注册信息安全专业人员

——应急响应工程师

知识体系大纲

发布日期：2019 年 1 月 1 日

生效日期：2019 年 1 月 1 日

中国信息安全测评中心

网神信息技术（北京）股份有限公司

目 录

第1章　前　言

网络空间信息安全作为我国信息化建设健康发展的重要因素，关系到贯彻落实科学发展观、全面建设小康社会、构建社会主义和谐社会和建设创新型社会等国家战略举措的实施，是国家安全的重要组成部分。在网络空间信息系统安全保障工作中，人，是最核心、也是最活跃的因素，人员的信息安全意识、知识与技能已经成为保障信息系统安全稳定运行的重要基本要素之一。

注册信息安全专业人员（CISP）是对我国网络基础设施和重要信息系统的信息安全专业人员进行资质评定的重要形式。多年来为落实我国有关政策“加快信息安全人才培养，增强全民信息安全意识”的指导精神，构建信息安全人才体系发挥了巨大作用。

本大纲从我国国情出发，结合我国网络基础设施和重要信息系统安全保障的实际需求，以知识体系的全面性和实用性为原则，明确规定了注册信息安全专业人员（应急响应）应当掌握的知识要点，是 CISP-IRE 教材编制，讲师授课，学员学习，以及考试命题的重要依据。

本大纲包含以下章节：

第 2 章　应急响应工程师知识体系概述
第 3 章　知识类：应急响应概况
第 4 章　知识类：应急响应基础
第 5 章　知识类：应急响应事件监测
第 6 章　知识类：应急响应事件分析与处置
第 7 章　知识类：应急响应典型事件

第2章　注册信息安全专业人员-应急响应工程师知识体系概述

- 注册信息安全专业人员应急响应工程师，英文为 Certified Information Security Professional - Incident Response Engineer ，简称 CISP-IRE。证书持有人员主要从事信息安全技术领域应急响应工作，具有了解应急响应概况、应急响应基础、应急响应事件监测、应急响应事件分析和处置的基本知识和能力。

2.1 知识体系框架结构

CISP-IRE 知识体系使用组件模块化的结构，包括知识域、知识子域、知识点三个层次。

- 知识域：是知识类中由属于同一技术领域的知识内容构成的相对独立、成体系的知识集合；
- 知识子域：是对知识域进一步分解细化形成的完整的知识组件；
- 知识点：是构成知识子域的基本模块，每个知识子域由一至多个具体的知识点构成。

本大纲规定了知识子域中每一个知识点的内容和深度要求，分为“了解”、“理解”和“掌握”三类。

- 了解：是最低深度要求，学员需要正确认识该知识点的基本概念和原理；
- 理解：是中等深度要求，学员需要在正确认识该知识点的基本概念和原理的基础上，深入理解其内容，并可以进一步的判断和推理；
- 掌握：是最高深度要求，学员需要正确认识该知识点的概念、原理，并在深入理解的基础上灵活运用。

图 2-1 描述了知识体系的结构

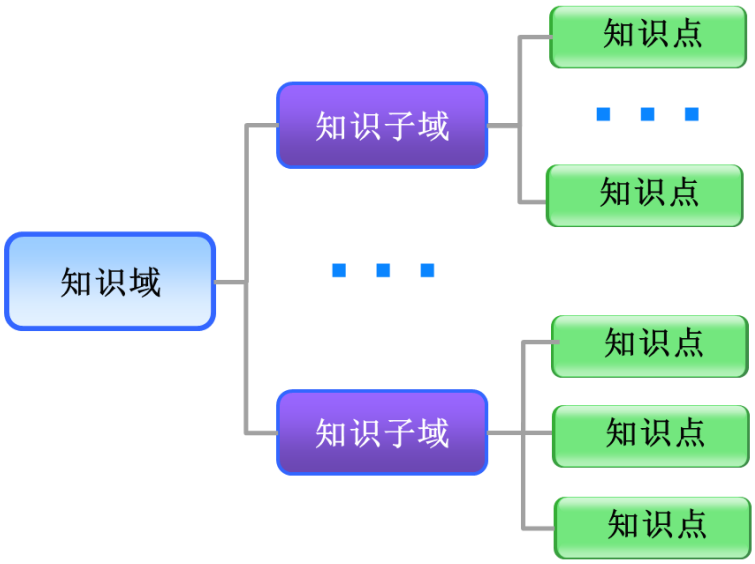

图 2-1：知识体系的组件模块结构

在整个知识体系结构中，共包括应急响应概况、应急响应基础、应急响应事件监测、应急响应事件分析与处置、企业应急响应典型事件五个知识域，每个知识域根据其逻辑划分为多个知识子域，每个知识子域由一个或多个知识点组成。

CISP-IRE 知识体系结构所包含的五个知识域，分别为：

- 应急响应概况：主要包括应急响应介绍、应急事件分类、应急响应启动条件、应急响应目标、应急响应预案制定与一般处置流程相关的技术知识。
- 应急响应基础：主要包括 Windows 应急、Linux 应急、日志分析、应急响应工具配备和介绍相关的技术知识。
- 应急响应事件监测：主要包括威胁情报运营、安全监控相关技术知识和实践。
- 应急响应事件分析与处置：主要包括事件分析、制定应急响应计划、响应处置工作流程、应急响应报告编写、事件跟踪总结相关技术知识和实践。
- 企业应急响应典型事件：主要包括有害程序事件、网络攻击事件、信息破坏事件、其它网络安全事件相关技术知识和实践。

图 2-2 描述了 CISP-IRE 的知识体系结构框架：

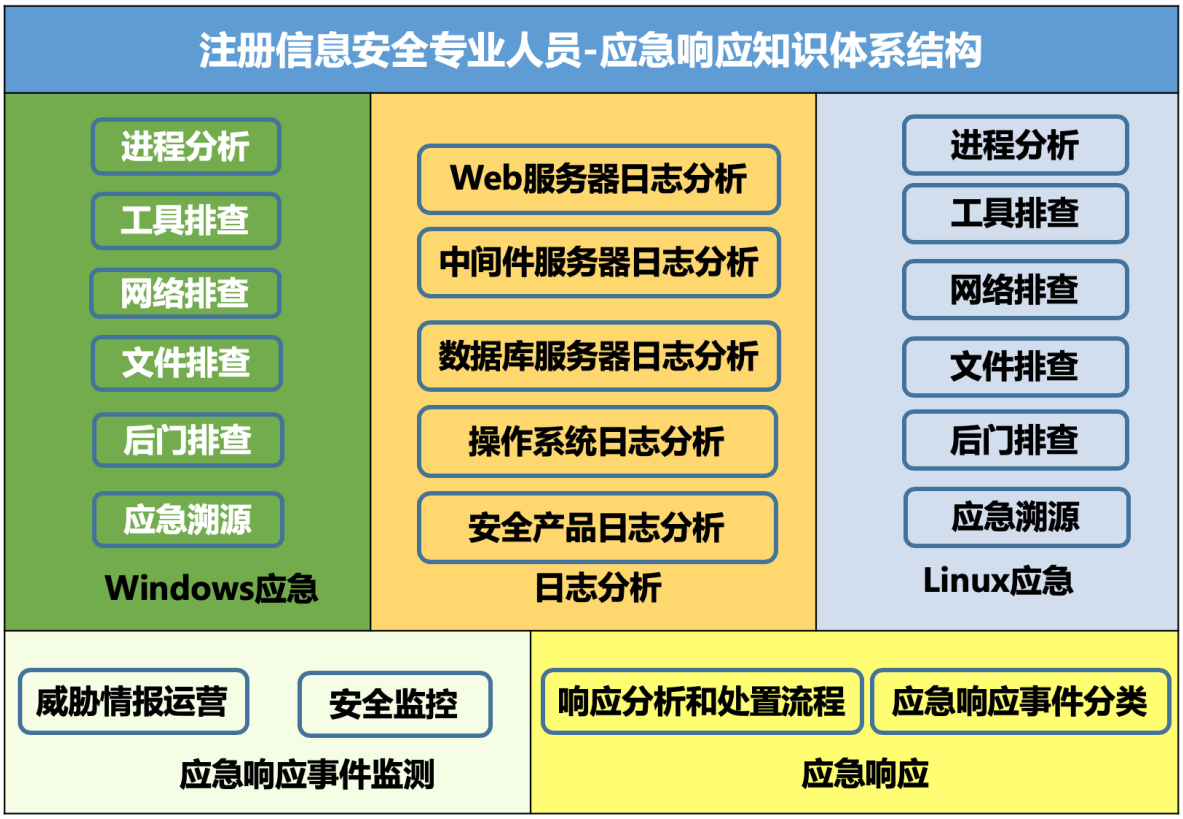

图 2-2：CISP-IRE知识体系结构框架

2.2 考试试题结构

CISP-IRE 考试题型为选择题与实操题,总分共 100 分，其中选择题 20 分，实操题 80 分，得到 70 分以上（含 70 分）为通过。

证书类别 知识类别	CISP-IRE
应急响应概述	10%
应急响应基础	30%
应急响应事件监测	10%
应急响应分析与处置	20%
企业应急响应典型事件	30%

表 2-1：CISP-IRE 试题结构

第3章　知识域：应急响应概况

即使是最好的信息安全基础设施也无法保证不会发生入侵或其它恶意行为。当信息安全事件发生时，相关组织必须拥有有效的计划和流程以及准备好应急的合格人员。而一个合格的应急人员需要具备以下的知识和技能：

- 掌握应急响应概况
- 掌握应急响应基础知识
- 掌握应急响应事件监测
- 掌握应急响应事件分析与响应处置
- 掌握企业应急响应典型事件

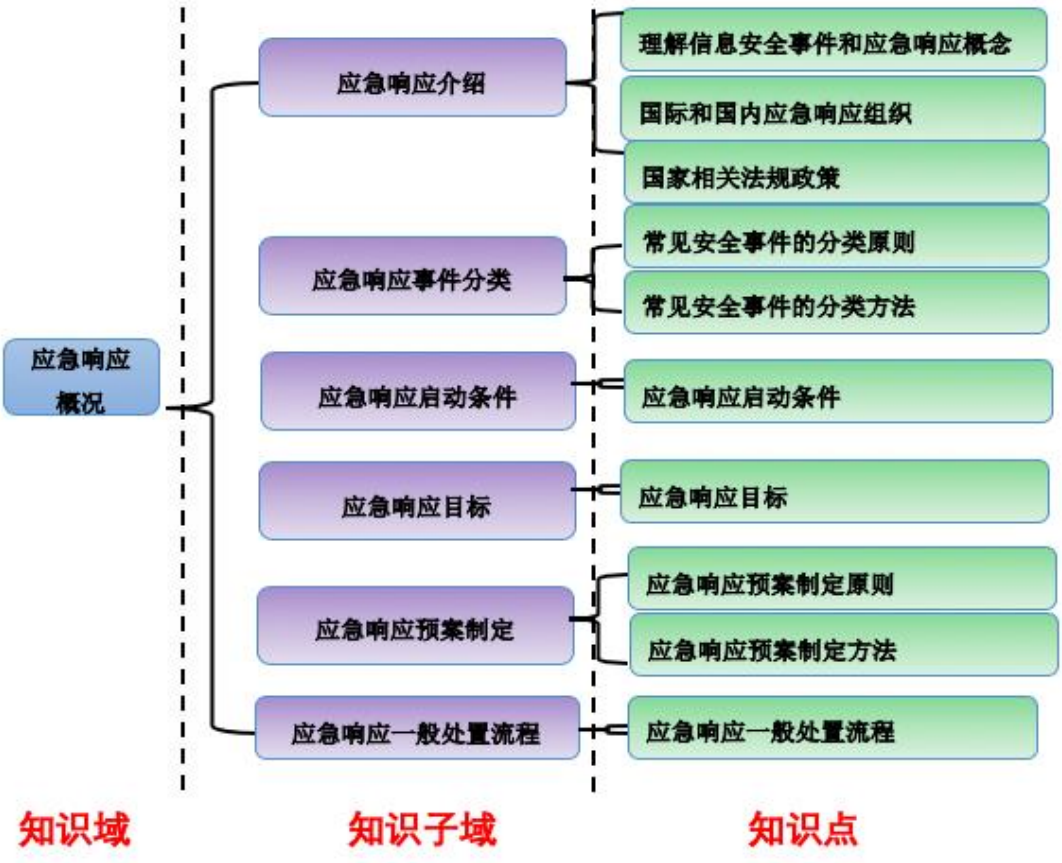

图 3-1：知识域：应急响应概述

3.1 知识子域：应急响应介绍

- 知识点：信息安全事件和应急响应概念
  - ◆了解常见的安全事件。
  - ◆理解应急响应基础概念以及了解应急响应的重要性。
- 知识点：国际和国内信息安全应急响应组织
  - ◆了解国际和国内信息安全应急响应组织。
- 知识点：国家相关法规政策
  - ◆了解国家和网络安全应急响应相关的法规政策。

3.2 知识子域：安全事件分类

- 知识点：安全事件分类原则
  - ◆了解常见安全分类并能够对安全事件进行分类。
- 知识点：安全事件分类方法
  - ◆掌握常见安全事件不同维度的分类方法。

3.3 知识子域：应急响应启动条件

- 知识点：应急响应启动条件
  - ◆了解应急响应不同的启动条件并根据不同的响应条件制定相应的响应级别。

3.4 知识子域：应急响应目标

- 知识点：应急响应目标
  - ◆ 理解应急响应目标并能为目标制定切实有效的应急响应计划。

3.5 知识子域：应急响应预案制定

- 知识点：应急响应预案制定原则
  - ◆ 掌握应急响应预案制定的原则与方法论。
- 知识点：应急响应预案制定方法

◆ 掌握针对不同应急响应情况下的应急响应预案制定的方法。

3.6 知识子域：应急响应一般处置流程

- 知识点：应急响应一般处置流程
  - ◆ 掌握应急响应一般处置流程并对流程进行深入理解。

第4章　知识域：应急响应基础

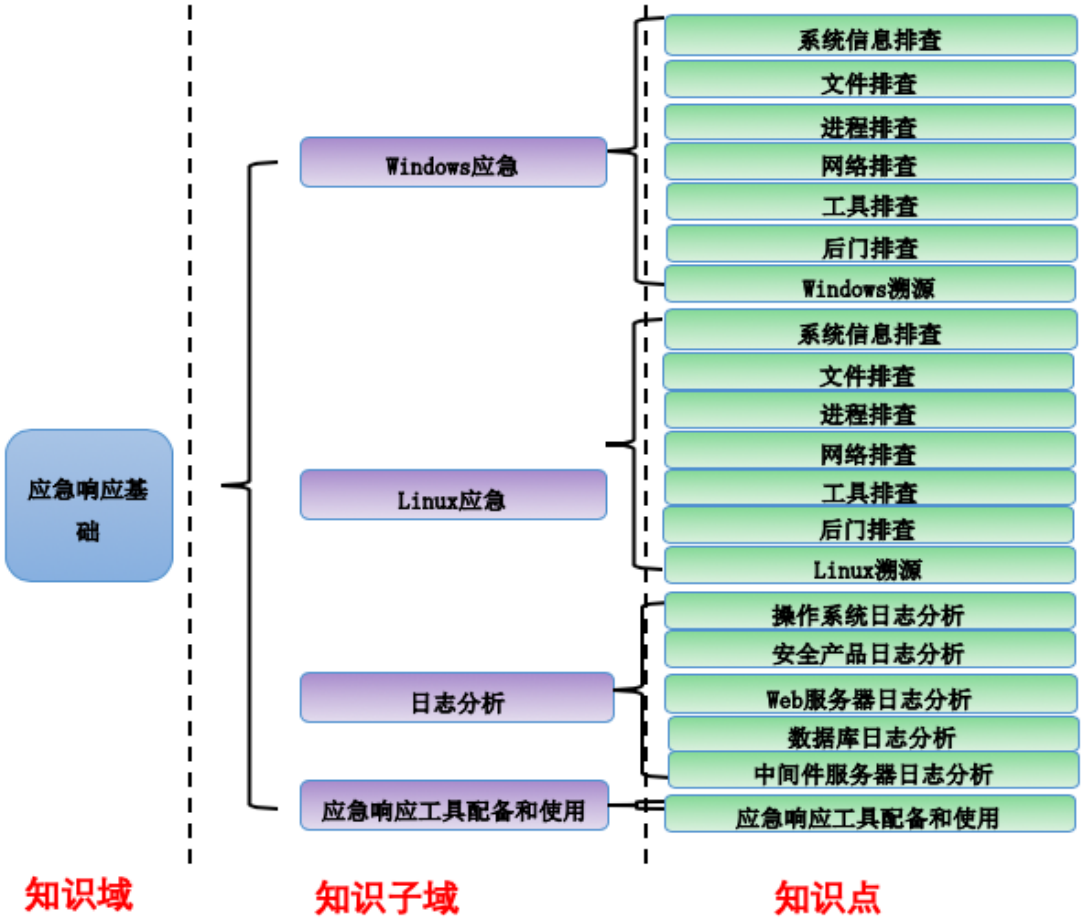

图 4-1：知识域：应急响应基础

4.1 知识子域：Windows 应急

Windows 服务器一直是挖矿木马、勒索病毒等安全事件的重灾区，攻击者将目光集中于 Windows 服务器的主要原因是服务器无论在性能上或者是在用户接触频率上对于攻击者而言都是极度友好的——服务器的性能大部分要远高于个人电脑，并且服务器大多是“疏于看管”的，挖矿木马可以长期潜伏，此外针对 PC 的一些安全事件也有很多，例如 PC 的挖矿木马家族 OnesystemCareMiner、HiddenPowerShellMiner、飞熊矿业等家族仍然在活跃中，其中网页挂马和破解

软件是这类挖矿木马最为常见的传播渠道。所以掌握 Windows 操作系统下的应急响应知识和技巧尤为重要。

Windows 下的应急响应需要掌握以下的知识和技能。

- 知识点：系统信息排查
  - ◆ 掌握 Windows 下系统信息排查的方法。
  - ◆ 掌握 Windows 下系统信息排查常用命令使用。
- 知识点：文件排查
  - ◆ 掌握 Windows 下文件排查的方法。
  - ◆ 掌握 Windows 下文件排查常用命令使用。
- 知识点：进程排查
  - ◆ 掌握 Windows 下进程排查的方法。
  - ◆ 掌握 Windows 下进程排查常用命令使用。
- 知识点：网络排查
  - ◆ 掌握 Windows 下网络排查的方法。
  - ◆ 掌握 Windows 下网络排查常用命令使用。
- 知识点：工具排查
  - ◆ 掌握 Windows 工具常用工具的使用。
- 知识点：后门排查
  - ◆ 了解 Windows 常见后门原理。
  - ◆ 掌握 Windows 下常见后门排查方法。
- 知识点：应急溯源
  - ◆ 掌握 Windows 下应急溯源知识和技巧。
  - ◆ 掌握 Windows 下常见的攻击手法。

4.2 知识子域：Linux 应急

Linux 是一套免费使用和自由传播的类 Unix 操作系统，目前在服务器市场占有率超过 80%。通过长期分析发现目前针对 Linux 主机的攻击目的，主要集中在捕获肉鸡进行挖矿与 DDoS 攻击上。掌握 Linux 平台下的知识和技能也是对每个应急响应人员来说是不可或缺的。

Linux 下的应急响应需要掌握以下的知识和技能。

- 知识点：系统信息排查
  - ◆ 掌握 Linux 下系统信息排查的方法。
  - ◆ 掌握 Linux 下系统信息排查常用命令使用。
- 知识点：文件排查
  - ◆ 掌握 Linux 下文件排查的方法。
  - ◆ 掌握 Linux 下文件排查常用命令使用。
- 知识点：进程排查
  - ◆ 掌握 Linux 下进程排查的方法。
  - ◆ 掌握 Linux 下进程排查常用命令使用。
- 知识点：网络排查
  - ◆ 掌握 Linux 下网络排查的方法。
  - ◆ 掌握 Linux 下网络排查常用命令使用。
- 知识点：工具排查
  - ◆ 掌握 Linux 工具常用工具的使用。
- 知识点：后门排查
  - ◆ 了解 Linux 常见后门原理。
  - ◆ 掌握 Linux 下常见后门排查方法。
- 知识点：应急溯源
  - ◆ 掌握 Linux 下应急溯源知识和技巧。
  - ◆ 掌握 Linux 下常见的攻击手法。

4.3 知识子域：日志分析

简单地说，日志就是计算机系统、设备、软件等在某种情况下记录的信息。具体的内容取决于日志的来源。例如，Unix 操作系统会记录用户登录和注销的消息，防火墙将记录 ACL 通过和拒绝的消息，磁盘存储系统在故障发生或者在某些系统认为将会发生故障的情况下生成日志信息。日志中有大量信息，这些信息告诉你为什么需要生成日志，系统已经发生了什么。例如，Web 服务器一般会在有人访问 Web 页面请求资源（图片、文件等等）的时候记录日志。如果用户访问

的页面需要通过认证，日志消息将会包含用户名。这就是日志数据的一个例子：可以使用用户名来判断谁访问过一个资源。通过日志，IT 管理人员可以了解系统的运行状况，安全状况，甚至是运营的状况。同样在发生安全事件的时候，日志对攻击溯源以及定位入侵原因尤为重要。

- 知识点：Web 服务器日志分析
  - ◆ 掌握常见 Web 服务器（如 Apache、Nginx）日志种类、位置以及排查方法。
  - ◆ 掌握常见 Web 服务器各种日志中各个字段的含义。
- 知识点：数据库服务器日志分析
  - ◆ 掌握常见数据库（Mysql、Sqlserver、Oracle、Redis 等）日志种类、位置以及排查方法。
  - ◆ 掌握常见数据库各种日志中各个字段的含义。
- 知识点：中间件服务器
  - ◆ 掌握常见中间件服务器（Weblogic、WebSphere、Jboss 等）日志种类、位置以及排查方法。
  - ◆ 掌握常见中间件服务器各种日志中各个字段的含义。
- 知识点：操作系统日志分析
  - ◆ 理解 Windows 和 Linux 下各种日志各个字段含义。
  - ◆ 掌握 Windows 和 Linux 下日志种类、位置以及排查方法。
- 知识点：安全产品日志分析
  - ◆ 理解常见安全产品下各种日志各个字段含义。
  - ◆ 掌握常见安全产品（常见软防、硬防）日志种类、位置以及排查方法。

4.4 知识子域：应急响应工具配备和使用

- 知识点：应急响应工具配备和使用
  - ◆ 掌握应急响应工具配备和使用。
  - ◆ 了解常见应急响应工具原理。

第5章　知识域：应急响应事件监测

在网络安全领域的知识是有所界定的。在互联网上发生不同的安全事件的解决方法也不一样。针对不同的安全需求，需要建立不同的问题模型，针对不同的分析对象需要采取不同的分析方法。企业安全技术人员要基于对可以获得的数据源（内部和外部）的理解，有针对性的确定分析逻辑。通过挖掘数据间的关系，总结规律，形成知识，及时发现和处理威胁。

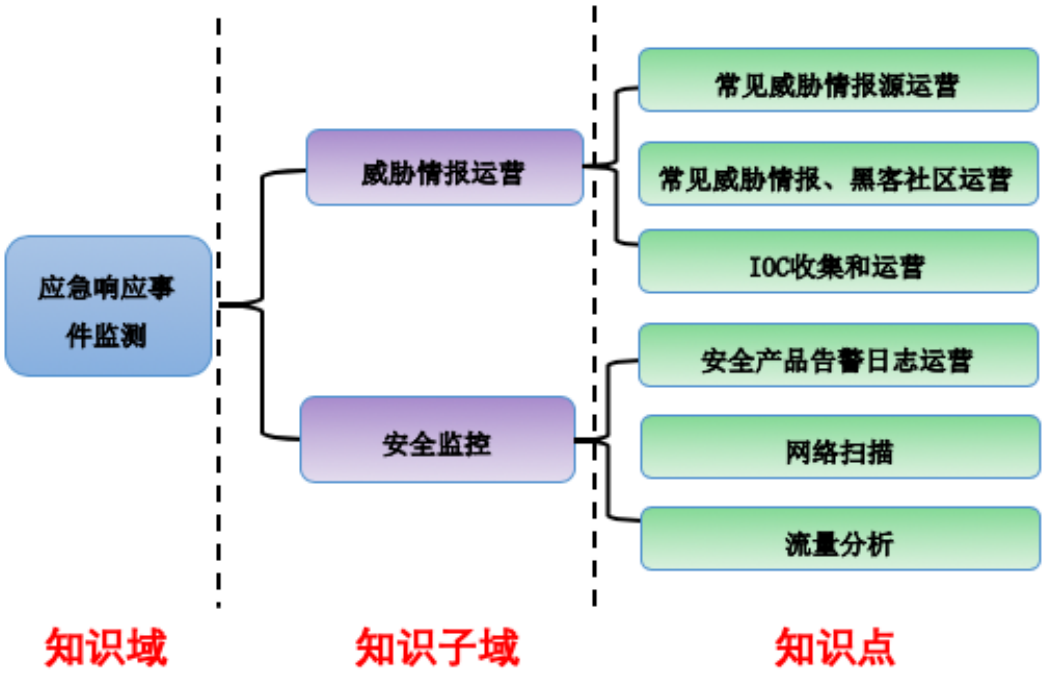

图 5-1：知识域：应急响应事件监测

5.1 知识子域：威胁情报运营

- 知识点：常见威胁情报源订阅
  - 了解有哪些威胁情报源。
  - 了解各个威胁情报源的特点。
- 知识点：常见威胁情报、黑客社区关注
  - 了解和关注常见威胁情报、黑客社区等。

- 知识点：IOC 收集和运营
  - 了解常见 IOC 种类。
  - 了解 IOC 收集和运营。

5.2 知识子域：安全监控

- 知识点：安全产品告警日志运营
  - 理解常见安全产品（WAF、IDS、IPS 等）使用。
  - 理解常见安全产品日志查看。
- 知识点：网络扫描
  - 掌握常见网络扫描工具的使用。
  - 了解常见网络扫描工具原理。
- 知识点：流量分析
  - 掌握常见抓包工具（wireshark、tcpdump）的使用。
  - 了解各个数据包的具体含义。

第6章　知识域：应急响应事件分析与处置

当安全事件已经发生的时候，作为安全人员需要对事件进行有效的分析，针对事件制定应急响应处置计划，并能够有效的去执行应急响应计划，后续完成应急响应报告并深刻反思发生安全事件的原因，防止类似的事件再次发生。

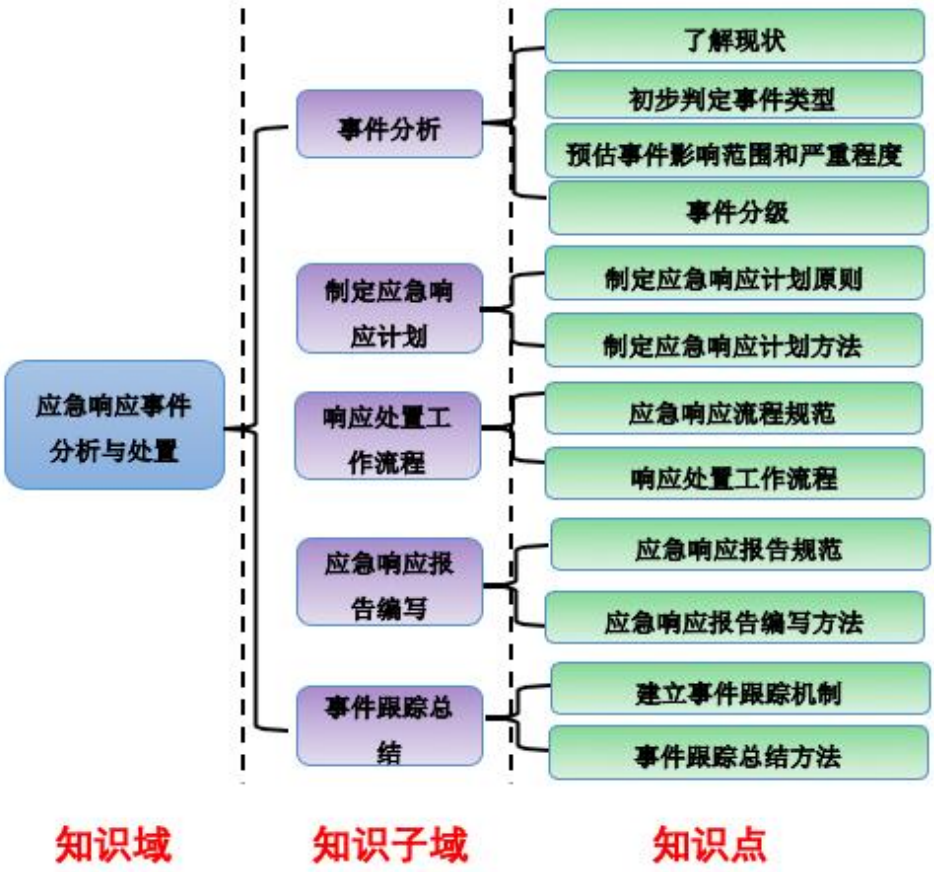

图 6-1：知识域：应急响应事件分析与响应处置

6.1 知识子域：事件分析

- 知识点：了解现状
  - 了解事件发生的时间、事件发生的环境、事件症状等。
- 知识点：初步判定事件类型

- 掌握安全事件分类的原则和方法。

- 知识点：预估事件影响范围和严重程度
  - 了解事件影响范围和严重程度的判定。
- 知识点：事件分级
  - 了解基本的事件分级（I 级特别重大、II 级重大、III 较大、IV 一般）。

6.2 知识子域：制定应急响应计划

- 知识点：制定应急响应计划原则
  - 理解应急响应计划的制定原则。
- 知识点：制定应急响应计划方法
  - 理解应急响应计划的制定方法论，能够根据不同的安全事件制定相应的应急响应方法。

6.3 知识子域：响应处置工作流程

- 知识点：应急响应流程规范
  - 掌握应急响应处置工作流程规范。
- 知识点：响应处置工作流程
  - 掌握准备阶段的方式方法。
  - 掌握检测阶段的事件检测方法和步骤。
  - 掌握抑制阶段对应的处置方式方法和步骤。
  - 掌握根除阶段对应的处置方式方法和步骤。
  - 掌握恢复阶段对应的处置方式方法和步骤。
  - 掌握跟进阶段对应的处置方式方法和步骤。

6.4 知识子域：应急响应报告编写

- 知识点：应急响应报告规范
  - 掌握应急响应报告规范。
- 知识点：应急响应报告编写方法

- 掌握应急响应报告编写方法。

6.5 知识子域：事件跟踪总结

- 知识点：建立事件跟踪机制
  - 掌握建立事件跟踪机制的方法并能够不断去完善。
- 知识点：事件跟踪总结方法
  - 掌握建立事件跟踪总结的方法。

第 7 章 知识域：企业应急响应典型事件

参考《国家网络安全事件应急预案》，这里将网络安全事件分为有害程序事件、网络攻击事件、信息破坏事件、其它网络安全事件。

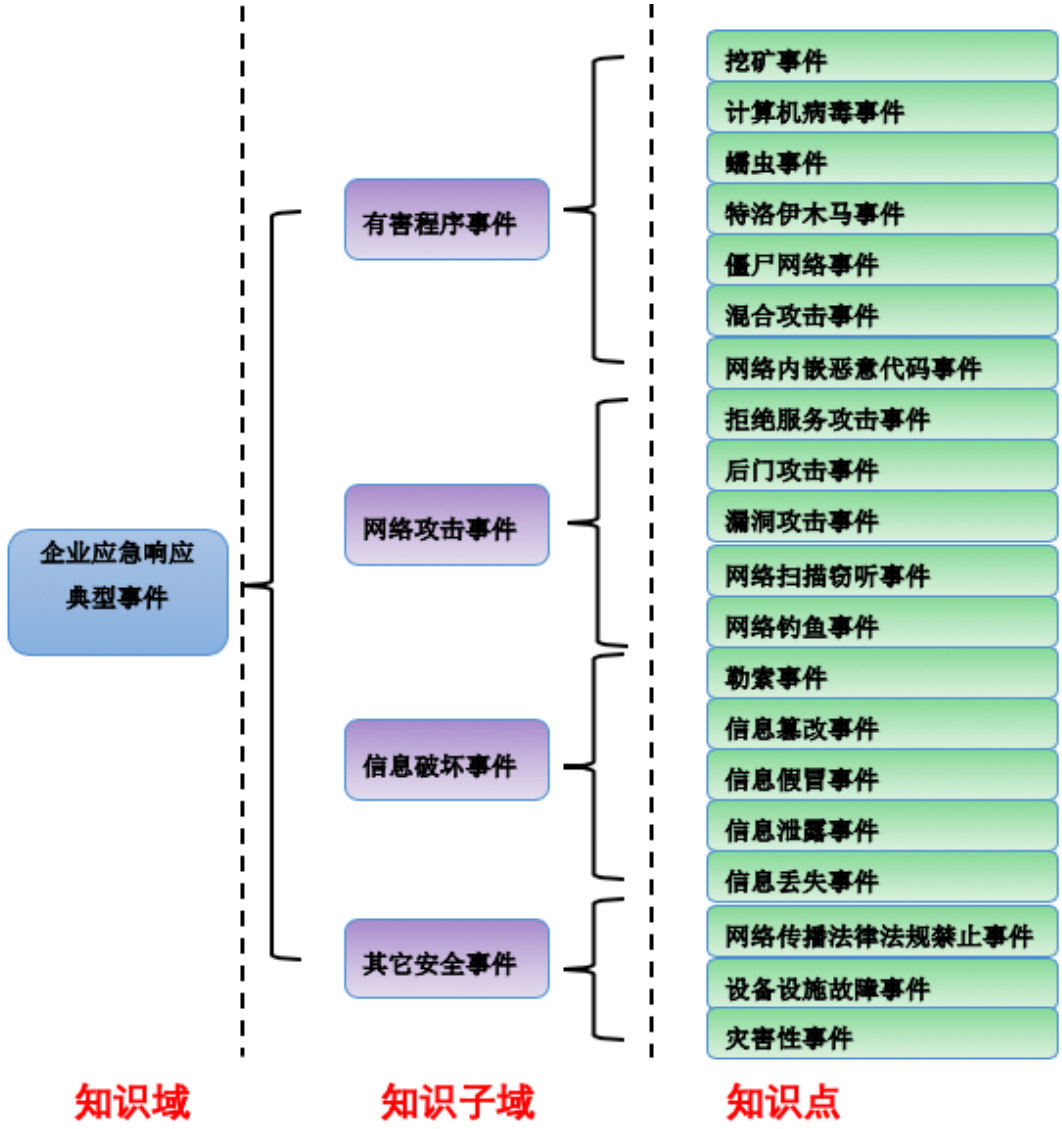

图 7-1：知识域：企业应急响应典型事件

7.1 知识子域：有害程序事件

- 知识点：挖矿事件
  - ◆ 理解计算机挖矿原理。

- ◆ 掌握计算机挖矿事件处置方法。

- 知识点：计算机病毒事件
  - ◆ 理解计算机病毒原理。
  - ◆ 掌握计算机病毒事件处置方法。
- 知识点：蠕虫事件
  - ◆ 理解蠕虫事件原理。
  - ◆ 掌握蠕虫事件处置方法。
- 知识点：特洛伊木马事件
  - ◆ 理解常见木马原理。
  - ◆ 掌握木马事件处置方法。
- 知识点：僵尸网络事件
  - ◆ 理解僵尸网络原理。
  - ◆ 掌握僵尸网络事件处置方法。
- 知识点：混合攻击事件
  - ◆ 理解混合攻击事件原理。
  - ◆ 掌握混合事件处置方法。
- 知识点：网页内嵌恶意代码事件
  - ◆ 理解常见网页内嵌恶意代码原理。
  - ◆ 掌握常见网页内嵌恶意代码事件处置方法。

7.2 知识子域：网络攻击事件

- 知识点：拒绝服务攻击事件
  - ◆ 理解拒绝服务攻击原理。
  - ◆ 理解拒绝服务攻击事件处置方法。
- 知识点：后门攻击事件
  - ◆ 理解常见后门原理。
  - ◆ 掌握常见后门事件处置方法。
- 知识点：漏洞攻击事件
  - ◆ 理解常见漏洞（不限系统漏洞和 Web 漏洞）原理。

- 掌握漏洞攻击事件处置方法。

- 知识点：网络扫描窃听事件
  - 理解常见扫描和网络窃听原理。
  - 掌握常见扫描和网络窃听处置方法。
- 知识点：网络钓鱼事件
  - 理解网络钓鱼事件原理。
  - 掌握钓鱼事件处置方法。

7.3 知识子域：信息破坏事件

- 知识点：勒索事件
  - 理解常见勒索软件原理。
  - 掌握勒索事件处置方法。
- 知识点：信息篡改事件
  - 理解常见信息篡改方式方法。
  - 掌握常见信息篡改事件处置方法。
- 知识点：信息假冒事件
  - 理解信息假冒事件原理。
  - 掌握信息假冒事件处置方法。
- 知识点：信息泄露事件
  - 掌握常见信息泄露方法手段。
  - 掌握信息泄露事件处置方法。
- 知识点：信息丢失事件
  - 了解常见信息丢失事件原理。
  - 掌握信息丢失事件处置方法。

7.4 知识子域：其它安全事件

- 知识点：网络传播法律法规禁止信息
  - 掌握网络传播法律法规禁止信息。
- 知识点：设备设施故障

- 了解设备设施故障原理。
- 掌握设备设施故障处置方法。

- 知识点：灾害性事件
  - 了解灾害性事件处置方法。