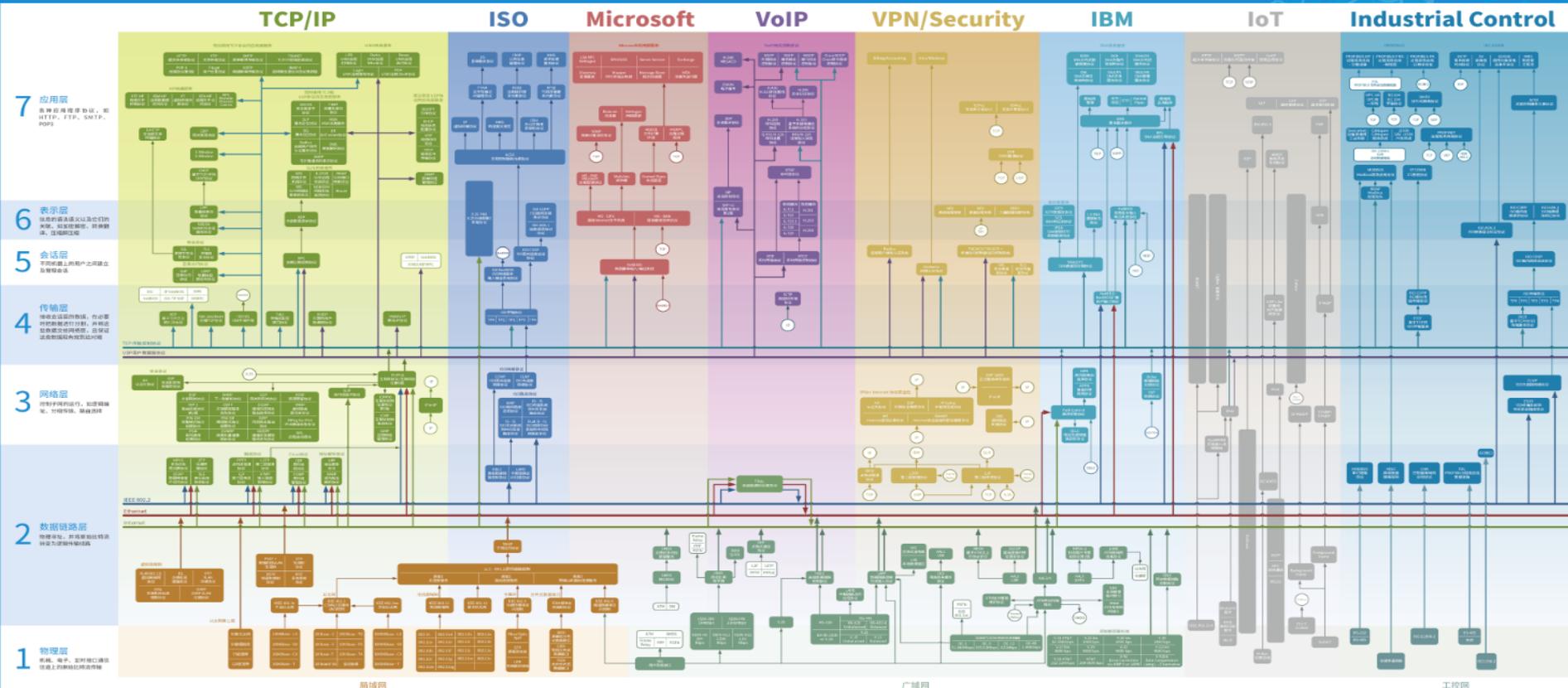




解构协议解码

李飞 成都科来软件有限公司 产品运营总监





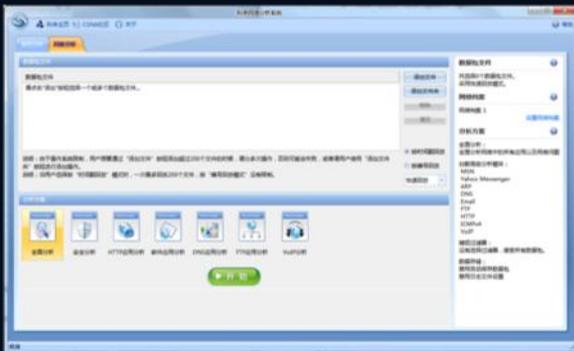
TCP/IP协议族目录一览表

应用层	表示层	会话层	传输层	网络层	数据链路层	物理层
HTTP, FTP, SMTP, POP3, Telnet, SSH, RDP, etc.	SSL, TLS, etc.	SETUP, etc.	TCP, UDP, etc.	IP, ICMP, etc.	PPP, HDLC, etc.	10BASE-T, etc.



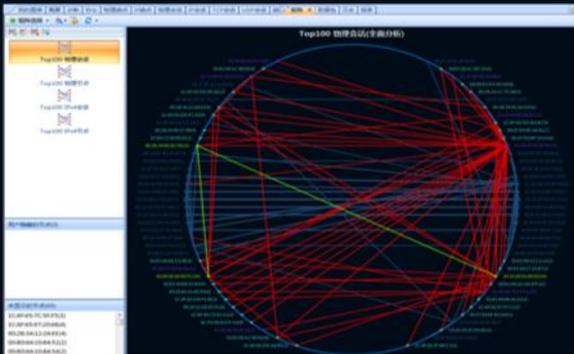


科来网络分析系统 (技术交流免费版)

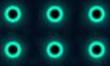


源IP	目的IP	源字节	目的字节	源包数	目的包数	源IP地址	目的IP地址
192.168.1.1	192.168.1.2	1024	1024	1	1	192.168.1.1	192.168.1.2
192.168.1.2	192.168.1.1	1024	1024	1	1	192.168.1.2	192.168.1.1
192.168.1.1	192.168.1.3	1024	1024	1	1	192.168.1.1	192.168.1.3
192.168.1.3	192.168.1.1	1024	1024	1	1	192.168.1.3	192.168.1.1
192.168.1.1	192.168.1.4	1024	1024	1	1	192.168.1.1	192.168.1.4
192.168.1.4	192.168.1.1	1024	1024	1	1	192.168.1.4	192.168.1.1
192.168.1.1	192.168.1.5	1024	1024	1	1	192.168.1.1	192.168.1.5
192.168.1.5	192.168.1.1	1024	1024	1	1	192.168.1.5	192.168.1.1
192.168.1.1	192.168.1.6	1024	1024	1	1	192.168.1.1	192.168.1.6
192.168.1.6	192.168.1.1	1024	1024	1	1	192.168.1.6	192.168.1.1
192.168.1.1	192.168.1.7	1024	1024	1	1	192.168.1.1	192.168.1.7
192.168.1.7	192.168.1.1	1024	1024	1	1	192.168.1.7	192.168.1.1
192.168.1.1	192.168.1.8	1024	1024	1	1	192.168.1.1	192.168.1.8
192.168.1.8	192.168.1.1	1024	1024	1	1	192.168.1.8	192.168.1.1
192.168.1.1	192.168.1.9	1024	1024	1	1	192.168.1.1	192.168.1.9
192.168.1.9	192.168.1.1	1024	1024	1	1	192.168.1.9	192.168.1.1
192.168.1.1	192.168.1.10	1024	1024	1	1	192.168.1.1	192.168.1.10
192.168.1.10	192.168.1.1	1024	1024	1	1	192.168.1.10	192.168.1.1

源IP	目的IP	源字节	目的字节	源包数	目的包数	源IP地址	目的IP地址
192.168.1.1	192.168.1.2	1024	1024	1	1	192.168.1.1	192.168.1.2
192.168.1.2	192.168.1.1	1024	1024	1	1	192.168.1.2	192.168.1.1
192.168.1.1	192.168.1.3	1024	1024	1	1	192.168.1.1	192.168.1.3
192.168.1.3	192.168.1.1	1024	1024	1	1	192.168.1.3	192.168.1.1
192.168.1.1	192.168.1.4	1024	1024	1	1	192.168.1.1	192.168.1.4
192.168.1.4	192.168.1.1	1024	1024	1	1	192.168.1.4	192.168.1.1
192.168.1.1	192.168.1.5	1024	1024	1	1	192.168.1.1	192.168.1.5
192.168.1.5	192.168.1.1	1024	1024	1	1	192.168.1.5	192.168.1.1
192.168.1.1	192.168.1.6	1024	1024	1	1	192.168.1.1	192.168.1.6
192.168.1.6	192.168.1.1	1024	1024	1	1	192.168.1.6	192.168.1.1
192.168.1.1	192.168.1.7	1024	1024	1	1	192.168.1.1	192.168.1.7
192.168.1.7	192.168.1.1	1024	1024	1	1	192.168.1.7	192.168.1.1
192.168.1.1	192.168.1.8	1024	1024	1	1	192.168.1.1	192.168.1.8
192.168.1.8	192.168.1.1	1024	1024	1	1	192.168.1.8	192.168.1.1
192.168.1.1	192.168.1.9	1024	1024	1	1	192.168.1.1	192.168.1.9
192.168.1.9	192.168.1.1	1024	1024	1	1	192.168.1.9	192.168.1.1
192.168.1.1	192.168.1.10	1024	1024	1	1	192.168.1.1	192.168.1.10
192.168.1.10	192.168.1.1	1024	1024	1	1	192.168.1.10	192.168.1.1



源IP	目的IP	源字节	目的字节	源包数	目的包数	源IP地址	目的IP地址
192.168.1.1	192.168.1.2	1024	1024	1	1	192.168.1.1	192.168.1.2
192.168.1.2	192.168.1.1	1024	1024	1	1	192.168.1.2	192.168.1.1
192.168.1.1	192.168.1.3	1024	1024	1	1	192.168.1.1	192.168.1.3
192.168.1.3	192.168.1.1	1024	1024	1	1	192.168.1.3	192.168.1.1
192.168.1.1	192.168.1.4	1024	1024	1	1	192.168.1.1	192.168.1.4
192.168.1.4	192.168.1.1	1024	1024	1	1	192.168.1.4	192.168.1.1
192.168.1.1	192.168.1.5	1024	1024	1	1	192.168.1.1	192.168.1.5
192.168.1.5	192.168.1.1	1024	1024	1	1	192.168.1.5	192.168.1.1
192.168.1.1	192.168.1.6	1024	1024	1	1	192.168.1.1	192.168.1.6
192.168.1.6	192.168.1.1	1024	1024	1	1	192.168.1.6	192.168.1.1
192.168.1.1	192.168.1.7	1024	1024	1	1	192.168.1.1	192.168.1.7
192.168.1.7	192.168.1.1	1024	1024	1	1	192.168.1.7	192.168.1.1
192.168.1.1	192.168.1.8	1024	1024	1	1	192.168.1.1	192.168.1.8
192.168.1.8	192.168.1.1	1024	1024	1	1	192.168.1.8	192.168.1.1
192.168.1.1	192.168.1.9	1024	1024	1	1	192.168.1.1	192.168.1.9
192.168.1.9	192.168.1.1	1024	1024	1	1	192.168.1.9	192.168.1.1
192.168.1.1	192.168.1.10	1024	1024	1	1	192.168.1.1	192.168.1.10
192.168.1.10	192.168.1.1	1024	1024	1	1	192.168.1.10	192.168.1.1





CSNA-A 《网络分析服务认证》 各种实战方法训练

CSNA-E 《网络分析体系认证》 网络分析知识体系

CSNA-S 《高级安全实战认证》 高级攻击分析为主





相关学习资源

FIIT 2019

软件下载

科来网络分析系统11.1 (技术交流免费版)

网络分析工具

科来MAC地址扫描器

科来Ping工具

科来数据包播放器

科来数据包生成器

学习资源

网络攻击与防范图谱

科来网络通讯协议图, TCP/IP网络协议图免费下载

科来网络故障诊断图

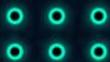
网络分析案例集

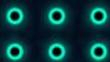
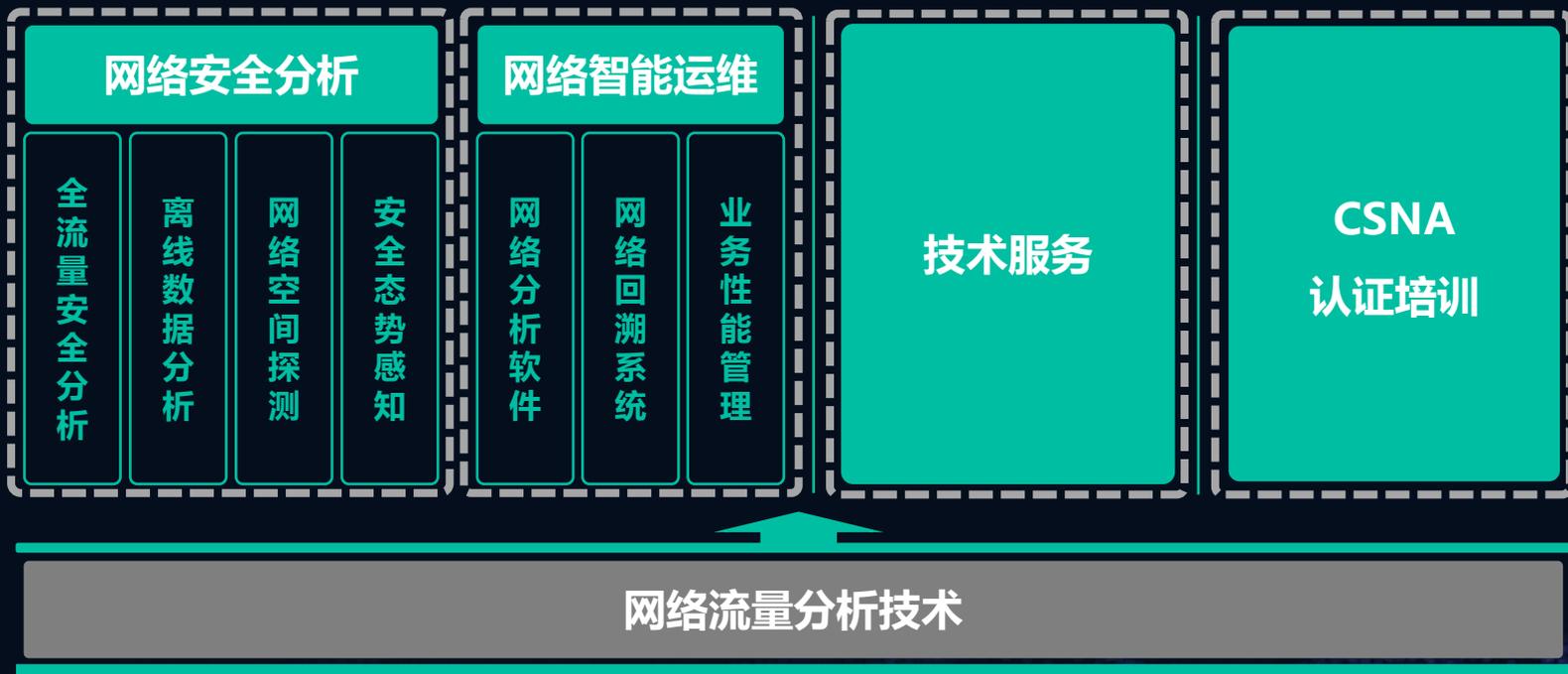
数据包样本

网络分析过滤器

网络分析技术学习资料

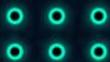
术语表







- ◆ 网络流量分析核心数据分析
- ◆ 基本的互联网通信协议都有在RFC文件内详细说明





协议解码举例

仪表盘 概要 诊断 以太网 - II 节点1-> 节点2 数据包 字节 协议 持续时间 字节->

节点1->	节点2	数据包	字节	协议	持续时间	字节->
192.168.10.138:3946	123.125.50.23:110	20	2,328 KB	POP3	0	647 B 1.6
192.168.10.138:3948	203.209.228.241:110	83	64.837 KB	POP3	1	1.827 KB 63.0
192.168.10.138:3951	203.209.228.241:110	82	64.774 KB	POP3	1	1.827 KB 62.9
192.168.10.138:3971	203.209.228.241:110	83	64.837 KB	POP3	0	1.827 KB 63.0
192.168.10.138:4013	203.209.228.241:110	82	64.774 KB	POP3	0	1.827 KB 62.9
192.168.10.138:4017	203.209.228.241:110	83	64.831 KB	POP3	0	1.884 KB 62.9
192.168.10.138:4145	203.209.228.241:110	84	64.894 KB	POP3	8	1.884 KB 63.0
192.168.10.138:4148	203.209.228.241:110	98	66.050 KB	POP3	22	2.351 KB 63.6

数据包 数据流 时序图

数据包 数据流 时序图

端点 1: IP 地址 = 192.168.10.138, TCP
端点 2: IP 地址 = 123.125.50.23, TCP

相对时间	概要	192.168.10.138: ...	
0.000000	Seq = 0, Next Seq = 1	Window = 8192	SYN →
0.173119			← SYN, ACK
0.173222	Seq = 1, Ack = 0, Next ...	Window = 68	ACK →
0.271441			← PSH, ACK, 载荷长度 = 87
0.277948	Seq = 1, Ack = 87, Nex...	Window = 67	PSH, ACK, 载荷长度 = 15 →
0.323141			← ACK
0.323317			← PSH, ACK, 载荷长度 = 15
0.335482	Seq = 16, Ack = 102, N...	Window = 67	PSH, ACK, 载荷长度 = 16 →
0.372609			← PSH, ACK, 载荷长度 = 37
0.381130	Seq = 32, Ack = 139, N...	Window = 67	PSH, ACK, 载荷长度 = 6 →

USER long_323

+OK Welcome to coremail Mail Pop3

+OK core mail

PASS [REDACTED]

+OK 26 message(s) [1203339 byte(s)]

STAT



可以输出结构化的元数据

IT 2019



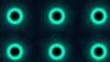
网络会话层元数据

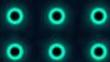
源IP、源端口、源IP国家、目的IP、目的端口、目的IP国家、协议、数据包个数、会话开始时间、会话结束时间、会话持续时间...



应用层元数据 (量巨大)

如HTTP协议，主要25个关键字段，包括user-agent、cookie、host、refer等；
如15种DNS协议字段、SMTP/POP3协议字段...







网络安全检测举例：网络窃密行为发现

2019

- ① **异常行为模型**：元数据模型：HTTP 1.1；Content-Type: image/png or jpg；Content-Length: >50MB；Or 数据交易次数>150
- ② **回溯分析**：发现HTTP头部标明传输为图片格式，但数据包头没有图片格式头部请求路径一致，每次“图片”大小不一样，每次传输超过100MB，传图片前2小时层解析过境外的服务器，并且有可疑通讯

```
GET /image/login_bt1.png HTTP/1.1
Referer: http://[redacted]com/image/
Accept: */*
Range: bytes=132645864-
User-Agent: Mozilla/4.0 (Windows 95;US) Opera 3.6
Host: mail.[redacted].com
Connection: Keep-Alive
Cache-Control: no-cache
```

```
HTTP/1.1 206 Partial Content
Content-Type: image/png
Accept-Ranges: bytes
ETag: "270443163"
Last-Modified: Thu, 03 Nov 2016 14:28:33 GMT
Content-Range: bytes 132645864-265289727/265289728
Content-Length: 132643864
Date: Fri, 04 Nov 2016 02:04:12 GMT
Server: nginx
```

```
GET /image/login_bt1.png HTTP/1.1
Referer: http://[redacted]com/image/
Accept: */*
Range: bytes=132645864-
User-Agent: Mozilla/4.0 (Windows 95;US) Opera 3.60 [en]
Host: mail.[redacted]com
Connection: Keep-Alive
Cache-Control: no-cache
```

```
HTTP/1.1 206 Partial Content
Content-Type: image/png
Accept-Ranges: bytes
ETag: "270443163"
Last-Modified: Thu, 03 Nov 2016 14:28:33 GMT
Content-Range: bytes 132645864-265289727/265289728
Content-Length: 132643864
Date: Fri, 04 Nov 2016 02:04:12 GMT
Server: nginx
```

新=椰}.编温}p.商穆0?5b錫M\?, 禱I購?\S?鸡畜筵閩廖?o鐘?鞣.%;
.豹#与錫錫賦?|?錫錫?Q(偏2穉e ..?烤.越y.部d1.8?7?鏗QL*4.
az.{} 藩-9R備n?z1?未.漫.?趁摻鴉'矮?蟻U簞7吟
f棉L? .娛.祇蟻 lq纈?.X?`关?消! y礪3B幹合p8Ep?星?饒盤椿
... ..

节点 1: IP 地址 = [redacted], TCP 端口 = 49667
节点 2: IP 地址 = 10.200.1.54, TCP 端口 = 80

```
GET /image/login_bt1.png HTTP/1.1
Referer: http://[redacted]com/image/
Accept: */*
User-Agent: Mozilla/4.0 (Windows 95;US) Opera 3.60 [en]
Host: [redacted].com
Connection: Keep-Alive
Cache-Control: no-cache
```

```
HTTP/1.1 200 OK
Content-Type: image/png
Accept-Ranges: bytes
ETag: "270443163"
Last-Modified: Thu, 03 Nov 2016 14:28:33 GMT
Content-Length: 265289728
Date: Fri, 04 Nov 2016 02:04:06 GMT
Server: nginx
```

? ? I.X .滑推騰?網環膠膠綫u?仿kmU摺<(8參.??O?w?强極[輯P站(Y
館腕_觸.筑呢錫x^a恰a^ ?0 錫.< 8半/ 嬰碼;P錫侯,濕魁.../道
f包?e ?早冷?o因蟻錫錫激攷?銳十傳i??还問[, ??伦.p錫R筵麥?訂
發?奇薩?這駝 錫l6?F彈透??.)僕 錫lv錫度?g?..rh b 3?錫 5



网络安全检测举例：用户与实体行为分析 (UEBA)

IT 2019

哪些用户访问？活跃度？

和哪些主机通信？

安全事件类型和频度



流量区间如何？

系统外联分布和频度

实体

通信协议有哪些？

IP、账号、主机

时间点

应用程序偏好

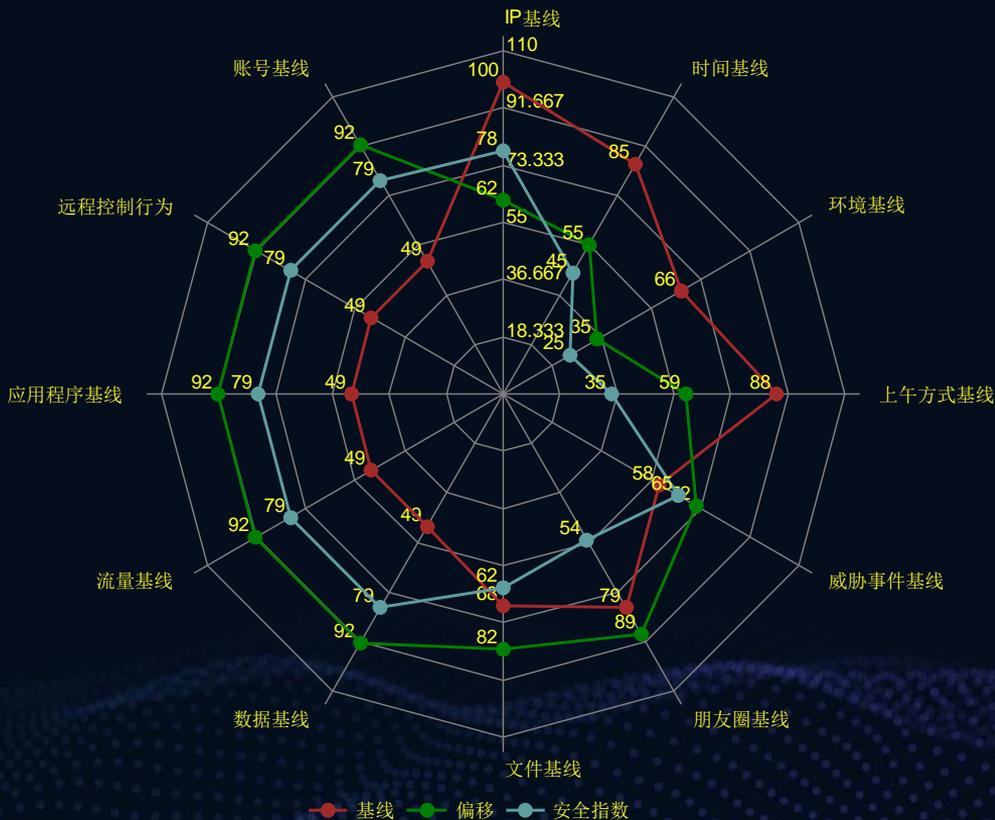


流量和频度

网络环境

人

设备环境





运行监控

网络运行 业务运行 交易行为

态势感知

网络攻击 资产态势 失陷主机

事件定位

全数据查询 多段对比 钻取式分析

驱动处置

处置建议 处置策略

数据分析

网络元数据建模

机器学习

告警归集

关联匹配

数据仓库

HDFS分布式文件系统

HBase分布式列存储数据库

流量数据

网络流量分析

终端数据

EDR, 杀毒

日志数据

防火墙、入侵防御
防病毒、入侵检测

其他接口

威胁情报
漏洞库, 事件通报



应用服务

设备信息

威胁情报

流量日志

• 端口 (选中查看服务信息, 最多同时选择3项)

- 81
- 83
- 443
- 80
- 21
- 22
- 1521
- 8080

• 服务

81	HTTP/1.1 200 OK Server: nginx/1.12.2 Date: Mon, 19 Nov 2018 07:20:38 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive BdpageType: 1 Bdqid: 0x86179b22000137ca
tcp	
xtremerat	
83	HTTP/1.1 200 OK Server: nginx/1.12.2 Date: Mon, 19 Nov 2018 07:20:38 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive BdpageType: 1 Bdqid: 0x86179b22000137ca
tcp	
http-simple-new	
81	HTTP/1.1 200 OK Server: nginx/1.12.2 Date: Mon, 19 Nov 2018 07:20:38 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive
81	HTTP/1.1 200 OK Server: nginx/1.12.2 Date: Mon, 19 Nov 2018 07:20:38 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive
tcp	

• 相关IP (10)

IP	标签	时间
1.2.4.3	低信誉IP	2018-10-18
2.4.3.5	恶意软件	2018-09-01
5.7.6.8	僵尸网络	2018-07-07

▼ 查看全部

• 相关域名 (5)

域名	标签	时间
xxx.com	低信誉IP	2018-10-18
xx.cn	恶意软件	2018-09-01
xxxx.net	僵尸网络	2018-07-07

▼ 查看全部

• 相关样本 (99)

样本	标签	时间
f43e45ff23ac52	信息窃取	2018-10-18



详细信

位置

ASN

应用程

操作系

设备类

所属组

运营商

• 端口

81

81

tcp



网络与交易性能分析

IT 2019

业务性能分析

Internet Banking

生成SLA报告 业务设置 集中监控 业务指标分析

监控

分析

2017-03-09 08:28:00 - 2017-03-09 09:28:00

< 警报

警报 >

刻度: 分钟 小时 天

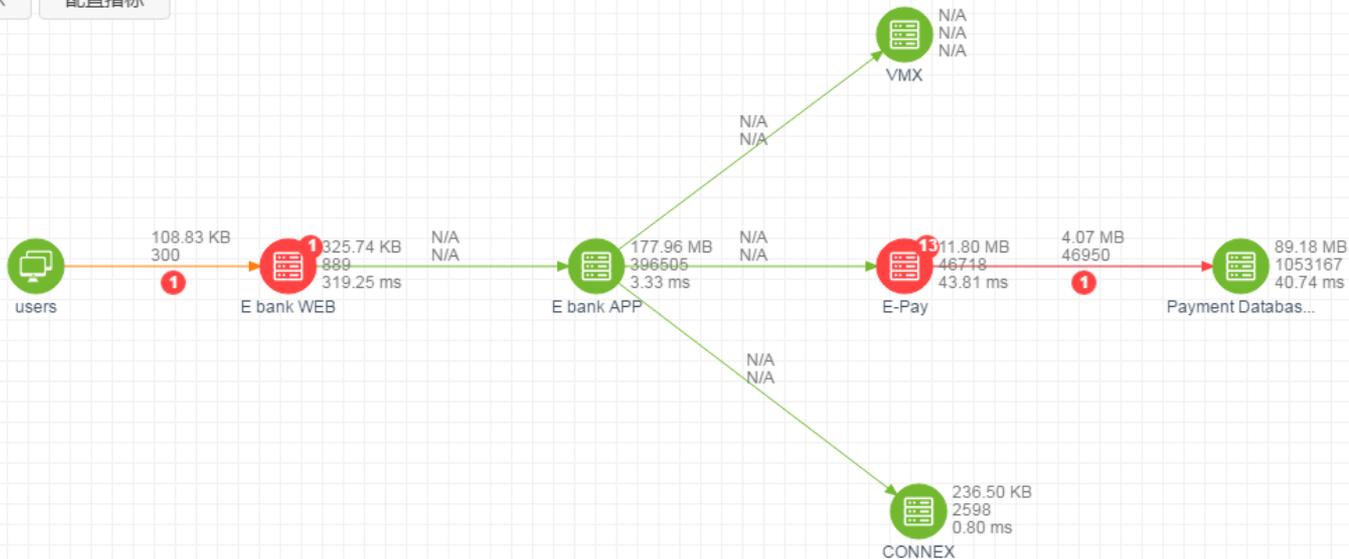
■ 正常 ■ 高 ■ 中 ■ 低



全景显示

居中显示

配置指标





协议解码

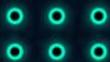
将非结构化数据转成结构化
为大数据分析做好数据准备

新的
协议

新协议、新协议版本
解码需求变更

解码
性能

流量快速增长
更高的性能需求





科来快速解码引擎 (FPDE)

Fast Protocol Decode Engine

专为协议解码设计的一种解释语言技术



灵活可扩展

协议、字段自定义
快速部署



高性能

万兆+全解码
高稳定性





科来网路元数据分析探针 (MDA)

FIIT 2019



- ◆ 单机1Gbps-40Gbps流量全解码
- ◆ 内置400+协议解码器
- ◆ 脚本化解码器开发语言，二次开发难度低
- ◆ 自定义解码数据封装
- ◆ 支持Kafka、Syslog、Flume等接口对外输出





REEBUF | 

THANKS