安全事件闭环流程管理

2019护网专项培训

NSFOCUS

CONTENTS

目 录

01

什么是安全事件闭环管理

NSFOCUS

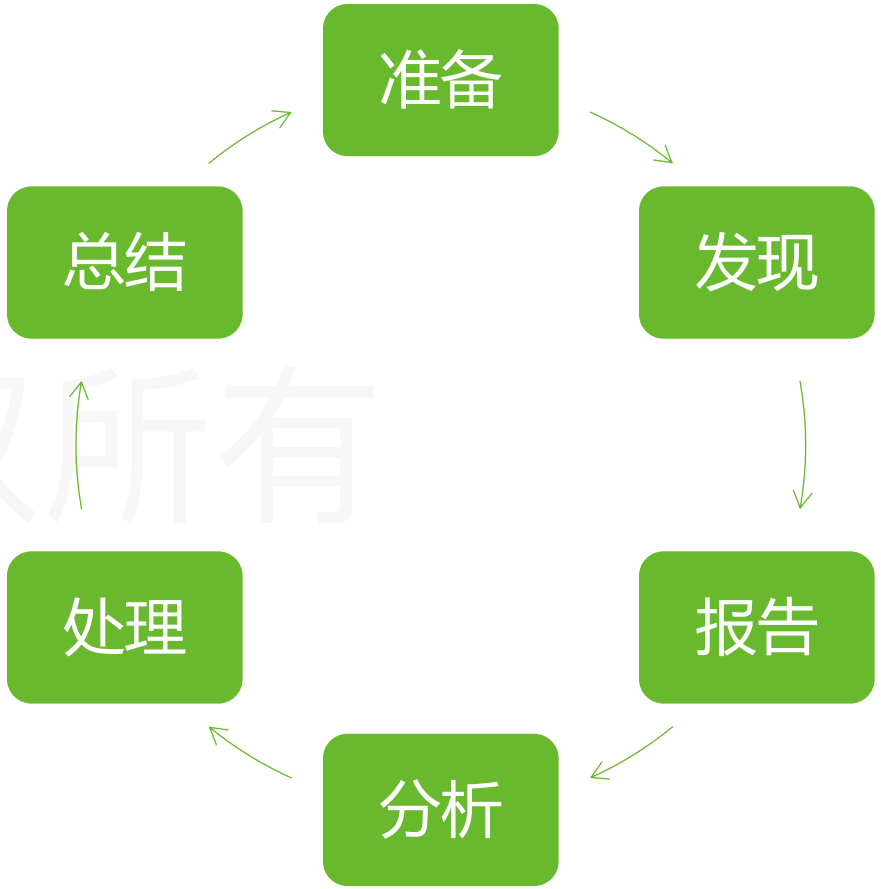
安全事件闭环管理概述

定义：

为高效解决护网行动中遇到安全事件，所涉及到的闭环管理流程，包括事前准备、事件发现、事件报告、事件分析、事件处理、事件总结

目的：

结合实际护网场景，以最快的速度发现并处置安全事件，做好安全事件闭环流程管理。



02

怎么做 安全事件闭环管理

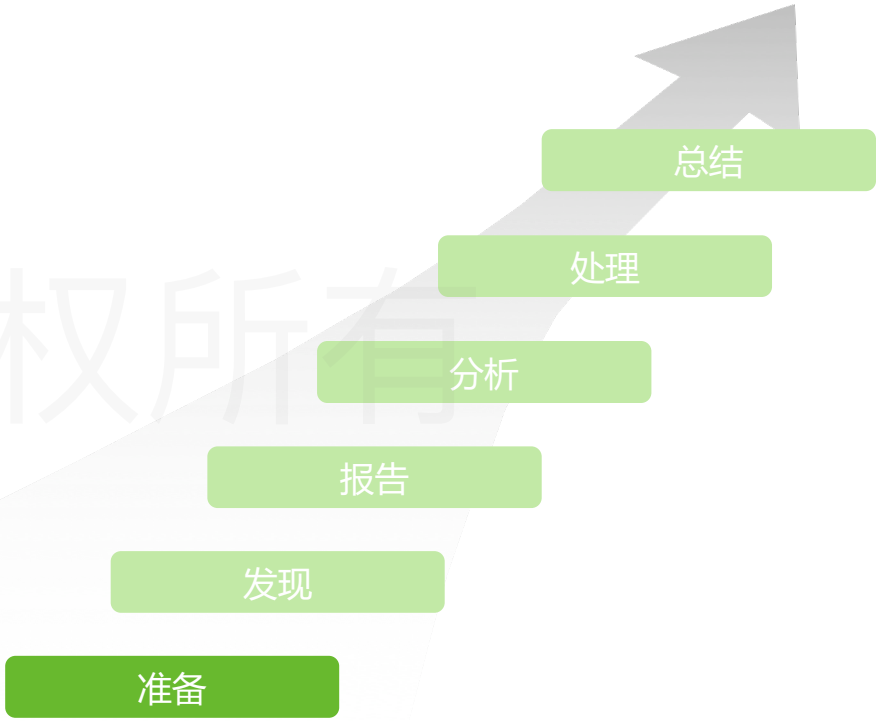
NSFOCUS

安全事件闭环流程

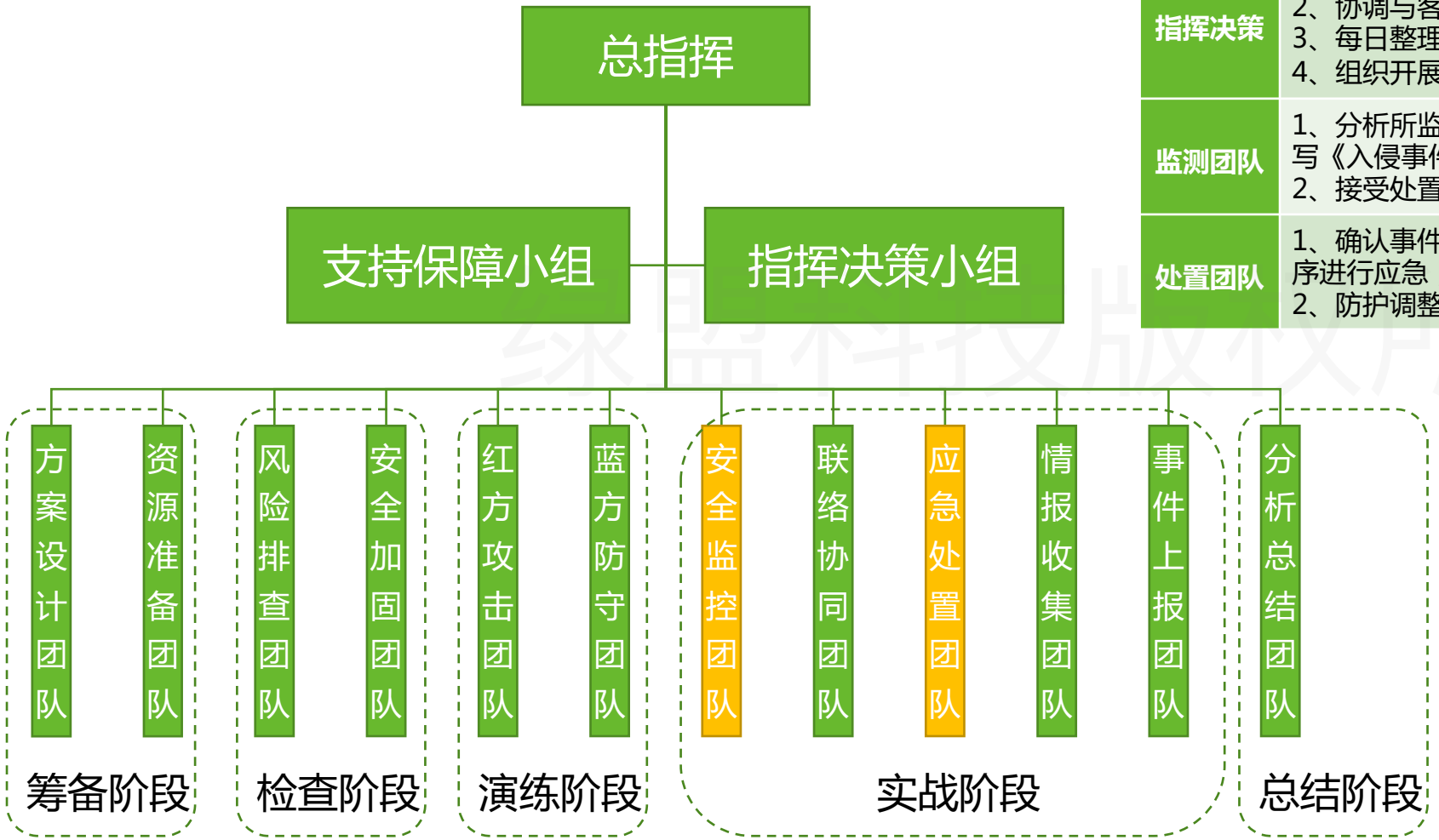
第一阶段-准备

准备阶段是应对应急响应事件发生而采取的技术和管理措施，人员、流程及工具

1. **应急响应管理**
   团队组建、事件定级、应急响应流程等
2. **应急响应技术**
   安全防护/检测设备、备份恢复措施、应急响应工具包等
3. **安全培训**
   为提高技术人员应急响应技能、熟悉应急预案而制定的安全培训



团队组建



角色	职责
指挥决策	1、协调监测组和处置组之间的工作； 2、协调与客户业务人员及维护人员对接工作； 3、每日整理日报及次日工作计划； 4、组织开展总结复盘会议并把关总结报告文档。
监测团队	1、分析所监测的设备及平台产生的安全日志，挖掘入侵事件，填写《入侵事件分析报告》提交给处置组。 2、接受处置组的防护策略调整方案，并调整防护策略。
处置团队	1、确认事件是否由正常业务引起，对真实攻击根据事件定级按次序进行应急，完成后编写提交《应急处置报告》； 2、防护调整策略输出到监测组，配合业务部门修补漏洞。

攻击行为

事件分级

- 根据攻击者活动提取出特征：扫描资产端口，猜解认证接口弱口令，挖掘web应用漏洞，扫描管理地址，对服务存在的高危漏洞尝试利用，发送钓鱼邮件，并根据特征制定入侵事件定级表：

序号	事件类型	事件等级
1	扫描事件	4级事件
2	爆破事件	3级事件
3	钓鱼事件	
4	高危漏洞利用事件	2级事件
5	木马事件	1级事件
6	内网扫描事件	
7	内网爆破事件	
8	内网高危漏洞利用事件	

安全事件闭环流程

第二阶段-发现

发现阶段确认是否有安全事件发生，及时评估造成的危害、影响范围、事件定级等，然后根据评估结果通知相关的人员进入应急的流程

1. **事件确认**
   根据安全设备告警、用户反馈、异常现象等确认是否发生安全事件及事件类型

2. **影响分析**
   确认事件影响范围、受影响系统、主机、事件定级

安全事件闭环流程

第三阶段-报告

根据发现的异常现象或攻击告警，填写事件上报表，并发送相关团队

1 **事件上报**
填写《事件上报表》，发送至指挥及事件处置团队

2 **启动应急响应**
按照应急响应管理制度及预案，启动应急响应流程

序号	事件类型	攻击源IP	攻击源地理位置	攻击目标IP	目标系统	攻击次数	报警设备	上报人	攻击结果	攻击起始时间	攻击结束时间	处置结果
1												
2												

安全事件闭环流程

第四阶段-分析

本阶段主要任务是通过事件分析查明事件原因及危害，对攻击路径进行分析并溯源

1 **入侵分析**
通过对受影响的主机、网络进行详细排查，确认问题原因，常见排查内容包括：进程、端口、服务、注册表、账号、安全日志等

2 **攻击溯源**
根据入侵分析结果，确认是否可以定位攻击源，并进行进一步分析

安全事件闭环流程

第五阶段-处理

本阶段主要任务是对确认的安全事件进行处置，降低事件影响、避免安全事件的扩散和安全事件对受害系统的持续性破坏

1. **遏制措施**
   通过安全设备对相关IP、端口、URL等进行访问控制、优化安全设备规则阻断如扫描、漏洞利用等攻击

2. **根除措施**
   对相关漏洞进行修复、包括操作系统漏洞、应用漏洞等

3. **恢复措施**
   木马后门清除、账号密码重置、服务端口恢复、重新部署应用等

NSFOCUS

安全事件闭环流程

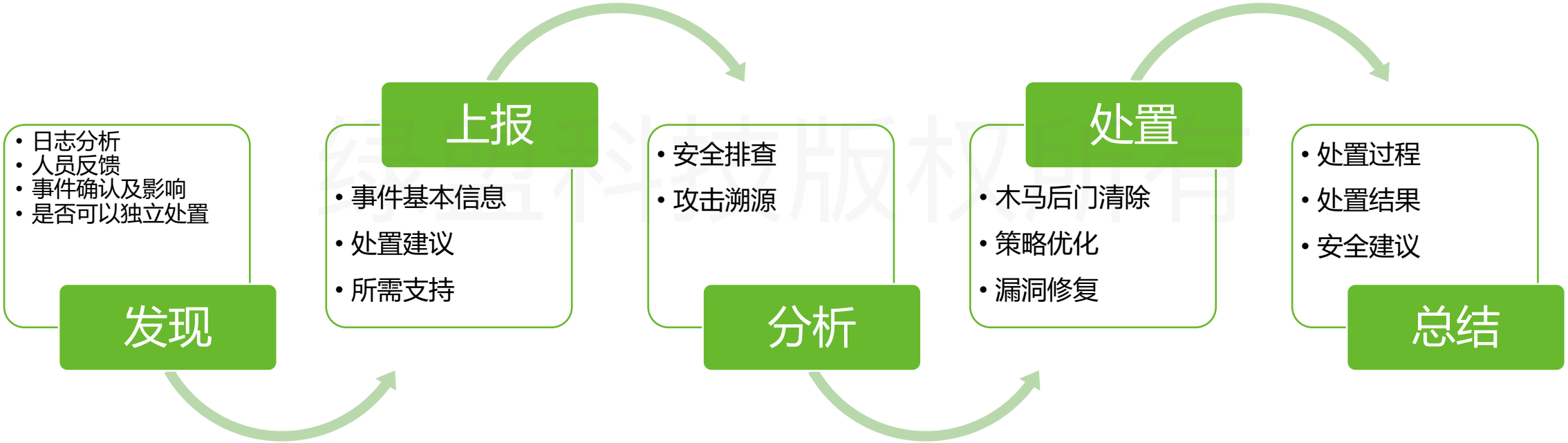
第六阶段-总结

对安全事件进行详细的总结和回顾，并出具报告，内容包括事件现象、发生时间、处理人员、处置过程、结论建议等

1. **事件总结**
   对整个安全事件处置过程进行详细记录和分析，出具《应急处置报告单》

2. **事件上报**
   对指挥组进行事件上报

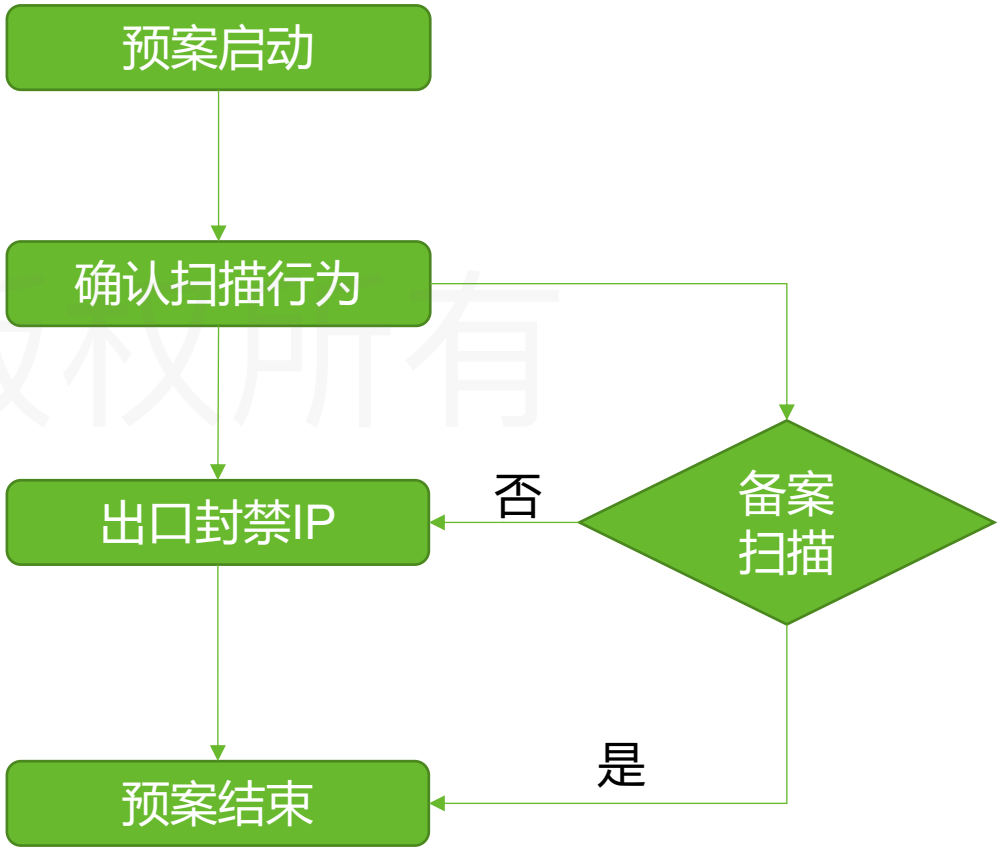
总结


发现
• 日志分析
• 人员反馈
• 事件确认及影响
• 是否可以独立处置
上报
• 事件基本信息
• 处置建议
• 所需支持
分析
• 安全排查
• 攻击溯源
处置
• 木马后门清除
• 策略优化
• 漏洞修复
总结
• 处置过程
• 处置结果
• 安全建议

四级事件处置流程

事件现象及特征

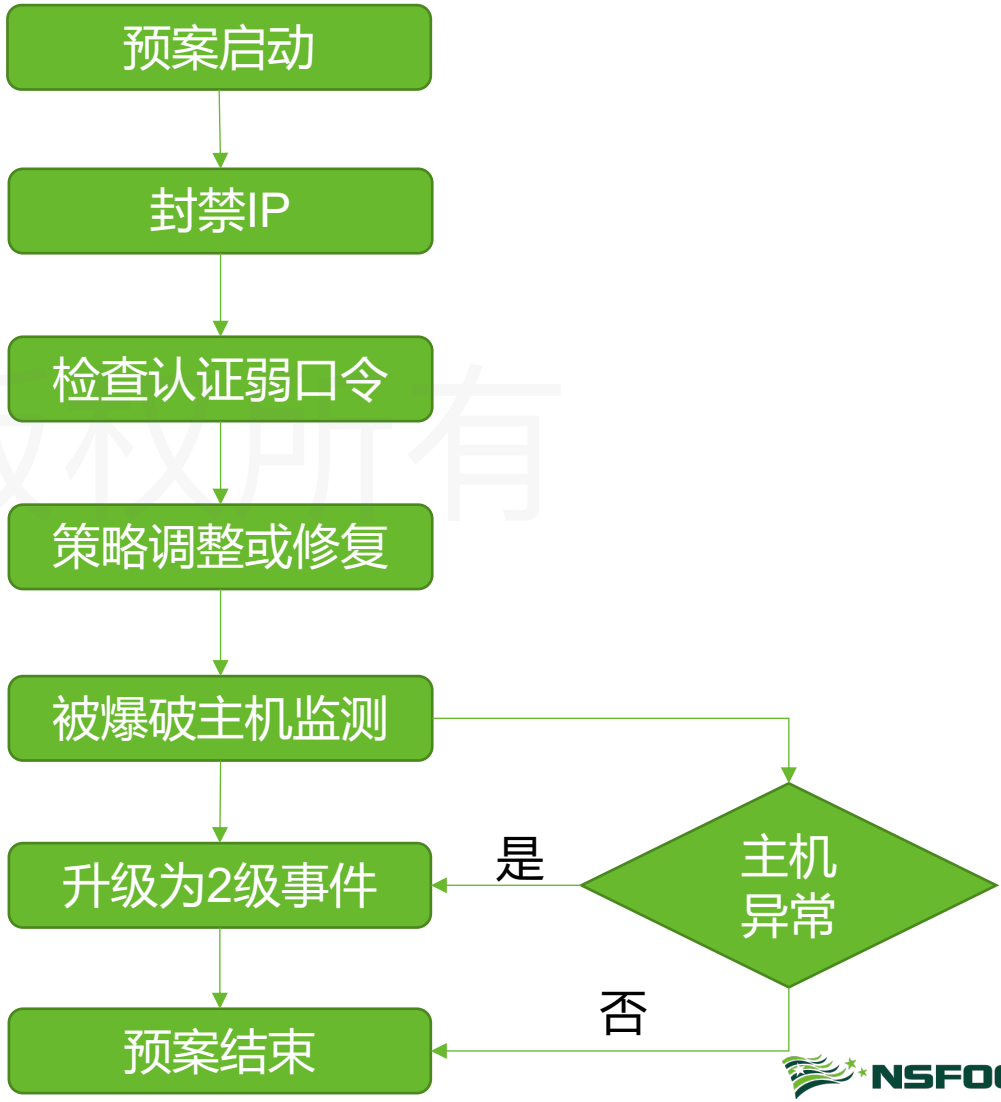
- 安全设备告警存在扫描行为，包括WEB漏洞扫描及系统漏洞扫描
- 安全设备告警短时间内产生大量攻击探测行为



三级事件处置流程

事件现象及特征

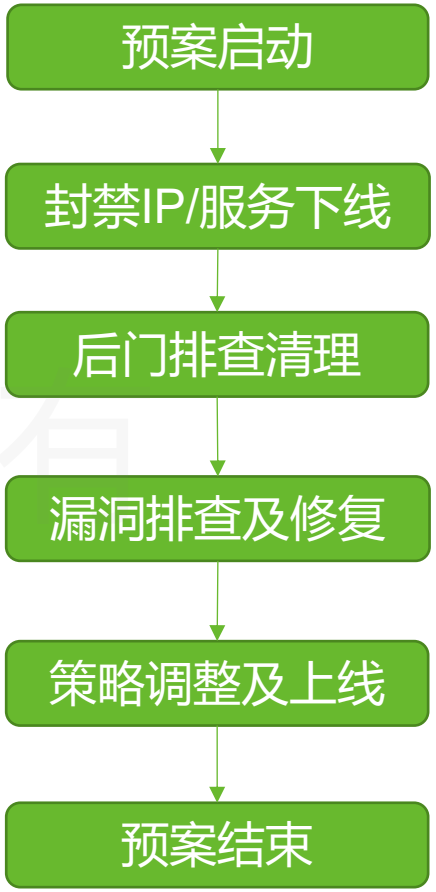
- 认证日志产生大量且频率较高的错误认证记录，常见如SSH、SMB、RDP、HTTP、HTTPS等。



二级事件处置流程

事件现象及特征

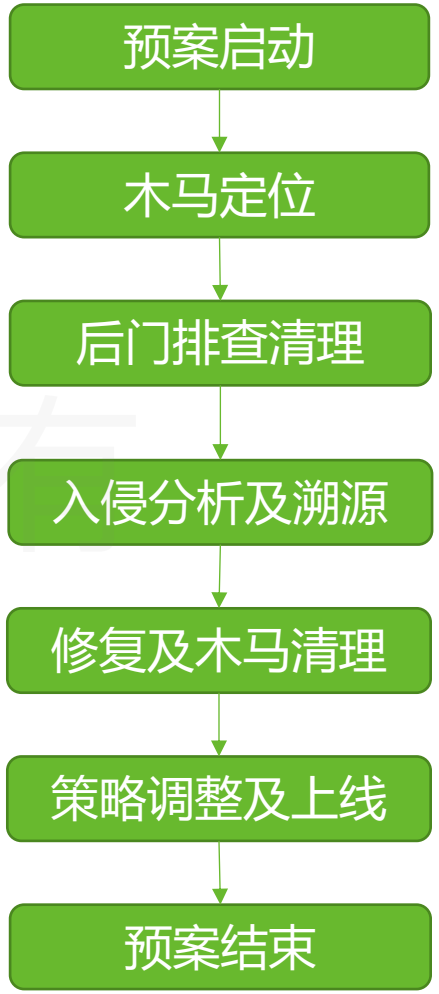
- 远程代码执行漏洞利用、数据相关触发安全设备告警
- 主机存在漏洞利用痕迹
- 数据库存在大量非正常操作



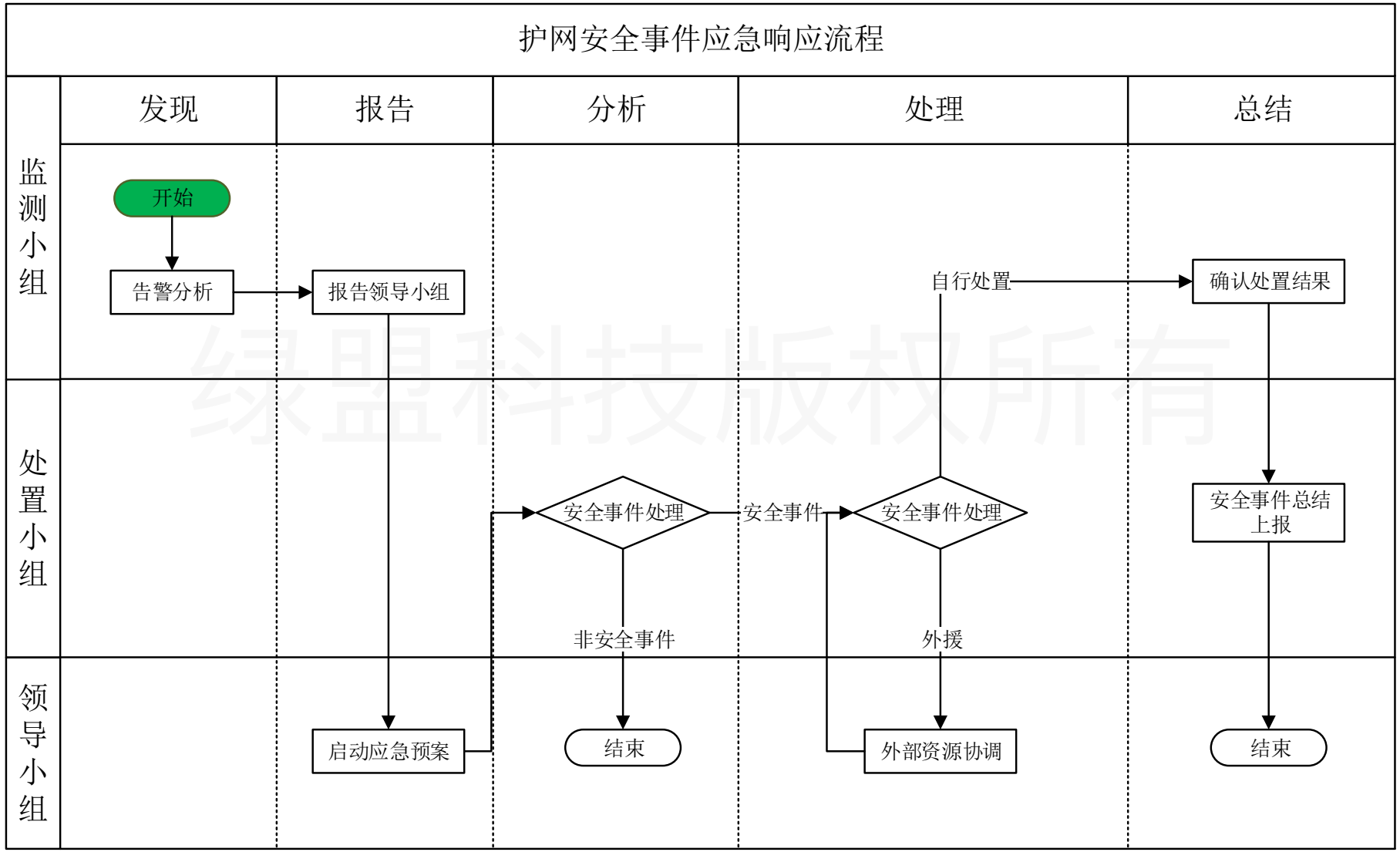
一级事件处置流程

事件现象及特征

- 主机存在与外部主机CC通信或异常连接
- 公网主机上出现webshell木马文件
- 来源地址为内网IP的对其他主机的告警连接，漏洞利用，口令破解，扫描行为



安全事件处置流程



03

常见问题分析

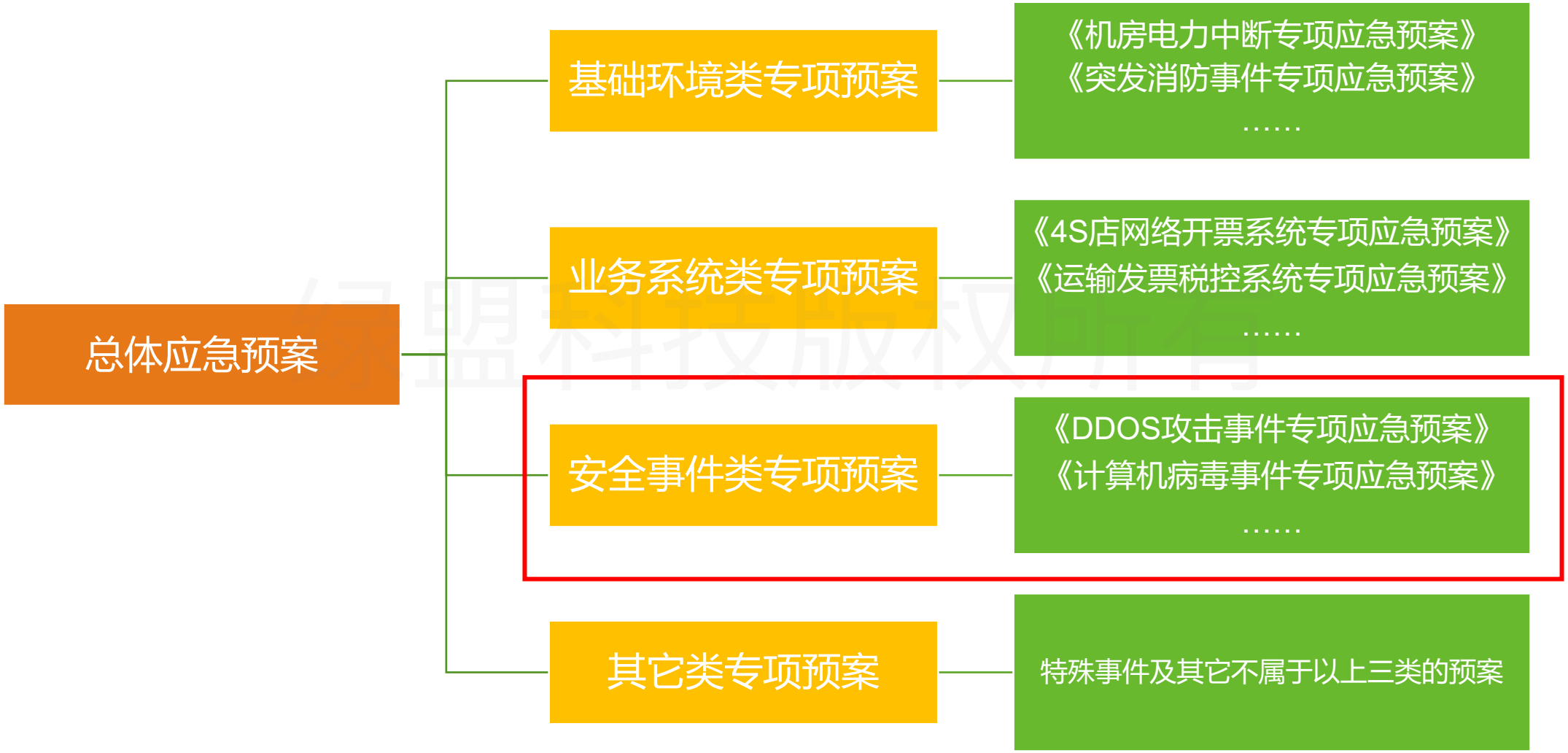
本次培训目的是什么？

- 了解安全事件闭环管理流程及相关活动；
- 提高安全事件处置规范性及效率；
- 明确护网期间安全事件处置工作内容；
- 更好的协助客户及远程团队完成安全事件处置

什么是应急预案？

- 是法律法规的必要补充，是从常态向非常态转变的工作方案，目的是在既有的制度安排下尽量提高应急反应速度。
- 对应急组织体系与职责、人员、技术、指挥与协调等预先做好具体安排，明确在突发事件发生之前，发生过程中以及刚刚结束之后，谁来做，做什么，何时做，以及相应的处置方法和资源准备。
- 重点规范必要的监测预警和必要的应急恢复。
- 是立足于现有资源的应对方案，主要使应急资源找得到、调得好、用得好，而不是能力建设的实施方案。

应急预案分类



如果客户没有应急预案怎么办？

常见表现：

- 内部人员分工不明确，可能只有一个接口人；
- 无安全事件处置、汇报流程；
- 无安全事件报告、处置模板；

做好几个工作：

- 1、安全事件监控和收集；
- 2、对安全事件进行初步分析和确认；
- 3、确认是否可以独立处置；
- 4、详细做好事件记录；
- 5、及时汇报接口人；
- 6、事件处置或协助处置；
- 7、完成安全事件处置报告；

安全事件无法解决怎么办？

- 事件现象：异常登录、发现webshell、数据泄露等等
- 事件类型：远程代码执行、弱口令攻击、任意文件上传等等
- 发生时间：事件发生的时间
- 影响目标：业务系统、主机
- 攻击结果：包括攻击者目前所得权限、当前的具体损失（有形和无形资产）、具体哪些数据被窃、被毁、被篡改等。
- 客户需求：遏制、排查、溯源
- 处置方式：远程、现场
- 日志收集：中间件日志、系统日志、安全设备日志
- 权限需求：目标服务器登录用户名、密码
- 联系人：客户接口人、系统/主机管理员

应急处置报告单

附录C：应急处置报告单

单位名称：　　报告时间：　　年　月　日　时　分

应急处置报告单			
报告人		联系方式	
信息系统名称		主要用途	
监控团队上报信息			
主要处理过程及结果			
存在问题及建议			
总体组处理意见			
总体组组长签字：			

谢谢！

NSFOCUS