

应急响应处置使用指南

1.概述应急响应处置是指在发生安全事件时，采取的一系列措施和行动，以识别、评估、控制和恢复受影响的系统。这包括收集信息、判断事件类型、深入分析、清理处置和产出报告等步骤。

2.核心组成应急响应处置通常包括以下核心组成部分：

- 信息收集：收集客户信息和受影响主机信息，包括样本。
- 事件分类：判断事件的性质，如勒索、挖矿、断网或 DoS 攻击等。
- 深入分析：包括日志分析、进程分析、启动项分析和样本分析。
- 清理处置：采取行动杀掉恶意进程，删除恶意文件，打补丁或修复文件。
- 报告产出：整理并输出完整的安全事件报告。

3.应急响应处置流程

3.1 准备阶段

- 建立应急响应团队：组建专业的应急响应团队，明确成员职责。
- 制定应急响应计划：根据可能的安全事件类型，制定详细的应急响应计划。
- 准备应急响应工具：准备必要的工具和资源，如安全信息和事件管理（SIEM）系统、日志分析工具、威胁情报平台等。

3.2 事件识别

- 监测和报警：通过监控系统发现异常行为，并触发报警。
- 初步评估：对报警进行初步评估，确定是否需要启动应急响应流程。

3.3 信息收集

- 收集日志：收集相关系统的日志，包括系统日志、应用日志和安全设备日志。
- 分析网络流量：分析网络流量，以确定攻击来源和攻击方式。
- 收集样本：收集可疑文件或恶意软件样本，以便进一步分析。

3.4 事件分析

- 判断事件类型：根据收集的信息，判断事件的类型和严重程度。
- 深入分析：进行深入分析，包括恶意软件分析、攻击溯源等。

3.5 事件处置

- 隔离受影响系统：将受影响的系统从网络中隔离，以防止攻击扩散。
- 清除威胁：清除恶意软件，修复被破坏的系统和数据。
- 应用补丁：对系统漏洞打补丁，防止再次受到攻击。

3.6 恢复和重建

- 恢复服务：在确保威胁完全清除后，恢复受影响的服务。
- 重建系统：对于严重受损的系统，可能需要重建系统和数据。

3.7 报告和后续

- 编制报告：编制详细的事件报告，包括事件概述、分析结果和处置措施。
- 后续改进：根据事件分析结果，改进安全措施和应急响应流程。

4.应急响应处置工具

- 日志分析工具：如 Splunk、ELK Stack。
- 威胁情报平台：如 ThreatConnect、Threat Intelligence Platform。
- 安全信息和事件管理（SIEM）系统：如 IBM QRadar、AlienVault USM。
- 恶意软件分析工具：如 Cuckoo Sandbox、Malware Analysis Tool。

5.维护与管理

- 定期培训：定期对应急响应团队进行培训，提高他们的技能和知识。
- 审计和合规：确保应急响应处置活动符合行业标准和法规要求。

- 持续改进：根据每次事件的处置结果，持续改进应急响应流程和工具。

6.应用场景应急响应处置适用于各种规模的组织，特别是那些对信息安全有严格要求的金融机构、医疗机构、教育机构和政府机构。

7.优势

- 快速响应：在安全事件发生时能够快速响应，减少损失。
- 减少风险：通过有效的应急响应处置，降低安全事件对组织的影响。
- 合规性：帮助组织满足各种法规和标准对信息安全的要求。
- 增强信任：提高客户和合作伙伴对组织信息安全管理能力的信任。通过遵循本指南，组织可以有效地进行应急响应处置，确保在安全事件发生时能够迅速采取行动，保护组织的信息资产和业务连续性。