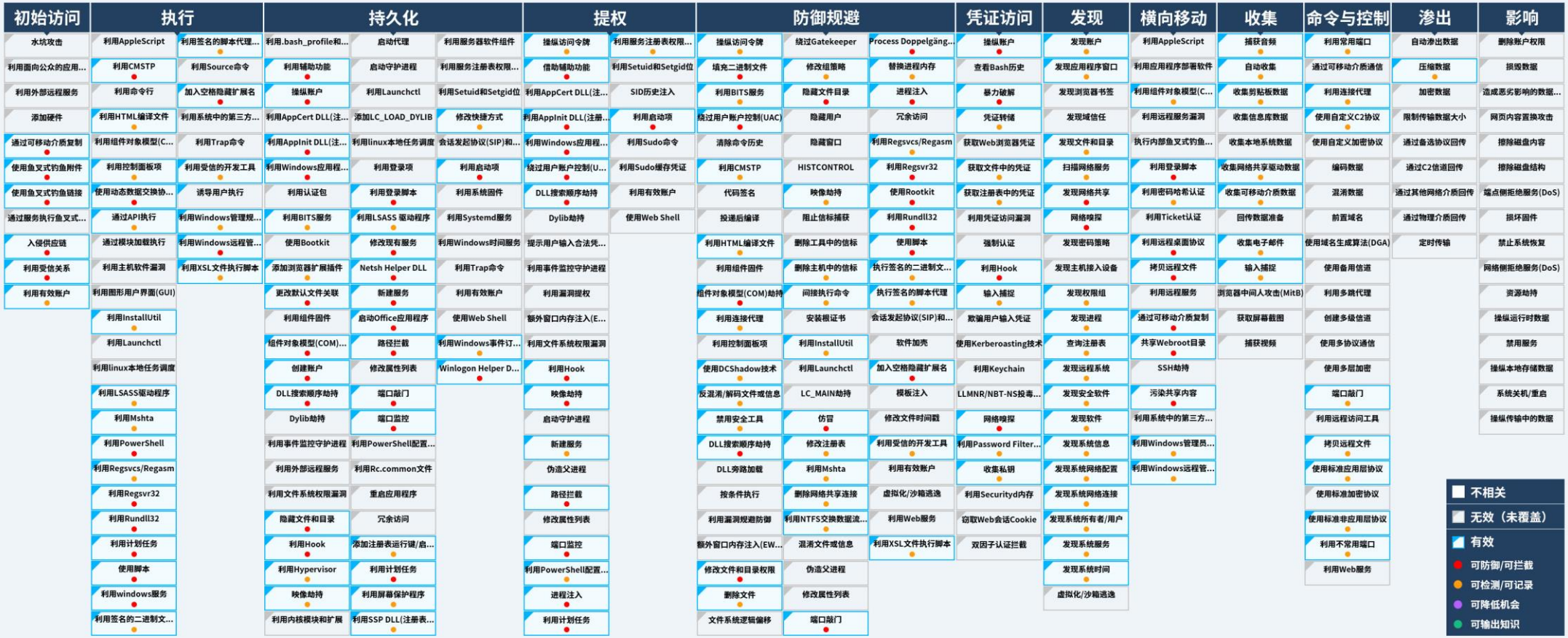
Knowing Is Half The Battle —— G.I. Joe

是故胜兵先胜而后求战，败兵先战而后求胜

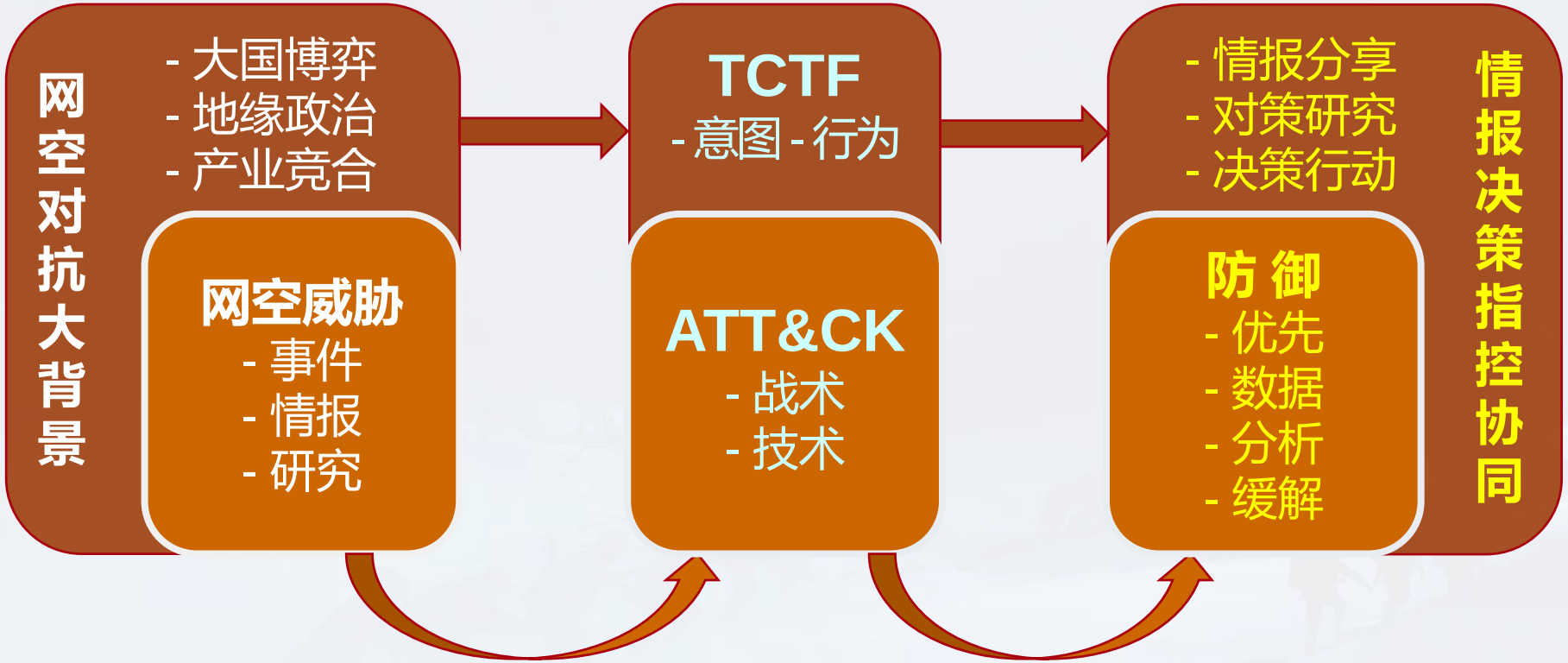
—— 孙子

- **理解对手与威胁，如此方能：**
  - 分析防御差距
  - 检测/缓解攻击者着重使用的技术
  - 跟踪特定对手的技术集合
  - 指导攻击者模拟
  - 评价安全技术，优化安全部署
  - 分析攻击行为与威胁发展态势
  - 等 等

安天智甲ATT&CK覆盖度



防御能力 & 客户收益


网空对抗大背景
- 大国博弈
- 地缘政治
- 产业竞合
网空威胁
- 事件
- 情报
- 研究
TCTF
- 意图 - 行为
ATT&CK
- 战术
- 技术
- 情报分享
- 对策研究
- 决策行动
防 御
- 优先
- 数据
- 分析
- 缓解
情报决策指控协同

谢谢大家