计算机科学
COMPUTER SCIENCE

ATT&CK框架下基于事件序列关联的网络高级威胁检测系统

张宇翔, 韩久江, 刘建, 鲜明, 张洪江, 陈宇, 李子源

引用本文

张宇翔, 韩久江, 刘建, 鲜明, 张洪江, 陈宇, 李子源ATT&CK框架下基于事件序列关联的网络高级威胁检测系统[J]. 计算机科学, 2023, 50(6A): 220600176-7.

ZHANG Yuxiang, HAN Jiujiang, LIU Jian, XIAN Ming, ZHANG Hongjiang, CHEN Yu, LI Ziyuan. Network Advanced Threat Detection System Based on Event Sequence Correlation Under ATT&CK Framework [J]. Computer Science, 2023, 50(6A): 220600176-7.

计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.220600176

ATT&CK 框架下基于事件序列关联的网络高级威胁检测系统

张宇翔[1]　韩久江[1]　刘　建[1]　鲜　明[1]　张洪江[2]　陈　宇[1]　李子源[3]
1 国防科技大学电子科学学院　长沙 410000
2 安康学院电子与信息工程学院　陕西 安康 725000
3 31438 部队　沈阳 110031
(zyx998522@163.com)

摘　要　随着网络技术的快速发展,网络世界攻防对垒愈发激烈,高级网络威胁行为层出不穷,但目前网安分析人员在实际运维中对多步攻击行为的过程描述仍存在一定差异,造成了巨大的语义沟通成本。为了解决在网络高级威胁检测中的这一痛点问题,采用 ATT&CK 网络对抗行为框架作为多步攻击行为的统一描述语言,设计实现了一套基于事件序列关联的网络高级威胁检测系统,通过事件序列关联模型可以实现对多步攻击行为的有效检测,并通过 ATT&CK 攻击矩阵可视化呈现,有助于分析人员明晰恶意攻击的手段、策略及目的,分析人员通过检测系统呈现出的技术和战术,采取相应的防御措施,能够降低攻击者的攻击效果。实验结果表明,检测系统检出率可达 96.43%,对网络攻击事件中的分析人员解决"防守困境"具有极大的现实意义。

关键词:对抗性战术;技术和常识;多步攻击检测;事件序列关联;高级持续威胁
中图法分类号　TP393.0

Network Advanced Threat Detection System Based on Event Sequence Correlation Under ATT&CK Framework

ZHANG Yuxiang[1],HAN Jiujiang[1],LIU Jian[1],XIAN Ming[1],ZHANG Hongjiang[2],CHEN Yu[1] and LI Ziyuan[3]
1 College of Electronic Science and Technology,National University of Defense Technology,Changsha 410000,China
2 College of Electronics and Information Engineering,Ankang University,Ankang,Shaanxi 725000,China
3 31438 Unit,Shenyang 110031,China

Abstract　With the rapid development of network technology,the network world is becoming more and more fierce in attack and defense confrontation,and advanced network threat behaviors are emerging,but there are still some differences in the process description of multi-step attack behaviors in the actual operation and maintenance of the current network security analysts,which causes huge semantic communication costs. In order to solve this pain point problem in network advanced threat detection,ATT&CK network adversarial behavior framework is adopted as the unified description language of multi-step attack behavior,and a network advanced threat detection system based on event sequence association is designed and implemented,which can achieve effective detection of multi-step attack behavior through event sequence association model and visualize the presentation through ATT&CK attack matrix,which helps analysts to clarify the means,strategies and purposes of malicious attacks,and analysts can reduce attacker's attack effect by taking corresponding defense measures through the techniques and tactics presented by the detection system. Experimental results show that the detection rate of the detection system can reach 96.43%,which is of great practical significance for analysts to solve the "defense dilemma" in network attacks.

Keywords　Adversarial tactics,Techniques and common knowledge,Multi-step attack detection,Event sequence correlation,Advanced persistent threats

1　引言

随着网络技术的快速发展,人类社会已经进入网络信息时代,在二十一世纪,网络已经深深地渗透到民众日常生活的各个角落中,已然成为当今人类社会必不可少的基础服务。但同时,网络世界中威胁层出不穷,攻防对垒愈发激烈,网络空间安全已成为国家政治、经济、生活正常运行的前提,现阶段,包括我国在内的诸多国家和地区已将网络空间安全作为国家安全的重要组成部分[1]。目前在网络空间中的最大威胁便是由专业组织发起的 APT 攻击[2-3],APT 攻击(Advanced Persistent Threat)全称是"高级持续性威胁攻击",也被称为定向威胁攻击,指某组织对特定对象展开的持续有效的攻击

基金项目:国家自然科学基金(61801489);湖南省自然科学基金(2020JJ5666)
This work was supported by the National Natural Science Foundation of China(61801489) and Natural Science Foundation of Hunan Province(2020JJ5666).
通信作者:韩久江(1069930599@qq.com)

活动。我国就是 APT 攻击的主要受害国之一，自我国正式接入互联网后便踏上了与世界上的病毒木马等网络攻击斗智斗勇的征程，中国也遭受了愈发频繁复杂的网络攻击[4]。这种攻击活动具有极强的隐蔽性和针对性，通常会运用受感染的各种介质、供应链和社会工程学等多种手段实施先进的、持久的、有效的威胁和攻击，从攻击开始到达成目的，有的 APT 攻击甚至可能潜伏长达数年。

而且在网络安全领域，攻击者往往拥有得天独厚的优势，加之不断扩充的海量网络武器库，使得攻击者可以对组织、个人进行恶意攻击，与之相反的防守方则处于敌暗我明的被动地位，需要用有限的资源去对抗无限的安全威胁，本文将这种攻防不对称的情况称作“防守者困境”。“防守者困境”始终围绕几个核心问题：我们是否能检测到 APT 攻击？防御方案是否有效？安全防御优先级如何确定？不同安全工具防御范围是否有重叠？

IOC(Indicators of Compromise)全称是“威胁情报”，是用于描述特定攻击活动中主机或网络行为特征的基本指示数据[5]，一般为网络流量中或者操作系统上观察到的能高度表明计算机被入侵的痕迹，例如某某病毒的 Hash 值、C&C 服务器的 IP 地址等。起初防守方利用 IOCs 威胁情报进行攻击检测，通俗地讲，威胁情报就像是当计算机被入侵时所表现出来的某种特征，我们将这些威胁情报搜集起来整理成库，当计算机再次表现出库中的某些特征时就可判定计算机已经被入侵了[6-7]。Bianco 对威胁情报提出了痛苦金字塔模型[8]，用于对 IOCs(Indicators of Compromise)情报进行分类并描述其在攻防对抗中的价值以及应用难度。正如图 1 的痛苦金字塔所示，文件的哈希值是最简单、最基础的威胁情报信息，其价值也最低，利用难度也最小，IP 地址、域名、网络/主机证据、工具、战术等价值依次提升，其给攻击方造成的难度和痛苦也递增。

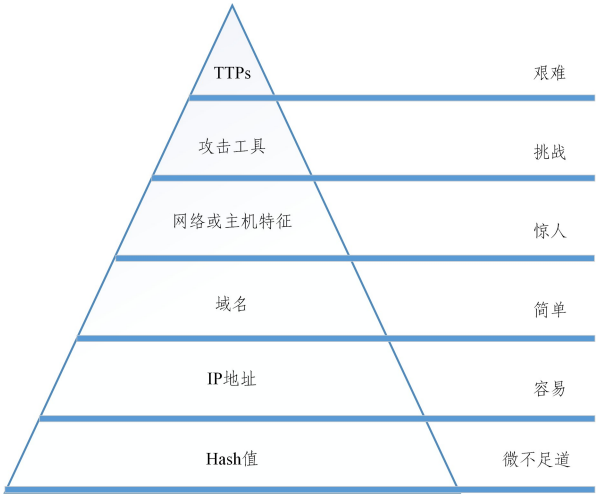


图 1 痛苦金字塔模型

Fig. 1 Pain pyramid model

目前广泛应用的分析、检测基础仍然以金字塔模型底层的 IOC 为主[9-11]，例如病毒样本的 HASH 值、域名、IP、注册表、流量等信息，但底层的 IOC 威胁情报并不能表达攻击者如何与受害系统交互，只能表示其是否受害而无法体现过程，只能表示“是与否”“黑与白”，它反映的是现在所处的状态和发生的事件，不能表达“攻击过程”这种具有方向性的特性。除此之外，IOC 还有一个缺点就是不稳定性，特别是 Hash，IP 等，攻击者可以轻易改变。通常多个 IOC 其实表达的是同一个攻击过程。总而言之，IOC 方便检测、但是不善于描述攻击，因此针对高级技战术层面的网络高级威胁检测研究亟待开展。

2 ATT&CK 框架

2.1 框架简介

2003 年，MITRE 公司[12]为了解决网络攻防中存在的“防守者困境”，基于现实网络攻防中发生的真实攻击事件，创建了一个对抗战术和技术知识库，即 Adversarial Tactics, Techniques, and Common Knowledge，简称 ATT&CK[13-15]。ATT&CK 框架区别于其他框架的最显著的特点就是整个框架是基于攻击者的视角构建的。其以攻击者执行攻击的步骤构建整体框架，通过攻击方式的平台、来源、场景等维度对攻击行为进行归类划分。

由于 ATT&CK 框架内容丰富、实战性强，在实战中具有更全面的效用，得到了业内的广泛关注，图 2 给出了关键词 ATT&CK 在 Google Trends 中的热度趋势。

图 2 ATT&CK 框架的热度发展趋势

Fig. 2 Hot trend of ATT&CK framework

迄今为止，ATT&CK 框架已经确定为 3 个板块，分别是 ATT&CK for Enterprise(用于传统企业网络和云技术)、ATT&CK for Mobile(用于移动通信设备)和 ATT&CK for ICS(用于工业控制系统)[16]，如表 1 所列。

表 1 ATT&CK 技术领域

Table 1 ATT&CK technology field

技术领域	适用平台
ATT&CK for Enterprise	Linux, macOS, Windows, AWS, Azure, GCP, SaaS, Office365, Azure AD, Containers
ATT&CK for Mobile	Android, iOS
ATT&CK for ICS	N/A

在 ATT&CK 框架中，战术代表了实施 ATT&CK 技术的原因，是攻击者执行某次攻击的战术目标。战术介绍了各项技术的环境类别，并涵盖了攻击者在攻击时执行行动的标准、标记等信息。例如持久化、发现、横向移动、执行和数据窃取等战术。技术代表着攻击者通过执行动作来实现战术目标的方式，也可以理解为攻击者通过执行一个动作要获取的“内容”。例如，攻击者可能会转存凭证，之后可能使用这些凭证进行横向移动。

2.2 发展现状

目前，ATT&CK 框架介绍了攻击者在攻击过程中采用的 14 项战术、180 多项技术、360 多项子技术，其中包括特定技术和通用技术，以及有关知名攻击组织及其攻击活动的背景信息和攻击中所使用的技术、战术。其围绕对抗的战术、

技术和常识进行分类，通过矩阵的方式呈现。ATT&CK 框架将攻击者视角下完整的攻击序列拆分成了不同的战术，在每个战术中，根据攻击者使用的攻击方法不同划分为不同的技术，技术是实现战术目标的方式[17]。图 3 给出了 ATT&CK 框架中的技术分布情况。

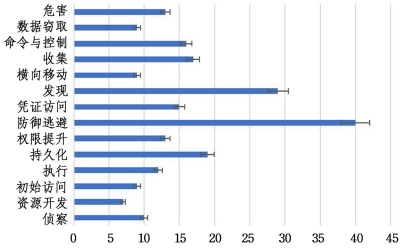


图 3　ATT&CK 框架中技术分布情况

Fig. 3　Distribution of technologies in ATT&CK

ATT&CK 框架自 2015 年发布以来，经过 10 个版本的更迭，现已逐渐发展成为高细粒度、高准确度的安全知识框架。战术由最初的 8 项发展到现在的 14 项；技术由最初的 60 多项发展到现在的 180 多项，其中子技术达 360 余项。ATT&CK 框架所覆盖的知识范围逐年增加，变化情况如图 4 所示。

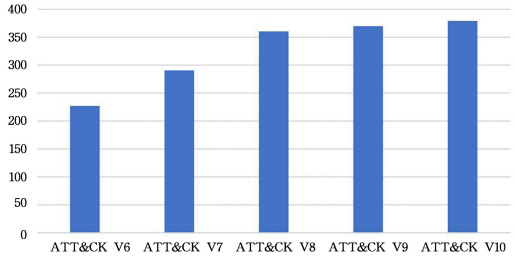


图 4　ATT&CK 框架子技术变化情况

Fig. 4　Changes in ATT&CK framework technology

3　系统构建与实现

3.1　系统模型

基于事件序列关联的威胁检测系统，面向 ATT&CK 网络对抗行为知识库框架建立描述标准进行分析研究，目的是实时监控网络环境中的各类事件，对大量数据进行过滤处理并实现分布式存储，在不同事件间关联分析，对网络高级威胁行为检测告警，并通过 ATT&CK 矩阵的形式将攻击者使用的技战术信息、攻击路径及进程可视化，呈现给网络安全分析人员。该威胁检测系统模型如图 5 所示。

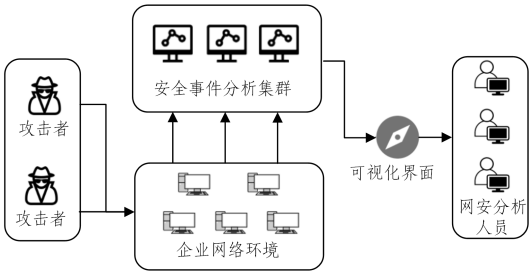


图 5　基于事件序列关联的网络高级威胁检测系统模型

Fig. 5　Network advanced threat detection system model based on security event sequence correlation

(1)攻击者。指代一个 APT 攻击组织及其攻击者，攻击者利用企业网络环境中存在的漏洞，利用网络攻击武器对企业网络环境进行渗透、入侵等操作，通过若干技术执行达到战术目标，以实现网络高级威胁行为。

(2)企业网络环境。企业网络环境是目前遭受网络高级威胁的主要目标，企业网络的架构也是经典的网络拓扑结构，搭建企业网络环境作为攻防双方的“战场”具有很强的现实意义。攻击者通过嗅探漏洞入侵网络环境达到其攻击的目的意图，分析人员则监控网络环境，实现发现异常、识别攻击、缓解症状、修补漏洞等一系列防守行为。

(3)安全事件分析集群。多台服务器组成分布式系统作为安全事件分析集群的物理设备基础。该集群是整个系统的核心部分，负责从企业网络环境中采集各种主机、安全设备及软件生成的数据源，接着对探针采集的数据进行分布式存储，确保数据存储持久化的可靠性。安全事件分析集群可以实现数据过滤、增、删、查等操作，支持在不同事件之间关联，创建关联规则或警报，实现对安全信息与事件的高效可靠管理。

(4)可视化界面。安全事件分析集群分析处理完毕的信息交由可视化界面接收，可视化界面对其进行展示。可视化前端基于 ATT&CK 攻击矩阵进行攻击行为的展示，以 ATT&CK 网络对抗行为知识库描述网络高级威胁行为，展示攻击路径中使用的技战术信息。

(5)网络安全分析人员。网络安全分析人员通过可视化界面获取安全事件分析集群处理的结果，获取上述技战术信息及攻击路径信息，同时分析人员可以根据需要对安全事件分析集群进行基础操作及规则创建等一系列交互，满足网络安全分析人员的分析需求。

3.2　系统实现

面向 ATT&CK 框架基于事件序列关联的网络高级威胁检测系统按照业务功能进行模块化分类，主要分为数据采集层模块、索引存储层模块、事件分析层模块以及态势可视化层模块。系统总体框架及各模块详情如图 6 所示。

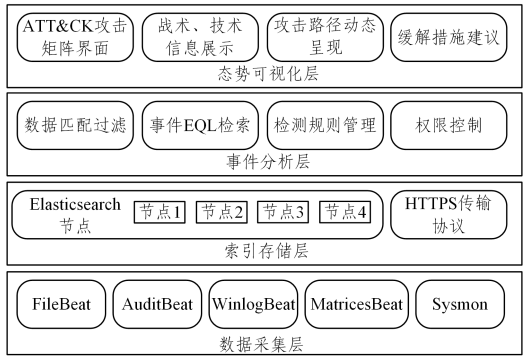


图 6　基于事件序列关联的网络高级威胁检测系统框架

Fig. 6　Framework for advanced network threat detection system based on security event sequence correlation

3.2.1　数据采集层

数据采集层基于 Sysmon 和 Elastic Stack 技术栈中的 Beats 组件实现具体功能。系统监视器(Sysmon)是 Windows 系统服务和设备驱动程序，其功能主要是监视系统中特定活动并将其记录到 Windows 事件日志中[18]。Elastic Stack[19]是由 Elasticsearch，Logstash，Kibana 及 Beats 组成的数据处理工具链，是目前开源界最流行的实时数据分析解决方案。Beats 组件是轻量级(资源高效、无依赖性、小型)和开放源代码日志

发送程序的集合，这些日志发送程序充当安装在基础结构中不同服务器上的代理，用于收集日志或指标。

使用 Beats 组件置入企业网络环境中的待监测主机作为采集探针，由其采集主机行为日志数据。目前，企业网络环境中主流操作系统主要分为 Windows 和 Linux，监测采集模块针对不同操作系统特性提供不同的采集方案，具体如表 2 所列。

表 2 Windows 和 Linux 中监测探针部署方案

Table 2 Monitoring probe deployment solutions in Windows and Linux

探针名称	监测目标操作系统	功能
Winlogbeat	Windows	采集 Windows 主机行为日志
Sysmon	Windows	监控 Windows 主机行为事件
Auditbeat	Linux	监控采集用户行为和系统进程
Filebeat	Windows Linux	监控采集主机特定日志文件
Matricebeat	Windows Linux	监控采集主机各项指标信息

3.2.2 索引存储层

索引存储层底层基于 Elastic Stack 技术栈中的 Elasticsearch 实现具体架设，Elasticsearch 是基于 Lucene 的全文搜索引擎，是 Elastic Stack 技术栈最核心的项目，它可以帮我们对数据进行快速的搜索及分析。Elasticsearch 是一个使用 Java 开发的开源搜索和分析引擎，其通过把底层 Lucene 封装起来，向外部提供 RESTful API 接口，使得数据的全文检索变得非常简便[20]。Elasticsearch 采用分布式数据存储，使得日志中的每个字段都可以被索引，可以处理同源异构的日志。

本文索引存储层 Elasticsearch 存储节点由 4 个独立节点构成分布式存储系统。企业网络环境中会产生海量数据，数据采集层探针采集到各类主机的数据后，通过 HTTPS 协议将数据传输至索引存储层，索引存储层按照不同主机类别创建索引文档，并在不同节点创建索引文档的分片和副本进行分布式存储。

3.2.3 事件分析层

事件分析层是整个网络高级威胁检测系统的核心业务层，建立在事件序列关联模型基础上，通过模型将索引存储层的数据进行安全事件实体化，从而进行事件间的序列关联，通过 Python 语言调用 EQL 查询语言编写实现事件分析层的相关功能。EQL（Event Query Language）全称“事件查询语言”，是一种用于基于事件的时间序列数据（如日志、指标和跟踪）的查询语言。EQL 提供了抽象，允许用户执行有状态的查询，识别事件序列，跟踪进程的父子关系，跨多个数据源的连接，并执行堆叠，Elasticsearch 搜索引擎从 v7 版本后均支持 EQL 进行查询[21]。

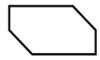
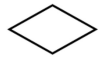
（1）事件序列关联模型

定义 1（模型定义） 事件序列关联模型是安全事件实体 O、操作关系 R 及关联检测规则 P 的集合，包括 3 个关键元素，可以定义为 $M=\{O,R,P\}$。

定义 2（事件关联图定义） 事件关联图定义为一张有向无环图 $G=(V,E)=(O,R)$，其中 V 是图中顶点的集合，与模型中安全事件实体集合 O 一一对应，表示网络中捕获到的安全事件；E 是图中边的集合，对应于模型中操作关系集合 R，用于描述安全事件间的关联关系。为了更直观清晰地展现事件关联图，表 3 列出了事件关联图的安全事件实体样式。

表 3 进程实体与其他实体间操作关系及其样式

Table 3 Relationships between process entities and other entities and their styles of operation

安全事件实体类型	进程对实体类型的操作关系	说明	样式
文件 File	pf_create pf_delete pf_read pf_write	进程创建文件 进程删除文件 进程读取文件 进程写入文件	
进程 Process	access create terminate	进程访问另一个进程 进程创建另一个进程 进程终止	
服务 Service	ps_create ps_delete ps_pause ps_start ps_stop	进程创建服务 进程删除服务 进程暂停服务 进程开启服务 进程停止服务	
网络 Network	pn_bind pn_listen pn_close	网络套接字绑定 进程开启网络监听 进程关闭网络监听	

其中，安全事件实体 O 表示网络中捕获的安全事件实体，包括进程（process）、文件（file）、服务（service）、网络（network）4 类实体类型，具体实体对象用符号 o 表示，即 $O\in\{o_1,\cdots,o_n\}$。操作关系 R 表示安全事件实体间的操作关系与相互作用，具体关系用符号 r 表示，即 $R\in\{r_1,\cdots,r_n\}$。

操作关系表示某个安全事件实体对另一个安全事件实体的操作，例如，一个进程实体创建了另一个进程实体、一个进程实体读取了一个文件实体，操作关系可以刻画不同安全事件实体间的交互关系，描述了主机使用者的操作行为。由于除进程实体外其他几类事件实体之间的相互依赖关系较弱，且无法形成有效关联，如文件实体无法创建服务实体，因此本模型选择进程实体对其进行串联[22-23]，定义进程与其他实体间的操作关系如表 3 所列。

关联检测规则 P 是描述攻击事件序列模式规律的先验知识集合，面对网络环境中可能发生的网络威胁，构建攻击事件序列关联检测规则库，每条规则由若干事件序列与关系构成。可以通过规则匹配从事件关联图中检测出攻击技术与上下文关联信息，为事件分析层的功能实现注入灵魂。

（1）场景案例

事件分析层业务基于事件序列关联模型，具体包括采用 EQL 语言对模型中的安全事件实体进行匹配过滤和检索查询，针对模型事件关联检测规则的配置管理以及操作权限控制等功能。下文通过几个有代表性的情景案例来直观说明事件分析层主要功能的实现方法。

案例 1 数据匹配过滤

针对简易数据匹配，可以满足网络安全分析人员进行特定的 IOC 检索需求，用于基础的 IOC 检索。下述代码进行字段的匹配操作，过滤掉无关信息，检索出 sha256 符合要求的事件并进行展示。

process where sha256==“080b7c2b705fbada3e05746e6fed52549d53a90367efd2da78c4a47c91087642”

对于网络安全分析人员来说，了解特定事件发生的所有事件是必要且有益的，通过控制时间窗口进行检索，下述命令

使用名为 any 的特殊事件类型，针对所有事件进行匹配，匹配出 2022 年 4 月 15 日 10 点至 2022 年 4 月 15 日 10 点 03 分这 3 分钟内发生的所有事件。

any where timestamp_utc >="2022-04-15 10:00:0Z" and timestamp_utc <="2022-04-15 10:03:0Z"

同时，事件分析层还可以实现类似于 unix 管道符的功能，需要说明的是，其可以根据特定需求进行多重管道处理，得到期望条件下的检索结果。下述代码包含两个管道处理，通过匹配过滤后便得到 2022 年 4 月 13 日之后最先出现的网络目的地址及端口号。

network whereevent_subtype_full=="connection_ _event"

| uniquedestination_address,destination_port

| filtertimestamp_utc >="2022-04-13"

案例 2　事件序列检索

在现实网络环境下很多行为并不具备原子性，而是跨越了多个事件，事件分析层利用 Sequence 结构定义了一系列有序事件。

sequence with maxspan=1h

[file where event_subtype_full=="file_create_event" and user_name!="SYSTEM"] by file_path

[process where user_name!="SYSTEM"] by process_path

[process where user_name=="SYSTEM"] by process_path

上述代码使用 Sequence 结构，将时间范围限制在一定范围内，结构中的每个 item 都由方括号[〈event query〉]之间的事件查询来描述，使用 by 关键字匹配值，检索出哪些文件是由非系统用户创建，并且先是作为非系统进程运行，后来又在一小时内作为系统级进程运行的。该功能可以对若干事件进行序列检索，进而描绘出特定行为的执行路径。

案例 3　威胁事件关联检测规则配置

针对网络威胁行为，事件分析层利用 ATT&CK 网络对抗行为知识库进行规则配置。需要说明的是本系统配置了 92 条基于 ATT&CK 框架的威胁搜寻和安全分析检测规则，在本案例中挑选 T1117 技术 Regsvr32 为例进行说明。

Regsvr32 为攻击者提供了一种简单而优雅的方式来执行本地代码或脚本，攻击者可以在本地存放资源或从远程位置加载它们。由于该技术利用了 Windows 平台的一个受信任的组件，不容易被禁用或限制，而且检测取决于对进程级遥测的密切检查，因而受到攻击者们的特别青睐和广泛使用[24]。由于它的衍生攻击载体允许通过 regsvr32 执行 VBScript 和 Jscript，因此这些脚本可以用来制作和执行有效载荷，而不需要调用本地的 wscript.exe 和 cscript.exe 处理程序，目前该技术仍然有效且常见。

根据 ATT&CK 网络对抗行为知识库对规则进行配置，利用事件检索是谁首先调用 regsvr32.exe 进程；再根据 CAR-2019-04-003：Squiblydoo 漏洞行为，检查是否存在恶意脚本的加载，即检查 regsvr32.exe 以后是否加载 scrobj.dll 库。在大部分情况下，攻击者往往使用恶意脚本连接到远程服务器或下载其他文件。综上，实质上是对一系列事件的序列检索，使用事件关联图表示如图 7 所示。

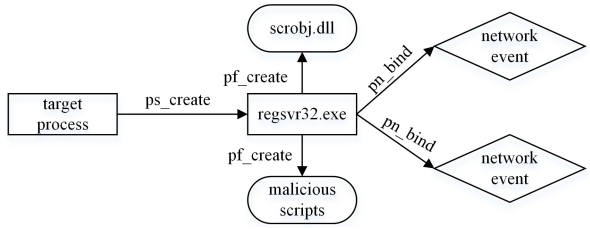


图 7　威胁事件关联图

Fig. 7　Threat event association diagram

在本例中事件为 regsvr32.exe 进程事件、scrobj.dll 库加载事件及同一过程中的所有网络事件，威胁事件关联检测规则如下：

sequence by process.pid

[process where process.name=="regsvr32.exe"]

[process where dll.name=="scrobj.dll"]

[network where true]

3.2.4　态势可视化层

态势可视化层主要实现对事件分析层输出结果的可视化，其基于 ATT&CK 攻击矩阵刻画网络威胁行为，将攻击者使用的技战术信息、攻击路径及进程可视化，呈现给网络安全分析人员。图 8 给出了 ATT&CK for Enterprise 的矩阵模型。

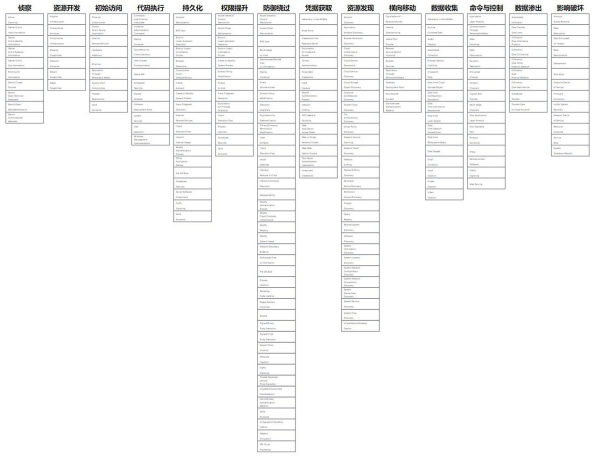


图 8　ATT&CK for Enterprise 攻击矩阵模型

Fig. 8　ATT&CK for Enterprise attack matrix model

态势可视化层可以清晰动态地呈现网络威胁行为，并提供一定的缓解措施建议，使得网络安全分析人员可以明晰此次网络威胁行为中对应的攻击手段、策略、目的。安全事件分析集群检测到攻击数据，并采取相应的防御措施，针对可能出现的下一步攻击行为进行预判，进而采取针对性的防护策略，能够有效降低攻击方的攻击效果，对网络攻击事件中的网安分析人员具有极大的实际意义。

4　实验分析

4.1　实验环境

本文基于 Openstack 超融合云平台模拟构建满足需求的网络实验环境，具有快速构建、复用等优势。实验场景由 3 部分组成：1）攻防网络环境；2）攻击机；3）安全事件分析集群。表 4 列出了场景中各部分虚拟机的具体信息。

表 4 实验场景中各部分虚拟机具体信息

Table 4 Specific information of each part of virtual machine in experimental scenario

场景名	虚拟机类型	数量/台	虚拟机配置
攻防网络环境	Ubuntu 20.04 LTS 64 bit	3	Intel © Core™ i3-7100 CPU @ 3.90 GHz×2 CPU, 8 GB 内存
	Microsoft Windows 7 64 bit	2	
攻击机	Kali Linux 64bit	1	
安全事件分析集群	Ubuntu 20.04 Server 64 bit	4	

4.2 实验方法

由于难以在现网中收集到 ATT&CK 框架所有技术对应的攻击日志数据，故本文采用 CALDERA 攻击工具实施攻击过程，模拟 APT 攻击行为。CALDERA[25] 是 MITRE 公司开源的一个网络安全框架，它建立在 ATT&CK 框架之上，能够实现自动化或手动对目标进行模拟攻击。CALDERA 主要由核心系统和插件两部分组成。

CALDERA 核心功能主要由界面中的 agents(远程控制探针部署)、adversaries(对手选择)、operations(选择对手后自动化攻击)模块提供，此外 CALDERA 提供了 19 个默认插件。

在实验中 CALDERA 被部署在 Kali Linux 虚拟机内作为攻击机，安全事件分析集群由 4 台 Ubuntu 20.04 Server 版组成，攻防网络环境由 3 台 Ubuntu 20.04 和 2 台 Windows 7 构成。实验在一定的良性行为的基础之上由攻击机对攻防网络环境进行渗透攻击，利用 CALDERA 实现基于 ATT&CK 框架的技战术攻击行为，同时，安全事件分析集群通过采集探针(Sysmon 和 Beats 组件)对网络环境存在的主机日志进行收集，通过配置的威胁搜寻和安全分析检测规则进行检索匹配，最终将结果呈现在可视化界面上。

4.3 实验测试及结果

根据前文的介绍可以明确目前 ATT&CK 框架有 180 多项技术、360 多项子技术，根据每年的各类网络安全报告和网络安全攻防经验，选择了攻击者最常使用的十大攻击技术(其中包括 4 项子技术)作为本文实验测试的攻击技术，具体技战术如表 5 所列。在实际网络攻防中，网络高级威胁行为并不一定要覆盖所有 ATT&CK 框架中的全部战术，专业的 APT 组织在绝大部分攻击中往往仅仅挑选特定的战术来实现战略意图，毕竟在网络攻防中利用越少的战术去实现目标是攻击者们一直追求的。本实验模拟的网络威胁行为包括 6 个战术步骤，涵盖了必要且常用的战术范围，具有很强的实战性，能够保证实验测试的有效性和可靠性。

表 5 实验测试攻击技战术表

Table 5 Experimental test attack technique and tactics

战术编号	战术名称	技术编号	技术名称
TA0002	执行	T1059	命令和脚本解析器
		T1059.001	PowerShell
		T1059.003	Windows Cmd Shell
TA0005	防御逃避	T1218	利用已签名二进制文件执行
		T1218.011	Rundll32
		T1218.005	Mshta
TA0003	持久化	T1543	创建或修改系统进程
TA0002	执行	T1053	计划任务
TA0006	凭证访问	T1003	操作系统凭证转储
TA0004	权限提升	T1055	进程注入
TA0005	防御逃避	T1027	混淆文件或信息
TA0011	命令与控制	T1105	入口工具转移
TA0002	执行	T1569	系统服务
TA0005	防御逃避	T1036	伪装

该系统的有效性主要依据检出率(Recall)和虚警率(False Alarm)来衡量[26]。检出率是成功识别攻击技术占数据中真实攻击技术总数的比例，虚警率是将正常行为判断为攻击行为的数量占算法检测出的攻击行为总数的比例。本文从这两个角度衡量语义规则的攻击行为检测能力。

实验中，对相同网络攻防环境分别进行 4 次上述攻击，图 9 给出了基于 ATT&CK 攻击矩阵的可视化界面，可以直观地感受攻击态势。实验结果显示，在该场景下检出率平均值为 96.43%，虚警率平均值为 7.35%，实验中 4 次攻击检出率和虚警率的情况如图 10 所示。

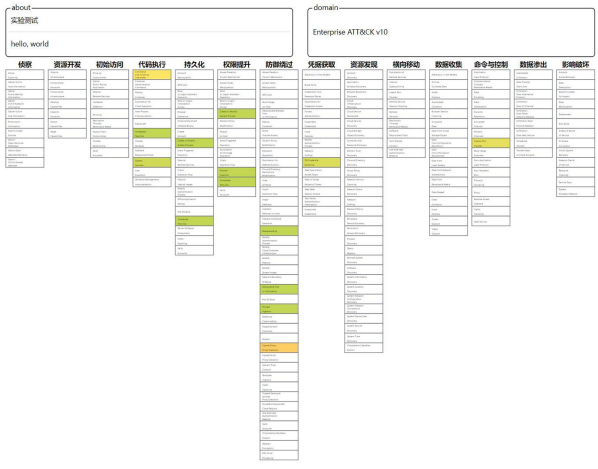


图 9 ATT&CK 攻击矩阵界面

Fig. 9 Visualization interface of ATT&CK attack matrix

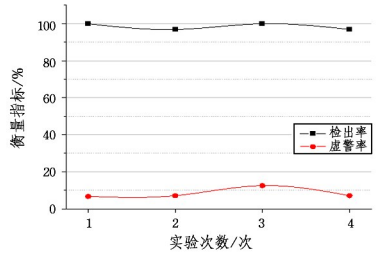


图 10 4 次攻击检出率和虚警率

Fig. 10 Quadruple attack detection rate and false alarm rate

实验中 4 次攻击下各战术的检出率和虚警率如图 11 所示，ATT&CK 中定义的某些技术是正常操作，但是在一定的事件序列下就会成为多步攻击的某一步骤，例如 PowerShell 和 Windows Cmd Shell 均是正常操作，但是在攻击执行过程中却是威胁行为。实验表明，本系统通过事件序列及上下文信息具体分析，将虚警率维持在较低水平，同时也保证了重要事件的饱和记录。

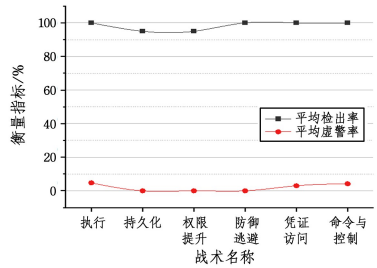


图 11 各战术的检出率和虚警率

Fig. 11 Detection rate and false alarm rate of each tactic

通过上述实验可以发现，本文设计实现的基于事件序列

关联模型的网络高级威胁检测无论是在检测结果呈现方式还是检测性能上都有很好的效果，分析其原因：一方面是采用 ATT&CK 框架作为攻击的统一描述，大大降低了描述攻击的语义沟通成本；另一方面系统采用事件序列关联模型建立了安全事件序列匹配规则库，其本质是基于先验知识的图匹配，因此检测效果很好。

结束语 在攻防世界中，网安分析人员往往会陷入“防守困境”中，降低网络高级威胁检测中针对多步攻击行为描述的语义沟通成本是亟待解决的关键问题。为此，本文在 ATT&CK 网络对抗行为框架下，设计实现了一套基于事件序列关联平台的网络高级威胁检测系统。本系统通过数据采集层实现对网络环境中的相关安全事件的实时收集，随后传输至索引存储层进行持久化存储，接着利用事件分析层基于事件序列关联模型实现事件序列的关联、检测、告警功能，最后通过态势可视化层基于 ATT&CK 攻击矩阵进行呈现。本文设计的 ATT&CK 框架下基于事件序列关联的网络高级威胁检测系统可以实现在技战术层面上对多步攻击行为的有效检测，能满足网安分析人员的分析需求，对分析人员解决“防守困境”具有很强的现实意义。

参 考 文 献

[1] 求是网. 牢固树立和践行总体国家安全观 谱写新时代国家安全新篇章[EB/OL]. (2022-04-15)[2022-04-20]. https://www.secrss.com/articles/41379.

[2] MITTAL S, JOSHI A, FININ T. Cyber-all-Intel: An AI for Security Related Threat Intellige[J]. arXiv: 1905.02895, 2019.

[3] TOUNSI W, RAIS H. A Survey on Technical Threat Intelligence in the Age of Sophisticated Cyber Attacks[J]. Computers & Security, 2018, 72: 212-233.

[4] 奇安信威胁情报中心. 全球高级持续性威胁(APT) 2021 年度报告[EB/OL]. (2022-03-25)[2022-04-20]. https://www.secrss.com/articles/40646.

[5] MANDIANT. IOC Editor User Guide [EB/OL]. https://www.fireeye.com/content/dam/fire eye-www/services/freeware/ug-ioc-editor.pdf.

[6] KUROGOME Y, OTSUKI Y, KAWAKOYA Y, et al. EIGER: Automated IOC Generation for Accurate and Interpretable Endpoint Malware Detection[C]// The 35th Annual Computer Security Applications Conference. 2019: 687-701.

[7] LIAO X J, YUAN K, WANG X F, et al. Acing the IOC Game: Toward Automatic Discovery and Analysis of Open-Source Cyber Threat Intelligence[C]// The 2016 ACM SIGSAC Conference on Computer and Communications Security. 2016: 755-766.

[8] BIANCO D. The pyramid of pain [EB/OL]. http://detect-respond.blogspot.com /2013/03/the-pyr amid-of-pain.html.

[9] CTI2020 Threat Connect [EB/OL]. https://threatconnect.com/wpcontent/uploads/Survey_CTI2020_ThreatConnect.pdf.

[10] ANDRESS J. Working with indicators of compromise[J]. Journal Information Systems Security Association (ISSA), 2015, 5: 14-20.

[11] BARNUM S. Standardizing cyber threat intelligence information with the Structured Threat Information eXpression (STIX)[J]. MITRE Corporation, 2012, 11: 1-22.

[12] Corporate Overview of The MITRE Corporation[EB/OL]. https://www.mitre.org /about/corpor ate-overview.

[13] STROM B E, APPLEBAUM A, MILLER D P, et al. Mitre att&ck: Design and philosophy[R]. Technical report, 2018.

[14] STROM B E, BATTAGLIA J A, KEMMERER M S, et al. Finding cyber threats with ATT&CK-based analytics[R]. Technical Report, The MITRE Corporation, 2017.

[15] OOSTHOEK K, DOERR C. SoK: ATT&CK Techniques and Trends in Windows Malware[C]// International Conference on Security and Privacy in Communication Systems. Cham: Springer, 2019: 406-425.

[16] Matrix Enterprise of MITRE ATT&CK [EB/OL]. https://attack.mitre.org/matrices/enterprise/.

[17] HE S G, YUAN Y, ZHU Z, et al. Domain threat detection based on ATT&CK framework[J]. Information Technology and Network Security, 2021, 40(12): 15-18, 25.

[18] Microsoft. Sysmon v13.24[EB/OL]. https://do cs.microsoft.com/en-us/sysi-nternals/downloads/sys mon. 2021.

[19] Official Website. Elasticsearch. org. [EB/OL]. [2014-02-04]. https://www.el-astic.co/elasticsearch/.

[20] WANG Y C. Design and implementation of a real-time log analysis system based on ELK Stack[D]. Beijing: Beijing University of Posts and Telecom munications, 2018.

[21] Elasticsearch Corporation. Elasticsesrch guide [EB/OL]. https://www.elastic.co/guide/en/elasticsearch/reference/current/index.html.

[22] HASSAN W U, GUO S, LI D, et al. Nodoze: Combatting threat alert fatigue with automated provenance triage[C]// Network and Dis tributed Systems Security Symposium. 2019.

[23] LIU Q, LI Y, DUAN H, et al. Knowledge Graph Construction Tech niques[J]. Journal of Computer Research and Development, 2016, 53(3): 582-600.

[24] Red Canary's Top MITRE ATT&CK Techniq ues: #3 Regsvr32 [EB/OL]. (2021-08-20)[2022-04-02]. https://redcanary.com/blog/3-technique-regsvr 32-t1117/.

[25] MITRE. CALDERA [EB/OL]. (2021-06)[2022-04-10]. https://hgithub.com/mitre/caldera.

[26] PAN Y F, ZHOU T Y, ZHU J H, et al. Semantic rule construction for APT attacks based on ATT&CK[J]. Journal of Information Security, 2021, 6(3): 77-90.

ZHANG Yuxiang, born in 1998, master. His main research interests include network and information security, cloud computing and big data security.

HAN Jiujiang, born in 1998, master. His main research interests include network and information security, cloud computing and big data security.