网络安全应急响应概述

1.网络安全应急响应基本概念

应急响应，其英文是Incident Response或EmergencyResponse，通常是指一个组织为了应对各种意外事件的发生所做的准备，以及在事件发生后所采取的措施。其目的是减少突发事件造成的损失，包括人民群众的生命、财产损失，国家和企业的经济损失，以及相应的社会不良影响等。

应急响应工作主要包括以下两方面：

第一，未雨绸缪，即在事件发生前先做好准备

例如，开展风险评估，制订安全计划，进行安全意识的培训，以发布安全通告的方法进行预警，以及各种其他防范措施。

第二，亡羊补牢，即在事件发生后采取的响应措施，其目的在于把事件造成的损失降到最小

这些行动措施可能来自人，也可能来自系统。例如，在发现事件后，采取紧急措施，进行系统备份、病毒检测、后门检测、清除病毒或后门、隔离、系统恢复、调查与追踪、入侵取证等一系统操作。

2.网络安全应急响应的能力

1）数据采集、存储和检索能力

（1）能对全流量数据协议进行还原；

（2）能对还原的数据进行存储；

（3）能对存储的数据快速检索。

2）事件发现能力

（1）能发现高级可持续威胁（Advanced PersistentThreat，APT）攻击；

（2）能发现Web攻击；

（3）能发现数据泄露；

（4）能发现失陷主机；

（5）能发现弱密码及企业通用密码；

（6）能发现主机异常行为。

3）事件分析能力

（1）能进行多维度关联分析；

（2）能还原完整杀伤链；

（3）能结合具体业务进行深度分析。

4）事件研判能力

（1）能确定攻击者的动机及目的；

（2）能确定事件的影响面及影响范围；

（3）能确定攻击者的手法。

5）事件处置能力

（1）能在第一时间恢复业务正常运行；

（2）能对发现的病毒、木马进行处置；

（3）能对攻击者所利用的漏洞进行修复；

（4）能对问题机器进行安全加固。

6）攻击溯源能力

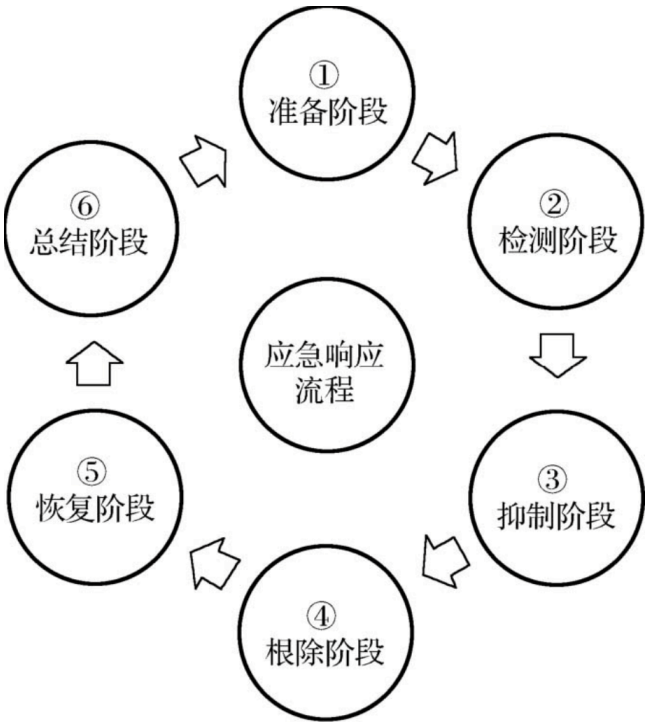
（1）具备安全大数据能力；

（2）能根据已有线索（IP地址、样本等）对攻击者的攻击路径、攻击手法及背后组织进行还原。

3.网络安全应急响应的方法

PDCERF方法最早于1987年提出，该方法将应急响应流程分成准备阶段、检测阶段、抑制阶段、根除阶段、恢复阶段、总结阶段。根据应急响应总体策略为每个阶段定义适当的目的，明确响应顺序和过程。

但是，PDCERF方法不是安全事件应急响应的唯一方法。在实际应急响应过程中，不一定严格存在这6个阶段，也不一定严格按照这6个阶段的顺序进行。但它是目前适用性较强的应急响应通用方法。



1）准备阶段

准备阶段以预防为主。主要工作涉及识别机构、企业的风险，建立安全政策，建立协作体系和应急制度。按照安全政策配置安全设备和软件，为应急响应与恢复准备主机。依照网络安全措施，进行一些准备工作，例如，扫描、风险分析、打补丁等。如有条件且得到许可，可建立监控设施，建立数据汇总分析体系，制定能够实现应急响应目标的策略和规程，建立信息沟通渠道，建立能够集合起来处理突发事件的体系。

2）检测阶段

检测阶段主要检测事件是已经发生的还是正在进行中的，以及事件产生的原因。确定事件性质和影响的严重程度，以及预计采用什么样的专用资源来修复。选择检测工具，分析异常现象，提高系统或网络行为的监控级别，估计安全事件的范围。通过汇总，查看是否发生了全网的大规模事件，从而确定应急等级及其对应的应急方案。

一般典型的事故现象包括：

（1）账号被盗用；

（2）骚扰性的垃圾信息；

（3）业务服务功能失效；

（4）业务内容被明显篡改；

（5）系统崩溃、资源不足。

3）抑制阶段

抑制阶段的主要任务是限制攻击/破坏波及的范围，同时也是在降低潜在的损失。所有的抑制活动都是建立在能正确检测事件的基础上的，抑制活动必须结合检测阶段发现的安全事件的现象、性质、范围等属性，制定并实施正确的抑制策略。抑制策略通常包含以下内容：

（1）完全关闭所有系统；

（2）从网络上断开主机或断开部分网络；

（3）修改所有的防火墙和路由器的过滤规则；

（4）封锁或删除被攻击的登录账号；

（5）加强对系统或网络行为的监控；

（6）设置诱饵服务器进一步获取事件信息；

（7）关闭受攻击的系统或其他相关系统的部分服务。

4）根除阶段

根除阶段的主要任务是通过事件分析找出根源并彻底根除，以避免攻击者再次使用相同的手段攻击系统，引发安全事件。并加强宣传，公布危害性和解决办法，呼吁用户解决终端问题。加强监测工作，发现和清理行业与重点部门问题。

5）恢复阶段

恢复阶段的主要任务是把被破坏的信息彻底还原到正常运作状态。确定使系统恢复正常的需求内容和时间表，从可信的备份介质中恢复用户数据，打开系统和应用服务，恢复系统网络连接，验证恢复系统，观察其他的扫描，探测可能表示入侵者再次侵袭的信号。一般来说，要想成功地恢复被破坏的系统，需要干净的备份系统，编制并维护系统恢复的操作手册，而且在系统重装后需要对系统进行全面的安全加固。

6）总结阶段

总结阶段的主要任务是回顾并整合应急响应过程的相关信息，进行事后分析总结和修订安全计划、政策、程序，并进行训练，以防止入侵的再次发生。基于入侵的严重性和影响，确定是否进行新的风险分析，给系统和网络资产制作一个新的目录清单。这一阶段的工作对于准备阶段工作的开展起到重要的支持作用。总结阶段的工作主要包括以下3方面的内容：

（1）形成事件处理的最终报告；

（2）检查应急响应过程中存在的问题，重新评估和修改事件响应过程；

（3）评估应急响应人员相互沟通在事件处理上存在的缺陷，以促进事后进行更有针对性的培训。

4.网络安全应急响应现场处置流程

在日常工作中遇到更多的是在事件发生后进行的问题排查及溯源。常见网络安全应急响应场景有勒索病毒、挖矿木马、Webshell、网页篡改、DDoS攻击、数据泄露、流量劫持，如图所示。

常见网络安全应急响应场景在现场处置过程中，先要确定事件类型与时间范围，针对不同的事件类型，对事件相关人员进行访谈，了解事件发生的大致情况及涉及的网络、主机等基本信息，制定相关的应急方案和策略。随后对相关的主机进行排查，一般会从系统排查、进程排查、服务排查、文件痕迹排查、日志分析等方面进行，整合相关信息，进行关联推理，最后给出事件结论。网络安全应急响应分析流程如图所示。