防守基础安全指引

为提高我省关键信息基础设施安全防护水平，构建网络安全综合防控体系，广东省公安厅网络警察总队积极组织广东省“HW2020”攻防演习；此次演习制作《HW 演习防守基础安全指引》，希望发挥公安机关、安全专家、专业机构、用户单位各自优势，构建威胁情报可共享、安全风险早预防、安全事件快处置、违法犯罪共打击的“打防一体”网络安全防 HW，做到一点预警、全网联动的网络“安全罩”。

大部分企业的网络安全建设并没有系统化的考量，《HW 演习防守基础安全指引》希望引导防守方了解 HW 演习的要求，结合企业实际情况开展工作，配置基础安全设备提升网络安全防护能力，面对常见类型攻击时知晓应对操作，并建立 7*24 小时应急保障体系。

一、HW 演习的防守要求

1、建议由各单位领导层人员负责整体防守指挥。包括从上而下的统一协调调度，推动建立防守保障机制，推动防守工作的执行、进行防守资源的申请

2、需要整理并更新企业的相关网络资产清单，包括互联网资产、办公资产等。

3、需要建立对网络资产的基础安全保障能力，包括基

础安全设备和相应的人员。

4、有相关的人员针对企业自身资产进行 7*24 监测预警，针对高风险威胁告警进行分析，研判、处置并上报公安机关。

二、资产梳理

防守方需要对自身目标系统及关联资产梳理，形成资产清单。资产清单应包括 IP 地址、操作系统、中间件、应用软件、域名、端口、服务、责任人、联系方式等，便于快速的进行资产定位、风险处置、应急等工作的开展。

1、针对互联网资产梳理

缩减或集中互联网出入口。一是对所有的互联网出入口，按照就近归并的原则进行缩减或集中；二是对于新建系统，保证其网络出口统一；三是做好 VPN 的入口管理。

加强域名管理，缩减应用。一是废弃域名及时清理；二是网站归集，对于互联网上的多个域名，尽量集中、集约建设，方便统一防护。

互联网暴露敏感信息梳理。包括对文档信息（云盘、文库）、代码（github、gitee）、人员信息等进行发现、清理或联系上传者或平台方删除等工作。

互联网资产扫描。企业自身组织或采购安全服务商服

务，探测自身在互联网上暴露的资产，发现未知资产和风险端口，与现有资产清单进行对比梳理，形成准确的资产清单，并对风险端口进行评估关闭。

测试和临停梳理。测试系统和临时关停下线的系统，无法做到有效防护应做好访问控制或下线。

2、其他资产梳理

个人办公电脑的登记审核。一是包括 IP、MAC 地址、操作系统、是否安装防毒软件、二是对新增办公电脑要做好准入要求，对安全补丁、防病毒、密码强度等进行检查。

办公设备的登记审核。包括打印机、复印机、扫描仪、传真机，保密文件存储介质、电子门禁等。

网络设备的登记审核。包括交换机、路由器、网关、防火墙等，要做好相关梳理，如无必要不应暴漏在公网，并核查相关安全策略。

网络安全产品登记审核。包括 WAF、NF、IDS、IPS、HIDS、EDR、邮件网关、杀毒软件、网页防篡改等，并确认其安全补丁是否更新，安全策略及日志留存是否开启。

3、新增资产

新增资产归类登记。包括新增的 IP、域名、敏感文件、业务代码、新上线业务、新增测试环境、新增安全设备等

需要分类登记建档，并定期对变更状态进行更新，如测试环境在测试后应及时下线关停。

新增资产的上线核查。新增业务系统应由公司内部安全团队或第三方进行新上线检测，杜绝安全隐患；新增安全设备需检查安全策略配置并确保正常生效后启用；敏感文件和代码需做好相应的加密措施；办公设备需符合安装防病毒软件、开启防火墙等后才可使用，禁止无保护状态接入办公网。

三、建立网络安全防护能力

1、常见的网络拓扑

任何一家参与 HW 的防守单位，网络拓扑、业务应用各不相同，为了便于理解，我们从多家单位的网络拓扑中抽出共性特征，做出如图 2-1 的网络拓扑。

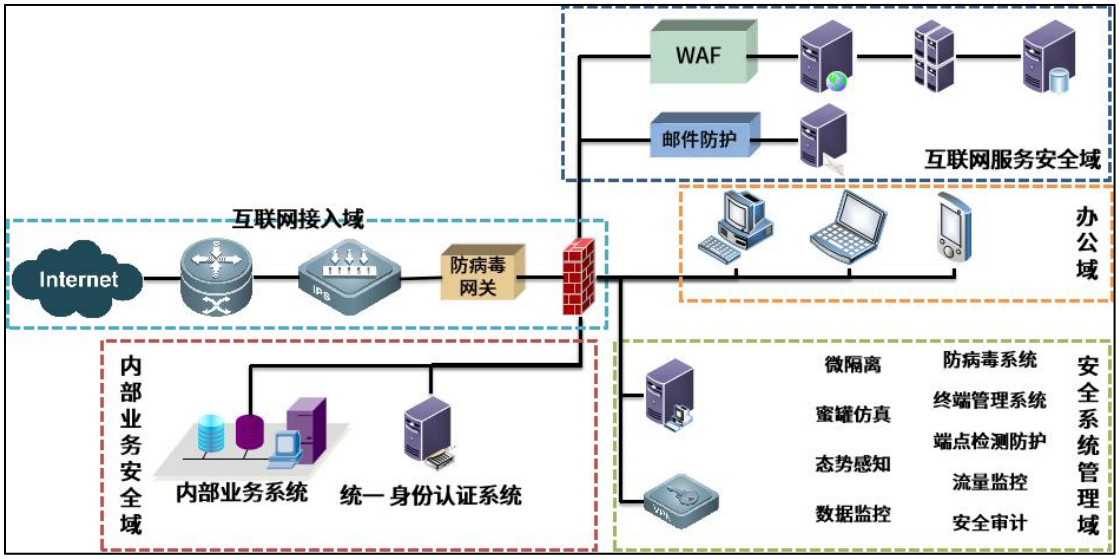


图 3-1：采用较多的网络安全拓扑

安全域的划分分为互联网接入域（负责互联网访问的接入及防护）、互联网服务安全域（负责面向互联网服务的业务系统）、办公域（员工办公使用）、内部业务安全域（公司内部使用的业务系统）、安全系统管理域（需要与互联网进行交互、但不向互联网提供服务的系统）。

2、安全域的划分和全局防护

安全域划分。一是根据业务、功能、地域、安全需求等划分安全域；二是安全域的访问采取访问控制（网络防火墙、主机防火墙）、恶意监测防护（入侵防护、恶意代码检测）等安全防护措施；三是业务流量与管理流量分离，攻击者即便攻破一个安全子域，也无法控制数据库或是获取数据；四是明确核心业务与非核心业务应用的管理边界与责任。安全子域之间的必须进行有效的访问控制，必须进行有效的流量攻击检测，才能阻拦攻击者在安全域之间的纵向渗透和横向移动。五是采用认证、加密、访问控制等技术措施，建立网络、应用、数据纵向防护和日志审计措施，及时发现非法行为。

网络层精细化管制。一是在网络层，利用防火墙设置 IP 白名单，仅开放必需向互联网提供业务支撑的应用前端；二是在应用层，利用 WAF，设置服务白名单，仅开放必需

向互联网提供的最小服务。三是梳理内部的网络应用，将网络流量按照管理、业务、应用进行分流，不同的流量互不干扰；四是管理端口仅允许授权可信源访问；五是加强VPN等设备的认证与访问控制；六是部署必要的安全防护设备，如域间的访问使用IPS、防病毒网关等对访问流量进行安全性监测；七是关停非必要系统、应用、服务、设备，减少不必要开放服务带来的安全风险；八是建立覆盖整个网络的流量监控体系，对全网的流量行为、尤其是异常流量进行监控。

3、常见的基础安全设备和防护措施

Web服务防护。一是使用**防火墙**控制控制访问源，仅允许访问业务端口；二是部署**Web应用防火墙**对应用层的攻击进行防护；三是部署**网页防篡改**系统对网页篡改攻击进行防护；四是部署主机**HIDS（主机型入侵检测系统）/EDR（端点监测响应）**产品，提升安全防护能力。

数据库防护。一是使用防火墙控制控制访问源，仅允许访问业务端口；二是部署**数据库防火墙**防范应用层的攻击；三是部署数据库审计产品对数据库的访问进行审计，对高危操作进行限制；四是按照访问源和角色进行授权管理；五是对数据按敏感程度进行分库、分级，完善访问控制措施，敏感数据采用加密传输、加密存储。

邮件系统防护。一是部署具备反垃圾邮件、防病毒或有沙箱功能的**邮件网关**进行安全防护；二是定期梳理邮箱帐户，禁用或删除不使用的帐户；三是对邮箱的登录地进行白名单与黑名单限制；四是进行弱口令检测，强制要求使用复杂口令，并通过技术手段控制定期更改口令。

集权系统安全精细管控。一是仅允许内部访问；二是强制用户定期修改、并强制使用强壮口令；三是重命名发生信息泄露的帐户；四是实时审计帐户变更、用户登录等相关日志；五是进行安全加固，修复已知的安全漏洞。

移动 APP。采用签名认证、更新前进行完整性验证、加壳混淆防范逆向、使用安全键盘、使用证书加密传输、敏感数据加密存储等技术手段提升安全防护能力。

VPN 防护。采用多因子认证保证 VPN 的登录安全，控制 VPN 设备的访问范围,对 VPN 的内部访问进行安全检测。

其他防护。建立外部威胁情报共享联盟，对恶意 IP 等实时同步，并在安全设备封禁；确保所有使用的产品或设备有进行安全更新。

4、其他的日常工作

企业需建立 7*24 小时的网络安全保障体系,应配备专职人员或外包服务团队及时查看安全防护系统的防护日志、威胁情报、收集漏洞信息，进行安全加固工作，对安全事

件进行处置。在利用好已有的安全防护设备外，建议企业针对现有的网络资产进行风险检查，如：

安全漏洞扫描。对主机系统、应用系统进行漏洞扫描，并验证漏洞有效性，形成漏洞列表，跟进漏洞的整改情况。同时对历史漏洞、网内弱口令进行自查和整改。

系统渗透测试。远程或现场开展渗透测试，发现安全漏洞隐患，形成漏洞列表，跟进漏洞的整改情况。

安全基线检查。对网络设备、安全设备、主机（操作系统、数据库、中间件）、应用系统等进行身份鉴别、访问控制、安全审计、规则更新升级、安全配置等方面的安全基线检查，对基线核查中发现的不符合项，制定基线更改方案，按计划对不符合项整改。

敏感信息梳理。一是制定敏感信息列表；二是通过联系信息的上传者、站点的运营方删除互联网上的敏感信息；三是对邮件服务器内的邮件进行归档，然后删除邮件服务器上含有敏感信息的邮件；四是对办公用机上的敏感信息，对于不是必须使用的，要求主机所有者进行删除，对于需要使用的信息，加密存储；五是对服务器上的敏感信息，不使用者统一进行彻底删除，若需使用，统一存储到备份系统中，并设定严格的访问权限。

弱口令治理。一是通过技术手段强制设定的口令必须满足复杂口令的要求；二是通过技术或管理手段要求每个

帐户（尤其是邮件系统、可在互联网上访问的系统）进行一次口令更改操作；三是使用安全工具进行弱口令探测，杜绝诸如“单位名称简称@123”等符合复杂口令要求的弱口令、杜绝曾经泄露过的口令；四是考虑对泄露过的帐户名、缺省帐户名进行重命名。

漏洞治理。一是制作信息资产的漏洞清单；二是制定漏洞修复方案，漏洞修复方案包括但不限于安装补丁、修改配置、更改访问控制、更改权限、部署安全防护设备等；三是对安全漏洞隐患、安全风险，积极整改并形成整改跟踪记录表，确保各层面问题整改到位；四是在完成漏洞修复后进行漏洞修复验证工作；五是梳理残留风险，以备后续进行风险处置或在安全应急中为事件提供分析依据。

进行安全意识培训。一是面向全体员工加强网络安全意识培训；二是不定期组织进行 1 次安全钓鱼演习，通过粹不及防的实战演练，监督安全培训的实际效果，并输出相应的检测报告，对相对薄弱的安全意识环节、部门进行定向培训，提升安全能力及意识；三是开展常态化网络安全意识宣传，通过制作屏保、漫画、视频短片等形式，在办公场所、食堂等地进行定期的内容灌输，强化每个员工的安全意识。四是对培训内容进行考核。

参加 HW 防守联盟。下载防守联盟交流 APP，加入相关行业防守群，同步防守信息。注册广东省网络安全应急响

应平台（https://www.gdcert.com.cn），上报安全事件，查看安全情报、安全资讯、漏洞通报，寻求安全应急响应等。

四、应急响应

企业应建立应急响应保障体系，建议如下：

一是开展信息安全攻防护演练；二是在演练中评估相应的应急预案和应急处置流程，并在演练过程中或演练结束后对应急预案和应急处置流程进行修订；三是精减应急处置流程，保证应急流程能够高效、优质的运行。四是建立 7*24 小时应急防护机制。

1、应急响应中的人员职责和工作

各单位情况不一，为便于理解，梳理人员通用职责和工作如下，各单位可根据自身实际情况调整。

企业负责人：领导建立企业的网络安全机制，协调企业各部门联动，开展应急响应工作，并同公安机关沟通、汇报网络安全事件的处置情况。

信息安全部门负责人：负责组织与指挥网络安全事件的处置工作，确定网络安全事件分级，并向企业负责汇报事件的处置情况。

信息安全工程师，应在第一时间判断事件类型，锁定

问题资产、记录 IP、恶意应用程序、查找未授权账号密码、保留相关日志，协调安全设备供应商和安全服务提供商参与相关响应。组织人员对安全设备如，WAF、堡垒机、VPN\防火墙等进行告警梳理，封堵安全事件的相关恶意 IP，并调整优化安全策略，若因为产品代码造成安全事件，则应协助开发工程师加固、修复相关漏洞。在安全事件处置完毕后出具《应急响应报告》

运维部门负责责人：负责组织与协调运维人员配合应急响应人员查找、加固、修改产品安全配置，保障非安全事件业务的正常运行。

运维工程师，应在第一时间配合查找、提取目标服务器或应用的相关日志，配合排查异常行为账号，审计堡垒机相关操作记录，并保障业务系统的正常运行。

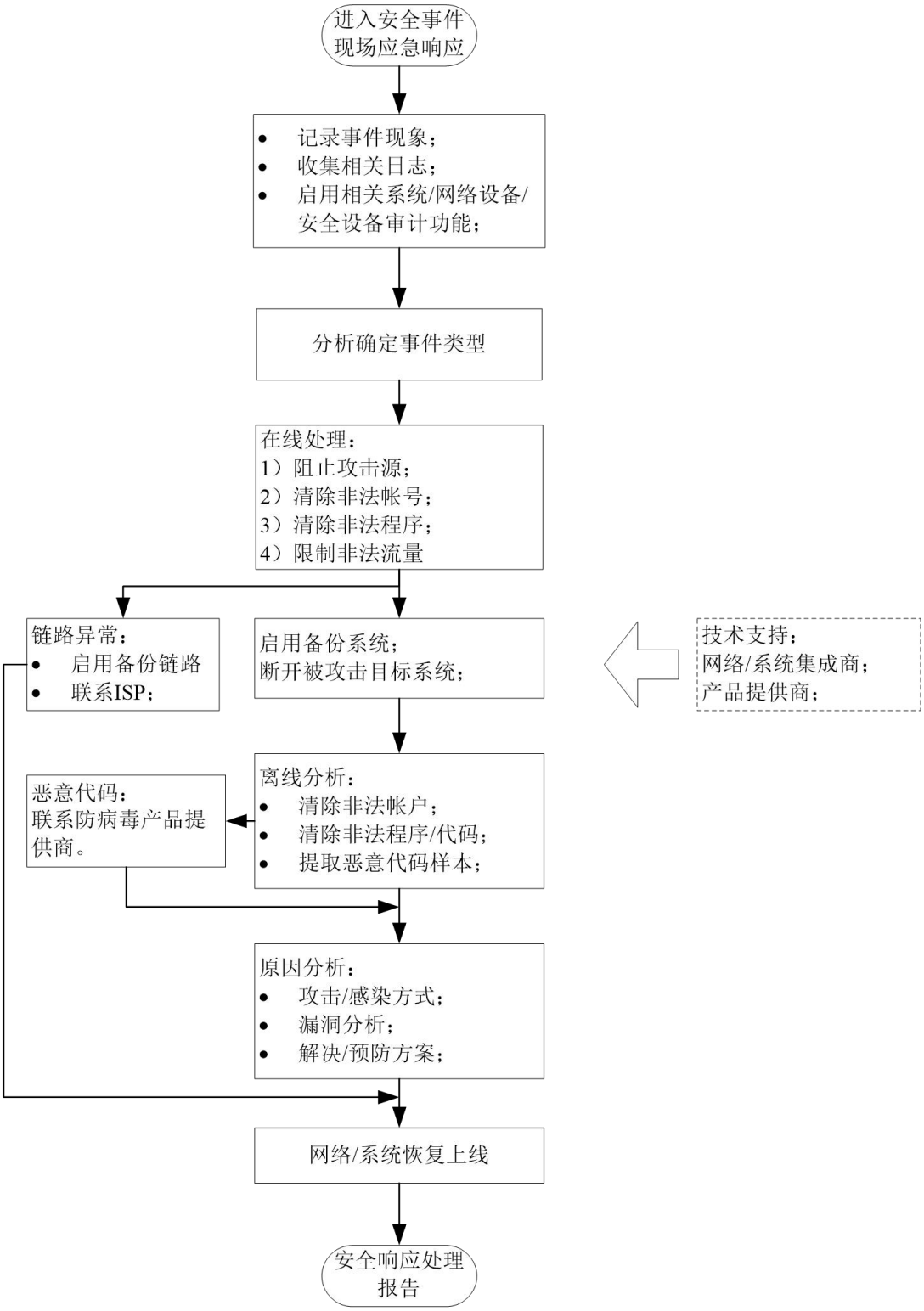
开发部门负责人：负责组织与协调开发工程师加固、修复系统代码层面发现的问题，确保事件发生后可及时修补漏洞，避免安全事件再次发生。

安全设备供应商商：应在收到企业协助信息后，第一时间派出工程师，对自身产品的配置、策略和功能进行检查与优化，协助查找解决问题，并定期对产品进行更新升级。

安全服务提供商：应在收到企业协助信息后，第一时间针对企业所发生的安全事件进行响应，提供专业的应急

响应人员协助查找，解决相关问题，并在事件结束后出具《应急响应报告》。

2、应急响应的流程



3、常见的应急事件

3.1 扫描事件

安全运营人员发现疑似攻击事件告警，如某 IP 对本单位网站提交了大量扫描探测攻击,立即上报应急委员会，并进行初步评估。

应急工程师或安全应急服务商对事件诊断并进行现场处理，快速识别扫描源。扫描源可以通过态势感知平台或者系统日志进行查看。并封堵 IP 或者 IP 段。

由运维人员对扫描 IP 进行封堵，加入黑名单。一般建议单个 IP 封堵；但是如果 IP 较多，可以封堵 IP 段，之后再进行详细梳理扫描源。

事件现场处置工作结束后，记录事件上报模板，并由单位总指挥和防御者联盟分享攻击信息，上报事件。

3.2 漏洞入侵事件

安全运营人员发现安全设备出现事件告警，如某服务器被植入挖矿病毒。立即上报应急委员会，并进行初步评估。

应急工程师或安全应急服务商对事件诊断并进行现场处理，对于漏洞入侵系统攻击，我们通常采取以下应急措施：根据可疑文件等异常信息进行排查。查看系统目前的

网络连接情况，如果发现不正常的网络连接，应当立即断开与它的连接。通过查看系统进程、服务和分析系统日志文件，来检查系统攻击者在系统中执行的操作，以便做相应的恢复；依据分析结果，进行处置。清除 webshell 等残留文件，恢复系统正常运行。

通过分析系统日志文件，或者通过弱点检测工具来了解攻击者入侵系统所利用的漏洞，并升级补丁修补漏洞。

事件现场处置工作结束后，记录事件上报模板，并由单位总指挥和防御者联盟分享攻击信息，上报事件。

3.3 口令破解事件

安全运营人员发现安全设备出现事件告警，如某 IP 对网站进行口令暴破，立即上报应急委员会，并进行初步评估。

应急工程师或安全应急服务商对事件诊断并进行现场处理，口令爆破具有以下特征：1、攻击者使用单个用户名在一定时间段内,使用不同的有规律的密码进行登录尝试；2、或者攻击者使用单个密码在一定时间段内，使用不同的有规律的用户名进行登录尝试。

为了防止口令爆破攻击，可通过系统日志尽快识别梳理爆破 IP，添加黑名单，并修改或提醒用户修改使用的密码。密码策略可强制使用位数较长、无规律、大小写数字

符号混杂的密码，并采取双因子认证。

事件现场处置工作结束后，记录事件上报模板，并由单位总指挥和防御者联盟分享攻击信息，上报事件。

3.4 后门木马事件

安全运营人员发现安全设备出现事件告警，如某内网服务器被植入 webshell 后门，立即上报应急委员会，并进行初步评估。

应急工程师或安全应急服务商对事件诊断并进行现场处理，如果攻击者正在实施网页挂马攻击，攻击未成功，则要求运维人员在网络边界防火墙、入侵防御系统上过滤攻击源地址和操作行为，即封堵攻击 IP；将被攻击的机器进行网络隔离后，处理后门木马攻击事件。排查 webshell、木马后门、其他恶意程序、图片、文字等内容，并在服务器上安装恶意程序查杀工具进行全面检查。可以根据文件修改时间进行排查清除工作。

通过日志，分析事件发生的原因，进行封堵修复。如果是通过漏洞攻击，可使用漏洞工具全面检查服务器漏洞，并更新系统补丁。对后门木马攻击事件关联机器修复后，进行测试无问题，经过指挥部办公室批准后可重新上线。

事件现场处置工作结束后，记录事件上报模板，并由单位总指挥和防御者联盟分享攻击信息，上报事件。

3.5 钓鱼邮件事件

安全运营人员发现安全设备出现事件告警，如某邮件服务器拦截到大批量钓鱼邮件，立即上报应急委员会，并进行初步评估。

应急工程师或安全应急服务商对事件诊断并进行现场处理，钓鱼邮件具有以下特征：1、邮件内容主题为爱好关注、中奖优惠、警告威慑，诱导点击文字、图片链接，内容及链接跳转目标涉及到账号密码，当用户在跳转的钓鱼网站上输入账号密码，即可被获取。2、邮件携带附件，当用户下载点击后，终端机器可能会被黑客控制。

如发生邮件钓鱼事件，建议及时更换邮箱密码，检查邮箱是否有关联其他邮箱，是否有自动转发邮件等配置，及时更换钓鱼目标系统的账号密码，提取攻击者邮箱及 IP，并通告同事朋友，举报钓鱼邮件为垃圾邮件，若打开钓鱼附件，应检查系统可疑进程并进行病毒查杀。

事件现场处置工作结束后，记录事件上报模板，并由单位总指挥和防御者联盟分享攻击信息，上报事件。

3.6 DDOS 事件

安全运营人员发现安全设备出现事件告警，如某服务器经常性发生宕机，立即上报应急委员会，并进行初步评估。

应急工程师或安全应急服务商对事件诊断并进行现场处理，将被攻击的机器进行网络隔离后，对安全设备上的日志进行分析，根据攻击时间来确定攻击 IP，并要求运维人员在网络边界防火墙、入侵防御系统上封堵攻击 IP，暂时缓解危害。

事后可通过采用分布式集群防御，如高防 CDN，IP 清洗服务等方式防御 DDOS 攻击。

事件现场处置工作结束后，记录事件上报模板，并由单位总指挥和防御者联盟分享攻击信息，上报事件。

3.7 勒索病毒事件

安全运营人员发现安全设备出现事件告警，如某服务器或终端中了勒索病毒。立即上报应急委员会，并进行初步评估。

应急工程师或安全应急服务商对事件诊断并进行现场处理，切断服务器或终端网络，防止勒索病毒进一步扩散，通过文件后缀，确定勒索病毒种类，查看是否存在解密工具。检查安全设备日志，看是否存在攻击行为，检查最早出现异常和对外开放的主机，如系统启动项，计划任务，系统日志、端口连接、进程等是否异常。

依据分析结果，确认入侵路径，及时进行封堵修复。如果是通过漏洞攻击，可使用漏洞工具全面检查服务器漏

洞，并更新系统补丁。

事件现场处置工作结束后，记录事件上报模板，并由单位总指挥和防御者联盟分享攻击信息，上报事件。

3.8 挖矿病毒事件

安全运营人员发现安全设备出现事件告警，如某服务器或终端出现 CUP 占用率接近 100%，系统卡顿，系统出现异常进程等异常行为。立即上报应急委员会，并进行初步评估。

应急工程师或安全应急服务商对事件诊断并进行现场处理，切断服务器或终端网络，防止挖矿病毒进一步扩散，检查安全设备日志，看是否存在攻击行为，检查最早出现异常和对外开放的主机，如系统启动项，计划任务，系统日志、端口连接、进程等是否异常。依据分析结果，进行处置，结束挖矿进程，删除启动项或计划任务中的挖矿脚本，修复入侵途径。

事件现场处置工作结束后，记录事件上报模板，并由单位总指挥和防御者联盟分享攻击信息，上报事件。