大数据网络安全可视化设计

系统架构部　　UCD-康向荣

NSFOCUS

一、背景与现状

二、可视化的设计与分析

三、可视化的发展趋势

安全数据的大数据化

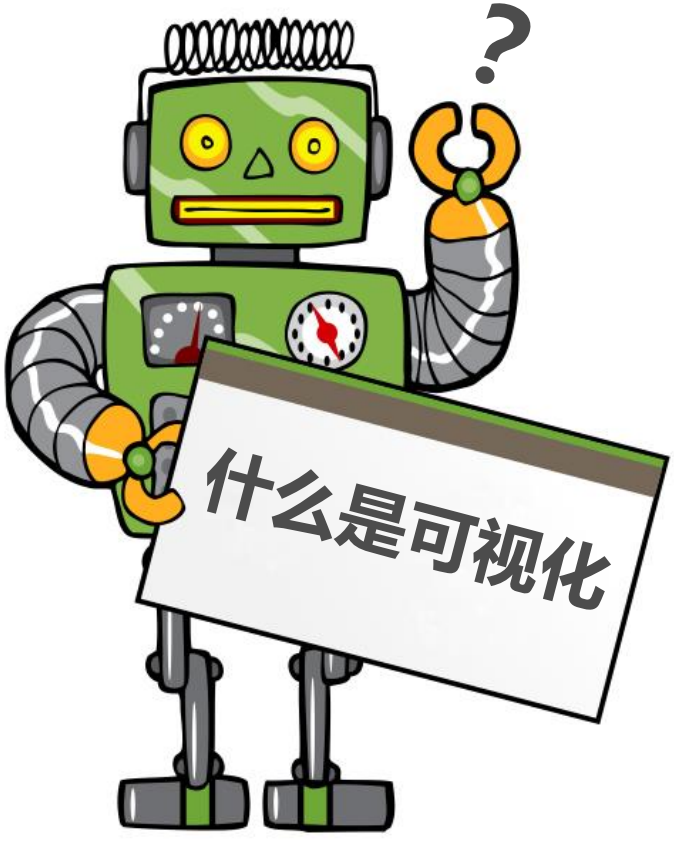

GENERATION
DEFENDING
MODEL
VULNERABILITY
SOLUTIONS
PRACTICAL
BEHAVIOR
CYBERSECURITY
FRAMEWORK
ORGANIZATION
IMPROVING
TRUST
STUDY
LESSONS
PROGRAM
SERVICES
DEVELOPMENT
RESPONSE
CYBER
MALWARE
MAKING
PASSWORDS
INFORMATION
BUSINESS
INCIDENT
SYSTEMS
MACHINE
COMPLIANCE
ATTACKS
COMPANY
DEVICE
BASED
INTELLIGENCE
NETWORK
SOFTWARE
DETECTION
APPLICATION
PREVENTING
SOCIAL
APPROACH
HACKING
TECHNOLOGY
RISK
CLOUD
APPS
CASE
INSIDER
THREAT
DIGITAL
BIG
INDUSTRY
MOBILE
INNOVATION
NEW
TRANSFORMING
USING
MANAGEMENT
DATA
EFFECTIVE
LEVERAGING
COMPROMISED
ENTERPRISE
WORLD
ENVIRONMENT
INFRASTRUCTURE
BUILDING
PROTECTING
THINGS
DEFENSE
CONTROL
FUTURE
TESTING
ENGINEERING
CRITICAL
AUTHENTICATION
BREACH
ANALYSIS
AWARENESS
GOVERNMENT
INTERNET
IDENTITY
ARCHITECTURE
STANDARDS
ADVANCED
HACKERS
AUTOMATION
SHARING
ANALYTICS
PRIVACY
LEARNING
ACCESS
ENCRYPTION
IMPLEMENTING
UNDERSTANDING
OPERATIONS
STRATEGY
MITIGATION
COMMUNICATING

海量、高速、多变的信息资产，

需要对它进行经济的、创新性的**信息处理**

从而获得超越以往的洞察力、决策支持能力和处理的自动化。

——Gartner


?
什么是可视化

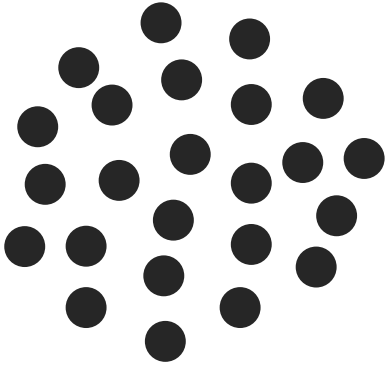
网络威胁可视化


FireEye
Subscribe to FireEye Alerts
[X] NEW ATTACK: FROM [BULGARIA] TO [PERU]
[X] NEW ATTACK: FROM [ALGERIA] TO [SAUDI ARABIA]
[X] NEW ATTACK: FROM [UNITED STATES] TO [TURKEY]
FIREEYE CYBER THREAT MAP
LOCAL TIME
11:01:29
ATTACKS TODAY
16,702
APT
UNITED STATES
Backdoor.APT.Feritdet
NETHERLANDS
PORTUGAL
ALGERIA
BULGARIA
TURKEY
INDIA
ATTACKERS
TOP COUNTRIES
(PAST 30 DAYS)
TARGETS
TOP COUNTRIES
(PAST 30 DAYS)
Powered by FireEye Labs
TOP 5 REPORTED INDUSTRIES [PAST 30 DAYS]
EDUCATION
GOVERNMENT: FEDERAL
ENERGY/UTILITIES
MANUFACTURING
HIGH-TECH
The "FireEye Cyber Threat Map" is based on a subset of real attack data, which is optimized for better visual presentation. Customer information has been removed for privacy.

信任圈可视化

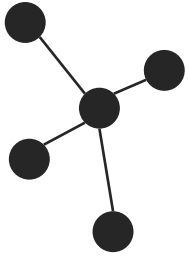
● 相互关注的人　● 你关注的人　● 关注你的人

可视化的三种视角



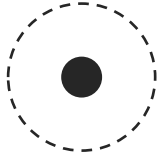
宏观视角

（模式）



关联视角

（联系）



微观视角

（单个节点）

可视化有哪些好处？

- **易感知**

  使人们更容易感知网络数据信息，且每次感知更多信息

- **识别风险快**

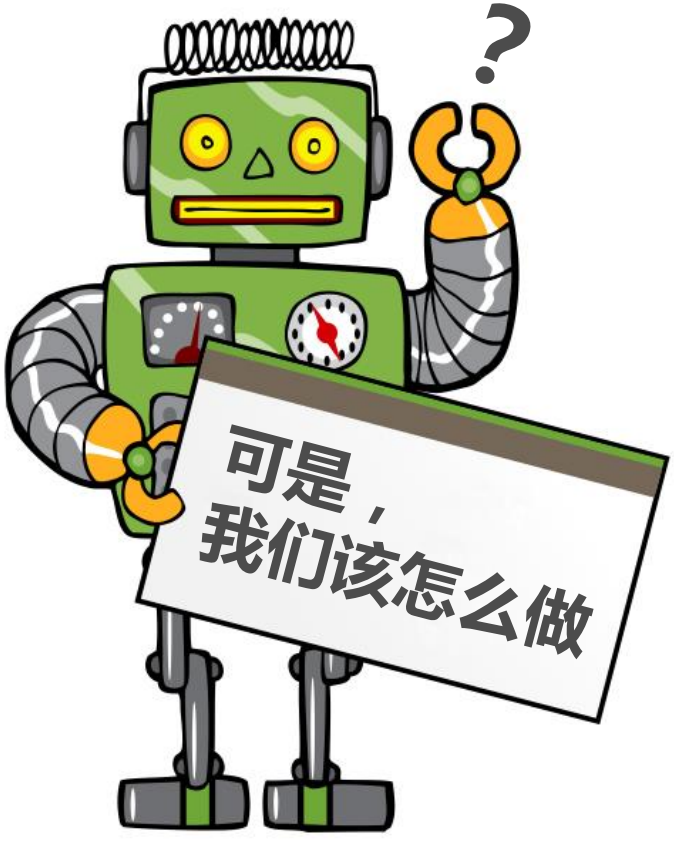
  快速识别数据模式和数据差异、发现数据的异常值或错误

- **易分类**

  识别聚类，便于对网络入侵事件进行分类

- **可预测**

  能从中发现新的攻击模式，做到提前防御，对攻击趋势做出预测


?
可是，
我们该怎么做

NSFOCUS

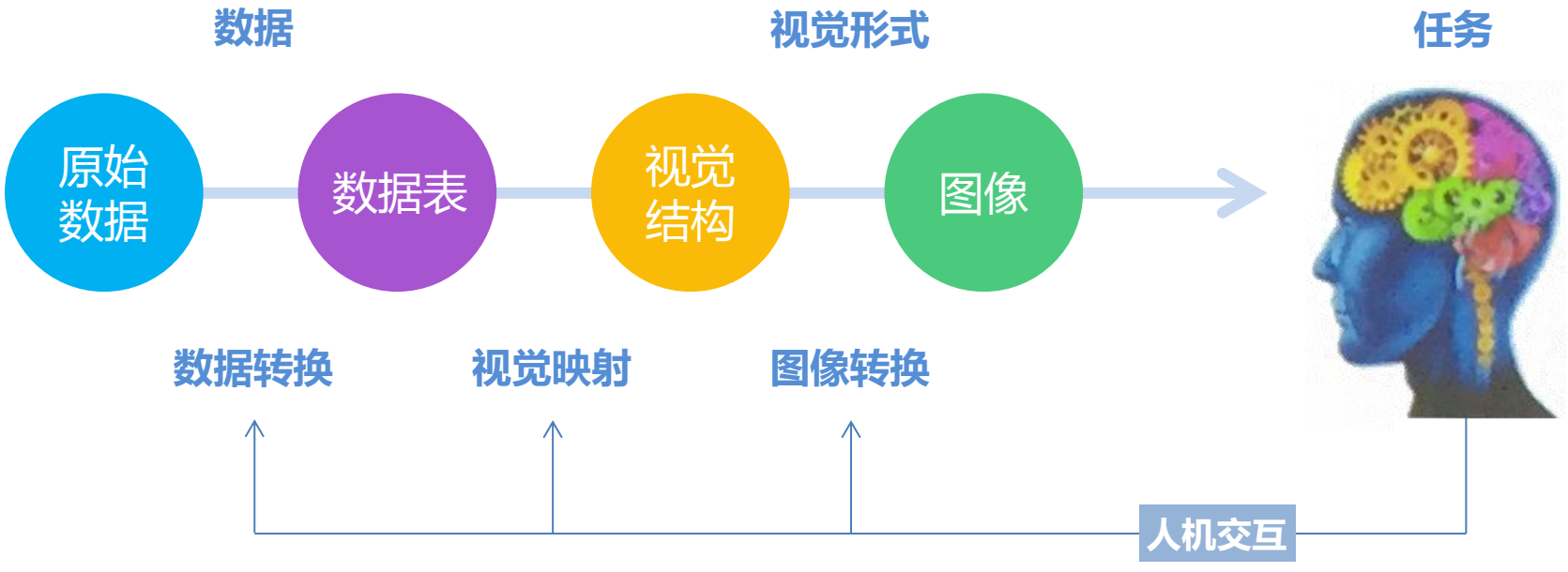
一、背景与现状

二、可视化的设计与分析

三、可视化的发展趋势

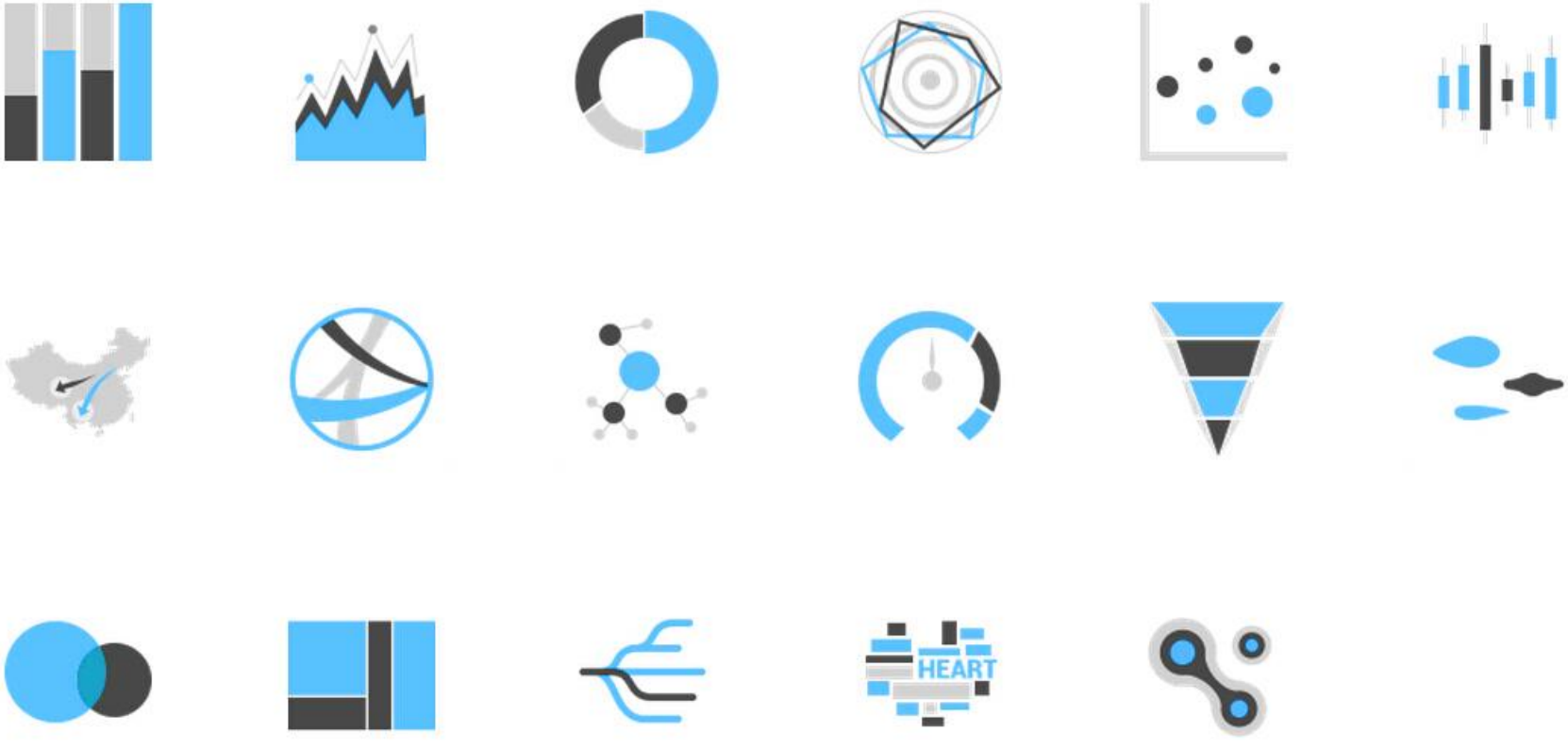
讲一个故事

找到数据和处理数据



可视化参考模型

选择可视化方式




故事
+
数据
+
设计
=
数据
可视化

7

一起来数数

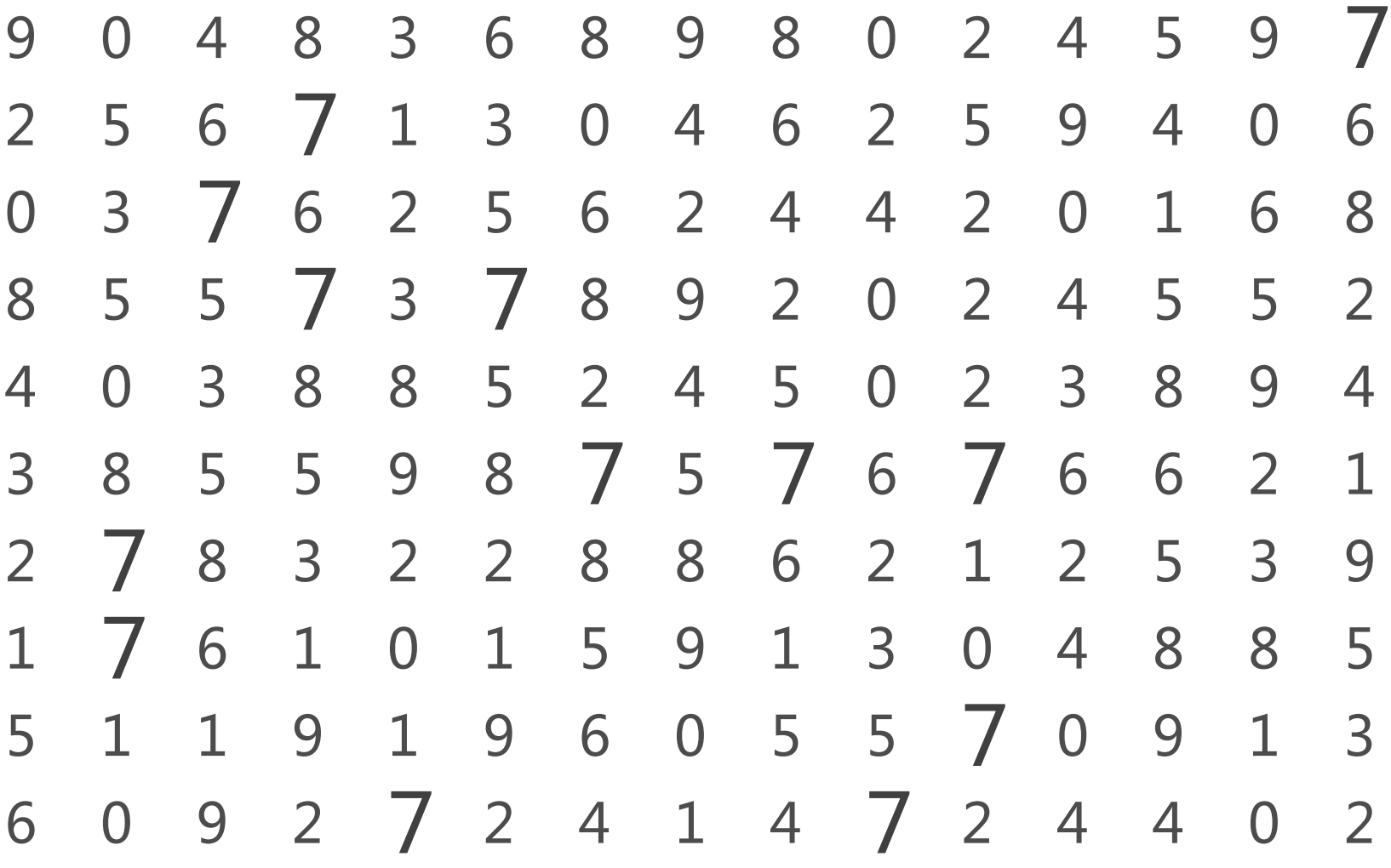
9	0	4	8	3	6	8	9	8	0	2	4	5	9	7
2	5	6	7	1	3	0	4	6	2	5	9	4	0	6
0	3	7	6	2	5	6	2	4	4	2	0	1	6	8
8	5	5	7	3	7	8	9	2	0	2	4	5	5	2
4	0	3	8	8	5	2	4	5	0	2	3	8	9	4
3	8	5	5	9	8	7	5	7	6	7	6	6	2	1
2	7	8	3	2	2	8	8	6	2	1	2	5	3	9
1	7	6	1	0	1	5	9	1	3	0	4	8	8	5
5	1	1	9	1	9	6	0	5	5	7	0	9	1	3
6	0	9	2	7	2	4	1	4	7	2	4	4	0	2

NSFOCUS

9 0 4 8 3 6 8 9 8 0 2 4 5 9 7
2 5 6 7 1 3 0 4 6 2 5 9 4 0 6
0 3 7 6 2 5 6 2 4 4 2 0 1 6 8
8 5 5 7 3 7 8 9 2 0 2 4 5 5 2
4 0 3 8 8 5 2 4 5 0 2 3 8 9 4
3 8 5 5 9 8 7 5 7 6 7 6 6 2 1
2 7 8 3 2 2 8 8 6 2 1 2 5 3 9
1 7 6 1 0 1 5 9 1 3 0 4 8 8 5
5 1 1 9 1 9 6 0 5 5 7 0 9 1 3
6 0 9 2 7 2 4 1 4 7 2 4 4 0 2

NSFOCUS

9	0	4	8	3	6	8	9	8	0	2	4	5	9	7
2	5	6	7	1	3	0	4	6	2	5	9	4	0	6
0	3	7	6	2	5	6	2	4	4	2	0	1	6	8
8	5	5	7	3	7	8	9	2	0	2	4	5	5	2
4	0	3	8	8	5	2	4	5	0	2	3	8	9	4
3	8	5	5	9	8	7	5	7	6	7	6	6	2	1
2	7	8	3	2	2	8	8	6	2	1	2	5	3	9
1	7	6	1	0	1	5	9	1	3	0	4	8	8	5
5	1	1	9	1	9	6	0	5	5	7	0	9	1	3
6	0	9	2	7	2	4	1	4	7	2	4	4	0	2


9 0 4 8 3 6 8 9 8 0 2 4 5 9 7
2 5 6 7 1 3 0 4 6 2 5 9 4 0 6
0 3 7 6 2 5 6 2 4 4 2 0 1 6 8
8 5 5 7 3 7 8 9 2 0 2 4 5 5 2
4 0 3 8 8 5 2 4 5 0 2 3 8 9 4
3 8 5 5 9 8 7 5 7 6 7 6 6 2 1
2 7 8 3 2 2 8 8 6 2 1 2 5 3 9
1 7 6 1 0 1 5 9 1 3 0 4 8 8 5
5 1 1 9 1 9 6 0 5 5 7 0 9 1 3
6 0 9 2 7 2 4 1 4 7 2 4 4 0 2

9	0	4	8	3	6	8	9	8	0	2	4	5	9	[7]
2	5	6	[7]	1	3	0	4	6	2	5	9	4	0	6
0	3	[7]	6	2	5	6	2	4	4	2	0	1	6	8
8	5	5	[7]	3	[7]	8	9	2	0	2	4	5	5	2
4	0	3	8	8	5	2	4	5	0	2	3	8	9	4
3	8	5	5	9	8	[7]	5	[7]	6	[7]	6	6	2	1
2	[7]	8	3	2	2	8	8	6	2	1	2	5	3	9
1	[7]	6	1	0	1	5	9	1	3	0	4	8	8	5
5	1	1	9	1	9	6	0	5	5	[7]	0	9	1	3
6	0	9	2	[7]	2	4	1	4	[7]	2	4	4	0	2

9	0	4	8	3	6	8	9	8	0	2	4	5	9	7
2	5	6	7	1	3	0	4	6	2	5	9	4	0	6
0	3	7	6	2	5	6	2	4	4	2	0	1	6	8
8	5	5	7	3	7	8	9	2	0	2	4	5	5	2
4	0	3	8	8	5	2	4	5	0	2	3	8	9	4
3	8	5	5	9	8	7	5	7	6	7	6	6	2	1
2	7	8	3	2	2	8	8	6	2	1	2	5	3	9
1	7	6	1	0	1	5	9	1	3	0	4	8	8	5
5	1	1	9	1	9	6	0	5	5	7	0	9	1	3
6	0	9	2	7	2	4	1	4	7	2	4	4	0	2

NSFOCUS

9	0	4	8	3	6	8	9	8	0	2	4	5	9	7
2	5	6	7	1	3	0	4	6	2	5	9	4	0	6
0	3	7	6	2	5	6	2	4	4	2	0	1	6	8
8	5	5	7	3	7	8	9	2	0	2	4	5	5	2
4	0	3	8	8	5	2	4	5	0	2	3	8	9	4
3	8	5	5	9	8	7	5	7	6	7	6	6	2	1
2	7	8	3	2	2	8	8	6	2	1	2	5	3	9
1	7	6	1	0	1	5	9	1	3	0	4	8	8	5
5	1	1	9	1	9	6	0	5	5	7	0	9	1	3
6	0	9	2	7	2	4	1	4	7	2	4	4	0	2

9	0	4	8	3	6	8	9	8	0	2	4	5	9	7
2	5	6	7	1	3	0	4	6	2	5	9	4	0	6
0	3	7	6	2	5	6	2	4	4	2	0	1	6	8
8	5	5	7	3	7	8	9	2	0	2	4	5	5	2
4	0	3	8	8	5	2	4	5	0	2	3	8	9	4
3	8	5	5	9	8	7	5	7	6	7	6	6	2	1
2	7	8	3	2	2	8	8	6	2	1	2	5	3	9
1	7	6	1	0	1	5	9	1	3	0	4	8	8	5
5	1	1	9	1	9	6	0	5	5	7	0	9	1	3
6	0	9	2	7	2	4	1	4	7	2	4	4	0	2

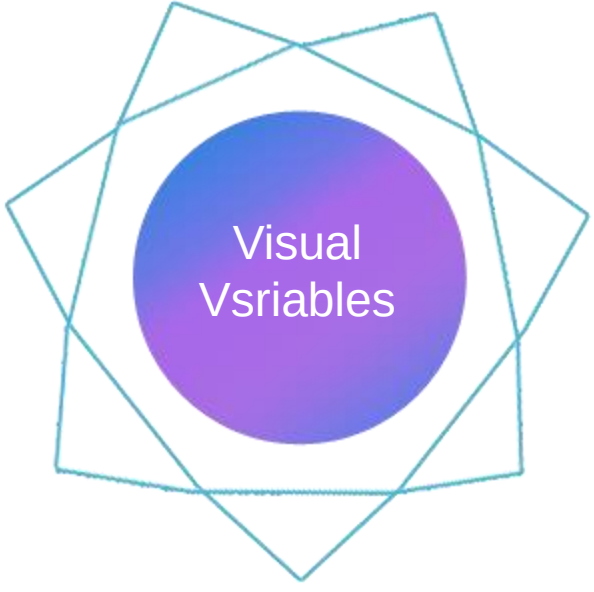
7	7	4	8	3	6	8	9	8	0	2	4	5	9	9
7	7	6	0	1	3	0	4	6	2	5	9	4	0	6
7	7	8	6	2	5	6	2	4	4	2	0	1	6	8
7	5	5	1	3	4	8	9	2	0	2	4	5	5	2
7	0	3	8	8	5	2	4	5	0	2	3	8	9	4
7	8	5	5	9	8	4	5	8	6	4	6	6	2	1
7	0	8	3	2	2	8	8	6	2	1	2	5	3	9
7	2	6	1	0	1	5	9	1	3	0	4	8	8	5
7	1	1	9	1	9	6	0	5	5	3	0	9	1	3
7	0	9	2	2	2	4	1	4	1	2	4	4	0	2

视觉可视化构成元素

形状
Shape

位置
Position

尺寸
Size



值
Value

方向
Orientation

色彩
Color

纹理
Texture

可视化的设计流程

案例一：XX办大屏幕数据可视化设计

需求：查看全国范围内，各个行业的漏洞分布和趋势

2.1 漏洞概况

漏洞类别：高危险[28] 中危险[57] 低风险[47]

端口	协议	服务	漏洞
--	ICMP	--	ICMP timestamp请求响应漏洞 允许Traceroute探测
53	UDP	dns	远端DNS服务允许递归查询
53	TCP	dns	检测到远端DNS服务正在运行中
135	TCP	msrpc	DCE/RPC服务枚举漏洞
137	UDP	netbios-ns	可通过NetBIOS名字服务端口远程获取系统信息
445	TCP	smb	Microsoft Windows SMB2报文协商越界内存引用漏洞(MS09-050)【原理扫描】 可通过空会话访问远程主机 可以获取远端Native Lan Manager版本
1521	TCP	oracle-tns	Oracle Database "CTXSYS.DRVDISP"本地权限提升漏洞 Oracle Database Server远程Core RDBMS漏洞(CVE-2011-2230) Oracle Database Enterprise Manager的Database Control组件未明影响和远程攻击漏洞（CVE-2007-5530） Oracle Database Core RDBMS组件type 6数据包拒绝服务攻击漏洞 Oracle Database Server Spatial组件远程安全漏洞(CVE-2012-3220) Oracle Enterprise Manager Grid Control HTTP请求远程溢出漏洞 Oracle Database Server RDBMS远程Core RDBMS漏洞(CVE-2011-2239) Oracle 2008年4月更新修复多个安全漏洞(CVE-2008-1813) Oracle 2009年7月紧急补丁更新修复多个漏洞（CVE-2009-0987） Oracle 2008年4月更新修复多个安全漏洞（CVE-2008-1816） Oracle 2010年10月更新修复多个Oracle Database安全漏洞

[redacted]网站监测平台

危险级别 (多选) X 3

最近24小时监测漏洞数

116,466

累计客户数

1,004

累计监测网站数

3,052

漏洞平均数量：低 >0 >100 >1000 高

NSFOCUS

漏洞平均数量 | 漏洞类型统计

江西	7,010
重庆	1,855
内蒙古	1,361
福建	966
辽宁	959
北京	902
山东	855
青海	745
江苏	584
上海	450

漏洞事件数量变化趋势

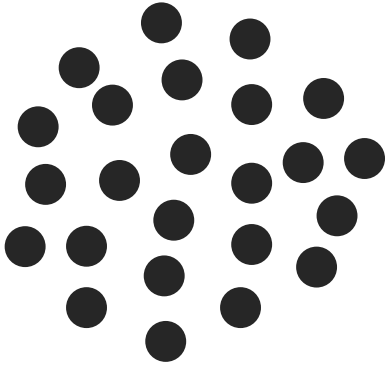
行业 全国

1. 分析数据

元 数 据：漏洞事件

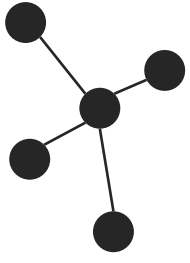
维　　度：地理位置、数量、时间、类别、级别

查看视角：



宏观视角

（模式）



关联视角

（联系）

形状
Shape

色彩
Color

尺寸
Size

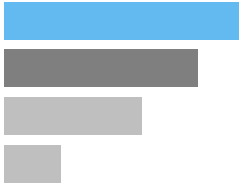
位置
Position

方向
Orientation

2. 匹配图形

地图

分布



TOP

453,123

数字

趋势图

3. 确定风格——大屏幕特点

深色背景

空间局限

宽大

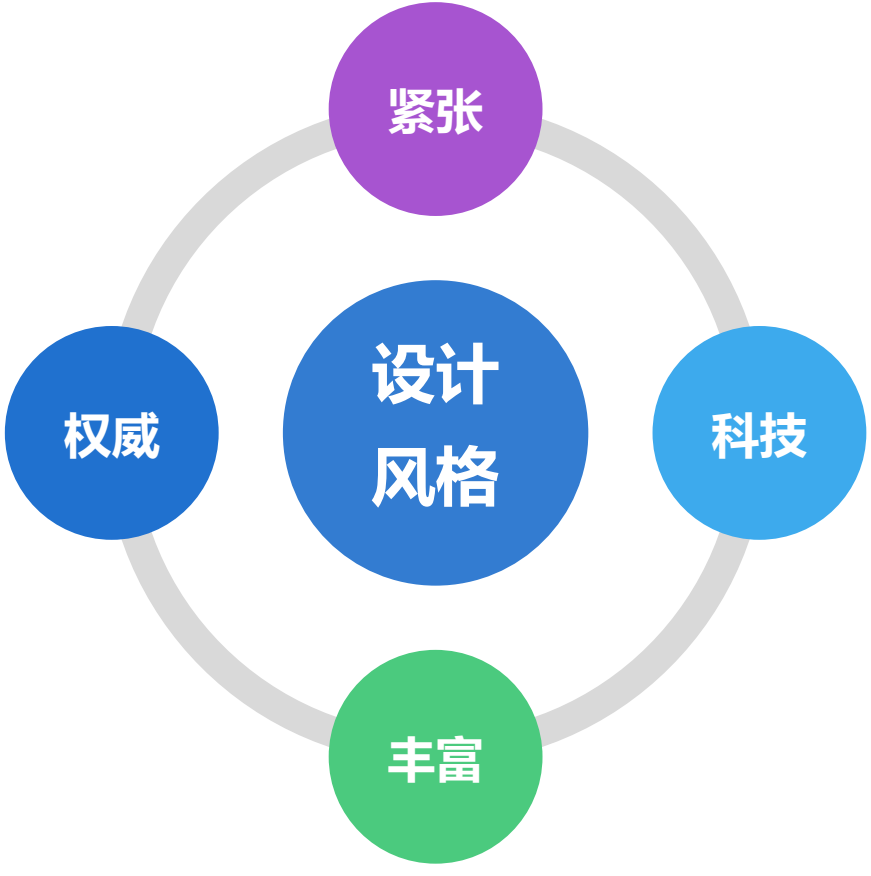
面积巨大

不可操作

空间局限

单独主题

3. 确定风格



1、色彩定位

标准色

辅助色

2、视觉风格：扁平化

4. 优化图形

- 深底，高亮的地图，多颜色的攻击动画特效，适合大屏上快速吸引人眼球及紧张感强烈；
- 红、黄、蓝呈现高、中、低危的漏洞数量分布情况；
- “Z”字型的视觉呈现，简洁清晰，重点突出。

1、维度表现

每个维度，只用一种表现，清晰易懂

2、动效设计

时间的把握和情感的控制

3、数量控制

考虑页面最后出现的时候太密或太疏时用户的感受


NSFOCUS
危险级别
(多选) X 3
最近24小时监测漏洞数
56,625
累计客户数
1,017
累计监测网站数
3,683
漏洞平均数量
漏洞类型统计
重庆 2,994
江西 2,182
内蒙古 1,892
安徽 1,879
山东 1,040
福建 981
青海 727
北京 473
天津 412
辽宁 363
漏洞平均数量：低 >0 >100 >1000 高
漏洞平均数量变化趋势
行业 全国
3k
2k
1k
0k
2015-04-26
2015-05-03
2015-05-10
2015-05-17
2015-05-24
2015-05-31
2015-06-07
2015-06-14
2015-06-21
2015-06-28
2015-07-05
2015-07-12
全国 金融 政府 能源 运营商 教育 医疗 国际 互联网 其他

5. 检查测试

- **Review需求**

  过一遍需求是不是能够满足

- **实地测试**

  将效果放上大屏，看是否方便阅读，动效是否达到预期，色差是否能接受

- **可用性测试**

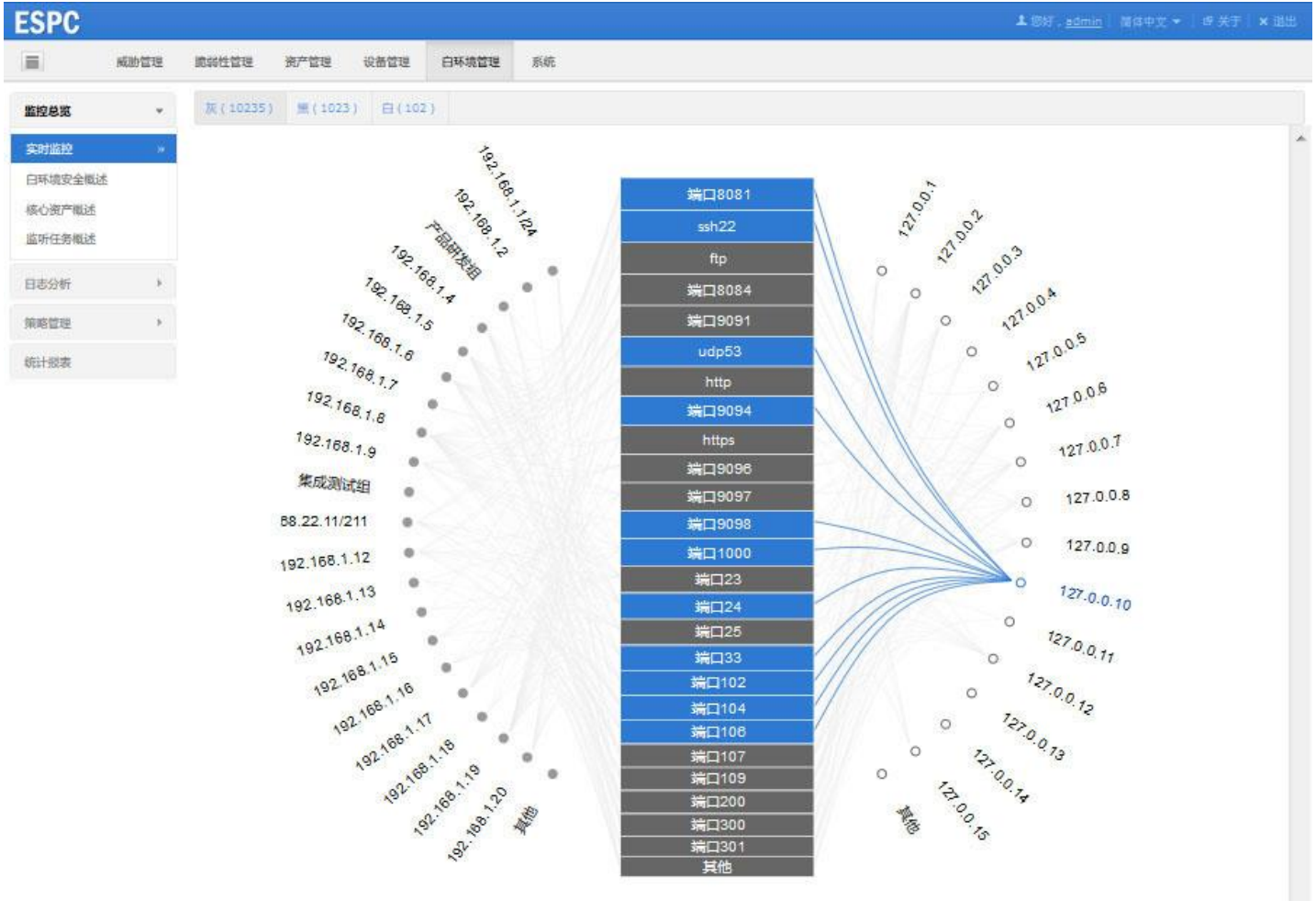
  能否一句话描述大屏，同时用户能够理解

案例二：白环境可视化设计

需求：业务内部的流向梳理清楚

时间	源		目的		事件名称	次数	事件源	操作
2012-06-13 09:06:30	信息管理部	李	人力资源	刘	违反白环境--信息管理部访问财务部	1	IPS事件	
2012-06-13 09:05:30	信息管理部	李	研发一部	张	SQL注入攻击	15	WAF事件	
2012-06-13 08:44:30	研发三部	张	人力资源	马	通过HTTP协议下载可执行文件	3	IPS事件	
2012-06-13 08:40:30	产品管理中心	李	财务部	王	盗链行为	4	WAF事件	
2012-06-13 08:30:30	国际拓展部	丁	人力资源	刘	Web常规攻击	49	IPS事件	
2012-06-13 09:05:30	人力资源	刘	产品管理中心	张	违反白环境-信息管理部访问财务部	98	WAF事件	
2012-06-13 08:44:30	研发一部	张	人力资源	马	SQL注入攻击	60	IPS事件	
2012-06-13 08:40:30	人力资源	马	财务部	王	通过HTTP协议下载可执行文件	55	WAF事件	
2012-06-13 08:30:30	财务部	王	研发三部	李	盗链行为	49	IPS事件	
2012-06-13 08:40:30	研发三部	李	财务部	王	Web常规攻击	55	WAF事件	
2012-06-13 09:06:30	信息管理部	李	人力资源	刘	违反白环境--信息管理部访问财务部	1	IPS事件	
2012-06-13 09:05:30	信息管理部	李	研发一部	张	SQL注入攻击	15	WAF事件	
2012-06-13 08:44:30	研发三部	张	人力资源	马	通过HTTP协议下载可执行文件	3	IPS事件	
2012-06-13 08:40:30	产品管理中心	李	财务部	王	盗链行为	4	WAF事件	
2012-06-13 08:30:30	国际拓展部	丁	人力资源	刘	Web常规攻击	49	IPS事件	
2012-06-13 09:05:30	人力资源	刘	产品管理中心	张	违反白环境-信息管理部访问财务部	98	WAF事件	
2012-06-13 08:44:30	研发一部	张	人力资源	马	SQL注入攻击	60	IPS事件	
2012-06-13 08:40:30	人力资源	马	财务部	王	通过HTTP协议下载可执行文件	55	WAF事件	
2012-06-13 08:30:30	财务部	王	研发三部	李	盗链行为	49	IPS事件	
2012-06-13 08:40:30	研发三部	李	财务部	王	Web常规攻击	55	WAF事件	
2012-06-13 09:06:30	信息管理部	李	人力资源	刘	违反白环境--信息管理部访问财务部	1	IPS事件	
2012-06-13 09:05:30	信息管理部	李	研发一部	张	SQL注入攻击	15	WAF事件	
2012-06-13 08:44:30	研发三部	张	人力资源	马	通过HTTP协议下载可执行文件	3	IPS事件	
2012-06-13 08:40:30	产品管理中心	李	财务部	王	盗链行为	4	WAF事件	
2012-06-13 08:30:30	国际拓展部	丁	人力资源	刘	Web常规攻击	49	IPS事件	
2012-06-13 09:05:30	人力资源	刘	产品管理中心	张	违反白环境-信息管理部访问财务部	98	WAF事件	
2012-06-13 08:44:30	研发一部	张	人力资源	马	SQL注入攻击	60	IPS事件	
2012-06-13 08:40:30	人力资源	马	财务部	王	通过HTTP协议下载可执行文件	55	WAF事件	
2012-06-13 08:30:30	财务部	王	研发三部	李	盗链行为	49	IPS事件	
2012-06-13 08:40:30	研发三部	李	财务部	王	Web常规攻击	55	WAF事件	

案例二：白环境可视化设计

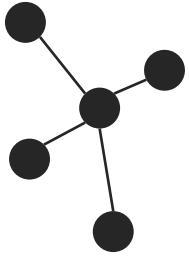


1. 分析数据

元 数 据：事件

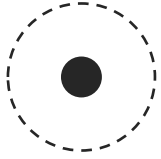
维　　度：时间、源IP、目的IP、应用

查看视角：



关联视角

（联系）

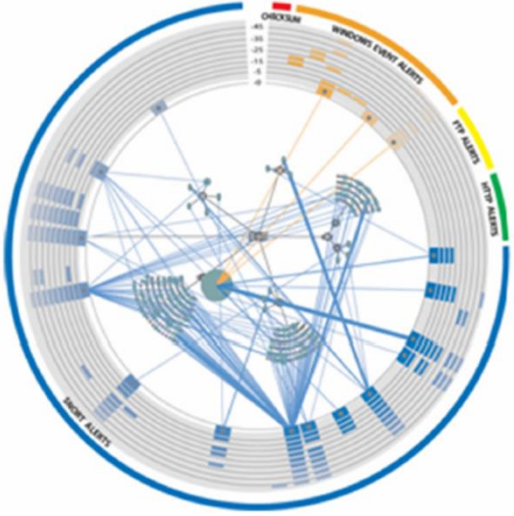


微观视角

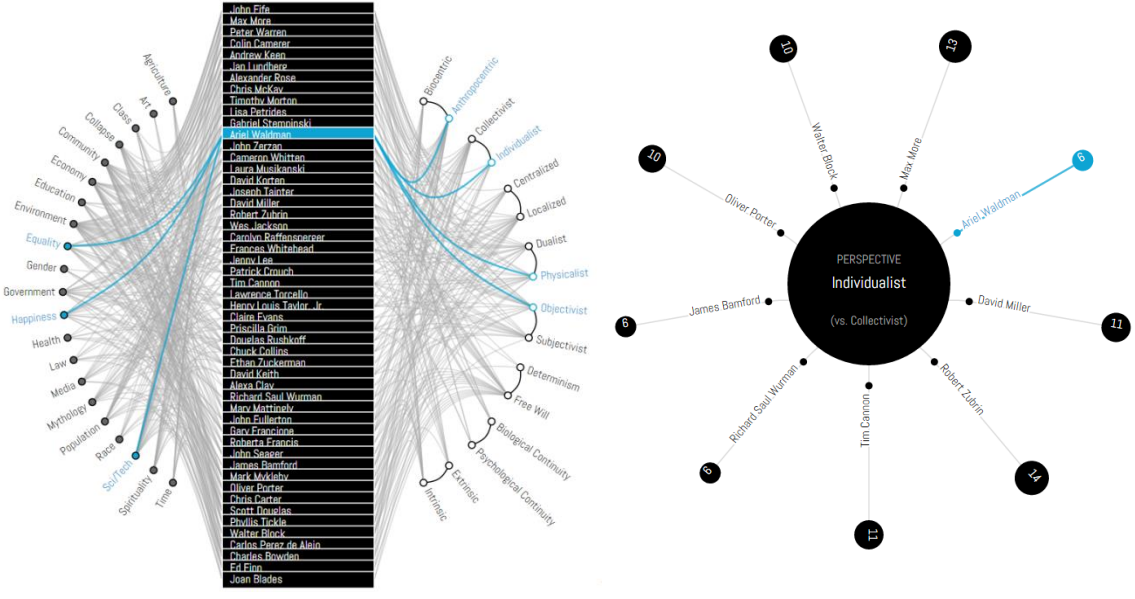
（单个节点）

2. 匹配图形

和弦图



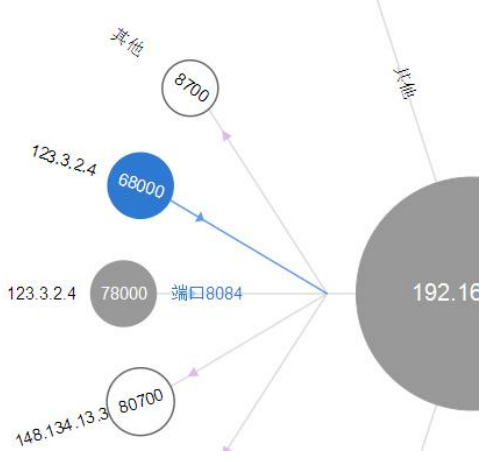
力导向布局图

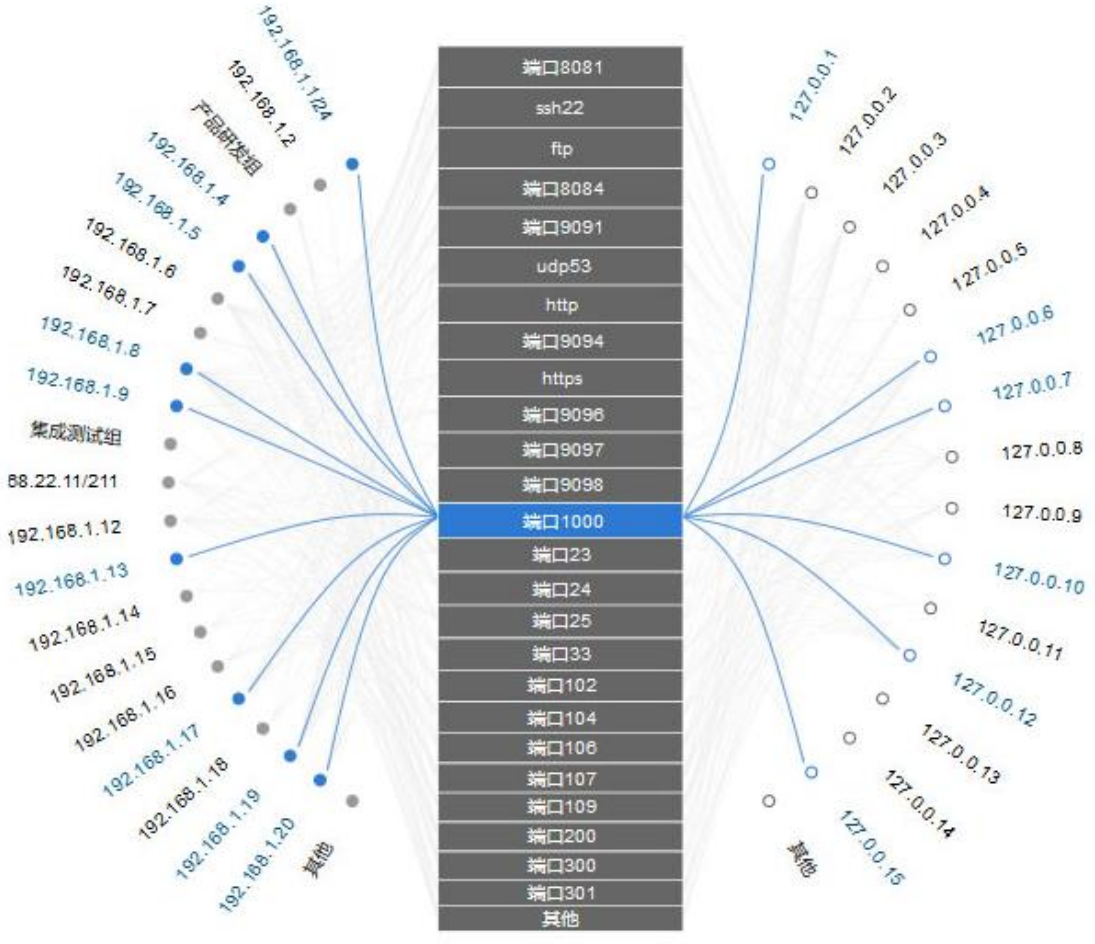


3. 优化图形

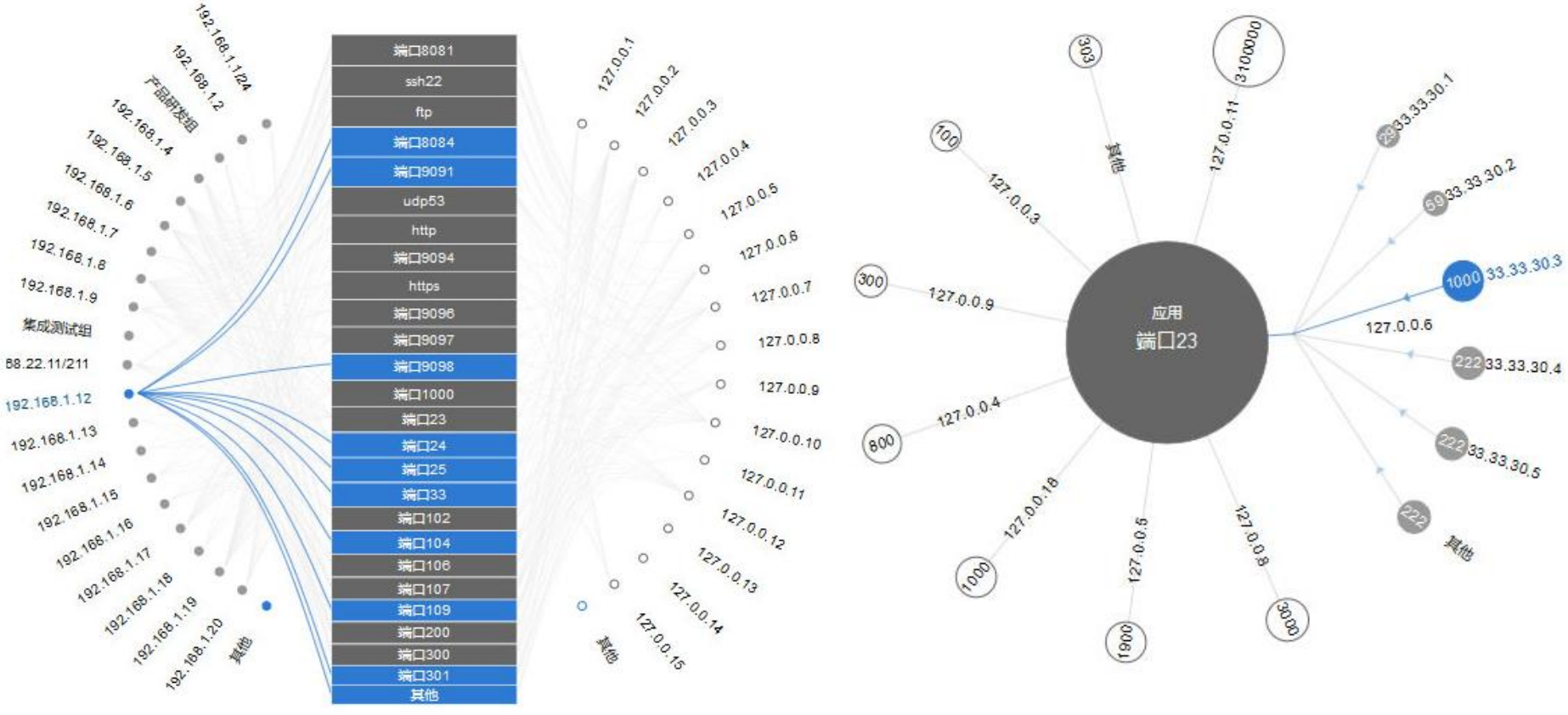
我们改过的细节：

- 太密或太疏时用户的感受，取TOP N
- 弧度、标准色的优化
- IP名称超长的处理
- 微观视角中，源和目的分别以蓝色和紫色区分，同时在线上加上箭头，方便理解





4. 检查测试


192.168.1.124
192.168.1.2
产品研发组
192.168.1.4
192.168.1.5
192.168.1.6
192.168.1.7
192.168.1.8
192.168.1.9
集成测试组
88.22.11/211
192.168.1.12
192.168.1.13
192.168.1.14
192.168.1.15
192.168.1.16
192.168.1.17
192.168.1.18
192.168.1.19
192.168.1.20
其他
端口8081
ssh22
ftp
端口8084
端口9091
udp53
http
端口9094
https
端口9096
端口9097
端口9098
端口1000
端口23
端口24
端口25
端口33
端口102
端口104
端口106
端口107
端口109
端口200
端口300
端口301
其他
127.0.0.1
127.0.0.2
127.0.0.3
127.0.0.4
127.0.0.5
127.0.0.6
127.0.0.7
127.0.0.8
127.0.0.9
127.0.0.10
127.0.0.11
127.0.0.12
127.0.0.13
127.0.0.14
127.0.0.15
其他
应用
端口23
303
其他
3100000
127.0.0.11
100
127.0.0.3
300
127.0.0.9
800
127.0.0.4
1000
127.0.0.18
1900
127.0.0.5
3000
127.0.0.8
127.0.0.6
1000
33.33.30.3
222
33.33.30.4
222
33.33.30.5
222
其他
59
33.33.30.2
33.33.30.1

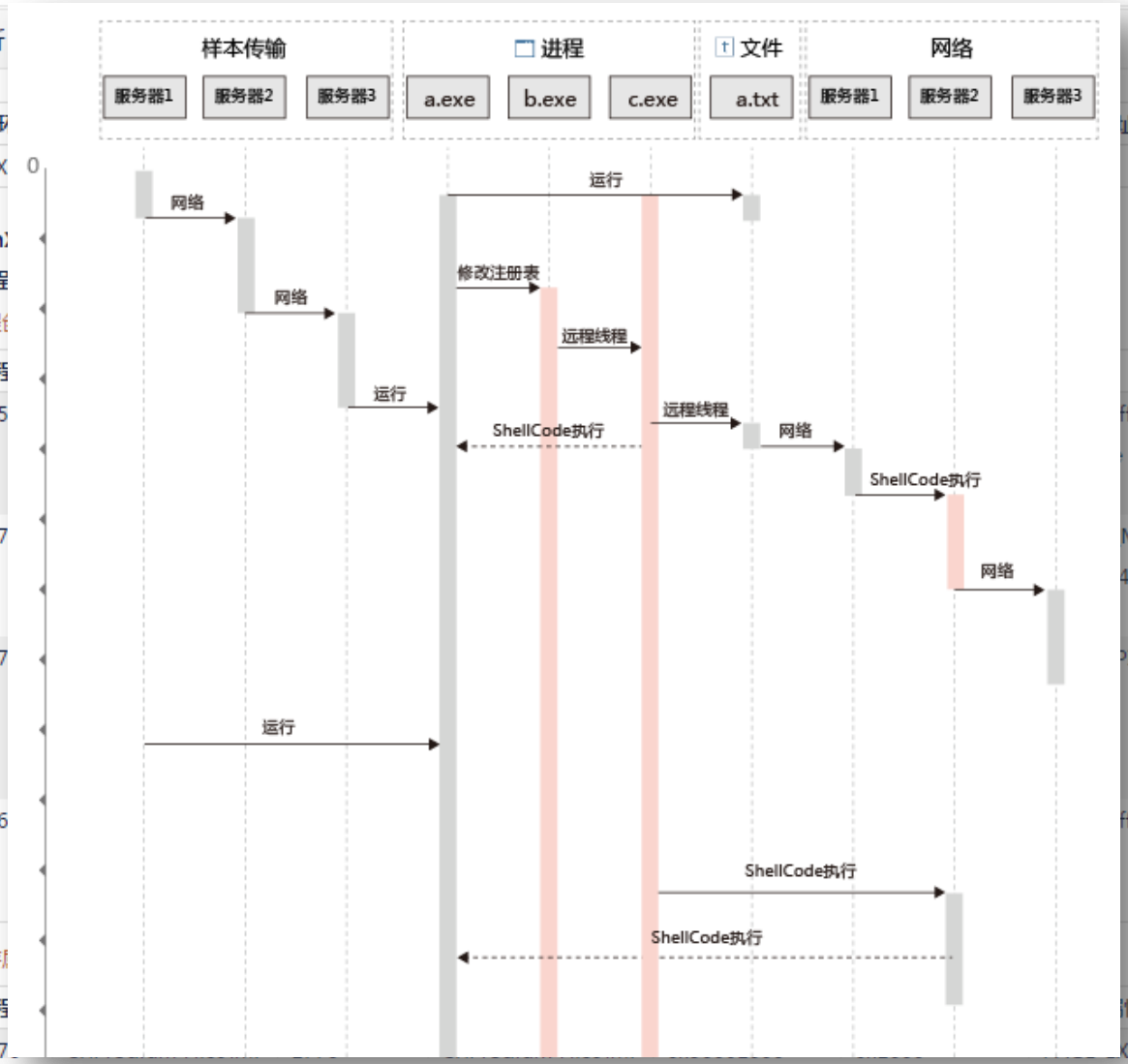
案例三：NGTP威胁可视化

全攻击链防护

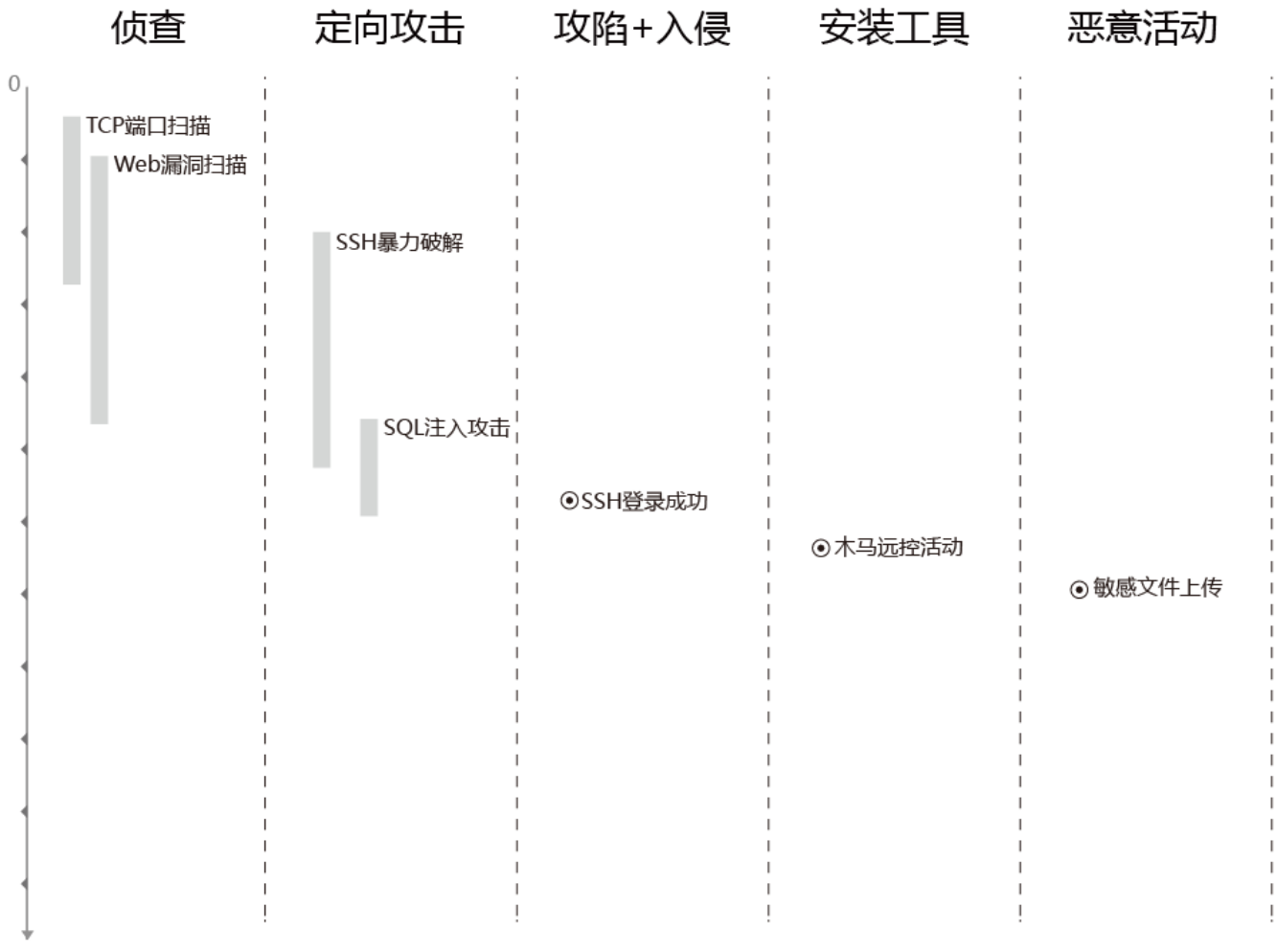
威胁可视化

Kill chain	进入	潜伏	盗取
	侦察 → 武器化 → 传输 → 利用漏洞 → 木马安装 → C & C → 目标达成		
防护方案	进不来	藏不住	带不走
	• 基于动态、静态等方式检测通过web、邮件等途径进入的各种恶意软件 • 发现挂马、钓鱼、盗链网站的访问行为，及时拦截	• 发现内网被感染主机的扫描探测行为 • 发现内网被感染主机的回连行为并及时拦截	• 敏感数据外发拦截 • 基于关联分析，回溯展现整个攻击全过程
关键组件	NGIPS+TAC+Email Gateway（3rd Party Ready）	NGIPS+TAC	NGIPS(DLP组件）

某恶意软件的行为分析可视化



全攻击链的可视化


侦查
定向攻击
攻陷+入侵
安装工具
恶意活动
0
TCP端口扫描
Web漏洞扫描
SSH暴力破解
SQL注入攻击
SSH登录成功
木马远控活动
敏感文件上传

可视化的设计流程

小结

1. 可视化设计流程
2. 案例分析

   案例一：XX办大屏幕数据可视化设计

   案例二：白环境可视化设计

   案例三：NGTP威胁可视化

注意：

整体考虑，顾全大局

注意细节的匹配、一致性

充满美感，对称、和谐

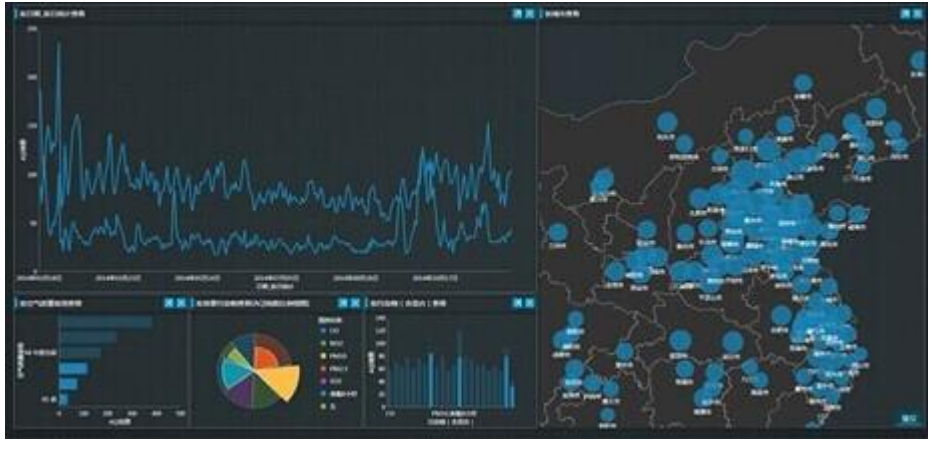
一、背景与现状

二、可视化的设计与分析

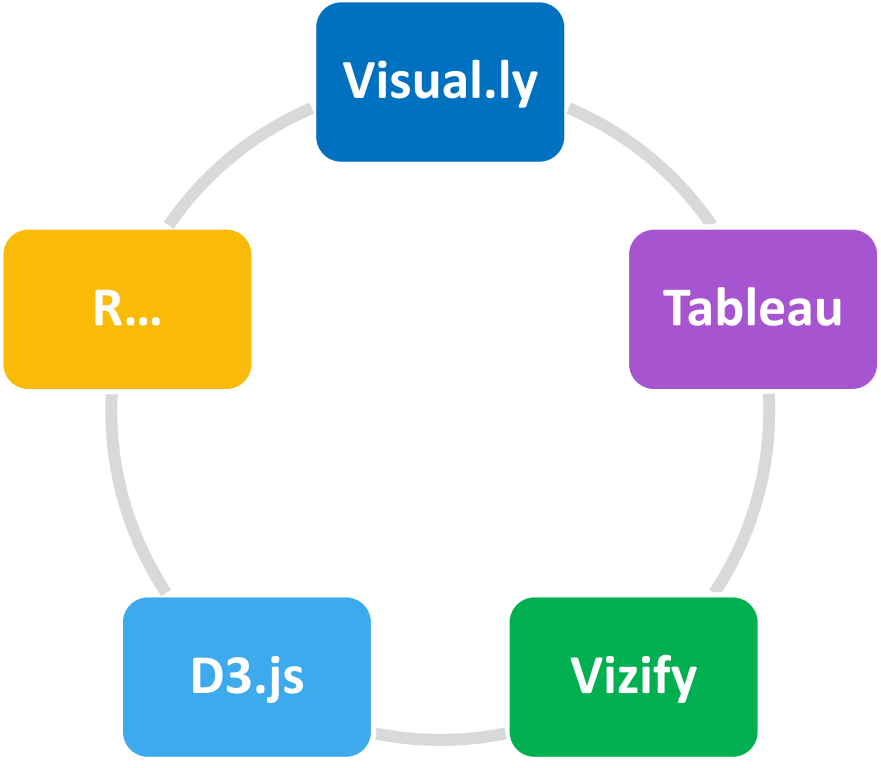
三、可视化的发展趋势

可视化的发展趋势

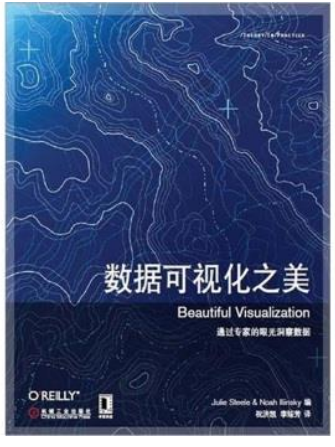
1. 实时显示、处理大规模网络数据
2. 多数据源、多视图、多人协同分析
3. 智能化，自动报警和防御



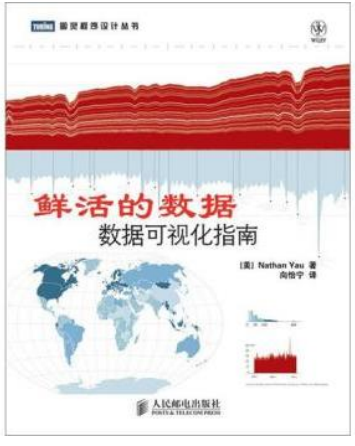
推荐几个可视化的工具



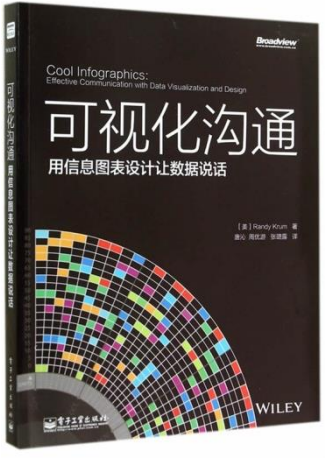
数据可视化书籍



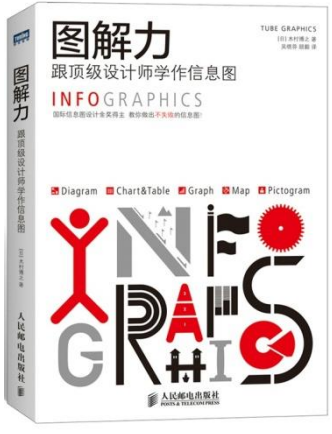
数据可视化之美



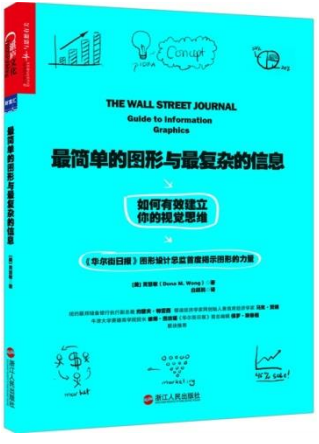
鲜活的数据



可视化沟通



图解力



最简单的图形与最复杂的信息

Q & A

NSFOCUS