序号	ATT&CK 攻击技术	防守方机会空间	AD 防御技术	实践用例
1	T1001 - 数据混淆	可以检测到攻击活动使用了混淆技术。	DTE0028 - PCAP 收集	防守方可以捕获失陷系统的网络流量，并寻找可能表示数据混淆的异常网络流量。
2	T1001 - 数据混淆	可以发现攻击者试图隐藏数据，避免让防守方发现。	DTE0031 - 协议解码器	防守方可以开发协议解码器，解密网络捕获数据并公开攻击者的命令与控制流量及其渗透活动。
3	T1003 - OS 凭据转储	可以部署绊索，当攻击者接触到网络资源或使用特定技术时就会触发警报。	DTE0012 - 凭据诱饵	防守方可以在系统的各个位置布置诱饵骗凭据，并建立警报，如果攻击者获取了凭据并尝试使用这些凭据，则将触发警报。
4	T1005 - 从本地系统收集敏感数据	在对抗交战场景下，可以通过确保本地系统存储着大量内容来增强真实性。	DTE0030 - 文件诱饵	防守方可以部署各种文件诱饵，提高本地系统的真实性。
5	T1005 - 从本地系统收集敏感数据	在对抗交战场景下，可以提供有关各种主题的内容，查看哪些类型的信息会引起攻击者的兴趣。	DTE0030 - 文件诱饵	防守方可以部署各种文件诱饵，确定攻击者是否对特定文件类型、主题等感兴趣。
6	T1006 - 直接访问卷	防守方可以观察攻击者并控制他们可以看到哪些东西、可以产生什么影响和/或可以访问哪些数据。	DTE0036 - 软件修改、监控	防守方可以使用与直接存取卷相关的API调用，查看正在进行什么活动、正在传输什么数据，或影响该API的调用功能。
7	T1007 - 发现系统服务	防守方可以观察攻击者并控制他们可以看到哪些东西、可以产生什么影响和/或可以访问哪些数据。	DTE0003 - API 监控	防守方可以监控和分析操作系统的功能调用，以进行检测和报警。
8	T1007 - 发现系统服务	防守方可以观察攻击者并控制他们可以看到哪些东西、可以产生什么影响和/或可以访问哪些数据。	DTE0036 - 软件修改、监控	防守方可以修改命令，显示攻击者希望在系统上看到的服务，或向他们显示其意料之外的服务。
9	T1008 - 备用通信信道	可以修改网络，允许/拒绝某些类型的流量，对网络流量进行降级或以其他方式影响攻击者的活动。	DTE0026 - 网络变换	防守方可以识别并拦截特定的攻击命令和控制（C2）流量，查看攻击者的响应方式，这可能会让攻击者暴露其他C2信息。
10	T1010 - 应用程序窗口发现	可以为攻击者提供各种应用程序，这样在攻击者进行发现任务时，防守方就可以发现完整信息。	DTE0004 - 应用仿真	在对抗交战场景下，防守方可以打开并使用系统上安装的应用程序的任何特定子集，控制在什么时间点向攻击者提供什么内容。
11	T1011 - 其他网络介质的数据渗漏	在对抗交战场景下，可以实施安全控制措施，这有助于在长期交战中实现防御目标。	DTE0032 - 安全控制措施	防守方可以阻止攻击者启用Wi-Fi或蓝牙接口，防止其连接到周围的接入点或设备并用于数据渗出。
12	T1012 - 查询注册表	防守方可以观察攻击者并控制他们可以看到哪些东西、可以产生什么影响和/或可以访问哪些数据。	DTE0011 - 诱饵	防守方可以创建注册表对象诱饵，并使用Windows注册表审计来监控对这些注册表对象的访问情况。
13	T1014 - Rootkit	可以阻止攻击者的计划行动，并迫使他们暴露其他TTP。	DTE0001 - 管理员访问权限	防守方可以删除管理员访问权限，迫使攻击者执行权限升级来安装Rootkit。
14	T1014 - Rootkit	在对抗交战场景下，可以采取安全控制措施，让攻击者完成一个任务并扩大交战范围。	DTE0032 - 安全控制措施	在对抗交战场景下，防守方可以确保，通过安全控制措施，不受信代码旨在一个系统上执行。
15	T1016 - 系统网络配置发现	可以影响攻击者，引导其转向你希望与他们交战的系统上来。	DTE0011 - 诱饵	防守方可以创建面包屑或蜜标，诱使攻击者使用系统诱饵或网络服务。
16	T1018 - 远程系统发现	防守方可以观察攻击者并控制他们可以看到哪些东西、可以产生什么影响和/或可以访问哪些数据。	DTE0036 - 软件修改、监控	防守方可以更改远控命令的输出，隐藏您不想受到攻击的模拟元素，并提供您希望与攻击者开战的模拟元素。
17	T1018 - 远程系统发现	在对抗交战场景下，可以通过确保系统诱饵中都是攻击者期望在侦察过程中看到的信息来提高真实性。	DTE0011 - 诱饵	防守方可以在系统诱饵的ARP缓存表、主机文件等中创建条目，提高设备的真实性。
18	T1020 - 自动化数据渗出	可以收集网络数据并分析其中包含的攻击者活动。	DTE0028 - PCAP 收集	收集所有网络流量的完整数据包捕获信息后，您可以查看通过网络连接发生了什么情况，并确定命令和控制流量和/或数据渗出活动。
19	T1020 - 自动化数据渗出	可以发现攻击者试图隐藏数据，避免让防守方发现。	DTE0031 - 协议解码器	防守方可以开发协议解码器，解密网络捕获数据并公开攻击者的命令与控制流量及其渗透活动。
20	T1021 - 远程服务	可以通过网络流量的监控，确定不同协议、异常流量模式、数据传输等，确定是否存在攻击者。	DTE0027 - 网络监控	防守方可以对异常的流量模式、大量或意外的数据传输以及可能显示存在攻击者的其他活动进行网络监控并发出报警。
21	T1021 - 远程服务	在对抗交战场景下，可以引入系统诱饵，从而影响攻击者的行为或让您观察他们是如何执行特定任务的。	DTE0017 - 系统诱饵	防守方可以部署一个运行远程服务的系统诱饵（例如telnet、SSH和VNC），并查看攻击者是否尝试登录该服务。
22	T1025 - 来自可移动介质的数据	在对抗交战场景下，可以通过部署内容来影响攻击者的行为，测试他们对特定主题的兴趣或提高系统或环境的真实性。	DTE0030 - 文件诱饵	防守方可以在附加存储空间中部署各种文件诱饵。数据可能包括与特定人物角色相匹配的主题、攻击者感兴趣的主题等。
23	T1025 - 来自可移动介质的数据	在对抗交战场景下，可以提供有关各种主题的内容，查看哪些类型的信息会引起攻击者的兴趣。	DTE0030 - 文件诱饵	防守方可以部署各种文件诱饵，确定攻击者是否对特定文件类型、主题等感兴趣。
24	T1027 - 混淆的文件或信息	在对抗交战场景下，可以引入系统诱饵，从而影响攻击者的行为或让您观察他们是如何执行特定任务的。	DTE0017 - 系统诱饵	防守方可以部署系统诱饵来研究攻击者如何以及何时混淆文件并隐藏信息。
25	T1029 - 计划传输	可以通过网络流量的监控，确定不同协议、异常流量模式、数据传输等，确定是否存在攻击者。	DTE0027 - 网络监控	防守方可以对异常的流量模式、大量或意外的数据传输以及可能显示存在攻击者的其他活动进行网络监控并发出报警。
26	T1030 - 限制数据传输大小	可以收集网络数据并分析其中包含的攻击者活动。	DTE0028 - PCAP 收集	收集所有网络流量的完整数据包捕获信息后，您可以查看通过网络连接发生了什么情况，并确定命令和控制流量和/或数据渗出活动。
27	T1030 - 限制数据传输大小	可以使用工具和控件来阻止攻击者的活动。	DTE0031 - 协议解码器	防守方可以开发协议解码器，解密网络捕获数据并公开攻击者的命令与控制流量及其渗透活动。
28	T1033 - 发现系统所有者/用户	防守方可以观察攻击者并控制他们可以看到哪些东西、可以产生什么影响和/或可以访问哪些数据。	DTE0036 - 软件修改、监控	防守方可以通过修改或替换展示系统用户的常用命令来影响攻击者的活动。
29	T1036 - 伪装	可以通过识别和警告异常行为，检测是否存在攻击者。	DTE0007 - 行为分析	防守方可以在非标准位置或正在创建异常进程或连接的文件中查找已知文件。

30	T1037 - 登录脚本	可以利用登录脚本的完好副本并经常进行恢复还原，防止攻击者反复使用这些脚本来启动恶意软件。	DTE0006 - 基线	防守方可以频繁重复地将系统还原到经过验证的基线，消除攻击者的持久化机制。
31	T1039 - 网络共享驱动器中的数据	在对抗交战场景下，可以通过部署内容来影响攻击者的行为，测试他们对特定主题的兴趣或提高系统或环境的真实性。	DTE0030 - 文件诱饵	防守方可以在附加存储空间中部署各种文件诱饵。数据可能包括与特定人物角色相匹配的主题、攻击者感兴趣的主题等。
32	T1039 - 网络共享驱动器中的数据	在对抗交战场景下，可以提供有关各种主题的内容，查看哪些类型的信息会引起攻击者的兴趣。	DTE0030 - 文件诱饵	防守方可以部署各种文件诱饵，确定攻击者是否对特定文件类型、主题等感兴趣。
33	T1040 - 网络嗅探	防守方可以观察攻击者并控制他们可以看到哪些东西、可以产生什么影响和/或可以访问哪些数据。	DTE0036 - 软件修改、监控	通过更改通常在系统上找到的网络嗅探程序的输出结果，可以防止攻击者看到特定内容或防止攻击者使用结果。
34	T1040 - 网络嗅探	可以向攻击者展示诱饵进程，以影响其行为，测试其兴趣或提高系统或环境的真实性。	DTE0016 - 进程诱饵	防守方可以在真实系统上运行进程，创建网络工件供攻击者收集。这些工件可能包含诸如凭据、主机名等数据，从而引导攻击者将系统诱饵和网络作为目标。
35	T1040 - 网络嗅探	可以诱使攻击者公开其他TTP。	DTE0025 - 网络仿真	防守方可以添加更多不同端点、服务器、路由器和其他设备，让攻击者拥有更广泛的攻击面。这可能导致攻击者暴露其他功能。
36	T1041 - 使用命令与控制信道窃取	可以通过阻止/取消阻止到达其命令和控制（C2）位置的流量，阻止或允许攻击者的渗透活动。	DTE0026 - 网络变换	防守方可以通过阻止/取消阻止不必要的端口和协议来阻止或允许使用替代协议进行数据渗出。
37	T1041 - 使用命令与控制信道窃取	可以通过阻止/取消阻止到达其命令和控制（C2）位置的流量，阻止或允许攻击者的渗透活动。	DTE0026 - 网络变换	防守方可以限制网络流量，降低攻击者的数据渗出速度或降低渗出数据的可靠性。
38	T1046 - 网络服务扫描	防守方可以观察攻击者并控制他们可以看到哪些东西、可以产生什么影响和/或可以访问哪些数据。	DTE0036 - 软件修改、监控	防守方可以更改远控命令的输出，隐藏您不想受到攻击的模拟元素，并提供您希望与攻击者开战的模拟元素。
39	T1046 - 网络服务扫描	可以研究攻击者并收集有关攻击者及其工具的第一手资料。	DTE0017 - 系统诱饵	防守方可以将系统诱饵添加到网络中，从而让攻击者可以使用多种网络服务。防守方可以观察攻击者在试图使用哪些网络服务。
40	T1047 - WMI	在对抗交战场景下，可以允许或限制管理员访问权限，从而有助于您实现防御目标。	DTE0001 - 管理员访问权限	防守方可以从本地用户中删除管理员访问权限，防止攻击者利用WMI。
41	T1047 - WMI	可以实施安全控制措施，阻止攻击者使用Windows管理规范（WMI），诱使他们泄露新的TTP。	DTE0032 - 安全控制措施	防守者可以加固具有管理员访问权限的帐户，还可以限制任何用户使用WMI进行远程连接。
42	T1048 - 备用协议上的数据渗出	可以通过阻止/取消阻止到达其命令和控制（C2）位置的流量，阻止或允许攻击者的渗透活动。	DTE0026 - 网络变换	防守方可以通过阻止/取消阻止不必要的端口和协议来阻止或允许使用替代协议进行数据渗出。
43	T1049 - 系统网络连接发现	防守方可以观察攻击者并控制他们可以看到哪些东西、可以产生什么影响和/或可以访问哪些数据。	DTE0036 - 软件修改、监控	防守方可以修改、监控列举系统网络连接的常用命令的输出结果。他们可以使用系统诱饵和/或网络来修改、监控输出结果，或者将输出中的真实系统删除，从而让攻击者远离真实系统。
44	T1052 - 物理介质上的数据渗出	可以通过控制交战环境的各个方面来确定攻击者的能力或偏好。	DTE0029 - 外围设备管理	防守方可以使用诱饵外围设备（例如外部Wi-Fi适配器、USB设备等）来确定攻击者是否试图使用这些设备用于数据渗出。
45	T1053 - 计划任务	可以研究攻击者并收集有关攻击者及其工具的第一手资料。	DTE0001 - 管理员访问权限	防守方可以在系统上启用管理员访问权限，查看攻击者是否利用该访问权限来创建计划任务以启动其恶意软件或工具。
46	T1053 - 计划任务	可以研究攻击者并收集有关攻击者及其工具的第一手资料。	DTE0017 - 系统诱饵	防守方可以配置具有有限限制的系统诱饵，查看攻击者是否创建或更改了计划任务以启动其恶意软件。
47	T1053 - 计划任务	可以进行成功概率适度偏高的检测。	DTE0034 - 系统活动监控	如果攻击者创建了新的计划任务或更改了现有任务，则防守方可以捕获系统活动日志并生成警报。
48	T1055 - 进程注入	在对抗交战场景下，可以实施安全控制措施，这有助于在长期交战中实现防御目标。	DTE0032 - 安全控制措施	防守方可以实施安全控制措施，以影响进程注入技术，例如AppLocker或旨在监控CreateRemoteThread事件的防病毒/EDR工具。
49	T1056 - 捕获用户输入	可以向攻击者提供内容，以影响其行为，测试其对特定主题的兴趣或提高系统或环境的真实性。	DTE0011 - 诱饵	防守方可以使用键盘记录器或其他工具将诱饵数据提供给攻击者，从而形成对抗。
50	T1057 - 进程发现	防守方可以观察攻击者并控制他们可以看到哪些东西、可以产生什么影响和/或可以访问哪些数据。	DTE0036 - 软件修改、监控	防守方可以修改命令，不再显示正在运行的进程的真实列表，从而向攻击者隐藏了必要的主动防御进程。
51	T1057 - 进程发现	可以向攻击者展示诱饵进程，以影响其行为，测试其兴趣或提高系统或环境的真实性。	DTE0016 - 进程诱饵	防守方可以在系统上运行诱饵进程来吸引攻击者。
52	T1059 - 命令行界面	防守方可以观察攻击者并控制他们可以看到哪些东西、可以产生什么影响和/或可以访问哪些数据。	DTE0036 - 软件修改、监控	防守方可以修改、监控系统命令的输出结果，更改攻击者在其活动期间可能使用的信息。
53	T1059 - 命令行界面	防守方可以观察攻击者并控制他们可以看到哪些东西、可以产生什么影响和/或可以访问哪些数据。	DTE0036 - 软件修改、监控	防守方可以修改用于删除文件的命令功能，以便在删除文件之前将文件复制到一个安全位置。
54	T1059 - 命令行界面	防守方可以观察攻击者并控制他们可以看到哪些东西、可以产生什么影响和/或可以访问哪些数据。	DTE0034 - 系统活动监控	防守方可以通过监控他们在系统上执行的命令和/或脚本创建的进程来检测是否存在攻击者。
55	T1068 - 利用漏洞进行权限升级	可以研究攻击者并收集有关攻击者及其工具的第一手资料。	DTE0001 - 管理员访问权限	防守方可以将系统用户配置为没有管理员访问权限，确保要通过漏洞利用才能进行权限升级。
56	T1069 - 组权限发现	在对抗交战场景下，可以影响攻击者在系统上执行命令时能够看到哪些内容。	DTE0036 - 软件修改、监控	防守方可以修改、监控系统的软件来更改攻击者显示组权限信息的结果。
57	T1070 - 删除主机上的指标	在对抗交战场景下，可以允许或限制管理员访问权限，从而有助于您实现防御目标。	DTE0001 - 管理员访问权限	防守方可以限制管理员访问权限，迫使攻击者提升权限，删除系统中的日志和捕获的工件。
58	T1070 - 删除主机上的指标	可以通过识别和警告异常行为，检测是否存在攻击者。	DTE0007 - 行为分析	防守方可以查找系统上命令执行的异常情况。这可能会暴露潜在的恶意活动。
59	T1071 - 标准应用层协议	可以通过网络流量的监控，确定不同协议、异常流量模式、数据传输等，确定是否存在攻击者。	DTE0027 - 网络监控	防守方可以对异常的流量模式、大量或意外的数据传输以及可能显示存在攻击者的其他活动进行网络监控并发出报警。

60	T1072 - 利用第三方软件部署工具	可以研究攻击者并收集有关攻击者及其工具的第一手资料。	DTE0017 - 系统诱饵	在对抗交战场景下，防守方可以部署诱饵软件部署工具，以查看攻击者在其活动期间是否尝试使用这些工具。
61	T1074 - 暂存数据	在对抗交战场景下，可以通过部署内容来影响攻击者的行为，测试他们对特定主题的兴趣或提高系统或环境的真实性。	DTE0030 - 文件诱饵	防守方可以围绕系统部署带有已知哈希值的各种文件诱饵。如果发现这些哈希值在系统中或网络外移动，则可以进行检测。
62	T1078 - 有效凭证	可以使用让系统看起来更真实的用户帐户。	DTE0010 - 账户诱饵	防守方可以创建诱饵用户帐户，让系统诱饵或网络看起来更真实。
63	T1078 - 有效凭证	可以部署绊索，当攻击者接触到网络资源或使用特定技术时就会触发警报。	DTE0012 - 凭据诱饵	防守方可以在系统的各个位置布置诱饵凭据，并建立警报，如果攻击者获取了凭据并尝试使用这些凭据，则将触发警报。
64	T1078 - 有效凭证	可以准备好用户帐户，看起来使用过而且更真实。	DTE0008 - 伪装真实业务环境	防守方可以通过登录诱饵帐户并按照整个欺骗流程使用诱饵帐户来准备系统诱饵，从而在系统中创建看起来更真实的工件。
65	T1080 - 污染共享内容	可以向攻击者提供内容，以影响其行为，测试其对特定主题的兴趣或提高系统或环境的真实性。	DTE0011 - 诱饵	防守方可以在对抗交战网络中部署网络共享诱饵，查看攻击者是否将其用于有效载荷传递或横向移动。
66	T1082 - 系统信息发现	可以向攻击者提供内容，以影响其行为，测试其对特定主题的兴趣或提高系统或环境的真实性。	DTE0011 - 诱饵	当攻击者进行系统信息发现时，防守方可以使用诱饵，从而让攻击者对系统留下一个错误印象。
67	T1083 - 文件与目录发现	可以向攻击者提供内容，以影响其行为，测试其对特定主题的兴趣或提高系统或环境的真实性。	DTE0011 - 诱饵	防守方可以利用文件诱饵与目录来提供可供攻击者使用的内容。
68	T1087 - 账户发现	防守方可以观察攻击者并控制他们可以看到哪些东西、可以产生什么影响和/或可以访问哪些数据。	DTE0036 - 软件修改、监控	防守方可以更改帐户列举命令的输出结果，从而隐藏帐户或显示不存在的帐户。
69	T1087 - 账户发现	在对抗交战场景下，可以在列举过程中向攻击者提供诱饵帐户。	DTE0010 - 账户诱饵	在对抗战中，防守方可以利用诱骗帐户向攻击者提供内容并鼓励其他活动。
70	T1087 - 账户发现	可以利用各种类型的诱骗帐户来查看攻击者对哪些内容最感兴趣。	DTE0013 - 设置多类诱饵	防守方可以准备各种诱骗帐户，并查看攻击者会对哪些特定类型、特定权限和组访问权限的账户感兴趣。
71	T1090 - 连接代理	可以阻止试图通过代理进行连接的攻击者。	DTE0026 - 网络变换	防守方可以通过使用网络允许和阻止列表来拦截流向已知匿名网络和C2基础结构的流量。
72	T1091 - 通过可移动介质进行复制	可以部署绊索，当攻击者接触到网络资源或使用特定技术时就会触发警报。	DTE0034 - 系统活动监控	防守方可以监控系统中是否使用了可移动介质。
73	T1091 - 通过可移动介质进行复制	可以使用安全控制措施来阻止或允许攻击者的活动。	DTE0032 - 安全控制措施	防守方可以禁用Autorun，防止在将可移动介质插入系统后自动执行恶意软件。
74	T1091 - 通过可移动介质进行复制	可以研究可移动介质，查看其是否受到感染以及将其插入系统诱饵或网络时会发生什么情况。	DTE0023 - 缓解攻击向量	防守方可以将可疑的可移动介质设备连接到系统诱饵，并查看启用autorun后会发生什么情况。
75	T1091 - 通过可移动介质进行复制	可以阻止攻击者使用可移动介质来破坏断网系统或气隙系统。	DTE0022 - 隔离	防守方可以设置保护，这样一来，只有在通过单独的审核流程清除了驱动器之后，才能安装可移动介质。
76	T1092 - 通过可移动介质进行通信	可以通过控制交战环境的各个方面来确定攻击者的能力或偏好。	DTE0029 - 外围设备管理	在拦截了攻击者用来中继命令的可移动介质后，防守方可以将可移动介质插入系统诱饵或网络中，观察正在中继的命令以及攻击者接下来会做什么。
77	T1092 - 通过可移动介质进行通信	可以通过控制交战环境的各个方面来确定攻击者的能力或偏好。	DTE0023 - 缓解攻击向量	在拦截了攻击者用来中继命令的可移动介质后，防守方可以将可移动介质插入系统诱饵或网络中，观察正在中继的命令以及攻击者接下来会做什么。
78	T1095 - 标准非应用层协议	可以通过识别和警告异常行为，检测是否存在攻击者。	DTE0007 - 行为分析	防守方可以检测到使用的非标准协议。通过对某个系统或一组系统的协议流量骤增的情况进行行为分析，防守方可能能够检测到攻击者的恶意通信。
79	T1098 - 账户修改、监控	可以进行成功概率适度偏高的检测。	DTE0034 - 系统活动监控	防守方可以进行监控，若用户帐户在正常工作时间之外发生更改或从远程位置等发生更改，则进行报警。
80	T1098 - 账户修改、监控	可以研究攻击者并收集有关攻击者及其工具的第一手资料。	DTE0010 - 账户诱饵	防守方可以使用诱饵帐户并监控这些账户是否进行了某些活动，表明账户遭到攻击者控制。
81	T1098 - 账户修改、监控	可以使用安全控制措施来阻止或允许攻击者的活动。	DTE0032 - 安全控制措施	防守方可以强制执行严格的身份验证要求，例如更改密码、双因素身份验证等，以影响或破坏攻击者的活动。
82	T1102 - 网络服务	可以通过识别和警告异常行为，检测是否存在攻击者。	DTE0007 - 行为分析	防守方可以检测是否使用了外部网络服务用于通信中继。通过对系统通信的域、通信频率和通信时间点进行异常行为分析，防守方可能能够识别恶意流量。
83	T1104 - 多阶段通信信道	可以检测到用于命令和控制的未知进程并破坏该进程。	DTE0022 - 隔离	防守方可以隔离用于命令和控制的未知进程，并阻止未知进程访问Internet。
84	T1104 - 多阶段通信信道	可以修改、监控网络，允许/拒绝某些类型的流量，对网络流量进行降级或以其他方式影响攻击者的活动。	DTE0026 - 网络变换	防守方可以实施可以感知协议的IPS，来限制系统与Internet上的未知位置进行通信。
85	T1105 - 远程文件拷贝	可以收集网络数据并分析其中包含的攻击者活动。	DTE0028 - PCAP 收集	收集所有网络流量的完整数据包捕获信息后，您可以查看通过网络连接发生了什么情况，并确定命令和控制流量和/或数据渗出活动。
86	T1106 - 通过API执行	防守方可以观察攻击者并控制他们可以看到哪些东西、可以产生什么影响和/或可以访问哪些数据。	DTE0036 - 软件修改、监控	防守方可以修改系统调用，中断通信，然后将攻击路由到系统诱饵，阻止完全执行等。
87	T1106 - 通过API执行	防守方可以观察攻击者并控制他们可以看到哪些东西、可以产生什么影响和/或可以访问哪些数据。	DTE0003 - API 监控	防守方可以监控操作系统功能调用，查找攻击者是否使用和/或滥用了功能调用。
88	T1110 - 暴力破解	可以进行成功概率适度偏高的检测。	DTE0034 - 系统活动监控	防守方可以监控用户登录活动，查看是否有攻击者使用了暴力破解技术。
89	T1111 - 双因素身份验证拦截	可以研究攻击者并收集有关攻击者及其工具的第一手资料。	DTE0032 - 安全控制措施	在对抗交战场景下，防守方可以有意地增加令牌的有效时间窗口，查看攻击者是否能够获取和利用令牌。

90	T1111 - 双因素身份验证拦截	如果攻击者没有按照公司记录在案的SOP（标准操作流程）操作，防守方就有可能会检测到攻击者的活动。	DTE0033 - SOP（标准操作流程）	防守方可以实施SOP（标准操作流程），限制用户在不调用其他进程的情况下多次使用2FA或MFA。
91	T1112 - 修改注册表	如果攻击者进行任何更改，防守方就可以利用注册表信息的完好副本，还原注册表。	DTE0006 - 基线	防守方可以启用对特定键的注册表审核，在每次更改值时产生报警，并将这些键还原到基线值。
92	T1112 - 修改注册表	可以研究攻击者并收集有关攻击者及其工具的第一手资料。	DTE0034 - 系统活动监控	防守方可以监控进程和命令行参数，攻击者可能会使用进程和命令行参数来更改或删除Windows注册表中的信息。
93	T1113 - 屏幕截图	可以向攻击者提供内容，以影响其行为，测试其对特定主题的兴趣或提高系统或环境的真实性。	DTE0011 - 诱饵	防守方可以在屏幕上显示诱饵，引起攻击者的兴趣，引导攻击者进一步作战。
94	T1114 - 电子邮件收集	可以影响攻击者，引导其转向你希望与他们交战的系统上来。	DTE0011 - 诱饵	防守方可以植入包含欺骗性内容和面包屑的电子邮件诱饵，诱使攻击者使用系统诱饵。
95	T1115 - 剪贴板数据	可以为攻击者引入一些数据，以影响他们的未来行为。	DTE0011 - 诱饵	防守方可以将诱饵插入系统的剪贴板中，以供攻击者查找。
96	T1119 - 自动收集	在对抗交战场景下，可以通过部署内容来影响攻击者的行为，测试他们对特定主题的兴趣或提高系统或环境的真实性。	DTE0030 - 文件诱饵	防守方可以部署各种文件诱饵，查看攻击者是否自动收集了这些文件中的任何文件。
97	T1120 - 外围设备发现	可以评估攻击者是否有兴趣连接外围设备。	DTE0029 - 外围设备管理	防守方可以将一个或多个外围设备连接到系统诱饵，查看攻击者是否对这些外围设备感兴趣。
98	T1120 - 外围设备发现	可以通过控制交战环境的各个方面来确定攻击者的能力或偏好。	DTE0029 - 外围设备管理	防守方可以插入USB驱动器，并查看攻击者发现和检查驱动器的速度。
99	T1123 - 音频捕获	可以向攻击者提供内容，以影响其行为，测试其对特定主题的兴趣或提高系统或环境的真实性。	DTE0011 - 诱饵	防守方可以添加诱饵音频内容，让攻击者相信他们的音频捕获工作正在有效运行。
100	T1123 - 音频捕获	可以更改系统，防止攻击者捕获音频内容。	DTE0020 - 硬件修改	防守方可以移除或禁用系统的麦克风和网络摄像头，从而无法进行音频捕获。
101	T1124 - 系统时间发现	防守方可以观察攻击者并控制他们可以看到哪些东西、可以产生什么影响和/或可以访问哪些数据。	DTE0036 - 软件修改、监控	如果防守方知道攻击者所针对的是哪个特定区域，那么防守方就可以更改命令的输出内容，返回系统时间，以返回攻击者希望看到的内容。
102	T1125 - 视频捕获	可以向攻击者提供内容，以影响其行为，测试其对特定主题的兴趣或提高系统或环境的真实性。	DTE0011 - 诱饵	防守方可以添加视频内容，让攻击者相信他们的捕获工作正在有效运行。
103	T1125 - 视频捕获	可以更改系统，防止攻击者捕获视频内容。	DTE0020 - 邮件修改	防守方可以删除或禁用系统的网络摄像头，并删除任何视频捕获应用程序，让攻击者无法进行视频捕获。
104	T1127 - 受信任的开发工具	可以进行成功概率适度偏高的检测。	DTE0034 - 系统活动监控	防守方可以通过监控他们在系统上执行的命令和/或脚本创建的进程来检测是否存在攻击者。
105	T1129 - 通过模块加载执行	防守方可以观察攻击者并控制他们可以看到哪些东西、可以产生什么影响和/或可以访问哪些数据。	DTE0036 - 软件修改、监控	防守方可以修改系统调用，中断通信，然后将攻击路由到系统诱饵，阻止完全执行等。
106	T1132 - 数据编码	可以发现攻击者试图隐藏数据，避免让防守方发现。	DTE0031 - 协议解码器	防守方可以开发协议解码器，解密网络捕获数据并公开攻击者的命令与控制流量及其渗透活动。
107	T1133 - 外部远程服务	可以确定攻击者是否已获得了网络中的有效帐户凭据，并他们是否正试图使用这些凭据通过远程服务访问您的网络。	DTE0017 - 系统诱饵	防守方可以设置诱饵VPN服务器，并查看攻击者是否尝试使用有效帐户对其进行身份验证。
108	T1134 - 篡改访问令牌	防守方可以观察攻击者并控制他们可以看到哪些东西、可以产生什么影响和/或可以访问哪些数据。	DTE0036 - 软件修改、监控	防守方可以使用虚假数据用于提供凭据或重定向凭据请求，从而将攻击者引诱到网络诱饵或系统中。
109	T1134 - 篡改访问令牌	可以通过识别和警告异常行为，检测是否存在攻击者。	DTE0007 - 行为分析	防守方可以进行行为分析来检测常见的访问令牌篡改技术，并允许或拒绝这些操作。
110	T1135 - 网络共享发现	在对抗交战场景下，防守方可以引入诱饵，吸引攻击者进一步作战。	DTE0011 - 诱饵	防守方可以利用网络诱饵共享来提供攻击者可能会利用的内容。
111	T1135 - 网络共享发现	可以向攻击者提供各种不同的网络诱饵共享，查看攻击者查看和使用了哪些内容。	DTE0013 - 设置多类诱饵	防守方可以为攻击者提供各种网络诱饵共享，并查看攻击者是否对某些具有特定名称、权限等的共享感兴趣。
112	T1136 - 创建账户	可以进行成功概率适度偏高的检测。	DTE0033 - SOP（标准操作流程）	防守方可以检测在可接受进程之外创建的用户帐户。
113	T1137 - 启动Office应用程序	可以进行成功概率适度偏高的检测。	DTE0034 - 系统活动监控	防守方可以收集系统进程信息，并查找与Office进程相关的异常活动。
114	T1140 - 反混淆/解码文件或信息	防守方可以观察攻击者并控制他们可以看到哪些东西、可以产生什么影响和/或可以访问哪些数据。	DTE0003 - API 监控	防守方可以监控和分析操作系统的功能调用，以进行检测和报警。
115	T1176 - 浏览器扩展	可以使用工具和控件来阻止攻击者的活动。	DTE0006 - 基线	防守方可以强制删除公司策略禁止的浏览器扩展。
116	T1185 - 浏览器中间人	在对抗交战场景下，可以准备一些用户的浏览器数据（会话、Cookie等），让浏览器看起来更真实，且内容丰富。	DTE0008 - 伪装真实业务环境	随着时间的推移，防守方可以在系统诱饵上执行Web浏览任务，从而为攻击者提供强大的浏览器数据集，这些数据看起来很逼真，并且有可能在攻击者对抗交战时使用。
117	T1187 - 强制身份验证	为了延长对抗交战时间或启用检测，可以给攻击者带来一些您希望攻击者收集和使用的凭据。	DTE0012 - 凭据诱饵	防守方在攻击者试图进行强制身份验证漏洞利用时，可以在交战所在服务器上部署凭据诱饵。
118	T1187 - 强制身份验证	可以修改、监控网络，允许/拒绝某些类型的流量，对网络流量进行降级或以其他方式影响攻击者的活动。	DTE0026 - 网络变换	防守方可以允许或拒绝来自网络的出站SMB请求，从而影响强制身份验证是否成功。防守方可以选择将出站SMB请求重定向到系统诱饵，阻止凭据窃取。
119	T1189 - 网站挂马攻击	可以研究攻击者并收集有关攻击者及其工具的第一手资料。	DTE0017 - 系统诱饵	防守方可以使用系统诱饵访问失陷网站，查看其运行方式（研究漏洞利用顺序、收集相关工件等）。

120	T1189 - 网站挂马攻击	可以发现攻击者的攻击人物或对象。	DTE0013 - 设置多类诱饵	防守方可以使用一个诱饵或具有不同网址、操作系统、Web浏览器、语言设置的一组诱饵，来确定访问失陷网站的每个系统是否都收到了恶意载荷，还是只有特定系统收到了。
121	T1189 - 网站挂马攻击	可以使用失陷的挂马网站开始与攻击者进行长期交战，并观察攻击者漏洞利用后的TTP。	DTE0014 - 网络诱饵	防守方若想要了解失陷后攻击者的对抗活动，则可以使用网络诱饵中的失陷网站，其中，该网络诱饵中某个系统是专为让攻击者顺利通过最初渗透，从而实现对抗交战而设计的。
122	T1190 - 利用互联网上应用程序的缺陷	可以部署绊索，当攻击者接触到网络资源或使用特定技术时就会触发警报。	DTE0017 - 系统诱饵	防守方可以使用运行面向公众的应用程序的系统诱饵，来查看攻击者是否试图破坏该系统并了解其TTP。
123	T1190 - 利用互联网上应用程序的缺陷	可以给攻击者呈现几个面向公众的应用程序方案，查看攻击者所针对的是哪个应用程序。	DTE0013 - 设置多类诱饵	防守方可以使用多种系统诱饵来研究攻击者，并确定他们选择利用哪种面向公众的应用程序。
124	T1195 - 供应链攻击	部署之前，可以在受控环境中测试和验证硬件和/或软件的添加情况。	DTE0014 - 网络诱饵	防守方可以在隔离的系统或网络上安装任何可疑的硬件或软件，并监视非标准行为。
125	T1197 - BITS 作业	可以在系统上使用安全控制措施，以影响攻击者是否会取得成功。	DTE0032 - 安全控制措施	防守方可以使用基于主机的工具来检测常见的持久化机制，并成功阻止进程执行。
126	T1197 - BITS 作业	可以监控系统上的日志，了解攻击者的常见行为方式，并对攻击者的活动进行检测。	DTE0034 - 系统活动监控	通过收集系统日志，防守方可以进行检测，从而发现异常的BITS使用情况。
127	T1199 - 可信关系	如果确定并限制了受信合作伙伴的授权行为，在攻击者利用信任关系时就更容易被发现。	DTE0034 - 系统活动监控	防守方可以监控受信任伙伴的访问情况，检测未经授权的活动。
128	T1200 - 硬件接入	可以在隔离的环境中测试硬件接入情况，并确保攻击者无法使用。	DTE0022 - 隔离	防守方可以在隔离的系统上安装任何可疑的硬件，并监视非标准行为。
129	T1201 - 密码策略发现	在对抗交战场景下，可以影响攻击者在系统上执行命令时能够看到哪些内容。	DTE0036 - 软件修改、监控	防守方可以更改密码策略描述，从而让攻击者不确定确切的要求是什么。
130	T1202 - 间接命令执行	可以通过识别和警告异常行为，检测是否存在攻击者。	DTE0007 - 行为分析	防守方可以进行行为分析，标明系统上的某项活动正在以非标准方式执行命令。这可能表明存在恶意活动。
131	T1203 - 利用客户端漏洞获取执行权限	可以研究攻击者并收集有关攻击者及其工具的第一手资料。	DTE0017 - 系统诱饵	防守方可以使用系统诱饵来查看，攻击者是否利用易受攻击的软件来攻陷系统。
132	T1203 - 利用客户端漏洞获取执行权限	可以发现攻击者的攻击人物或对象。	DTE0004 - 应用仿真	防守方可以在系统诱饵上安装一款或多款应用程序，其中系统上存在不同的补丁程序级别，以此来查看攻击者会如何利用这些应用程序。
133	T1204 - 用户执行	可以研究攻击者并收集有关攻击者及其工具的第一手资料。	DTE0018 - 引爆恶意软件	防守方可以在系统诱饵上执行对抗恶意软件，并检查其行为或可能与攻击者交战以获得进一步的情报。
134	T1205 - 流量特征	可以通过网络流量的监控，确定不同协议、异常流量模式、数据传输等，确定是否存在攻击者。	DTE0027 - 网络监控	防守方可以对异常的流量模式、大量或意外的数据传输以及可能显示存在攻击者的其他活动进行网络监控并发出报警。
135	T1207 - 域控制器	可以通过识别和警告异常行为，检测是否存在攻击者。	DTE0007 - 行为分析	防守方可以进行行为分析，以指示域控制器上或针对域控制器的活动。与域计划任务不同步的活动，或导致与网络上特定系统的流量骤增的活动，都可能是恶意活动。
136	T1210 - 利用远程服务	可以为攻击者提供各种应用程序，以查看攻击者喜欢什么或影响他们的操作。	DTE0004 - 应用仿真	防守方可以使用各种各样的应用程序来保护系统诱饵或进程。可以对这些应用程序进行加固以测试攻击者的能力，也可以对这些应用程序进行漏洞利用，诱使攻击者朝该方向发展。
137	T1211 - 利用漏洞实现防御绕过	可以为攻击者提供各种应用程序，以查看攻击者喜欢什么或影响他们的操作。	DTE0004 - 应用仿真	防守方可以使用各种各样的应用程序来保护系统诱饵或进程。可以对这些应用程序进行加固以测试攻击者的能力，也可以对这些应用程序进行漏洞利用，诱使攻击者朝该方向发展。
138	T1212 - 利用漏洞获取凭证访问的权限	在对抗交战场景下，可以使用系统上的各种应用程序来查看攻击者试图利用什么来获取凭据。	DTE0004 - 应用仿真	防守方可以在系统诱饵或网络诱饵上使用各种应用程序，以查看攻击者试图利用什么来获取凭据。
139	T1213 - 信息存储库中的数据	在对抗交战场景下，可以通过部署内容来影响攻击者的行为，测试他们对特定主题的兴趣或提高系统或环境的真实性。	DTE0030 - 文件诱饵	防守方可以在附加存储空间中部署各种文件诱饵。数据可能包括与特定人物角色相匹配的主题、攻击者感兴趣的主题等。
140	T1213 - 信息存储库中的数据	在对抗交战场景下，可以提供有关各种主题的内容，查看哪些类型的信息会引起攻击者的兴趣。	DTE0030 - 文件诱饵	防守方可以部署各种文件诱饵，确定攻击者是否对特定文件类型、主题等感兴趣。
141	T1216 - 利用已签名脚本代理执行	可以通过识别和警告异常行为，检测是否存在攻击者。	DTE0007 - 行为分析	防守方可以查找系统上命令执行的异常情况。这可能会暴露潜在的恶意活动。
142	T1217 - 发现浏览器书签发	可以向攻击者提供内容，以影响其行为，测试其对特定主题的兴趣或提高系统或环境的真实性。	DTE0011 - 诱饵	防守方可以使用诱饵让攻击者对系统本质形成错觉，诱使攻击者继续交战。
143	T1218 - 利用已签名的二进制文件代理执行	可以阻止攻击者的计划行动，并迫使他们暴露其他TTP。	DTE0036 - 软件修改、监控	防守方可以监控操作系统功能调用，查找攻击者是否使用和/或滥用了功能调用。
144	T1218 - 利用已签名的二进制文件代理执行	可以研究攻击者并收集有关攻击者及其工具的第一手资料。	DTE0018 - 引爆恶意软件	防守方可以利用系统诱饵上或网络诱饵中的签名二进制文件引爆恶意代码，以查看其行为方式或诱使攻击者进一步交战。
145	T1218 - 利用已签名的二进制文件代理执行	可以进行成功概率适度偏高的检测。	DTE0003 - API 监控	防守方可以监控和分析操作系统的功能调用，以进行检测和报警。
146	T1219 - 远程访问工具	可以研究攻击者并收集有关攻击者及其工具的第一手资料。	DTE0017 - 系统诱饵	防守方可以在整个网络的系统诱饵上安装远程访问工具，以查看攻击者是否将这些工具用于命令和控制。
147	T1220 - XSL 脚本处理	可以通过识别和警告异常行为，检测是否存在攻击者。	DTE0007 - 行为分析	防守方可以通过行为分析来检测XSL进程是否有异常行为。
148	T1221 - 模板注入	可以研究攻击者并收集有关攻击者及其工具的第一手资料。	DTE0017 - 系统诱饵	防守方可以部署易于获得访问权限并安装了Office的系统诱饵。可以监控系统诱饵，以查看攻击者是否试图将恶意软件注入Office模板。
149	T1222 - 修改文件或目录权限	在对抗交战场景下，可以通过部署内容来影响攻击者的行为，测试他们对特定主题的兴趣或提高系统或环境的真实性。	DTE0030 - 文件诱饵	防守方可以将内容有用的文件呈现给攻击者，但可以锁定权限，目的是迫使攻击者公开其TTP来规避限制。

150	T1480 - 执行防护	可以通过识别和警告异常行为，检测是否存在攻击者。	DTE0007 - 行为分析	防守方可以进行行为分析，以检测是否有攻击者对常用防护进行检查，例如VM工件检查、连续存储区和/或设备的列举、域信息等等。
151	T1480 - 执行防护	可以为攻击者提供各种应用程序，以查看攻击者喜欢什么或影响他们的操作。	DTE0004 - 应用仿真	防守方可以使用各种各样的应用程序来保护系统诱饵或进程。可以对这些应用程序进行加固以测试攻击者的能力，也可以对这些应用程序进行漏洞利用，诱使攻击者朝该方向发展。
152	T1482 - 域信任发现	防守方可以创建网络诱饵，在执行信任发现时让系统可以发现网络诱饵，以此延长攻击者的交战时间。	DTE0014 - 网络诱饵	防守方可以创建一个网络诱饵，其中包含易于发现并吸引攻击者的系统。
153	T1482 - 域信任发现	为了延长对抗交战时间或启用检测，可以给攻击者带来一些您希望攻击者收集和使用的凭据。	DTE0012 - 凭据诱饵	防守方可以在多个位置部署凭据诱饵，增加攻击者发现和使用凭据诱饵的几率。
154	T1484 - 修改组策略	可以部署绊索，当攻击者接触到网络资源或使用特定技术时就会触发警报。	DTE0034 - 系统活动监控	防守方可以使用Windows事件日志监控目录服务的更改情况。发生更改则表示存在网络攻击者。
155	T1485 - 销毁数据	可以测试如果防守方有选择地替换了被破坏的数据，攻击者会怎么做。	DTE0005 - 备份与恢复	防守方可以确保定期备份数据，并且备份可以从系统脱机存储。如果检测到攻击者破坏或更改了数据，则防守方可以选择性地从备份中还原数据，以查看攻击者的反应。
156	T1485 - 销毁数据	可以阻止攻击者的计划行动，并迫使他们暴露其他TTP。	DTE0036 - 软件修改、监控	防守方可以修改、监控系统上的命令，因此，攻击者无法通过常规方式删除数据。
157	T1485 - 销毁数据	可以进行成功概率适度偏高的检测。	DTE0034 - 系统活动监控	防守方可以使用进程监控来查找是否执行了某些通常用于数据销毁的实用程序（例如SDelete）。
158	T1486 - 数据加密	可以进行成功概率适度偏高的检测。	DTE0034 - 系统活动监控	防守方可以使用进程监控来查找是否执行了某些通常用于勒索软件和其他数据加密的实用程序。
159	T1486 - 数据加密	可以测试如果防守方有选择地替换了加密数据，攻击者会怎么做。	DTE0005 - 备份与恢复	防守方可以确保定期备份数据，并且备份可以从系统脱机存储。如果检测到攻击者破坏或更改了数据，则防守方可以选择性地从备份中还原数据，以查看攻击者的反应。
160	T1489 - 服务停止	可以通过识别和警告异常行为，检测是否存在攻击者。	DTE0007 - 行为分析	防守方可以查找系统服务状态中的异常情况并对可疑情况发出报警，从而检测到潜在的恶意活动，并对系统进行分类，以重新启用已停止的服务。
161	T1490 - 禁用系统恢复	可以进行成功概率适度偏高的检测。	DTE0034 - 系统活动监控	防守方可以使用进程监控来查找通常用于禁用系统恢复的命令执行情况和命令行参数。
162	T1491 - 篡改	可以通过监控网站未经授权的变更情况来检测是否有（内部或外部）攻击者修改了网站内容。	DTE0034 - 系统活动监控	防守方可以监控网站的内容意外更改，并在检测到活动时生成警报。
163	T1491 - 篡改	可以通过快速恢复更改后的内容来破坏攻击者的篡改活动。	DTE0005 - 备份与恢复	防守方可以确保定期备份数据，并且备份可以从系统脱机存储。如果检测到攻击者破坏或更改了数据，则防守方可以选择性地从备份中还原数据，以查看攻击者的反应。
164	T1495 - 固件损坏	可以进行成功概率适度偏高的检测。	DTE0034 - 系统活动监控	防守方可以收集系统活动信息，并检测与固件交互的命令。这样可以加快系统的恢复速度。
165	T1496 - 资源劫持	可以通过识别和警告异常行为，检测是否存在攻击者。	DTE0007 - 行为分析	通过查找主机资源消耗中的异常并对可疑活动发出报警，防守方偶尔可以检测到系统资源的异常使用情况。
166	T1497 - 逃避虚拟化/沙箱检测	可以部署虚拟系统诱饵，查看攻击者是否发现了虚拟化或对虚拟化做出什么反应。	DTE0017 - 系统诱饵	防守方可以部署虚拟系统诱饵，查看攻击者是否识别出虚拟化并做出反应。
167	T1497 - 逃避虚拟化/沙箱检测	可以布置诱饵，让非虚拟系统看起来像虚拟化系统，以了解攻击者会有何反应。	DTE0011 - 诱饵	防守方可以植入文件、注册表项、软件、进程等，让系统看上去像一个VM，但实际上并不是。
168	T1498 - 网络拒绝服务	可以更改网络配置，破坏攻击者试图通过拒绝服务来影响网络或系统的企图。	DTE0026 - 网络变换	防守方可以配置网络设备来分析网络流量，检测潜在的DoS攻击并进行适当的调整来缓解这种情况。
169	T1499 - 端点拒绝服务	可以更改网络配置，破坏攻击者试图通过拒绝服务来影响网络或系统的企图。	DTE0026 - 网络变换	防守方可以配置网络设备来分析网络流量，检测潜在的DoS攻击并进行适当的调整来缓解这种情况。
170	T1499 - 端点拒绝服务	可以阻止攻击者的计划行动，并迫使他们暴露其他TTP。	DTE0032 - 安全控制措施	防守方可以将系统配置为拦截在一定时间段内出现多次身份验证失败的任何系统。
171	T1505 - 服务器软件组件	可以研究攻击者并收集有关攻击者及其工具的第一手资料。	DTE0004 - 应用仿真	防守方可以安装具有可扩展功能的诱饵服务。
172	T1518 - 软件发现	可以为攻击者提供各种应用程序，以查看攻击者喜欢什么或影响他们的操作。	DTE0004 - 应用仿真	防守方可以在系统上安装各种软件包，让系统看起来是使用过的而且内容丰富。这将为攻击者提供一系列软件，以便攻击者与其他技术进行交互并可能暴露其他技术。
173	T1525 - 植入容器镜像	可以通过识别和警告异常行为，检测是否存在攻击者。	DTE0007 - 行为分析	防守方可以监控用户与镜像和容器的交互情况，以识别哪些镜像和容器是异常添加或更改的。
174	T1526 - 云服务发现	可以在网络诱饵中增添服务，以确定攻击者是否注意到并尝试了解有关服务的更多信息。	DTE0014 - 网络诱饵	防守方可以使用网络诱饵并将其植入云服务中，以查看攻击者如何利用这些资源。
175	T1528 - 窃取应用访问令牌	培训并鼓励用户报告来路不明的应用程序授权请求，从而可以检测到其他防御措施无法检测到的攻击。	DTE0035 - 用户培训	制定一项计划来培训用户如何识别和报告第三方应用程序的请求授权情况，从而可以创建“人体传感器”，有助于检测应用程序令牌被盗的情况。
176	T1529 - 系统关闭/重启	可以研究攻击者并收集有关攻击者及其工具的第一手资料。	DTE0017 - 系统诱饵	防守方可以部署系统诱饵，以查看攻击者是否试图关闭或重启设备。
177	T1530 - 来自云存储对象的数据	在对抗交战场景下，可以通过部署内容来影响攻击者的行为，测试他们对特定主题的兴趣或提高系统或环境的真实性。	DTE0030 - 文件诱饵	防守方可以在附加存储空间中部署各种文件诱饵。数据可能包括与特定人物角色相匹配的主题、攻击者感兴趣的主题等。
178	T1530 - 来自云存储对象的数据	在对抗交战场景下，可以提供有关各种主题的内容，查看哪些类型的信息会引起攻击者的兴趣。	DTE0030 - 文件诱饵	防守方可以部署各种文件诱饵，确定攻击者是否对特定文件类型、主题等感兴趣。
179	T1531 - 删除账户访问权限	可以进行成功概率适度偏高的检测。	DTE0034 - 系统活动监控	防守方可以进行监控，若用户帐户在正常工作时间之外发生更改或从远程位置等发生更改，则进行报警。

180	T1534 - 内部鱼叉式攻击	可以通过识别和警告异常行为，检测是否存在攻击者。	DTE0035 - 用户培训	制定一项计划，培训用户报告他们没有发送但出现在已发送文件夹中的电子邮件。
181	T1535 - 未使用/不支持的云区域	可以通过识别和警告异常行为，检测是否存在攻击者。	DTE0007 - 行为分析	防守方可以利用未使用的云区域来检测是否存在攻击者。通过对来自非正常区域、与网络进行交互的云主机进行行为分析，可以检测到潜在的恶意活动。
182	T1578 - 修改云计算基础架构	可以监控系统上的日志，了解攻击者的常见行为方式，并对攻击者的活动进行检测。	DTE0034 - 系统活动监控	防守方可以监控系统外的日志，即使在系统上删除日志后也可以检测到攻击者的活动。
183	T1537 - 将数据传输到云账户中	可以通过识别和警告异常行为，检测是否存在攻击者。	DTE0007 - 行为分析	防守方可以检测是否有攻击者企图渗入云帐户。这可以检测到，某个系统是不是在连接通常不会连接、没有使用通常会使用的账号、或在通常不常用的时间段内连接这些云服务供应商。
184	T1538 - 云服务仪表盘	为了延长对抗交战时间或启用检测，可以给攻击者带来一些您希望攻击者收集和使用的凭据。	DTE0012 - 凭据诱饵	防守方可以在多个位置部署凭据诱饵，增加攻击者发现和使用凭据诱饵的几率。
185	T1539 - 窃取网络会话Cookie	可以使用安全控制措施来阻止或允许攻击者的活动。	DTE0032 - 安全控制措施	防守方可以加固身份验证机制，以确保仅拥有会话cookie不足以与另一个系统进行身份验证。
186	T1539 - 窃取网络会话Cookie	可以在系统中布置诱饵cookie，以此来诱导攻击者锁定诱饵目标。	DTE0008 - 伪装真实业务环境	防守方可以（作为诱饵用户）向许多诱饵站点进行身份验证，从而为攻击者提供一系列的会话Cookie，供其在对抗交战过程中使用。
187	T1542 - 预启动操作系统	可以在系统上使用安全控制措施，以影响攻击者是否会取得成功。	DTE0032 - 安全控制措施	防守者可以使用可信平台模块技术和安全的启动进程来防止系统完整性受到损害。
188	T1543-创建或修改系统进程	可以使用安全控制措施来阻止或允许攻击者的活动。	DTE0032 - 安全控制措施	防守方可以选择加固或削弱系统的安全控制措施，以影响攻击者修改或创建系统进程的能力。
189	T1578 - 修改云计算基础架构	可以通过识别和警告异常行为，检测是否存在攻击者。	DTE0007 - 行为分析	防守方可以通过分析传入的网络连接来检测是否有攻击者在尝试打开某个端口。通过查找网络流量中的异常情况，识别潜在恶意流量。防守方还可以查看服务突然在以前未使用的端口上进行侦听的异常情况。
190	T1546 - 事件触发执行	可以使用工具和控件来阻止攻击者的活动。	DTE0006 - 基线	防守方可以频繁重复地将系统还原到经过验证的基线，消除攻击者的持久化机制。
191	T1546 - 事件触发执行	可以研究攻击者并收集有关攻击者及其工具的第一手资料。	DTE0001 - 管理员访问权限	防守方可以允许管理员访问系统诱饵或网络，从而让攻击者使用事件触发的执行。
192	T1547 - 启动或登录自动执行	可以使用工具和控件来阻止攻击者的活动。	DTE0006 - 基线	防守方可以存储注册表启动密钥的完好副本，并经常恢复还原，这可以防止攻击者在系统启动时使用注册表启动秘钥来启动恶意软件。
193	T1548 - 滥用提权控制机制	可以在系统上使用安全控制措施，以影响攻击者是否会取得成功。	DTE0032 - 安全控制措施	防守方可以使用基于主机的工具，以便对攻击者滥用提权控制机制是否成功产生影响。
194	T1550 - 使用备用身份验证材料	可以通过识别和警告异常行为，检测是否存在攻击者。	DTE0007 - 行为分析	防守方可以在帐户的身份验证入口处及身份验证内容中寻找异常情况，以检测潜在的恶意意图。
195	T1578 - 修改云计算基础架构	尽管攻击者可能会尝试删除或更改重要的工件，但在此之前可能会有一段时间可以检索到。	DTE0005 - 备份与恢复	防守方可以定期备份系统信息，并将其发送到备用位置进行存储。
196	T1552 - 不安全凭据	为了延长对抗交战时间或启用检测，可以给攻击者带来一些您希望攻击者收集和使用的凭据。	DTE0012 - 凭据诱饵	防守方可以在多个位置部署凭据诱饵，增加攻击者发现和使用凭据诱饵的几率。
197	T1553 - 破坏可信控件	可以通过控制交战环境的各个方面来确定攻击者的能力或偏好。	DTE0032 - 安全控制措施	在对抗交战的场景下，防守方可以实施薄弱的安全控制措施，让攻击者可以破坏这些安全控制措施，引诱攻击者进一步攻击。
198	T1553 - 破坏可信控件	防守方可以观察攻击者并控制他们可以看到哪些东西、可以产生什么影响和/或可以访问哪些数据。	DTE0003 - API 监控	防守方可以监控和分析操作系统的功能调用，以进行检测和报警。
199	T1554 - 攻击客户的软件二进制文件	可以通过识别和警告异常行为，检测是否存在攻击者。	DTE0007 - 行为分析	防守方可以监控客户端应用程序的异常行为，例如非典型模块负载、文件读/写或网络连接。
200	T1555 - 密钥库中的凭据	为了延长对抗交战时间或启用检测，可以给攻击者带来一些您希望攻击者收集和使用的凭据。	DTE0012 - 凭据诱饵	防守方可以在多个位置部署凭据诱饵，增加攻击者发现和使用凭据诱饵的几率。
201	T1556 - 修改身份验证流程	可以在系统上使用安全控制措施，以影响攻击者是否会取得成功。	DTE0032 - 安全控制措施	防守方可以实施安全控制措施，迫使攻击者修改身份验证流程，才能收集或利用系统上的凭据。
202	T1556 - 修改身份验证流程	可以监控系统上的日志，了解攻击者的常见行为方式，并对攻击者的活动进行检测。	DTE0034 - 系统活动监控	防守方可以监控系统外的日志，即使在系统上删除日志后也可以检测到攻击者的活动。
203	T1557 - 中间人	可以通过网络流量的监控，确定不同协议、异常流量模式、数据传输等，确定是否存在攻击者。	DTE0027 - 网络监控	防守方可以监控网络流量，以发现与已知MiTM行为相关的异常情况。
204	T1558 - 窃取或伪造Kerberos票据	可以通过控制交战环境的各个方面来确定攻击者的能力或偏好。	DTE0025 - 网络仿真	防守方可以设置使用Kerberos身份验证的网络以及使用Kerberos进行身份验证的系统。这样，防守方就可以查看攻击者是否有能力窃取或伪造Kerberos票据以进行横向移动。
205	T1558 - 窃取或伪造Kerberos票据	在对抗交战场景下，可以测试攻击者是否具有窃取或伪造Kerberos票证的能力。	DTE0032 - 安全控制措施	防守方可以保护Kerberos，防止攻击者利用票证进行身份验证或横向移动。 这可能导致攻击者暴露其他TTP。
206	T1559 - 跨进程通信	防守方可以观察攻击者并控制他们可以看到哪些东西、可以产生什么影响和/或可以访问哪些数据。	DTE0036 - 软件修改、监控	防守方可以修改系统调用，中断通信，然后将攻击路由到系统诱饵，阻止完全执行等。
207	T1560 - 存档已收集的数据	防守方可以观察攻击者并控制他们可以看到哪些东西、可以产生什么影响和/或可以访问哪些数据。	DTE0036 - 软件修改、监控	防守方可能会更改API，以公开正在存档、编码和/或加密的数据。这也可以用于破坏攻击者的操作，让数据不可用。
208	T1561 - 删除磁盘数据	防守方可以观察攻击者并控制他们可以看到哪些东西、可以产生什么影响和/或可以访问哪些数据。	DTE0036 - 软件修改、监控	防守方可以修改用于删除文件或格式化驱动器的命令功能，让这些命令功能在以特定方式使用时失效。
209	T1562 - 破坏防御	可以研究攻击者并收集有关攻击者及其工具的第一手资料。	DTE0004 - 应用仿真	防守方可以植入易于被攻击方删除的AV或监控工具。如果攻击者删除了这些内容，则他们可能会认为已经从系统中删除了监控，从而被诱使采取更公开的行动。

210	T1562 - 破坏防御	可以进行成功概率适度偏高的检测。	DTE0034 - 系统活动监控	防守方可以监控否有迹象表明攻击者在篡改安全工具和其他控件。
211	T1562 - 破坏防御	可以进行成功概率适度偏高的检测。	DTE0033 - SOP（标准操作流程）	防守方可以提供一套用于修改GPO的操作规程，并在不遵循该过程时发出警报以检测异常行为。
212	T1563 - 远程服务会话劫持	可以通过识别和警告异常行为，检测是否存在攻击者。	DTE0007 - 行为分析	防守方可以对在通常不活跃的时间段内在其他服务/系统中活跃的帐户查找异常情况，因为这可能表明存在恶意活动。
213	T1564 - 隐藏工件	可以阻止攻击者的计划行动，并迫使他们暴露其他TTP。	DTE0036 - 软件修改、监控	防守方可以修改、监控系统上的命令，因此，攻击者无法通过常规方式隐藏工件。
214	T1564 - 隐藏工件	可以部署绊索，当攻击者接触到网络资源或使用特定技术时就会触发警报。	DTE0034 - 系统活动监控	防守方可以监控用于隐藏系统中工件的已知命令以及与隐藏工件相关的活动。
215	T1565 - 数据修改、监控	在对抗交战场景下，可以观察攻击者如何修改、监控系统上的数据。	DTE0011 - 诱饵	防守方可以部署诱饵，以查看攻击者是否试图修改、监控系统或连网存储设备上的数据。
216	T1566 - 网络钓鱼	可以检测到网络钓鱼电子邮件，并阻止将邮件发送给目标收件人。	DTE0019 - 邮件管理	防守方可以拦截被电子邮件检测工具检测为可疑或恶意的电子邮件，并阻止将其发送给目标收件人。
217	T1566 - 网络钓鱼	可以检测到网络钓鱼电子邮件，并将其从目标收件人移至诱饵帐户进行数据读取和执行。	DTE0023 - 缓解攻击向量	防守方可以在打开和检查电子邮件之前将可疑电子邮件移至系统诱饵。
218	T1566 - 网络钓鱼	培训和鼓励用户报告网络钓鱼，从而检测到其他防御措施无法检测到的攻击。	DTE0035 - 用户培训	制定一项计划，培训并锻炼用户的反网络钓鱼技能，这可以创建“人体传感器”，有助于检测网络钓鱼攻击。
219	T1566 - 网络钓鱼	可以发现攻击者的攻击人物或对象。	DTE0015 - 角色诱饵	防守方可以将有关诱饵角色的个人帐户信息植入系统中，以查看攻击者是否在将来的活动中收集并使用该信息。
220	T1567 - 通过Web服务进行数据渗出	可以通过识别和警告异常行为，检测是否存在攻击者。	DTE0007 - 行为分析	防守方可以通过实施行为分析来检测是否有攻击者试图通过Web服务进行数据渗出。 这可以检测到通常无法连接到、或者在正常情况下不会连接这些Web服务的某个系统。
221	T1568 - 动态解决方案	如果您可以确定攻击者如何动态解析命令和控制（C2）地址，那么就可以使用该信息来识别攻击者的其他基础结构或工具。	DTE0021 - 狩猎	防守方可以使用有关已确定的动态解决方案运行方式的信息，以此来狩猎按同样方式行事但以前未检测到的对抗方案。
222	T1568 - 动态解决方案	攻击者可能试图动态确定要与之通信的C2地址。这样，防守方就有机会发现攻击者的其他基础结构。	DTE0026 - 网络变换	防守方可以拦截主要的C2域和IP，以确定恶意软件或攻击者是否有能力扩展到其他基础结构。
223	T1569 - 系统服务	防守方可以观察攻击者并控制他们可以看到哪些东西、可以产生什么影响和/或可以访问哪些数据。	DTE0003 - API 监控	防守方可以监控和分析操作系统的功能调用，以进行检测和报警。
224	T1569 - 系统服务	可以进行成功概率适度偏高的检测。	DTE0033 - SOP（标准操作流程）	防守方可以定义用于添加服务的操作过程，并在不按照该操作过程添加服务时（例如，攻击者添加服务时）发出警报，以检测异常行为。
225	T1570 - 工具横向转移	可以通过网络流量的监控，确定不同协议、异常流量模式、数据传输等，确定是否存在攻击者。	DTE0027 - 网络监控	防守方可以对异常的流量模式、大量或意外的数据传输以及可能显示存在攻击者的其他活动进行网络监控并发出报警。
226	T1570 - 工具横向转移	可以修改网络，允许/拒绝某些类型的流量，对网络流量进行降级或以其他方式影响攻击者的活动。	DTE0026 - 网络变换	防守方可以拦截攻击者在不同系统之间使用的特定协议，防止工具横向转移。
227	T1571 - 非标准端口	可以通过网络流量的监控，确定不同协议、异常流量模式、数据传输等，确定是否存在攻击者。	DTE0027 - 网络监控	防守方可以对异常的流量模式、大量或意外的数据传输以及可能显示存在攻击者的其他活动进行网络监控并发出报警。
228	T1572 - 隧道协议	可以通过网络流量的监控，确定不同协议、异常流量模式、数据传输等，确定是否存在攻击者。	DTE0027 - 网络监控	防守方可以监控哪些系统使用不常用的封装协议（例如通过TCP隧道传输的RDP）建立了连接。
229	T1573 - 加密信道	可以发现攻击者试图隐藏数据，避免让防守方发现。	DTE0031 - 协议解码器	防守方可以对恶意软件进行逆向工程，并开发可以解密和公开攻击者通信的协议解码器。
230	T1574 - 劫持执行流量	可以使用安全控制措施来阻止或允许攻击者的活动。	DTE0032 - 安全控制措施	防守方可以阻止执行不受信的软件。