应急响应服务方案

**文档说明**

|  |  |  |  |
| --- | --- | --- | --- |
| 文档负责人 | 黄国平 | 文档版本编号 | 1.0 |
| 起草人 | 黄国平 | 文档起草日期 | 2018.09 |
| 复审人 |  | 复审日期 |  |

**版本控制**

|  |  |  |  |
| --- | --- | --- | --- |
| 版本号 | 版本日期 | 创建/修订人 | 说明 |
| 1.0 | 2018.9.11 | 黄国平 | 文档创建 |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**版权声明**

本文档本文件中出现的任何文字叙述、文档格式、插图、照片、方法、过程等内容，除另有特别注明，均为保密信息。任何个人、机构未经杭州默安科技有限公司的书面授权许可，不得复制、引用或传播本文件的任何片断，无论通过电子形式或非电子形式。

|  |
| --- |
| 目录 |
| [1.1 基本概念 1](#_Toc524353192)  [1.2 应急响应的必要性 1](#_Toc524353193)  [1.3 客户收益 1](#_Toc524353194)  [2.1 政策文件或标准 2](#_Toc524353195)  [2.2 服务原则 2](#_Toc524353196)  [3.1 服务范围 3](#_Toc524353197)  [3.2 服务方式 3](#_Toc524353198)  [3.2.1 现场服务和远程服务 4](#_Toc524353199)  [3.2.2 单次服务和年度服务 4](#_Toc524353200)  [3.3 服务流程 4](#_Toc524353201)  [3.3.1 事件优先级定义 4](#_Toc524353202)  [3.3.2 事件处理流程 5](#_Toc524353203)  [3.3.3 事件升级流程 6](#_Toc524353204)  [3.4 服务特点 6](#_Toc524353205)  [3.5 服务报告 7](#_Toc524353206)  [3.6 服务注意事项 7](#_Toc524353207)  [3.6.1 使用安全的工具 7](#_Toc524353208)  [3.6.2 严格流程化操作 7](#_Toc524353209)  [3.6.3 操作记录 7](#_Toc524353210)  [4.1 Windows系统检测 8](#_Toc524353211)  [4.1.1 常规 8](#_Toc524353212)  [4.1.2 恶意代码 8](#_Toc524353213)  [4.2 类Unix系统检测 9](#_Toc524353214)  [4.2.1 常规 9](#_Toc524353215)  [4.2.2 恶意代码 9](#_Toc524353216)  [4.3 Web应用检测 9](#_Toc524353217)  [5.1 信息收集 10](#_Toc524353218)  [5.2 恶意代码检测 10](#_Toc524353219)  [5.3 Web日志分析 10](#_Toc524353220) |

# 服务概述

* 1. 基本概念

紧急响应（Emergency Response）又称为应急响应，是指安全技术人员在遇到突发事件后所采取的措施和行动。而突发事件则是指影响一个系统正常工作的情况。这里的系统包括主机范畴内的问题，也包括网络范畴内的问题，例如黑客入侵、信息窃取、拒绝服务攻击、网络流量异常、病毒爆发、网页篡改等。

应急响应的目标通常包括采取紧急措施和行动，恢复业务到正常服务状态；调查安全事件发生的原因，避免同类安全事件再次发生；在需要司法机关介入时，提供法律认可的数字证据等。

* 1. 应急响应的必要性

应急响应是一项需要充分的准备并严密组织的工作。它必须避免不正确的和可能是灾难性的动作或忽略了关键步骤的情况发生。这就需要掌握足够的安全技能，并且具备一定的追踪侦查能力、沟通能力、心理学知识并且掌握必要法律知识的专业安全人士的参与。大多数情况下，企业并不具有具备以上知识的专业人员。

安全厂商作为常年研究安全技术、实时跟踪安全动态的专业公司，对分析各种流行的安全问题和事件均有着自己成熟的思路和丰富的技术手段。在这方面，无疑能为其客户提供应急响应支持相关的服务内容。

应急响应是安全运维服务体系的一个重要组成部分。

* 1. 客户收益

对于客户而言，应急响应可以为其带来以下收益：

* 问题快速定位与处理

安全厂商凭借其在应急响应领域丰富的经验和强大的事件分析处理能力，能够更加快速地帮助客户追踪到事件的源头。而且，对于事件的应对方法，各厂商也有自己独到的经验和技巧。

* 提高安全技能

在支持人员与客户相关人员的交互过程中，可潜移默化地提升用户的安全技能。

# 服务的实施标准或原则

* 1. 政策文件或标准

默安科技应急响应服务将参考下列标准进行工作。

* ISO/IEC 27001:2005信息技术-安全技术-信息系统规范与使用指南
* ISO/IEC 13335-1: 2004 信息技术-安全技术-信息技术安全管理指南
* ISO/IEC TR 15443-1: 2005 信息技术安全保障框架
* ISO/IEC PDTR 19791: 2004 信息技术 安全技术 运行系统安全评估
* GB/T 20984-2007信息安全技术 信息安全风险评估规范
* GB/T 19715.1-2005 信息技术-信息技术安全管理指南
* GB/T 19716-2005 信息技术-信息安全管理实用规则
* GB/T 18336-2001 信息技术-安全技术-信息技术安全性评估准则
* GB/T17859-1999 计算机信息系统安全保护等级划分准则
* GB/T 20984-2007信息安全技术 信息安全风险评估规范
* GB/T 20988-2007信息系统灾难恢复规范
* GB/Z 20986-2007信息安全事件分类分级指南
* 默安科技安全服务工作规范、应急响应实施规范
* ……
  1. 服务原则

默安科技在提供应急响应服务中，将遵循下列原则。

* 保密性原则

保密性原则是安全服务中最重要的原则，它是鼓励客户实施安全服务的心理基础，同时也是对客户的人格及隐私权的最大尊重。应急响应的保密范围，包括实施过程的保密性和输出成果的保密性。对服务过程中获知的任何客户系统信息均属秘密信息，不得泄露给第三方单位或个人，不得利用这些信息进行任何侵害客户的行为；对服务的报告提交不得扩散给未经授权的第三方单位或个人。

* 标准性原则

默安科技应急响应服务将在国家法律、法规允许的范围内进行，特别是遵照并履行《全国人大常委会关于维护互联网安全的决定》相关规定等。

* 规范性原则

默安科技应急响应服务将按照默安安全服务工作规范、应急响应实施规范进行严格落实。由专业的安全服务人员依照规范的操作流程进行，对操作过程和结果要有相应的记录，提供完整的服务报告。

* 最小影响原则

应急响应服务工作应尽可能控制事件影响范围，避免其它系统和网络的二次事件扩散，快速控制、恢复以保证业务的正常运行。

# 默安科技应急响应服务

* 1. 服务范围

默安应急响应服务主要面向客户提供已发生安全事件的事中、事后的取证、分析及提供解决方案等工作。

默安科技可以帮助客户完成下列类型安全事件的应急响应支持：

* 应用服务瘫痪问题
* 网络阻塞、DDoS攻击问题
* 服务器遭劫持、页面篡改问题
* 系统异常宕机问题
* 恶意入侵、黑客攻击问题
* 病毒爆发问题
* 内部安全事故
* ……
  1. 服务方式

默安科技应急响应服务包括单次服务和年度服务两种形式，服务地点可以选择客户现场和远程两种方式，客户可以根据需要选择适合自己的服务。

* + 1. 现场服务和远程服务

根据服务地点，可以分为现场服务和远程服务两种。

**现场服务**：指接到客户紧急服务请求，支持人员在最短时间内赶赴客户现场，协助客户分析事件可能的原因，解决各类安全事件。

**远程服务**：指通过电话、QQ远程协助、远程临时接入等非现场的活动，协助客户分析事件可能的原因，解决各类安全事件。

* + 1. 单次服务和年度服务

根据服务的周期，可以分为单次服务和年度服务两种。

**单次服务**：指为客户提供的一次性应急响应服务。一般由发生安全事件的客户临时申请应急响应支持人员参与应急事件处理，支持人员在分析完所有客户提供的信息后，向客户提交应急响应报告。

**年度服务**：服务期限以年为单位，服务年度内为客户提供有限次数的应急响应支持工作，每次服务均会提供详细的应急响应报告。

* 1. 服务流程

默安科技应急响应服务流程主要包括事件处理流程和事件升级流程两部分。

* + 1. 事件优先级定义

默安科技结合自身经验，在实践中总结制定出了一套合理的安全事件分级结构对应表，并且针对于不同级别的事件拟定切实可行的快速处理方式和临时解决办法。安全等级划分标准如下：

事件安全级别划分标准

|  |  |
| --- | --- |
| **事件优先级** | **描述** |
| 紧急事件 | 客户提供业务的系统由于安全原因崩溃、系统性能严重下降，已无法提供正常服务。例如：本地区出口路由由于网络安全原因非正常中断，严重影响用户使用。公众服务由于安全原因停止服务或者造成恶劣影响的。 |
| 严重事件 | 用户内部的业务支持系统由于安全事件出现问题，导致不能运转正常不稳定。部分服务由于安全原因中断，影响用户正常使用 |
| 一般事件 | 由于安全原因导致系统出现故障，但不影响用户正常使用。客户提出安全技术咨询、索取安全技术资料、技术支援等。 |

* + 1. 事件处理流程

默安科技应急响应服务事件处理流程主要分为三个阶段，包括前期准备、应急响应实施及成果汇报：

* 前期准备

在实施应急响应工作前，客户经理或项目经理收到客户申请应急响应支持，由客户经理或项目经理协调内部技术支持人员和客户技术人员第一时间取得联系，了解事件发生情况。技术人员判断事件类型，是否需要启用应急响应服务。

* 应急实施

在判断事件类型可能为安全事件，启用应急响应后，技术人员通过现场或非现场等方式进行信息收集工作，详细了解掌握事件发生的始终、现状、可能的影响，对事件进行详细分析，提供事件处理建议，并协助客户解决事件。

* 成果汇报

待事件处理结束后，技术人员整理事件分析、事件处理的过程记录和相关资料，撰写应急响应服务事件报告，提交给客户。对于大型、复杂的应急响应过程还需进行整体的事件处理汇报工作。



应急响应服务事件处理流程

* + 1. 事件响应机制

默安科技在收到事件告警后，15分钟内进行故障事件的鉴别，如果是安全事件，则立即启动应急响应服务流程，如果不是安全事件，立即回复相关人员，并建议寻求其他方面的支持。

默安科技对于一般事件首先采取安全咨询的方式帮助用户自行解决，当用户安全管理员经过努力无法自行解决时，默安科技工程师将采用应急响应服务通过远程或本地服务方式帮助用户解决安全事件。

默安科技对于严重和紧急事件，将启用应急响应服务，安排工程师以最快的交通工具即可出发赶赴现场，按照安全应急响应服务流程帮助用户尽快抑制风险和恢复业务。

* 1. 服务特点
* 经验主导，成果保证

在应急响应支持方面，默安科技多年来积累了丰富的经验。无论是所收集信息的完整性，还是事件分析过程的科学性和准确性都在业内处于领先的位置。在经验与技术的完美结合之下，能够更加容易捕获信息中的蛛丝马迹，为事件分析去的突破性进展打下基础。

* 流程清晰，规范服务

默安科技应急响应服务采用规范化管理，支持人员均严格按照设定的流程来进行各项工作。而默安科技的应急服务规范和流程均来自于多年的应急响应实践，完全符合应急响应事件处理的相关要求。在确保获得分析事件必需数据的同时，也防止了可能对事件目标产生的影响。

* 1. 服务报告

在应急响应工作完成后一个工作日内，默安支持人员将会为客户提供一份应急响应报告。

在报告中，支持人员将会所收集的信息对整个安全事件的来龙去脉进行详尽的分析，并最终给出分析结果。

除此之外，支持人员还将根据分析结果提出解决方案和相关的安全建议，为事件的后期处理提供参考。输出如下报告：

* 《XX应急响应报告》
  1. 服务注意事项

应急响应是一项时效性很强的服务，当错过某个时间点或者某个关键的步骤都有可能影响到后期分析所得的结果，所以，默安科技建议客户在发生安全事件后不可惊慌失措，尽可能保留现场，如果因为特殊原因无法保留现场，也需要劲量搜集事件对象的相关信息，为后续的事件分析和解决提供帮助。对于应急响应服务中可能出现的各种不确定因素可采用下列措施予以规避。

* + 1. 使用安全的工具

应急响应过程中，支持人员可能需要帮助客户去收集分析数据，势必会用到一些专门的工具。默安科技在选择信息收集工具时均对要使用的工具进行了严格的测试，确保工具不会对使用目标产生任何的影响，更加不会扰乱安全事件相关的痕迹。

* + 1. 严格流程化操作

应急响应过程中，支持人员将严格按照默安科技应急响应支持流程来进行相关工作，确保不进行任何多余操作、不遗漏任何必要的信息。

* + 1. 操作记录

应急响应过程中，支持人员会对服务过程中所进行的每项操作都进行详细的记录，包括执行了什么命令、复制了什么文件等，以便出现意外后进行追查。

# 应急响应方法论

* 1. Windows系统检测
     1. 常规

安全事件发生以后，常常有蛛丝马迹遗留在下列信息当中，处理安全事件时通常会收集这些信息来帮助应急响应支持人员的分析工作。

* 用户
* 自启动项目
* 进程和服务（含模块）
* 驱动
* 网络连接
* 文件
* 日志
* 注册表
  + 1. 恶意代码

对于黑客入侵、病毒传播等类型的安全事件来说，支持人员必须要做的一项工作就是要检测事件目标是否已经被植入了恶意代码。恶意代码可能具有以下几类功能中的一种，常常需要依赖于第三方检测工具来进行检测：

* 感染文件
* 寄居NTFS交换数据流
* 线程注入
* SPI
* ActiveX自启动
* 端口复用
* Rootkit
  1. 类Unix系统检测
     1. 常规

同Windows类似，Unix也有一些常规的信息可供支持人员分析：

* 用户
* 自启动项
* 进程和服务（含模块）
* 网络连接
* 文件
* 日志
* 软件包完整性检查
  + 1. 恶意代码

由于Unix恶意代码的种类较少，检测目标也以Rootkit为主，其它恶意代码基本在常规检测中通过分析即可得出结果。

* 1. Web应用检测

当安全事件发生在Web应用上面的时候，支持人员会用到Web应用检测相关的技术，其中最主要的是Web应用访问日志分析工作，通过分析可以发现下列类型的安全事件：

* 远程扫描
* 注入攻击
* URL跨站脚本攻击
* 错误参数构造
* HTTP权限配置错误

# 服务相关工具

本章节列出部分常见的应急响应支持工具，但并不能完整包括真实环境下全部应急响应工具。

* 1. 信息收集

信息收集工具

|  |  |
| --- | --- |
| **工具名称** | **官方地址** |
| **Process Explorer** | http://www.microsoft.com |
| **LP\_Check** | http://www.dragonsoft.com |
| **Autoruns** | http://www.microsoft.com |
| **Streams** | http://www.microsoft.com |
| **Filemon** | http://www.microsoft.com |
| **Regmon** | http://www.microsoft.com |
| **Tcpview** | http://www.microsoft.com |

* 1. 恶意代码检测

恶意代码检测工具

|  |  |
| --- | --- |
| **工具名称** | **官方地址** |
| **Chrootkit** | http://www.chkrootkit.org |
| **Rootkit hunter** | http://www.rootkit.nl |
| **Icesword** | -- |
| **Rootkit unhooker** | http://rku.nm.ru/ |
| **Sysprot** | http://sites.google.com/site/sysprotantirootkit/ |

* 1. Web日志分析

Web日志分析工具

|  |  |
| --- | --- |
| **工具名称** | **官方地址** |
| **LogParser** | http://www.microsoft.com |
| **XLogan** | http://www.axeuk.com/xlogan/ |
| **AWstats** | http://awstats.sourceforge.net/ |