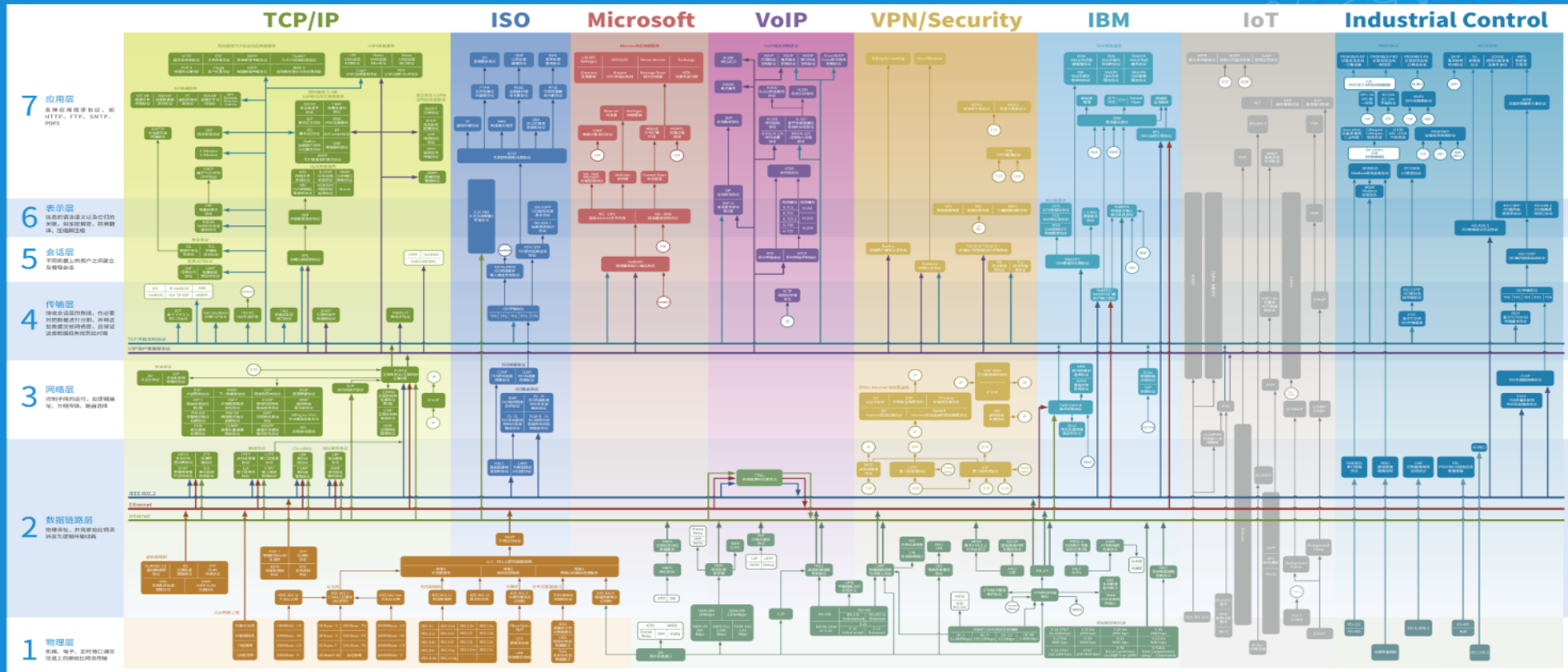
解构协议解码

李飞 成都科来软件有限公司 产品运营总监

科来®

网络通讯协议图2019版

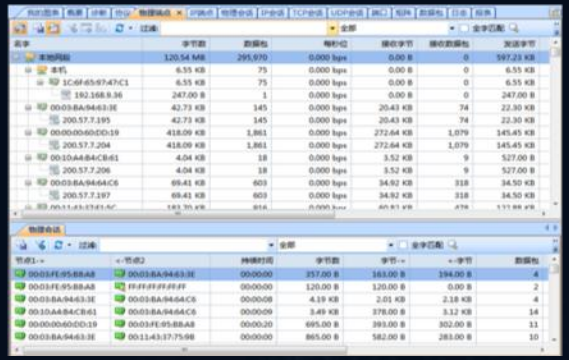
Network Communication Protocols Map

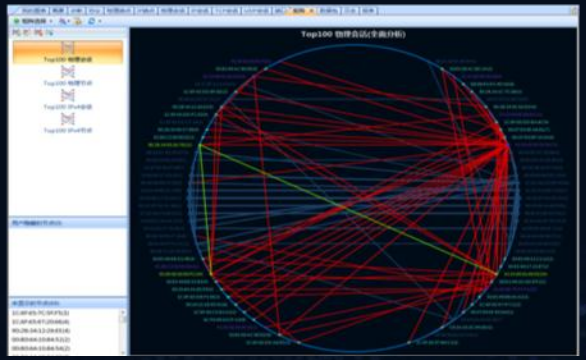


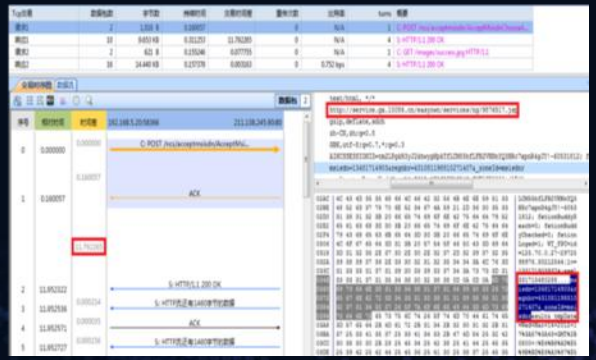
TCP/IP协议簇常见协议信息

科来网络分析系统（技术交流免费版）

FIT 2019







CSNA网络分析认证

FIT 2019

CSNA-A《网络分析服务认证》各种实战方法训练

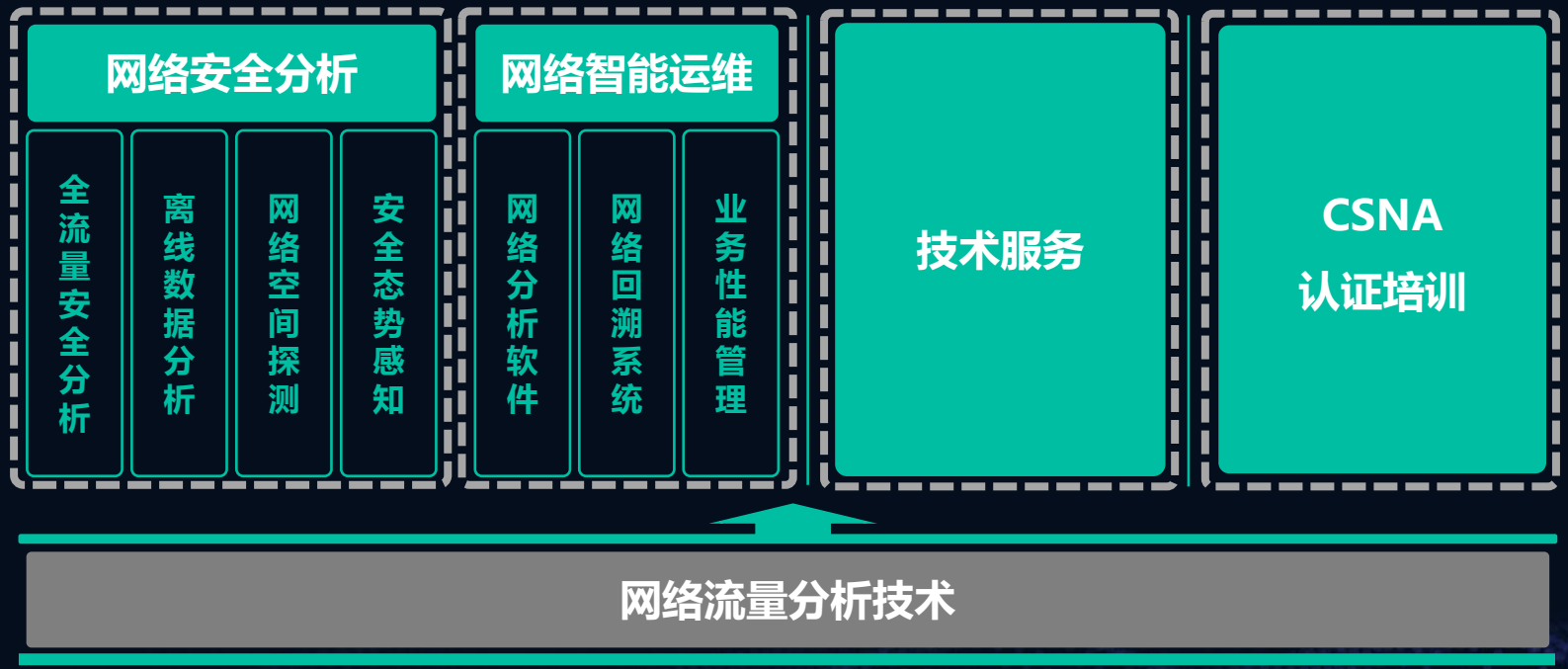
CSNA-E《网络分析体系认证》网络分析知识体系

CSNA-S《高级安全实战认证》高级攻击分析为主

相关学习资源

软件下载	学习资源
科来网络分析系统11.1（技术交流免费版）	网络攻击与防范图谱
网络分析工具	科来网络通讯协议图，TCP/IP网络协议图免费下载
科来MAC地址扫描器	科来网络故障诊断图
科来Ping工具	网络分析案例集
科来数据包播放器	数据包样本
科来数据包生成器	网络分析过滤器
	网络分析技术学习资料
	术语表

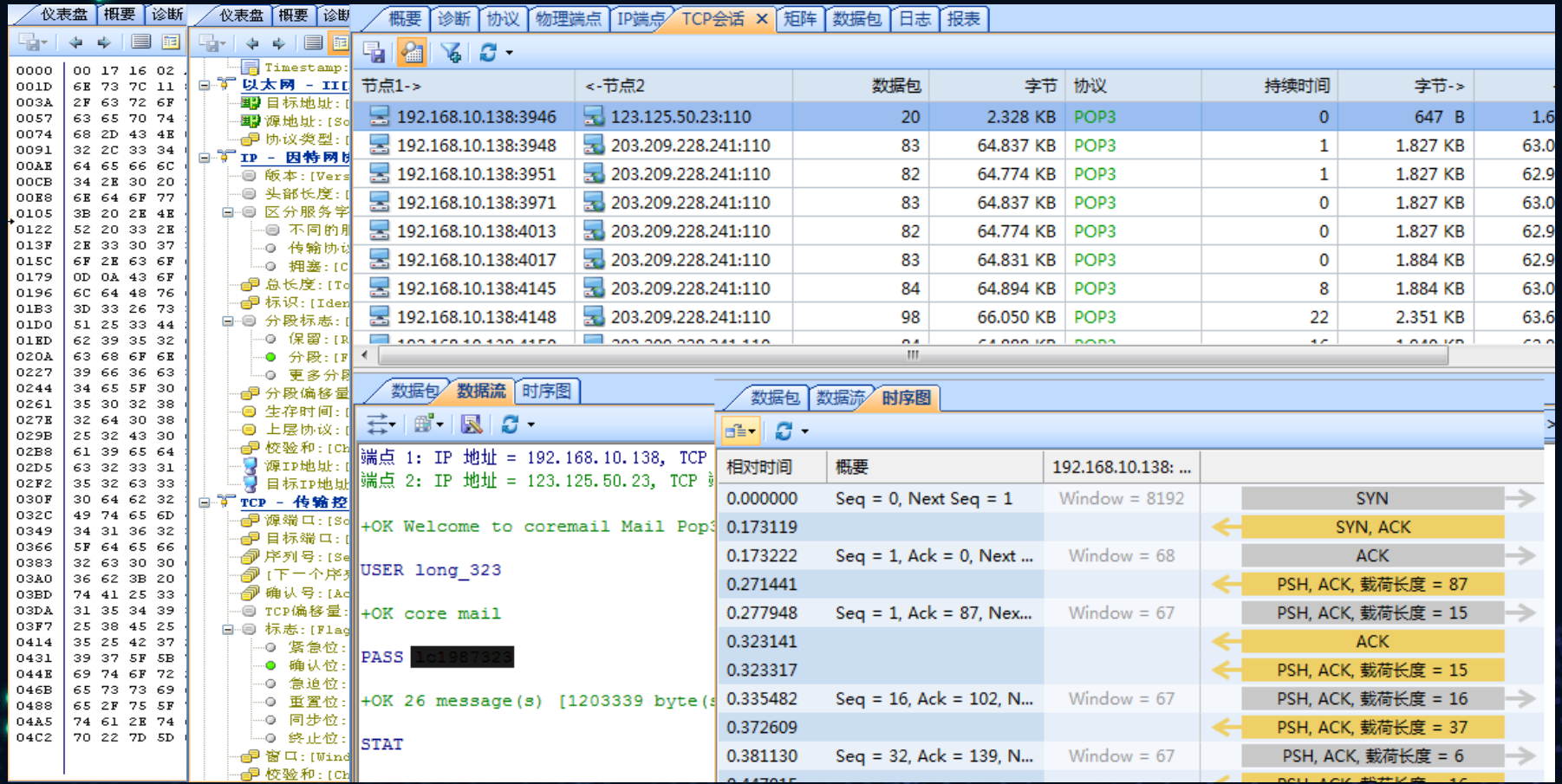
公司业务架构


网络安全分析
全流量安全分析
离线数据分析
网络空间探测
安全态势感知
网络智能运维
网络分析软件
网络回溯系统
业务性能管理
技术服务
CSNA
认证培训
网络流量分析技术

网络流量分析的一般过程

- 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


概要 诊断 协议 物理端点 IP端点 TCP会话 矩阵 数据包 日志 报表
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
192.168.10.138:3948 203.209.228.241:110 83 64.837 KB POP3 1 1.827 KB
192.168.10.138:3951 203.209.228.241:110 82 64.774 KB POP3 1 1.827 KB
192.168.10.138:3971 203.209.228.241:110 83 64.837 KB POP3 0 1.827 KB
192.168.10.138:4013 203.209.228.241:110 82 64.774 KB POP3 0 1.827 KB
192.168.10.138:4017 203.209.228.241:110 83 64.831 KB POP3 0 1.884 KB
192.168.10.138:4145 203.209.228.241:110 84 64.894 KB POP3 8 1.884 KB
192.168.10.138:4148 203.209.228.241:110 98 66.050 KB POP3 22 2.351 KB
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
+OK Welcome to coremail Mail Pop3
USER long_323
+OK core mail
PASS
+OK 26 message(s) [1203339 byte(s)
STAT
数据包 数据流 时序图
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

可以输出结构化的元数据

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；

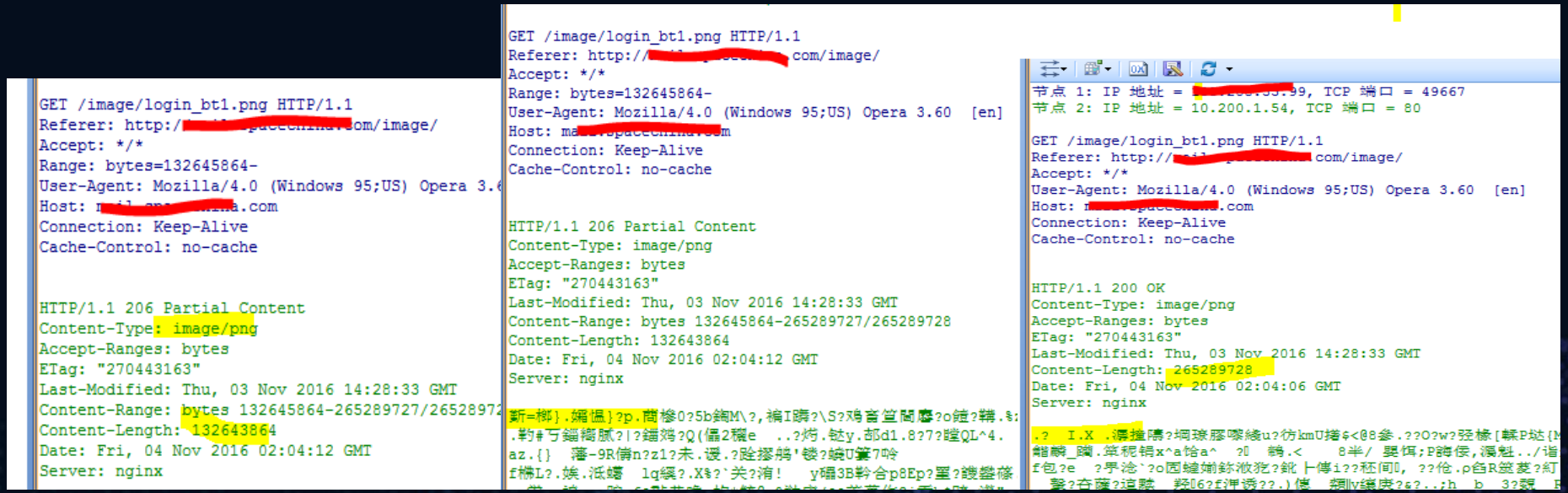
如15种DNS协议字段、SMTP/POP3协议字段…

应用与业务场景

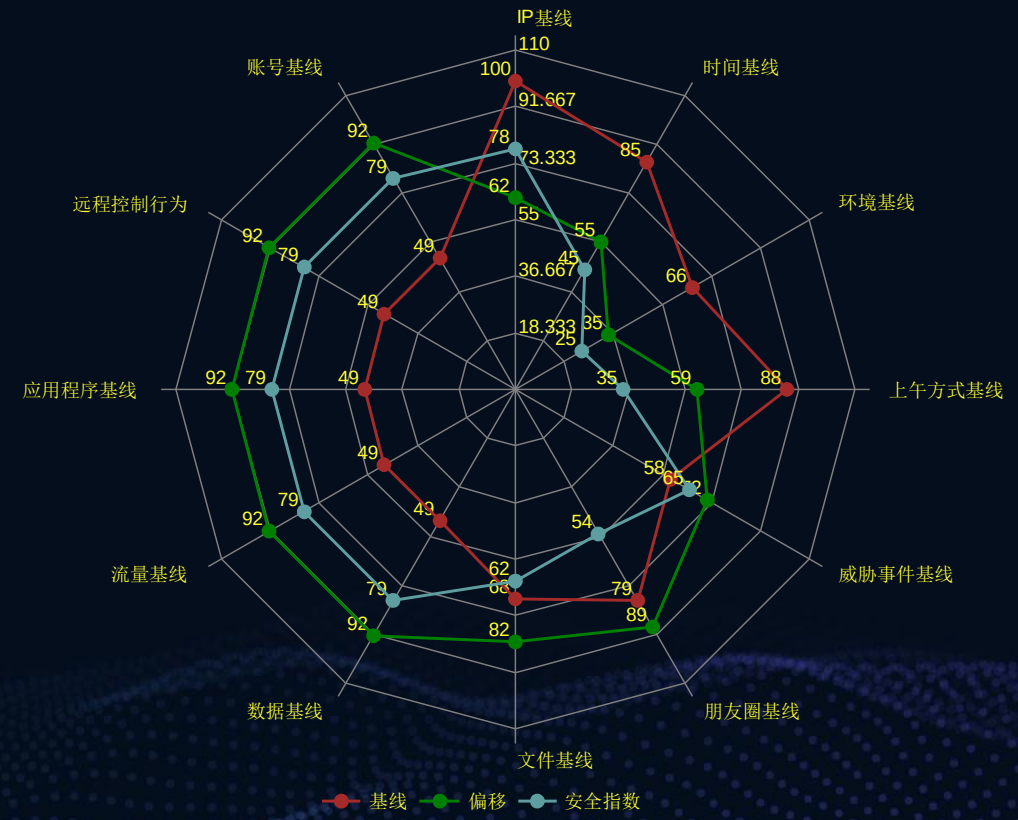
网络安全检测举例：网络窃密行为发现

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



网络安全检测举例：用户与实体行为分析（UEBA）



安全态势感知

运行监控	态势感知
网络运行 业务运行 交易行为	网络攻击 资产态势 失陷主机
事件定位	**驱动处置**
全数据查询 多段对比 钻取式分析	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

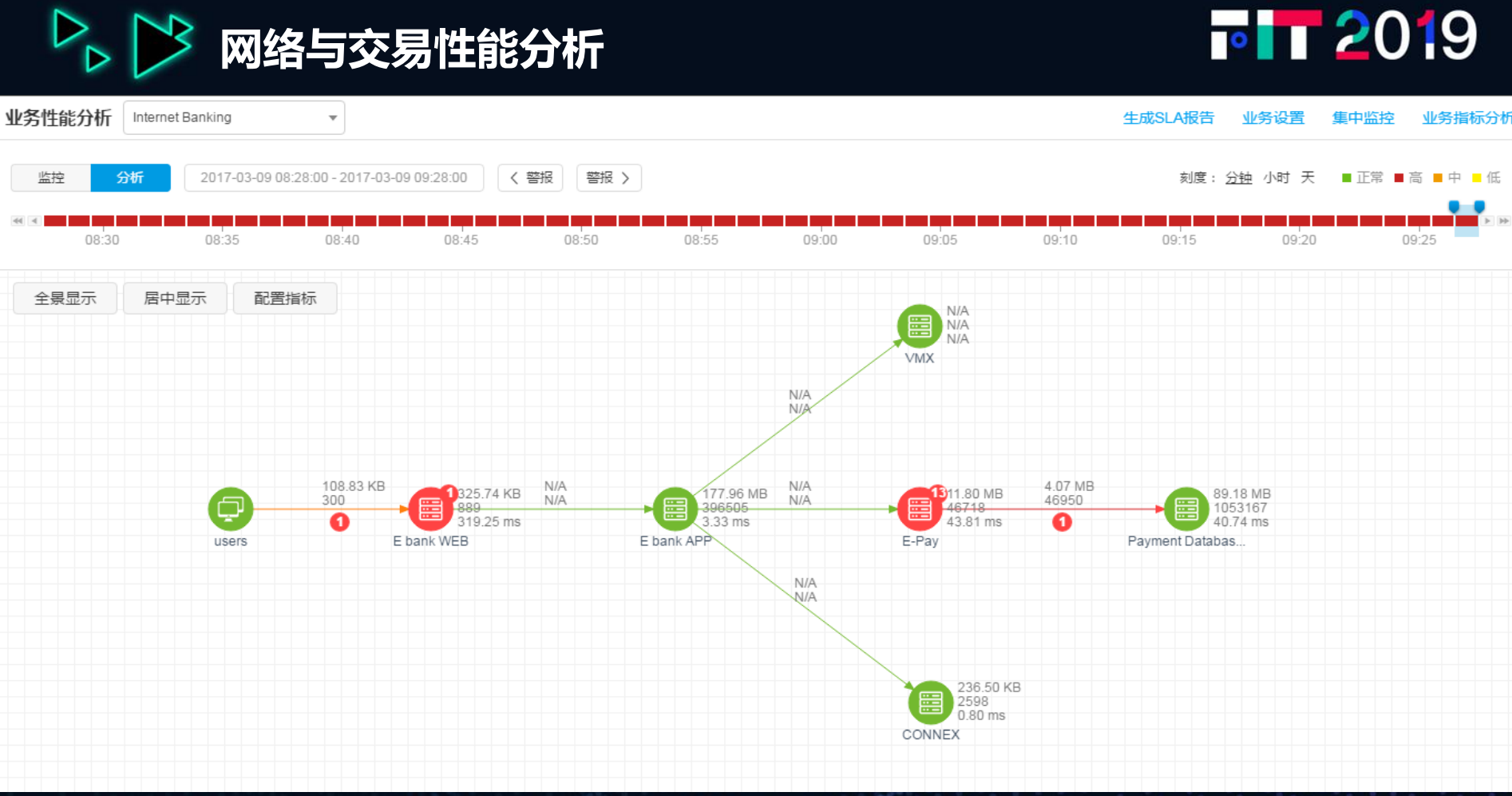
数据仓库	
HDFS分布式文件系统	HBase分布式列存储数据库

流量数据	终端数据	日志数据	其他接口
网络流量分析	EDR，杀毒	防火墙、入侵防御 防病毒、入侵检测	威胁情报 漏洞库，事件通报

网络空间探测


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
tcp
xtremerat
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
83
tcp
http-simple-new
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
81
tcp
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
详细信
位置
ASN
应用程
操作系
设备类
所属组
运营商
• 端口
81
• 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

网络与交易性能分析


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
08:30
08:35
08:40
08:45
08:50
08:55
09:00
09:05
09:10
09:15
09:20
09:25
全景显示
居中显示
配置指标
users
108.83 KB
300
1
E bank WEB
325.74 KB
889
319.25 ms
1
N/A
N/A
E bank APP
177.96 MB
396505
3.33 ms
N/A
N/A
VMX
N/A
N/A
N/A
N/A
N/A
E-Pay
11.80 MB
46718
43.81 ms
13
4.07 MB
46950
1
Payment Databas...
89.18 MB
1053167
40.74 ms
N/A
N/A
CONNEX
236.50 KB
2598
0.80 ms

协议解码面临的挑战

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

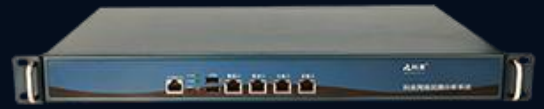
快速部署

高性能

万兆+全解码

高稳定性

科来网路元数据分析探针（MDA）



- 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

FREEBUF | FIT

THANKS