

Atomic Red Team可用于测试个别技术和程序，以验证行为分析和监视功能是否按预期工作。Atomic Red Team存储库有许多原子测试，每个原子测试都有一个专用于已测试的ATT & CK技术的目录。您可以在 [ATT & CK矩阵格式](#)。

要开始测试，请选择 [T1135](#) 页以查看详细信息和记录的不同类型的原子测试。这些测试中的每一个都包含有关该技术是什么，所支持的平台以及如何执行该测试的信息。

## 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` !

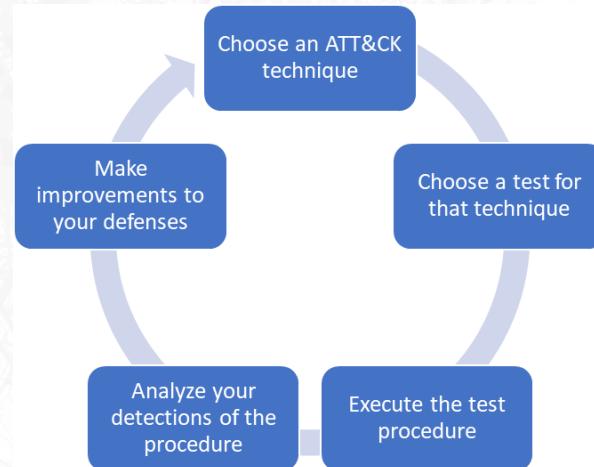
```
net view \\#{computer_name}
```

T1135原子测试详细信息

我们看到有三个测试选项，并决定选择 #2 来通过命令提示符进行测试。因此，我们打开命令提示符，复制并粘贴命令，添加计算机名称，然后执行命令。

我们刚刚执行了第一个原子测试！完成此操作后，我们可以看一看我们是否希望检测到的是我们实际检测到的。例如，也许我们在SIEM工具中进行了行为分析，当执行“网络视图”时应该发出警报，但是我们发现它没有触发，因此我们发现没有从主机正确导出日志。您可以对问题进行故障排除和解决，现在，您已经进行了可衡量的改进，以帮助您将来有更多机会使用此过程来吸引对手。

这些奇异的测试使您可以将激光重点放在单个ATT & CK技术上，这使得构建基于ATT & CK的防御性覆盖面更加容易，因为您可以从针对单个技术的单个测试开始，然后从那里扩展。



带有ATT & CK的原子测试循环

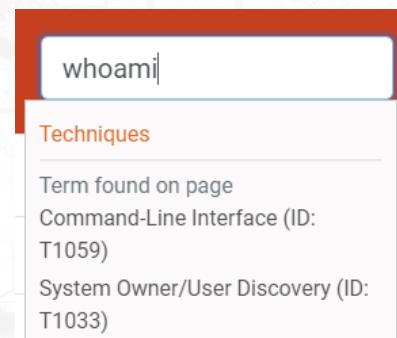
奖励级别1.5内容：是否有使用Atomic Red Team进行对手仿真测试的流程，并准备好进行一些有助于将行为序列链接在一起的工作？查看 [卡尔德拉](#) 下一个！CALDERA是由MITER创建的自动敌对仿真系统，它具有映射到ATT & CK技术的许多内置行为。它允许操作员在构建测试时选择一种技术或将多种技术链接在一起，这使您可以开始自动执行测试行为序列，而不必手动执行单个原子测试。您可以使用预构建的场景之一，也可以通过选择映射到您要测试的某些ATT & CK技术的过程（在CALDERA中称为“能力”）来定义更特定的场景。

## 2级

对于那些已经具备红队能力的人来说，您可以从ATT & CK与现有业务的整合中受益匪浅。在撰写报告和讨论缓解措施时，将红队参与中使用的技术映射到ATT & CK提供了一个通用框架。

首先，您可以采用现有的计划中的操作或工具，并将其映射到ATT & CK。将红队程序映射到ATT & CK类似于将威胁情报映射到ATT & CK，因此您可能需要查看Katie关于第1章中概述的六步过程的建议。

幸运的是，有时映射技术可以像搜索ATT & CK网站上使用的命令一样简单。例如，如果我们在红队操作中使用了“whoami”命令，则可以在ATT & CK网站上进行搜索，然后发现可能适用两种技术：[系统所有者/用户发现 \( T1033 \)](#) 和 [命令行界面 \( T1059 \)](#)。



搜索功能开启 [HTTPS://ATTACK.MITRE.ORG](https://attack.mitre.org)

让您开始将红队程序映射到ATT & CK的另一个有用资源是 [APT3对手仿真领域手册](#)，它细分了APT3所使用的逐个命令动作，所有动作均映射到ATT & CK。

Category	Built-in Windows Command	Cobalt Strike	Metasploit
<b>Discovery</b>			
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	shell net config workstation	
	net config server	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

摘录自我们的“APT3模拟仿真领域手册”

**如果您的红色团队正在使用类似 钻击 要么 帝国，好消息-这些已经映射到ATT & CK。有了映射到ATT & CK的各个命令，脚本和工具，您现在就可以计划您的参与。**

一些红色团队拥有经过实践检验的真实工具包和操作方法。他们知道什么有效，因为它一直有效。但是，他们并不总是知道，他们经过尝试的真实TTP中有多少与可能针对组织的已知威胁重叠（或不重叠！）。这导致在理解防御措施与您实际要防御的防御措施的堆叠程度方面存在一些差距，这些攻击者针对的是您的环境，而不一定是红色团队本身。

我们希望确保我们不仅在使用这些技术，因为我们的工具可以执行这些技术-我们想模仿一个我们真正希望提供更多价值的对手。例如，我们可以与我们的CTI团队交谈，他们告诉我们他们担心伊朗组织（OilRig）的目标定位。

由于所有内容都由ATT & CK构成，因此我们可以使用 [ATT & CK导航器](#) 将我们可以使用现有工具（例如Cobalt Strike）进行的技术与我们知道OilRig基于开源报告完成的技术进行比较。（您可以查看 [演示](#) 在下一个图形中，钻击技术为红色，OilRig技术为蓝色，Cobalt Strike可以执行且OilRig使用的技术为紫色。）

这些紫色的技术为我们提供了一个开始使用我们已经拥有的工具并执行对我们组织来说是优先事项的技术的地方。

Trusted Relationship	Critical User Interface	Browser Extensions	EVN Windows Permissions	Compressed Firmware	Conditional Device	Remote Services	Imp. Capture	Fallout Chapters	Resource Hijacking
Valid Accounts	Installable	Change Default File	EVN System Permissions	Compressed Object Model	Host Prism	FileServer	Man in the Browser	Multi-thread Communication	Runtime Data Manipulation
Lucknow	Component Framework	Hooking		Control Panel Themes	Kerberoasting	HTTPD/SSH/High Port	Man in the Browser	Multi-hop Persistence	Service Bus
Local Job Scheduling	Cloud Native Object Model	Cloud Migration	EVN System Permissions	OSCheckin	Keychain	Cloud Replication	Session Capture	Multi-hop Persistence	Staged Data Manipulation
LSA API Driver	Cloud Native Object Model	Cloud Migration	EVN System Permissions	PowerShell	Logon Scripts	Cloud Replication	Session Capture	Multi-hop Persistence	Staged Data Manipulation
Malina	LLT Search Order	New Service		Disallowing Resource Tools	Ntldr Booting	Cloud Replication	Session Capture	Multi-hop Persistence	System Configuration
Phantom	Cloud Hooking	Path Interception		DLL Search Order	Password Filter DLL	Cloud Replication	Session Capture	Multi-hop Persistence	Port Knocking
Rage/ragam	External Remote Services	Port Monitor		DLL Side-Loading	Private Keys	Cloud Replication	Session Capture	Multi-hop Persistence	Remote Access Tools
Ragev2	Fileless	Port Monitor		EVN System Permissions	Recovery Policy	Cloud Replication	Session Capture	Multi-hop Persistence	Remote File Copy
Reaver	Fileless	Port Monitor		EVN System Permissions	Recovery Policy	Cloud Replication	Session Capture	Multi-hop Persistence	Remote File Copy
Redacted Tech	Hooking	Redacted Task		EVN Windows Memory	Recovery Policy	Cloud Replication	Session Capture	Multi-hop Persistence	Remote File Copy
RingZero	Hypercar	Hypercar Report		File Deletion		Cloud Replication	Session Capture	Multi-hop Persistence	Remote File Copy
Saving The Execution	Image File Execution	Image File Execution		File Deletion	EVN System Permissions	Cloud Replication	Session Capture	Multi-hop Persistence	Remote File Copy
Scorpion	Image File Execution	Image File Execution		File Deletion	EVN System Permissions	Cloud Replication	Session Capture	Multi-hop Persistence	Remote File Copy
Scorpion/Scorpion	Image File Execution	Image File Execution		File Deletion	EVN System Permissions	Cloud Replication	Session Capture	Multi-hop Persistence	Remote File Copy
Source	Launch Daemon	Buds		Group Policy Modification		Cloud Replication	Session Capture	Multi-hop Persistence	Remote File Copy
Spikes after Phoenix	Launched	Buds Caching		Group Policy Modification		Cloud Replication	Session Capture	Multi-hop Persistence	Remote File Copy
Third-party Software	LC_LOAD_ZLIB Addict	Valid Accounts		Hidden Icons		Cloud Replication	Session Capture	Multi-hop Persistence	Remote File Copy
Time	Logon Script Processing	New Shell		Hidden Icons		Cloud Replication	Session Capture	Multi-hop Persistence	Remote File Copy
Trusted Developer Utility	Logon Script			HISTCONTROL		Cloud Replication	Session Capture	Multi-hop Persistence	Remote File Copy
User Execution	Logon Scripts			Image File Execution		Cloud Replication	Session Capture	Multi-hop Persistence	Remote File Copy
Windows Management	LMDBS Driver			Indicator Blocking		Cloud Replication	Session Capture	Multi-hop Persistence	Remote File Copy
XLS Script Processing	New Service			Indicator Blocking		Cloud Replication	Session Capture	Multi-hop Persistence	Remote File Copy
	Office Applications Startup			Indicator Removal on Host		Cloud Replication	Session Capture	Multi-hop Persistence	Remote File Copy
	Path Interception			Job[get] Command		Cloud Replication	Session Capture	Multi-hop Persistence	Remote File Copy
	Port Knocking			Install Root Certificate		Cloud Replication	Session Capture	Multi-hop Persistence	Remote File Copy
	Port Monitor			Install[tl]		Cloud Replication	Session Capture	Multi-hop Persistence	Remote File Copy
	Recomm			LC_MN_Hijacking		Cloud Replication	Session Capture	Multi-hop Persistence	Remote File Copy
	Signature [File Keys]			Masquerading		Cloud Replication	Session Capture	Multi-hop Persistence	Remote File Copy
	Re-opened Applications			Modify Registry		Cloud Replication	Session Capture	Multi-hop Persistence	Remote File Copy
	Scheduled Task			Mount		Cloud Replication	Session Capture	Multi-hop Persistence	Remote File Copy
	Screen-reader			Network Share Connection		Cloud Replication	Session Capture	Multi-hop Persistence	Remote File Copy
	Session Token Provider			NTFS File Attributes		Cloud Replication	Session Capture	Multi-hop Persistence	Remote File Copy
	Service Registration			Object Protection		Cloud Replication	Session Capture	Multi-hop Persistence	Remote File Copy
	Service Start/Stop			Print Modification		Cloud Replication	Session Capture	Multi-hop Persistence	Remote File Copy
	Service Start/Stop			Process Creation		Cloud Replication	Session Capture	Multi-hop Persistence	Remote File Copy
	Service Modifications			Process Decoupling		Cloud Replication	Session Capture	Multi-hop Persistence	Remote File Copy
	Service Modifications			Process Hollowing		Cloud Replication	Session Capture	Multi-hop Persistence	Remote File Copy
	Shared Memory			Process Injection		Cloud Replication	Session Capture	Multi-hop Persistence	Remote File Copy
	Shared Memory			Process Reinject		Cloud Replication	Session Capture	Multi-hop Persistence	Remote File Copy
	System Primes			Reprocess Request		Cloud Replication	Session Capture	Multi-hop Persistence	Remote File Copy
	SystemService			Reprocess[0]		Cloud Replication	Session Capture	Multi-hop Persistence	Remote File Copy
	Time Providers			Rootkit		Cloud Replication	Session Capture	Multi-hop Persistence	Remote File Copy
	Time			Run[12]		Cloud Replication	Session Capture	Multi-hop Persistence	Remote File Copy
	Valid Accounts			Run[13]		Cloud Replication	Session Capture	Multi-hop Persistence	Remote File Copy
	Web Shell			Setuid Policy		Cloud Replication	Session Capture	Multi-hop Persistence	Remote File Copy
	Windows Driver API			Setgid Policy		Cloud Replication	Session Capture	Multi-hop Persistence	Remote File Copy
	Windows Helper DLL			Setuid Root Policy		Cloud Replication	Session Capture	Multi-hop Persistence	Remote File Copy
				Software Patching		Cloud Replication	Session Capture	Multi-hop Persistence	Remote File Copy
				Software Patching		Cloud Replication	Session Capture	Multi-hop Persistence	Remote File Copy
				Template Injection		Cloud Replication	Session Capture	Multi-hop Persistence	Remote File Copy
				Timestamping		Cloud Replication	Session Capture	Multi-hop Persistence	Remote File Copy
				Trusted Developer Utility		Cloud Replication	Session Capture	Multi-hop Persistence	Remote File Copy
				Windows Application Sandbox		Cloud Replication	Session Capture	Multi-hop Persistence	Remote File Copy
				Web Service		Cloud Replication	Session Capture	Multi-hop Persistence	Remote File Copy
				XSL Script Processing		Cloud Replication	Session Capture	Multi-hop Persistence	Remote File Copy

ATT & CK矩阵显示钻打击和石油钻井技术重叠

除了识别出Cobalt Strike和OilRig之间的重叠之外，分析还可以显示在哪里有机会改变红队的行为，超出他们通常采用的程序级别。

在某些情况下，可能会在红队使用的工具中以特定方式实施一项技术，但是未知对手会以这种方式执行该技术。掌握这些知识有助于红色团队使用不同测试之间的行为，以更好地涵盖在对手仿真过程中已知的威胁。在这一点上，我们还可以添加我们想使用命令或脚本手动执行的技术。然后，我们可以在导航器中添加有关执行技术的顺序以及执行方式的注释。

虽然在计划红队行动时映射到ATT & CK有很多好处，但在与蓝队进行沟通时，一旦执行了行动，我们也将获得丰厚的回报。如果他们将分析，检测和控制映射回ATT & CK，则您可以轻松地以通用语言与他们进行交流，以了解您的所作所为和成功之处。在报告中包含ATT & CK Navigator图像（甚至保存的Navigator图层）可以帮助此过程，并为他们提供模板进行改进。

**2.5级奖励内容：**使用ATT & CK计划参与度并报告结果后，请尝试使用 [APT3仿真计划](#) 或者 [ATT & CK评估第一轮方案](#) 根据该计划进行模拟APT3的参与度，以显示针对特定对手群体的基准测试。

### 3级

至此，您的红色团队正在将ATT & CK整合到运营中，并在与蓝色团队进行沟通中找到价值。为了提高您的团队及其所具有的影响力，您可以与组织的CTI团队合作，使用他们通过创建自己的对手模拟计划收集的数据，针对特定的对手量身定制针对性。

创建自己的对手模拟计划将最大程度地利用红色团队与您自己的威胁情报相结合的优势：这些行为是从针对您的现实对手中看到的！红色团队可以将该intel转换为有效的测试，以显示哪些防御措施运作良好以及需要改进哪些资源。当安全性测试暴露可见性和控制差距时，如果您很有可能显示已知对手已利用了可见性和控制差距，那么影响会更高。将您自己的CTI与对手的仿真工作联系起来，既可以提高测试的有效性，又可以提高高层领导制定变更的输出。我们建议如下图所示的五步过程，以创建对手仿真计划，执行操作并推动防御性改进。（有关该过程的更详细的概述，请参见Katie Nickels和Cody Thomas在 [使用ATT & CK的基于威胁的对手仿真](#)。）

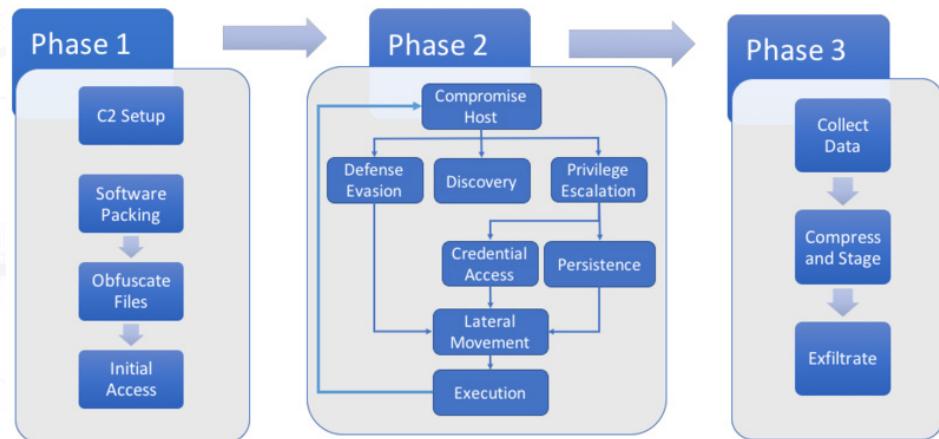


制定不利的模拟计划的过程

1。 收集威胁情报 —根据对组织的威胁来选择对手，并与CTI团队一起分析有关对手所做工作的情报。除了可以公开获取的信息外，还可以根据组织的知识来结合起来，以记录对手的行为，他们所采取的行动，无论是粉碎还是抢劫还是缓慢而缓慢。

2。 提取技术 -以与将红队操作映射到ATT & CK技术相同的方式，将需要的intel映射到与intel团队一起使用的特定技术。您可以将您的CTI团队指向第1章，以帮助他们学习如何执行此操作。

3。 分析和组织 -现在您掌握了有关敌人及其运作方式的大量信息，可以轻松地从中创建特定计划的方式将该信息绘到其行动流程中。例如，下面是MITER团队为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，您知道红队希望做什么，请找出如何实施该行为。考虑：

- ?? 威胁组如何使用这种技术？
- ?? 小组是否根据环境情况改变了使用哪种技术？
- ?? 我们可以使用哪些工具来复制这些TTP？

5， 模拟对手 —通过制定计划，红色团队现在可以执行和执行仿真任务。正如我们建议所有使用ATT & CK的红队参与活动一样，红队应与蓝队紧密合作，以深入了解蓝队可见性中的差距及其存在的原因。

一旦完成整个过程，红色和蓝色团队便可以与CTI团队一起确定重复执行该过程的下一个威胁，从而创建一个连续的活动来测试针对现实行为的防御措施。

## 摘要

本章向您展示了如何使用ATT & CK进行红队和对手仿真，无论您拥有什么资源（包括如果您还没有红队）。我们希望您在本书中一直观察到，这些主题中的每个主题都是相互依存的，而威胁情报则可以帮助您创建可以通过对手仿真进行验证和改进的分析，而所有这些都使用ATT & CK的通用语言。下一章（也是最后一章）将讨论如何使用ATT & CK进行评估和工程设计，从而完善我们的《ATT & CK入门》系列。

# 评估与工程

安迪·阿普鲍姆 ( Andy Applebaum )

在前面的章节中，我们介绍了如何使用ATT & CK入门。用于威胁情报，用于检测和分析和进行对手模拟。在第四部分中，我们将讨论评估和工程设计，向您展示如何使用ATT & CK来衡量防御能力并进行改进。本章在许多方面都以先前的内容为基础，因此，如果您还没有阅读过的话，建议您先阅读它们。

为了使此过程更易于访问（并与其它各章一起进行），我们根据复杂性和资源可用性将本节分为三个级别：

?? 1级 对于那些刚开始可能没有很多资源的人

?? 2级 对于那些中级团队开始成熟的人

?? 3级 对于拥有更高级网络安全团队和资源的人员而言，“评估”入门一开始听起来可能令人恐惧-谁喜欢被评估？-但是ATT & CK评估是更大的过程的一部分，该过程为安全工程师和架构师提供有用的数据以证明基于威胁安全性改进：

- 1.评估当前的防御方式如何与ATT & CK中的技术和对手相提并论
- 2.确定当前覆盖范围内优先级最高的差距
- 3.修改防御措施（或获取新的防御措施）以弥补这些差距



评估与工程过程

评估和工程级别为 累积的 并彼此建立。即使您认为自己是一支高级网络安全团队，我们仍然鼓励您从1级开始，逐步完成此过程，以进行更大规模的评估。

## 1级

如果您与无法访问大量资源的小型团队合作，并且正在考虑进行全面评估，请不要这样做。立即创建ATT & CK矩阵的彩色编码热图以可视化覆盖范围的想法很吸引人，但更可能使您对ATT & CK筋疲力尽，而不是兴奋地使用它。相反，从小处着手：选择一种技术来关注，确定该技术的覆盖范围，然后进行适当的工程改进以开始检测它。通过这种方式开始，您可以练习如何进行更大的评估。

**提示：**不确定从哪种技术开始？查阅第1章，了解如何使用ATT & CK和威胁情报选择起点。

选择了一种技术后，您将需要弄清楚该技术的覆盖范围。虽然您可以使用自己的标题，但我们建议从以下几种险种入手：

- ?? 您现有的分析可能会检测到该技术；
- ?? 您的分析将无法检测到该技术，但是您需要引入正确的数据源来检测它。要么
- ?? 您当前未使用正确的数据源来检测该技术。

**提示：**刚开始时，将评分类别保持简单：是否可以检测到它？

衡量覆盖率的一个好方法是查看您的分析，看看它们可能已经涵盖了哪些技术。这可能很耗时，但值得付出努力：许多SOC已经具有可以映射回ATT & CK的规则和分析，即使它们最初并不是设计成这样做的。通常，您需要引入有关该技术的其他信息，这些信息可以从该技术的ATT & CK页面或外部来源获得。

例如，假设我们正在研究[远程桌面协议 \( T1076 \)](#) 并且我们有以下警报：

1. 通过端口22的所有网络流量
2. AcroRd32.exe产生的所有进程
3. 任何名为tscon.exe的进程
4. 通过端口3389的所有内部网络流量

查看“远程桌面协议”的ATT & CK技术页面，我们可以快速看到规则3与“检测”标题下指定的规则匹配。快速的网络搜索显示，由规则4指定的端口3389也与该技术相对应。

## 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.

远程桌面协议的检测文本

如果您的分析已经掌握了这项技术，那就太好了！记录您对该技术的报道，然后选择一种新的方法来再次开始该过程。如果您不了解它，请查看该技术的“ATT&CK”页面上列出的数据源，并确定您是否可能已经提取了正确的数据来构建新的分析。如果是的话，那只是建立一个整体的问题。

但是，如果您没有获取正确的数据源，应该怎么做？这就是工程学发挥作用的地方。请看一下该技术的“ATT&CK”页面上列出的数据源，作为可能的起点，并尝试评估您开始收集每个数据源的难度以及如何使用它们的有效性。

提示：Windows事件日志是经常引用的数据源，它提供了许多ATT&CK技术的可见性。Malware Archaeology的Windows是开始使用事件日志的好资源 [ATT&CK测井备忘单](#)，它将Windows事件映射到您可以使用它们检测到的技术。

可以使用过程命令线参数检测到的244种ATT & CK技术中的97种，可以通过Windows事件4688加以研究

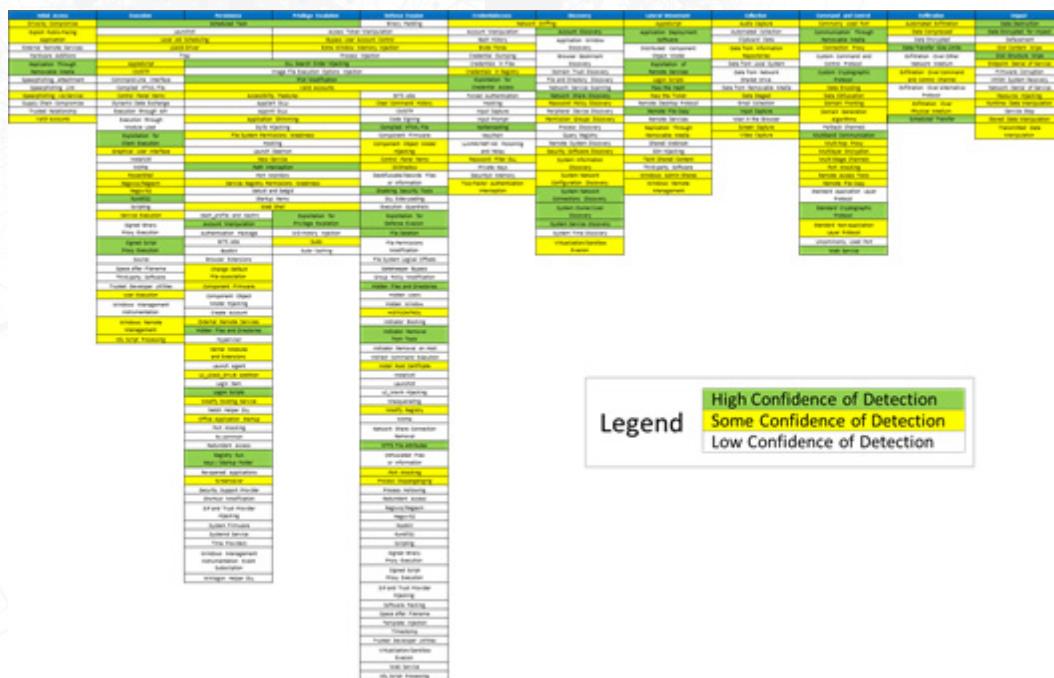
升至下一个级别：不要止步于一项技术，而是要多次运行此过程，并在每次运行的每种策略中选择一项（或两项）新技术。使用 [ATT & CK导航器](#)，这非常适合 [生成热图](#)

ATT & CK 覆盖范围。

一旦您对流程感到满意，就可以进行数据源分析，并给出一个热图，以了解在引入数据源时可以检测到哪些技术。一些可以帮助您入门的资源包括 Olaf Hartong 的 [ATT & CK Datamap 项目](#)、[德勤](#) 和 MITRE 自己的 [ATT & CK 脚本](#)

2级

一旦您熟悉了此过程并可以使用更多资源，您将理想地扩展您的分析以涵盖ATT & CK矩阵的相当大的子集。此外，您可能想使用更高级的覆盖方案来说明保真度以及检测。在这里，我们建议将桶装覆盖范围推荐到低一些要么高。我们有信心在我们的SOC中使用工具或分析工具来提醒该技术。



最终评估可能会像什么的示例

**提示：**尝试评估覆盖范围时，不必担心精确度高-您评估的目的是了解您是否具有一般检测技术的工程能力。为了获得更高的准确性，我们建议您运行[对手模拟练习](#)，如第3章所述。

扩展后的范围使分析分析变得稍微复杂一些：每个分析现在都可以映射到许多不同的技术，而不是以前的一种技术。此外，如果您发现一个涵盖特定技术的分析方法，而不仅仅是标记该技术已被涵盖，您还需要弄清楚该分析方法的覆盖范围保真度。

提示：对于每个分析，我们建议找到其输入的内容，并查看其如何映射回ATT&CK。例如，您可能有一个分析来查看特定的Windows事件。要确定此分析的范围，您可以在 [Windows ATT&CK记录备忘单](#) 或类似的存储库。您还可以使用ATT&CK网站分析您的分析。下图显示了搜索端口22的检测示例，该示例显示在 [常用端口](#) ATT&CK技术。

The screenshot shows the MITRE ATT&CK homepage. At the top, there is a navigation bar with links to Matrices, Tactics, Techniques, Groups, Software, Resources, and Blog. A search bar is located at the top right, with the number '22' entered. Below the search bar, a red box highlights the term 'Techniques'. To the right of the search bar, a tooltip displays the message 'Term found on page'. The main content area features a section titled 'Tweets by @MITREattack' with a tweet from Johnny Curran (@SW\_Johnny5) about a security update. On the right side, a sidebar displays a list of techniques related to port 22, including 'Commonly Used Port (ID: T1043)', 'DLL Side-Loading (ID: T1073)', 'Modify Existing Service (ID: T1031)', 'Modify Registry (ID: T1112)', 'System Information Discovery (ID: T1082)', 'System Network Configuration Discovery (ID: T1016)', and 'System Owner/User Discovery (ID: T1033)'.

22端口的ATT & CK站点搜索

要考虑的另一个重要方面是与技术一起列出的组和软件示例。这些描述了对手使用某种技术的程序或特定方式。通常，它们代表现有分析可能涵盖或未涵盖的技术变体，并且在评估您对技术的涵盖程度时应考虑入置信度评估中。

## Examples

Name	Description
APT3	APT3 will copy files over to Windows Admin Shares (like ADMIN\$) as part of lateral movement. <sup>[5]</sup>
APT32	APT32 used Net to use Windows' hidden network shares to copy their tools to remote machines for execution. <sup>[6]</sup>
BlackEnergy	BlackEnergy has run a plug-in on a victim to spread through the local network by using PsExec and accessing admin shares. <sup>[7]</sup>
Cobalt Strike	Cobalt Strike can use Window admin shares (C\$ and ADMIN\$) for lateral movement. <sup>[8]</sup>
Deep Panda	Deep Panda uses net.exe to connect to network shares using net use commands with compromised credentials. <sup>[9]</sup>
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. <sup>[10]</sup>

WINDOWS ADMIN股份示例

除了查看分析之外，您还需要开始分析工具。为此，我们建议遍历每个工具（为每个工具创建一个单独的热图）并提出以下问题：

?? 该工具在哪里运行？根据工具在何处运行（例如在外围或在每个端点上），使用特定策略可能会更好或更坏。

?? 该工具如何检测？是否使用一组静态的“已知不良”指标？还是在做某些行为？

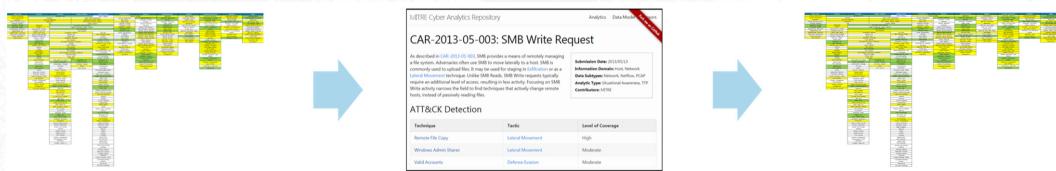
?? 该工具监视哪些数据源？知道了工具监视的数据源后，您就可以推断出它可以检测到哪些技术。

回答这些问题可能很困难。并非所有供应商都发布此类信息，并且经常在您搜寻此类信息时，最终会找到营销材料。尽量不要花太多时间陷入细节问题，而是选择画一些关于一般覆盖范围的笔触。

要创建覆盖的最终热图，请汇总工具和分析的所有热图，并记录下 **最高** 覆盖每种技术。

作为提高覆盖率的第一步，我们建议您使用我们之前提到的分析开发流程的更高级版本：

1. 创建您想在短期内重点关注的高优先级技术的列表。
2. 确保您获取正确的数据，以开始针对您所关注的技术编写分析。
3. 开始构建分析并更新覆盖率图表。



从您当前的覆盖范围开始，添加分析并相应地更新您的覆盖范围

您可能还想开始升级您的工具。在分析文档时，请跟踪可能用于增加覆盖范围的任何可选模块。如果您遇到任何问题，请研究在网络上启用它所需的资源，并将其与它提供的覆盖范围进行平衡。

如果找不到工具的任何其他模块，也可以尝试将它们用作备用数据源。例如，您可能无法安装 [西蒙](#) 在每个端点上，但是您现有的软件可能能够转发您可能无法访问的相关日志。

**升至下一个级别：**一旦开始实施其中的一些更改并提高了覆盖范围，下一步就是介绍 [对手模拟](#)，尤其是原子测试。每次您制作新的分析原型时，都要运行一个匹配的原子测试，看是否被抓住了。[如果您做到了，那就太好了！](#)如果没有，请查看遗漏的内容，并相应地完善分析。您也可以在 [使用基于ATT&CK的分析发现网络威胁](#) 有关此过程的更多指导。

### 3级

对于拥有更高级团队的人来说，增强评估的一种好方法是包括缓解措施。这有助于将评估从查看工具和分析及其检测到的内容转移到查看整个SOC。识别技术缓解方法的一个好方法是遍历SOC的每个策略，预防工具和安全控制，然后将它们映射到可能会影响的ATT & CK技术，然后将这些技术添加到您的热图中覆盖范围。我们最近 [缓解措施的重组](#) 使您可以查看每种缓解措施，并查看其所映射的技术。缓解技术的一些示例包括：

?? 蛮力 可以通过帐户锁定策略来缓解。

?? 部署中 [凭证守卫](#) 在Windows 10系统上可以 [凭证转储](#) 更加困难。

?? 强化的本地管理员帐户可以防止 [Windows管理员共享](#)。

?? 借力 [Microsoft EMET的攻击面减少](#) 规则可能会更难使用 [运行DLL32](#)。

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-useable, 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. <sup>[26]</sup>

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.

蛮力（左）和WINDOWS ADMIN股份的缓解（右）

扩展评估的另一种方法是与在您的SOC中工作的其他人进行面谈或非正式地聊天。这可以帮助您更好地了解您的工具的使用方式，并突出您可能不会考虑的差距和优势。您可能要问的一些示例问题包括：

?? 您最常使用哪些工具？他们的优缺点是什么？

?? 您看不到希望看到的哪些数据源？

?? 从检测角度来看，您最大的优点和缺点在哪里？

这些问题的答案可以帮助您扩大之前制作的热图。

**示例：**如果您以前发现了一个具有许多与ATT & CK相关的功能的工具，但人员仅使用它来监视Windows注册表，则应修改该工具的热图以更好地反映其使用方式。

与同事交谈时，请查看您先前创建的工具热图。如果您仍然对工具所提供的覆盖范围不满意，则可能需要评估新工具。给出每种潜在新工具的覆盖范围的热点图，并查看添加它如何帮助您扩大覆盖范围。

**提示：**如果您资源特别丰富，则可以站起来一个有代表性的测试环境来实时测试该工具，记录该工具在什么地方做得好和在哪里做得不好，以及添加它会如何影响您现有的覆盖范围。

最后，您可以通过实施更多的缓解措施来减少对工具和分析的依赖。查看ATT & CK中的缓解措施，以评估您是否可以实际实施这些缓解措施。在此过程中，请查阅您的检测热图；如果有一个高成本的缓解措施可以阻止您在检测方面做得很好的技术，那可能不是一个很好的权衡。

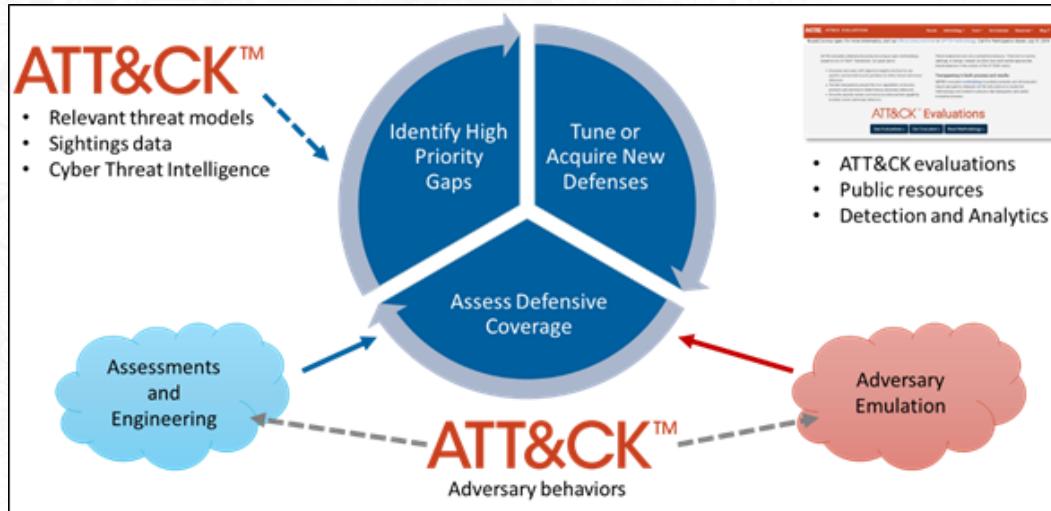
另一方面，如果存在低成本的缓解措施，则可以针对正在努力为其编写分析方法的技术来实施，那么实施这些措施可能是对资源的良好利用。

**提示：**在调查有利于缓解措施的删除检测时，请始终权衡潜在的可见性损失。确保在某些缓解措施或控制措施可能被绕过的情况下，您具有一定的可见性，以免错过这些事件。检测和缓解都应同时用作有效覆盖的工具。

## 摘要

评估防御并指导您的工程设计可能是ATT & CK入门的好方法。通过运行评估，您可以了解当前的覆盖范围，可以利用威胁情报来扩大这些覆盖范围，从而优先划分漏洞，然后通过编写分析来调整现有防御措施。

从长远来看，您不应该将自己想象成每周或什至每月进行评估。取而代之的是，您应该保持最近一次评估的运行状态标签，每次获取新信息时都对其进行更新，并定期运行对手模拟练习以抽查您的结果。随着时间的推移，网络中的变化以及所收集的内容可能会产生意想不到的后果，从而降低先前测试的防御措施的有效性。通过利用ATT & CK来显示防御如何叠加到实际威胁上，您将能够更好地了解自己的防御态势并确定改进的优先级。



可视化的攻击和使用情况

## 关于作者



安迪·阿普鲍姆（Andy Applebaum）是MITRE的首席网络安全工程师，他致力于应用和理论上的安全研究问题，主要涉及网络防御，安全自动化和自动化对手仿真领域。在MITRE工作之前，Andy在加州大学戴维斯分校获得了计算机科学博士学位。安迪是一个成熟的人

研究员，发表了许多论文，并在多个学术和行业会议上演讲，包括Black Hat Europe，SANS安全运营峰会，B Sides NOVA和FIRST会议。



凯蒂·尼克尔斯（Katie Nickels）是MITRE的ATT & CK威胁情报负责人，她专注于分享ATT & CK如何有助于迈向基于威胁的信息防御。她还是FOR578：网络威胁情报的SANS讲师。凯蒂（Katie）在网络防御，事件响应和网络威胁情报领域工作了近十年。她来自文科

具有史密斯学院和乔治敦大学学位的背景，拥护将文科能力应用于网络安全的力量。凯蒂（Katie）在她的名字中发表了十几本出版物，并在Black Hat，FIRST CTI研讨会，多次SANS峰会，Sp4rkcon和许多其他活动中的演讲中分享了她的专业知识。



亚当·彭宁顿是ATT & CK核心团队的成员，并且是ATT & CK博客的总编辑。在MITER的11年中，他大部分时间都在研究和宣扬使用欺骗手段进行情报收集。在加入MITRE之前，Adam是卡内基梅隆大学并行数据实验室的研究员，并获得了计算机科学和电气学士学位和硕士学位。

和计算机工程以及卡耐基梅隆大学2017年校友服务奖。亚当在许多场所发表和发表文章，包括FIRST CTI，USENIX Security和ACM Transactions on Information and System Security。



蒂姆·舒尔茨是MITRE的高级网络对抗工程师。他大部分时间都在促进红色和蓝色团队之间的协作，以帮助赞助商提高安全性。蒂姆（Tim）为MITRE的CALDERA项目做出了贡献，参加了ATT & CK评估，并促进了红色团队的参与。在从事MITER工作之前，Tim在Sandia担任网络安全研究员

国家实验室和数字取证实验室为执法人员创建培训内容。



布莱克·斯特罗姆 是MITER进行对手仿真的能力领域负责人，曾在网络防御，网络威胁情报，安全研究和对手仿真领域工作。自项目创立以来，ATT & CK的共同创始人布雷克（Blake）一直领导该项目。他还领导了CALDERA研究项目，以自动化对手仿真。他主张安全

通过在所有可以检测到或阻止对手的位置进行验证，因为防御者不应等待真正的入侵来查看其方法是否有效。Blake毕业于加利福尼亚大学伯克利分校的计算机科学专业。



约翰·韦德 是MITRE的首席网络安全工程师，他为ATT & CK项目和MITRE的赞助商从事防御性业务，威胁搜寻和分析。他是网络分析存储库的维护者之一，也是ATT & CK瞄准的负责人。在此之前，他是STIX 2.0规范的编辑。

## 关于ATT & CK

MITER ATT & CK™是基于现实世界观察结果的全球对抗性战术和技术知识库。ATT & CK知识库被用作私营部门，政府以及网络安全产品和服务社区中特定威胁模型和方法的基础。

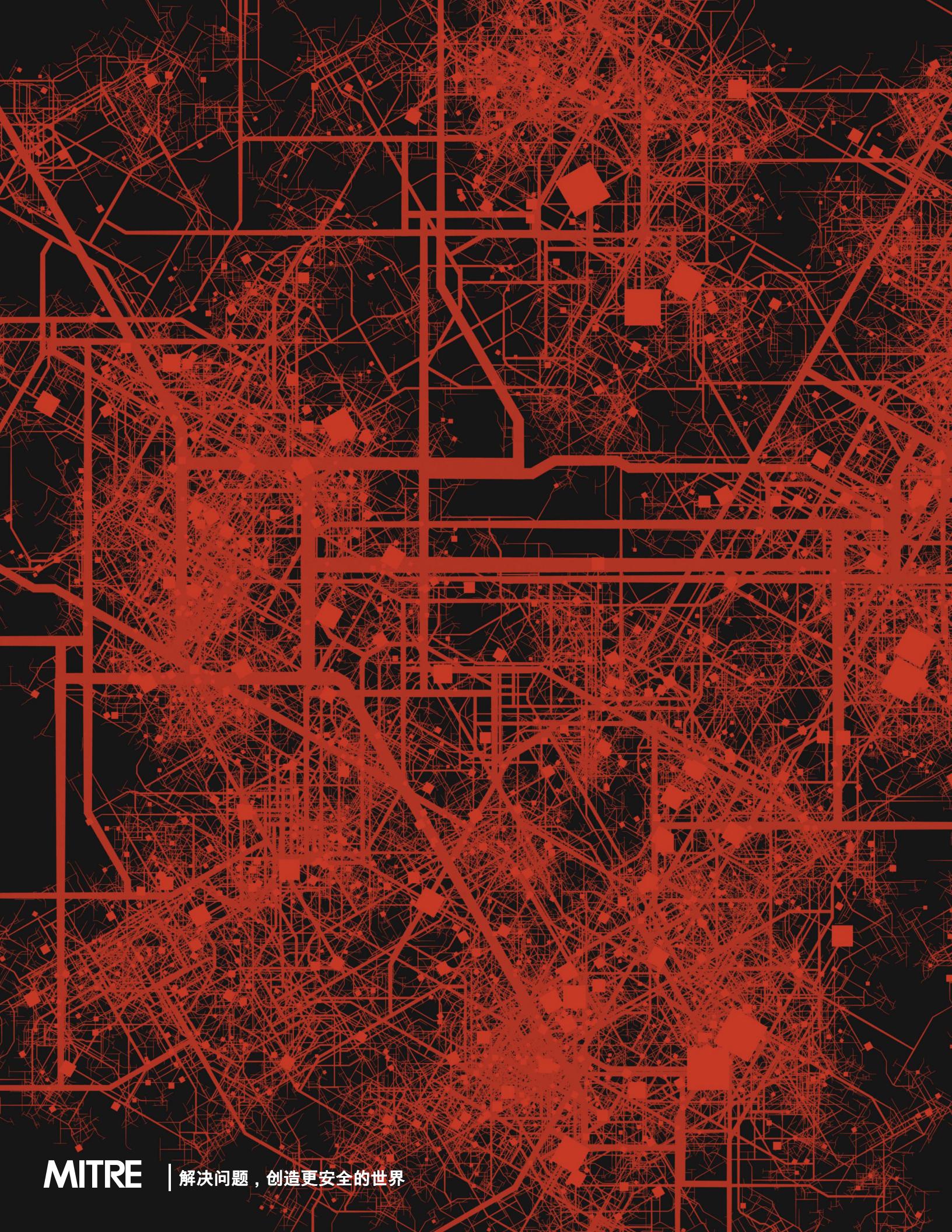
通过创建ATT & CK，MITRE通过将社区聚集在一起以开发更有效的网络安全，来履行其解决问题的任务，以实现更安全的世界。ATT & CK是开放的，任何个人或组织均可免费使用。

了解更多 [Attack.mitre.org](http://Attack.mitre.org)。

## 关于斜接

MITRE的任务驱动团队致力于解决问题，打造更安全的世界。通过公私合作伙伴关系以及联邦资助的研发中心的运营，我们在整个政府中共同努力应对国家安全，稳定与福祉的挑战。了解更多 [www.mitre.org](http://www.mitre.org)。

MITER ATT & CK™和ATT & CK™是MITER Corporation的商标。



**MITRE**

| 解决问题，创造更安全的世界