深云 SDP
应急响应白皮书

版本：v5.4

云深互联（北京）科技有限公司

电话：400-655-3303

法律声明

云深互联提醒您在阅读或使用《云深互联深云 SDP 应急响应白皮书》（“本文本”）之前仔细阅读、充分理解本法律声明（“本声明”）各条款的内容。如果您阅读或使用本文本，您的阅读或使用行为将被视为 对本声明全部内容的认可。

1. 您应当通过云深互联网站或云深互联提供的其他授权通道下载、获取本文本，且仅能用于自身的合法合规的业务活动。本文本的内容视为云深互联的保密信息，您应当严格遵守保密义务；未经云深互联事先书面同意，您不得向任何第三方披露本文本内容或提供给任何第三方使用。

2. 未经云深互联事先书面许可，任何单位、公司或个人不得擅自摘抄、翻译、复制本文本内容的部分或全部，不得以任何方式或途径进行传播和宣传。

3. 由于产品版本升级、调整或其他原因，本文本内容有可能变更。云深互联保留在没有任何通知或者提示下对本文本的内容进行修改的权利，并在云深互联授权通道中不时发布更新后的本文本。您应当实时关注用户文档的版本变更并通过云深互联授权渠道下载、获取最新版的本文本。

4. 本文本仅作为用户使用云深互联产品及服务的参考性指引，云深互联以产品及服务的“现状”、“有缺陷”和“当前功能”的状态提供本文本。云深互联在现有技术的基础上尽最大努力提供相应的介绍及操作指引，但云深互联在此明确声明对本文本内容的准确性、完整性、适用性、可靠性等不作任何明示或暗示的保证。任何单位、公司或个人因为下载、使用或信赖本文本 而发生任何差错或经济损失的，云深互联不承担任何法律责任。在任何情况下，云深互联均不对任何间接性、后果性、惩戒性、偶然性、特殊性或刑罚性的损害，包括用户使用或信赖本文 档而遭受的利润损失，承担责任（即使云深互联已被告知该等损失的可能性）。

5. 我们尊重知识产权，反对并打击侵犯知识产权的行为。任何组织或个人认为本文本内容可能侵犯其合法权益的，可以通过向云深互联提出书面权利通知，云深互联将在收到知识产权权利人合格通知后依法尽快处理。本文本中所有内容，包括但不限于图片、架构设计、页面布局、文字描述，均由云深互联和/ 或其关联公司依法拥有其知识产权，包括但不限于商标权、专利权、著作权、商业秘密等。非经云深互联和/或其关联公司书面同意，任何人不得擅自使用、修改、复制、公开传播、改 变、散布、发行或公开发表云深互联网站、产品程序或内容。此外，未经云深互联事先书面同意，任何人不得为了任何营销、广告、促销或其他目的使用、公布或复制云深互联的名称（包括但 不限于单独为或以组合形式包含“云深互联”、“CloudDeep”、“DeepCloud”、“深云 SDP”云深互联和/或其关联公司品牌，上述品牌的附属标志及图案或任何类似公司名称、商号、商 标、产品或服务名称、域名、图案标示、标志、标识或通过特定描述使第三方能够识别云深互联和/或其关联公司）。

6. 如若发现本文本存在任何错误，请与云深互联取得直接联系。

1 目的

为妥善应对和处置深云 SDP 系统突发事件。结合公司实际情况，特制定本应急预案。目的在于维护深云 SDP 系统正常运行，进一步完善信息系统管理机制，提高突发事件的应急处置能力。有效预防、及时控制和最大限度地消除各类突发事件的危害和影响，结合实际，特制定本应急预案。

2 适用范围

业务范围：适用于预防及处置深云 SDP 系统突发事件。

3 职责及权限

角色	职责及权限
应急处理工作小组（云深互联项目经理&项目负责人）	1. 负责领导、统一协调、组织开展深云 SDP 系统应急管理工作，紧急处理深云 SDP 系统重大应急事件和隐患。 2. 发生重大深云 SDP 系统突发事件时，负责启动本预案，下达应急任务。
实施组、开发组（云深互联工程师）	1. 承担计算机信息系统事故应急处理工作 2. 根据领导小组下达的命令和指示，负责组织指挥、协调应急行动，完成应急任务。
稽核组（云深互联测试工程师&项目负责人）	1. 负责监督处理工作及验证处理工作。

4 应急处理程序

4.1 深云 SDP 系统突发事件分类分级的说明

根据深云 SDP 系统突发事件的发生原因、性质，突发事件主要分为以下二类:

攻击类事件：指系统因非法入侵等导致业务中断、系统宕机、系统瘫痪等情况。

故障类事件：指系统因计算机软件故障、停电、人为误操作等导致业务中断、系统宕机、信息系统瘫痪等情况。

4.2 故障分级

按照突发事件的性质、严重程度、可控性和影响范围，将其分为一般故障、严重故障、重大故障三级。

（1）一般故障

系统中单个功能模块故障，但未影响业务系统运行，也未造成影响或经济损失的突发事件。

（2）严重故障

系统中单个功能模块故障导致分公司业务中断，可能造成较大业务影响或较大经济损失的突发事件。

（3）重大故障

系统中多个分公司节点或总公司骨干节点，由于故障引起的多个业务系统长时间中断，可能造成重大影响和巨大经济损失的突发事件。

4.3 系统应急预案启动

根据以上定义的故障分级，当系统事件的要素满足启动应急预案要求时，进入相应的应急启动流程。

（1）应急处理工作小组从业务人员或值班人员的故障申告得知系统异常事件后，应在第一时间赶赴系统故障现场。

（2）应急处理工作小组针对信息系统事件做出初步的分析判断。若是定性为以上攻击类/故障类事件，应急处理工作小组应及时告知实施组、开发组（1 小时内响应），进行现场或远程技术支持。明确故障可能造成的影响等级，并采取措施避免事件影响范围的扩大。

（3）应急处理工作小组在实施组、开发组的配合下，采取有力措施进行故障处理（2 小时内）。并由稽核组，验证处理结果，及时恢复系统的正常工作状态。

（4）如遇技术壁垒造成的故障，不能通过应急预案处理的问题。在一般故障情况下，实施组、开发组应在 24 小时内给与明确的处理修复时间。严重故障和重大故障，实施组、开发组应在 2 小时内给与明确的处理修复时间。

（5）应急处理工作小组通知各部门系统恢复正常，并向领导报告故障处理的基本情况。重大事件形成文字资料，以书面形式向上级报告。

（6）总结整个处理过程中出现的问题，并及时改进。

5 分类突发事件应急处理措施

5.1 黑客攻击时的紧急处置措施

（1）当有关值班人员深云 SDP 系统管理页面内容被篡改，或通过入侵监测系统发现有黑客正在进行攻击时，应立即向应急处理工作小组通报情况。

（2）实施组、开发组应在三十分钟内响应，并首先应将被攻击的服务器等设备从系统中隔离出来，保护现场，并同时向应急处理工作小组通报情况。

（3）实施组、开发组技术人员负责被攻击或破坏系统的恢复与重建工作。

（4）实施组、开发组技术人员会同相关支持人员追查非法信息来源。

（5）实施组、开发组技术人员组织相关支持人员会商后，向应急处理工作小组组长汇报有关情况。

（6）应急处理工作小组如认为情况严重，应立即向领导汇报。

5.2 Manager 管控平台遭破坏性攻击的紧急处置措施

Manager 管控平台必须存有备份，与相对应的数据必须有多日的备份，并将他们保存在安全处。

（1）一旦系统遭到破坏性攻击，应立即向实施组、开发组技术人员报告，并将该系统停止运行。

（2）实施组、开发组技术人员检查日志等资料，确定攻击来源。

（3）由实施组、开发组技术人员向应急处理工作小组汇报。

（4）应急处理工作小组认为情况严重的，应立即向领导汇报。

5.3 数据库安全紧急处置措施

（1）主要数据库应按双机热备设置，并至少要准备两个以上数据库备份。

（2）一旦数据库崩溃，应立即启动备用系统。

（3）在备用系统运行期间，实施组技术人员应对主机系统进行维修。

（4）如果两套系统均崩溃，实施组技术人员应立即向应急处理工作小组报告，应急处理工作小组如认为情况严重，应立即向领导汇报。同时通知相关部门暂缓使用系统。

（5）系统修复启动后，将第一个数据库备份取出，按照要求将其恢复到主机系统中。

（6）如因第一个备份损坏，导致数据库无法恢复，则应取出第二套数据库加已恢复。

（7）如果两个备份均无法恢复，应立即向应急处理工作小组汇报。

5.4 隐盾网关中断紧急处置措施

（1）隐盾网关主备环境，中断主环境后，实施组技术人员应立即启动备用主机接续工作。

（2）实施组技术人员应尽快判断故障节点，查明故障原因，并立即予以修复。

（3）如属运营商管辖范围，立即与运营商维护部门联系，要求恢复。

（4）如果主、备用环境同时中断，实施组技术人员应在判断故障节点，查明故障原因后，尽快研究恢复措施，并立即向应急处理工作小组汇报。

（5）经领导同意后，应通知相关部门相关原因，并暂缓使用系统。

5.5 关键人员不在岗的紧急处置措施

（1）对于实施组、开发组的关键岗位平时应做好人员储备，确保一项工作由两人能够操作。

（2）一旦发生实施组、开发组的关键人员不在岗的情况，首先应向应急处理工作小组汇报情况。

（3）经应急处理工作小组批准后，由备用人员上岗操作。

6 附则

本预案自公布之日起执行。

云深互联

云深互联，取名自唐代诗人贾岛的《寻隐者不遇》：“松下问童子，言师采药去。只在此山中，云深不知处”。寓意着公司的使命：通过新一代SDP（软件定义边界）网络隐身技术，让黑客找不到攻击目标，有效保护企业的数据资产，让每家企业的数据可以安全上云并且高效地互联互通。自2012年成立以来，已经成功服务不同行业的众多领先企业和中国500强企业，覆盖金融 、能源 、交通 、制造 、地产 、教育、政府等。成功获得晨兴资本、IDG资本、达晨创投等一系列知名投资机构数亿元融资。

深云SDP
DeepCloud

www.deepcloudsdp.com

软件定义边界（SDP）解决方案

云深互联（北京）科技有限公司

电话：400-655-3303