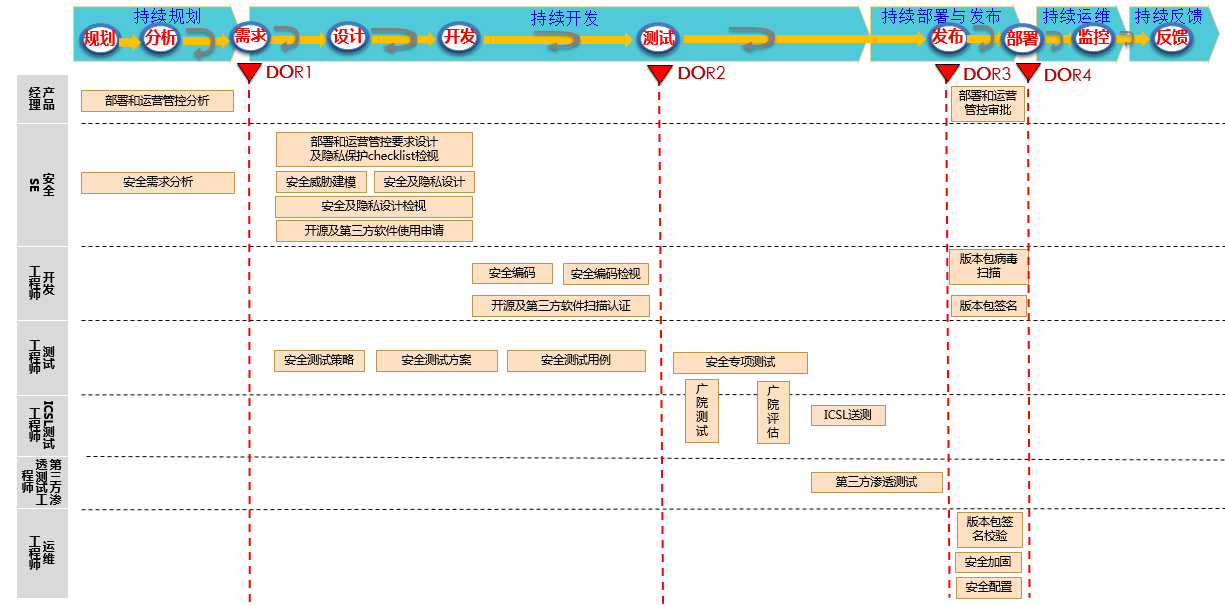
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **文件名称** | 消费者云服务DevOps安全与隐私研发过程操作指导书 | | | |
| **版 本** | V01.10 | **生效日期** | | 2017-06-24 |
| **文件编码** | PV\_Global\_CSBF\_CCS\_PDTO\_W315465 | **流程架构** | **L1** | 消费者云服务 |
| **拟 制 人** | 舒超/00302625  母大治/00162776 | **L2** | 产品开发与运维 |
| **审 核 人** | 吴永能/00339164 | **L3** |  |
| **批 准 人** | 吴永能/00339164  邹闻宇/00419519 | **L4** |  |
| **流程Owner** | 云平台开发部部长 |  |  |
| **适用范围** | 消费者云服务 | | | |

# DevOps-安全与隐私交付过程框架



# 操作指导

## 部署和运营管控分析

|  |  |
| --- | --- |
| **活动名称** | 部署和运营管控分析(双官审批要求分析) |
| **入口标准** | 全部来源的用户隐私合规需求（包括目标市场隐私保护及法律合规要求、公司部署和运营管控要求、已发布版本的部署和运营管控遗留问题） |
| **出口标准** | 交付件：   1. CBG云服务部署运营隐私合规策略 2. CBG隐私保护及网络安全-基于GAPP框架Checklist |
| **责任角色** | 产品经理 |
| **参与角色** | 业务运营经理、运维经理、SE、安全工程师 |
| **活动步骤** | 1. 产品经理针对目标市场隐私保护及法律合规要求及已发布版本的遗留问题，开展需求分析活动 2. 产品经理联合本活动的参与角色明确《云服务部署运营隐私合规策略》中自检项，对于有消费者界面的业务根据云服务部签发双官审批执行策略确定部署和运营管控评审(双官审批)的执行计划 3. 产品经理联合本活动的参与角色完成《CBG隐私保护及网络安全-基于GAPP框架Checklist》的分析活动 4. 对于确定的需要双官审批的版本产品经理联合本活动的参与角色分析《消费者云业务上线审批表 (法务)》并制定部署国家法务签署《消费者云业务上线审批表 (法务)》的执行计划 5. 产品经理制定执行第三方渗透测试计划 |
| **方法与工具、IT** | TALM、SVN |

## 安全需求分析

### 安全性威胁需求分析

|  |  |
| --- | --- |
| **活动名称** | 安全性威胁需求分析 |
| **入口标准** | 全部来源的安全需求（包括目标市场安全准入要求、关键客户安全需求、公司安全需求基线、产品线安全需求基线、上版本的安全遗留问题、威胁消减措施、隐私保护规范） |
| **出口标准** | 交付件：   1. 安全性威胁分析及需求说明书 2. 网络安全红线解读CheckList 3. 隐私保护设计规范自检checklist   标准：输出交付件已通过评审 |
| **责任角色** | 安全SE |
| **参与角色** | 产品经理、产品版本经理、安全TSE |
| **活动步骤** | 1、针对全部来源的安全需求（包括目标市场安全准入要求、关键客户安全需求、公司安全需求基线、产品线安全需求基线、上版本的安全遗留问题、威胁消减措施），开展需求分析活动，主要包括：（1）针对目标市场安全准入要求（法律、法规、认证等）进行分析，如果目标市场涉及敏感国家，针对敏感国家准入要求进行分析；（2）针对网络安全红线解读CheckList和隐私保护设计规范自检checklist进行检视，并输出检视结果；（3）针对公司网络安全基线（DFNS、安全红线），以及产品线的安全基线中推荐和强制的安全需求进行分析；（4）针对之前版本的安全遗留问题（内外部安全测试遗留问题、威胁分析遗留问题等）进行分析；（5）针对威胁消减措施进行分析。分析完成，将上述相应分析的结果纳入产品需求列表  2、针对High Level威胁分析(对于只做low-level威胁分析的版本必须有产品线和安全能力中心至少两位专家的邮件或书面确认)，输出High Level数据流图及ASTRIDE分析说明，在风险分析过程中加入攻击路径分析，进行攻击面最小化，对于DFD里需要分析的元素，所以元素都有进行ASTRIDE分析或进行合并分析说明，并纳入产品需求列表 |
| **方法与工具、IT** | TALM、SVN |

### 差异化需求分析

|  |  |
| --- | --- |
| **活动名称** | 差异化需求分析 |
| **入口标准** | 非首版本（默认是特性版本、编译版本或补丁版本） |
| **出口标准** | 交付件：差异化分析说明书  标准：输出交付件已通过评审 |
| **责任角色** | 安全SE |
| **参与角色** | 产品经理、产品版本经理、安全TSE |
| **活动步骤** | 分析当前版本跟上个版本的差异化，针对每个变更点评估是否存在安全需求，确定是否需要进行威胁建模和PIA分析，并将相应分析的结果纳入产品需求列表 |
| **方法与工具、IT** | TALM、SVN |

## 安全设计

### 部署和运营管控要求设计及隐私保护检视

|  |  |
| --- | --- |
| **活动名称** | 部署和运营管控要求设计及隐私保护checklist检视 |
| **入口标准** | 已经完成部署和运营管控分析活动并输出其交付件 |
| **出口标准** | 交付件：   1. 数据处理文档 2. 个人数据定义   3、CBG隐私保护及网络安全-基于GAPP框架Checklist |
| **责任角色** | 安全工程师，研发项目经理 |
| **参与角色** | 产品经理、业务运营经理、运维经理、SE、测试工程师(云侧)、测试工程师(端侧) |
| **活动步骤** | 1. 安全工程师基于部署和运营管控分析活动的交付件，完成《数据处理文档》和个人数据定义； 2. 安全工程师联合产品经理、业务运营经理、运维经理、SE和测试工程师针对《CBG隐私保护及网络安全-基于GAPP框架Checklist》逐项自检，对于自检通过的选项完成具体设计方案和验证方案，对于自检不通过以及不涉及项输出原因分析； 3. 研发项目经理制定本活动涉及的设计方案的执行计划； |
| **方法与工具、IT** | SVN |

### 安全威胁建模

|  |  |
| --- | --- |
| **活动名称** | ASTRIDE安全威胁建模 |
| **入口标准** | 已经完成安全性威胁分析及需求说明书 |
| **出口标准** | 交付件：安全性设计说明书内容中威胁建模章节  标准：输出交付件已通过评审 |
| **责任角色** | 安全SE |
| **参与角色** | 产品经理、产品版本经理、安全TSE |
| **活动步骤** | 1. 针对产品需求列表的所有特性进行low-level威胁建模，按照ASTRIDE七种威胁展开分析，包括：隐私、场景说明、数据流图、信任边界、外部交互方、数据流、数据存储和处理过程，保证所有元素都进行详细的分析 2. 继承上个版本的威胁分析情况，核对上个版本需求列表，遗留在后续版本落地的，在本版本进行分析 |
| **方法与工具、IT** | ASTRIDE、TALM、SVN |

### 安全及隐私设计

|  |  |
| --- | --- |
| **活动名称** | 安全及隐私设计 |
| **入口标准** | 1. 已经完成安全性威胁分析及需求说明书 2. 已经完成ASTRIDE安全威胁建模 |
| **出口标准** | 交付件：安全性设计说明书中安全设计方案  标准：输出交付件已通过评审 |
| **责任角色** | 安全SE |
| **参与角色** | 产品经理、产品版本经理、安全TSE |
| **活动步骤** | 1. 针对产品的详细认证方式、加密方式、权限控制方式、认证凭据和密钥的管理方式、相关敏感个人数据的保护方法、完整性保护方法、系统或协议的关键配置等进行分析 2. 明确加密等特性的加密算法、密钥长度等内容 3. 针对需求列表进行确认，保证对应需求存在对应的设计 4. 针对上个版本的遗留需求在本版本进行对应的分析 |
| **方法与工具、IT** | TALM、SVN |

### 安全及隐私设计检视

|  |  |
| --- | --- |
| **活动名称** | 安全及隐私设计检视 |
| **入口标准** | 已经完成安全性设计说明书 |
| **出口标准** | 交付件：安全及隐私保护设计检视Checklist（含已知设计问题及TOP观察项）  标准：输出交付件检视结果并通过评审 |
| **责任角色** | 安全SE |
| **参与角色** | 安全TSE、产品版本经理 |
| **活动步骤** | 针对安全性设计说明书进行安全及隐私保护设计检视Checklist（含已知设计问题及TOP观察项）检视，输出检视结果 |
| **方法与工具、IT** | SVN |

### 开源及第三方软件使用申请

|  |  |
| --- | --- |
| **活动名称** | 开源及第三方软件使用申请 |
| **入口标准** | 已经明确产品涉及的开源及第三方软件范围 |
| **出口标准** | 申请通过，申请电子流关闭 |
| **责任角色** | 安全SE |
| **参与角色** | 产品线第三方软件接口人、法务代表 |
| **活动步骤** | 1、所有使用到的开源及第三方软件，安全SE需在PDM电子流（<http://pdm.huawei.com/>）提交开源及第三方软件使用申请，并由法务代表＆产品线第三方软件接口人审核软件风险  2、若需使用的开源及第三方软件特定版本没有在PDM中，安全SE需在PDM电子流中提交开源及第三方软件入库申请（耗时较久，如涉及此项需尽早发起）  3、所有涉及开源及第三方软件使用变更（包括新增、废弃、使用方式变更），安全SE需在PDM电子流中重新提交开源及第三方软件使用变更申请，涉及多个子系统时，切勿分别提单，影响版本全量数据汇总  **开源及第三方软件范围识别：**  1、不管是源代码、库文件、还是最终可执行程序，只要包含在最终发布版本包中，都需要纳入开源及第三方软件管理范围  2、产品开发过程中使用的工具（包括开源工具），不会编译到版本中，也不会随版本对外发布，只需要纳入研发工具管理，收录到rTools，同时输出研发版本构建工具清单并在PDM发布(可按端侧和云侧的维度整理发布)  3、部分软件既在开发过程中作为研发工具使用，也会随最终版本包向外发布，需要同时遵循开源及第三方软件、研发工具的管控原则  4、需要向BT做ATIA交付的产品，涉及的研发工具也需要按开源及第三方软件管控  **开源及第三方软件申请填写的注意事项：**  1、开源软件通常存在包含引用其他组件的情况，如果A软件中包含了B软件，申请时只需填写A软件，但如果在维护过程中从原始开源社区等途径对B软件进行了替换活动，需要补充B软件的单独申请  2、开源软件除了自身申明的许可证外，软件里面的某部分或某个文件还有其他的许可证或许可声明，在填写第三方软件使用申请时，需要选择“是否含内嵌license”为“**是**”，选择这些不同类型的内嵌license或将内嵌license文本上传，方便IPR评审节点审批  **开源及第三方软件申请后的跟踪说明：**  1、产品提交的第三方软件申请电子流使用批准后，即LPDT完成审批，系统会给每个软件版本创建一个DTS单，里面列出此版本包括的所有第三方软件漏洞（继承申请的第三方软件除外）  2、当有新漏洞发放后，系统会给所有涉及此漏洞的所有产品每个漏洞创建一个DTS单，目前为凌晨0点自动触发，创建人和下一步处理人首先选SE，若系统未配置则改用开发代表，此操作后续还会进一步完善  3、安全漏洞处理要求及时限，参考《华为网字【2012】014号--关于产品安全漏洞响应的管理要求》<http://w3.huawei.com/info/cn/doc/viewDoc.do?did=2858831&cata=259971>  4、版本发布前，需要解决相关漏洞DTS单，注意，此类问题可能只是一般性问题，也可能涉及安全红线，需具体分析，相关处理人需提高网络安全敏感性  5、如果DTS单对应的产品版本已经废弃，需要尽快联系产品CMO把产品版本inactive，否则会产生很多废弃的无效问题单 |
| **方法与工具、IT** | PDM |

## 安全开发

### 安全编码

|  |  |
| --- | --- |
| **活动名称** | 安全编码 |
| **入口标准** | 产品版本已经完成开发 |
| **出口标准** | 输出代码静态扫描报告和告警处理清单，对于误报问题，要有误报理由和跟安全编码专家的确认记录，所有的非误报问题必须清零或者备案，且有备案记录 |
| **责任角色** | 开发工程师 |
| **参与角色** | 产品线安全编码专家、安全能力中心安全编码专家、产品三级SCM |
| **活动步骤** | 1. 进行代码静态安全扫描，输出代码静态扫描报告和告警处理清单，对所有扫描告警按照告警清理要求进行分析和处理，输出告警分析和处理记录，告警分析和处理正确、问题和误报描述详细、正确，对于问题和误报找产品三级SCM进行确认审核，经过产品三级SCM审核通过才可以入库 2. 针对代码问题修改提DTS问题单跟踪 3. 针对高风险模块开展危险API整改 4. 新增代码全部采用安全函数 5. 安全编码专家检查新代码、高风险模块老代码中的安全函数使用情况，确保安全函数在使用场景、缓冲区长度参数、返回值判断等方面不存在问题，不存在由于参数使用不当而引起的溢出或返回值判断/强转等引起的其他问题 6. 按流程要求使用安全编译选项，对于无法使用的选项找产品三级SCM进行确认审核 |
| **方法与工具、IT** | CodeDEX、DTS |

### 安全编码检视

|  |  |
| --- | --- |
| **活动名称** | 安全编码检视 |
| **入口标准** | 已经完成安全编码 |
| **出口标准** | 1、输出代码安全检视报告  （1）检视报告需包含高风险及新增/修改模块的检视结果  （2）代码检视记录表中需标出哪些是安全问题  （3）对于是问题的，需提供闭环解决方式，如DTS问题单等  2、输出安全编码TOP问题观察项排查结果，不存在安全编码TOP问题观察项遗留 |
| **责任角色** | 开发工程师 |
| **参与角色** | 产品线安全编码专家、安全能力中心安全编码专家、产品三级SCM |
| **活动步骤** | 1. 版本开发过程中对新增、修改代码进行例行的代码安全检视，并进行问题闭环，输出代码检视记录和问题处理结论 2. 识别版本的高风险模块（经过BU安全TMG审核）、并组织进行专项的代码安全检视、检视问题闭环，输出代码检视记录和问题处理结论 3. 安全编码专家审核代码安全检视报告、并进行代码抽检，抽检问题闭环 4. 排查安全编码TOP问题观察项，并进行问题闭环，输出安全编码TOP问题观察项排查结果 5. 代码只有经过产品三级SCM审核通过才可以入库 |
| **方法与工具、IT** | Smart IDE、DTS、SVN |

### 开源及第三方软件扫描认证

|  |  |
| --- | --- |
| **活动名称** | 开源及第三方软件扫描认证 |
| **入口标准** | 1. 使用已完成SDV/SIT测试的源代码进行扫描认证 2. 已完成认证前准备自检 |
| **出口标准** | 开源及第三方软件扫描认证报告 |
| **责任角色** | 开发工程师 |
| **参与角色** | CME、法务代表 |
| **活动步骤** | 1. 申请黑鸭服务器资源及CI环境配置 2. 在CI上启动黑鸦扫描 3. CI启动扫描完成后会邮件通知产品人员进行identify确认操作，identify人员按照邮件里的URL登录黑鸭服务器进行identify 4. identify确认完成后导出黑鸭报告 5. 二进制扫描，扫描完成后，产品人员需对二进制文件进行溯源确认 6. 漏洞解决 7. 产品完成二进制扫描及溯源后，需通知产品CME启动配置管理认证。产品CME根据配置管理认证检查项进行开源及第三方软件配置管理认证，通过认证后出具配置管理认证报告 8. 开源义务履行 9. 通过自助认证报告网站输出认证报告 10. 启动法务审核电子流  * 版本号使用要求：   开源及第三方软件认证申请电子流中使用的认证版本号必须和认证版本真实版本号保持一致   * 认证方式：   （1）全量认证：首次认证版本、平台架构发生变更或EMUI版本变化的首个版本以及商用发布的版本，代码必须进行全量扫描认证；  （2）增量认证：共主干，其中主线版本已经通过认证，相对于已认证主线版本的软件使用清单变化较小的版本，代码可以进行增量认证；  （3）共用认证：若自检证明使用的软件清单和使用方式与继承版本没有发生变化，并且代码完全共库管理，代码可以进行共同认证。   * 认证节奏：   （1）随EMUI发布的版本跟随EMUI版本节奏进行全量认证；  （2）独立发布的版本按M.S版本进行全量认证(M.S版本变化时做全量认证)；  （3）主线或分支发布的版本，采用共用认证/增量认证时，复用的版本的开源及第三方软件认证报告必须是三个月内的报告。 |
| **方法与工具、IT** | CI、PDM |

## 安全测试

### 内部测试

#### 安全测试策略

|  |  |
| --- | --- |
| **活动名称** | 制定安全测试策略 |
| **入口标准** | 1. 已经完成安全需求分析 2. 已经完成ASTRIDE安全威胁建模 |
| **出口标准** | 交付件：安全测试策略  标准：输出交付件已通过评审 |
| **责任角色** | 测试工程师 |
| **参与角色** | 安全TSE |
| **活动步骤** | 1、规划（SDV/SIT/SVT/迭代等）阶段开展的具体安全测试活动，明确各阶段测试范围、测试重点及出入口准则  2、对所有涉及的安全测试工具（含公司/产品线要求的工具，公司优选工具：端口扫描-Nmap、系统漏洞扫描-Nessus、DB漏洞扫描-NGS、Web漏洞扫描-AppScan、安全配置检查-secureCAT，fuzz测试-codenomicon/peach，Web安全测试Burpsuite，APK安全测试-SecDroid等）进行资源规划，并明确工具使用配置/规则或策略  3、对手工测试和自动化测试的范围进行分析，并明确两者的分工策略  4、对产品历史版本的安全问题分析，并依据分析结论给出测试策略  5、对涉及的继承特性/依赖平台的测试范围分析，并依据分析结论给出测试策略  6、对SCC安全用例基线和产品线安全基线用例的继承/落地给出测试策略  7、对所有业务重点特性给出测试策略  8、参考威胁建模的结果制定测试策略  9、对Fuzz测试给出测试策略  10、对产品涉及到的所有安全需求和要求（安全红线/安全基线/安全设计/隐私保护/安全准入/客户需求/开源及第三方等）给出对应的测试策略 |
| **方法与工具、IT** | SVN |

#### 安全测试方案

|  |  |
| --- | --- |
| **活动名称** | 制定安全测试方案 |
| **入口标准** | 1. 已经制定安全测试策略 2. 已经完成ASTRIDE安全威胁建模 3. 已经完成安全及隐私设计 |
| **出口标准** | 交付件：安全测试方案  标准：输出交付件已通过评审 |
| **责任角色** | 测试工程师 |
| **参与角色** | 安全TSE |
| **活动步骤** | 1、对所有安全测试重点进行详细分析，明确测试内容和测试方法（测试内容包含测试对象描述、测试点；测试方法包含对测试工具的配置说明和执行要求等内容）  2、对Fuzz测试对象（协议/API/文件解析/驱动等）进行全面分析，明确测试内容和Fuzz方法  3、对安全自动化测试进行分析，明确安全自动化实现方法  4、对测试组网和测试环境进行分析，明确组网安全和环境安全方面的测试内容和方法  5、对所有涉及的继承特性安全问题进行分析，明确测试内容和测试方法  6、使用基于威胁建模的测试设计方法（TMBT）来进行测试设计，全面分析测试内容，明确测试方法  7、使用TMBT工具和安全用例基线库开展安全测试设计  8、对产品涉及到的所有安全需求和要求（安全红线/安全基线/安全设计/隐私保护/安全准入/客户需求/开源及第三方等）的测试内容进行全面分析，明确测试测试内容和方法 |
| **方法与工具、IT** | TMBT、SVN |

#### 安全测试用例

|  |  |
| --- | --- |
| **活动名称** | 编写安全测试用例 |
| **入口标准** | 已经制定安全测试方案 |
| **出口标准** | 交付件：安全测试用例  标准：输出交付件已通过评审 |
| **责任角色** | 测试工程师 |
| **参与角色** | 安全TSE |
| **活动步骤** | 根据安全测试方案中的测试内容进行对应安全测试用例编写，用例内容描述完整、具体、清晰、可执行  用例覆盖要包含：1、安全设计阶段威胁建模识别出的所有威胁和落地的所有消减措施；2、适配SCC安全用例基线和产品线安全用例基线中适合产品的用例并100%落地；3、产品内部安全测试和ICSL/CSEC测试中发现的安全问题；4、最近历史版本/网上暴露的与产品相关的安全问题；5、产品涉及到的所有安全需求和要求（安全红线/安全基线/安全设计/隐私保护/安全准入/客户需求/开源及第三方等） |
| **方法与工具、IT** | TMSS、安全知识库（https://rnd-skb.huawei.com/user/testcaselib/homePage） |

#### 安全专项测试

|  |  |
| --- | --- |
| **活动名称** | 安全专项测试 |
| **入口标准** | 1. 产品版本属于送测ICSL版本范围 2. 版本转测试达到“版本转测试和发布的安全与隐私入口条件要求Checklist”中版本转测试要求 3. 至少完成一轮产品功能测试，无严重问题导致功能阻塞 4. 测试版本在安全环境已经部署完成，且完成端到端验证，环境可用无阻塞 |
| **出口标准** | 1、已经完成测试并输出安全测试报告，无红线和隐私问题遗留、无CVSS打分超过7分的严重问题遗留、无TOPN观察项问题遗留  2、版本发布达到“版本转测试和发布的安全与隐私入口条件要求Checklist”中版本发布要求  3、待澄清问题、送测范围、送测环境已经跟内网实验室沟通达成一致，并有沟通纪要证明  4、已经完成ICSL送测准备Checklist自检 |
| **责任角色** | 测试工程师 |
| **参与角色** | 安全设计代表、安全编码代表、产品测试经理、产品版本经理、ICSL测试经理 |
| **活动步骤** | 1、产品版本经理按入口条件要求提交转测试电子流  2、测试工程师进行转安全测试前的准备，包括：（1）产品讲解业务（含代码结构）；（2）基于威胁分析使用TMBT完成安全测试设计（需内部评审）；（3）制定版本安全测试策略（需内部评审）；（4）抽取安全测试用例（需内部评审）  3、测试工程师根据入口条件要求进行版本转安全测试入口条件评估，如果评估通过，进行内部转安全测试预测试；如果评估不通过，则版本打回。如果预测试通过就进行正式接收转测试申请，启动正式安全测试执行；如果预测试不通过，则版本打回  4、首轮安全测试，测试工程师执行分配的安全测试用例，同时将云安全历史问题库中的所有问题在SDV1版本中排查，SDV1最后1-2天例行开展全员内部找虫发散测试  5、产品版本经理组织修改安全测试期间发现的问题，产品测试经理组织对修复安全问题后的版本并行进行非安全测试：功能、性能、EMUI预置专项测试，在转安全测试回归版本前完成  6、安全测试SDVn最后一轮进行跟上一轮的代码比对检查，SDVn最后一轮内部交叉测试，不同责任田的产品安全测试工程师进行相互交叉测试  7、测试工程师组织内部结对开展送测checklist检查，检查通过，组织产品相关人召开送测评审会（包含安全设计代表、安全编码代表、产品测试经理、产品版本经理）  8、送测评审通过（待澄清问题、测试范围和测试环境，都已经跟ICSL测试经理达成一致），测试工程师输出会议纪要，并启动填写ICSL送测电子流进行送测 |
| **方法与工具、IT** | TMSS、DTS、云业务安全测试工具集、T2T、ICSL送测电子流（http://w3.huawei.com/bs/icsl/#!icsl/apply/index.html） |

### ICSL测试

#### ICSL送测

|  |  |
| --- | --- |
| **活动名称** | ICSL送测 |
| **入口标准** | 1. 主版本或次版本（默认采取ICSL测试模式，如果ICSL评估走广院，那么就采取广院测试模式）   2、已经按照送测计划提交ICSL送测电子流申请 |
| **出口标准** | 1. 已经完成测试，双方针对ICSL测试发现所有疑似问题无分歧   2、输出ICSL测试报告，无红线和隐私问题遗留、无CVSS打分超过7分的严重问题遗留 |
| **责任角色** | ICSL测试工程师 |
| **参与角色** | 安全设计代表、安全编码代表、产品版本经理、测试工程师 |
| **活动步骤** | 1. 测试工程师根据送测前评审会结论，在规定送测计划时间提交ICSL送测电子流 2. ICSL测试工程师接受电子流并根据送测计划组织测试 3. 测试过程中ICSL测试工程师将发现的所有疑似问题发给产品进行确认，测试工程师组织产品相关人员（包括：安全设计代表、安全编码代表、产品版本经理）对问题进行一一确认，在ICSL测试完成后统一回复ICSL测试工程师，并组织评审会进行双方分歧问题澄清 4. ICSL测试工程师会针对双方澄清达成一致的结果上ICSL内部评审会进行评审，评审完毕输出ICSL测试报告（如果针对问题澄清存在部分问题无法达成一致，产品版本经理可以准备材料上ICSL内部评审会申诉，由ICSL内部评审给出最终结论，如果对结论还有异议，可以上升到GSPO申诉） |
| **方法与工具、IT** | ICSL送测电子流（http://w3.huawei.com/bs/icsl/#!icsl/apply/index.html） |

#### 广院测试

|  |  |
| --- | --- |
| **活动名称** | 广院测试 |
| **入口标准** | 1、特性版本或编译版本（默认采取广院测试模式）  2、版本转测试达到“版本转测试和发布的安全与隐私入口条件要求Checklist”中版本转测试要求 |
| **出口标准** | 1、版本发布达到“版本转测试和发布的安全与隐私入口条件要求Checklist”中版本发布要求  2、无红线和隐私问题遗留、无CVSS打分超过7分的严重问题遗留、无TOPN观察项问题遗留，按ICSL要求提供的广院测试报告被ICSL评审通过，ICSL送测电子流关闭 |
| **责任角色** | 测试工程师 |
| **参与角色** | ICSL测试工程师、产品版本经理 |
| **活动步骤** | 1、产品版本经理按入口条件要求提交转测试电子流  2、测试工程师根据入口条件要求进行版本转安全测试入口条件评估，如果评估通过，进行内部转安全测试预测试；如果评估不通过，则版本打回。如果预测试通过就进行正式接收转测试申请，启动正式安全测试执行；如果预测试不通过，则版本打回  3、根据ICSL提供的测试用例集执行用例并输出ICSL要求的测试报告提交ICSL送测电子流评审  4、ICSL测试工程师组织ICSL内部评审（如果评审通过就关闭电子流；如果评审不通过则需要双方针对分歧点进行澄清说明直到评审通过），ICSL可以对提交的电子流版本发起广院抽测，但不影响版本的正常迭代发布计划 |
| **方法与工具、IT** | ICSL送测电子流（http://w3.huawei.com/bs/icsl/#!icsl/apply/index.html） |

#### 广院评估

|  |  |
| --- | --- |
| **活动名称** | 广院评估 |
| **入口标准** | 1、补丁版本（默认采取广院评估模式）  2、版本转测试达到“版本转测试和发布的安全与隐私入口条件要求Checklist”中版本转测试要求 |
| **出口标准** | 1、版本发布达到“版本转测试和发布的安全与隐私入口条件要求Checklist”中版本发布要求  2、无红线和隐私问题遗留、无CVSS打分超过7分的严重问题遗留、无TOPN观察项问题遗留，按ICSL要求提供的广院评估报告被ICSL评审通过，ICSL送测电子流关闭 |
| **责任角色** | 测试工程师 |
| **参与角色** | ICSL测试工程师、产品版本经理 |
| **活动步骤** | 1、产品版本经理按入口条件要求提交转测试电子流  2、测试工程师根据入口条件要求进行版本转安全测试入口条件评估，如果评估通过，正式接收转测试申请，根据差异化分析说明评估制定安全测试策略，明确不需要进行额外的安全测试，直接根据ICSL要求的测试报告提交ICSL送测电子流评审，ICSL测试工程师组织ICSL内部评审（如果评审通过就关闭电子流；如果评审不通过则需要双方针对分歧点进行澄清说明直到评审通过），ICSL可以对提交的电子流版本发起广院抽测，但不影响版本的正常迭代发布计划；如果评估不通过，则版本打回 |
| **方法与工具、IT** | ICSL送测电子流（http://w3.huawei.com/bs/icsl/#!icsl/apply/index.html） |

### 第三方渗透测试

|  |  |
| --- | --- |
| **活动名称** | 第三方渗透测试 |
| **入口标准** | 1. 需要走双官审批的版本（包括需要部署的主版本或不符合免双官审批条件的次版本） 2. 免双官审批的次版本（符合CBG隐私评估委员会已确定的免双官审批条件） 3. 免双官审批的特性版本、编译版本（符合第三方渗透测试必要性三方评审条件，且经过第三方渗透测试项目负责人、SCC安全代表和产品经理三方评审，需要开展第三方渗透测试） 4. 产品内部已经输出安全测试通过报告   第三方渗透测试必要性三方评审请参考以下指标，大于等于70分即需要评审：  （1）变更接口总数超过20个（10分）  （2）变更人机接口超过10个（20分）  （3）新引入第三方组件（10分）  （4）变更内容涉及支付或者隐私数据（50分） |
| **出口标准** | 1. 已经完成测试，并输出第三方渗透测试报告 2. 三方验收组（云服务安全代表、ICSL安全代表、SCC安全代表）已经完成验收，评审通过 |
| **责任角色** | 第三方渗透测试工程师 |
| **参与角色** | 产品经理、运维工程师、云服务安全代表、ICSL安全代表、SCC安全代表、第三方渗透测试项目负责人 |
| **活动步骤** | 1. 产品经理提出第三方渗透测试申请，第三方渗透测试项目负责人根据申请启动第三方渗透测试项目招标，确定第三方渗透测试供应商 2. 第三方渗透测试项目负责人根据产品提供的需求文档和第三方渗透测试供应商进行需求澄清，同时运维工程师根据安全专项测试输出的安全测试通过报告获取归档版本进行第三方渗透测试环境部署和调测 3. 第三方渗透测试供应商按计划派遣渗透测试工程师进行第三方渗透测试，测试完成输出第三方渗透测试报告 4. 三方验收组（云服务安全代表、ICSL安全代表、SCC安全代表）针对第三方渗透测试报告中发现的安全问题进行验收评审，给出验收评审结论（如果验收通过，则结束第三方渗透测试；如果验收不通过，有必须修改的安全问题，但评估修改无安全风险，则直接结束第三方渗透测试，无需进行第三方渗透测试回归；如果验收不通过，有必须修改的安全问题，且评估修改有一定安全风险，则需要进行第三方渗透测试回归，回归结束第三方渗透测试工程师刷新第三方渗透测试报告，三方验收组再次进行验收评审，直到评审通过） |
| **方法与工具、IT** | 侦察&扫描、漏洞利用 |

## 安全发布

### 版本包病毒扫描

|  |  |
| --- | --- |
| **活动名称** | 版本包病毒扫描 |
| **入口标准** | 待发布版本 |
| **出口标准** | 病毒扫描报告无病毒，病毒扫描报告归档VMP |
| **责任角色** | 开发工程师 |
| **参与角色** | 测试工程师 |
| **活动步骤** | 1. 版本包归档VMP 2. 提交版本转测试电子流，电子流会自动触发病毒扫描并将结果归档VMP或手动到VMP进行病毒扫描 3. 测试工程师检查病毒扫描报告是否有病毒，如果有病毒，需软件确认和进行整改；无病毒则通过（新发布流程上线后，发布系统自动做病毒防呆校验，通过方可发布；有病毒则需软件确认和进行整改） |
| **方法与工具、IT** | T2T、病毒中心、VMP、TPDM |

### 版本包签名

|  |  |
| --- | --- |
| **活动名称** | 版本包签名 |
| **入口标准** | 版本已经通过开源及第三方软件认证，满足发布标准 |
| **出口标准** | 版本包签名成功，公钥归档VMP |
| **责任角色** | 开发工程师 |
| **参与角色** | 无 |
| **活动步骤** | 提交版本发布电子流，版本发布流程会自动触发数字签名并归档公钥到VMP或手动在VMP触发数字签名，签名成功后公钥归档VMP |
| **方法与工具、IT** | TPDM、VMP |

## 安全部署

### 部署和运营管控审批

|  |  |
| --- | --- |
| **活动名称** | 部署和运营管控审批(双官审批) |
| **入口标准** | 1、版本发布区域国家的法务签署《消费者云业务上线审批表 (法务)》  2、通过安全测试(ICSL送测/广院测试/广院评估)  3、通过第三方渗透测试  **说明：在部署和运营管控分析活动中确定无需进行双官审批的业务版本，无需执行部署和运营管控审批(双官审批)活动** |
| **出口标准** | 获得 GSPO及CLO批准(双官审批) |
| **责任角色** | 产品经理 |
| **参与角色** | 业务运营经理、运维经理、安全工程师 |
| **活动步骤** | 1. 产品经理在CBG隐私评估委员会评估汇报通过； 2. 产品经理邮件或书面获得CPO批准或产品经理在CBG隐私评估委员会获得免双官审批评估结论； 3. 产品经理邮件获得GSPO及CLO批准或产品经理在CBG隐私评估委员会获得免双官审批评估结论； |
| **方法与工具、IT** | SVN |

### 版本包签名校验

|  |  |
| --- | --- |
| **活动名称** | 版本包签名校验 |
| **入口标准** | 软件仓版本包 |
| **出口标准** | 版本包签名校验通过 |
| **责任角色** | 运维工程师 |
| **参与角色** | 开发工程师 |
| **活动步骤** | 运维工程师部署安装包前先进行数字签名，签名通过后方可执实施自动化部署 |
| **方法与工具、IT** | CloudSop、蓝区VMP、数字签名中心 |

### 安全加固

|  |  |
| --- | --- |
| **活动名称** | 安全加固 |
| **入口标准** | 产品部署所需的基础环境（操作系统、数据库）已经安装完成 |
| **出口标准** | 按产品线安全加固规范完成基础环境的安全加固 |
| **责任角色** | 运维工程师 |
| **参与角色** | 无 |
| **活动步骤** | 1. 针对产品部署所需的基础环境的操作系统和数据库分别进行安全加固，执行安全加固脚本 2. 待加固完成后进行基础环境验证 |
| **方法与工具、IT** | 安全加固脚本 |

### 安全配置

|  |  |
| --- | --- |
| **活动名称** | 安全配置 |
| **入口标准** | 产品版本包已经部署在基础环境 |
| **出口标准** | 1. 按产品线安全配置规范完成产品版本的安全配置 2. 测试业务验证通过 |
| **责任角色** | 运维工程师 |
| **参与角色** | 测试工程师 |
| **活动步骤** | 1. 按照对应产品的业务安全配置规范进行安全配置，执行安全配置脚本 2. 待配置完成后测试工程师进行业务功能验证 |
| **方法与工具、IT** | 安全配置脚本 |

# 裁剪指南

|  |  |  |
| --- | --- | --- |
| **版本标识类型** | **裁剪活动** | **简要说明** |
| 1、主版本——版本号M（Major Version）：标识平台或整体架构。  2、次版本——版本号S（Senior Version）：标识局部架构、重大特性、或无法向前兼容的接口。 | 1、可裁剪掉“安全测试章节里面的广院测试和广院评估”  2、可裁剪掉“安全需求分析章节里面的差异化需求分析” |  |
| 1、特性版本——版本号F（Feature Version）：标识规划的新特性版本。  2、编译版本——版本号B（Build Version）：标识编译构建的版本号。 | 1. 可裁剪掉“安全测试章节里面的安全专项测试” 2. 可裁剪掉“安全测试章节里面的ICSL送测和广院评估” 3. 可裁剪掉“安全测试章节里面的第三方渗透测试” 4. 可裁剪掉“部署和运营管控分析章节”、“安全设计章节里面的部署和运营管控要求设计及隐私保护检视”、“安全部署章节里面的部署和运营管控审批” | 如果是3个月内的版本，可裁剪掉“安全设计章节里面的开源及第三方软件使用申请”、“安全开发章节里面的开源及第三方软件扫描认证” |
| 补丁版本——版本号SP（Service Pack Version）：禁止实现新特性。仅用于服务器软件及工具。 | 只保留“安全测试章节里面的广院评估”、“安全发布章节”、“安全部署章节里面的版本包签名校验”，其他全部可裁剪掉 |  |

**4文件拟制/修订记录**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **版本** | **拟制/修订责任人** | **拟制/修订日期** | **修订内容及理由** | **批准人** |
| V01.00 | 舒超/00302625  母大治/00162776 | 2016-8-24 | 根据评审组各位评审专家意见进行优化 | 蓝文广/00338846  苏杰/00336895 |
| V01.00 | 舒超/00302625  母大治/00162776 | 2017-6-9 | 优化刷新 | 吴永能/00339164  邹闻宇/00419519 |