网络安全应急响应

职业技能等级标准

标准代码：510027

（2021年2.0版）

奇安信科技集团有限公司 制定

2021年12月发布

目　次

前　言

本标准按照 GB/T 1.1-2009 给出的规则起草。

本标准起草单位：奇安信科技集团股份有限公司。

本标准主要起草人（按姓氏笔画排序）：于京、王隆杰、王巍、左英男、史宝会、包宏宇、初雪峰、冯涛、孙善学、杜辉、龙翔、李江涛、杨东晓、杨洪雪、何红、但唐仁、邹德清、张永印、张翀斌、张锋、周国烛、郑长亮、赵利民、赵波、段晓光、贾斌、唐辉、黄庆涛、崔凯、管小清等。

起草人来自以下单位：奇安信科技集团股份有限公司、北京电子科技职业学院、北京信息职业技术学院、北京工业职业学院、深圳信息职业技术学院、深圳职业技术学院、华中科技大学、武汉大学国家网络安全学院。

1　范围

本标准规定了网络安全应急响应职业技能等级对应的工作领域、工作任务及职业技能要求。

本标准适用于网络安全应急响应职业技能培训、考核与评价，相关用人单位的人员聘用、培训与考核可参照使用。

2　规范性引用文件

下列文件对于本标准的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本标准。凡是不注日期的引用文件，其最新版本适用于本标准。

GB/T 20270-2006 信息安全技术 网络基础安全技术要求

GB/T 20988-2007 信息安全技术 信息系统灾难恢复规范

GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求

GB/T 24363-2009 信息安全技术 信息安全应急响应计划规范

GB/T 28827.3-2012 信息技术服务 运行维护 第3部分：应急响应规范

GB/Z 20986-2007信息安全技术 信息安全事件分类分级指南

GB/Z 20985-2007 信息安全技术 信息安全事件管理指南

3　术语和定义

国家、行业标准界定的下列术语和定义适用于本标准。

3.1 信息系统

由计算机及其相关的和配套的设备、设施（含网络）构成的，按照一定的应用目标和规则对信息进行采集、加工、存储、传输、检索等处理的人机系统。

[GB/Z 20986-2007]

3.2 网络安全

通过采取必要措施，防范对网络的攻击、侵入、干扰、破坏和非法使用以及意外事故，使网络处于稳定可靠运行的状态，以及保障网络数据的完整性、保密性、可用性的能力。

[GB/T 22239-2019]

3.3 信息安全事件

由于自然或者人为以及软硬件本身缺陷或故障的原因，对信息系统造成危害，或在信息系统内发生对社会造成负面影响的事件。

[GB/Z 20986-2007]

3.4 业务影响分析

对业务功能及其相关信息系统资源进行分析，评估特定信息安全事件对各种业务功能的影响的过程。

[GB/T 24363-2009]

3.5 应急事件

导致或即将导致运行维护服务对象运行中断、运行质量降低，以及需要实施重点时段保障的事件。

[GBT 28827.3-2012]

3.6 应急响应

组织为预防、监控、处置和管理应急事件所采取的措施和活动。

[GBT 28827.3-2012]

3.7 应急响应计划

组织为了应对突发/重大信息安全事件而编制的，对包括信息系统运行在内的业务运行进行维持或恢复的策略和规程。

[GB/T 24363-2009]

3.8 灾难恢复

为了将信息系统从灾难造成的故障或瘫痪状态恢复到可正常运行状态、并将其支持的业务功能从灾难造成的不正常状态恢复到可接受状态而设计的活动和流程。

[GB/T 20988-2007]

3.9 风险评估

依据有关信息安全技术与管理标准，对信息系统及由其处理、传输和存储的信息的保密性、完整性和可用性等安全属性进行评价的过程。

[GB/T 20984-2007]

3.10 有害程序事件

有害程序事件是指蓄意制造、传播有害程序，或是因受到有害程序的影响而导致的信息安全事件。

[GBZ 20986-2007]

3.11 网络攻击事件

网络攻击事件是指通过网络或其他技术手段，利用信息系统的配置缺陷、协议缺陷、程序缺陷或使用暴力攻击对信息系统实施攻击，并造成信息系统异常或对信息系统当前运行造成潜在危害的信息安全事件。

[GBZ 20986-2007]

3.12 信息破坏事件

信息破坏事件是指通过网络或其他技术手段，造成信息系统中的信息被篡改、假冒、泄漏、窃取等而导致的信息安全事件。

[GBZ 20986-2007]

3.13 设备设施故障

设备设施故障是指由于信息系统自身故障或外围保障设施故障而导致的信息安全事件，以及人为的使用非技术手段有意或无意的造成信息系统破坏而导致的信息安全事件。

[GBZ 20986-2007]

4 适用院校专业

4.1 参照原版专业目录

中等职业学校：网络信息安全、计算机网络技术、计算机应用等信息技术类专业。

高等职业学校：信息安全与管理、计算机网络技术、计算机系统与维护、计算机应用技术、司法信息技术、司法信息安全等专业。

应用型本科学校：信息安全、网络空间安全、计算机科学与技术、网络工程、软件工程等专业。

4.2 参照新版专业目录

中等职业学校：计算机应用、计算机网络技术、软件与信息服务、数字媒体技术应用、大数据技术应用、移动应用技术与服务、网络信息安全、网络安防系统安全与防护、网站建设与管理、计算机与数码设备维修等专业。

高等职业学校：计算机应用技术、计算机网络技术、软件技术、数字媒体技术、大数据技术、云计算技术应用、信息安全技术应用、人工智能技术应用、嵌入式技术应用、工业互联网技术、区块链技术应用、移动应用开发、工业软件开

发技术、密码技术应用、物联网应用技术、网络安全与执法、司法信息安全、司法信息技术等专业。

应用型本科学校：信息安全、网络空间安全、计算机科学与技术、网络工程、软件工程等专业。

高等职业教育本科学校：计算机应用工程、网络工程技术、软件工程技术、数字媒体技术、大数据工程技术、云计算技术、信息安全与管理、人工智能工程技术、嵌入式技术、工业互联网技术、区块链技术、物联网工程技术、网络安全与执法等专业。

5 面向职业岗位（群）

【网络安全应急响应】（初级）：主要面向政府部门、企事业单位、网络安全企业、互联网企业等用人单位的信息安全运维和基础安全服务类岗位。

【网络安全应急响应】（中级）：主要面向政府部门、企事业单位、网络安全企业、互联网企业等用人单位的安全服务类岗位。

【网络安全应急响应】（高级）：主要面向政府部门、企事业单位、网络安全企业、互联网企业等用人单位与网络安全相关的研发、生产、管理类岗位。

6 职业技能要求

6.1 职业技能等级划分

网络安全应急响应职业技能等级分为三个等级：初级、中级、高级，三个级别依次递进，高级别涵盖低级别职业技能要求。

【网络安全应急响应】（初级）：掌握常见威胁情报平台的使用方法；掌握常见操作系统的应急排查及安全加固工作；能够根据日志分析可疑事件；并根据日志回溯事件发生点，会使用工具分析恶意软件行为；掌握常见应急响应分析工

具的使用；可以对常见网络攻击进行分析和处理；能够独立完成安全测试任务；可以在发生安全事件后根据备份文件快速恢复业务；根据业务需求对业务系统进行定期备份。

【网络安全应急响应】（中级）：可以根据系统日志发现是否存在攻击行为，除了系统和服务日志外，可以借助安全设备日志对安全事件进行排查；能够熟练使用各类安全工具对网络安全事件进行分析、响应、溯源；掌握对恶意代码的动静态分析，针对恶意代码的运作流程进行分析并作出详细报告；可以独立完成高级别的渗透测试任务；能够掌握对网络设备和安全设备的加固方法；针对安全事件可以给出防护措施和建议，并配合实施。

【网络安全应急响应】（高级）：能够对信息系统安全风险进行评估与处置；能够对企业网络安全进行分析并对整体加固设计方案；能够为企业组建应急响应组织，并制定相应的风险预警制度和应急响应方案；制定应急培训计划，定期组织应急演练；能够指导初级、中级网络安全人员共同完成网络安全应急响应工作。

6.2 职业技能等级要求描述

表 1 网络安全应急响应职业技能等级要求（初级）

工作领域	工作任务	职业技能要求（初级）
1.应急响应准备	1.1 应急响应组织建立	1.1.1 能根据工作要求，完成应急事件的日常值守工作； 1.1.2 能够根据工作要求，完成日常的监测和预警工作； 1.1.3 能够根据工作要求，记录日常应急工作日志； 1.1.4 能根据工作要求，完成应急响应小组内的其他工作；
	1.2 应急预案编制	1.2.1 理解信息安全事件分类分级指南等相关国家标准； 1.2.2 理解应急预案中规定的应急工作流程； 1.2.3 掌握应急预案中要求的应急工作方法； 1.2.4 根据应急预案要求对网络和信息系统进行监测； 1.2.5 根据应急预案的要求，对发现的风险进行预警和上报；
	1.3 系统备份	1.3.1 根据备份计划要求，对操作系统定期进行快照和文件备份； 1.3.2 根据备份计划要求，对数据库定期进行快照和数据备份； 1.3.3 根据备份计划要求，对网络设备定期进行快照和配置备份； 1.3.4 根据备份计划要求，对网络安全软件、设备进行快照和策略备份；
	1.4 系统加固	1.4.1 能利用注册表和安全策略实现 Windows 服务器的安全加固； 1.4.2 能根据要求正确配置 Windows 服务器的用户权限和文件系统权限； 1.4.3 能配置 Windows 服务器自身的防火墙； 1.4.4 能正确选择安装 Windows 系统版本的补丁
2.应急演练	2.1 应急演练方案制定	2.1.1 能根据应急演练方案,拟定应急演练通知，并对涉及到的部门进行通告； 2.1.2 能根据应急演练方案中的日程计划，编写具体的演练脚本； 2.1.3 能根据修改意见，对具体的演练脚本进行修改； 2.1.4 能根据应急演练方案的要求，盘点演练范

工作领域	工作任务	职业技能要求（初级）
		围内的 IT 资产并进行登记；
	2.2 应急演练实施	2.2.1 能够按照演练方案要求，完成具体的演练脚本执行； 2.2.2 能根据演练指令,模拟网络安全攻击的开展； 2.2.3 能根据演练指令，模拟系统发生故障的现象； 2.2.4 能根据演练指令，进行安全事件的应急处置；
	2.3 应急演练总结	2.3.1 能根据应急演练实际情况，编写演练过程记录； 2.3.2 能总结自己参与的部分工作，填写演练评价表； 2.3.3 能编写演练自我评价总结材料； 2.3.4 能够根据要求将演练方案、演练评估报告、演练总结报告等资料归档保存；
3.应急事件分析	3.1 系统信息收集分析	3.1.1 能利用工具和命令收集操作系统的硬件、系统组件、用户、补丁和应用软件等各种信息； 3.1.2 能利用工具和命令完成对操作系统主机名、版本、内核等信息的收集； 3.1.3 熟悉关键注册表的关键目录，能 Windows 操作系统的注册表导出和分析； 3.1.4 能利用工具和命令收集操作系统的进程、启动项等信息，并完成初步分析； 3.1.5 能利用工具和命令收集操作系统的服务、计划任务等信息，并完成初步分析； 3.1.6 能利用工具和命令收集操作系统的网络连接、端口开放等信息，并完成初步分析； 3.1.7 能利用工具和命令收集操作系统的账户信息，并完成初步分析；
	3.2 日志分析	3.2.1 能够通过系统自带程序或命令查看 Windows 系统中的安全日志，并根据日志查找异常登录信息，系统或应用程序崩溃信息等； 3.2.2 能够通过系统自带程序或命令查看 Linux 系统中的安全日志，并根据日志查找异常登录信息，系统或应用程序崩溃信息等； 3.3.3 能够依据系统日志文件、备份信息、应用程序日志，分析系统是否遭受溢出攻击，是否存在隐藏账号，是否存在非法使用账号等； 3.3.4 能够使用工具或命令导出系统日志，并利用第三方工具进行日志分析；
	3.3 流量分析	3.3.1 能够理解和配置网卡的混杂工作模式；

工作领域	工作任务	职业技能要求（初级）
		3.3.2 能够利用抓包工具，获取、保存 Windows 系统主机的网络流量数据； 3.3.3 能够利用抓包工具，获取、保存 Linux 系统主机的网络流量数据； 3.3.4 能够利用命令和工具，获取、保存网络设备的网络流量数据；
	3.4 威胁情报分析	3.4.1 能利用工具计算可疑文件的 Hash 值； 3.4.2 能使用威胁情报利用平台进行 Hash 查询，对可疑文件进行初步判断； 3.4.3 能使用威胁情报利用平台进行 IP 查询，对可疑数据包进行初步判断； 3.4.4 能使用威胁情报利用平台进行域名查询，对可疑网址进行初步判断；
	3.5 分析工具使用	3.5.1 能掌握 windows 操作系统命令的使用方法； 3.5.2 能掌握 Linux 中常用 shell 命令的使用方法； 3.5.3 能掌握进程监控管理工具的使用方法； 3.5.4 能掌握驱动程序管理工具的使用方法； 3.5.5 能掌握日志采集工具的使用方法； 3.5.6 能掌握流量抓包工具的使用方法；
4.应急事件处置	4.1 有害程序事件处置	4.1.1 能熟悉使用常见的防病毒软件，并能根据要求进行配置； 4.1.2 熟悉病毒和木马的基本分类和特征，能根据防病毒软件的查杀日志，分析常见的病毒和木马感染情况； 4.1.3 能利用日志和工具找到系统中的可疑程序，并进行样本提取； 4.1.4 能熟练地搭建和使用虚拟环境沙箱，对可疑程序进行初步分析和判断； 4.1.5 能根据要求收集有害程序的破坏现象和现场情况，连同样本一起进行上报； 4.1.6 能根据处置要求，完成对有害程序的隔离和清除；
	4.2 网络攻击事件处置	4.2.1 能根据日志判断攻击者实施攻击的时间范围，以便后续依据此时间进行溯源分析； 4.2.2 能通过在日志中发现的问题，针对攻击者活动路径，排查服务器中存在的漏洞，并进行分析； 4.2.3 能对已发现的漏洞进行漏洞复现，从而还原攻击者的活动路径； 4.2.4 能对已发现的 Webshell 文件进行清除工

工作领域	工作任务	职业技能要求（初级）
		作，并将之前发现的漏洞进行修复； 4.2.5 能通过设备记录信息，对访问异常 IP 进行封堵；
	4.3 信息破坏事件处置	4.3.1 能根据安全设备的预警信息和现场情况判断服务器是否遭受页面篡改； 4.3.2 能根据要求立即隔离被感染服务器，防止病毒继续感染其他服务器； 4.3.3 能对其他服务器进行排查，检查核心业务系统是否受到影响，生产线是否受到影响，并检查备份系统是否有植入后门； 4.3.4 能根据日志和文件痕迹排查攻击的入侵途径；
	4.4 设备故障处置	4.4.1 能找到故障设备，第一时间收集故障信息并进行上报； 4.4.2 能根据业务需要，将故障设备下线，保障网络通信不受影响； 4.4.3 能对设备的简单故障进行排查，快速修复设备； 4.4.4 能根据业务需要，将替换备机进行快速上线；

表 2 网络安全应急响应职业技能等级要求（中级）

工作领域	工作任务	职业技能要求（中级）
1.应急响应准备	1.1 应急响应组织建立	1.1.1 能根据应急响应组织要求，编写单位的应急响应管理制度和组织工作流程； 1.1.2 能根据要求，安排日常的监测与预警工作； 1.1.3 能够划分不同的应急小组，并设定责任人； 1.1.4 能协调应急响应小组涉及到的各方单位，完成协同作业；
	1.2 应急预案编制	1.2.1 能根据单位整体网络安全情况，编制通用的网络安全应急预案； 1.2.2 能根据评审要求，对应急预案进行修改和完善； 1.2.3 熟悉单位工作流程，能够完成应急预案的提交和发布工作； 1.2.4 能根据情况变化，进行应急预案的更新；
	1.3 系统备份	1.3.1 能根据安全要求，编制各系统具体的备份

工作领域	工作任务	职业技能要求（中级）
		计划； 1.3.2 能根据安全要求，检查系统快照和备份文件是否被破坏； 1.3.3 根据业务需求，检查网络是否存在单点故障点，在关键位置配置冗余链路； 1.3.4 根据业务需求，建立网络存储，存放备份文件；
	1.4 系统加固	1.4.1 能根据要求进行Linux服务器的安全加固配置； 1.4.2 能根据安全加固方案，完成对数据库的安全加固工作； 1.4.3 能根据安全加固方案，完成对中间件的安全加固工作； 1.4.4 能根据安全加固方案，完成交换机、路由器、防火墙等网络设备的安全加固；
2.应急演练	2.1 应急演练方案制定	2.1.1 能根据事件等级、演练规模、演练目的等，对演练组织进行职责划分； 2.1.2 根据单位安全要求，编制应急演练方案； 2.1.3 能根据应急演练方案，安排应急演练具体的日程计划； 2.1.4 能根据应急演练方案，编制演练经费预算；
	2.2 应急演练实施	2.2.1 在演练开始前组织演练动员和培训； 2.2.2 能协调各参演机构按照演练方案开始进行应急演练； 2.2.3 能对演练中上报的安全事件进行分级，启动对应的应急预案； 2.2.4 能对应急演练中的突发事件进行快速研判和处置；
	2.3 应急演练总结	2.3.1 能采集演练过程中各单位的完成情况，并形成演练记录； 2.3.2 能对参演人员进行访谈，并完成评价； 2.3.3 能根据演练的完成情况，编写演练评估报告； 2.3.4 根据演练记录、演练评估、演练方案等材料，对演练进行系统和全面的总结；
3.应急事件分析	3.1 系统信息收集分析	3.1.1 能分析系统的进程、服务、加载模块和启动项的异常情况； 3.1.2 能分析系统的用户信息，排查仿冒账户、隐藏账户、空口令账户和非法账户； 3.1.3 能分析系统启动项和计划任务，排查非法

工作领域	工作任务	职业技能要求（中级）
		程序； 3.1.4 能基于系统崩溃转储功能，实现内存获取； 3.1.5 能利用工具软件实现基于内核模式程序的内存获取； 3.1.6 能利用虚拟化快照，实现内存获取；
	3.2 日志分析	3.2.1 能借助 IPS、IDS、WAF 告警日志，对疑似攻击告警进行分析； 3.2.2 能借助安全网关设备，对可疑攻击 IP 进行排查； 3.2.3 能借助行为管理设备日志，对可疑外接流量进行排查； 3.2.4 能借助网络设备日志，对扫描和登录行为进行排查；
	3.3 流量分析	3.3.1 能根据数据包保存需求拆分、合并网络流量数据包； 3.3.2 能根据解析协议要求，在网络流量数据中筛选、重组指定的流量数据； 3.3.3 能解析数据包中携带的五元组信息、载荷内容等； 3.3.4 能利用工具对流量载荷中的文件进行还原
	3.4 威胁情报分析	3.4.1 能使用威胁情报平台查寻域名、URL、IP、文件 Hash、文件路径、文件名、数字签名、备案信息； 3.4.2 能通过配置，将单位的 SOC 等网络安全设备与威胁情报库进行关联对接； 3.4.3 能将威胁情报应用到企业的业务安全中，如账号风控，防欺诈，信息泄露等；
	3.5 分析工具使用	3.5.1 能掌握日志分析工具的使用方法； 3.5.2 能掌握内存镜像工具的使用方法； 3.5.3 能掌握进程 dump 工具的使用方法； 3.5.4 能掌握证据收集等工具的使用方法； 3.5.5 能掌握程序行为分析工具的使用方法； 3.5.6 能掌握在线恶意程序分析工具的使用方法； 3.5.7 掌握 webshell 检测软件的使用方法
4.应急事件处置	4.1 有害程序事件处置	4.1.1 能对有害程序常用的敏感路径、文件权限特征进行分析排查； 4.1.2 能根据应急事件发生的时间，对时间点前后的文件进行排查；

工作领域	工作任务	职业技能要求（中级）
		4.1.3 能根据以上分析结果，结合程序的行为进行综合判断，并编写分析报告； 4.1.4 熟悉蠕虫病毒、勒索软件、挖矿木马、webshell 等常见有害程序的特征，能根据具体情况给出相应的应急处置意见； 4.1.5 能在处理有害程序之后，利用备份对数据和业务进行还原和恢复；
	4.2 网络攻击事件处置	4.2.1 能对各种拒绝服务攻击抑制和处置； 4.2.2 能对各种弱口令攻击进行抑制和处置； 4.2.3 能对各种 DNS 欺骗攻击进行抑制和处置； 4.2.4 能对各种 SQL 注入攻击进行抑制和处置； 4.2.5 能对各种跨站脚本攻击进行抑制和处置
	4.3 信息破坏事件处置	4.3.1 能根据现象分析判断数据的泄露途径和流转路径； 4.3.2 能根据分析情况确定漏洞源头，并进行溯源分析； 4.3.3 能依据数据泄露事件类型、安全措施现状，制定应急处置策略； 4.3.4 能在应急处置之后，恢复服务器的数据和业务；
	4.4 设备故障处置	4.4.1 能对故障设备的情况做评估，判断是否更换设备； 4.4.2 能对设备的常见故障进行排查分析，并进行设备修复； 4.4.3 能协调并找到替换备机，保障网络和业务正常使用； 4.4.4 能编写故障应急处理总结报告；

表 3 网络安全应急响应职业技能等级要求（高级）

工作领域	工作任务	职业技能要求（高级）
1.应急响应准备	1.1 应急响应组织建立	1.1.1 能根据单位情况，组建应急响应组织； 1.1.2 能邀请第三方专家加入应急响应组织； 1.1.3 能够建立应急响应组织的考核机制，明确考核指标及方法； 1.1.4 能够负责应急响应组织日常的管理工作；
	1.2 应急预案编制	1.2.1 能根据具体情况，组织通用应急预案的评

工作领域	工作任务	职业技能要求（高级）
		审； 1.2.2 根据业务需求，对需要重点保护的核心系统编制专项应急预案； 1.2.3 能根据单位情况，制定应急预案的内部培训计划； 1.2.4 能面向高层部门，进行应急预案的汇报工作；
	1.3 系统备份	1.3.1 能根据业务需求，对各系统的备份计划进行审核和修改； 1.3.2 能根据业务需求，规划单位的整体数据备份方案，实现数据级备份； 1.3.2 能根据业务需求，规划单位的应用系统备份方案，实现系统级备份； 1.3.3 能根据业务需求，规划单位的多地多中心建设方案，以实现业务级备份；
	1.4 安全加固	1.4.1 能参考行业做法，编制单位的安全基线； 1.4.2 能根据安全基线要求，检查各系统基线符合情况； 1.4.3 能根据不同的安全等级，制定不同信息系统的安全加固方案； 1.4.4 能在重保等特殊时期，根据要求制定专项安全加固方案；
2.应急演练	2.1 应急演练方案制定	2.1.1 能建立演练组织，包括管理部门、指挥机构和参演机构； 2.1.2 能根据情况，对应急演练方案进行审核，并提出修改意见； 2.1.3 对涉及到重点时期或重点系统的演练方案，能够组织专家评审； 2.1.4 能根据情况，审查提交的演练经费预算计划；
	2.2 应急演练实施	2.2.1 能在演练正式开始前安排一次或多次预演； 2.2.2 能检查演练各环节准备是否到位； 2.2.3 能根据准备情况，在合适的时间下发演练启动通知； 2.2.4 能对演练实施全过程的指挥控制，随时掌握演练进展情况；
	2.3 应急演练总结	2.3.1 能分析演练记录及相关资料，对演练活动及组织过程做出客观评价； 2.3.2 能对提交的演练评估报告进行审核；

工作领域	工作任务	职业技能要求（高级）
		2.3.3 能根据演练评估报告，编写演练总结，并向上级部门汇报； 2.3.4 能根据演练总结，回顾单位的应急响应准备工作，并编写改进计划；
3.应急事件分析	3.1 系统信息收集分析	3.1.1 能够利用内存分析工具进行内存的导入和分析； 3.1.2 能够利用工具来分析内存中的入侵攻击痕迹； 3.1.3 能够利用工具对从内存中提取出来的文件进行分析，判别文件是否有恶意行为； 3.1.4 能根据内存和其他系统运行情况，进行系统信息的综合分析；
	3.2 日志分析	3.2.1 能掌握常见 Web 服务器、数据库、中间件的日志种类、存放位置以及排查方法； 3.2.2 能编写代码对日志信息进行汇总、分析、查询； 3.2.3 能利用开源工具或平台对系统日志、应用日志进行汇总、分析、查询； 3.2.4 能通过日志分析结果对攻击进行溯源分析；
	3.3 流量分析	3.3.1 利用沙箱，对流量还原文件进行威胁分析，判断是否存在恶意程序； 3.3.2 能够综合运用数据关联分析工具，挖掘数据包之间的数据关联关系； 3.3.3 能利用攻击特征库，检测流量中的常见扫描行为和常见的远控木马等攻击行为； 3.3.4 能够运用工具对流量信息和威胁情报进行碰撞比对，分析、挖掘攻击线索；
	3.4 威胁情报分析	3.4.1 能了解各种威胁情报源，掌握各个威胁情报平台的使用方法； 3.4.2 能根据业务情况和单位安全规划，建立单位自己的威胁情报库； 3.4.3 能结合分析工具和方法提取多种维度数据中的有效信息，形成威胁情报； 3.4.4 能根据情况，针对上级单位和兄弟单位建立情报的上报机制和协同分享机制；
	3.5 分析工具使用	3.5.1 能掌握沙盒、逆向分析等工具的使用方法； 3.5.2 能掌握常见静态分析工具和动态分析工

工作领域	工作任务	职业技能要求（高级）
		具的使用方法； 3.5.3 能掌握内存分析工具的使用方法； 3.5.4 能掌握系统内核分析工具的使用方法； 3.5.5 能掌握驱动程序管理工具的使用方法；
4.应急事件处置	4.1 有害程序事件处置	4.1.1 熟悉常见加密解密技术、加壳脱壳基本原理和步骤以及工具的使用，能对可疑程序进行手工脱壳和解密； 4.1.2 能对提交的可疑程序样本进行静态代码分析和动态调试； 4.1.3 能根据有害程序造成的破坏严重程度和规模进行综合评估，并启动相应等级的应急预案； 4.1.4 能对有害程序事件进行溯源，找到传播来源，并对网络薄弱环节进行相应的加固；
	4.2 网络攻击事件处置	4.2.1 熟悉拒绝服务攻击原理，能对各种拒绝服务攻击事件进行应急处置； 4.2.2 熟悉常见后门原理，能对各种常见后门事件进行应急处置； 4.2.3 熟悉常见系统漏洞和 Web 漏洞原理，能对各种漏洞攻击事件进行应急处置； 4.2.4 熟悉常见扫描和网络窃听原理，能对各种扫描和网络窃听事件进行应急处置； 4.2.5 熟悉常见网络钓鱼事件原理，能对各种钓鱼事件进行应急处置；
	4.3 信息破坏事件处置	4.3.1 熟悉常见信息篡改方式方法，能够处置各种信息篡改事件； 4.3.2 熟悉常见信息假冒事件原理，能够处理各种信息假冒事件； 4.3.3 熟悉常见信息泄露方式，能够处置各种信息泄露事件； 4.3.4 熟悉常见信息丢失事件原理，能够处置各种信息丢失事件；
	4.4 设备故障处置	4.4.1 能协调服务商和供应商，对复杂的设备故障进行排查分析，修复设备； 4.4.2 能对设备的故障原因进行综合分析，判断是否是网络攻击，并根据情况启动相应的应急预

工作领域	工作任务	职业技能要求（高级）
		案； 4.4.3 能根据故障应急处理总结，组织对所有设备的安全巡检工作，彻底排查隐患； 4.4.4 能总结安全巡检情况，改进设备的加固方案；

参考文献

[1] 《中等职业学校专业教学标准（试行）》目录

[2] 高等职业学校专业教学标准

[3] 教育部关于印发《职业教育专业目录（2021 年）》的通知（教职成〔2021〕2 号）

[4]《教育部关于公布 2019 年度普通高等学校本科专业备案和审批结果的通知》（教高函〔2020〕2 号）

[5]《教育部关于公布 2020 年度普通高等学校本科专业备案和审批结果的通知》（教高函〔2021〕1 号）

[6] 《中华人民共和国突发事件应对法》

[7] 《网络安全法》

[8] 《国家网络安全事件应急预案》

[9] 《关键信息基础设施安全保护条例（征求意见稿）》

[10] GB/T 38645-2020 信息安全技术 网络安全事件应急演练指南

[11] GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求

[12] GB/T 28827.3-2012 信息技术服务 运行维护 第 3 部分：应急响应规范

[13] GB/T 1.1-2009 标准化工作导则

[14] GB/T 24363-2009 信息安全技术 信息安全应急响应计划规范

[15] GB/T 20988-2007 信息安全技术 信息系统灾难恢复规范

[16] GB/Z 20986-2007 信息安全技术 信息安全事件分类分级指南

［17］ GB/Z 20985-2007 信息安全技术 信息安全事件管理指南

［18］ GB/T 20270-2006 信息安全技术 网络基础安全技术要求