RSA 2019观察： 威胁建模模型ATT&CK

绿盟科技 发布于 绿盟科技 2019-03-08 21:44

1. 前言

本届RSA中AI/ML是一个热点，当前的人工智能其实可以简单划分为感知智能（主要集中在对于图片、视频以及语音的能力的探究）和认知智能（涉及知识推理、因果分析等），当前算法绝大部分是感知算法，如何教会AI系统进行认知智能是一个难题，需要建立一个知识库，比如在做APT追踪就希望通过认知智能推理其意图，自动化跟踪样本变种等，比较有效的方法是采用威胁建模知识库方式，其中MITRE是一个很典型的公司，最早其主要做国防部的威胁建模，主要是情报分析，从事反恐情报的领域（起源是911后美国情报提升法案），后续延申到网络空间安全领域，其最大的特色就是分类建模，STIX情报架构就是MITRE构建，SITX1.0版本又很浓的反恐情报分析影子。到了STIX2.0阶段，其发现仅仅用TTP很难描述网络空间网络攻击和恶意代码，因此，在STIX2.0中，引入攻击和恶意代码2个相对独立的表述，攻击采用capec，恶意代码采用meac，但是capec和meac过于晦涩，其又在2015年发布了ATT&CK模型及建模字典，用来改进攻击描述。新模型更明确，更易于表达，合并了capec和meac，便于表达和分享，便于安全自动化，而且便于引入知识图谱等新的AI技术。在其官网上就描述了79个APT攻击组织（188个别名）的相关TTP例子。绿盟科技也展开类似的研究，构建了更大的知识图谱，用以进行APT组织的自动化追踪。

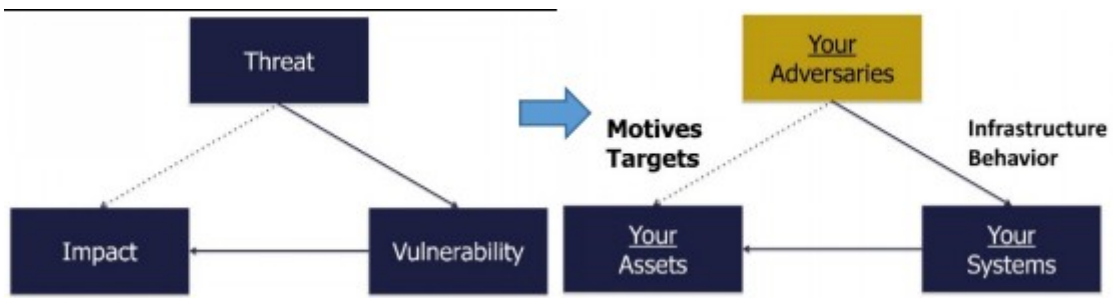
在2019年的RSA大会上，来自Freddy Dezeure公司的CEO Freddy Dezeure和MITRE组织的网络威胁情报首席战略官Rich Struse在《ATT&CK in Practice A Primer to Improve Your Cyber Defense》中介绍了如何利用ATT&CK模型开始建立和提升自己的防御体系；来自Carbon Black公司的高级威胁研究员Jared Myers在《How to Evolve Threat Hunting by Using the MITRE ATT&CK Framework》中介绍了如何用ATT&CK模型进行威胁捕获。

2. 越来越技术能力强大和敏捷的对手

Freddy以造成巨大影响的勒索软件Petya作为引子开始介绍。Petya是一款威力不亚于“WannaCry”的勒索软件，从6月份开始爆发，多个国家受此影响。作为一款勒索软件，它具备很明显的破坏意图，然而它最开始只是通过某个记账软件进行影响和传播，后来利用了泄露的NSA武器库（永恒之蓝漏洞）来进行蠕虫传播。Freddy根据这种情况进行推论，未来的攻击者将会更加灵活和更具变化性：

- 攻击者的基础设施会更具适应能力，能够针对更多不同的目标环境
- 攻击者入侵后会混杂于合法的用户行为中，比如使用合法的基础设施组件、滥用合法用户凭证或者重复执行合法用户行为
- 攻击者也会快速提升自己的能力，利用新漏洞和新泄露的工具

为了应对这种情况，Freddy认为可以建立威胁模型来对问题进行分析。从基于风险的模型开始着手，威胁会利用漏洞进行入侵，入侵后会造成勒索、数据窃取等不良影响。把研究问题的层次进一步提升，模型的威胁上升到其执行主体--攻击者，攻击者会利用漏洞执行一些操作对系统进行入侵，入侵之后的关键的目标在于对有价值的资产进行恶意操作。



根据这个威胁模型，需要从三个步骤开展防御：

1 明确自己的关键资产，会有哪些攻击者以及为什么对这些资产感兴趣

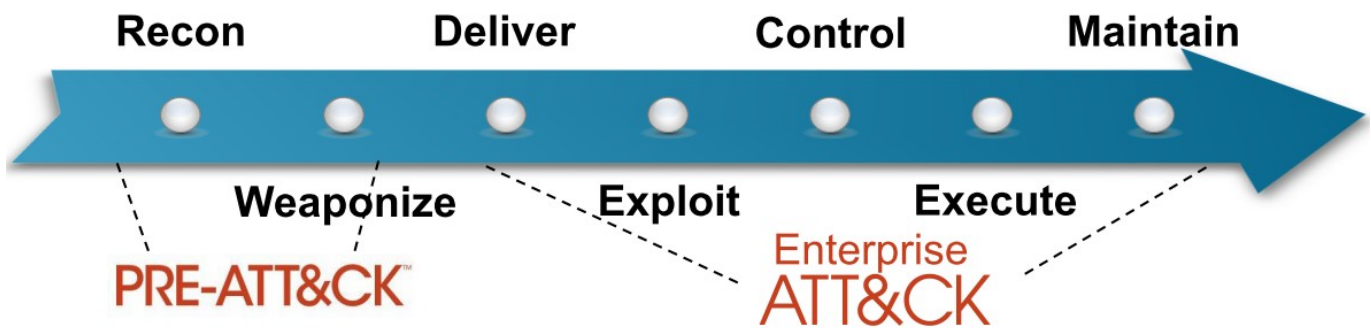
2 利用威胁情报最大限度地对攻击者的基础设施进行观察，比如IOC（Indicators of Compromise）、COA（Course Of Action）

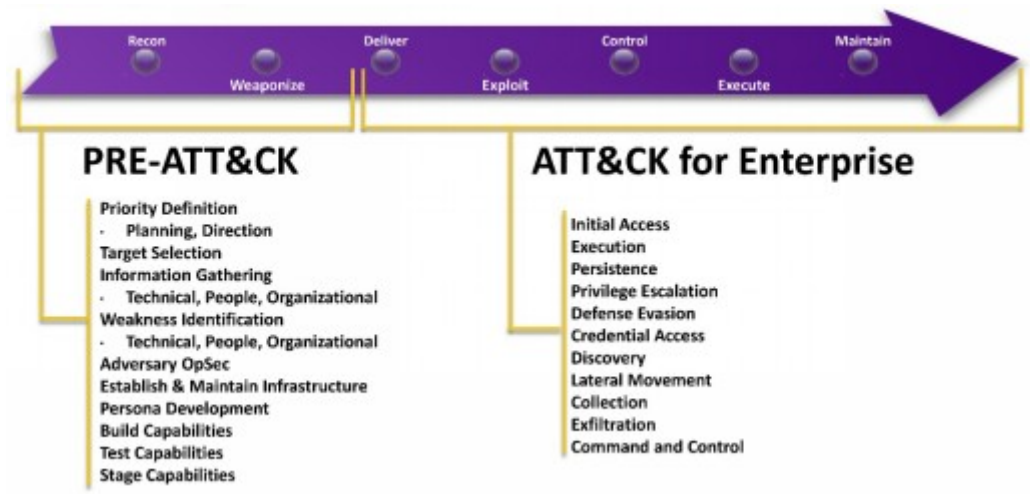
3 观察攻击者的TTP（技术、战术和过程），并将其应用于检测、防御和响应过程

Freddy对其中第三个步骤进行重点强调，因为这个是整个实践中最关键的步骤，需要引入Mitre ATT&CK模型来对攻击者的TTP进行检测、防御和响应。

3. ATT&CK模型

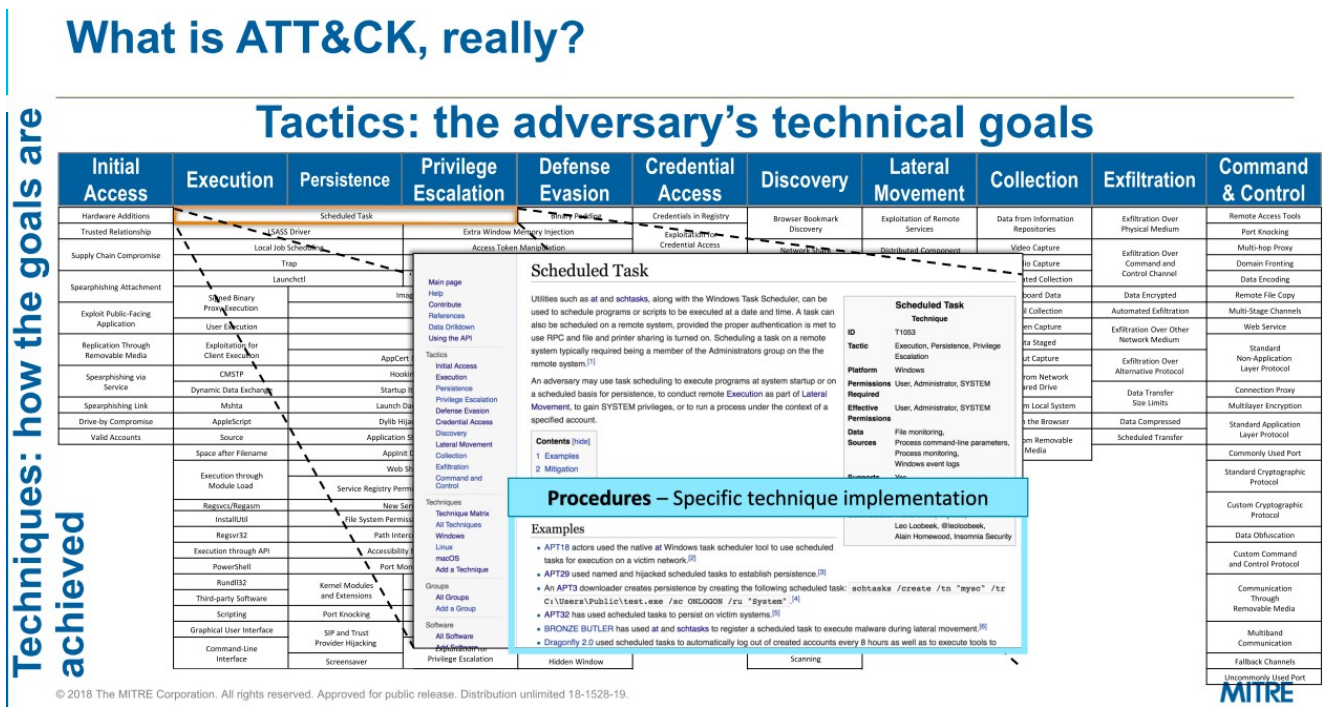
ATT&CK（ Adversarial Tactics, Techniques, and Common Knowledge）是一个反映各个攻击生命周期的攻击行为的模型和知识库。起源于一个项目，用于枚举和分类针对Microsoft Windows™系统的攻陷后的战术，技术和过程（TTP），以改进对恶意活动的检测。目前ATT&CK模型分为三部分，分别是PRE-ATT&CK，ATT&CK for Enterprise和ATT&CK for Mobile，其中PRE-ATT&CK覆盖攻击链模型的前两个阶段，ATT&CK for Enterprise覆盖攻击链的后五个阶段。



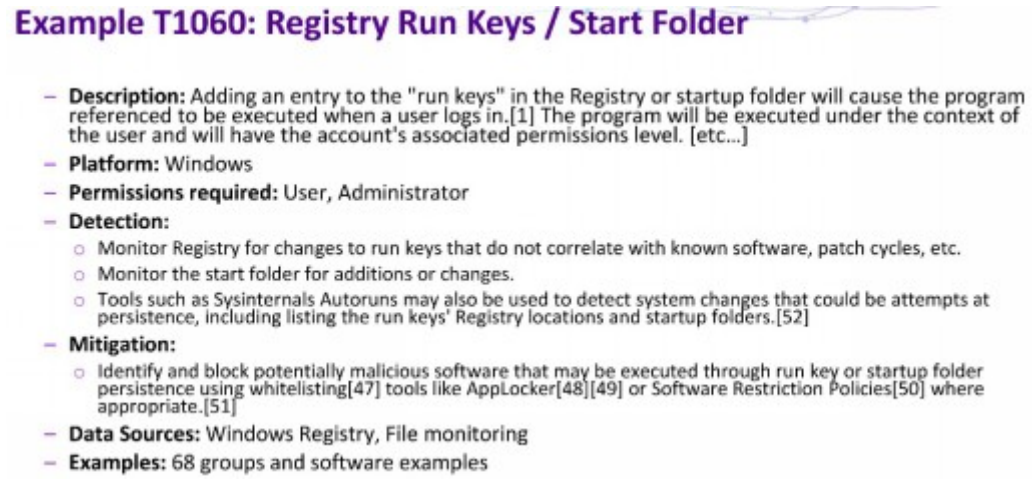


PRE-ATT&CK包括的战术有优先级定义、选择目标、信息收集、发现脆弱点、攻击性利用开发平台、建立和维护基础设施、人员的开发、建立能力、测试能力、分段能力。

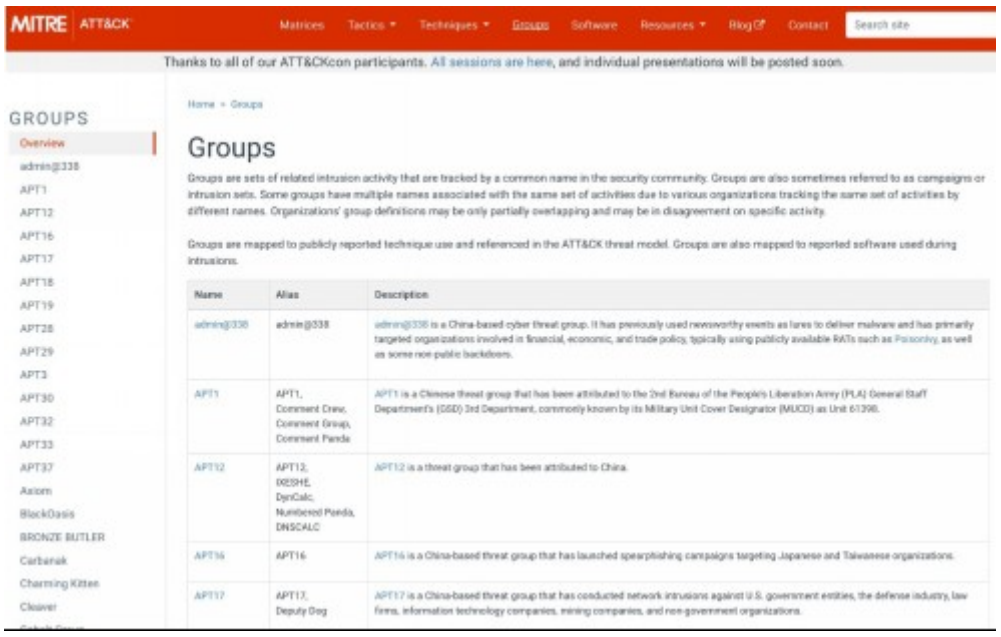
ATT&CK for Enterprise包括的战术有访问初始化、执行、常驻、提权、防御规避、访问凭证、发现、横向移动、收集、数据获取、命令和控制。



其中一个技术会被用于实现多个战术，过程则是该技术在实际攻击中的具体实现。比如“计划任务”（T1053）这个技术会被用于执行、常驻和提权这三个战术中。过程则以APT组织的历史攻击行为作为例子，比如APT3 使用schtasks /create /tn "mysc" /tr C:\Users\Public\test.exe /sc ONLOGON /ru "System" 命令来创建计划任务。一个具体的技术还会包含其它信息，比如针对的平台（Windows、Linux、Mac OS）、执行所需权限、检测手段和缓解手段等信息。



MITRE ATT&CK对这些技术进行枚举和分类之后，能够用于后续对攻击者行为的“理解”，比如对攻击者所关注的关键资产进行标识，对攻击者会使用的技术进行追踪和利用威胁情报对攻击者进行持续观察。MITRE ATT&CK也对APT组织进行了整理，对他们使用的TTP（技术、战术和过程）进行描述。

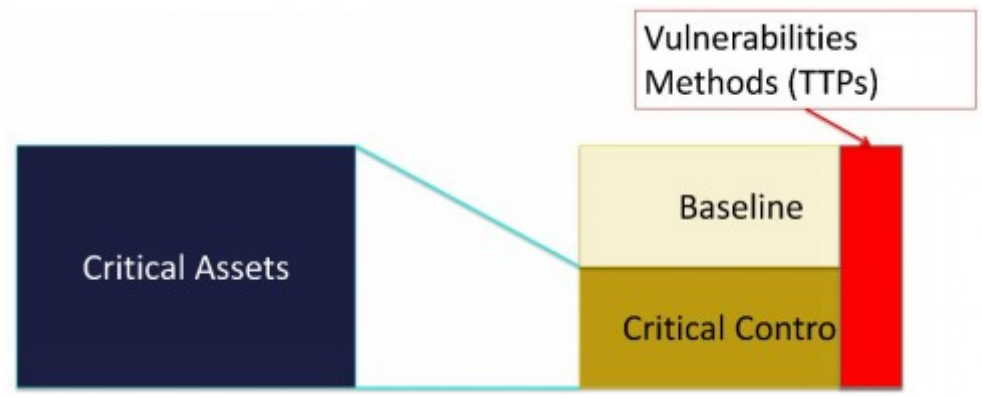


Freddy认为与其它模型相比，ATT&CK的关键价值在于其提供了一个通用的分类、可以根据需求对特定技术进行实现和覆盖，不需要实现模型所列举的整个技术矩阵，优先关注实际的预防、检测和响应。除此之外，ATT&CK使用通用语言对TTP进行描述，也提供基础的知识能够用于对TTP的观测，并且会持续对模型进行更新，不依赖于某个厂商，被广泛开源社区采用。

4 实践

4.1 提升防御能力

如何将ATT&CK应用于实际的防御体系中，Freddy认为首先需要理解作为防守方的可控部分。攻击者一般会利用漏洞对系统进行入侵，如果对关键资产进行操作，那会有部分动作涉及关键控制。那么对关键控制的行为进行调整和验证，就能够对攻击者的恶意行为进行捕获。

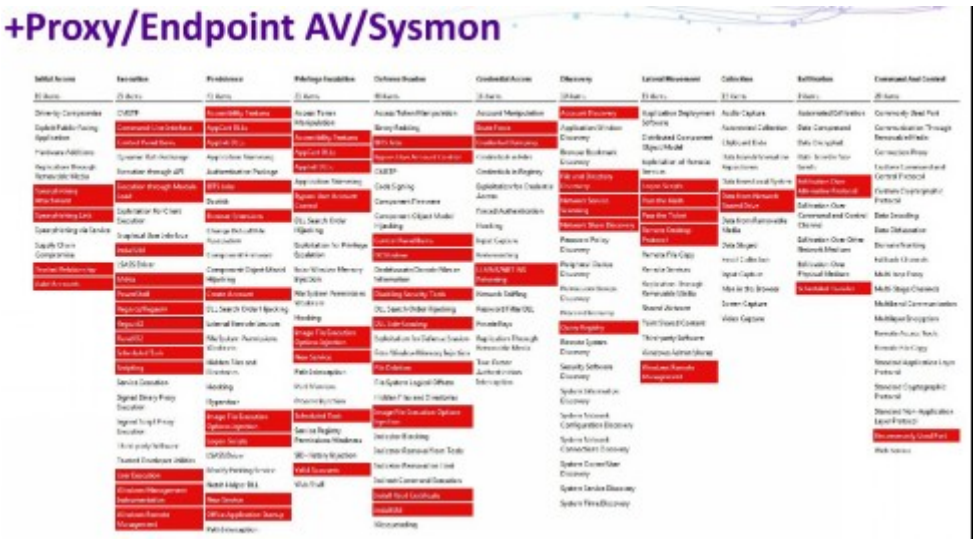


想要对关键控制的行为进行验证，需要先对自己的检测能力进行检查：

- 从收集的日志中识别攻击行为
- 设计分析体系，从攻击者的相关知识开始分析、或参考开源社区
- 部署分析程序，用于检测、捕获和能力改善

接着从已知的攻击组织所覆盖技术上分析，研究哪些技术会对关键资产造成严重影响。

再检查自身的检测能力能否对关键技术进行覆盖，比如使用代理、终端杀毒软件、系统监视器的日志所能覆盖的技术范围是否满足自己的需求。

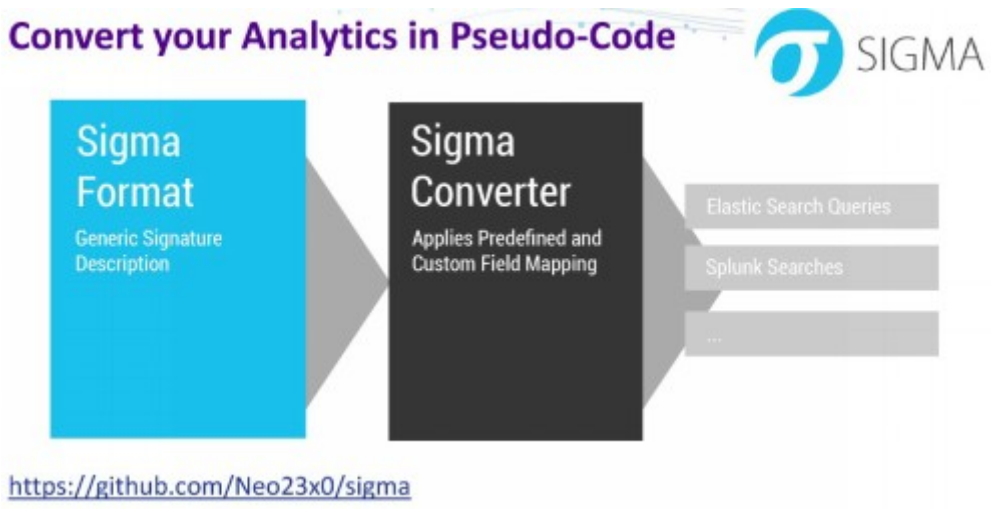


最终建立针对自身所需的分析程序：

1. 对自己关注的“技术”进行研究，阅读相关文档。参考现有的分析或者是开源社区的源码，将可能合法的行为与恶意行为进行区分。

2. 使用关注的技术进行模拟攻击演练，检查对应日志的记录情况

3. 自己写查询语句对日志进行事件搜索，不断进行测试和迭代，使用相关技术发起多种模拟攻击，减少误报



在日志事件搜索方面，Freddy对开源项目SIGMA进行介绍。目前，IOC和YARA规则在检测恶意网络连接和恶意文件起到重要作用，然而缺乏一种通用的能够从日志事件中描述特定事件的检测方法。人们收集日志数据进行分析都需要先从阅读大量的资料开始，之后再构建自己对日志数据的搜索方法和规则。由于没有一个标准化格式，因此人们也无法与他人分享自己的工作。

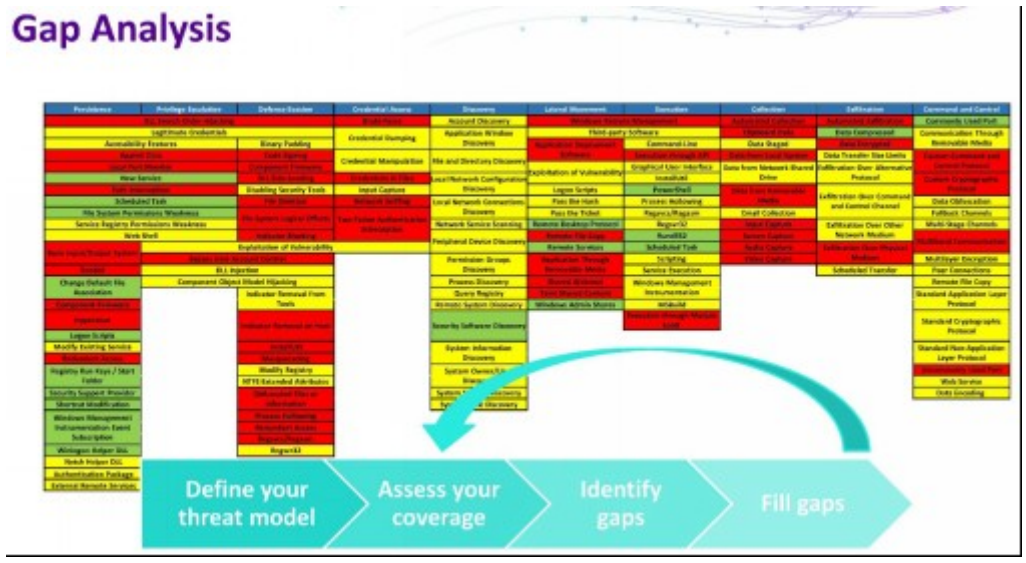
Sigma是一种通用开放的签名格式，允许以直接的方式描述相关的日志事件。其规则格式灵活，易于编写并适用于任何类型的日志文件。 该项目的主要目的是提供一种结构化的形式，研究人员或分析人员可以在其中描述他们曾经开发的检测方法，并使其与他人共享。使用sigma来进行规则编写和搜索，也能够避免过度依赖于特定厂商。目前在Sigma的项目中已经提供了针对APT、应用、Linux、Windows、网络、代理、Web等相关方面的日志规则。

在模拟攻击演练方面，Freddy介绍了四款基于ATT&CK模型的攻击测试工具：

- MITRE Caldera：一个自动攻击仿真系统，能够在Windows企业网络中执行攻陷后的恶意行为。
- Endgame RTA：一个针对Windows的Python脚本框架，用于蓝队测试他们对基于ATT&CK模型的恶意技术的检测能力。Endgame RTA可生成超过50种不同的ATT&CK 战术，包括一个二进制应用程序，可执行所需的活动。
- Red Canary Atomic Red Team：一个开源的小型，高度可移植的测试集合，映射到MITRE ATT和CK框架中的相应技术。 这些测试可用于验证检测和响应技术和过程。
- Uber Metta: 一个用于基础对抗模拟的工具，将多步的攻击者行为解析为yaml文件，并使用Celery将操作进行排队，自动化执行。

其中MITRE Caldera执行的动作由计划系统结合预配置的ATT&CK模型生成。这样的好处在于能够更好更灵活地对攻击者的操作进行模拟，而不是遵循规定的工作序列。自动模拟攻击者进行攻击演练，安全地重现发生过的攻击行为，不会对资产造成损害，并且能够重复执行以对防御能力和检测能力进行测试和验证。

通过不断地攻击演练测试，就能提升分析程序的检测能力，不断扩大技术覆盖范围，不断缩小与攻击者的差距。



4.2 威胁捕获

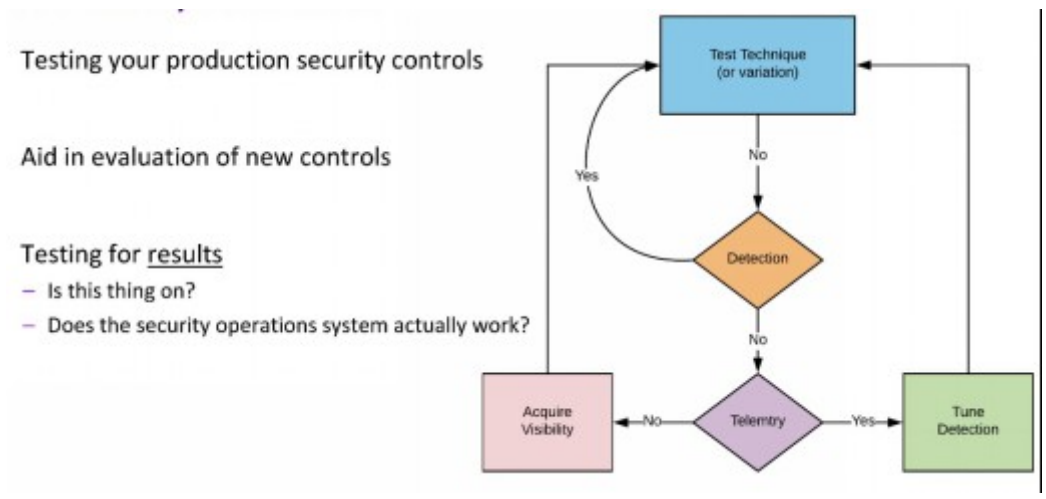
ATT&CK模型还能够应用用于威胁捕获。来自Carbon Black公司的高级威胁研究员Jared Myers在《How to Evolve Threat Hunting by Using the MITRE ATT&CK Framework》中介绍了如何运用ATT&CK模型进行威胁捕获。

Jared介绍说很多企业意识到，自己的资产是否会被攻破已经不再是一个问题了，更多需要关注的是什么时候被攻破。因此，许多企业需要的工具不仅能够检测和响应威胁，还能够对威胁进行搜寻和捕获，以快速识别内部的潜在危害。

在防御的基础之上，威胁捕获对整套分析体系提出了更高的要求：

- 能够利用工具对之前覆盖的技术检测出高质量的告警
- 分析思路集中于不容易检测到的地方
- 对分析的范围进行扩宽，比如通样的方法可能会用于不同的目的，又或者会采用其它的战术或技术来完成特定目的

在威胁捕获的实际实践中，同样需要不断测试和迭代来提升对未知威胁的检测能力



Jared以T1191 CMSTP作为例子进行展开，在开始研究之前可以先从MITRE WIKI 获取CMSTP的技术详情。

CMSTP

The Microsoft Connection Manager Profile Installer (CMSTP.exe) is a command-line program used to install Connection Manager service profiles. [1] CMSTP.exe accepts an installation information file (INF) as a parameter and installs a service profile leveraged for remote access connections.

Adversaries may supply CMSTP.exe with INF files infected with malicious commands. [2] Similar to Regsvr32 / "Squiblydoo", CMSTP.exe may be abused to load and execute DLLs [3] and/or COM scriptlets (SCT) from remote servers. [4] [5] [6] This execution may also bypass AppLocker and other whitelisting defenses since CMSTP.exe is a legitimate, signed Microsoft application.

CMSTP.exe can also be abused to Bypass User Account Control and execute arbitrary commands from a malicious INF through an auto-elevated COM interface. [3] [5] [6]

ID: T1191
Tactic: Defense Evasion, Execution
Platform: Windows
Permissions Required: User
Data Sources: Process monitoring, Process command-line parameters, Process use of network, Windows event logs
Supports Remote: No
Defense Bypassed: Application whitelisting, Anti-virus
Contributors: Ye Yint Min Thu Htut, Offensive Security Team, DBS Bank, Nik Seetharaman, Palantir
Version: 1.0

Jared分享了对CMSTP技术进行威胁捕获的研究思路，提示攻击者可能会采用少为人知的技术来进行信息传输，因此可以先检查是否存在关键的恶意行为指标，比如

- 是否建立网络连接
- 是否在临时目录创建子进程，进行命令交互等
- 是否从dllhost cmstp COM对象中创建的子进程

再从“是什么”和“怎么做”的思路来进行研究，比如：

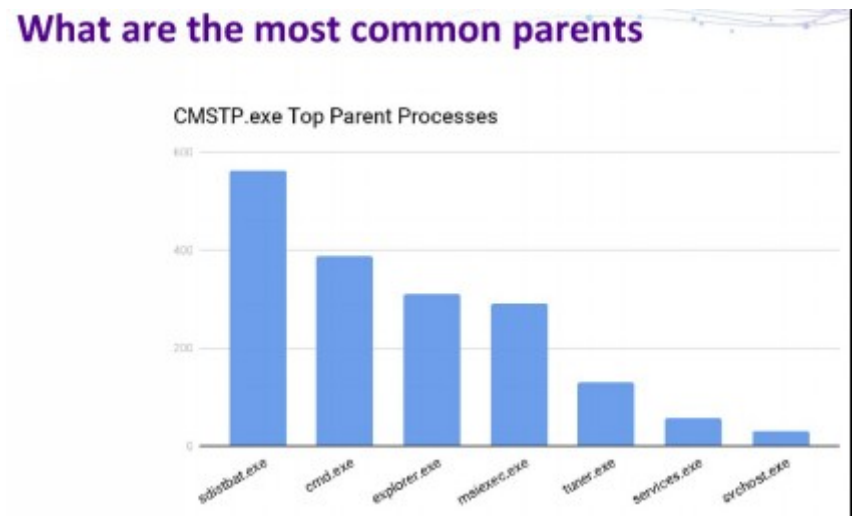
1. 二进制是不签名

3. 该二进制文件能否执行远程命令

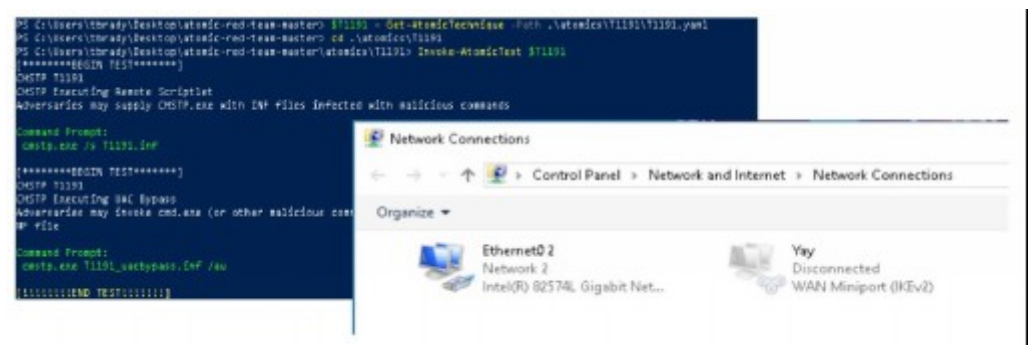
4. 该二进制在进程运行时是否会自动提权

也可以从该二进制的执行频率进行分析

还可以从父进程调用CMSTP的频率进行分析

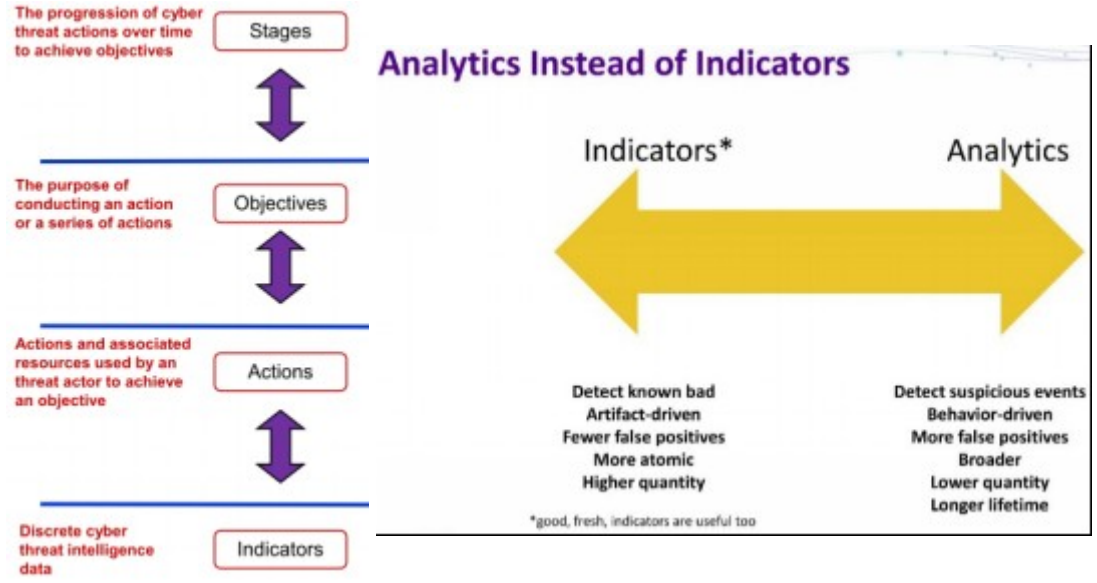


同样也可以使用atomic red team攻击演练工具进行在内部进行单元测试

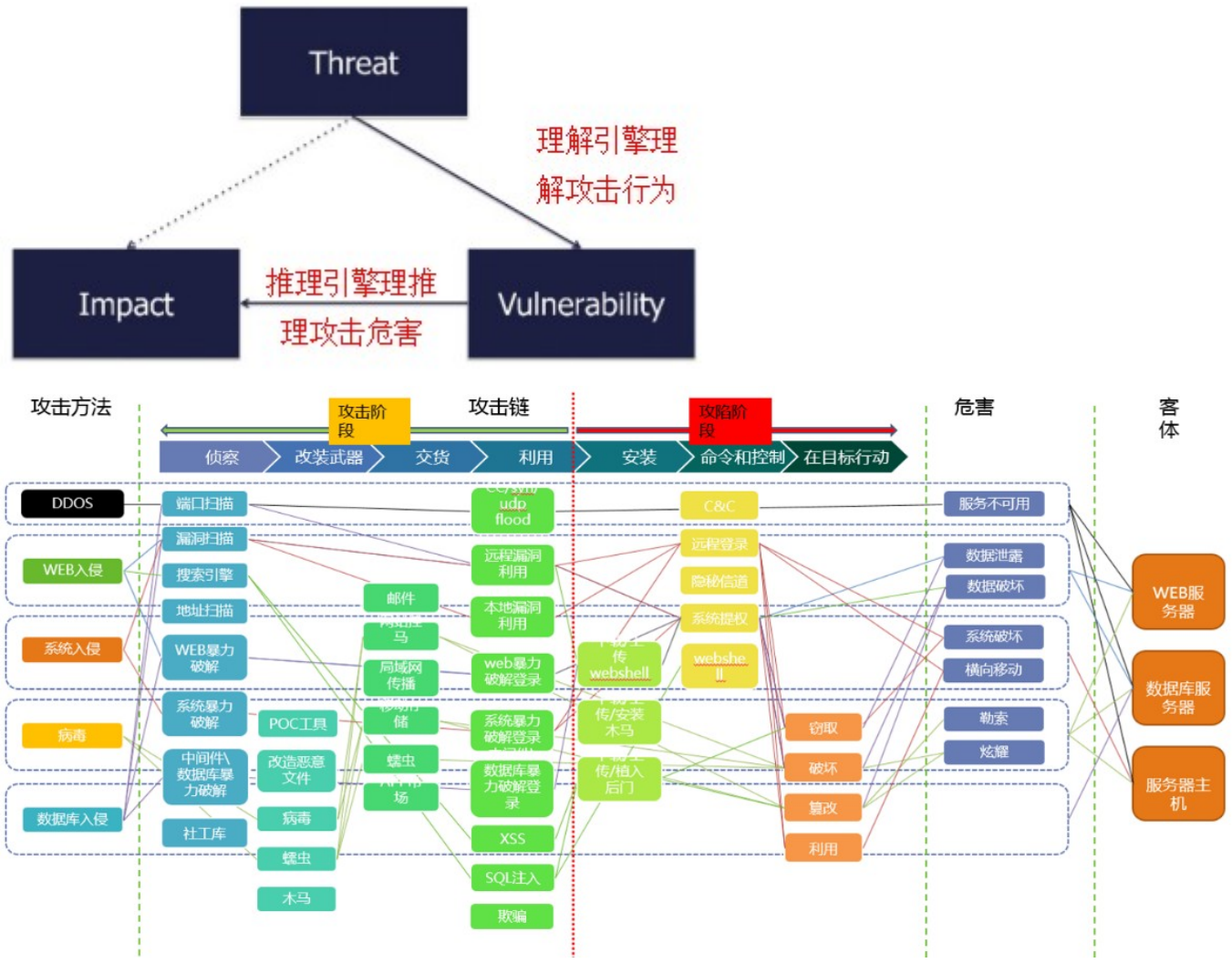


6. 绿盟科技建模研究实践

从建模的层次来看，ATT&CK模型的建模主要集中于行为层面，而传统防护设备的告警则属于指示器层。指示器层能够检测已知的恶意数据，由人为特征进行驱动，误报少，粒度小所以对应告警数量庞大。行为层的分析针对可疑的事件进行检测，由行为进行驱动，误报相对较多，粒度大所以事件数量少，生命周期更长。ATT&CK在行为层进行建模，一方面能够充分利用威胁情报的TTP进行知识共享，另一方面能够在更宏观的程度对攻击者进行画像，能够从具体的技术手段和指示器规则中解脱出来。



绿盟科技在威胁建模方面也是集中于行为层的抽象建模。针对防护设备产生的大量告警，绿盟科技使用理解引擎将海量告警理解为相应的攻击行为，对应为风险模型的威胁主体利用目标漏洞进行攻击。使用推理引擎推理攻击造成的危害，对应为风险模型的漏洞造成影响，并结合攻击链模型进行攻陷研判。



鉴于实际网络环境的复杂性，只对攻击行为进行建模来分析问题是远远不够的。因此绿盟科技结合知识图谱，设计了多个本体对整个网络威胁进行建模分析，并兼容MITRE组织的CAPEC、MAEC和ATT&CK等模型的接入和使用，能够从多方威胁情报中提取关键信息并作为知识对知识图谱进行扩展。

在能力提升方面，绿盟科技也使用还原真实攻击场景和模拟实际攻防演练的方式进行产品的测试，同时组织多次内部红蓝对抗对自身防御能力进行检验。

7. 小结

Freddy和Rich在《ATT&CK in Practice A Primer to Improve Your Cyber Defense》的分享侧重于对ATT&CK模型的实际应用落地，从威胁建模开始分析问题，先明确要抵御的攻击者和需要保护的关键资产，再介绍利用ATT&CK模型建立自己的分析防御体系的具体步骤，以及后续对自身的防御能力进行提升的方法，也介绍了不少有用的工具和资源。Jared在《How to Evolve Threat Hunting by Using the MITRE ATT&CK Framework》的分享则侧重于利用ATT&CK模型进行威胁捕获，介绍如何在建立防御体系之后对未知威胁进行挖掘，也分享了不少具体的研究思路。经过研究和比较，绿盟科技在建模思路上与ATT&CK模型基本处于同一层面，能力提升的思路也是一致，由于支撑业务的不同导致实现的功能有所区别，但其研究思路上还是具有很高的参考价值。

8. 相关资料

ATT&CK：https://attack.mitre.org/

SIGMA：https://github.com/Neo23x0/sigma

Mitre Caldera：https://github.com/mitre/caldera

Endgame Red Team Automation：https://github.com/endgameinc/RTA

Redcanary Atomic Red Team：https://www.redcanary.com/atomic-red-team/

Uber Metta：https://github.com/uber-common/metta

Advanced-Threat-Hunting-with-Carbon-Black：http://the.report/assets/Advanced-Threat-Hunting-with-Carbon-Black.pdf