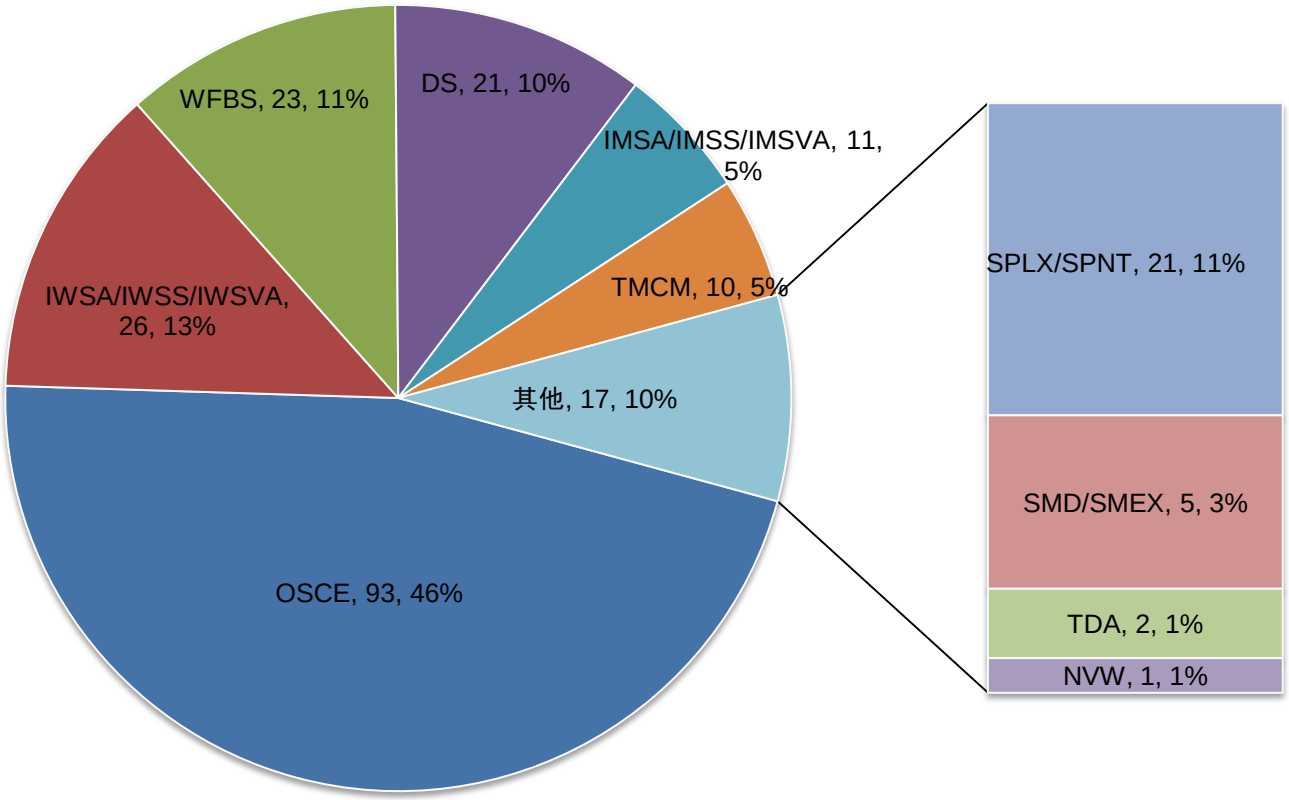
TREND MICRO 趋势科技 [全程护航 迈向云端]

第二季趋势科技产品问题
总结与分享

Freda Zhang
趋势科技培训部

第二季度产品案件排名



第二季度经典问题分享

案例一：OSCE案例

- 问题描述：
  - 用户的OSCE 8.0程序在打开控制台后提示无权限

案例一：OSCE案例

- 问题排错：
  - IIS日志

2013-06-03 10:16:51 W3SVC3 10.21.0.183 GET /officescan/console/html/cgi/cgiChkMasterPwd.exe - 4343 - 10.21.0.183 Mozilla/5.0+(Windows+NT+5.2;+rv:15.0)+Gecko/20100101+Firefox/15.0.1 403 19 1314

2013-06-03 10:17:03 W3SVC3 10.21.0.183 GET /officescan/console/html/cgi/cgiChkMasterPwd.exe - 4343 - 10.21.0.183 Mozilla/5.0+(Windows+NT+5.2;+rv:15.0)+Gecko/20100101+Firefox/15.0.1 403 19 1314

2013-06-03 10:17:03 W3SVC3 10.21.0.183 GET /officescan/console/html/cgi/cgiChkMasterPwd.exe - 4343 - 10.21.0.183 Mozilla/5.0+(Windows+NT+5.2;+rv:15.0)+Gecko/20100101+Firefox/15.0.1 403 19 1314

2013-06-03 10:17:04 W3SVC3 10.21.0.183 GET /officescan/console/html/cgi/cgiChkMasterPwd.exe - 4343 - 10.21.0.183 Mozilla/5.0+(Windows+NT+5.2;+rv:15.0)+Gecko/20100101+Firefox/15.0.1 403 19 1314

2013-06-03 10:17:07 W3SVC3 10.21.0.183 GET /officescan/console/html/cgi/cgiChkMasterPwd.exe - 4343 - 10.21.0.183 Mozilla/5.0+(Windows+NT+5.2;+rv:15.0)+Gecko/20100101+Firefox/15.0.1 403 19 1314

2013-06-03 10:17:08 W3SVC3 10.21.0.183 GET /officescan/console/html/cgi/cgiChkMasterPwd.exe - 4343 - 10.21.0.183 Mozilla/5.0+(Windows+NT+5.2;+rv:15.0)+Gecko/20100101+Firefox/15.0.1 403 19 1314

403.19 不能为这个应用程序池中的客户端执行 CGI

http://support.microsoft.com/kb/318380/zh-cn

案例一：OSCE案例

- 解决方案：

1.点击 [开始] > [所有程序] > [管理工具] > [Internet信息服务（IIS）管理器]

2.展开OfficeScan所在服务器[服务器名（本地计算机）] > [应用程序池] > [DefaultAppPool],检查[DefaultAppPool]是否处于运行状态。

右键点击选择“停止”，然后右键点击选择“启动”来重新启动[DefaultAppPool],检查问题是否能够解决。

3.如果问题仍然存在，请右击[DefaultAppPool]，选择属性，点击[标识]选项卡，在“预定义帐户”中选择“本地系统”选项，点击[确定]，弹出确认窗口，点击[是]确认.

4.重新启动IIS的服务，尝试打开控制台。

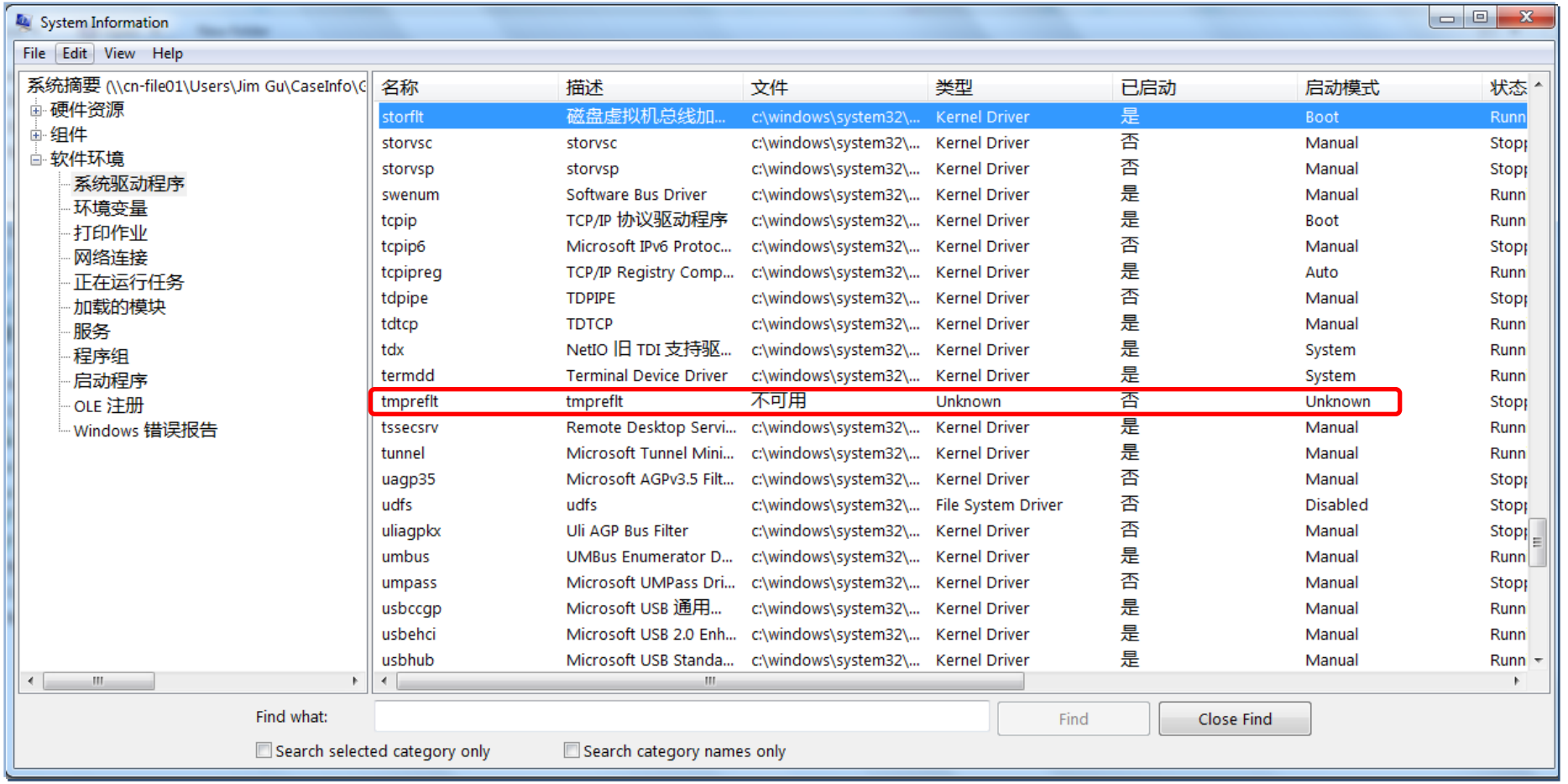
案例二：SPNT案例

- 问题描述：
  - 在WINDOWS 2008 日上安装SPNT 5.8的时候提示“先前版本的SPNT驱动程序已经存在，请重新启动目标计算机并重试”
  - 服务器上安装了OSCE的WEB控制台

案例二：SPNT案例

- 问题排错：
  - 确认删除过SPNT在该机上的有关注册表键值（Solution 68451）
  - 电脑也重新启动过，仍不能成功安装
  - 收集安装日志sp5.log

案例二：SPNT案例

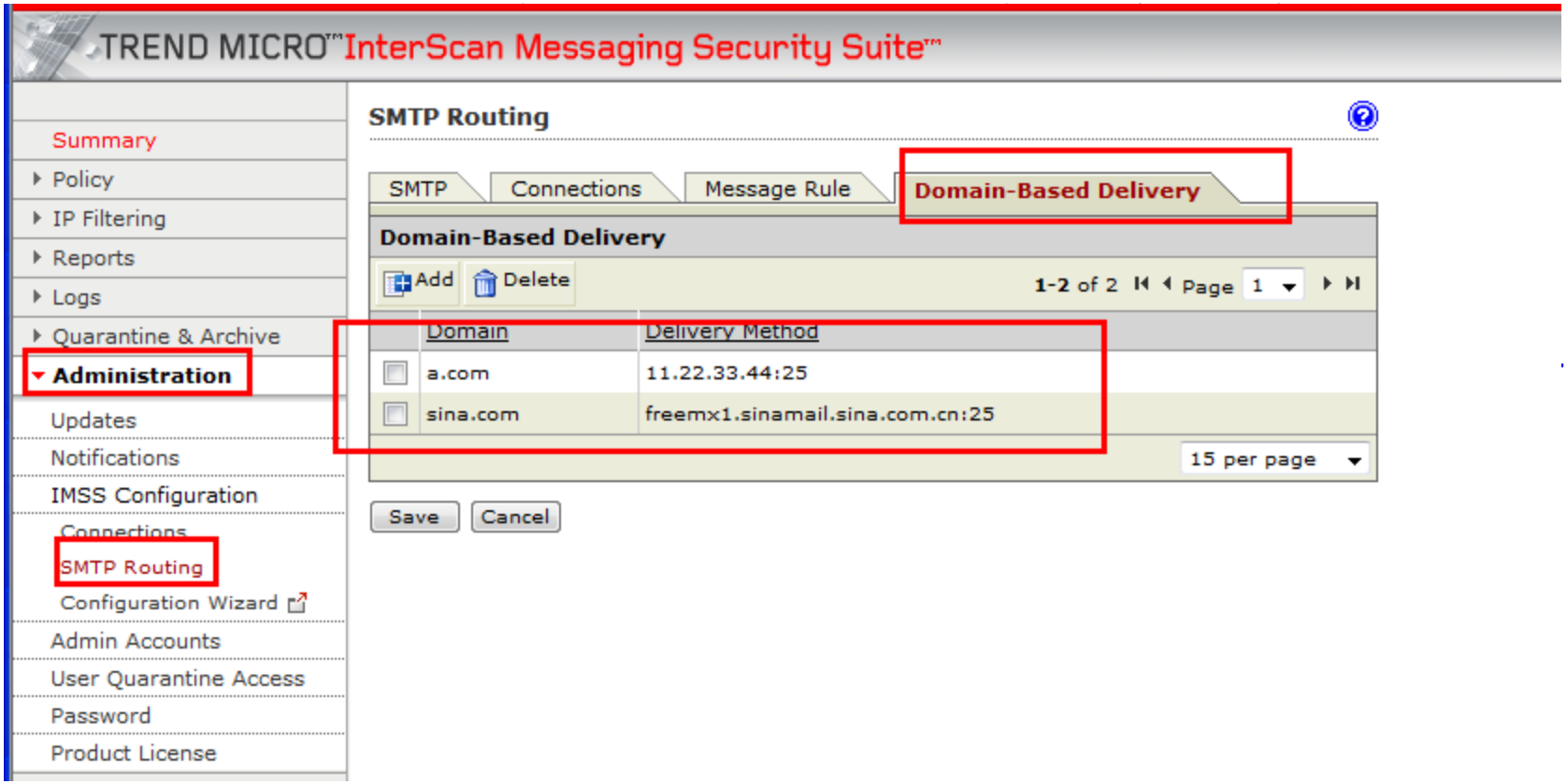


案例二：SPNT案例

- 解决方案
  - 卸载tmpreflt驱动
  - 重启服务器
  - 重新安装SPNT

案例三：IMSS案例

- 问题描述：



案例三：IMSS案例

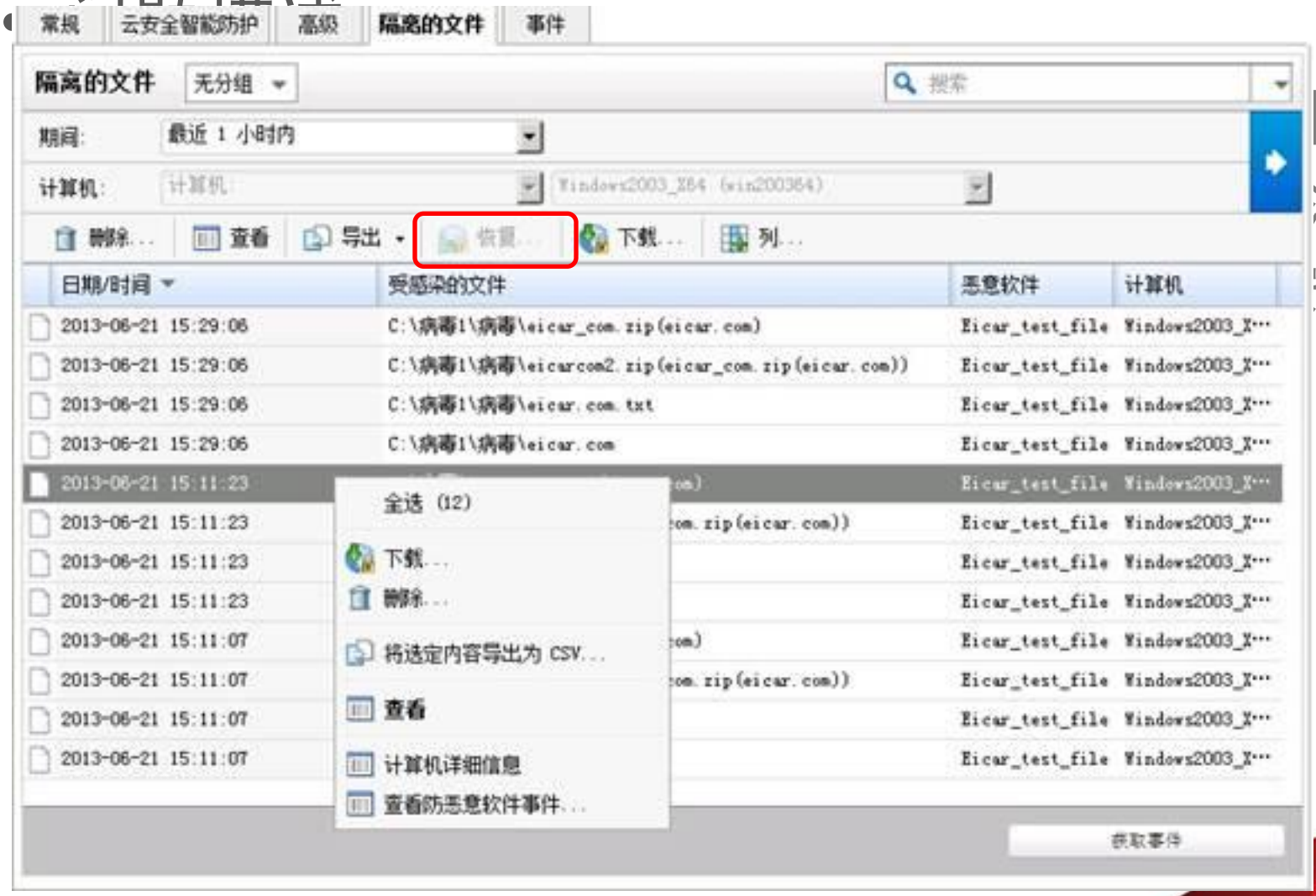
- 问题分析：
  - IMSS在domain-based delivery里面无法将同样的域名添加两次
  - hand off操作基于某个action之后才会触发操
  - 无法满足客户的该需求

案例三：IMSS案例

- Workaround方法：
  - 在IMSA的domain-based delivery里面添加一条记录，邮件服务器的地址填写FQDN名而非IP地址
  - 通过客户的DNS或者在IMSS服务器的host文件中手动将该FQDN名指向多个IP来实现客户的需求

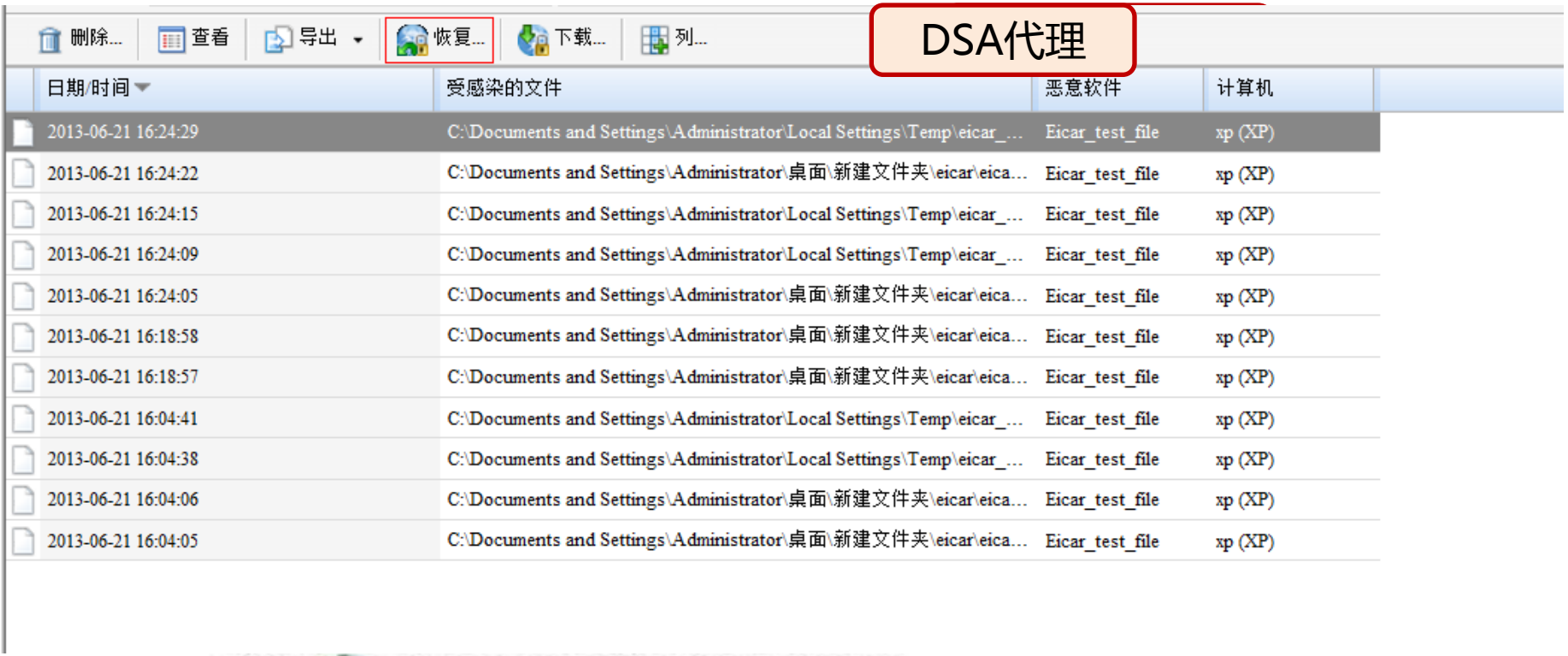
案例四：DS案例

- 问题描述



恢复
法通
键

案例四：DS案例



- 下载...（）可将隔离文件从计算机或虚拟设备移动到选定位置。
- 删除...（）可从计算机或虚拟设备删除一个或多个隔离文件。
- 将有关隔离文件（并非文件本身）的信息导出（）为 CSV 文件。
- 查看隔离文件的详细信息（）。
- 查看检测到恶意软件的计算机的**计算机详细信息**（）窗口。
- **查看防恶意软件事件...**（）显示与此隔离文件关联的防恶意软件事件。
- **添加或删除列**（）通过单击**添加/删除**可添加或删除列。
- 搜索（）特定隔离文件。

案例四：DS案例

- 结论：
  - 此“恢复”功能只适用于DSA,不适用与无代理防护

案例五：IWSA案例

- 问题描述：
  - 用户部分手机端WIFI接入热点，无法通过QQ连接服务器
  - 用户环境中问题了IWSVA5.1

案例五：IWSA案例

- 问题排错：
  - 其他桌面端及手机端的QQ都能正常访问服务器
  - 已检查其他防火墙或者可能做限制的设备，都已放行。

案例五：IWSA案例

- 问题分析：
  - 当一些HTTP流量数据包格式不符合标准HTTPS流量的数据格式时会导致IWSVA无法正常处理这些流量
- 解决方法
  - 通过开启tunnel_non_http_traffic 功能避免IWSVA对这些流量造成影响
    1. 使用SSH 方式登录IWSVA 5.1
    2. 输入clish 命令进入IWSVA 命令行控制台
    3. 输入‘enable’进入enable模式
    4. 输入‘configure module http non_http_bypass enable’

哪些您可以自己解决？

问题名称	解决方案来源	备注
服务器安装/升级部署咨询	SOP、Readme、AG	包括咨询服务器如何安装/升级、服务器支持哪些哪些系统等。
客户端部署咨询	AG、Readme	包括咨询客户端有哪些安装方式、客户端如何安装、客户端支持哪些操作系统等。
服务器占用空间过大/OSCE 10.0 WSS文件夹过大	KB	
咨询OSCE是否有某些功能/某些功能如何设置	Readme、AG	比如设备管理、漫游客户端等
web控制台密码重置	KB	
恢复隔离文件	AG、KB	
咨询OSCE下载地址	官网下载专区	
客户端卸载/退出密码重置	下载专区	
需要文档	KB	包括管理员手册、安装部署手册
服务器更改IP/主机名/安装方式		
哪些版本OSCE能够注册TMCM	Readme	
如何设置服务器从其他更新源更新	KB、AG	

遇到问题怎么办？

简单处理

- 系统日志、报警信息等
- 重启计算机、进程、服务等

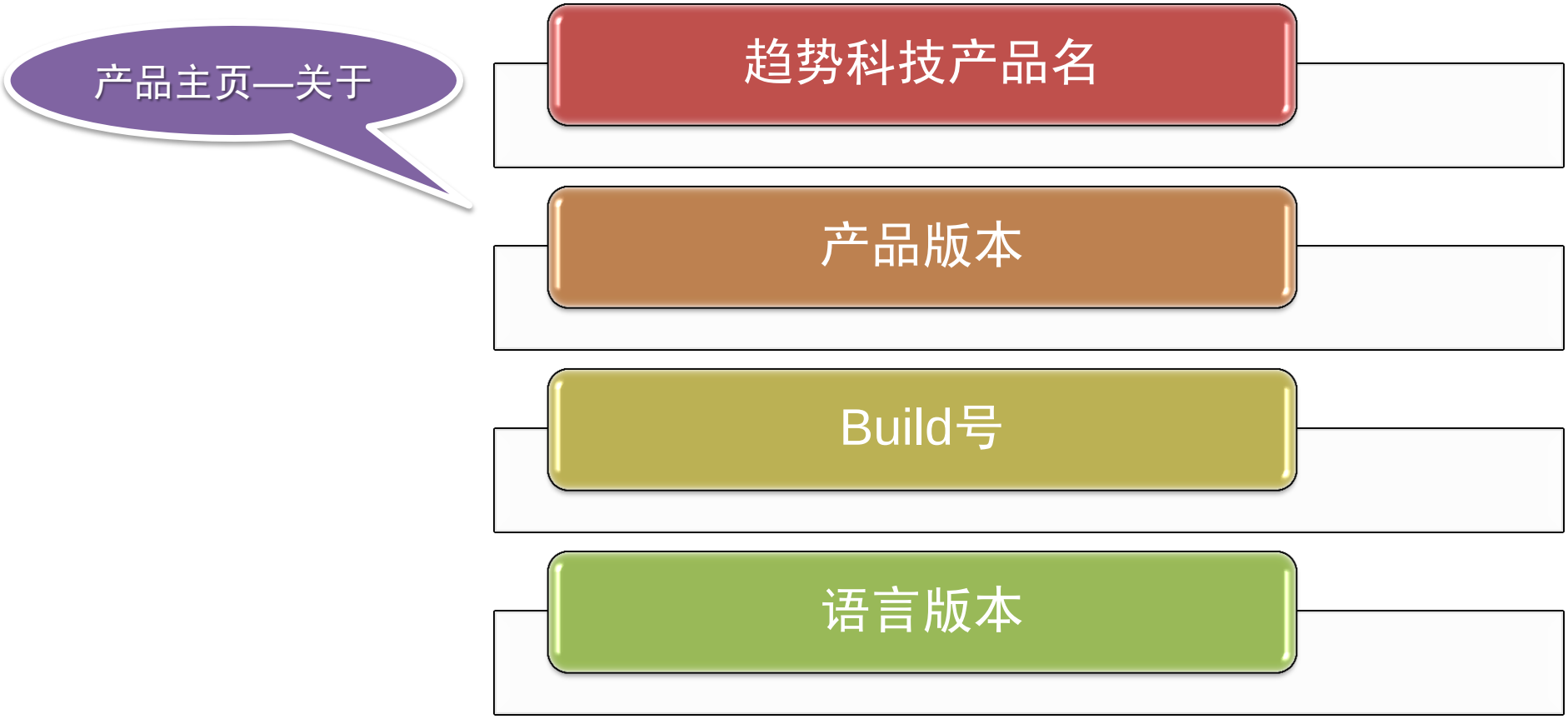
寻求帮助

- 产品知识库
- 自述手册、管理员文档等
- 趋势科技技术支持

深入判断

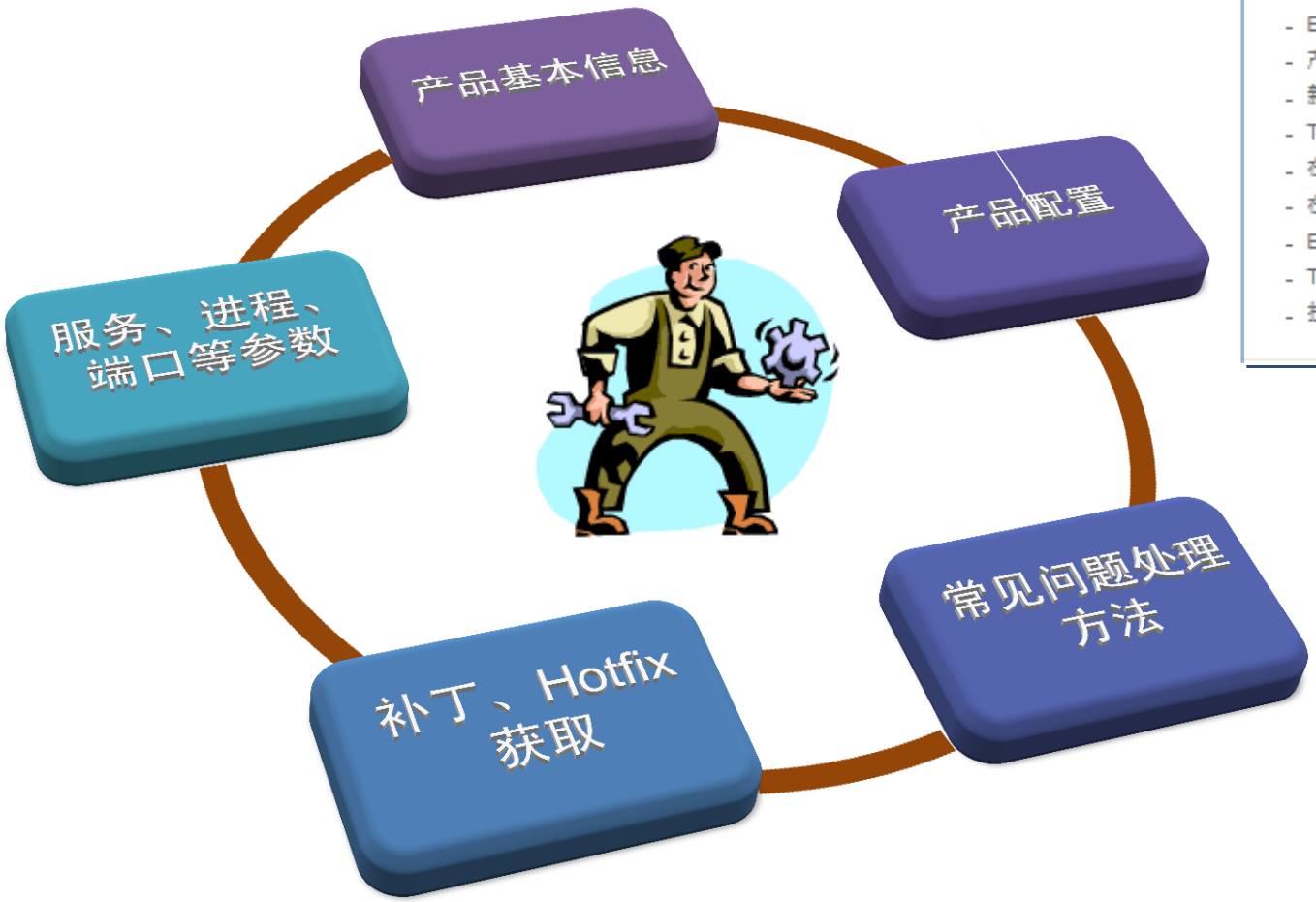
- 配置修改
- 参数调整
- 调试日志分析等

产品基本信息获取



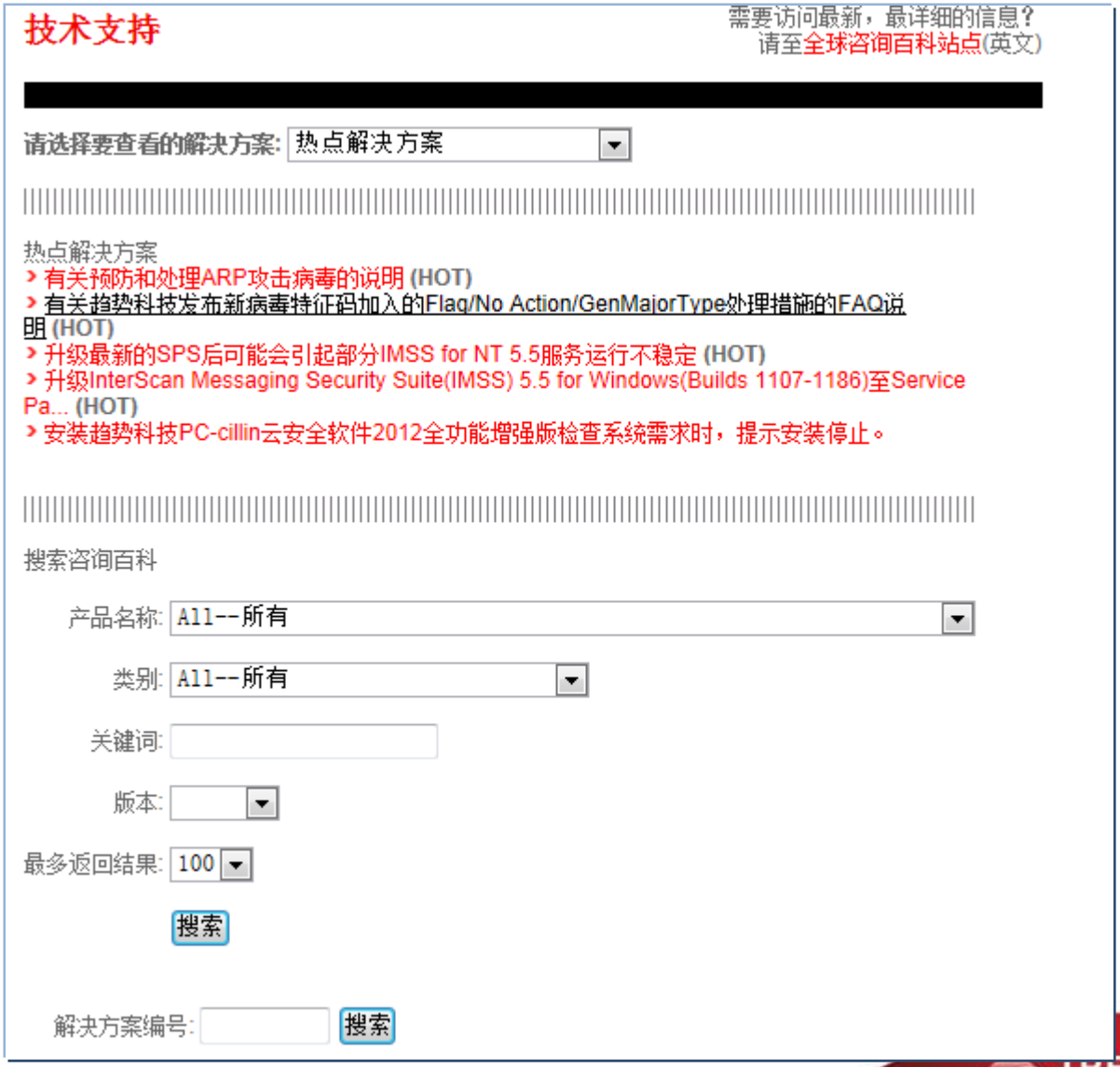
了解产品基本信息，有助于问题有效解决

产品知识库中有些什么？



知识库之搜索

- 选择正确参数帮助你获取最佳结果



知识库之关键字

- 问题类别
  - 更新、配置、升级、安装等
- 错误提示
  - “错误的应用程序 DBserver.exe”
  - ”
- 日志结果
  - 日志文件名
  - 日志中错误信息等

Faulting application DbServer.exe, version 10.0.0.1895, time stamp 0x4b6bdb4e, faulting module DbServer.exe, version 10.0.0.1895, time stamp 0x4b6bdb4e, exception code 0x40000015, fault offset 0x000c91b0, process id 0x1dfc, application start time 0x01cafb39285abdb6.

常用文档资料获取

- 管理员手册
- SOP文档
- 升级文档
- 自述文件
- ……

TREND MICRO 趋势科技 全程护航 迈向云端

谢谢!

爱趋势互动社区 www.iqushi.com

趋势CEO Eva微博　　趋势官方微博

趋势云计算安全博客　　趋势云计算安全网站