5GC 安全态势感知系统研究

刘亚天[1]，呼博文[1]，陈茂飞[2]，刘东鑫[2]
（1. 中国电信集团有限公司，北京 100033；
2. 中国电信股份有限公司研究院，广东 广州 510630）

摘　要：作为新一代移动通信的关键基础设施，5G 引入了新技术和新架构，同时也面临更复杂的安全风险和威胁。5GC 作为 5G 网络架构的关键部分，其安全需求一直是重要的研究课题。5GC 安全态势感知系统是应对 5G 安全挑战、助力高效安全运营 5G 网络的重要技术手段。首先介绍了安全态势感知的基本理念，分析了 5G 网络尤其是核心网的安全需求，并全面论述了 5GC 网络安全态势感知系统的设计，包括系统架构以及关键技术。

关键词：5G 核心网；5G 安全运营；网络安全态势感知
中图分类号：TP393
文献标志码：A
doi: 10.11959/j.issn.1000–0801.2022263

Study on the 5GC security situational awareness system

LIU Yatian[1], HU Bowen[1], CHEN Maofei[2], LIU Dongxin[2]
1. China Telecom Group Co., Ltd., Beijing 100033, China
2. Research Institute of China Telecom Co., Ltd., Guangzhou 510630, China

Abstract: As the key infrastructure for the next generation mobile network, 5G confronts more complex network security threats, targeting the new architecture and techniques that 5G evolves. Also as a key component of the 5G architecture, 5GC security has become an essential research topic. 5GC security situational awareness aims at understanding the current security situation and making tendency predictions in near future, which is an effective technique to counter network threats under 5G scenarios and enhance 5G operations more securely and effectively. The security situational awareness was firstly introduced, 5G particularly 5GC security demands were analyzed, then the detail design of 5GC security situational awareness system was addressed, including the system architecture and key techniques.

Key words: 5G core, 5G security operation, network security situational awareness

0　引言

Endsley[1-3]提出并完善了态势感知（situational awareness，SA）理论，强调对当下环境的认知和理解，并对发展的趋势进行预测。之后，Bass[4-5]将态势感知的理念引入安全领域，提出网络安全

收稿日期：2022−05−16；修回日期：2022−09−20

态势感知的概念。网络安全态势感知是对网络安全状态的一种持续认知过程，具体方法是通过融合各类原始数据，结合背景知识分析提取活动语义，进而整体性地理解网络当下所面临的各种威胁和风险，为安全决策提供支持[6-8]。网络安全态势感知弥补了传统安全防护各自为战、缺乏协同的不足，有效地提高了对安全事件分析和处置的能力，是网络安全监控技术进步的体现。

作为新一代移动通信网络，5G 引入的新技术和新特性同时也给安全运营带来新的挑战。运营商作为 5G 服务提供者，需要基于 5G 安全标准并结合自身安全运营的需求，更为完善地应对一系列安全问题。

（1）5G 安全标准对各个安全域的安全特性和过程进行了规范，运营商需要对单域内系统和模块的运行状态和面临的安全威胁整体进行监测；进一步地，在此基础上需要一个总体安全视图，对跨域跨层次的系统和模块进行统一安全监控。

（2）5G 网络架构演进带来的异构性和复杂性，攻击者可以从多个层面进行渗透攻击，单一维度的防护检测技术已经无法满足对针对性强、过程复杂的攻击活动分析的需要，因而要求一种能够整体上理解攻击意图、行为和后果的技术能力。

（3）5G 细粒度的运维要求和运维角色的多样化带来了配置错误的风险提升，而安全威胁、配置错误造成系统故障的影响范围更大，需要更高效的应急响应。

针对上述 5G 安全运营面临的挑战，本文提出应构建 5GC 安全态势感知系统，通过采集融合各类安全原始数据，对 5GC 网络安全态势进行整体理解和评估，快速分析溯源关键威胁，并联动协同响应处置，加快威胁识别、检测和处置闭环速度，提升安全运营效率，进一步提高 5G 网络安全运营的自动化和智能化水平。

1 5GC 安全态势感知需求

3GPP Release17 安全标准[9]对 5G 安全架构划分了接入、网络、用户、应用、基于服务的架构（service based architecture，SBA）和可视化与配置 6 个安全域。以安全态势感知系统的视角，如果获取上述各域的相关数据，能够实现相应域的安全态势感知。鉴于可能优先获取到的数据源，以及核心网在 5G 架构中起到的核心调度作用，下文着重探讨面向 5G 核心网（5G core，5GC）SBA 安全域的安全态势感知系统设计。其他域可以通过类似的架构和分析方法进行构建。

5GC 引入了云化技术实现对网元功能的解耦拆分，令其成为一个更灵活开放，并可持续动态拓展的网络架构，然而新架构也扩大了现有的攻击面，并引入了新的攻击面，5GC 安全态势需求如图 1 所

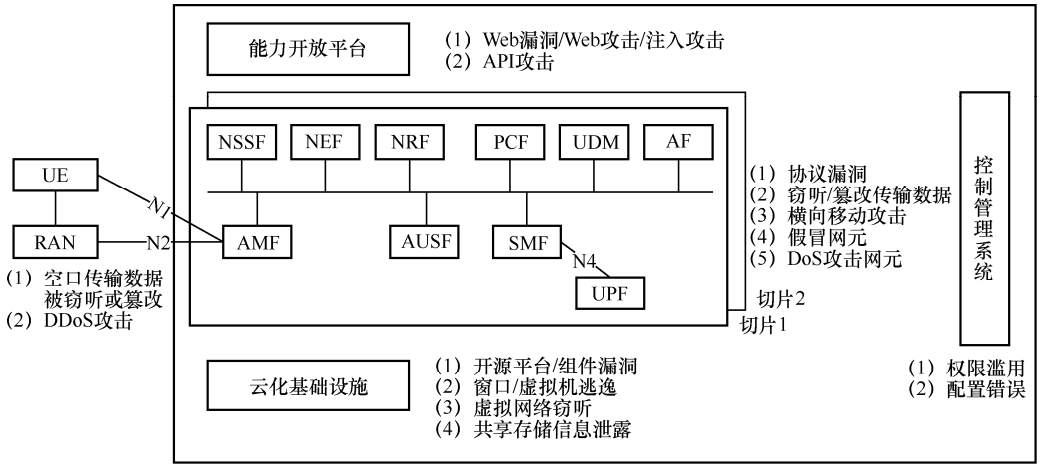


图 1 5GC 安全态势需求

示，5GC 接入侧、云化基础设施、网络平面、控制管理系统和能力开放平台都存在各自的安全风险。

（1）接入侧安全威胁

用户设备（user equipment，UE）/基站与 5GC 通信是通过接入和移动性管理功能（access and mobility management function，AMF），核心网和接入侧的接口包括 UE 的接口 N1、基站的接口 N2。通过空口传输的数据可能被窃听乃至篡改；基站与核心网的通信也面临和 IP 网络同样的安全威胁，例如攻击者可以通过海量被控制的终端对 5GC 接入侧发起分布式拒绝服务（distributed denied of service，DDoS）攻击，破坏 5GC 网元的可用性，影响甚至使 5GC 的正常服务瘫痪。

（2）云化基础设施威胁

核心网引入了云平台的技术，包括使用 x86 通用硬件平台替换了设备商自研专用平台，实现软硬件的解耦；网络功能虚拟化（network function virtualization，NFV）重构了传统的网络功能，虚拟网络功能（virtualized network function，VNF）实际部署在虚拟机甚至容器上。核心网的云化基础设施面临和云平台类似的安全威胁：针对大规模使用的开源平台/组件自身漏洞利用、虚拟机/容器逃逸可以对其他虚拟机甚至物理主机进行攻击以及共享物理存储数据隔离不完善导致的信息泄露等。

（3）网络安全威胁

5GC 的网络安全主要包括 VNF 之间控制面和数据面通信，以及统一对外服务接口通信流量等一系列网络平面安全。SBA 架构更加灵活高效的同时，也带来了新的安全风险。

- 虚拟网元之间的通信由超文本传输协议第二版（hypertext transport protocol 2.0，HTTP2）承载，其可能的漏洞会被攻击者利用以突破现有的安全机制。
- 攻击者渗透进入核心网后横向移动攻击，仿冒网元窃取通信数据，或者在网元中放置后门木马等。
- 随着开放网元数量的增长，由此带来了信令流量在数量和复杂度的急剧增加，诱发潜在产生信令风暴的风险。
- 由于分属不同切片的 VNF 共享了同一底层的物理/虚拟化资源，失陷的 VNF 可以利用漏洞突破隔离跨切片攻击其他 VNF。

（4）管理编排安全

5GC 主要使用网络功能虚拟化管理和编排（management orchestration & automation management，MANO）对更细粒度的服务化功能模块组件进行集中编排和管理，因此也面临新的安全威胁。

- 攻击者可以利用应用程序接口（application programming interface，API）服务的漏洞未经授权接入编排模块，并访问甚至修改其他网元服务。
- 如果未遵循恰当的访问模型，编排模块能够对超出其所需范围之外的对象进行操作，可能导致网元承载的控制和业务数据遭到泄露。
- 5G 细粒度的运维要求和运维角色的多样化意味着运维配置错误的风险提升，错误的配置可能导致 5G 网络遭受不必要的攻击。

（5）能力开放安全

5GC 提供网络服务和管理的开放功能，用户可以通过 API 方式灵活按需调用开放能力。网络能力开放接口采用互联网通用协议，会将互联网已有的安全风险引入 5GC，攻击者通过 API 对 5GC 进行渗透攻击成为新的高威胁攻击方式。

总体来看，5GC 架构演进带来了和原有移动通信网络不同的安全态势感知需求，主要体现在对于 5GC 网元和网络运行状态的实时监控、对各类攻击入侵行为的准确感知以及对安全趋势的及时预警。

2 5GC 安全态势感知系统设计

从数据层面来看，5GC 的安全态势感知系统，面临两大挑战：第一，由于连接海量终端，核心网内将产生大量信令数据交互，其自身也会产生海量的日志数据，数据规模增长速度快；第二，各类设备网元日趋复杂、数据来源广泛，包括信令数据、日志数据、配置数据以及部署的安全防护系统产生的告警信息等异构数据。传统的数据存储和分析架构在技术能力和成本方面都难以满足于对 5GC 安全态势感知的需要，同时基于大数据分析技术的安全态势感知系统被提出[10-11]。因此，本文认为 5GC 安全态势感知系统同样也需要采用大数据分析架构。5GC 安全态势感知系统架构如图 2 所示，系统总体分为数据源、数据采集与存储、5GC 安全分析以及 5GC 态势可视化 3 层架构。

2.1 数据采集与存储

（1）数据采集

5GC 安全态势感知系统的数据源主要分为以下几类。

- 网元数据：各网元产生的流量元数据、日志数据和策略配置数据等。
- 安全检测防护系统数据：5GC 部署的一系列安全检测防护系统，包括防火墙、入侵阻断系统（intrusion prevention system，IPS）和入侵检测系统（intrusion detection system，IDS）、全流量检测系统、蜜罐系统、Web 应用防火墙（Web application firewall，WAF）和主机/虚拟机安全探针等产生的日

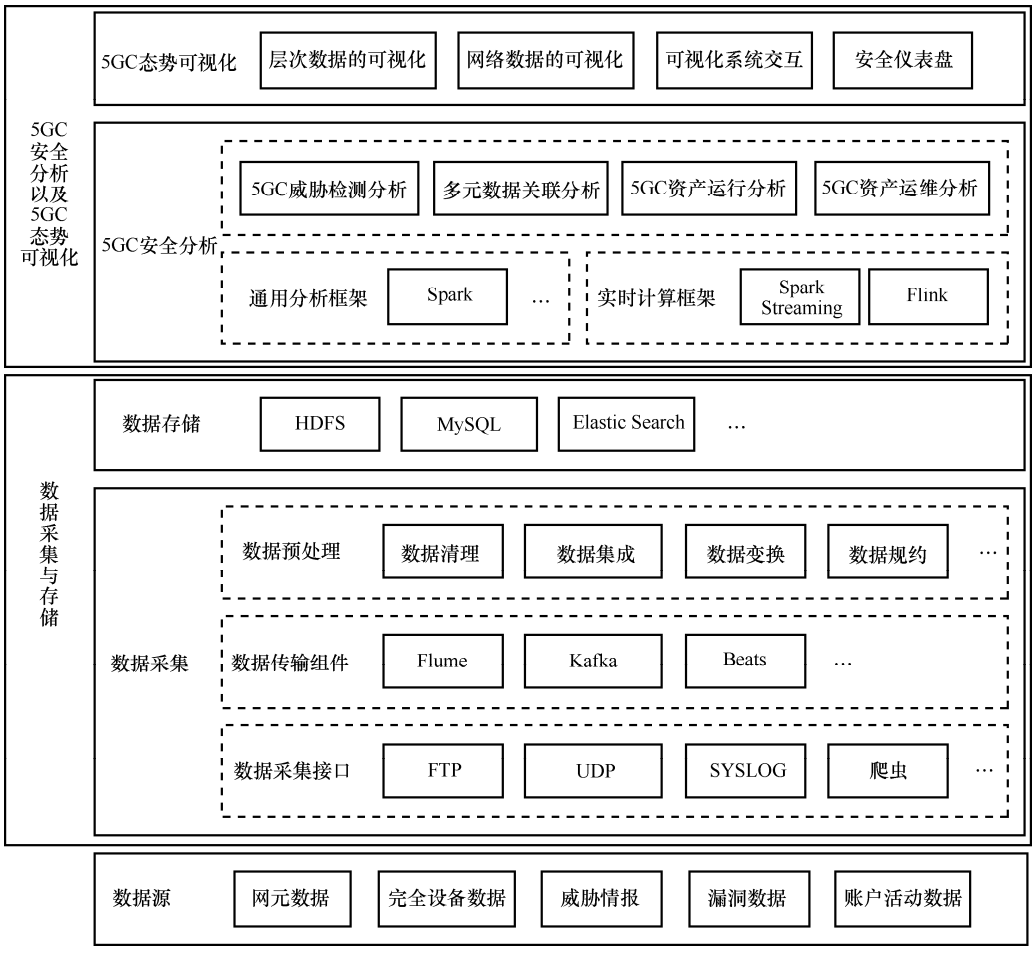


图 2 5GC 安全态势感知系统架构

志、流量数据和告警信息等。

- 漏洞数据：定期对 5GC 网元、虚拟机/物理机、安全设备等资产进行漏洞扫描产生的数据，包括操作系统、数据库、应用中间件是否存在已知可被利用的漏洞，漏洞是否已打补丁等。
- 账户活动数据：5GC 网元、网管及安全防护系统等都纳入统一安全管理系统（authentication、authorization、account 和 audit，4A 系统）进行管理，会产生相应的账户活动数据。
- 威胁情报：与安全威胁相关的情报信息，包括公开的漏洞和攻击手段等。

各网元、安全防护系统和网管系统等支持的传输协议不同，安全态势感知系统需要支持各类数据采集传输方式：第一，传统的文件日志传输协议，如 FTP/SFTP、SYSLOG 等；第二，流量数据通过 UDP 等协议传输；第三，大数据架构下采集传输的组件，如 Flume 和 Kafka 等；第四，网络爬虫可以爬取公开的威胁情报信息；第五，5GC NWDAF 网元实现为运营商管理的网络分析逻辑功能，可以对网络功能（network function，NF）提供分析信息，因此可以从 NWDAF 网元获取网元运行数据。

（2）数据预处理

由于数据来源不同、结构各异，采集的数据可能包含了大量缺失值或者异常值，以及同类型数据标准不统一，因此需要对采集的数据进行预处理，主要包括数据清洗和标准化。

- 数据清洗主要处理源数据中的遗漏数据、空缺值和异常值，删除冗余数据等。系统的各类数据源，如资产信息数据和威胁情报等都可能存在上述问题，需要有针对性地进行清洗。5GC 资产管理系统的日志信息、安全告警信息也可能产生冗余，需要进行去重和归并，降低数据规模，提升系统分析的效率。
- 数据标准化主要是由于不同厂商的系统设备的数据标准、格式等不完全一致，如网元日志数据和安全告警信息的标准不同。因此需要对同类型的数据源按照标准化格式统一进行适配，便于存储和后续分析。

（3）数据存储

数据存储设计需要考虑不同数据源对存储的要求不同，需要根据数据规模增长的速度和实时性等要求有针对性地加以存储，也要满足后续的计算分析乃至可视化的需要。总体来看，系统的数据存储主要包括以下 3 种类型。

- Hadoop 分布式文件系统（Hadoop distributed file system，HDFS）作为 Hadoop 开源生态平台的存储核心，通过横向扩展能够满足数据增量带来的动态扩展容量要求。系统多类原始数据，包括原始流量数据、日志和告警数据等都可以首先在 HDFS 存储，并作为之后提取分析的存储池。
- Elasticsearch 以倒排索引为核心，使存储、索引、搜索都变得更高效灵活。系统将原始的资产日志信息、安全事件告警信息和威胁情报等进行预处理之后存储入 Elasticsearch，便于进一步的安全分析。
- 将一些不经常性变化、比较规则的数据存入关系型数据库，例如网元资产信息数据、资产配置数据等。

2.2　5GC 安全态势

安全态势分析以 5GC 资产为核心，主要分为对资产活动状态的监测分析、对网络威胁的监测分析以及基于分析结果对当下 5GC 安全态势进行评估和预警，5GC 安全态势分析逻辑如图 3 所示。

2.2.1　5GC 资产运行监测

资产运行监测分析主要目的在于监测 5GC 资产（各网元、子系统/组件等）的活动情况，识别资产运行状态是否异常等。异常检测主要有基于

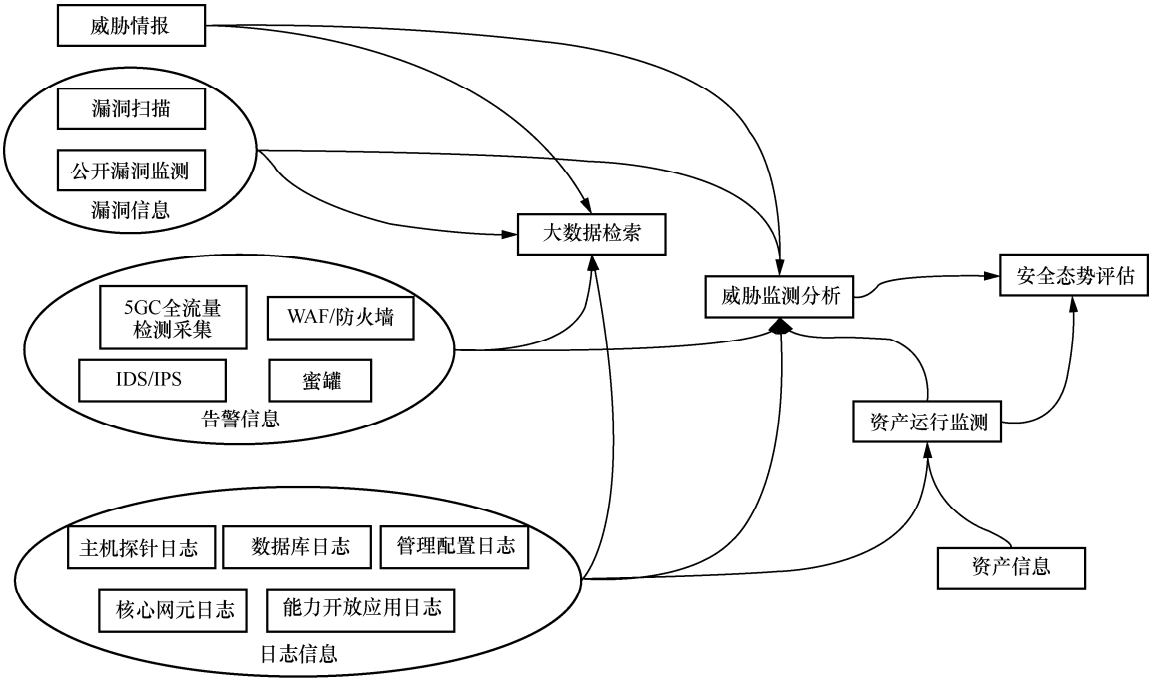


图 3　5GC 安全态势分析逻辑

统计模型和基于机器学习的方法[12-14]，结合 5GC 资产数据自身特点，本文使用构建动态基线和流量访问矩阵方法监测 5GC 资产活动。

（1）构建资产活动动态基线

通过对资产运行时生成的日志以及流量元数据等进行跟踪，构建资产运行基线。基线构建方法主要有设置固定阈值、基于统计和机器学习的方法[15-16]。固定阈值灵活性较差，基于统计值的方法不能很好地捕捉数据实时变化，本文使用基于机器学习的构建方法，并结合固定阈值，对 5GC 资产活动进行监测。构建主要分为 3 个步骤，包括通过模型训练生成模型库、基于模型生成动态基线以及结合固定阈值生成告警。5GC 资产动态基线如图 4 所示。

步骤 1　模型训练

动态基线实质上是一种对时间序列数据的挖掘分析，业界常用的方法有长短期记忆（long short-term memory，LSTM）、boosting 等。以 LSTM 为例，对原始数据预处理之后，首先构造训练数据：选择 7 天范围内的时序数据，考虑数据在相同时间段附近具有强相关性，使用 n（默认 30 min）时间窗口方法构造训练数据集。构造训练数据及见表 1，训练数据包括 D 日 T 时（min）的数据值作为目标值，以及 $D-1$ 日至 $D-7$ 日 $T-15$ 到 $T+15$

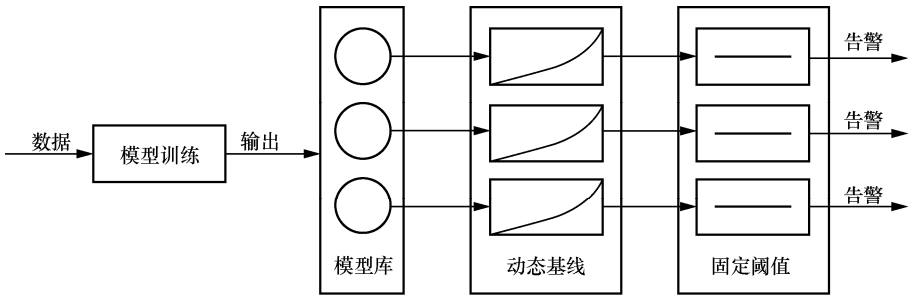


图 4　5GC 资产动态基线

表 1　构造训练数据集

日	*D*−7	*D*−6	*D*−5	*D*−4	*D*−3	*D*−2	*D*−1	*D*
分钟	*T*−15,*T*+15	*T*−15,*T*+15	*T*−15,*T*+15	*T*−15,*T*+15	*T*−15,*T*+15	*T*−15,*T*+15	*T*−15,*T*+15	*T*

时（min）的一共 211 维数据值。

针对监测对象的 1 440 min（每日），共有（211×1 440）训练数据集，以 LSTM 模型进行训练，并以均方根误差值（root mean square error，RMSE）进行验证，得到模型后输入模型库。

步骤 2　生成动态基线

每日循环使用 *D*−1 至 *D*−7 的历史数据，输入模型预测 *D* 日共 1 440 个时间点的值，形成动态基线保存到数据库，作为监测对象活动状态的基准。

步骤 3　结合阈值生成告警

在动态基线的基础上，可以根据具体的业务场景需求结合专家经验设置相应的阈值，如果基线数据值超过阈值则触发生成告警。

该方法能够较好地满足 5GC 复杂网络下各类对象监控的要求，并可以进一步优化，例如训练多个不同模型并择优输出[16]。

基于上述构建动态基线的方法，可以对 5GC 资产活动进行监测分析，基于动态基线分析 5GC 资产活动见表 2，包括不限于各网元、子系统/组件和承载基础设施等。

表 2　基于动态基线分析 5GC 资产活动

5GC 资产	监测对象	活动分析
网元	AMF	DDoS 攻击、信令风暴
	UPF	UPF 交互异常
	NEF	API 交互异常
子系统/组件	管理系统	用户活动异常
承载基础设施	云化基础设施	主机/虚拟机运行异常

- AMF 活动监测。对 AMF 数据构建基线以监测接入侧的活动情况：第一，对 AMF 相关消息统计频次构建基线，如初始注册消息（registration request）等，可以监测接入侧信令风暴和 UE/基站对核心网的信令 DDoS 攻击；第二，分析 UE 注册/去注册消息，建立 UE 注册基线模型，经过数据关联可以识别异常行为的 UE 终端。
- UPF 活动监测。5G 高速可靠数据传输在核心网层面均需通过用户面功能（user plane function，UPF）实现。UPF 通过 N4 接口与会话管理功能（session management function，SMF）通信，通过监测下沉边缘的 UPF 和在大区/省中心的 SMF 的消息交互，构建行为基线，能够监测异常交互。
- NEF 活动监测。对网络开放功能（network exposure function，NEF）API 的访问数据构建基线，可以监测 API 调用活动异常。
- 用户活动监测。5GC 网元、网管及安全系统都统一纳入 4A 系统管理。分析 4A 系统日志可以对用户的日常使用情况构建动态基线，监测用户活动异常，例如用户异常登录或者对账户的攻击（账号猜解和密码爆破等）。
- 云化基础设施活动监测。分析主机/虚拟机安全探针的日志数据并构建动态基线，监测主机/虚拟机的运行状态，包括物理/虚拟资源、网络流量、端口使用的异常等。

（2）建立网元访问控制矩阵

3GPP 标准定义了一系列参考点（reference point）作为两个不同功能体之间相互约定的访问接口。基于参考点梳理 5GC 网元访问控制矩阵，5GC 网元访问参考点见表 3，监测网元异常访问，对不在访问矩阵列出的访问流量触发告警，增强内部横向威胁的监测能力。

表 3　5GC 网元访问参考点

5GC 网元	AMF	AUSF	NEF	NRF	NSSF	NWDAF	PCF	SMF	UDM	UDR	UPF
AMF	N14	N12			N22		N15	N11	N8		
AUSF									N13		
NEF											
NRF											
NSSF						N24					
NWDAF							N23				
PCF								N7			
SMF								N16	N10		N4
UDM											
UDR											
UPF											N9

同时，由于灵活性和可拓展性，标准也定义了一系列服务化接口（service-based interface）实现网元之间的访问。通过监测网元服务化接口的调用情况，对不在访问矩阵的网元之间接口调用生成告警。

2.2.2　5GC 威胁监测

运营商在 5GC 部署了一系列安全防护系统，如通过在 5GC 网络部署全流量采集探针，5GC 全流量探针如图 5 所示，使用统一 DPI 方式将 5GC 内部网元间的流量送入全流量采集探针设备进行检测，生成的安全告警信息作为态势感知系统的数据源，安全态势分析融合相关数据进行关联分析。

文献[17]介绍了针对 5G 网络的安全渗透测试框架和方法，攻击者往往需要通过信息搜集（如社会工程、钓鱼邮件等）、漏洞利用获取权限、

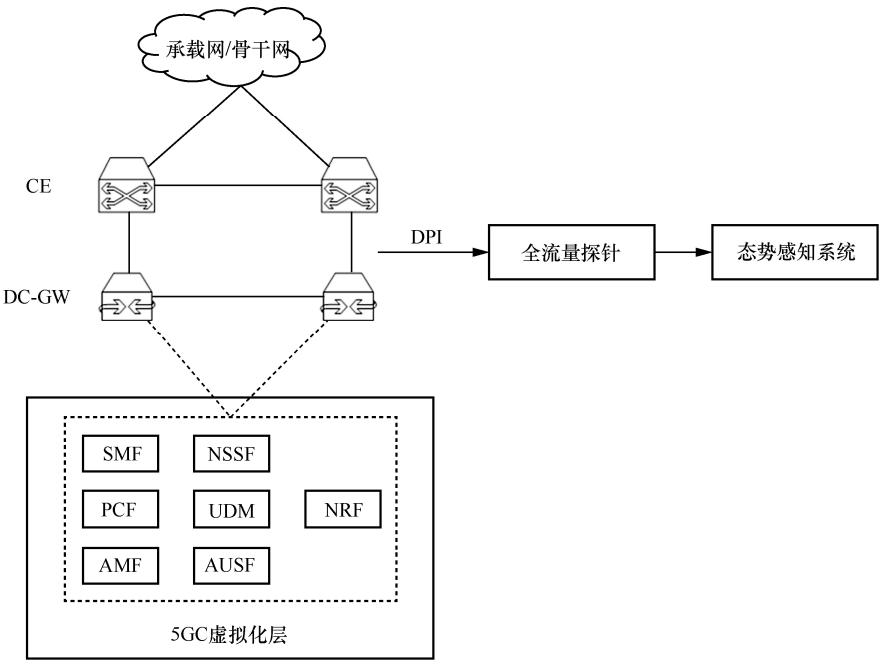


图 5　5GC 全流量探针

横向移动渗透、留置后门木马等一系列阶段实施入侵。由于攻击方式、时间先后等因素，单一维度的安全防护系统只能检测到部分的攻击特征，无法对整体攻击活动进行分析感知。5GC 威胁监测分析如图 6 所示，5GC 威胁监测分析主要融合分布在不同系统的安全数据，挖掘捕捉安全信息之间真实联系，尽可能地还原攻击链条，将分散的安全信息重构为一整体的攻击活动，进而从整体上理解高威胁的入侵行为。

（1）过滤冗余/误报告警信息

部署在 5GC 内的安全防护系统由于检测方法的局限，不可避免地会生成误报和其他冗余告警信息。海量冗余/误报安全告警信息分散了分析人员精力，让其难以关注真正有价值的安全威胁。5GC 安全态势感知系统面向安全运营并要产生预期的效用，首要过滤各种冗余/误报的安全告警，筛选真正有价值的安全告警。过滤本质上属于分类问题，主流是使用基于规则和机器学习模型的方法。

- 基于规则的多维特征过滤。安全告警信息通常包含多个特征维度的信息，主要包括：规则 ID、IP 端口四元组、攻击判定、攻击描述、攻击特征信息等。对于经分析后判定结果和攻击特征不符的误报告警，或者其他冗余告警，可以通过构造其相应特征信息的规则进行过滤。基于规则进行过滤的方法往往性能和准确率较高，不足在于需要根据数据变化持续对规则进行完善。
- 基于机器学习方法过滤。文献[18]通过对安全从业人员具体使用安全工具情况的调研，对安全工具生成大量误报告警信息进行了定性研究。文献[18]认为应该从可靠性、可解释性、分析信息和上下文关联等维度来提高机器学习模型的准确率，减少安全防护系统生成的误报告警。

（2）关联分析

关联分析是融合各类安全数据的关键技术，文献[19]讨论了关联分析的主流方法：基于相似度、基于序列和基于实例的方法。基于相似度的方法，主要通过算法计算告警信息的相似度，对相似度高的告警信息进行归并。该方法适用于分析单一攻击的告警信息，如扫描探测类等。基于序列的方法，主要包括基于时间序列、因果序列等，单一的时间序列并不能直接关联攻击行为，因果序列需要引入专家知识。基于实例的方法，通过学习攻击样例挖掘攻击模式，构造安全知识库，并通过模式关联告警信息。该方法基于专家知识分析准确度较高，不足之处在于难以分析未知的攻击行为。安全知识库包括主流的安全攻击框架（如 ATT&CK 和 Cyber Kill Chain 模型等），近年来安全知识图谱也不断地在业界中实践并推广[20]。以安全知识图谱方法对告警信息进行关联分析，主要可以分为构建 5GC 安全知识图谱和使用知识图谱进行关联两个部分。

- 构建 5GC 安全知识图谱。安全知识图谱对 5GC 安全数据进行预处理后，转化为<实

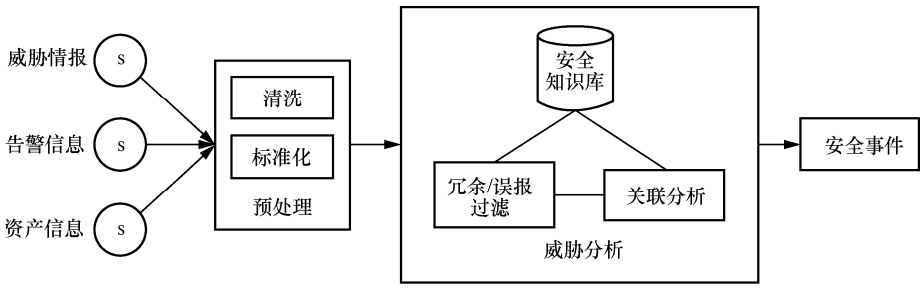


图 6　5GC 威胁监测分析

体，关系，实体>三元组的集合，实体之间通过关系相互联结构成网状的安全知识库，构建 5GC 安全知识图谱如图 7 所示，主要包括漏洞信息、攻击信息、资产信息以及这些信息之间的关系等。安全知识图谱中存储的是离散的三元组数据，每一个三元组数据代表一个单步攻击和导致单步攻击的因素之间的关系。多步攻击通常是以攻击链的形式发生的，可以看作多个单步攻击的组合，反映了攻击步骤之间的依赖关系。

- 基于知识图谱关联。经过预处理和过滤之后的告警信息，可以使用聚类算法对相似度高的告警进行聚合分析，经过聚合后告警信息标准化格式为<触发告警规则 ID、起始时间、源 IP 地址、源端口、目的 IP 地址、攻击判定结果、攻击描述、攻击特征>。基于知识图谱关联分析如图 8 所示，按照时间排序，并依据源/目的 IP 地址，将不同攻击目标产生的攻击信息与安全知识图谱匹配，命中返回对应的单步攻击。进一步地，如果采集数据的时间先后顺序复合攻击链的顺序一致，IP 的传播关系符合前一节点的目的 IP 地址和后一节点的源 IP 地址一致，则将告警信息对应的单步攻击关联起来，生成攻击图。

2.2.3 5GC 安全态势评估

对 5GC 资产进行监测分析，并需要结合分析生成的安全事件信息对事件进行综合评估，可以对事件信息按照威胁程度进行分类或者排序，优先输出高威胁的安全事件，供安全分析人员决策分析，乃至后续应急响应。对安全事件的评估可以采取定性和定量的方法。

- 定性的方法可以基于安全分析人员的专业

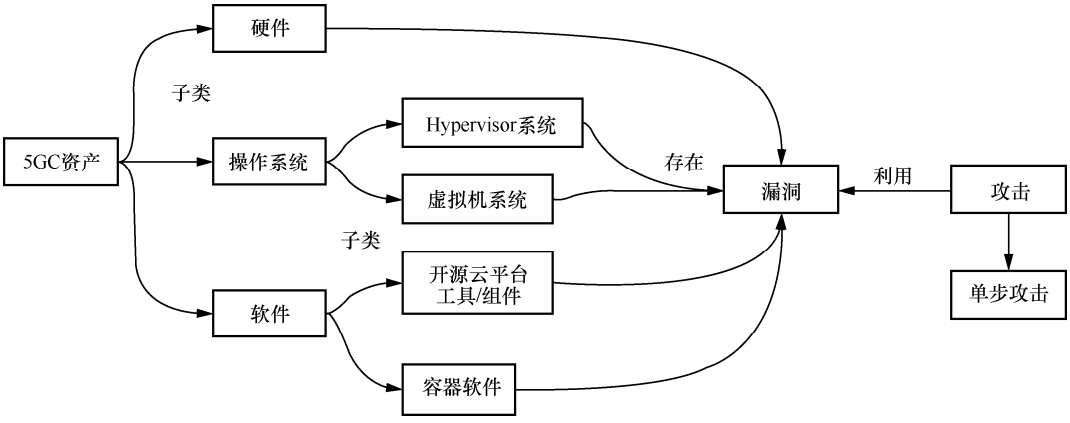


图 7 构建 5GC 安全知识图谱

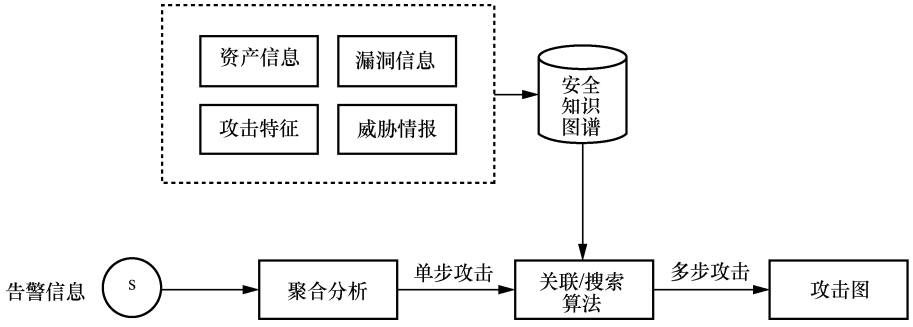


图 8 基于知识图谱关联分析

知识和经验，结合现有的普遍接受的分级方法，对安全事件的威胁程度按照攻击类型、频次或者资产重要性以及异常程度等信息进行定级分析，通常输出高危、中危和低危 3 类事件。

- 定量的方法可以通过构建面向资产威胁和资产自身运行情况的安全指标，根据安全事件发生的等级、频次以及资产运行异常等级等信息，采用统计或者机器学习的方法计算相应指标值，并按照由高到低的方式输出。

2.3　5GC 安全态势可视化

安全态势可视化的目标是真实性和关联性。真实性要求准确还原数据表达出来的安全态势环境；关联性要求通过可视化提供的信息，协助安全决策者建立不同片段关联关系，了解过去、认识现在以及预测将来。

对于不同类型的安全态势数据信息，其可视化形式也不尽相同。层次化数据可视化需要对数据层次关系进行有效刻画，可采取树状结构，使用节点间链接、空间填充或混合方法等形式进行。网络型数据结构非线性关系数据的可视化表达，可采取图结构，需要注重网络布局、网络属性可视化以及用户交互，常用节点链接法、相邻矩阵法或混合方法展现。

同时，安全态势可视化系统还必须关注用户交互性。通过用户与系统的人机交互，可在有限的可视化空间载入和展示更加丰富的数据，让用户得到自己需要的数据理解和分析，更有效地协助支持安全决策。常见的交互方式按粒度从细到粗有观察点交互、图形元素交互、图形结构交互等，其交互目的需要考虑用于增强、探索和启发态势数据对用户的作用。

2.4　应用实践

基于上述研究，本文开发了一套 5GC 态势感知系统，并在现网进行了试点验证。这套系统采集了核心网各个网元的流量元数据、日志数据和账户活动数据，以及安全检测防护系统例如防火墙的告警信息等多种异构数据源。根据第 2.2 节提到的分析方法，对 5GC 的安全态势进行了实时分析和监测。

- 通过梳理网元 IP 地址、组件版本、访问端口、合法访问控制策略等信息，对网元活动构建动态基线和访问控制矩阵，并根据现网实时数据不断调整直至稳定。系统有效发现了多个网元基线合规的安全风险，包括有系统和网元没有接入 4A 系统，设备间使用信任关系跳转登录，部分内部网元可以通过 SSH 信任关系进行免密登录，有系统内部终端保存了所辖系统的登录方式和用户密码，安全风险极高。
- 同时，对接入的安全告警日志进行误报过滤，事件过滤比超过 90%；并对特定攻击场景的告警日志进行关联、聚合，能够将千余条甚至万余条告警日志汇聚输出为 10 余条高价值的安全事件，压降比超过 100∶1，有效提升安全人员排查安全风险的效率。

5GC 安全态势感知系统弥补了原有 5GC 安全可观测性的不足，并增强了对安全威胁分析和感知的能力，有效提高了一线安全人员发现、排查和处置安全风险的效率。

3　结束语

与一般的安全态势感知系统相比，5GC 态势感知系统的独特性体现在对 5G 网络特有流量，例如信令面流量的威胁检测，以及对 5GC 网元的持续安全监控，进而能够与其他安全检测防护系统联动，打造 5GC 网络安全运营识别、保护、检测和响应的高效闭环。

值得注意的是，在全球数字化变革浪潮中，运营商由于业务系统繁多，参与安全建设的厂商

众多，安全能力之间容易出现冗余并呈现“孤岛”效应。因此，近年来部分运营商持续推进以安全中台为核心的安全体系建设，可以整合安全数据与能力，提升安全运营效率，打造架构统一、生态开放的云网端安全能力体系。在此背景下，5GC 态势感知系统如何融入这一安全体系的建设中，也是值得探索和研究的课题，例如，5GC 安全态势感知的数据源可以直接应用来自安全中台的安全大数据，相关的安全态势分析功能也可以基于安全中台的计算分析引擎实现。总体来看，5GC 安全态势感知系统架构和关键技术方案仍有待在实践中不断提高和完善。

参考文献：

[1] ENDSLEY M R. Design and evaluation for situation awareness enhancement[J]. Proceedings of the Human Factors Society Annual Meeting, 1988, 32(2): 97-101.

[2] ENDSLEY M R. Toward a theory of situation awareness in dynamic systems[J]. Human Factors: the Journal of the Human Factors and Ergonomics Society, 1995 37(1): 32-64.

[3] ENDSLEY M R. Measurement of situation awareness in dynamic systems[J]. Human Factors: the Journal of the Human Factors and Ergonomics Society, 1995 37(1): 65-84.

[4] BASS T. Multisensor data fusion for next generation distributed intrusion detection systems[C]//Proceedings of the IRIS National Symposium on Sensor and Data Fusion. 1999: 24-27.

[5] BASS T. Intrusion detection systems and multisensor data fusion[J]. Communications of the ACM, 2000, 43(4): 99-105.

[6] 席荣荣，云晓春，金舒原，等. 网络安全态势感知研究综述[J]. 计算机应用, 2012, 32(1): 1-4, 59.
XI R R, YUN X C, JIN S Y, et al. Research survey of network security situation awareness[J]. Journal of Computer Applications, 2012, 32(1): 1-4, 59.

[7] 龚俭，臧小东，苏琪，等. 网络安全态势感知综述[J]. 软件学报, 2017, 28(4): 1010-1026.
GONG J, ZANG X D, SU Q, et al. Survey of network security situation awareness[J]. Journal of Software, 2017, 28(4): 1010-1026.

[8] 石乐义，刘佳，刘祎豪，等. 网络安全态势感知研究综述[J]. 计算机工程与应用, 2019, 55(24): 1-9.
SHI L Y, LIU J, LIU Y H, et al. Survey of research on network security situation awareness[J]. Computer Engineering and Applications, 2019, 55(24): 1-9

[9] 3GPP. Security architecture and procedures for 5G system: TS 33.501 R17[S]. 2021.

[10] 管磊，胡光俊，王专. 基于大数据的网络安全态势感知技术研究[J]. 信息网络安全, 2016(9): 45-50.
GUAN L, HU G J, WANG Z. Research on network security situational awareness technology based on big data[J]. Netinfo Security, 2016(9) : 45-50

[11] 琚安康，郭渊博，朱泰铭. 基于开源工具集的大数据网络安全态势感知及预警架构[J]. 计算机科学，2017，44(5): 125-131.
JU A K, GUO Y B, ZHU T M. Framework for big data network security situational awareness and threat warning based on open source toolset[J]. Computer Science, 2017, 44(5): 125-131.

[12] 卿斯汉，蒋建春，马恒太，等. 入侵检测技术研究综述[J]. 通信学报, 2004, 25(7): 19-29.
QING S H, JIANG J C, MA H T, et. al. Research on intrusion detection techniques: a survey[J]. Journal of China Institute of Communications, 2004, 25(7): 19-29

[13] 张蕾，崔勇，刘静，等. 机器学习在网络空间安全研究中的应用[J]. 计算机学报, 2018, 41(9): 1943-1975.
ZHANG L, CUI Y, LIU J, et al. Application of machine learning in cyberspace security research[J]. Chinese Journal of Computers, 2018, 41(9): 1943-1975

[14] 卓琳，赵厚宇，詹思延. 异常检测方法及其应用综述[J]. 计算机应用研究, 2020, 37(S1): 9-15.
ZHUO L, ZHAO H Y, ZHAN S Y. Overview of anomaly detection methods and applications[J]. Application Research of Computers, 2020, 37(S1): 9-15.

[15] 桂永宏. 业务系统安全基线的研究及应用[J]. 计算机安全, 2011(10): 23-27.
GUI Y H, Study and applications of operation system security baseline[J]. Computer Security, 2011(10): 23-27

[16] 马玉超. 基于机器学习的动态基线性能时序数据异常检测研究与应用[J]. 中国金融电脑, 2020(6): 51-59.
MA Y C. Research and application of anomaly detection for performance time-sequence data by dynamic baseline based on machine learning[J]. Financial Computer of China, 2020(6): 51-59.

[17] 解晓青，余晓光，余滢鑫，等. 5G 网络安全渗透测试框架和方法[J]. 信息安全研究, 2021, 7(9): 795-801.
XIE X Q, YU X G, YU Y X, et al. Penetration test framework and method of 5G cyber security[J]. Journal of Information Security Research, 2021, 7(9): 795-801.

[18] ALAHMADI B A, AXON L, MARTINOVIC I. 99% false positives: a qualitative study of SOC analysts' perspectives on

security alarms[C]//Proceedings of the 31st USENIX Security Symposium (USENIX Security). 2022:10-12

[19] 琚安康, 郭渊博, 朱泰铭, 等. 网络安全事件关联分析技术与工具研究[J]. 计算机科学, 2017, 44(2): 38-45.
JU A K, GUO Y B, ZHU T M, et al. Survey on network security event correlation analysis methods and tools[J]. Computer Science, 2017, 44(2): 38-45.

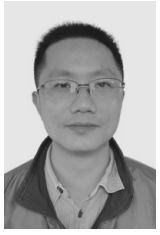
[20] 贾焰, 亓玉璐, 尚怀军, 等. 一种构建网络安全知识图谱的实用方法[J]. Engineering, 2018, 4(1): 117-133.
JIA Y, QI Y L, SHANG H J, et al. A practical approach to constructing a knowledge graph for cybersecurity[J]. Engineering, 2018, 4(1): 117-133.

[作者简介]

刘亚天（1974− ），男，中国电信集团有限公司网络和信息安全管理部网安处处长，主要研究方向为安全能力框架和规划、建设、应用等。

呼博文（1984− ），男，现就职于中国电信集团有限公司网络和信息安全管理部，主要研究方向为安全中台规划、建设、应用以及5G 网络安全架构等。

陈茂飞（1986− ），男，中国电信股份有限公司研究院工程师，主要研究方向为网络安全、程序分析。



刘东鑫（1985− ），男，中国电信股份有限公司研究院工程师，主要研究方向为网络安全、大数据安全。