网络安全事件专家团队远程应急的功能实现探讨

周肃然　麦海新　叶贺杰
中国联合网络通信有限公司东莞市分公司　广东　东莞　523009

摘　要：传统的网络安全应急响应模式已无法满足快速、高效处置的需求。本文提出了一种网络安全快速响应能力平台的构建方案，旨在通过专家团队协作、便携应急终端及云上管控平台的综合应用，实现安全事件的分钟级响应和快速处置。文章详细阐述了平台的实现方式、应急业务流程及各功能模块，并探讨了其应用场景与推广前景。

关键词：网络安全；应急响应；专家团队；便携终端；云管控平台

引言

近年来，网络安全威胁日益严峻，安全事件的快速响应和处置成为维护网络空间安全的关键。传统的应急响应模式存在响应时间长、依赖个人能力及工具不规范等问题。因此，本文提出了一种新型的网络安全快速响应能力平台，以破解这些痛点，提升应急处置的效率和规范性。

1 网络安全事件应急处置痛点分析与应急平台构想

1.1 痛点分析

1.1.1 响应时效性问题

网络安全事件通常具有突发性和不可预测性，初步的问题诊断往往仅能通过与客户的简要沟通来进行。随后，需要根据问题的性质尽快调配具备相关专业技能的工程师赴现场处理。然而，当现场工程师遇到难以解决的问题时，常常需要寻求电话支持、远程技术援助，甚至需要从其他地区调配更专业的工程师。这一过程耗时且效率低下，导致应急响应时间无法得到有效保障[1]。

1.1.2 技术人员专业能力要求严苛

随着计算机技术的日新月异，信息网络日益复杂化，网络环境中充斥着大量敏感信息，甚至包括国家机密。这种环境不可避免地会吸引全球范围内的各种安全威胁，例如信息泄露、数据窃取、数据篡改、非法数据增减以及计算机病毒等。因此，对应急处置人员的技术能力提出了极高的要求。遗憾的是，当前网络安全专业人才依然稀缺，难以满足行业对高技术能力的迫切需求。

1.1.3 应急处置工具缺乏统一性

信息网络的迅猛发展和多样化的技术环境，要求应急处置工具能够适配不同的网络接入、控制和扫描需求。在实际操作中，工程师可能需要寻求远程专家协助，但由于缺乏标准化的应急处置工具，处置效率受到严重影响。此外，在处理敏感和重要数据时，为确保客户和技术人员的安全，应急处置过程需要进行详细的取证和记录。然而，目前常常需要工程师在处理问题的同时，使用手机或相机进行拍照记录，这种做法严重影响了工作效率。

1.2 平台构想

针对网络安全事件应急处置的现存痛点，构想一个全面且规范的网络安全快速响应平台至关重要。该平台构想主要包含以下三个核心组成部分：

1.2.1 应急专家团队

通过建立高效的安全专家团队协作机制，可以有效缓解当前网络安全技术人员短缺的问题。在此机制下，多个技术专家能够同时对某一网络安全应急事件进行协同处理，这不仅提升了处置效率，还解决了单一工程师技能偏颇或不足的问题，从而确保更全面、专业的应急响应[2]。

1.2.2 应急便携终端

这些终端设备可由客户预先采购并放置在关键位置，或由就近的工作人员快速携带至应急现场。通过这种方式，可以显著减少现场响应时间，提升应急处理的时效性。

1.2.3 管控平台

该平台旨在实现对应急专家团队人员和便携终端设备的综合管理。通过精细的人员与设备接入认证、授权、审计、角色分配等机制，确保人员与设备的无缝对接和高效协作。此外，该平台还具备强大的可扩展性，能够集成多种功能模块，如提供标准化的应急工具，以确保应急过程的效率与规范性。特别是通过集成堡垒机功能，可以对整个应急过程进行全面的监管和取证，从而保障操作过程的透明性和可追溯性。

2 实现方式与功能模块

2.1 急专家团队

应急团队的构建可分为以下三个核心组成部分：首先是监管团队，该团队主要由网信部门、行业监管机构

的代表以及客户的管理层人员组成。这些成员在平台上拥有查看权限，主要负责对应急处理过程进行跟踪和监督。为确保信息安全，他们的系统账号将根据实际情况，由系统管理的客服人员临时创建并分配相应的角色。一旦应急处理结束，这些账号将会被回收。其次是现场应急处置团队，这个团队的成员主要来自应急支持单位或合作伙伴。他们不需要具备极高的技术水平，但需要有很强的机动性，以便在网络安全事件发生后能够迅速到达现场，并确保应急终端设备能够及时上线并接入平台。根据实际情况，这部分人员可能不会分配平台账号，或者会分配一个应急支持工程师的账号，以便他们能够有效地参与应急处置工作。最后是应急专家团队，这个团队进一步分为常驻专家团队和外部专家团队。常驻专家团队会提前在系统上进行注册，并被分配相应的账号和权限角色。而外部专家团队则会在需要时由平台客服临时添加，他们的权限角色与常驻应急团队保持一致。应急处理结束后，这些临时添加的账号也将被回收[3]。

2.2 便携应急终端

2.2.1 应急终端内部构造

便携应急终端采纳了先进的虚拟化技术，以EXSI虚拟化平台为基础，能够与管控平台的VCENTER实现互联，既可接受VCENTER的全面管控，也具备独立工作的能力。此终端在初始化时便预置了多个系统和应用软件，利用快照技术，可以迅速恢复到初始状态，从而确保整个平台的稳定性和可靠性。为了构建一个灵活且高效的工作环境，应急终端内部构建了一个小型局域网。这个局域网基于性能卓越的X86平台工控小主机，并安装了EXSI虚拟化软件，形成了一个功能完备的虚拟化网络环境。

2.2.2 应急终端系统组成及其功能

①EXSI虚拟化平台的Web管理模块，不仅负责对应急终端内的虚拟机资源进行分配和管理，同时还能够与云上管控平台进行注册与联动。根据接入用户的角色以及虚拟机的权限配置，该模块能够智能地分配和管理虚拟机功能模块的资源。

②此终端预装了多个标准化的应急系统和软件虚拟机，例如KALI等，这些系统和软件能够用于安全扫描、渗透测试以及系统分析等任务，从而有效地对客户内网进行问题排查与分析。现场工程师可以直接利用这些预装的软件工具进行应急处理工作，大大提高了工作效率。

③此外，该终端还支持对孤岛设备（即那些网络隔离或无法接入互联网的设备）进行远程操控。通过采用USB键鼠模拟结合USB视频采集卡的解决方案，实现了远程键盘和鼠标的操作以及屏幕画面的回传功能，而且无需在孤岛设备的主机上安装任何额外的软件。

2.3 云上管控平台

2.3.1 云端统一管理平台的构建

云端管理平台与终端管理平台在技术和架构上保持高度一致性，同样采用虚拟化技术部署，其内部网络结构也设计为一个小型虚拟局域网。这种设计确保了管理的统一性和便捷性。统一管理平台功能实现路径如下图：

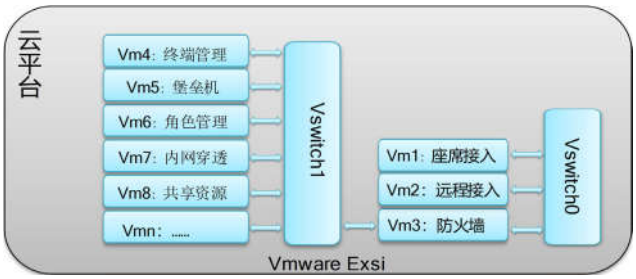

图1 统一管理平台功能实现路径示意图

2.3.2 系统组件及其核心功能

①出口防火墙：配置有公网IP地址或域名，负责对外提供安全的接入服务。其功能涵盖应急终端的回传接入管理，以及为应急专家团队和监管部门人员提供远程访问接口。

②VCENTER虚拟服务器：作为应急终端盒子的核心管理组件，它执行应急终端设备的在线状态监测、角色权限的分配与管控等任务。

③远程接入认证管理虚拟服务器：专注于管理应急团队及监管部门人员的VPN接入认证，确保只有合法用户能够远程接入系统。

④堡垒机：在应急团队通过堡垒机访问系统后，根据预先分配的角色和权限，对应急终端进行安全操作。堡垒机能够全面记录和审计用户的所有操作行为，包括执行的命令和输出结果。这些记录可以是简要的日志形式，也可以是完整的操作屏幕录制，以便后续进行事件取证和溯源。

⑤内网穿透服务端：该组件在应急终端与管控平台之间建立起多种类型的安全隧道，例如HTTP代理、TCP隧道、UDP隧道、SOCKS代理以及P2P连接等。这些隧道为应急工程师提供了远程接入应急现场网络的能力，从而能够利用应急终端高效地进行应急处置工作。

⑥共享资源服务：提供一个集中的存储资源共享环境，其中包括报告的上传与管理功能，以及丰富的知识库、案例库和工具库等资源。这些共享资源为团队提供了便捷的信息获取途径，助力提升应急响应的效率和准

确性[4]。

3 应急业务流程与应用场景

3.1 应急业务流程

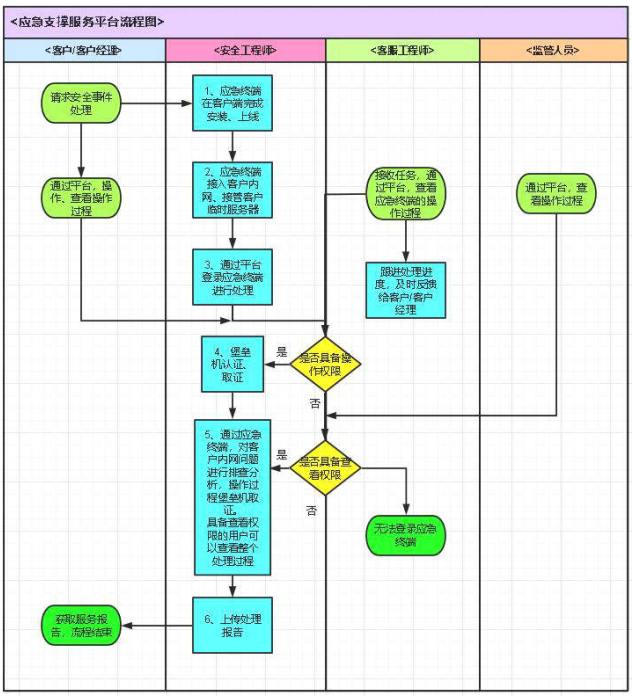

图2 应急业务流程示意图

3.2 应用场景

3.2.1 常态化应急管理场景

在此场景下，应急终端作为一种常态化服务支持设备，发挥着重要作用。客户通过采购安全支撑服务，将应急终端设备预先放置在用户机房，并完成接入环境的部署，确保应急终端设备持续在线。在这种状态下，应急终端主要充当网络探针和服务前端的角色。安全服务提供商可以借助这些终端，定期对用户内部网络进行网络安全巡查、检测、隐患排查以及风险评估等工作。一旦发生安全事件，应急终端能够确保服务提供商第一时间介入，并迅速进行处置。

3.2.2 突发事件应对场景

该场景主要应对突发情况下的应急工作，特别是在应急现场缺乏专业人员和设备时。在这种情况下，管理部门或主管部门会紧急调配应急工程师前往现场进行处理。就近的应急前端人员（并不一定是专业的应急工程师）会携带应急终端迅速到达现场，完成设备的加电和网络接入工作。随后，后台的应急团队通过远程平台协同处理应急事故。在这种突发场景下，应急终端设备到达现场的时间取决于设备提前分发到各个区域的细致程度。设备到达现场后，现场人员无需具备高度专业的技术知识，只需熟练地将设备上电、开启WIFI热点，并配合远程应急团队做好现场的物理连接工作即可。

4 推广应用前景

在网络安全领域，针对APT攻击、勒索病毒、高危漏洞利用以及重要信息系统的保卫防守等重大突发事件，传统的处置方式往往受限于组织间的隔阂与沟通不畅。而本方案则针对这一问题，通过引入应急作战室机制，实现了跨组织的高效协同。具体而言，当重大安全事件发生时，本方案能够迅速集结组织内外所有可用的专家资源，构建成一个虚拟团队。这个团队不受地域、机构或部门的限制，成员间可以实时进行消息沟通、线索数据共享及研判。通过高效的协同工作，团队成员能够迅速对应急事件进行会诊，确定最佳处置策略，并通过人机交互指令下发，确保处置措施的准确执行。这一机制的引入，不仅打破了传统应急响应中的组织壁垒，更在实战中展现了极高的协同处置效率。无论是在线索追踪、威胁分析，还是在快速响应和恢复系统方面，本方案都表现出了显著的优势。展望未来，随着网络安全威胁的日益复杂化，这种高效、灵活的协同处置模式将变得更为重要。本方案不仅适用于大型企业或政府机构的网络安全防护，也同样适用于中小企业，为其提供强有力的安全支撑。因此，本方案具有广阔的推广应用前景，有望成为未来网络安全领域的重要发展方向。

结语

本文提出的网络安全快速响应能力平台构建方案，有效解决了传统应急响应模式中的痛点问题，实现了安全事件的快速响应和高效处置。通过应急专家团队、便携应急终端和云上管控平台的综合应用，提升了应急处置的效率和规范性，具有广阔的推广应用前景。

参考文献

[1]郝志强,杨佳宁,张晓帆.面向多场景融合的工控安全应急响应系统研究[J].工业信息安全,2022,(08):6-11.

[2]王明.网络安全与应急响应[J].信息安全与通信保密技术,2020,6(2):34-46.

[3]荣晓燕,史宜会,桑磊,等.网络安全应急能力评估方法研究[J].保密科学技术,2022,(06):58-65.

[4]金京犬.网络安全应急响应日志分析服务技术研究[J].萍乡学院学报,2022,39(03):65-68.