电力数据中台安全自动化响应方案研究

周小明[1],齐 俊[2,3],王 磊[1],罗 晨[4],郑福宇[5],张文杰[2]
(1. 国网辽宁省电力有限公司,辽宁 沈阳 110004;
2. 国网辽宁省电力有限公司 信息通信分公司,辽宁 沈阳 110006;
3. 沈阳工业大学 电气工程学院,辽宁 沈阳 110870;
4. 中国电力科学研究院有限公司/电力网络安全防护与监测技术实验室,江苏 南京 210000;
5. 北京邮电大学,北京 100876)

摘 要:电力数据中台包含了涉及国家安全与民生安全的数据,需要在识别到异常后及时响应并得到有效处理。电力数据中台现有的响应流程是多人、多系统、多界面的,在异常处理效率与自动化程度上均有待提升。针对需要协同处置的安全任务场景,安全编排自动化与响应(SOAR)技术是一种解决方案。当前SOAR技术在云平台、医疗、物联网等应用场景有较多实际应用,相关产品较为成熟。然而当前对于SOAR技术的研究与应用未结合电力数据中台异常源多、异常种类多、异常之间关联关系复杂的特点。该文基于SOAR技术与电力数据中台的特点,提出了一种针对电力数据中台的安全自动化响应方案,旨在结合异常间的关联性,对所有异常进行标准化、统一化处理。该方案抽象化描述了数据中台异常的处理流程,提出了标准化的电力数据防护流程,依此设计了系统架构,并与现有响应方案进行了对比。实验表明该安全自动化响应方案在及时性、准确性、灵活性上均有提升。这证明该方案能够提升安全防护系统的处理效率,为电力数据中台及时响应并自动化处理异常提供了解决方案。

关键词:电力数据中台;安全编排自动化与响应;自动化响应;安全防护;脚本编排
中图分类号:TP273+.5 **文献标识码**:A **文章编号**:1673-629X(2025)07-0032-09
doi:10.20165/j.cnki.ISSN1673-629X.2025.0050

Research on Security Orchestration Automation and Response System for Power Data Center

ZHOU Xiao-ming[1], QI Jun[2,3], WANG Lei[1], LUO Chen[4], ZHENG Fu-yu[5], ZHANG Wen-jie[2]
(1. State Grid Liaoning Electric Power Supply Company Limited, Shenyang 110004, China;
2. Information & Telecommunication Branch, State Grid Liaoning Electric Power Supply Co., Ltd., Shenyang 110006, China;
3. School of Electrical Engineering, Shenyang University of Technology, Shenyang 110870, China;
4. State Grid Laboratory of Power Cyber-security Protection and Monitoring Technology, China Electric Power Research Institute, Nanjing 210000, China;
5. Beijing University of Posts and Telecommunications, Beijing 100876, China)

Abstract: The power data center contains data related to national security and people's safety, and needs to respond to anomalies in a timely manner and be handled effectively after they are recognized. The existing response process of power data center is multi-person, multi-system, and multi-interface, which needs to be improved in terms of abnormality handling efficiency and automation. For this type of security task scenario that requires collaborative handling, security orchestration automation and response (SOAR) technology is a solution. Currently, SOAR technology has more practical applications in cloud platforms, healthcare, IoT and other application scenarios, and related products are more mature. However, the current research and application of SOAR technology has not taken into account the characteristics of multiple anomaly sources, multiple anomaly types, and complex correlation between anomalies in power data. Based on the SOAR technology and the characteristics of power data center, we propose a security automation response scheme for power data

收稿日期:2024-11-22 **修回日期**:2025-03-26
基金项目:国家电网公司总部科技项目(5700-202328293A-1-1-ZN)
作者简介:周小明(1978-),男,博士,教授级高级工程师,研究方向为数字化、网络安全、数据安全;通讯作者:郑福宇(2001-),男,硕士研究生,研究方向为数字化、电力信息安全。

center, which aims to standardize and unify all the anomalies by combining the correlation between the anomalies. The scheme abstractly describes the processing flow of anomalies in the data center, proposes a standardized power data protection process, designs the system architecture accordingly, and compares it with the existing response methods. Experiments show that the proposed security automation response scheme improves in timeliness, accuracy, and flexibility. It is proved that this scheme can improve the processing efficiency of the security protection system, and provides a solution for the power data center to respond to and automate the abnormalities in a timely manner.

Key words: power data center; security orchestration automation and response; automated response; security protection; scripting

0　引　言

近年来,能源电力企业着重通过数字化方式推动电网智能化升级和企业数字化转型[1],企业与用户的数据大规模进入电力数据中台,其中不乏企业与用户的敏感数据。《数据安全治理白皮书 5.0—电力数据安全治理实践》[2]指出电力数据被窃取、破坏的安全事件仍频繁发生,而电力数据中台中的敏感数据若遭窃取和破坏,轻则导致用户隐私泄露、身份盗窃,重则导致国家能源战略泄露,甚至导致军事行动泄密,严重危害国家安全[3-4]。因此需要加强电力数据中台的安全防护策略,提升电力数据中台自动化响应效率,保障电力数据中台的安全。

当前,电力数据中台的异常检测与处理方法众多。然而,独立的异常检测与处理单元存在诸多弊端,包括标准化程度低、更新维护困难,且缺乏整体视角下的综合分析。因而需要将异常及其处理方法整合到一个具备综合处理能力的技术框架中才能提升异常的处理效率。

SOAR (Security Orchestration, Automation and Response,安全编排自动化与响应)是一系列技术的合集,它能够帮助企业和组织收集安全运维团队监控到的各种信息,并对这些信息进行事件分析和告警分类,然后在剧本的指引下,利用人机结合的方式帮助安全运维人员定义、排序和触发标准化的事件响应活动[5]。文献[6-7]针对现有安全方面面临的挑战,提出了 SOAR 技术,并通过相关应用实践说明了 SOAR 可能存在的价值。在电力数据中台中,异常来源众多,人员维护复杂且易遗漏,因而需要 SOAR 技术为其组织、收集安全信息。

现有的 SOAR 技术包括 TheHive、Cortex XSOAR、Chronicle SOAR 和 Shuffle[8]。在“阿里云-云安全中心-威胁分析与响应”[9]中存在 SOAR 防护策略与云产品结合的实例。“威胁分析与响应”模块通过关注主机日志、网络层数据以及云产品数据,结合 SOAR 技术实现了云防火墙、API 网关防护等操作的编排与自动化响应。文献[10]以阿里云工程师的常见处理流程为例,论述了自动化编排技术能够缩短应急事件的处理周期,阐述了 SOAR 的实战意义。文献[11]在现有蜜罐解决方案无法保证网络安全的背景下结合 SOAR 引擎,根据攻击者行为动态部署蜜罐,有效吸引攻击者,增加其停留时间。文献[12]主要介绍了一种用于部署行为蜜罐的 SOAR 引擎,以解决面对新型攻击、零日攻击及内部威胁时现有安全工具和技术存在的局限性问题。文献[13]使用 SOAR 平台整合了安全功能,安全事件的检测、分析、响应等环节可以在 SOAR 平台上连贯进行,提升了安全运营效率。文献[14]将 SOAR 技术应用在气象信息化网络安全防护中,减轻网络安全运维过程中繁琐的处置步骤,提升处置效率,让网络检测、告警、处置更加有效。文献[15]中使用 SOAR 收集企业内所有安全设备的威胁告警数据,结合内部工作流驱动标准化的安全事件响应活动,提升了清除安全威胁的效率。文献[16]提出将 SOAR 组件引入 5G MEC,实现了威胁情报收集、安全事件响应编排和执行自动化,所设计的方案可以依据剧本快速灵活部署,反应时间短,可有效抵御常见攻击。在物联网领域,文献[17]以物联网为背景给出了 SOAR 技术在该场景下的整体架构,设计了安全事件的标准处理流程,实现了高效智能编排。文献[18]分析大规模物联网、超连接网络环境,用相关数据指出安全事件发生的频率以及检测、分析和应对安全事件所需的时间都在增加,需要借助 SOAR 技术帮助员工根据标准化工作流程应对高级安全威胁。在医疗领域,文献[19]聚焦于“互联网+医疗”的场景,分析了当前医院网络安全的常见问题,实现了 SOAR 技术在福建中医药大学附属人民医院的实际应用,显著缩短了问题出现后的系统响应时间。

这些 SOAR 的应用实例说明安全编排与自动化响应在统一编排处理方面的有效性。电力数据中台系统同气象信息化网络、物联网等领域存在诸多共性,具体表现为均需处理海量异常信息、面临繁杂的异常种类,且处理过程呈现出“多人、多系统、多界面”的特点。因而选用 SOAR 方法对电力数据中台的异常进行自动化处理。

在电力领域中,鲜有将 SOAR 应用至实际系统的相关研究。文献[20]关注了新型电力系统中 SOAR 方法的应用现状,针对新型电力系统面临的 APT 攻击进行了研究。该文章侧重于如何及时发现潜在的 APT 攻击迹象并为之后的机器学习提供良好数据。

该方法只能针对电力数据中台的 APT 异常进行识别并处理。对于现有电力数据中台异常来源与种类多、关联关系复杂的特点,该方案无法高效处理。

综上所述,SOAR 技术在不同领域的安全运维场景下有着广泛应用,能够有效地对安全威胁进行及时响应与有效处理。但针对电力数据中台,现有 SOAR 技术未能结合电力数据中台异常的数据特点,不能直接将其他成熟使用的 SOAR 系统迁移至电力数据中台。

基于已有研究,该文做出的主要贡献如下:

(1)针对电力数据中台异常发生的类型特点、数量特点,基于 SOAR 技术,设计了电力数据中台的安全自动化响应方案。

(2)给出详细的实体定义方式与系统设计方案,提供了标准化的电力数据防护流程,为电力数据中台安全自动化响应方案的实现提供了参考。

1 概念引入

结合 SOAR 技术与电力数据中台的运行场景,该方案引入一系列关键概念来构建安全防护体系,其中异常、安全事件、告警、案件、案件类型和剧本是核心实体。本节针对实体定义的必要性进行说明。

(1)异常。

异常实体的引入旨在汇聚电力数据中台不同系统的异常情况,将其转化为规格化输入,从而提高整个安全防护体系对异常情况的识别和处理效率。

(2)安全事件。

安全事件特指与电力系统的网络、数据或基础设施安全相关的威胁或攻击行为。安全事件的产生表示可能发生了较为严重的问题,需要运维人员着重关注这些问题并及时处理。

(3)告警。

告警实体的作用是向相关运维人员发出通知,明确告知运维人员系统可能存在的问题类型,促使运维人员及时应对可能出现的安全威胁。

(4)案件。

案件实体能够将一组相关的告警进行流程化、持续化的调查分析与响应处置。若没有案件实体,告警将呈零散状态,无法有效整合与关联。例如,当电力数据中台遭受复杂攻击时,可能产生多个涉及不同告警类型、设备和时间范围的告警。若无案件实体聚合这些告警,运维人员将难以从整体上把握安全事件全貌,易遗漏关键信息,导致对异常或安全事件的处理出现偏差。

(5)案件类型。

案件类型实体在电力数据中台安全防护体系中具有特殊性,它不仅是案件实体的一个字段,独立定义还可优化剧本选择逻辑,为同类案件处理提供更多途径。单独定义的必要性在于:一方面,它能针对某类案件定义独立于具体案件的处理逻辑,通过抽象归纳共性特征,增强系统对未知案件的适应性;另一方面,系统依据案件类型匹配剧本,一个剧本对应一类案件的处理方案,而非某个具体案件的处理方式。

(6)剧本。

剧本实体的引入源于电力数据中台面临的复杂异常事件众多,需统一规范处理流程。剧本实体明确规定了处理过程的具体步骤与动作顺序,以此确保不同人员在处理相同类型的数据中台异常时遵循一致流程,进而提升处理的准确性与效率。

(7)动作。

动作实体的引入能满足多样化的安全防护需求,避免重复开发。动作作为可在防护软件上执行的具体操作,可根据实际安全需求和业务场景灵活组合,构建应对各类安全事件的处理流程,有效保障系统安全。

2 安全自动化响应方案设计

电力数据中台存储着大量敏感数据集,且配备众多服务接口。若调用不当或权限分配失误,极有可能导致严重且难以估量的后果。这些服务接口也是恶意程序实施攻击进而获取敏感数据的最便捷途径。因此,一旦遇到异常情况,就需要运维人员迅速做出响应并加以处理。针对这一处理流程,本研究提出了一套自动化响应方案。

2.1 处理方案流程设计

该文设计的处理方案流程如图 1 所示。方案提出的电力数据中台处理流程通过增加实体与相应的映射方式,最终实现了数据中台异常的自动化处理。

处理方案的输入为数据中台中检测到的异常,其数据将被持久化存储于数据库中。

输入到电力数据中台的异常并非均与安全行为相关。而对于安全事件则需要引起运维人员的特别关注,及时处理,因而需要进行“安全事件识别”。若不是安全事件,则针对数据中台异常进行异常规则匹配,判断是否需要被映射成为告警;如果是安全事件,则首先将数据中台异常映射成为安全事件,之后根据该类安全事件的处理规则判断是否需要被映射成为告警;如果上述的异常或安全事件暂不处理,则需要对该类异常或安全事件进行记录。

大量告警信息可能在短时间内产生,单独处理每个告警会增加处理复杂性和工作量,且难以从整体把握安全态势。因此,系统会按照一定的时间周期和逻辑规则,根据告警类型对告警进行聚合。之后依据已

有案件的告警类型将聚集的告警组合成案件,便于进行统一的调查分析和响应处置。每个案件在处理时会根据案件类型自动匹配并调用相应的剧本,进行自动化处理。不同类型的案件对应不同的剧本,确保处理过程的准确性和高效性。

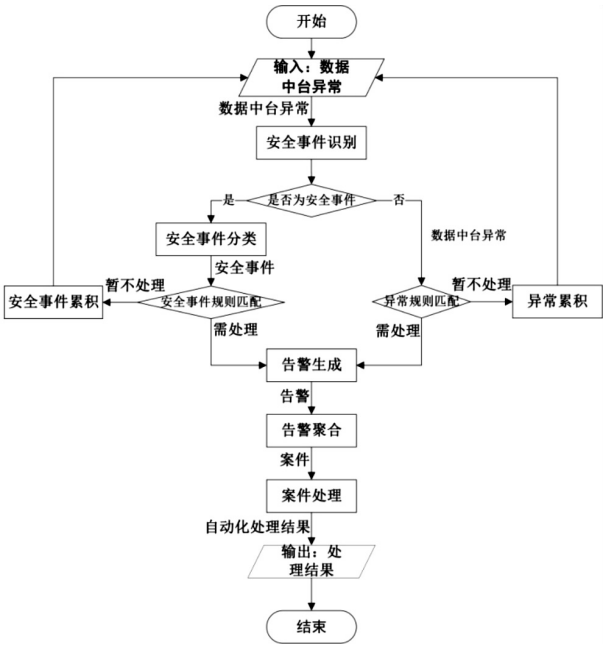

图 1　方案流程

经过剧本中定义的一系列动作的执行,案件得到处理,系统输出处理结果,标志着整个安全自动化响应流程的完成。

2.2　实体及其转化关系设计

前文提到了相关实体并概述了其作用,本节针对电力数据中台中的概念、实体以及它们之间的关系构建领域模型类图,如图 2 所示。

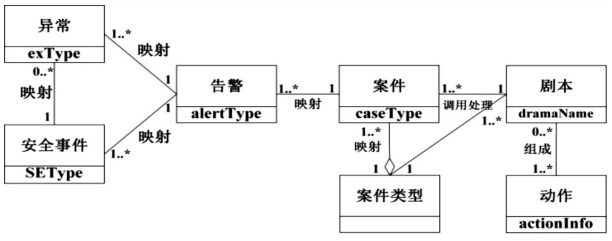

图 2　电力数据中台自动化响应领域模型类图

下面给出相关实体的定义及转化关系。

(1)异常(EX)。

异常的形式化定义如式 1 所示。

$$EX = < exInfo, exType, interval > \quad (1)$$

其中, interval $\in T^{IN}$ 表示起始时间和终止时间,即: $T^{IN} = \{[begin_i, end_i] \mid i \in N^*\}$。后续的实体定义的 interval 与该 interval 含义相同。exInfo 为异常的具体信息,包括对异常方式、表现形式等方面的描述,多用于展示给用户查看。exType 为异常类型,为分类处理异常提供相关信息。

(2)安全事件(SE)。

安全事件的形式化定义如式 2 所示。

$$SE = < id, exType, SEType, SEInfo, interval > \quad (2)$$

安全事件是计算机系统中针对入侵等安全行为导致的异常情况的集合。

exType 用于精确标识不同异常的具体类别。通过精细划分异常的类别,系统能够更加准确地将异常转化为安全事件。

SEType 代表了安全事件的类别,它将有关安全行为的异常信息进行了归类和整合,使得系统可以从宏观上把握这些异常的整体情况。

SEInfo 与 exInfo 类似,是对安全事件的详细描述,用于展示给运维人员。

异常与安全事件之间建立多对一的映射关系,这是因为并非所有异常均与安全行为有关,根据安全事件的定义并不需要均转化为安全事件。另外,多种安全方面的异常可能在攻击方式、攻击平面等方面有相似性,是同一类安全威胁,则这些类型的异常也可以被映射为同一类型的安全事件。

(3)告警(Alert)。

告警的形式化定义如式 3 所示。

$$Alert = < id, alertType, equipType, interval, hasDealed > \quad (3)$$

alertType 用于对告警进行精确的分类。不同的告警类型可能涉及不同类型的安全事件和异常活动,需要采用不同的处理策略。

equipType 是告警发生时系统所处的设备类型,可分为 PC 端、ios 端、安卓端等,也可继续进行详细划分。依此划分的原因是对于不同设备类型,处理方式、调用接口会略有不同,因而需要定义不同的处理方式进行处理。

alertType 与 equipType 并无直接的关联关系,一种 equipType 中可以同时发出多个 alertType 的告警;一种 alertType 的告警也可以在多种设备中同时发生。最终处理方式的决定需首先关注 alertType ,它决定防护的主要逻辑;而 equipType 用来解决同一防护逻辑中由于系统不同造成调用接口的微小改变。

hasDealed 表明当前告警是否已被处理,新案件的生成只会针对未被处理的告警进行。

在安全事件与告警信息的关联处理方面,本方案采用了多对一的设计架构。告警信息并非针对每个安全事件均会生成,而是在满足管理员所设定的安全事件匹配规则时才予以触发。安全事件匹配规则通常可依据安全事件的出现频率、类型以及影响范围等维度进行映射定义。在实际的电力数据中台系统中,运维

人员能够设定诸多类似的映射规则,从而赋予系统较强的拓展性与灵活性。

数据中台异常与告警也为多对一关系。这些除安全事件以外其他异常的规则匹配方式与安全事件规则匹配方式相似,通常从出现频率、异常类型等方面进行映射的定义。

(4)案件(Case)。

案件的形式化表示如式 4 所示。

$$\text{Case} = < \text{id}, \text{caseTypeId}, \text{strategyId}, \text{aiOrManual}, \text{interval} > \tag{4}$$

caseTypeId 作为案件类型的标识,能够与其他实体进行关联,便于系统其他步骤在用到案件时能尽快查找对应的案件。

strategyId 即剧本 id,系统可以根据 strategyId 快速找到适用的剧本,从而高效地执行案件处理任务。aiOrManual 字段记录了案件实际处理过程中采用的方式。在自动化程度不断提高的今天,许多案件处理任务已经可以通过自动化工具或系统来完成。然而,在遇到未知情况或处理失败情况时,仍需要人工进行干预和决策。

告警映射成为案件的方式可根据电力数据中台实际情况制定,本方案只给出了一种可能的映射方式。设当前数据中台环境在 t 时间范围内出现的告警类型集合为 $\text{AlertType}_t = \{\text{at}_1, \text{at}_2, \cdots, \text{at}_n\}$,设数据库中已有案件类型的集合为 $C = \{c_1, c_2, \cdots, c_m\}$,对于每个案件类型 $c_i \in C$,有告警类型集合属性 $\text{alertTypes}(c_i) = \{\text{at}_{i1}, \text{at}_{i2}, \cdots, \text{at}_{ik}\}$。首先检查是否存在 $\text{at} \in \text{Alert}_t$,使得存在 $c_i \in C$ 满足 $\text{at} = \text{alertTypes}(c_i)$,若有则生成案件。否则执行如下操作:

●计算 Alert_t 与所有已有案件告警类型集合的最大交集 $I_t = \max(\bigcap_{c_i \in C} \text{alertTypes}(c_i))$,将 I_t 对应的案件记录在集合 C' 中;

●计算差集 $\text{Alert}_t' = \text{Alert}_t - I_t$;

●若 $\text{Alert}_t' = \varnothing$ 或 $\text{Alert}_t = \text{Alert}_t'$,则结束流程;

●令 $\text{Alert}_t = \text{Alert}_t'$,重复第一步。

结束后,$\forall c' \in C'$,$\exists i, c_i \in C$,生成案件 c_i,该案件的剧本 id 使用案件 c_i 的 strategyId。若 $\text{Alert}_t' = \varnothing$,则进入下一环节;若 $\text{Alert}_t' \neq \varnothing$,则生成案件类型 CaseType 与案件 Case,案件类型 CaseType 的 alertTypes 属性填入 Alert_t;Case 的 caseTypeId 填入新生成 caseType 的 id,aiOrManual 字段填入 manual 表示该案件被人工处理,同时生成人工处理通知。

例如已有案件 Case:

Id = 1, alertTypes = $\{A, B, C\}$, strategyId = A

Id = 2, alertTypes = $\{A, C, D\}$, strategyId = B

现有被聚合的告警 alert:

Id = 1, alertType = A

Id = 2, alertType = B

Id = 3, alertType = F

该案件的告警类型集合为 $\{A, B, F\}$,$\{A, B, F\} \not\subset \{A, B, C\}$ 且 $\{A, B, F\} \not\subset \{A, C, D\}$,不能应用任何已有案件所对应的剧本,因而首先计算最大交集 $I_t = \max \bigcap_{c_i \in C} \text{alertTypes}(c_i)$,与之交集最大的已有案件为 id = 1 的案件,加入到 C' 中,同时得到最大交集 $I_t = \{A, B\}$;计算差集 $\text{Alert}_t' = \text{Alert}_t - I_t$,得到 $\text{Alert}_t' = F$。继续执行算法流程,最终得到 $\text{Alert}_t = \text{Alert}_t' = F$。此时对 C' 中的所有案件生成新案件。新案件的剧本 id 使用 id = 1 案件的剧本 id,即生成:

Id = 3, alertTypes = $\{A, B, C\}$, strategyId = A

另需生成新的案件类型,其 alertTypes 属性填入 $\{F\}$;另外生成新的案件,caseTypeId 填入新生成案件类型的 id。最后需转入人工处理,将 aiOrManual 设置为 manual。

在电力数据中台安全防护体系中,告警与案件的映射方案具有多样性,上述映射方案仅作设计参考。相同环境下相同异常的处理方式在多数情况下一致。因而在告警类型与案件间建立多对一关系。相同类型的多个告警对应同一类案件,避免重复处理,可提升处理速率。依据既定映射关系,系统能准确地将告警映射成为案件,减少人为失误。

(5)案件类型(CaseType)。

案件类型的形式化表示如式 5 所示。

$$\text{CaseType} = < \text{id}, \text{dramaId}, \text{onUse}, \text{caseType}, \text{alertTypes} > \tag{5}$$

案件类型确保在自动化编排的过程中能够精准地选择最合适的剧本进行处理。单独定义的原因是针对某一种案件类型可以定义相关独立逻辑,而与具体案件无关,因而不再延续使用案件实体中的案件类型字段。

dramaId 表示这一案件类型的案件使用哪一剧本进行自动化处理。dramaId 与 strategyId 的不同点在于 strategyId 仅记录某一条案件的处理使用的剧本 id,而 dramaId 记录的是该类所有案件的推荐剧本 id。onUse 表示当前案件类型能否使用 id 为 dramaId 的剧本,onUse = 1 表示能够使用。caseType 是当前的案件类型。alertTypes 表示该案件类型能够解决告警集合为 alertTypes 的案件。

本方案采取了一个案件类型对应多个案件的设计。这种设计能够针对一类案件统一设置处理逻辑、处理开关等,提高了系统的自动化响应能力。

(6)动作(Action)。

动作的形式化表示如式 6 所示。

$$\text{Action} = < \text{id}, \text{actionName}, \text{actionInfo}, \text{actionCreator} > \tag{6}$$

在安全编排响应过程中,动作是安全程序执行的核心组成部分。每一个动作都代表着在某一防护软件上的原子化服务。日常运维人员可以根据实际的安全需求和业务场景进行自主创建。一旦创建完成,这些动作将被持久化存储于动作库中,成为自动化编排响应过程中的可调用资源。

每个动作都有一个唯一的名称 actionName,以便于识别和引用。actionCreator 字段用于标识动作的创建者,这可以是具有不同权限和角色的用户,如 root 用户、编排管理人员或日常运维人员。随着动作库的不断扩充和使用数据的积累,编排管理人员可以根据实际需求,调整该动作的 actionCreator 属性,以扩大其使用范围或优化其管理策略。这种动态调整机制使得动作库能够不断适应新的安全需求和业务场景,保持其灵活性和适应性。

(7)剧本(Drama)。

剧本的形式化表示如式 7 所示。

$$\text{Drama} = < \text{dramaName}, \text{caseType}, \text{allNums}, \text{sucNums}, \text{failNums}, \text{actDAG} > \tag{7}$$

dramaName 字段用于命名剧本,需要保证唯一性。这不仅有助于管理和调用,还能让运维人员快速了解剧本的用途和适用范围。

caseType 字段用于记录处理案件的类别,为系统提供了自动化响应推荐的基础。当系统检测到某类案件时,可以根据 caseType 字段快速找到相应的剧本,并进行自动化响应。

failNums、sucNums 和 allNums 分别表示剧本的失败次数、成功次数和总次数。这些数据为计算剧本的成功率提供了依据,使得系统能够评估剧本的性能并不断优化。

actionDAG 字段以文本形式存储了动作流程图的详细信息,展示了动作之间的执行顺序和依赖关系。通过解析 actionDAG 字段,系统能够准确地执行剧本中的每一个动作,实现自动化响应的目标。

一个案件类型可以对应多个剧本的对应关系。这是因为在不同的环境条件下,不同剧本的处理成功率不同,需要对每个类型的案件存储一定数量的剧本,才能在自动化响应时有更多的选择。

动作是处理过程的最小单元;剧本是针对案件类型处理的最小单元。一个剧本由多个动作以一定的顺序组成,形成了一个有向无环图。设动作集合 $\text{Action} = \{a_1, a_2, \cdots, a_n\}$,每一个动作有唯一的名称,在此用函数 $\text{description}(a_i)$ 表示动作描述为.exe 的可执行程序名称。设剧本集合为 $\text{Drama} = \{d_1, d_2, \cdots, d_n\}$,定义有向无环图 $G = (V, E)$,其中 $V \subseteq \text{Action}$,即每个节点代表一个动作,$E \subseteq V \times V$,对于 $(u, v) \in E$,表示动作 u 需要在动作 v 之前发生,用 $u \rightarrow v$ 表示。对于有向无环图 G,定义 $I_G = \{v \in V \mid \text{indegree}(v) = 0\}$,其中 $\text{indegree}(v)$ 表示节点 v 的入度,则 I_G 表示有向无环图 G 中所有入度为 0 的点。初始 I_G 中的所有节点均可作为剧本的起始节点。定义 $O_G = \{v \in V \mid \text{outdegree}(v) = 0\}$,其中 $\text{outdegree}(v)$ 表示节点 v 的出度,则 O_G 表示有向无环图 G 中所有出度为 0 的点,它们可以被当作剧本的结束节点。编排剧本时,若两个动作有先后顺序关系,则 $(u, v) \in E$。

一个剧本可以由多个动作组成,一个动作也可以出现在多个剧本中,两者为多对多关系。这种多对多的设计使得系统在自动化响应时能够拥有更多的选择空间,提高了系统的灵活性和适应性。

3　系统设计方案

本方案针对 SOAR 的核心,设计了如图 3 所示的系统架构,分为安全事件处理、告警信息处理、案件信息处理、剧本动作编排、自动化响应。

图 3　系统架构

在安全事件处理中,本方案设计了三个主要步骤:安全事件识别、安全事件类型定义以及安全事件生成。安全事件识别的任务是判断数据中台异常是否由与电力系统的网络、数据或基础设施安全相关的威胁或攻击行为引起。安全事件类型定义步骤由管理员在系统运行前根据安全威胁风险定义哪些类型异常为安全事

件。最后,根据安全事件识别逻辑自动化生成安全事件。

告警信息处理中有异常规则匹配、安全事件规则匹配、告警生成这三个步骤。异常规则匹配与安全事件规则匹配主要通过对异常或安全事件的出现频率、种类、影响范围等相关参数进行观测,结合已有规则,最终生成告警。

案件信息处理分为案件类型处理与案件处理两个部分。案件类型处理是在当前聚合的告警未能匹配已有案件时进行,需要综合已有的剧本信息、案件信息,创建新的案件类型。案件处理是聚合一定时间范围内的告警,根据已有案件以及剧本,合理生成案件。

剧本动作编排主要分为动作编排与剧本编排两个部分。电力数据中台涉及的场景多、差异性大、环境复杂,因而在动作编排中,运维人员需要根据实际场景构建电力业务的原子化服务。在剧本编排中,运维人员需要根据已有的原子化服务,设计执行逻辑,最终实现组件化高效编排。

自动化响应模块中,系统根据剧本定义的动作顺序进行自动化处理,从而在较短的时间内自动化处理每一个告警。处理过后的结果会被保存到数据库中持久化存储,便于后期查找、溯源问题。

4 实验分析

实验分析中主要将自动化响应系统与未使用自动化响应系统的传统处理方式进行对比。

4.1 测试指标

处理时间:从异常发生到异常完成处理所用时间。实验中规定触发异常为异常发生时刻,调用所有处理接口之后发送 ACK 作为完成处理时刻。

处理准确度:对于每个异常,设定某一接口调用序列作为理想答案。在此引入编辑距离的概念。编辑距离是一种衡量两个序列相似度的方法,它通过计算将一个序列转换为另一个序列所需的最少操作次数来实现,这些操作包括插入、删除和交换。

规定插入的花费为 3,删除的花费为 2,交换的花费为 1。这是因为需要插入操作意味着实际调用执行的接口数量比理想处理方案少,则可能导致某些重要接口未能调用;删除操作代表实际调用执行的接口数量比理想处理多,则可能导致非必要异常处理,影响数据中台性能;交换操作意味着某些操作乱序,则可能导致部分操作因前置操作未完成而无法完成。定义两序列完全相同时,编辑距离为 0。

最后,定义处理准确度计算公式为:$S_{\text{accurate}} = \frac{L_{\text{original}}}{S_{\text{distance}} + 1}$,其中 S_{accurate} 为处理准确度,L_{original} 为理想序列的长度,S_{distance} 为编辑距离。处理准确度 S_{accurate} 越大,表示实际调用序列与理想序列越相似,处理越准确。

处理灵活性:在本测试中用调整危险等级的方式进行方案灵活性的测试。规定某种场景下,某一类型异常由低危转化为高危,在发送同样频率的异常情况下,用系统处理的及时性衡量处理灵活性。

4.2 实验环境

本实验中,不同方式的响应均在 windows11 操作系统上运行,详细参数如下:

处理器:Intel Core i7 13620H;

内存类型为 DDR5,内存大小为 16 GB。

4.3 实验步骤

实验模拟在质检、传输模块中同时发现异常,质检模块出现的异常应当调用接口 A 进行处理,传输模块出现的异常需要依次调用接口 B、C 进行处理。因而理想方案为依次调用 ABC 三个接口。

现有数据中台的异常处理方式是“多人、多系统、多界面”的,实验需要 2 人分别在质检系统与传输管理系统中进行调用接口操作。“安全编排与自动化响应”系统方案使用开发好的独立软件,需要 1 人在该系统的相关界面上进行监控与操作。初始时已设定好相关异常处理的 DAG。

首先基于现有数据中台的异常处理方式与步骤处理异常;之后使用基于本方案设计的系统对异常进行处理。测试并记录相关数据。在每一种处理方式中,进行下面三组实验。

(1)在程序处理单个异常的函数模块中加入时钟打印指令,便于记录某个异常的处理时间。实验开始后每 30 秒产生一个相同的异常,持续 20 分钟,记录相关参数。设定触发异常处理的阈值为 2,即每出现两个相同的异常进行一次处理。本组实验用来验证本方案的有效性、高效性。

(2)其他条件不变,实验开始 10 分钟后,在不停机的情况下提升该类异常的危险等级,通过前端系统修改自动化响应系统中该异常的阈值,之后再持续 10 分钟记录相关数据。本组实验用来验证本方案的灵活性。

(3)其他条件不变,将发起异常程序修改为以 180 秒为一个周期,一个周期内每 60 秒产生一个不同的异常,共 3 类不同的异常种类。假设每类异常的理想方案均不相同,分别为依次调用 ABC 接口、依次调用 ABF 接口、依次调用 DEC 接口,且设定触发每类异常处理的阈值均为 1。持续实验 20 分钟,记录相关数据。本组实验模拟电力数据中台不同异常源带来的异常信息,用来验证本方案在处理不同异常时的有效性

及准确性。

现有数据中台处理方法的实验数据为人工记录,自动化响应系统的实验数据为程序打印得到。

4.4　实验结果

使用 4.3 中(1)的实验方案试验。

数据中台现有方法的处理时间如表 1 所示。

表 1　实验组 1-现有方法处理时间　s

时间	处理时间	时间	处理时间
62	5	…	…
121	4	1 202	5
183	8		

使用自动化响应的系统处理时间如表 2 所示。

表 2　实验组 1-自动化响应系统处理时间

时间/s	处理时间/ms	时间/s	处理时间/ms
60	789	…	…
120	720	1 200	695
180	679		

每 60 秒进行一次数据记录是因为设定的异常处理阈值为 2。在系统初始化好相关异常处理 DAG 时,自动化响应系统的处理时间远远小于数据中台的现有方法。并且数据中台现有的半自动化处理方式需要人工进行操作,处理时间不稳定。在处理准确度方面,两种方法的准确度均为 3,即编辑距离均为 0,说明它们都能够很好地处理出现的异常。

使用 4.3 中(2)的实验方法重复试验。

数据中台现有方案的处理时间如表 3 所示。

表 3　实验组 2-现有方法处理时间　s

时间	处理时间	时间	处理时间
62	7	602	9
122	5	640	7
181	6	664	12
…	…	…	…
571	8	1 203	6

使用自动化响应的系统处理时间如表 4 所示。

表 4　实验组 2-自动化响应系统处理时间

时间/s	处理时间/ms	时间/s	处理时间/ms
60	707	600	699
120	695	630	730
180	754	660	711
…	…	…	…
540	743	1 200	676

可以看到,修改该类异常的危险等级对单个异常的处理时间无明显影响,自动化响应的系统处理效率仍然高于数据中台现有方案。在数据中台现有方案的处理时间中,640 秒时处理的是 630 秒产生的异常,延迟了 10 秒处理是因为危险等级刚刚调整,人工处理未能及时调整。而自动化响应的处理系统则能够在 600 秒调整危险等级后及时对 630 秒的异常进行处理。可以看出自动化响应系统能够在处理逻辑变化时灵活做出及时调整,有较高的灵活性。并且在自动化响应的加持下,能够在处理策略变化后比数据中台现有方法更稳定地响应异常。

最后使用 4.3 中(3)的实验方案重复试验。

数据中台现有方案的处理时间如表 5 所示。

表 5　实验组 3-现有方法处理时间　s

时间	处理时间	时间	处理时间
62	7	360	9
122	10	420	7
181	15	480	10
240	8	…	…
300	12	1 203	6

使用自动化响应的系统处理时间如表 6 所示。

表 6　实验组 3-自动化响应系统处理时间

时间/s	处理时间/ms	时间/s	处理时间/ms
60	650	420	661
120	710	480	723
180	804	540	791
240	643	600	639
300	696	…	…
360	836	1 200	678

在数据中台现有方案中,针对不同类型的异常需要调用不同的接口,需要人类决策,耗时更长且易出错。在使用自动化响应系统后,系统能够针对每类异常快速判断应当使用什么剧本处理,处理时间稳定且低于数据中台现有方案的处理时间。

在处理准确度方面,自动化响应系统也拥有一定优势。在数据中台现有方法的实验中,664 秒对 660 秒出现的异常进行处理。660 秒的异常应当依次调用 ABF 接口进行处理,而在实验中,误操作为了分别调用 BACF 接口。此时使用数据中台现有方法处理的数据准确度为 $S_{\text{accurate}} = \frac{3}{(1+2)+1} = 0.75$,而自动化响应系统处理的数据准确度依然为 3,说明在某些情况下,本方案给出的安全自动化响应方案能够更好地防止处理准确度的降低。

4.5　实验总结

通过上述三个实验方法的测试,可以发现依据本方案开发的安全自动化响应系统有处理时间短、处理准确度高、处理灵活性强的特点,能够在一定程度上对

电力数据中台中种类复杂多样的异常进行自动化处理。在实际场景中,异常种类的数量远大于文中测试的数量,它们间的关联程度也将变得更加复杂。通过实验说明了该方案应用于实际电力数据中台的可行性,但若希望将该自动化响应方案应用于实际场景,则需要进行与实际系统更贴合、更详尽的测试。

5 结束语

该文根据安全编排与自动化响应技术(SOAR)设计了电力数据中台安全自动化响应方案,实现了安全自动化响应系统。它集成了多种系统、应用程序和工具,实现了自动化的异常处理流程,使安全团队能够更专注于高价值的安全分析和工作。

在未来,自动化响应方案还可以进一步优化。异常规则与安全事件规则可以根据实际业务进行扩展,告警、案件的生成过程可交由人工智能生成。所用实验数据较为简单且对于所有异常均初始化好 DAG 处理流程。在实际应用该方案时还需要进行更为复杂的实验测试,并对未能初始化 DAG 时的处理效果进行评估,才能最终投入生产使用。

参考文献:

[1] 中华人民共和国人民政府国务院. 国务院关于印发“十四五”数字经济发展规划的通知. 国发〔2021〕29 号[EB/OL](2022-01-12)[2025-01-24]. https://www.gov.cn/zhengce/content/2022-01/12/content_5667817.htm.

[2] 中关村网络安全与信息化产业联盟数据安全治理专业委员会. 数据安全治理白皮书 5.0[EB/OL](2023-05-18)[2025-01-24]. https://13115299.s21i.faiusr.com/61/1/ABUIABA9GAAggqejowYo5bPKkAY.pdf.

[3] 晏 庆,崔浩贵,刘 冰,等. 大数据时代下计算机信息网络安全问题研究[J]. 无线互联科技,2024,21(17):102-104.

[4] 周千荷,高 月. 智驭未来,安全先行:智能汽车软件供应安全的挑战与对策[J]. 智能网联汽车,2024(4):76-79.

[5] 华为技术有限公司. 什么是 SOAR?[EB/OL]. (2023-07-18)[2025-01-23]. https://info.support.huawei.com/info-finder/encyclopedia/zh/SOAR.html.

[6] 廖 雯. 安全编排与自动化响应的探索与场景实践[J]. 信息网络安全,2020(S2):102-105.

[7] 黄海波,蒋金桥,朱丽娜. 安全编排自动化与响应技术综述[J]. 工业信息安全,2024(2):32-38.

[8] ΤΣΙΑΤΚΑΣ N. Open-source security orchestration, automation and response (SOAR) platform deployment and use[D]. Piraeus: University of Piraeus, 2023.

[9] 阿里云. 云安全中心. 威胁分析与响应[EB/OL]. (2009-02-24)[2025-01-23]. https://yundun.console.aliyun.com/?spm=a2c4g.11186623.0.0.336f46c7jiETR3&p=sas&accounttraceid=b64a2216d77e453d9cef0c66188f8cd3wnxn#/productAccess/cn-hangzhou.

[10] 束维国. 基于安全编排自动化与响应技术在网络安全应急响应中的应用探索[J]. 现代工业经济和信息化,2022,12(8):112-114.

[11] BARTWAL U, MUKHOPADHYAY S, NEGI R, et al. Security orchestration, automation, and response engine for deployment of behavioural honeypots[C]//2022 IEEE conference on dependable and secure computing (DSC). Edinburgh: IEEE, 2022:1-8.

[12] VAST R, SAWANT S, THORBOLE A, et al. Artificial intelligence based security orchestration, automation and response system[C]//2021 6th international conference for convergence in technology (I2CT). Maharashtra: IEEE, 2021:1-5.

[13] KINYUA J, AWUAH L. AI ML in security orchestration, automation and response future research directions[J]. Intelligent Automation & Soft Computing, 2021, 28(2):527-545.

[14] 张彩云,张新禹. SOAR 技术在气象信息化网络安全防护中的应用研究[J]. 网络安全技术与应用,2023(12):107-109.

[15] 武静雅,郑 磊,郑毓武,等. SOAR 对企业数字化安全运营的重要性探讨[J]. 网络空间安全,2023,14(3):67-70.

[16] 罗 威,姜元建,殷炜俊,等. 基于 SOAR 的电力 5G MEC 安全解决方案[J]. 现代电子技术,2024,47(10):151-158.

[17] 谢国涛,常超杰,范云飞. 物联网安全编排、自动化与处置响应技术研究[J]. 邮电设计技术,2023(4):38-41.

[18] LEE M, JANG-JACCARD J, KWAK J. Novel architecture of security orchestration, automation and response in internet of blended environment[J]. Computers, Materials & Continua, 2022, 73(1):199-223.

[19] 吴灵菲,孙 攀. 安全编排自动化与响应在医院中的应用场景探索[J]. 信息与电脑:理论版,2024,36(18):91-93.

[20] 李若彤. 新型电力系统 APT 攻击防御策略集的安全编排与自动化响应方法[D]. 北京:华北电力大学(北京),2024.