网络应急响应平台系统

1. 系统总体要求

本系统要求解决某市针对各企业在日常工作中遇到的各种网络安全事件的各项事务性工作管理，将工作内容以派单的表现形式，通报下发、追踪反馈、处罚及消除等各项环节的进度和各项信息，实现日常工作的数据化、可视化、便捷化。

1.1 平台涉及的用户角色

平台包括四类用户角色：

A、市级一级安全管理用户

平台的各类安全事件通报、热点事件发布的最初发起者，将上级部门下发的各类文件精神或本身工作中发现的威胁情报、安全事件、安全热点事件派发给各下属各辖区管理用户；

B、市级各辖区安全管理用户

接收或自行发布上级市级一级用户 A 下发的涉及本辖区的各企业的网络安全事件通报、热点事件，直接处理或将其下发至涉事受监管企业；对安全事件处理的反馈结果做出处置，并反馈上级；

C、受监管企业部门用户

企业关键基础设施的信息系统负责人员。

根据市级各辖区安全管理用户 B 所发布的安全热点事件及时更新、维护本企业的信息系统;针对上级部门下发的涉及本企业信息系统的安全事件,及时核验、整改后提交反馈报告。对不能独立处置的可以要求第三方安全服务公司进行上门支持。

D、第三方安全服务公司用户

与市级管理部门签约的安全服务或与受监管企业单位签约的技术支持公司。针对企业受监管企业用户 C 下发的安全事件，接单后对涉事企业发起预约，上门检测、核实事件、进行应急响应服务等工作，完成后向企业受监管企业用户 C 提交检测/处置报告。

各级用户账号密码，由管理员账号添加后派发，不开放注册。

2.2 主要功能模块

2.2.1 登录平台

通过用户账号密码登录平台。

2.2.2 用户管理

这个功能主要针对平台管理员，包括功能如下：

1、单位类型管理

基于用户性质，编辑用户的用户类型：市级单位、市级各辖区单位、受监管企业单位、签约技术支持/安全服务单位。

2、单位管理

显示建立的单位列表，并能够进行单位新建、修改和删除操作。

单位信息应包括：单位名称、单位地址、单位类型、单位负责人及联系方式、单位网安管理员及联系方式。

3、用户列表

显示建立的用户列表，并能够进行用户新建、修改和删除操作，能够进行系统授权管理。

用户信息应包括：姓名、电话、邮件、微信号、所属单位、单位类型、启用状态以及信息操作等字段。

4、登录日志

用于显示每一个账号的登录日志列表（支持数据列表的分页显示）。

2.1.3 系统（平台）管理

不同角色的用户登录系统平台后都可以看到：首页工作台以及主要的三大功能模块：

1、事务管理（监控）

包括待办事项、处理中事项、已完成事项三个部分。

点击任何一个，显示该项中的数据列表。

事件类型分：违处信息、网络攻击、恶意软件、信息泄露、安全威胁/漏洞。

事件信息包括：事件编号、单位名称、事件发布时间段、事件类型、事件处

理状态、具体事件描述等。（事件信息需要在此基础上扩展）

2、安全事件管理

包括安全事件通报、热点事件发布、处理中事件、已完成事件。

根据通报对象点对点推送。

对安全事件通报、热点事件发布，只有市级一级单位和市级辖区单位可以进行发布。

能够通过查询，查看指定事情的处理进度或处理状态。

能够根据指定时间段、事件、辖区、企业名称等查询，并列出数据列表。

3、数据统计

包括对已通报、已处理、处理中、未处理事件进行**分类统计**，要列出列表，或绘制图形显示。