TREND MICRO™ Securing Your Web World

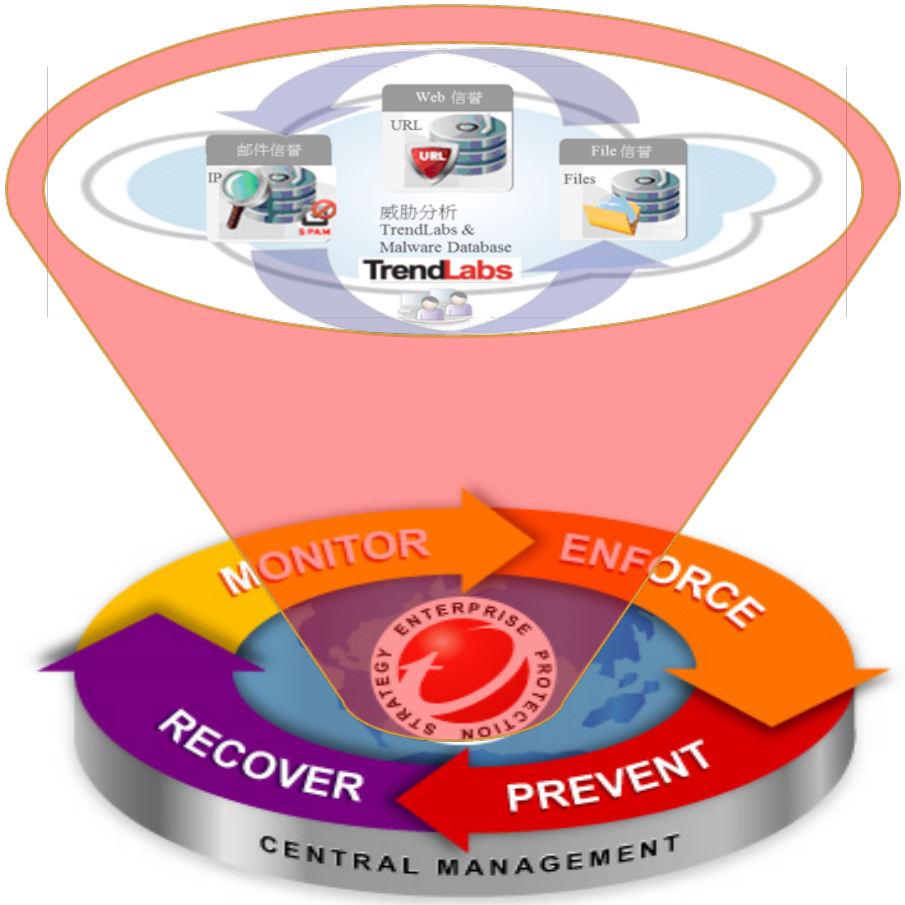
威胁預警平台:TMSP2.6 介绍

Jay Lin

Agenda

- 趨勢科技威脅預警解決方案
- TMSP 介紹
- TMSP 模組架構
- TMSP 功能介紹
- 趨勢科技威脅預警解決方案價值

趋势科技企业威胁管理战略



MONITOR
监控

威胁可视化

ENFORCE
阻斷

中断威胁活動

Remediation

專家治理

損害恢復

PREVENT
防护

安全加固

TREND MICRO

企业威胁管理战略

威胁预警解决方案

威胁预警平台

TMSP

威胁发现设备 (TDA)

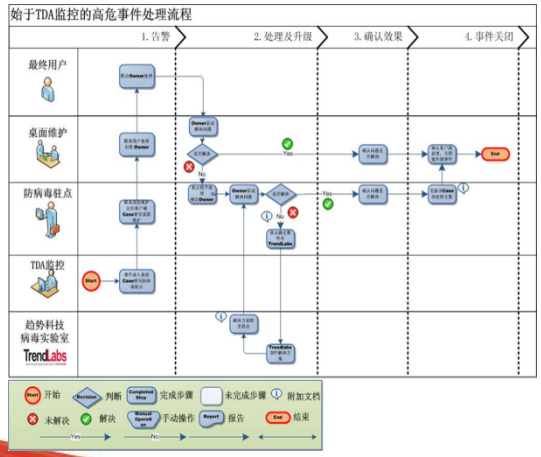
主要功能:

- **全网威胁预警平台,威胁管理仪表板**
- **定位感染源**
- **智能分析技术**
- **日周月报表,威胁趋势,威胁说明与处理建议**

威胁治理解决方案

主要功能:

- 7X24 监控运维中心
- 流程规划
- 中国病毒实验室资源支撑
- 专属客户经理
- 全国覆盖认证服务伙伴



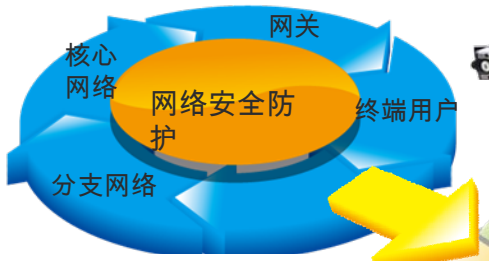
威胁阻断解决方案

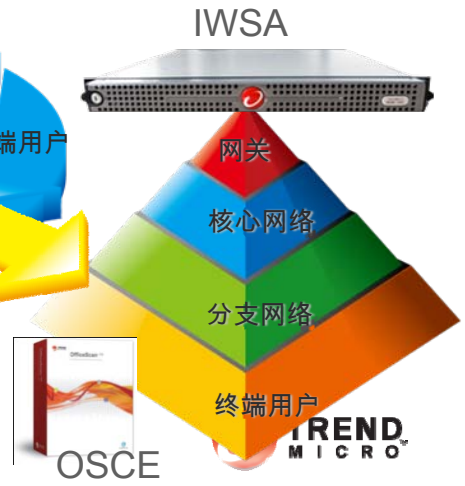
网络防毒墙NVW 3500i/1500i

主要功能:

- TDA 联动 阻断高危威胁
- 隔离感染电脑
- 断电直通
- 报表

威胁防护解决方案



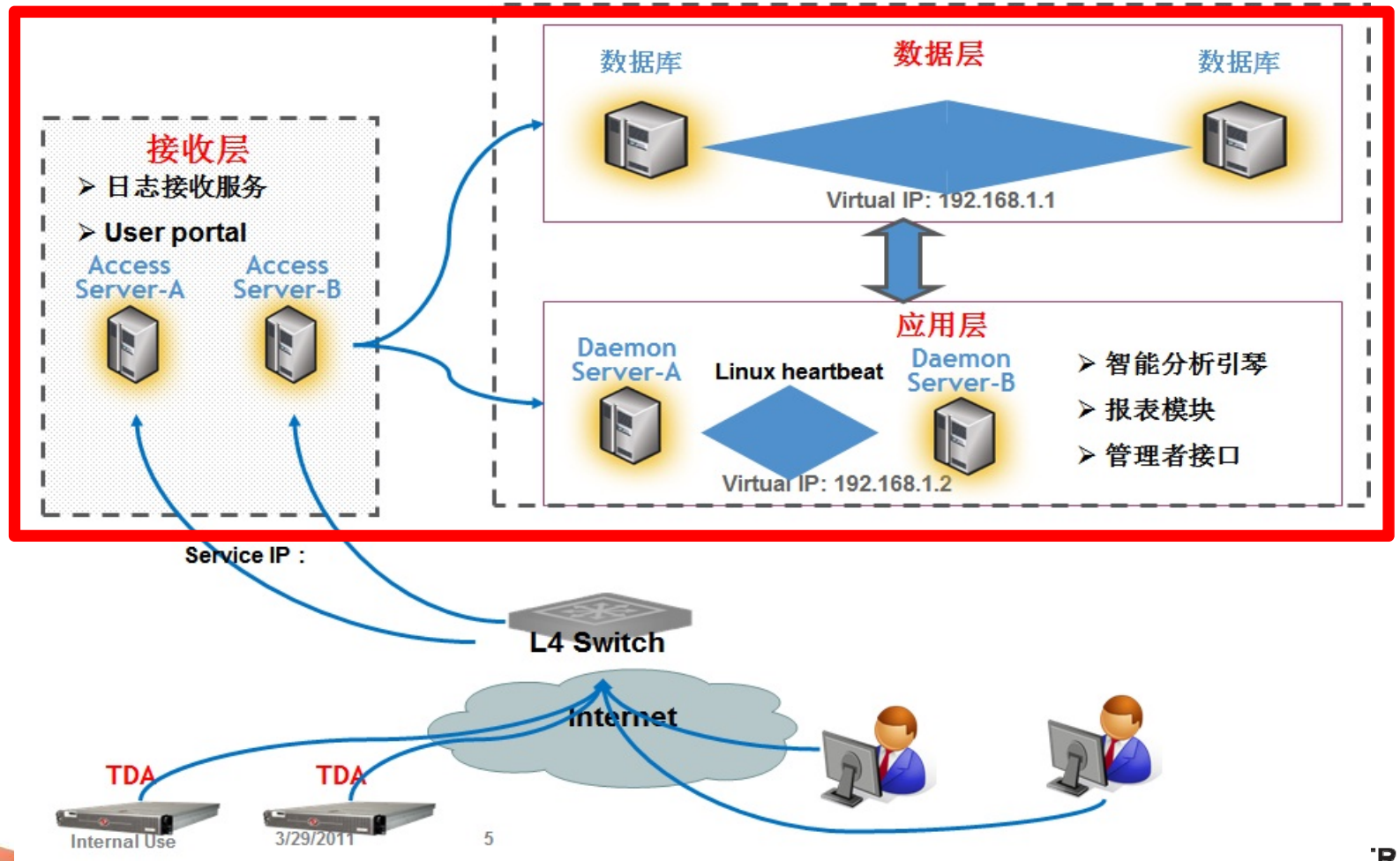


主要功能:

- 阻断网页与邮件的威胁
- 提高带宽利用率
- 统一终端安全管理平台

TMSP：軟件架構內容

***接收層:**TMSP前端应用服务器，负责提供門戶網站,威脅儀表板和日志接收等功能
***應用層:**数据分析服务器，负责提供管理控制台，数据分析，报表生成，通知等功能
***數據層:**后台数据库，负责提供数据存储和优化

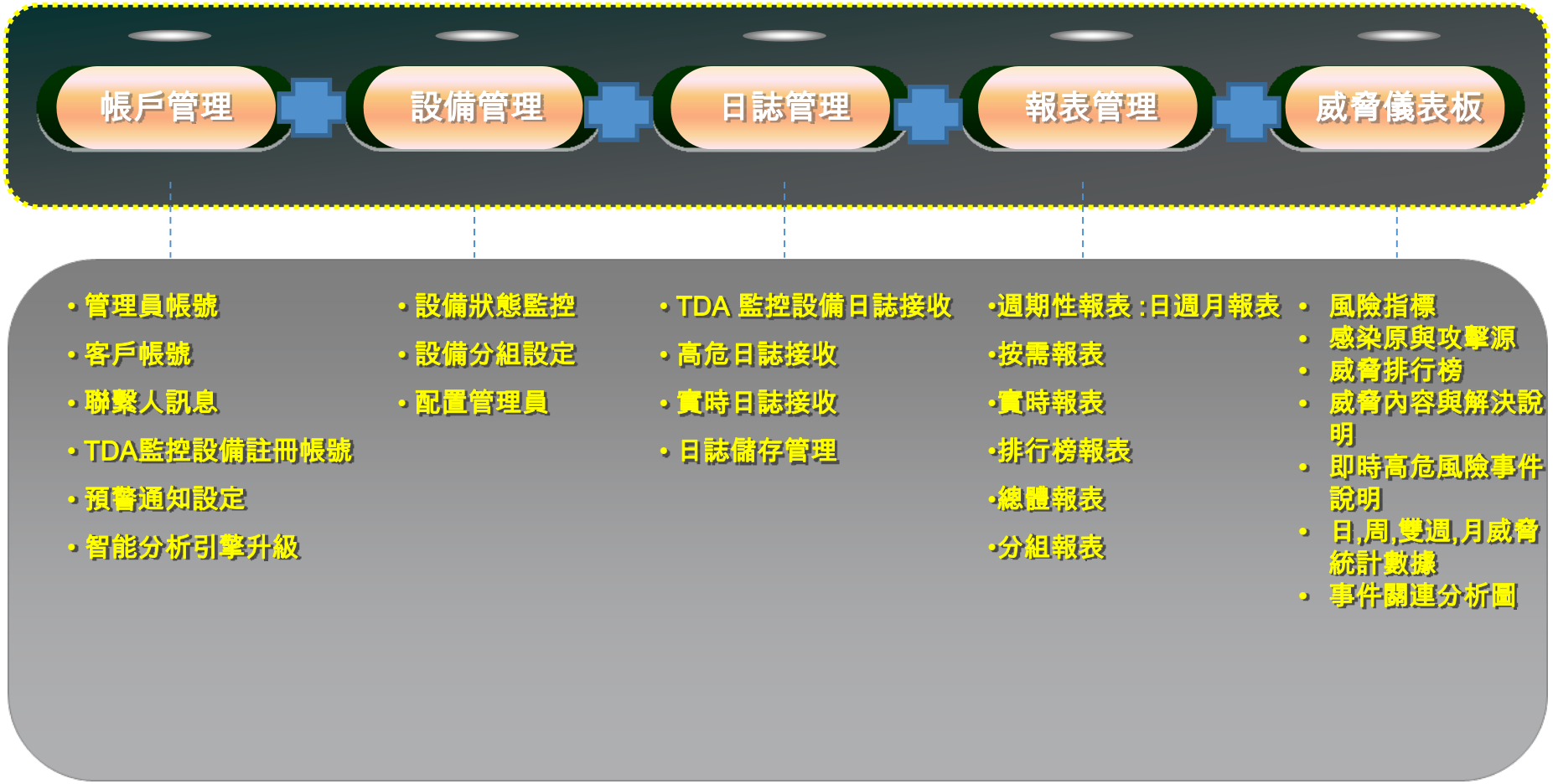


威脅預警平台TMSP

- 威脅預警平台將客戶環境中海量的日誌,抽絲剝繭找出環境中的威脅事件
- 告知威脅的本質,風險的含量
- 告知威脅的源頭與目的
- 讓客戶環境中威脅:數據化,圖形化達到威脅的可見性

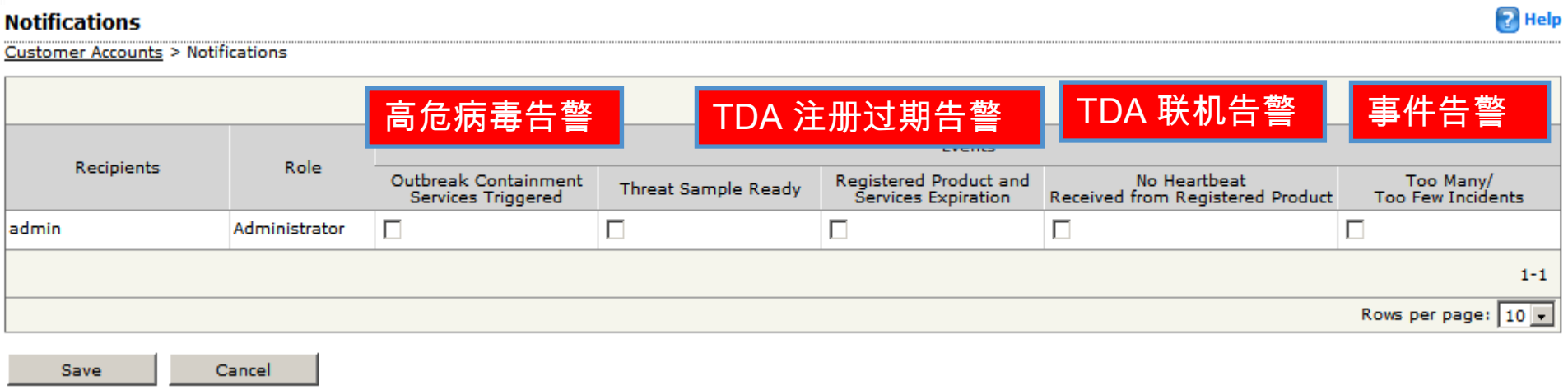
企业威胁的可见性

TMSP的功能模塊



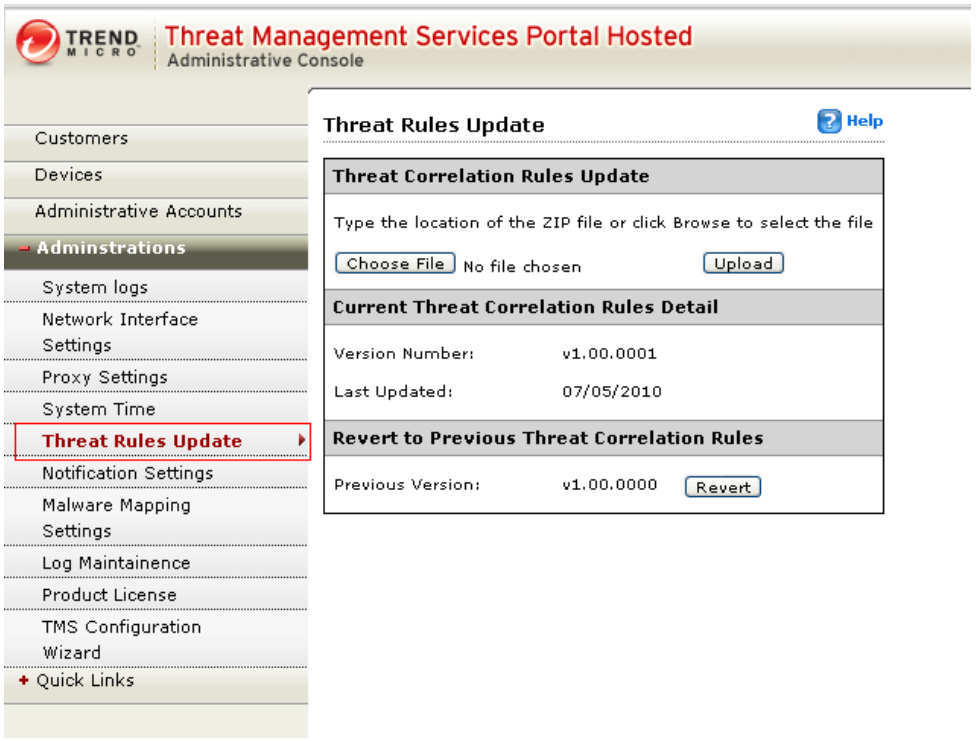
帳戶管理

- 账号管理
  - 管理员账号
    - TMSP 系統管理員，进行TMSP系統設定,建立客戶帳號
  - 客户账号
    - 用于登录TMSP威脅儀表板，報表下載
  - 聯繫人信息
    - 預警通知郵件訊息
    - TDA 監控設備註冊帳號
  - 預警通知設定
  - 智能分析引擎升級



TMSP 规则更新与回复

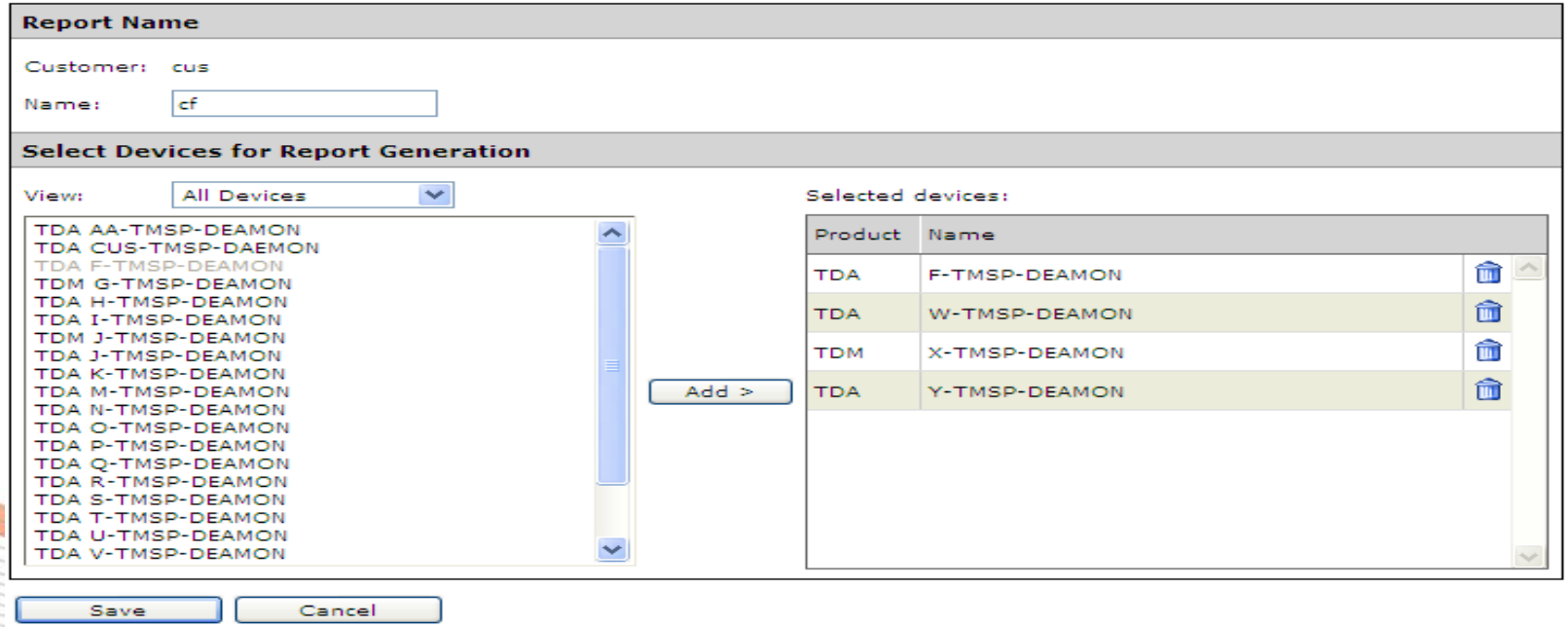
- TMSP 规则主要是对于 TDA 上传的日志进行关连交叉分析
- 提供TMSP 规则版本
- 提供TMSP 规则包更新
  - 网页手工更新
  - 压缩包密码保护
- 规则回复
  - 提供TMSP 规则回复功能



设定TDA 设备监控群组

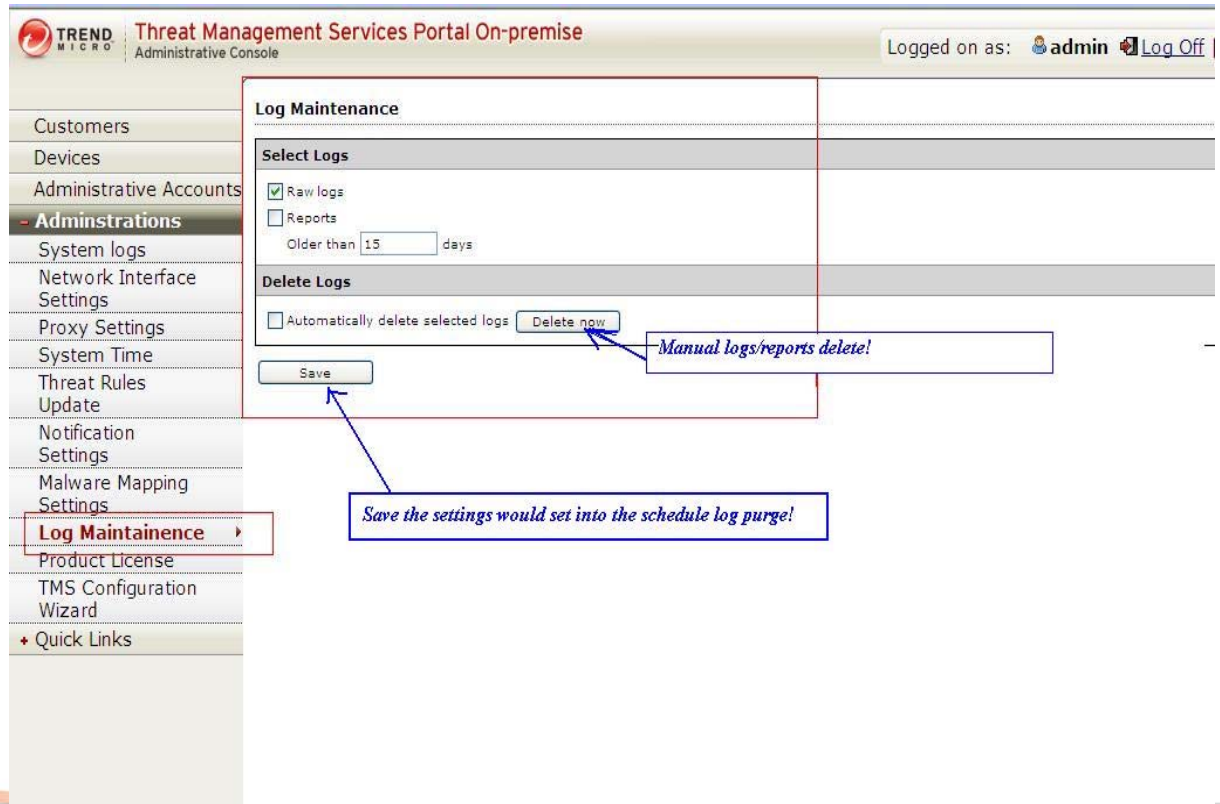
适用于多台TDA 的环境:

- 设定哪几台TDA 属于同一个群组
- 一台TDA 可以被设定到不同的群组中
- TMSP 可以对群组产生报表
- 例如 XXX公司,购买5 台TDA .分布在北京与上海 .
  - 可以进行设定TDA 1,2,3 为上海群组
  - TDA 4,5 属于 北京群组 .
  - TDA 1,2,3,4,5 为集团群组
  - TMSP 会产生上海,北京,集团群组的报表



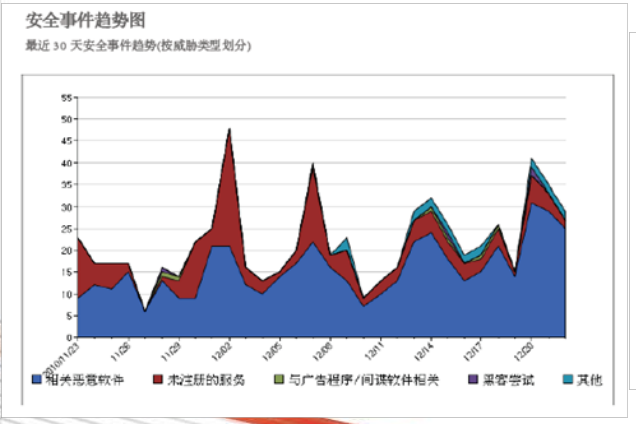
日志管理

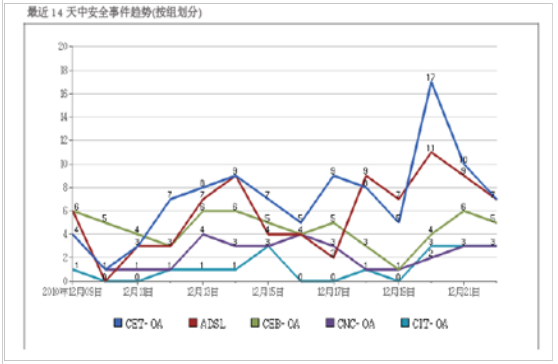
1. 日誌種類
   - 周期日志:TDA威脅日誌,Web信譽偵測日誌,中斷程序應用日誌,網路文件傳輸日誌
   - 實時日誌 : 已確定威脅日誌
   - 高危日誌 :屬於高危威脅.偵測事件以OPS_ 開頭命名,作為高危病毒預警通知
2. 日誌接收
   - 週期日誌上傳: 以TDA 日誌上傳設定為主,最快 6 小時
   - 實時日誌:每10分鐘接收一次,
   - 高危日誌:偵測即上傳
3. 日誌維護
   - 設定維護週期
   - 自動/手動維護
   - TDA 原始日誌



報表管理

1. 報表種類
   - 周期報表 :日/周/月報表 ,自動寄送
   - 實時報表 :攻擊源,威脅行為,IP分組,攻擊協議
   - 按需報表 : 自設時間週期,運行總結報告
   - 行業對比報表: 行業對比,全部客戶對比,風險等級對比,威脅類型對比,威脅事件對比
2. 報表內容
   - 安全事件趨勢圖
   - 威脅事件趨勢圖
   - 客戶部門威脅對比
   - 安全事件綜數
   - 高風險客戶端：多重感染行為,高風險威脅
   - 各類威脅排行榜數據
   - 威脅事件說明,影響,分析與建議





2. 蠕虫病毒通过漏洞传播

前十攻击源与分组

攻击源	分组	计数
10.128.17.1	CET-OA	105
10.128.12.104	CET-OA	2
10.128.64.128	CET-OA	2
192.168.2.54	adsl-CET&CIC	2
10.128.32.133	CET-OA	2
10.128.162.69	CIC-OA	1
10.128.131.175	CIC-OA	1
10.128.131.201	CIC-OA	1

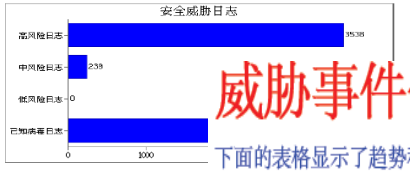
前十攻击目标与分组

攻击目标	分组	计数
10.110.97.43		105
10.129.156.1		1

日報表說明

每日安全威胁日志统计

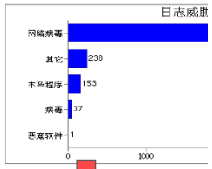
下面的图表显示了TDA在报表统计范围期间内所检测到的日志统计.这个数字显示了TDA所收集的原始日志数量。



威胁事件侦测摘要

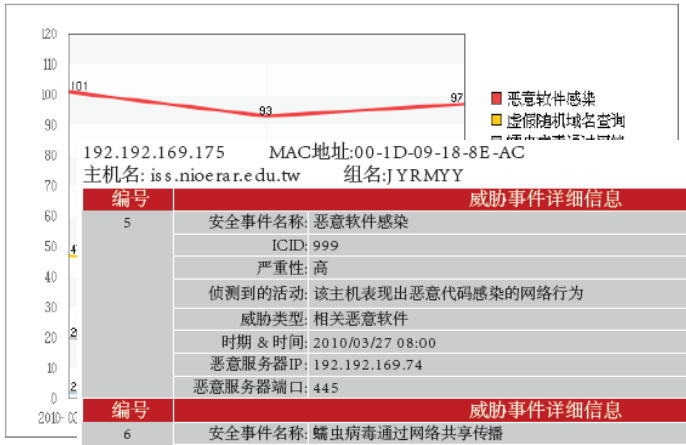
下面的表格显示了趋势科技TMSP威胁管理平台利用先进的云安全和关联分析技术对TDA设备上传的日志进行交叉分析后过滤过去三天威胁趋势在的重要风险。

下面的图表显示了TDA在报表统计日期范围内的原始日志数量。



在报告期内总共发现 165

威胁类型
恶意软件感染
虚假随机域名查
蠕虫病毒通过网络共
通过SMB进行暴力



192.192.169.175 MAC地址:00-1D-09-18-8E-AC
主机名: iss.nioerar.edu.tw 组名:JYRMYY

编号	威胁事件详细信息	返回起始位置
5	安全事件名称: 恶意软件感染	
	ICID: 999	
	严重性: 高	
	侦测到的活动: 该主机表现出恶意代码感染的网络行为	
	威胁类型: 相关恶意软件	
	时期 & 时间: 2010/03/27 08:00	
	恶意服务器IP: 192.192.169.74	
	恶意服务器端口: 445	

编号	威胁事件详细信息	返回起始位置
6	安全事件名称: 蠕虫病毒通过网络共享传播	
	ICID: 82	
	严重性	
	侦测到的活动	
	威胁类型	
	时期 & 时间	
	恶意软件名称	
	攻击的主机的数量	

CN-江阴人民医院_daily_report_2010_03_27_zh_cn.pdf (666 KB)

亲爱的用户，您好！
昨日贵单位的TDA设备主要检测到以下威胁，具体详情请参考附件PDF文档，谢谢！

威胁行为	影响	检测次数	主要受影响客户机	处理建议	备注
恶意软件感染	影响系统运行，网络性能，下载新病毒	97	192.192.186.246 192.192.186.23 192.192.186.87 192.192.182.227 192.192.186.200	闪电杀毒手	该主机表现出恶意代码感染的网络行为
虚假随机域名查询	组建僵尸计算机网络	43	192.192.182.16 192.192.186.72 192.192.186.127 192.192.186.45 192.192.186.75	使用闪电杀毒手和downad专杀工具清毒	已检测到来自该主机的Kraken通信。
蠕虫病毒通过网络共享传播	攻击网络，暴力破解域账号	24	192.192.186.17 192.192.186.147 192.192.182.158 192.192.182.242 192.192.182.26	设置复杂系统口令，关闭不必要的共享目录，使用闪电杀毒手进行清毒	WORM_DOWNAD.AD PE_LOOKED.AC-O PE_LOOKED.AC
通过SMB进行暴力攻击	破解系统帐号	1	192.192.186.87	闪电杀毒手和sysclean清毒	该主机多次通过SMB协议登录到多个主机，均失败。

功能	提供专业分析报告
优势	庞大的规则数据库 7*24小时专家值守
价值	降低管理复杂度 体现IT管理绩效 避免同类威胁产生

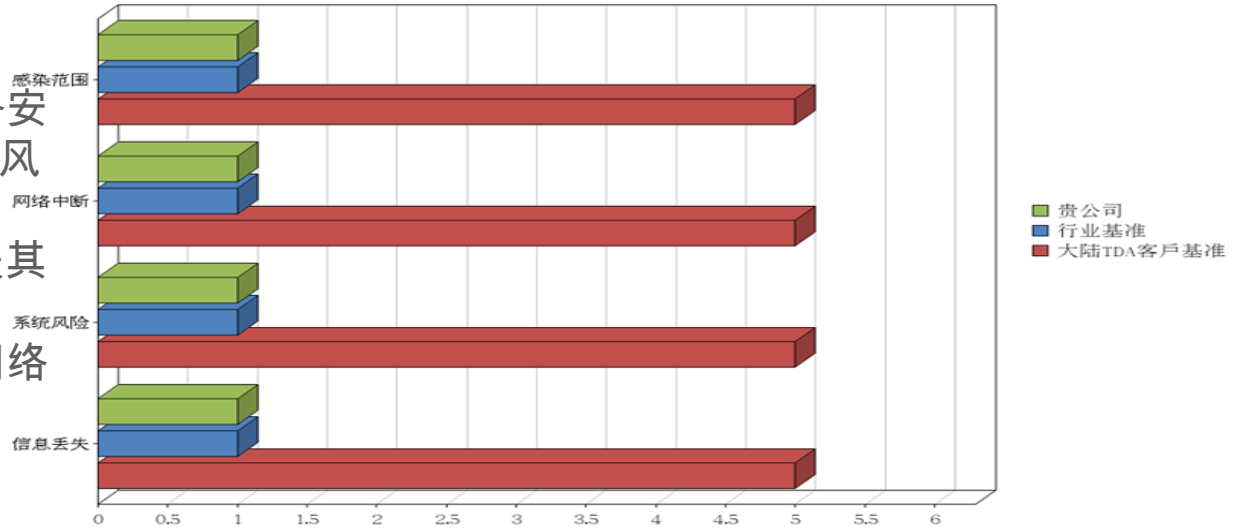
行業比對報表

风险水平基准摘要

报告会从四个方面来衡量企业网络安全,分别为感染范围,网络中断,系统风险,信息丢失

其数值范围在1~9内,数值越高代表其风险越高。

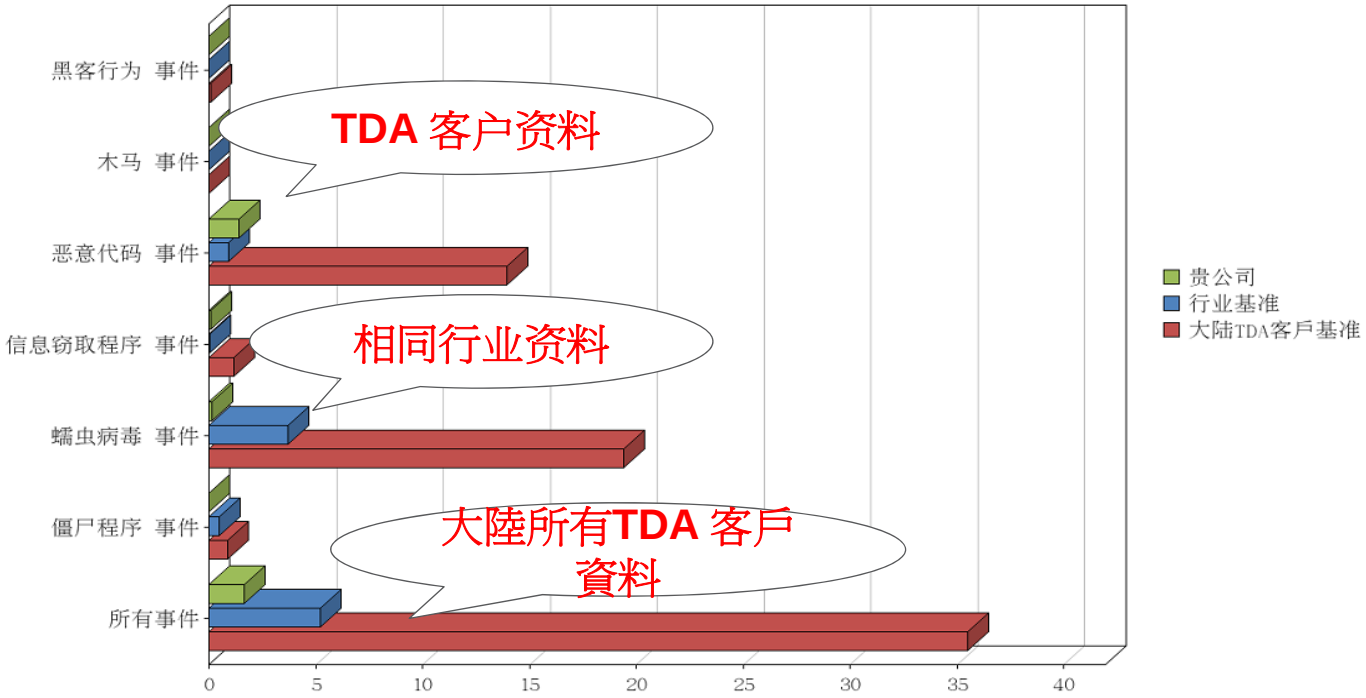
客户通过数据对比可以了解自身网络安全在行业中处于何种水平



威脅類型比對:

此处列出报告期间内客户网络中各类威胁事件的每日平均数量

客户可以通过此表了解自身网络中存在的主要威胁，以及行业中目前存在的主要问题。



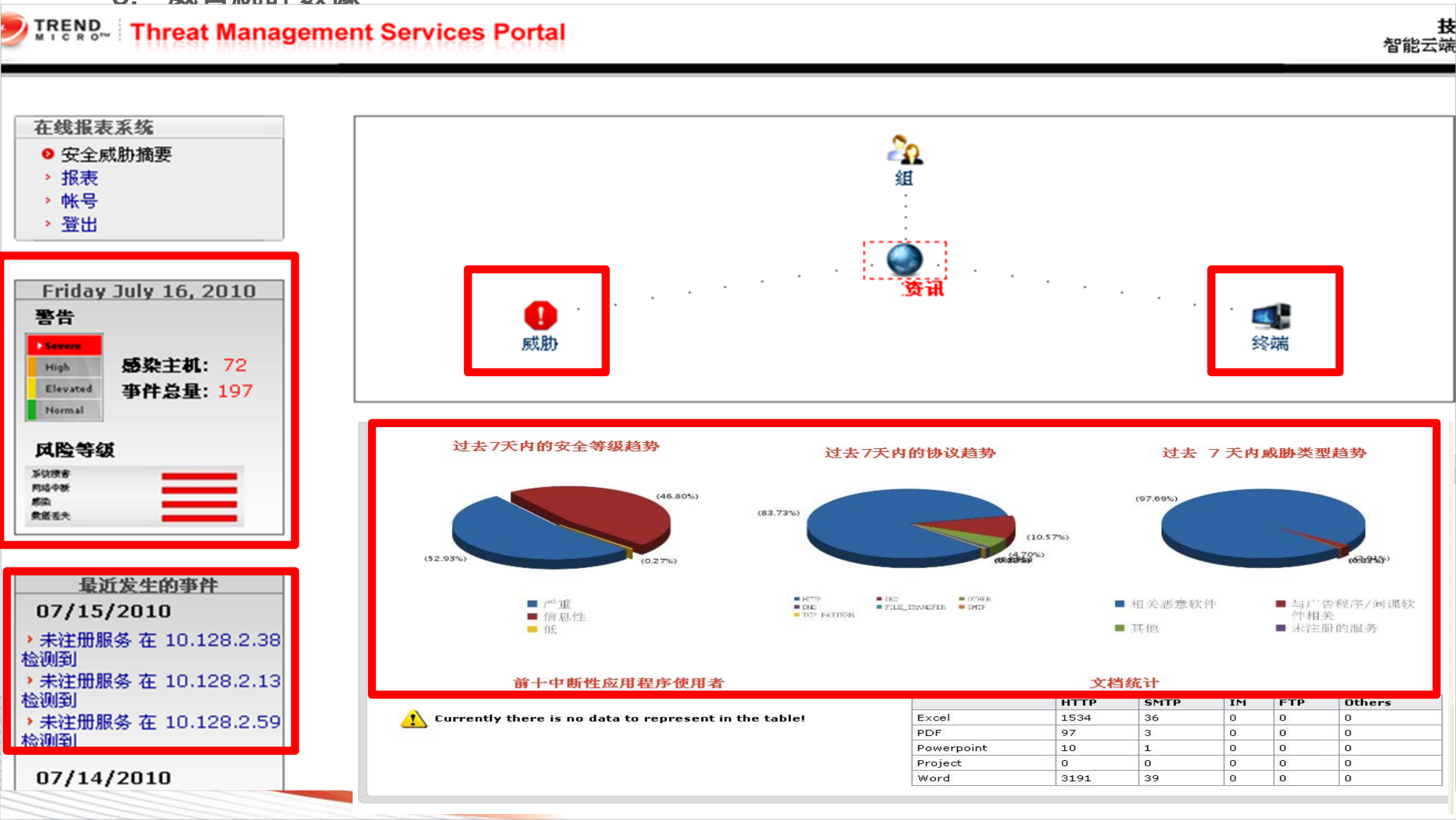
部门威胁分析

最近 14 天中安全事件趋势(按组划分)

所属分组	11月18日	11月19日	11月20日	11月21日	11月22日	11月23日	11月24日	11月25日	11月26日	11月27日	11月28日	11月29日	11月30日	12月01日
顾桥	正常	正常	正常	正常	正常	正常	正常	正常	正常	正常	正常	中风险	高风险	中风险
丁集新	正常	正常	高风险	正常	正常	正常	正常	正常	正常	正常	正常	中风险	正常	正常
东方医院	正常	正常	正常	正常	正常	正常	正常	正常	正常	正常	正常	正常	正常	正常
救护大队	正常	中风险	正常	正常	正常	正常	正常	中风险	中风险	正常	正常	中风险	中风险	中风险
瓦地院	正常	正常	正常	正常	正常	正常	正常	正常	正常	正常	正常	正常	正常	正常
李一矿	正常	正常	正常	正常	正常	正常	正常	正常	正常	正常	正常	正常	中风险	中风险
安装分公司	正常	正常	正常	正常	正常	正常	正常	正常	正常	正常	正常	正常	正常	正常
谢一矿	正常	正常	正常	正常	中风险	正常	正常	正常	正常	正常	正常	正常	正常	中风险
丁集	正常	正常	中风险	正常	正常	正常	中风险	正常	正常	正常	正常	正常	正常	正常
潘三矿	中风险	正常	正常	正常	正常	中风险	正常	中风险	正常	正常	中风险	高风险	中风险	高风险
谢桥	正常	正常	正常	正常	正常	正常	正常	正常	正常	正常	正常	正常	正常	正常
潘一矿	正常	正常	中风险	正常	中风险	正常	中风险	正常	正常	正常	中风险	中风险	中风险	正常
留守处	正常	正常	正常	正常	正常	正常	正常	正常	正常	正常	正常	正常	正常	正常
勘探公司	正常	正常	正常	中风险	正常	正常	正常	正常	正常	正常	正常	正常	中风险	正常

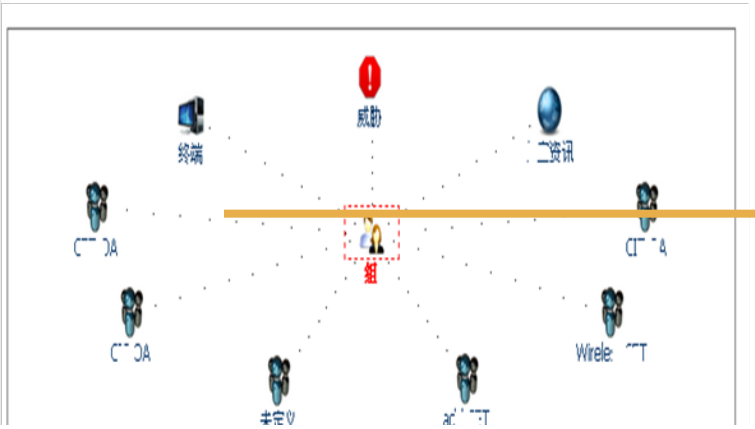
全网恶意威胁的可见性:威胁管理仪表版

1. 公司風險指標: 公司目前的風險等級
2. 定位感染原與攻擊源
3. 威脅內容與解決說明
4. 即時高危風險事件 說明
5. 威脅統計數據



智能分析平台

1. 威脅事件內容
2. 安全事件追蹤
3. 即時高危風險事件 說明



cetisa02.gi.compal.com

主机名/IP 地址:	cetisa02.gi.compal.com
IP地址:	10.128.2.38
监测网络:	CET-OA
MAC地址:	00-08-21-B4-B8-42
威胁等级:	严重

威胁详细信息

威胁详细信息

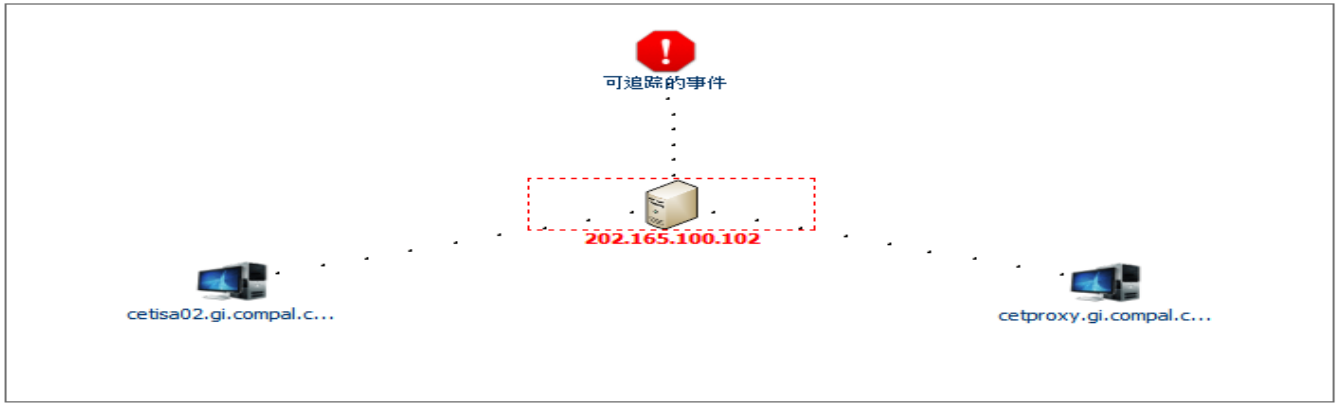
主机名/IP 地址	监测网络	已访问过的 URL	日期
cetisa02.gi.compal.com	CET-OA	http://pzrk.ru/img/logo4.gif?13b4e=80718&id=12589214702 4	03/15/2011 08:08:31
joyce_qi_xp2.gi.compal.com	CET-OA	http://pzrk.ru/img/logo4.gif?13b4e=80718&id=12589214702 4	03/15/2011 08:08:31
robert_gao.gi.compal.com	CET-OA	http://pzrk.ru/img/logo4.gif?1d08116=30441750&id=125892147024	03/11/2011 00:07:33
cetisa01.gi.compal.com	CET-OA	http://pzrk.ru/img/logo4.gif?1d08116=30441750&id=125892147024	03/11/2011 00:07:03
light_wu1.gi.compal.com	CET-OA	http://pzrk.ru/img/logo4.gif?16a8c=92812&id=12589214702 4	03/10/2011 15:41:44
cetisa01.gi.compal.com	CET-OA	http://pzrk.ru/img/logo4.gif?16a8c=92812&id=12589214702 4	03/10/2011 15:41:13

19 发现可追踪的事件

查看以往数据: 7 更新

事故原因

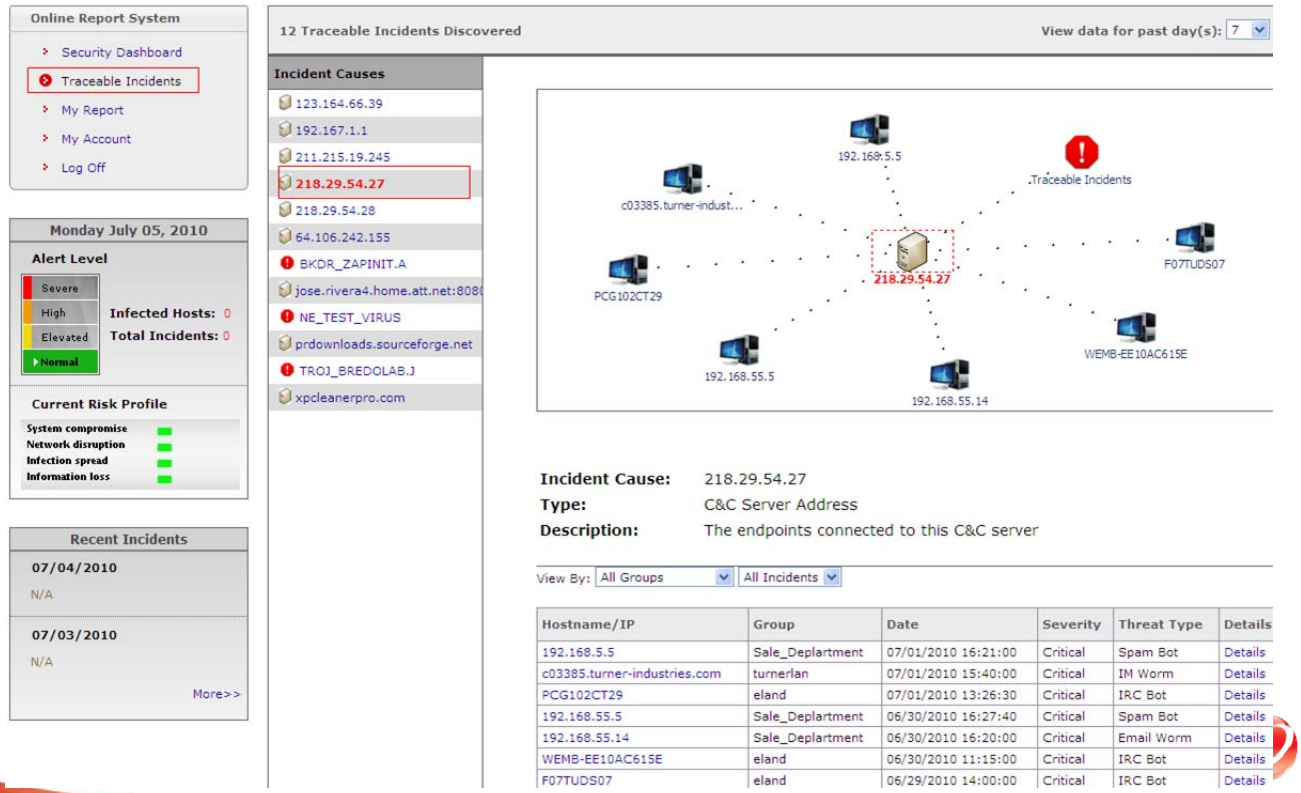
- 125.89.197.2
- 202.165.100.101
- 202.165.100.102
- 202.165.100.103
- 202.165.100.106
- 204.74.215.203
- 211.144.152.62
- 30xc1cjh91.com
- 61.155.169.146
- 7gafd33ja90a.com
- 873hgf7xx60.com
- l33t.brand-clothes.net
- lj1i16b0.com
- MS02-039_SQL_SERVER_RES
- n16fa53.com
- pica.banjalucke-ljepotice.ru
- pzrk.ru



事件起因:	202.165.100.102
类型:	可疑恶意源服务器
描述:	终端从这个服务器下载恶意软件

事件关连分析图

- 在门户网站中提供事件关连分析图
- 事件关连分析图提供以下关连项目
  - 连到相同C&C 控制服务器 的客户端展示图
  - 连到相同恶意代码下载网站的客户端展示图
  - 感染相同恶意代码的客户端展示图
  - …



TMSP 版本比较

项目	TMSP 企業版	TMSP 雲端版
定位	單一企業使用	服務大量客戶使用
需要多台安装	否	是
需要IP 数	4(可以手工设定成2 IP数)	6
门户网站 User portal	Yes	Yes
报表功能	Yes	Yes
报表模版更新	Yes	Yes
规则更新	Yes	Yes
TDA 设备联机监控通知	Yes	Yes
分级报表功能	Yes	Yes
日志维护功能	Yes	Yes
事件关连分析图	Yes	Yes
最多可支持TDA 数	5 台	100台
是否需要付费	Yes(公开报价500,000RMB)	No

TREND MICRO

系統需求

RESOURCES	REQUIREMENTS
Host machine	• 64 位元 * CPU • 2.0GHz processor minimum • 2.4GHz Intel™ Xeon™ E5530 processor recommended • RAM • 2GB minimum • 16GB recommended • Hard disk space • 50GB minimum • 2TB recommended • At least 1 network interface card (NIC)

TREND MICRO

TDS 威脅預警解決三大价值

了解网路内容的安全性与使用性,让关键的服务可以拥有较多的资源,大大提高网络流量利用率

定位准确，降低病毒查找时间与海量日志分析处理,节省人力成本

报表简单易懂,大大提高安全威胁的掌控度与操作性