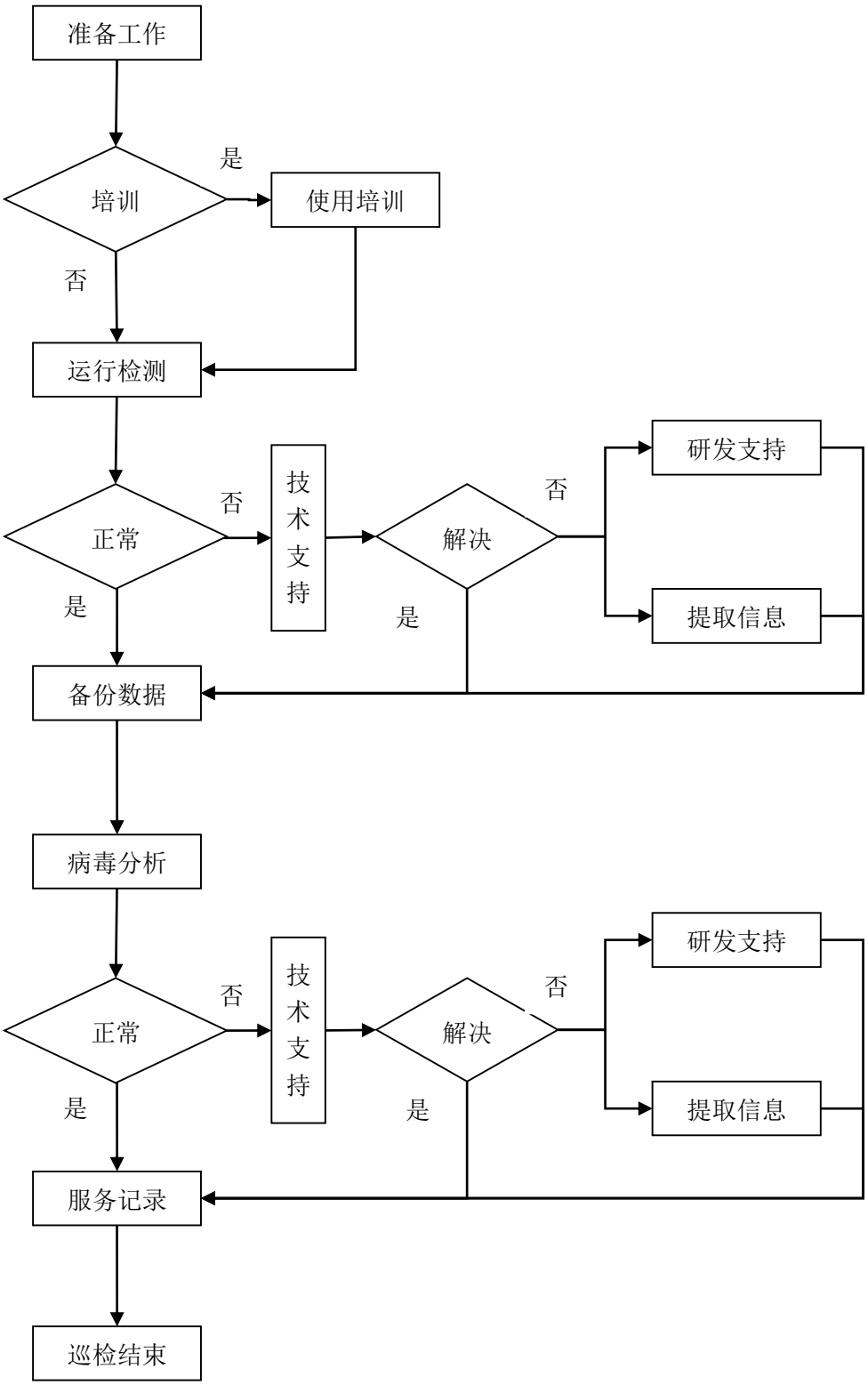
企业产品巡检服务

1. 现场巡检服务

1) 服务概述

由指定的高级安全顾问与客户建立紧密的长期合作关系，定期为客户提供上门巡检服务，服务内容包括：产品使用培训、产品运行检测、病毒日志分析、现场技术支持等服务。综合现场巡检的信息，提供内容可定制的巡检报告。

2) 服务流程


准备工作
培训
是
使用培训
否
运行检测
正常
否
技术支持
解决
否
研发支持
是
提取信息
是
备份数据
病毒分析
正常
否
技术支持
解决
否
研发支持
是
提取信息
是
服务记录
巡检结束

3) 服务内容

由指定的高级安全顾问与客户建立紧密的长期合作关系，定期为客户提供上门巡检服务。通过深入了解客户的实际复杂环境、依靠深厚的技术专业知识，为客户提供优质的现场巡检服务，并为客户提供详细的病毒分析和病毒防范建议。确保客户从软件投资中获得最大收益。

具体服务内容如下：

- **产品使用培训**
  - 依据客户的需求，提供定制化的产品使用培训。如：漏洞扫描工具使用等。优化客户使用产品的效率。
  - 针对产品熟练度低的用户，提供针对性的产品使用培训。使客户掌握日常管理中所需的技能。
  - 及时为客户提供新产品或新功能的使用培训，使客户迅速适应新产品或新功能并掌握使用。
- **产品运行检测**
  - 检查瑞星系统中心相关服务是否正常运行。
  - 登录控制台，查看重要事件中是否有报错。
  - 检查中心升级是否正常，手动通知升级或是运行升级包一次，确保中心升级正常。
  - 在控制台进行一些常规操作，如：系统中心设置等。检测相关功能是否可以正常使用。
  - 检查确认上下级通讯代理运行正常。
  - 通过客户端列表，检查客户端升级是否正常。客户端是否在中心正常显示。
  - 通过客户端列表,先后挑选一台和多台客户端，进行如下操作：开启或关闭指定监控、设置防毒策略、设置主动防御规则等，检查是否可以进行正常设置，并关注事件日志和运行日志消息。
  - 在客户端生成日志，确保中心可以正常接受日志上报。
  - 打开日志管理工具，查看事件日志，查看是否有客户端非法卸载记录。
  - 备份系统中心数据、数据库日志文件、分组策略等信息。
- **病毒日志分析**
  - 通过日志管理工具，查看本阶段病毒总体概况。同上一阶段粗略比较，掌握病毒总体发展趋势。
  - 通过 TOP 工具，查看病毒或染毒客户端排行，对重点对象进行详细分析。可在日志明细

中，通过病毒名称，准确定位染毒客户端。或是通过客户端计算机名称或是 IP 地址，查看详细的染毒情况。

- 通过日志管理工具趋势分析，分析指定客户端或病毒在该阶段的走势。
- 针对染毒严重的客户端或是多台客户端感染的病毒，通过病毒明细查看染毒文件、访问染毒文件路径、感染时间，进一步了解病毒的行为。
- 通过日志管理工具下级中心病毒明细查询工具，查询下级中心的染毒情况，并对重点染毒计算机和病毒予以关注。
- 通过日志管理工具趋势比较，在多个中心中，或是单独中心分组间进行比较，分析病毒感染趋势和染毒客户端数量趋势。

- **现场技术支持**

- 针对中心运行异常的情况，可根据具体的错误提示或现象进行处理。
- 针对在控制台查看异常的客户端，可以到本地查看运行情况，并进行处理。
- 针对客户端与中心之间存在通讯异常的情况，可协助客户检查是否存在端口占用，端口未开放等情况。
- 针对产品冲突等问题，可快速定位原因并提取相关信息，如遇特殊情况，可以快速协调研发人员上门服务。
- 通过病毒日志分析，针对重点病毒，可以提供处理方法和防范建议，避免病毒的进一步扩散。
- 针对当前最新版无法查杀的病毒，可以提取瑞星听诊器等日志和可疑文件，争取尽快入库解决此病毒的查杀。
- 针对杀毒软件误报等问题，可以指导客户设置排除查杀目录、从隔离区恢复可疑文件等方式，将误报的影响降到最低。并将误报文件及时反馈，解决误报问题。
- 针对病毒劫持杀毒软件、未知病毒现象等问题，可以使用工具手动快速解决问题或是提取重要信息，尽快反馈解决。如遇特殊情况，可以快速协调研发人员上门服务。
- 针对通过局域网传播的病毒，可以协助客户确定病毒源进行查杀，并加强防范措施。

- **巡检报告**

根据备份的病毒数据库文件和现场了解的情况，为客户提供内容可定制的巡检报告。默认情况下，巡检报告包含以下内容：

- 本阶段病毒风险分析，根据病毒数量、染毒计算机数量和病毒破坏性，确定本阶段的安全等级。

- 本阶段与上一阶段的病毒数量、染毒计算机数量等趋势比较。
- 本阶段重点染毒客户端病毒情况分析，详细分析病毒来源、感染途径和造成的危害，并提供防范建议。
- 本阶段重点病毒分析。详细分析病毒来源、感染途径和造成的危害，并提供防范建议。根据实际情况可以提供专杀工具。
- 本阶段网内计算机漏洞情况，按照漏洞等级分布，并告知漏洞可能造成的影响。
- 中心间染毒趋势比较、中心各组之间染毒趋势比较、指定病毒分析等内容可以定制。

4) 服务总结和建议

随着病毒的不断发展，病毒展现了更强的变异性和破坏性，不易处理。如果能够做好防御措施，降低感染病毒的风险，可以为企业 IT 管理人员节省大量的工作。瑞星现场巡检服务正是基于这样的考虑，通过安排指定人员上门巡检，了解客户的实际网络复杂环境，为客户提供良好的防范建议和主动防御计划。通过指定人员的长期跟踪服务，更充分的了解客户情况。针对最新病毒，可以提供及时有针对性的防范建议。通过产品使用培训，可以使客户全面了解软件的功能，以便于软件被正确的使用，提高病毒防范效果。在进行现场技术支持过程中，客户可以较直观的观看产品运行检测和病毒处理过程，快速提高自身能力。通过定时长期有效的沟通，瑞星公司不断的为客户提供更好的客户管理和产品增值服务。从态度和责任上，与客户的安全防病毒工作走在一起。

5) 服务意义

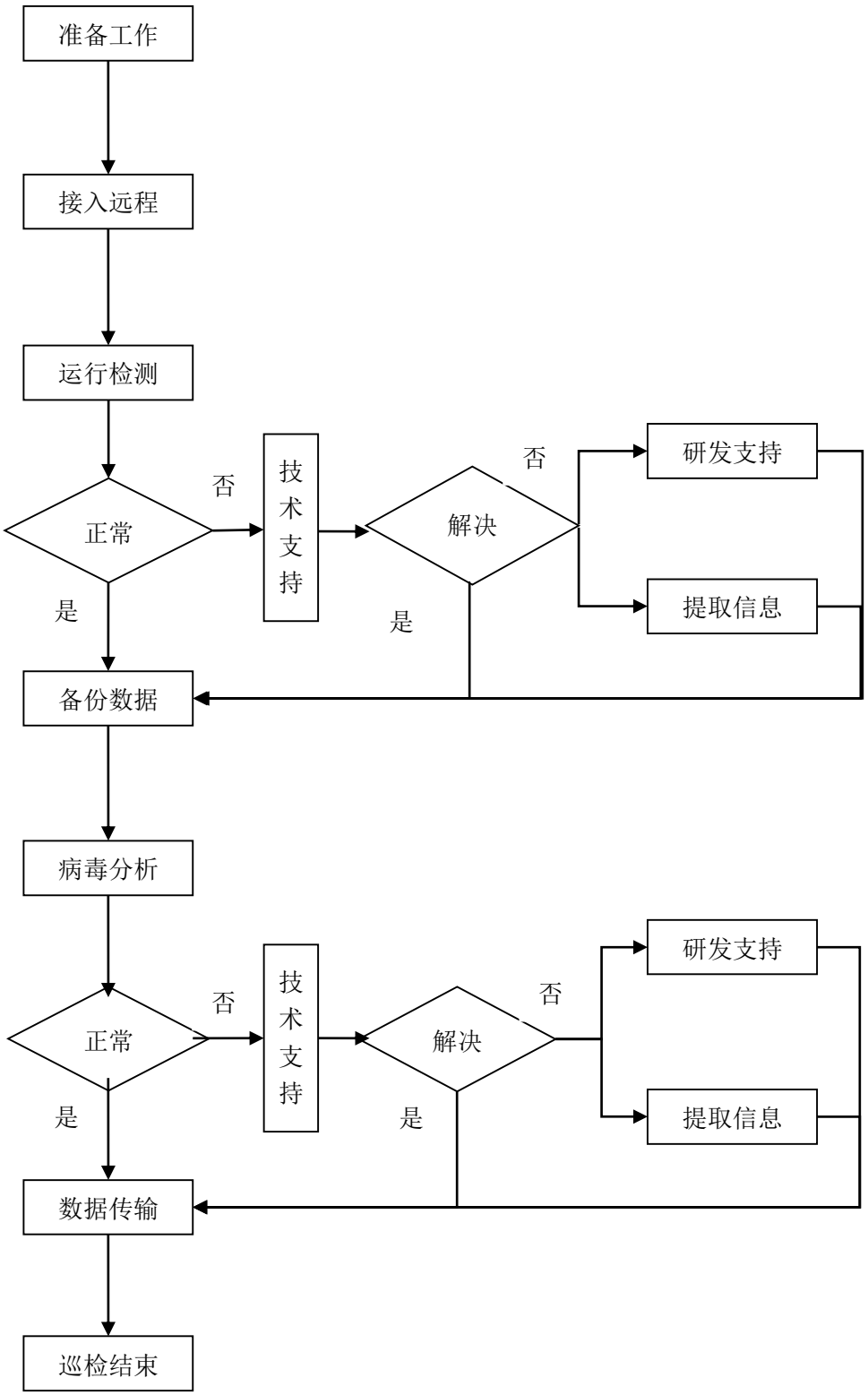
- 指定的高级安全顾问跟踪服务，对企业安全状况了解更充分，可提供优质的现场技术支持服务和针对性的防病毒建议。
- 通过长期的趋势比较分析，直观呈现病毒感染数量变化趋势和染毒计算机数量变化趋势，使客户对自己的安全状况一目了然。
- 根据客户的需求和产品的更新换代，为客户提供产品使用培训，使产品在防病毒工作中发挥更好的作用。
- 每个阶段的安全状况通过巡检报告的形式呈现，使客户直观具体的了解本阶段病毒概况并及时检测病毒防范工作的成效。

2. 远程巡检服务

1) 服务概述

由指定的高级安全顾问与客户建立紧密的长期合作关系，定期为客户提供远程巡检服务，服务内容包括：产品运行检测、病毒日志分析、远程技术支持等服务。综合远程巡检的信息，提供内容可定制的巡检报告。

2) 服务流程


准备工作
接入远程
运行检测
正常
否
技术支持
解决
否
研发支持
提取信息
是
是
备份数据
病毒分析
正常
否
技术支持
解决
否
研发支持
提取信息
是
是
数据传输
巡检结束

3) 服务内容

由指定的高级安全顾问与客户建立紧密的长期合作关系，定期为客户提供远程巡检服务。通过深入了解客户的实际复杂环境、依靠深厚的技术专业知识，为客户提供优质的远程巡检服务，并为客户提供详细的病毒分析和病毒防范建议。确保客户从软件投资中获得最大收益。

具体服务内容如下：

- 产品运行检测
  - 检查瑞星系统中心相关服务是否正常运行。
  - 登录控制台，查看重要事件中是否有报错。
  - 检查中心升级是否正常，手动通知升级或是运行升级包一次，确保中心升级正常。
  - 在控制台进行一些常规操作，如：系统中心设置等。检测相关功能是否可以正常使用。
  - 检查确认上下级通讯代理运行正常。
  - 通过客户端列表，检查客户端升级是否正常。客户端是否在中心正常显示。
  - 通过客户端列表,先后挑选一台和多台客户端，进行如下操作：开启或关闭指定监控、设置防毒策略、设置主动防御规则等，检查是否可以进行正常设置，并关注事件日志和运行日志消息。
  - 打开日志管理工具，查看事件日志，查看是否有客户端非法卸载记录。
  - 备份系统中心数据、数据库日志文件、分组策略等信息。
- 病毒日志分析
  - 通过日志管理工具，查看本阶段病毒总体概况。同上一阶段粗略比较，掌握病毒总体发展趋势。
  - 通过 TOP 工具，查看病毒或染毒客户端排行，对重点对象进行详细分析。可在日志明细中，通过病毒名称，准确定位染毒客户端。或是通过客户端计算机名称或是 IP 地址，查看详细的染毒情况。
  - 通过日志管理工具趋势分析，分析指定客户端或病毒在该阶段的走势。
  - 针对染毒严重的客户端或是多台客户端感染的病毒，通过病毒明细查看染毒文件、访问染毒文件路径、感染时间，进一步了解病毒的行为。
  - 通过日志管理工具下级中心病毒明细查询工具，查询下级中心的染毒情况，并

对重点染毒计算机和病毒予以关注。

- 通过日志管理工具趋势比较，在多个中心中，或是单独中心分组间进行比较，分析病毒感染趋势和染毒客户端数量趋势。

- 现场技术支持
  - 针对中心运行异常的情况，可根据具体的错误提示或现象进行处理。
  - 针对在控制台查看异常的客户端，提供处理建议。
  - 针对客户端与中心之间存在通讯异常的情况，可协助客户检查是否存在端口占用，端口未开放等情况。
  - 针对产品冲突等问题，可快速定位原因并提取相关信息。
  - 通过病毒日志分析，针对重点病毒，可以提供处理方法和防范建议，避免病毒的进一步扩散。
  - 针对当前最新版无法查杀的病毒，可以提取瑞星听诊器等日志和可疑文件，争取尽快入库解决此病毒的查杀。
  - 针对杀毒软件误报等问题，可以指导客户设置排除查杀目录、从隔离区恢复可疑文件等方式，将误报的影响降到最低。并将误报文件及时反馈，解决误报问题。
  - 针对病毒劫持杀毒软件、未知病毒现象等问题，可以使用工具手动快速解决问题或是提取重要信息，尽快反馈解决。
  - 针对通过局域网传播的病毒，可以协助客户确定病毒源进行查杀，并加强防范措施。

- 巡检报告

  根据备份的病毒数据库文件和现场了解的情况，为客户提供内容可定制的巡检报告。默认情况下，巡检报告包含以下内容：
  - 本阶段病毒风险分析，根据病毒数量、染毒计算机数量和病毒破坏性，确定本阶段的安全等级。
  - 本阶段与上一阶段的病毒数量、染毒计算机数量等趋势比较。
  - 本阶段重点染毒客户端病毒情况分析，详细分析病毒来源、感染途径和造成的危害，并提供防范建议。
  - 本阶段重点病毒分析。详细分析病毒来源、感染途径和造成的危害，并提供防范建议。根据实际情况可以提供专杀工具。

- 本阶段网内计算机漏洞情况，按照漏洞等级分布，并告知漏洞可能造成的影响。
- 中心间染毒趋势比较、中心各组之间染毒趋势比较、指定病毒分析等内容可以定制。

4) 服务意义

- 指定的高级安全顾问跟踪服务，对企业安全状况了解更充分，可提供优质的远程技术支持服务和针对性的防病毒建议。
- 通过长期的趋势比较分析，直观呈现病毒感染数量变化趋势和染毒计算机数量变化趋势，使客户对自己的安全状况一目了然。
- 每个阶段的安全状况通过巡检报告的形式呈现，使客户直观具体的了解本阶段病毒概况并及时检测病毒防范工作的成效。