护网行动信息安全应急预案

2020年 8月

目 录

第一章　总则

1.1 编制目的

为规范 XXXX 股份有限责任公司（以下简称“集团公司”　）护网演习信息安全事件应急工作，提高应对突发信息安全事件的综合管理水平和应急处置能力，　　形成决策科学、措施有力、反应迅速的应急工作机制，有效防范信息系统风险，确保信息系统的安全、持续、稳定运行，降低信息安全事件的危害，特制定本预案。

1.2 编制依据

以国家有关法规、规章、相关政策为依据，指导集团公司信息安全总体应急预案的编制工作。适用性法规标准主要有：

《中华人民共和国网络安全法》

《中华人民共和国突发事件应对法》　（国家主席令第　69 号）

《中华人民共和国计算机信息系统安全保护条例》　　（国务院令第　147 号）

《国家突发公共事件总体应急预案》

《国家网络与信息安全事件应急预案》

《国务院有关部门和单位制定和修订突发事件应急预案框架指南》　　（国办函 [2004]33 号）

《GB/T 19715.1-2005　信息技术　安全技术　信息技术安全管理指南》

《GB/Z 20986-2007 信息技术　信息安全事件分类分级指南》

《GB/T 20988-2007 信息安全技术　信息系统灾难恢复规范》

《GB/T 22239-2008 信息安全技术　信息系统安全等级保护基本要求》

《ISO 22301:2012 业务连续性管理体系》

《XXXX　集团有限公司突发事件总体应急预案》

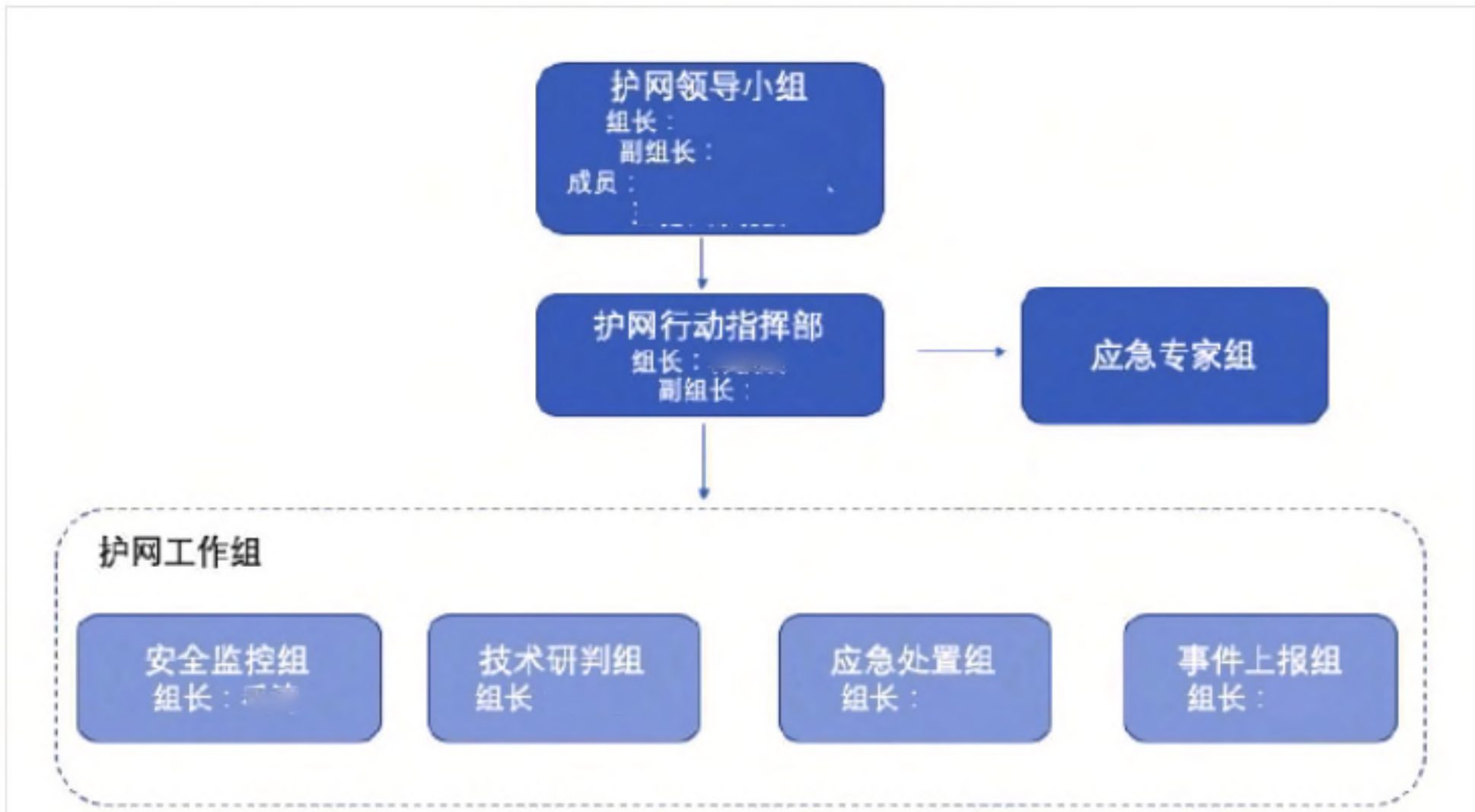
1.3 适用范围

本预案适用于集团公司总部及子分公司在护网演习期间网络与信息安全事件的预防、通报和应急处置工作。

第二章 组织机构及职责

2.1 集团公司组织机构

护网期间，集团公司护网工作由网络安全与信息化领导小组牵头，成立护网行动指挥部、护网工作组、应急专家组对护网工作进行组织及整体把控。



总部成立护网 2019 领导小组，负责护网工作的重大决策，统一领导和指挥调度，由集团网络安全和信息化分管领导任组长。

成立护网行动指挥部，负责网络安全保障的工作部署、监督检查与应急调度。信息化部主要领导任组长，各业务职能部门和各单位信息分管领导为小组成员，其中办公厅负责护网指挥大厅场所及后勤保障，财务部负责护网行动专项资金保障，法务部负责护

网期间法律纠纷问题。

指挥部下设护网工作组，负责护网具体组织协调、技术支撑相关工作，护网工作组下设安全监控组、技术研判组、应急处置组、事件上报组。

安全监控组负责利用各类监测类设备发现并初步确认攻击事件。

技术研判组负责根据上报事件，通过流量、日志及告警行为等信息，进行全面溯源分析，确认攻击事件的行为及影响范围，为应急处置组提供处置建议。

应急处置组负责则在事件发生时进行隔离、断网，全面的排查、处置与恢复。

事件上报组负责形成事件应急处置报告，上报护网工作组。

各工作组织人员安排详见附件一。

2.2 子分公司护网工作组

护网演习期间，各子分公司参照集团公司组织架构，自行设置各工作组，设置各工作组与集团公司联系接口人员。

2.3 通联方式

护网演习过程中的通联方式由以下几种：

电话

针对护网演习中的紧急事件通过手机、座机对事件相关人员进行实时通报。护网期间所有参与护网工作人员需保证手机 24h 开机。

事件上报平台

在事件处置完毕后，事件处置人员通过事件上报平台向相关人员上报完整处置材料。

OA 系统

在护网演习期间重大事件发生时，通过 OA 系统直接向指挥部集团领导进行正式汇报。

第三章　事件分级分类

3.1 事件分级

3.1.1　一级事件

若演习目标被控制，则定义事件为一级事件，对应《　　XXXX 集团有限公司突发事件总体应急预案》安全红色预警及应急Ⅰ级响应。

3.1.2　二级事件

若重要系统或设备被控制，则定义事件为二级事件，对应《　　XXXX 集团有限公司突发事件总体应急预案》安全红色预警及应急Ⅰ级响应。

3.1.3　三级事件

若内网一般设备被控制，则定义事件为三级事件，对应《　　XXXX 集团有限公司突发事件总体应急预案》安全橙色预警及应急Ⅱ级响应。

3.1.4　四级事件

若 DMZ 区一般设备被控制，则定义事件为四级事件，对应《　　XXXX 集团有限公司突发事件总体应急预案》安全黄色预警及应急Ⅲ级响应。

3.1.5　五级事件

若 DMZ 区设备遭到攻击或内网终端遭到攻击，　则定义事件为五级事件。 对应《XXXX 集团有限公司突发事件总体应急预案》安全黄色预警及应急Ⅲ级响应。

3.2 事件分类

3.2.1 木马后门事件

木马后门事件主要包括：服务器中检测存在 WEB Shell 脚本木马、远程控制、键盘记录、Rootkit 等木马程序，将导致应用系统及服务器被黑客持续控制，甚至可作为跳板机进行对其他资产的深入攻击。

3.2.2 异常登录事件

异常登录事件主要包括：应用系统和服务器中检测存在克隆账号、隐藏账号，以及存在未授权用户、异常时间、异常来源登录等。

3.2.3 钓鱼邮件事件

钓鱼邮件事件主要包括：邮件附件包含恶意代码、恶意链接，从而可导致员工内部主机被控，或泄露重要敏感信息。

3.2.4 漏洞攻击事件

漏洞攻击事件往往从攻击人员漏洞扫描探测发现漏洞开始，之后通过对漏洞点进行分析并深入利用，从而从存在漏洞系统获取相应的敏感信息甚至直接拿下系统的控制权限。

3.2.5 暴力破解事件

暴力破解事件主要包括：对主机、终端设备、应用系统账号密码的暴力破解，黑客通过信息收集，生成暴力破解字典，或根据已泄露的密码进行撞库，从而可能导致系统密码被黑客破解。

3.2.6　数据窃取事件

数据窃取事件主要包括：敏感信息爬取，利用任意文件读取等漏洞窃据敏感文件，利用 SQL 注入漏洞等窃取数据库敏感信息，以及入侵成功后拖取数库等行为。

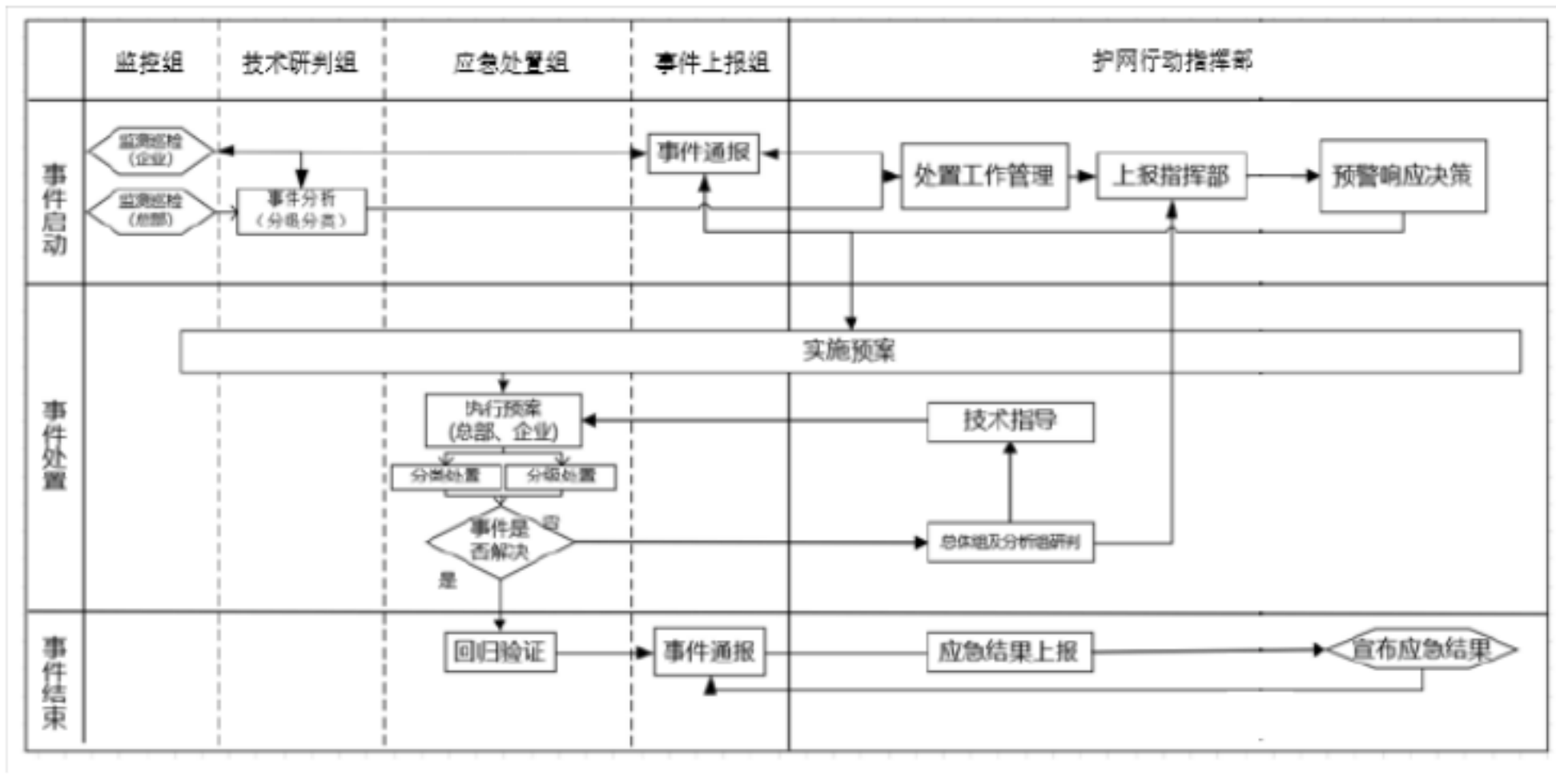
3.2.7　拒绝服务事件

拒绝服务事件主要包括： CC 攻击、DOS 攻击、DDOS 攻击、DRDOS 攻击。一旦遭受拒绝服务攻击，可导致服务器宕机，网络阻塞，从而破坏正常的业务稳定运行。

第四章　应急处置总体流程

安全事件处置流程由护网行动指挥部进行制定，在安全事件发生时由安全监控组、技术研判组、应急处置组、事件上报组、护网行动指挥部按照以下流程协调配合最终达到有效完成安全事件处置的目的。

总体工作流程图如下图所示：



第五章　事件分级流转

按照扁平化指挥原则，通过建立护网行动即时通讯群组，总部在群组中及时发布预

警信息指令，子分公司及时通过群组向总部进行事件汇报。针对重大事件的发生，总部及子分公司相关人员应第一时间通过电话向总部领导汇报情况。正式情况材料按照处置流程通过 OA 系统、事件上报平台上报。

5.1 一级事件

总部：

在演习过程中发生一级安全事件时，技术研判组应当在第一时间通过即时通讯群组及电话的形式向护网行动指挥部报告事件情况，并生成安全事件简报上报护网行动指挥部，不得迟报、谎报、瞒报和漏报，护网行动指挥部对事件简报内容进行确认，并部署应急处置组迅速开展应急处置工作。

在事件处置完成后，应急处置组应立即梳理出信息安全事件书面报告交付事件上报组，由其通过事件上报平台向事件有关部门进行通报。同时信息安全事件书面报告的内容要简明、准确，主要包括：时间、地点、信息来源、事件起因和性质、基本过程、已造成的后果影响及涉及财产损失、影响范围、发展趋势、处置情况、拟采取的措施、单位全称、联系人和联系电话等。

子分公司：

按照护网行动指挥部统一安排配合其进行事件处置。

5.2 二级事件

总部：

在演习过程中发生二级安全事件时， 处置流程与一级事件相同。 在事件处置完成后，应急处置组可在一个工作日内，梳理出信息安全事件书面报告（报告要求同一级响应报告内容）交付事件上报组，由其通过事件上报平台向事件有关部门进行通报。

子分公司：

子分公司工作组应当在第一时间通过即时通讯群组及电话的形式向总部上报组报告事件情况，并提交事件证据相关材料，事件上报组需在收到子分公司上报信息后，将相关材料信息转交技术研判组，由技术研判组对子分公司上报信息进行研判，子分公司在

技术研判组指导下完成事件处置。在事件处置完成后的一个工作日内，梳理出信息安全事件书面报告（报告要求同一级响应报告内容），通过事件上报平台向总部事件上报组进行通报。

5.3 三级事件

总部：

在演习过程中发生三级安全事件时，技术研判组应当在第一时间通过及时通讯群组向事件相关人员及护网行动指挥部报告事件情况，汇报流程与一级相同，不得迟报、谎报、瞒报和漏报，同时迅速开展应急处置工作。在事件处置完成后的在一个工作日内，梳理出信息安全事件书面报告（报告要求同一级响应报告内容），通过事件上报平台向相关部门进行通报。

子分公司：

子分公司工作组应当在第一时间通过即时通讯群组及电话的形式向事件上报组报告事件情况，并自行完成事件处置。在事件处置完成后，应在一个工作日内，梳理出信息安全事件书面报告（报告要求同一级响应报告内容），通过事件上报平台向总部事件上报组进行通报。

5.4 四级事件

总部：

在演习过程中发生四级安全事件时，技术研判组应当在第一时间通过及时通讯群组向事件相关人员及护网行动指挥部报告，汇报流程与一级相同，不得迟报、谎报、瞒报和漏报，同时迅速开展应急处置工作。在事件处置完成后，应在两个工作日内，梳理出信息安全事件书面报告（报告要求同一级响应报告内容），通过事件上报平台向相关部门进行通报。

子分公司：

子分公司工作组应当在第一时间通过即时通讯群组及电话的形式向事件上报组报告事件情况，并自行完成事件处置。在事件处置完成后，应在两个工作日内，梳理出信息

安全事件书面报告（报告要求同一级响应报告内容），通过事件上报平台向总部事件上报组进行通报。

5.5 五级事件

总部：

在演习过程中发生五级安全事件时，技术研判组应当在第一时间通过及时通讯群组向事件相关人员及护网行动指挥部报告，不得迟报、谎报、瞒报和漏报，同时迅速开展应急处置工作。在事件处置完成后，在演习结束前，应在两个工作日内，梳理出信息安全事件书面报告（报告要求同一级响应报告内容），通过事件上报平台向相关部门进行通报。

子分公司：

子分公司工作组应当在第一时间通过即时通讯群组及电话的形式向事件上报组报告事件情况，并自行完成事件处置。在事件处置完成后，在演习结束前，梳理出信息安全事件书面报告（报告要求同一级响应报告内容），通过事件上报平台向总部事件上报组进行通报。

5.6 事件级别调整

总部：

在进行应急处理过程中，如应急处置组发现事件影响程度及范围不符合初步判定，应及时与技术研判组沟通，同时向护网行动指挥部反馈，由其共同对事件级别进行重新判定。

在总部接到子分公司上报的二级及以上事件后，应由技术研判组对事件级别进行判定，若确认级别为三级及以下事件，则通过事件上报组向子分公司反馈，由子分公司按照新事件级别进行处置。

子分公司：

在进行应急处理过程中，如发现事件影响程度及范围不符合初步判定，应及时对事件级别进行重新判定及处置。

第六章　监测与巡检

6.1 实时监测

总部及各子分公司对演习目标、 重点目标及安全防护设备的报警信息进行实时监测，分析甄别网络中设备被控制的报警和线索信息，并按照应急处置预案进行处置。

监测要求：

护网演习期间进行 7*24 小时不间断监测， 监测发现的可疑信息及时提交技术研判组研判。

监测范围：

监测范围为安全防护设备及演习相关业务系统。

6.2 安全巡检

总部及各子分公司对非演习目标系统、一般设备、互联网暴露设备进行安全巡检，分析甄别异常信息，并按照应急处置预案进行处置。

巡检要求：

总部组及子分公司应急处置组负责对本单位的资产进行巡检， 其中非演习目标系统、互联网暴漏设备每隔 2 小时巡检一次并填写“ 安全巡检记录单 ”，一般设备每隔 4 小时巡检一次并填写“ 安全巡检记录单 ” 。

巡检范围：

巡检范围为非演习目标系统、一般设备、互联网暴露设备。

第七章　应急响应

7.1 事件分级响应

7.1.1　一级事件

由护网行动指挥部根据《 XXXX 集团有限公司网络与信息安全事件应急预案》发布网络安全红色预警及启动应急Ⅰ级响应。

应急处置组向护网行动指挥部响应时间要求：

事件等级	事件进程	跟踪周期和通报时间
一级	未明确被控原因	每隔 30min 通报一次直至被控原因明确
	已明确被控原因	每隔 30min 通报一次直至明确修复期限
	已明确修复期限	每隔 1h 通报一次直至修复结束

7.1.2　二级事件

由护网行动指挥部根据《 XXXX 集团有限公司网络与信息安全事件应急预案》发布网络安全红色预警及启动应急Ⅰ级响应。

应急处置组向护网行动指挥部响应时间要求：

事件等级	事件进程	跟踪周期和通报时间
二级	未明确被控原因	每隔 1h 通报一次直至被控原因明确
	已明确被控原因	每隔 1h 通报一次直至明确修复期限
	已明确修复期限	每隔 2h 通报一次直至修复结束

7.1.3　三级事件

由护网行动指挥部根据《 XXXX 集团有限公司网络与信息安全事件应急预案》发布网络安全橙色预警及启动应急Ⅱ级响应。

应急处置组向护网行动指挥部响应时间要求：

事件等级	事件进程	跟踪周期和通报时间
三级	未明确被控原因	每隔 2h 通报一次直至被控原因明确
	已明确被控原因	每隔 1h 通报一次直至明确修复期限
	已明确修复期限	每隔 2h 通报一次直至修复结束

7.1.4 四级事件

由护网行动指挥部根据《 XXXX 集团有限公司网络与信息安全事件应急预案》发布网络安全黄色预警及启动应急III级响应。

应急处置组向护网行动指挥部响应时间要求：

事件等级	事件进程	跟踪周期和通报时间
四级	未明确被控原因	每隔 2h 通报一次直至被控原因明确
	已明确被控原因	每隔 1h 通报一次直至明确修复期限
	已明确修复期限	每隔 2h 通报一次直至修复结束

7.1.5 五级事件

由护网行动指挥部根据《 XXXX 集团有限公司网络与信息安全事件应急预案》发布网络安全黄色预警及启动应急III级响应。

应急处置组向护网行动指挥部响应时间要求：

事件等级	跟踪周期和通报时间
五级	酌情通报。

7.2 事件分类处置

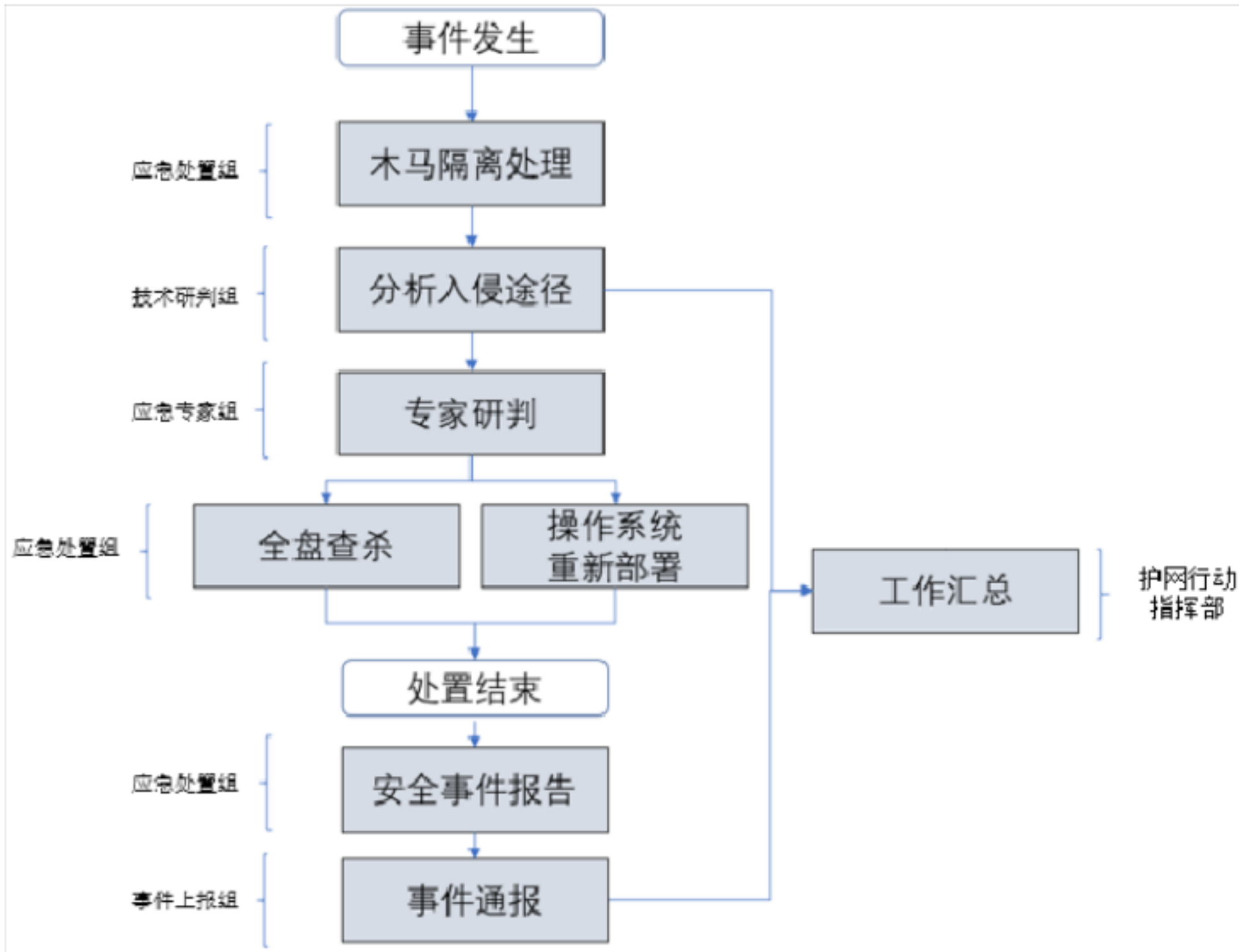
针对具体的攻击事件，总部及子分公司应急处置组应根据不同事件类型，按照以下处置方法进行有效处置。

7.2.1　木马后门事件处置

处置方法：

发现木马后门后，先针对出现木马后门设备进行断网隔离处理，同时将该设备日志进行备份留存分析入侵途径，随后根据总部技术研判组研判结果对操作系统进行重新部署或病毒软件进行全盘查杀。

处置流程：

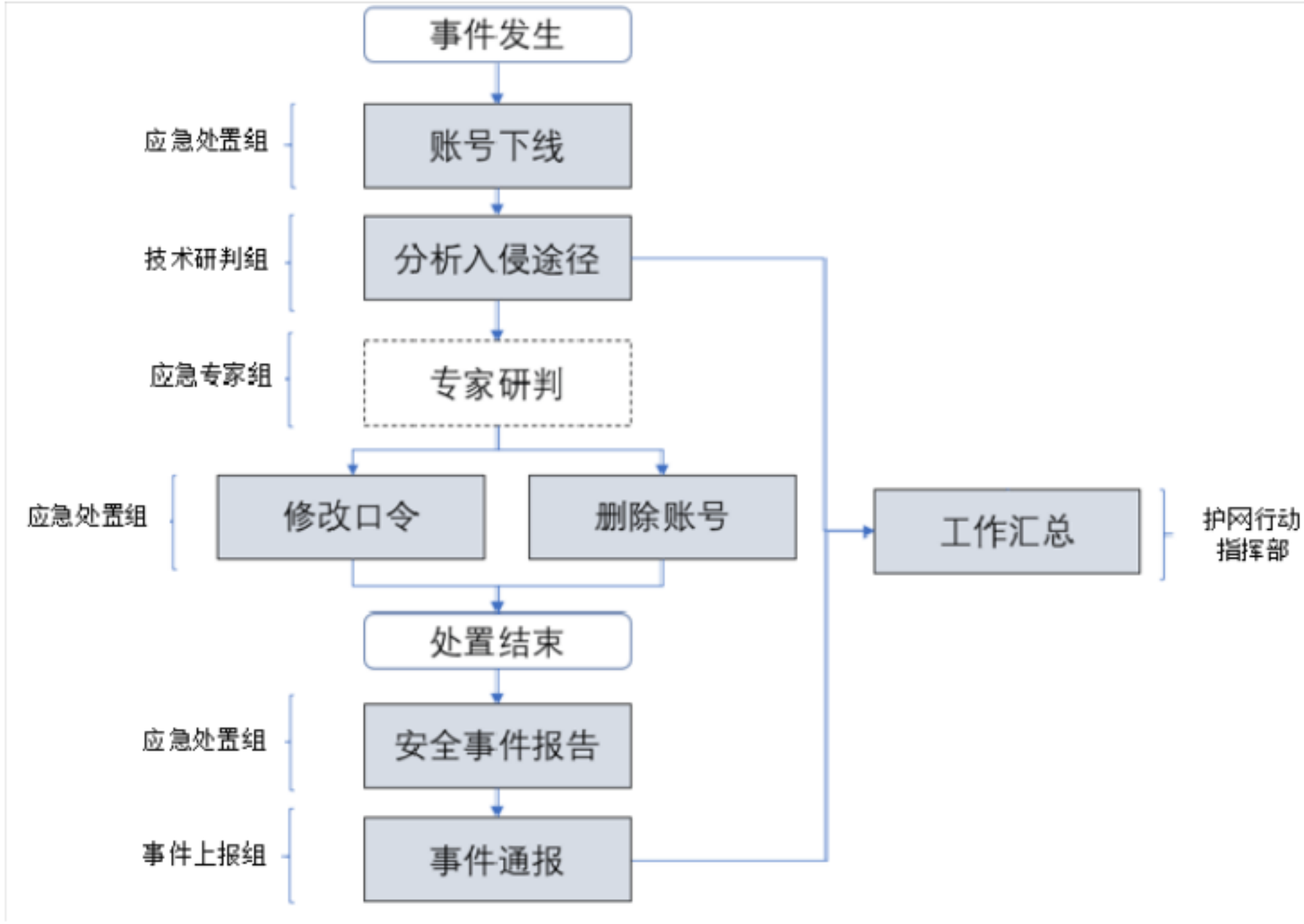


7.2.2　异常登录事件处置

处置方法：

检测到异常登录时，优先将相关账号下线并留存账号相关日志，随后针对问题账号采取修改口令或删除账号等方式进行处理。

处置流程：

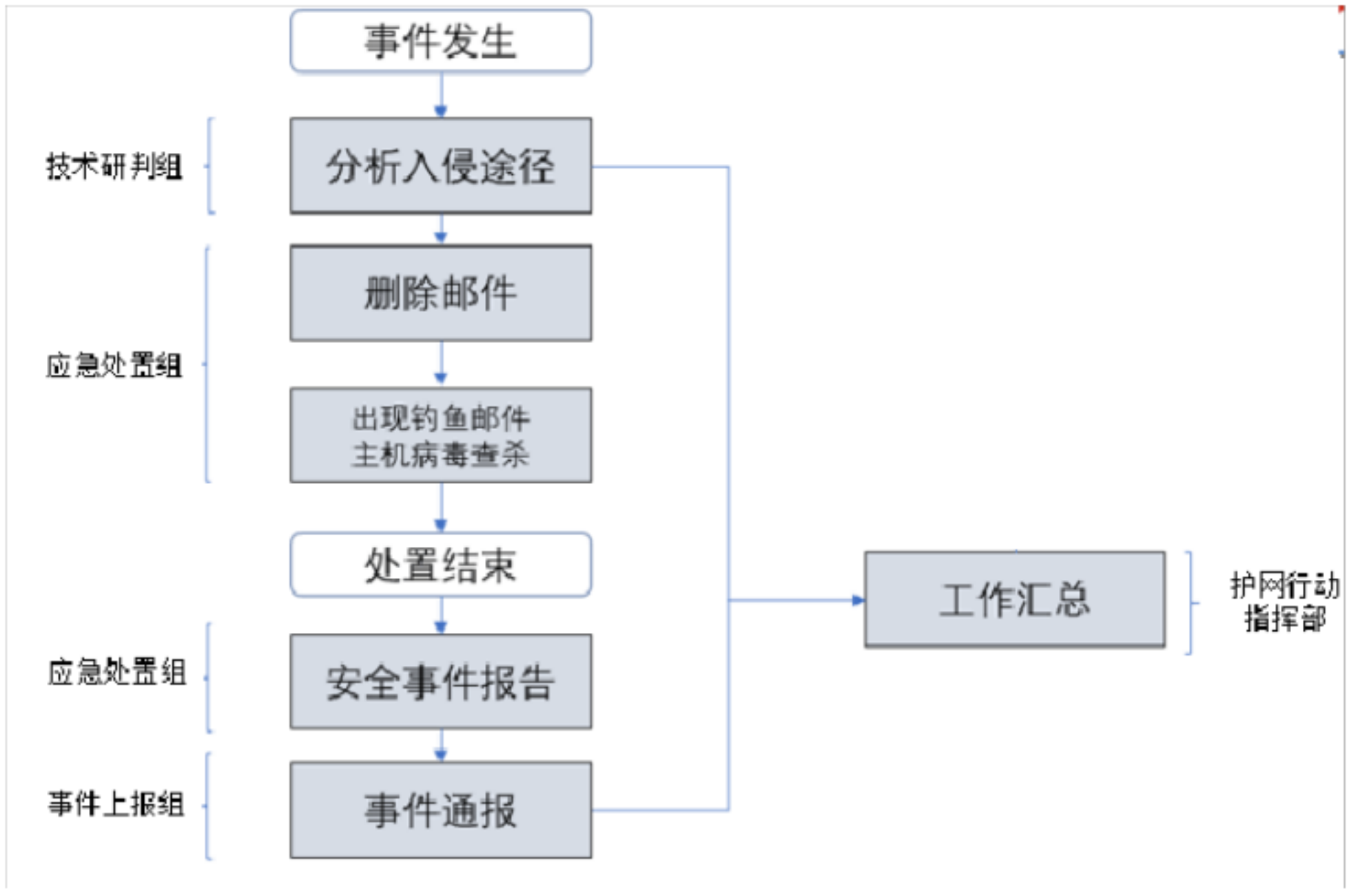


7.2.3 钓鱼邮件事件处置

处置方法：

对邮件内链接仔细核查溯源， 删除相关邮件并对收到钓鱼邮件的主机进行病毒查杀。

处置流程：



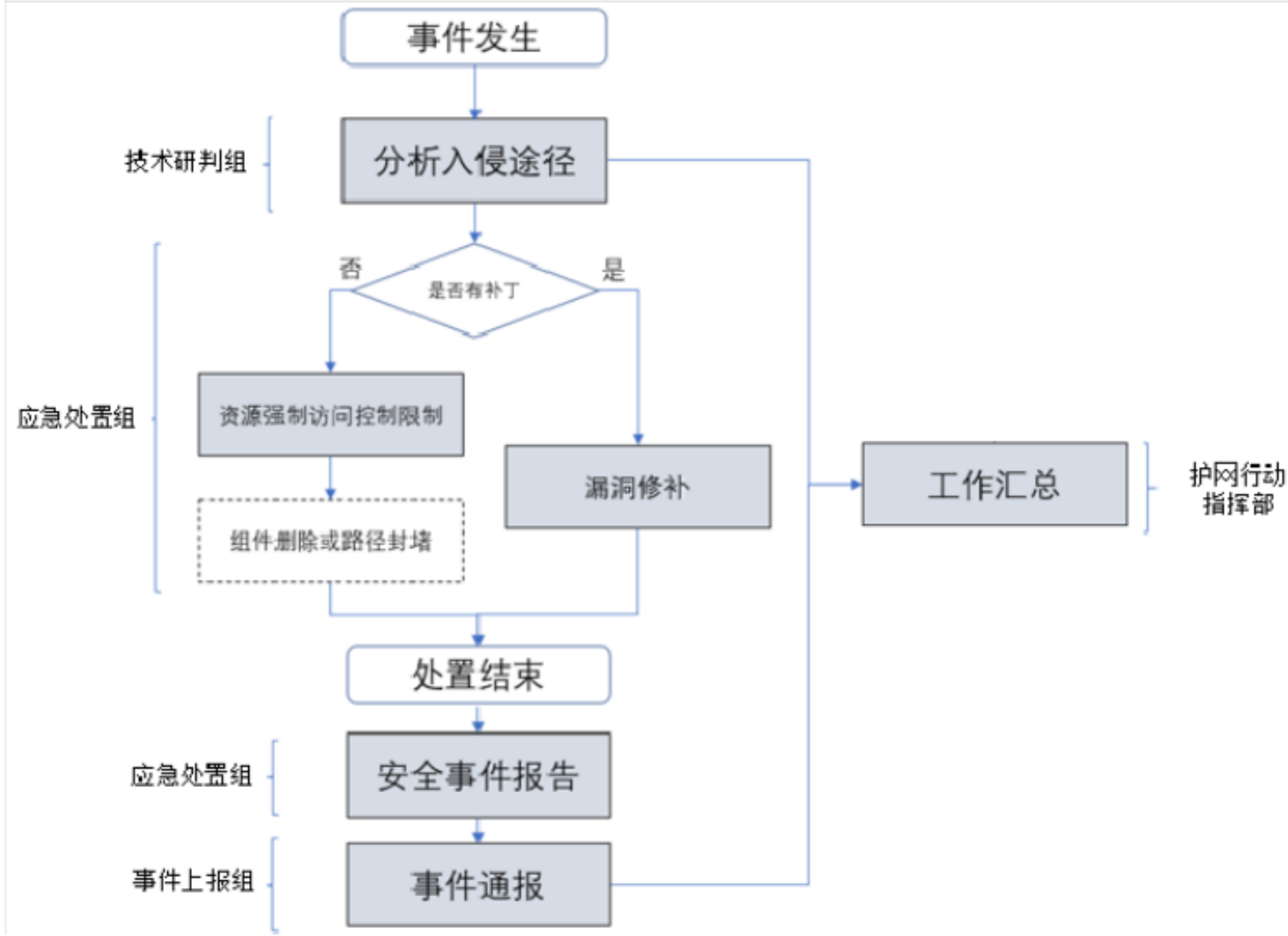
7.2.4　漏洞攻击事件处置

处置方法：

1)　无补丁情况，采取“ 白名单 ” 策略，基于对自身业务系统路径架构的有效管理，对正常服务的路径进行加白，在主机配置强制访问控制策略，对进程、驱动等资源进行强制管理；针对特定漏洞进行组件删除和路经封堵等策略进行防护，随时关注补丁完成情况及时完成补丁修补工作。

2)　有补丁情况，加强信息系统漏洞巡检和补丁修复，采取相应技术手段，检查漏洞修复情况，并督促整改。

处置流程：

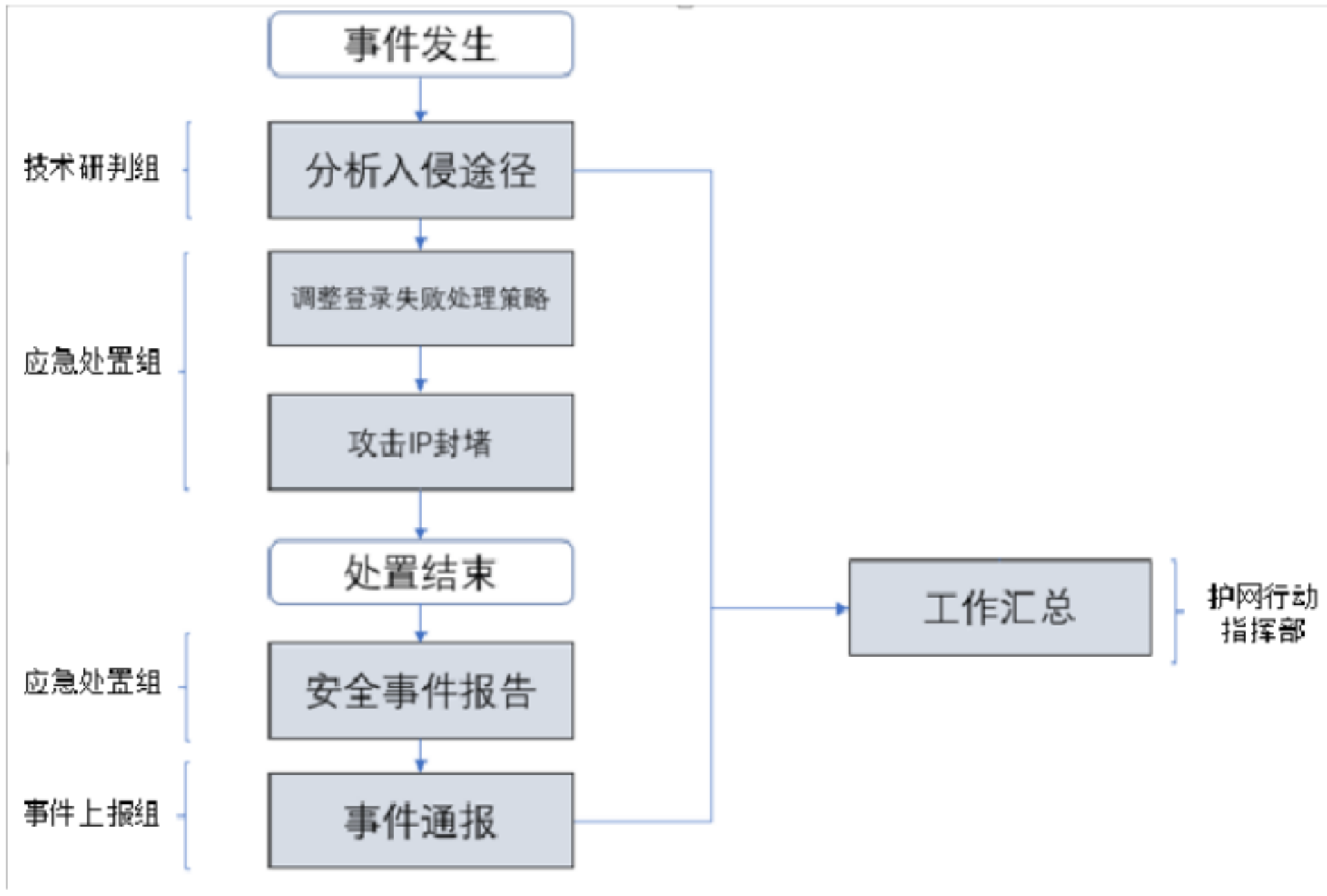


7.2.5　暴力破解事件处置

处置方法：

针对产生暴力破解事件的相关攻击　IP 进行有效封锁，并关注出现被暴力破解事件系统运行状态。

处置流程：

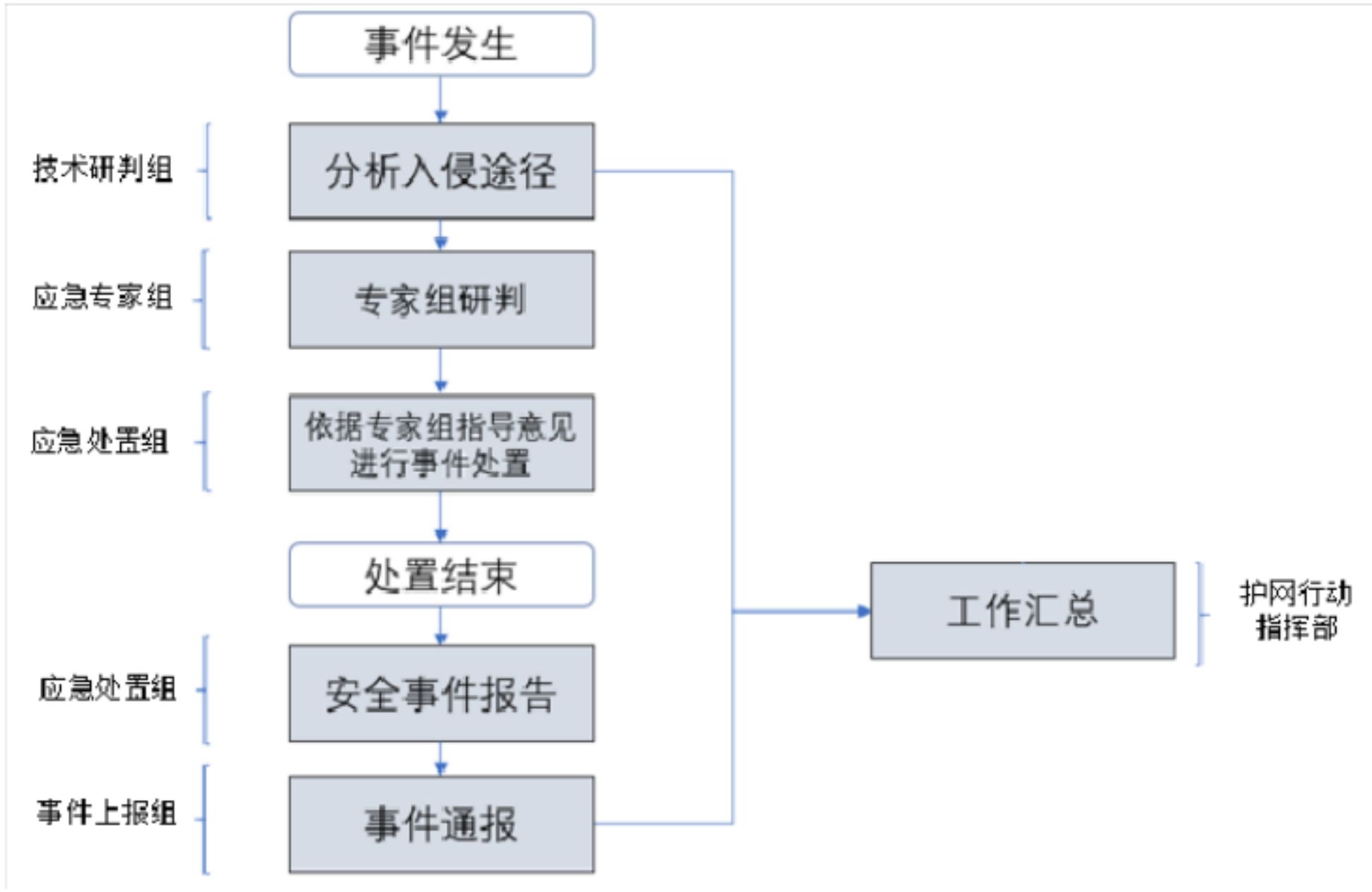


7.2.6　数据窃取事件处置

处置方法：

组织技术研判组对失窃数据内容及范围进行研判，根据研判结果向相关业务主管部门进行通报，相关业务主管部门在收到通报后，应在第一时间根据技术研判组研判建议采取相关处置措施，防止事件升级。

处置流程：

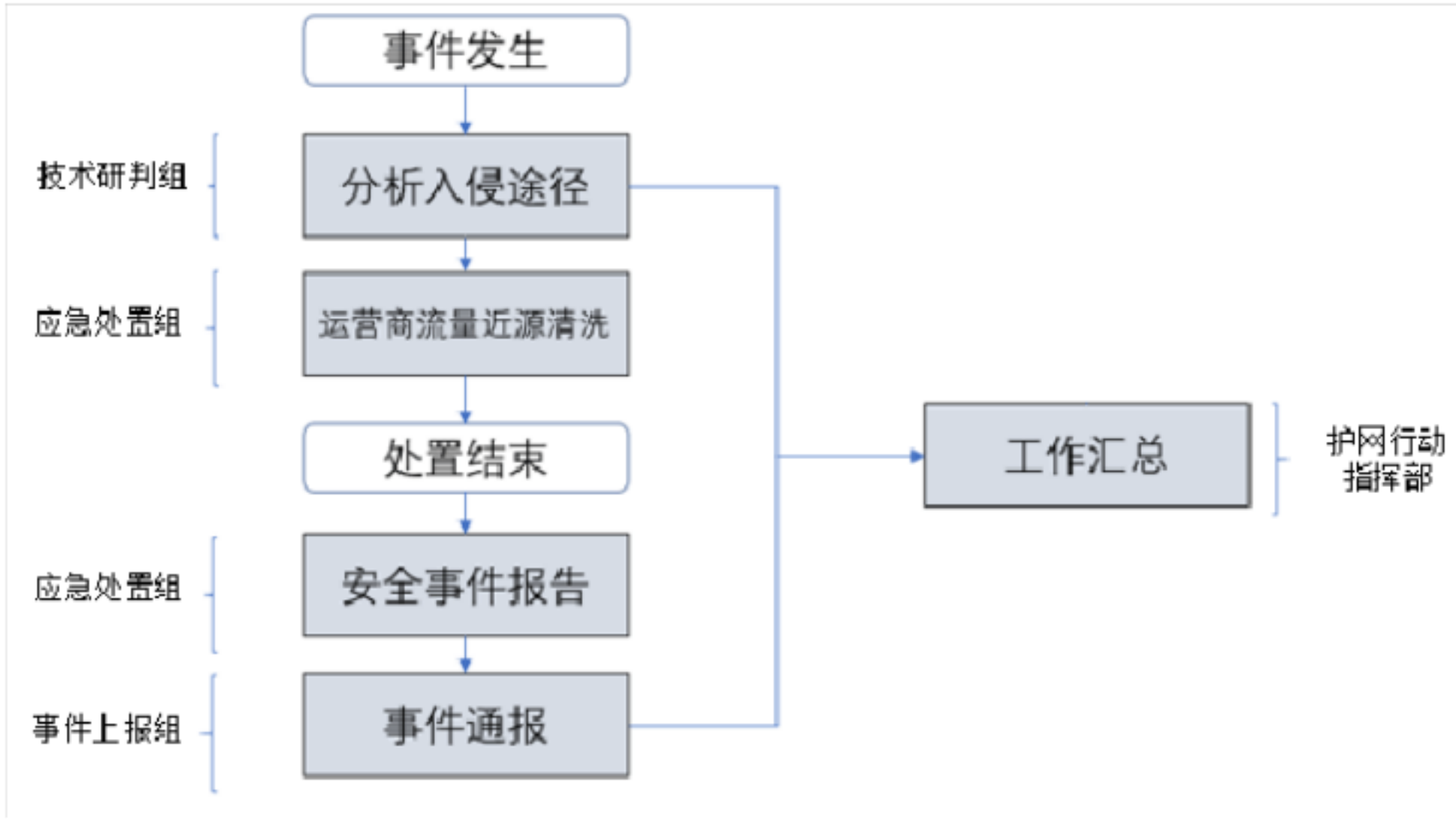


7.2.7　拒绝服务事件处置

处置方法：

借助互联网出口运营商防护资源实现拒绝服务流量近源清洗，并关注出现拒绝服务攻击事件系统的运行状态。

处置流程：



护网行动相关工作小组从外部情报、 日常监控、业务部门或其他途径得到报警信息，及时进行分析判断。如属于日常运维故障，则由相关运维人员进行处理；如判断为信息安全事件，信息安全工作小组分析事件影响， 判断事件级别， 填写信息安全事件报告 （报告模板参见附件二）。

（1）III级及IV级信信息安全事件对信息系统运行效率影响较小， 信息安全工作小组可在应急处置完毕后向信息安全工作小组组长汇报。

（2）Ⅰ级及Ⅱ级信息安全事件对信息系统运行效率影响较大， 信息安全工作小组组长立即向信息安全领导小组组长进行报告，并启动信息安全专项应急预案。信息安全领导小组分析信息安全事件影响，确认事件级别，对应急处置过程进行监管。对于需要上报外部监管机构的信息安全事件，经信息安全领导小组组长审批通过后进行上报。

(3)信息安全工作小组如需公安机关或国家互联网应急中心等国家机构协助解决信息安全事件，由信息安全工作小组组长提出协助处置申请，信息安全领导小组分析协助处置请求，协调相关机构，协助集团公司进行处置。

事件报告流程如下所示：

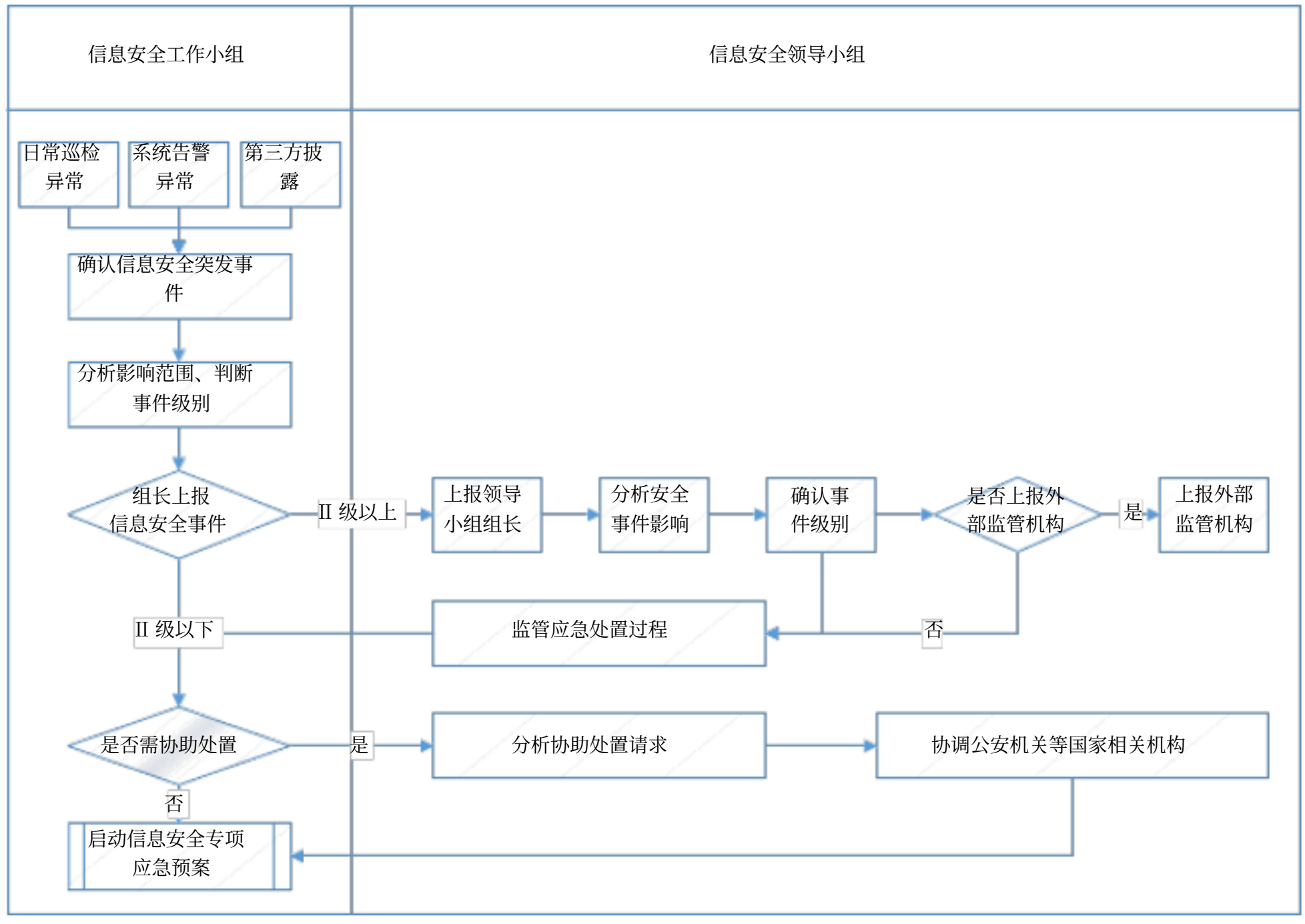


图 1 事件报告流程图

7.3 事件应急关闭

在完成事件处置后，应急处置小组将处置结果上报护网行动指挥部，由护网行动指挥部通过事件上报组发布指令，宣布事件处置工作结束。

附件

附件一：集团公司护网行动信息安全应急组织机构成员名单

组织机构	角色	部门	姓名	手机	邮箱	备注
护网行动指挥部	组长					
	副组长					
	组员					
	组员					
	组员					
	组员					
	组员					
应急专家组						
安全监控组						
技术研判组						

组织机构	角色	部门	姓名	手机	邮箱	备注
应急处置组						
事件上报组						