FREEBUF
企业安全俱乐部

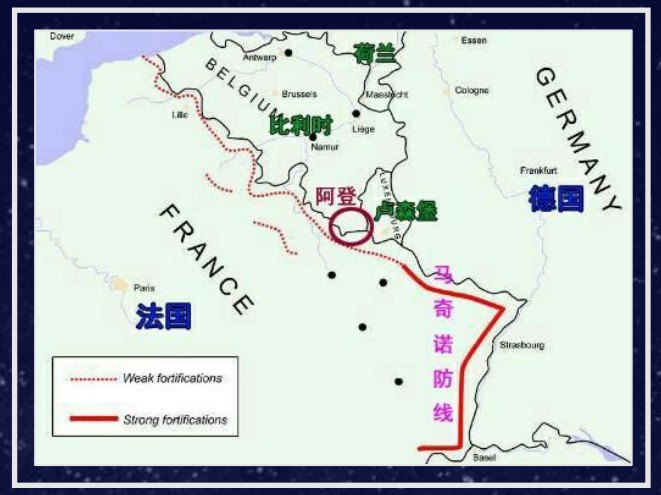
安全事件的发现、分析、响应与取证

周宏斌

北京兰云科技有限公司

生活中的故事

马奇诺防线—坚固但被绕过

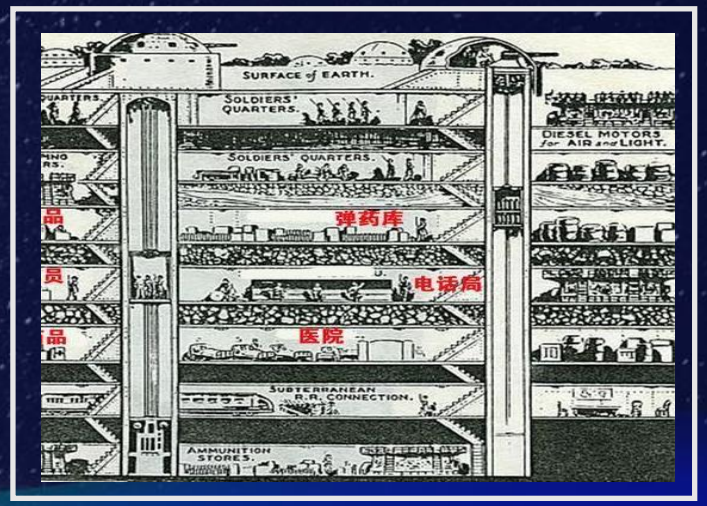


马奇诺防线耗时11年，造价50亿法郎，全长约390公里，土方工程量达1200万立方米，耗混凝土约150万立方米，耗钢铁量达15万吨。防线建成后，每年要消耗国防经费的一半，国内的反对声音越来越大，所以马奇诺防线并没有覆盖法国全境，仅防御法德边境。

第二次世界大战期间，德军忌惮马奇诺防线的威力，转而从比利时与法国的交界处寻找突破口，绕过马奇诺防线。1940年5月德军诱使英法联军支援荷兰，偷袭阿登高地(比利时和法国交界处)，联合荷兰德军将联军围困在敦克尔克。而马奇诺防线也因为德军袭击其背部而失去作用。

坚固的马奇诺防线为什么没有让法国固若金汤？

被动的防御手段无法应对作战方式的瞬息万变。



在虚假的安全感下，民众抵抗意志瓦解。

交通事故—事故分析与责任认定

商丘发生一起三车相撞事故 一车前脸完全撞坏

社会　商丘广播1007　2018-05-21 19:50　68 评论

B车由北向东左转，被突如其来的A车迎面撞上，A车撞上B车之后继续向西北方向，正巧迎面撞上正在路口等待进入机动车道的C车，司机都反映事故的原因可能是A车速过快，连撞两车。

商丘三车相撞的事故 责任认定出来了……

2018-05-23 05:53:41　来源: 直播商丘

道路交通事故认定书（简易程序）

第 411402201805210652 号

事故时间	2018 年 05 月 21 日 08时 15 分			天气	小雨
事故地点	河南省商丘市梁园区平原南路918(115.62966,34.426913)				
当事人	张[illegible]	驾驶证或身份证号码	4[illegible]	联系电话	1[illegible]
交通方式	小型汽车	机动车型号、牌号	豫N[illegible]	保险凭证号	20[illegible]38
当事人	宋[illegible]	驾驶证或身份证号码	41[illegible]	联系电话	[illegible]
交通方式	小型汽车	机动车型号、牌号	豫N[illegible]	保险凭证号	13[illegible]78
交通事故事实及责任	2018年05月21日08时15分，甲方：张[illegible]，驾驶车牌号为：豫N[illegible]的车辆，乙方：宋[illegible]，驾驶车牌号为：豫N[illegible]的车辆，在河南省商丘市梁园区平原南路918处发生交通事故。甲方：张[illegible]违反了相对方向来车左转弯车辆未让直行车辆，或右转弯车辆未让左转弯车辆先行的之规定，根据《中华人民共和国道路交通安全法实施条例》第九十一条之规定认定：张[illegible]承担全部责任，宋[illegible]不承担责任。				

当事人 [illegible]　[illegible]

交通警察 NZ00048 逯群典

（印章）

2018 年 05 月 21 日

商丘广播1007

B车转弯未让行A车，A车无责！！

福尔摩斯—案件还原与取证

There is no perfect crime in the world.

--Sherlock Holmes

被动的防护方式
成本高，易绕过

欠缺有效的技术支撑
案件分析艰难，低效

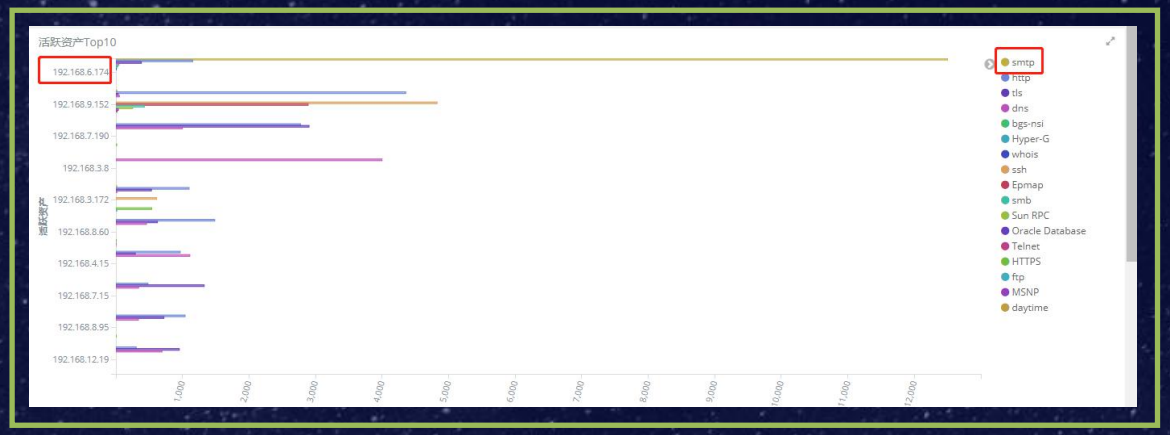
网络中的案例

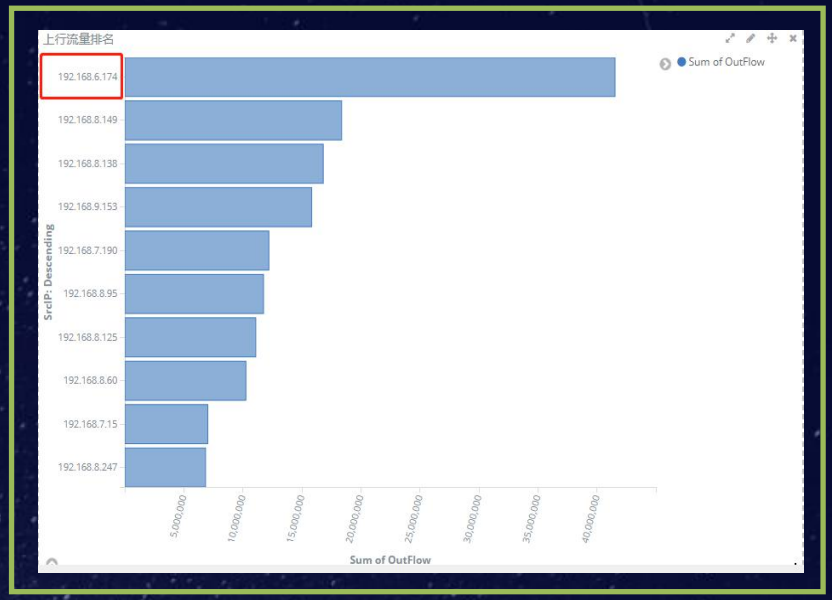
一个真实的案例-流量异常

13:30~13:35 5分钟内，内网整体流量突增

一个真实的案例—协议异常

6.147主机30min内上行流量排名第一，活跃资产排名第一，最活跃的协议类型为SMTP，为邮件协议





近30min的异常流量是由可疑主机的邮件访问行为引起的

一个真实的案例—邮件异常

主机邮件访问频率为40次/30s，排除人为操作，目的IP存在规律性，皆为美国IP。

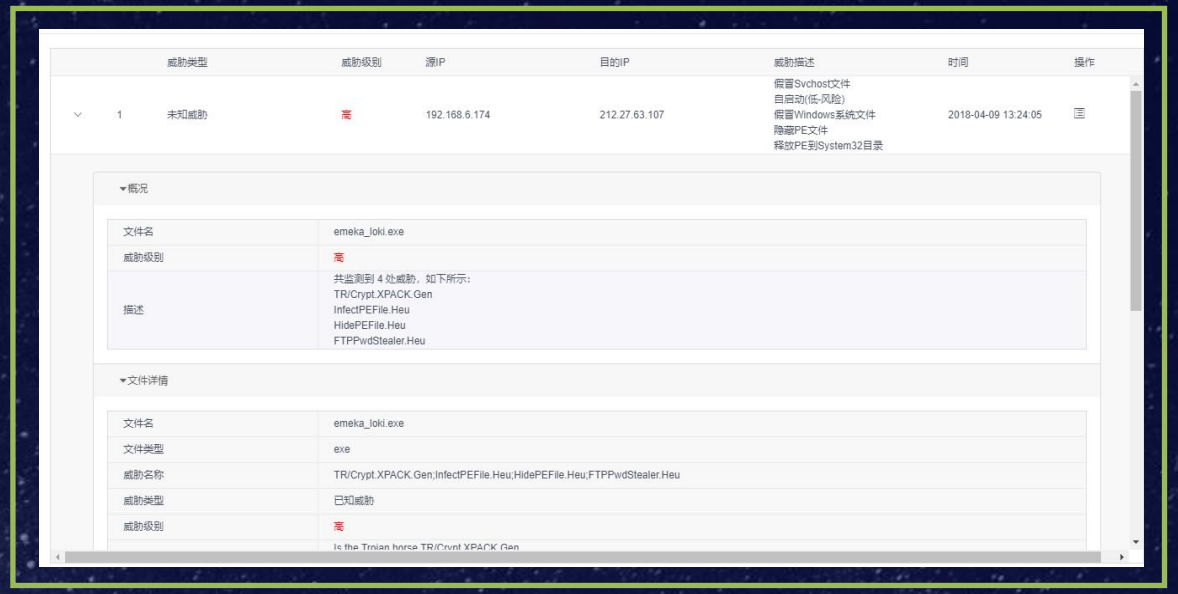
一个真实的案例—邮件内容异常（虚构）

云标签越大，表示信息出现的频率越高，可发现可疑主机发送邮件中包含相当比例的敏感信息。

可疑主机可能是中了病毒，自动外发含敏感信息的邮件

一个真实的案例—程序行为异常

通过对沙箱检测结果的关联，发现可疑主机
在 13:24，有下载病毒行为，在事件上与以上分析
的异常行为事件的发生先后顺序高度契合。



	威胁类型	威胁级别	源IP	目的IP	威胁描述	时间	操作
1	未知威胁	高	192.168.6.174	212.27.63.107	假冒Svchost文件 自启动(低-风险) 假冒Windows系统文件 隐藏PE文件 释放PE到System32目录	2018-04-09 13:24:05	

概况

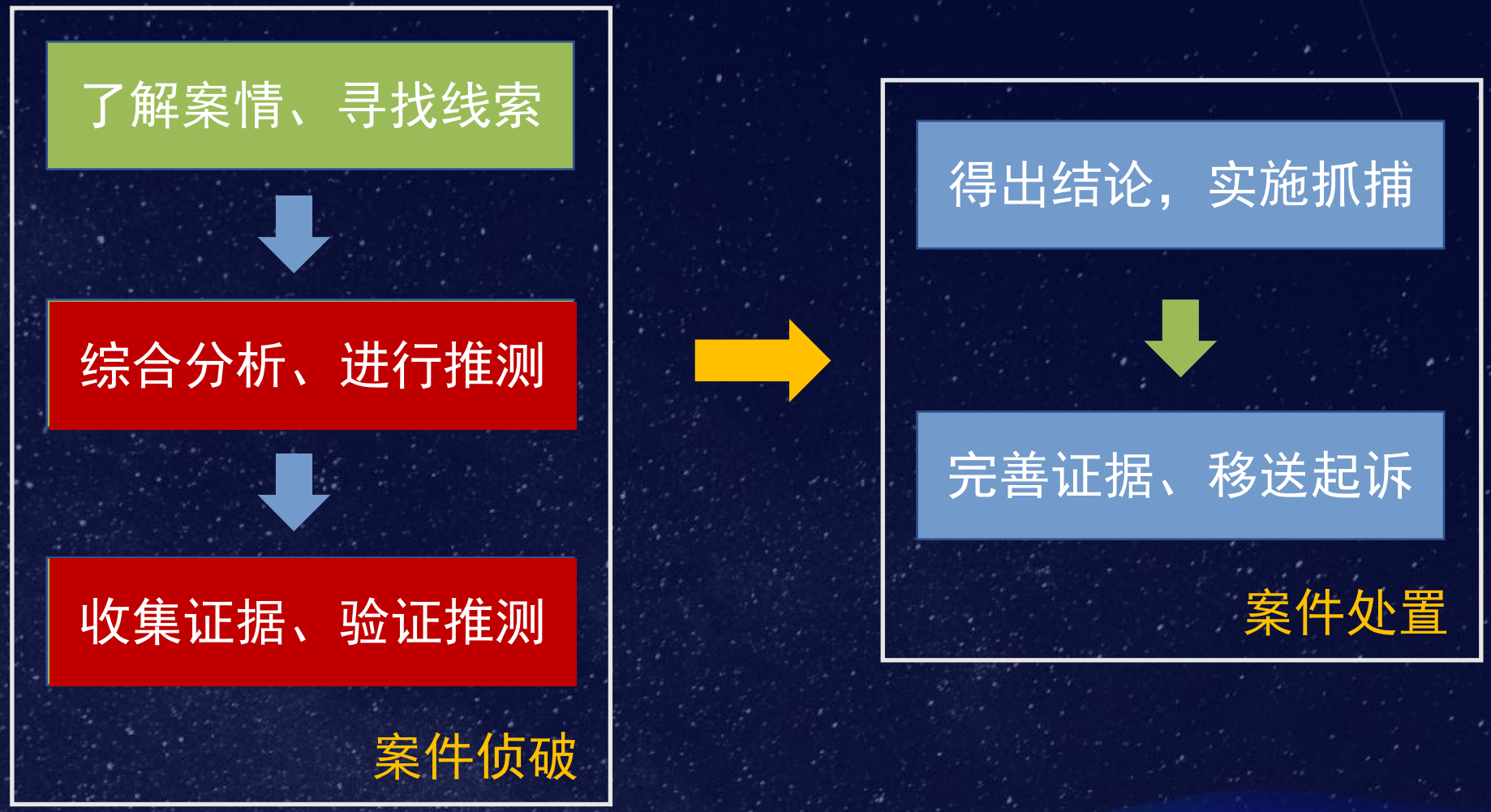
文件名	emeka_loki.exe
威胁级别	高
描述	共监测到 4 处威胁，如下所示： TR/Crypt.XPACK.Gen InfectPEFile.Heu HidePEFile.Heu FTPPwdStealer.Heu

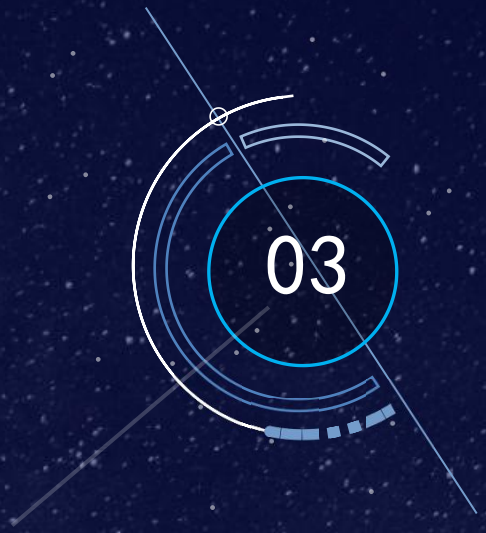
文件详情

文件名	emeka_loki.exe
文件类型	exe
威胁名称	TR/Crypt.XPACK.Gen;InfectPEFile.Heu;HidePEFile.Heu;FTPPwdStealer.Heu
威胁类型	已知威胁
威胁级别	高
	Is the Trojan horse TR/Crypt.XPACK.Gen

内网主机下载了含有病毒的文件，造成主机失控

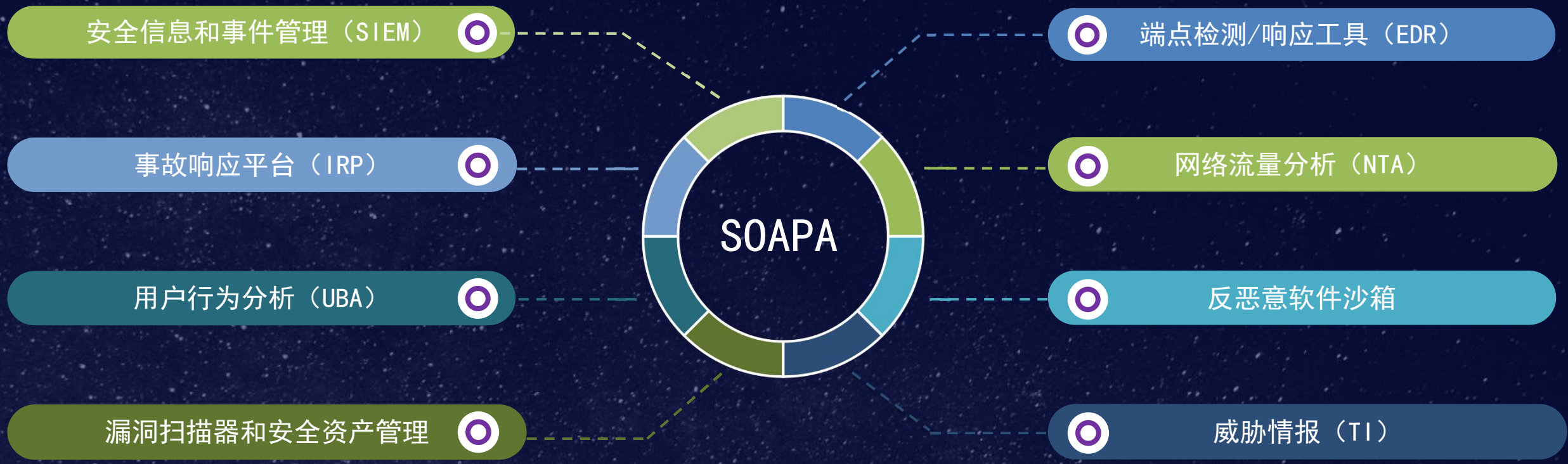
案件处理流程





兰云的实践

安全运营与分析平台架构（SOAPA）



反恶意软件沙箱

系统级沙箱

系统模拟

- 模拟真实的Windows操作系统
- 监视程序运行期间的系统API调用，并识别危险的API调用
- 基于行为分析技术，弥补传统基于特征码匹配的不足

系统沙箱
行为检测点全、检测精度准

应用级沙箱

文档检测

- 模拟文档加载环境（Office 、Adobe Reader）
- 监视文档加载过程的API调用，并识别出危险的API调用

浏览器模拟

- 模拟Web浏览器（IE、Firefox、Chrome）运行环境
- 监视解析过程的所有浏览器行为，并识别出危险行为
- 关注缓冲区溢出、恶意跳转、软件逻辑脆弱性攻击等

应用沙箱
软件版本全、检测效率高

反恶意软件沙箱

文件详情

描述	共监测到 4 处威胁，如下所示： AutorunL.Heu RemoteInjectionWinProc.Heu MapToSysProc.Heu InjectExplorer.Heu

▸文件详情

▸威胁详情

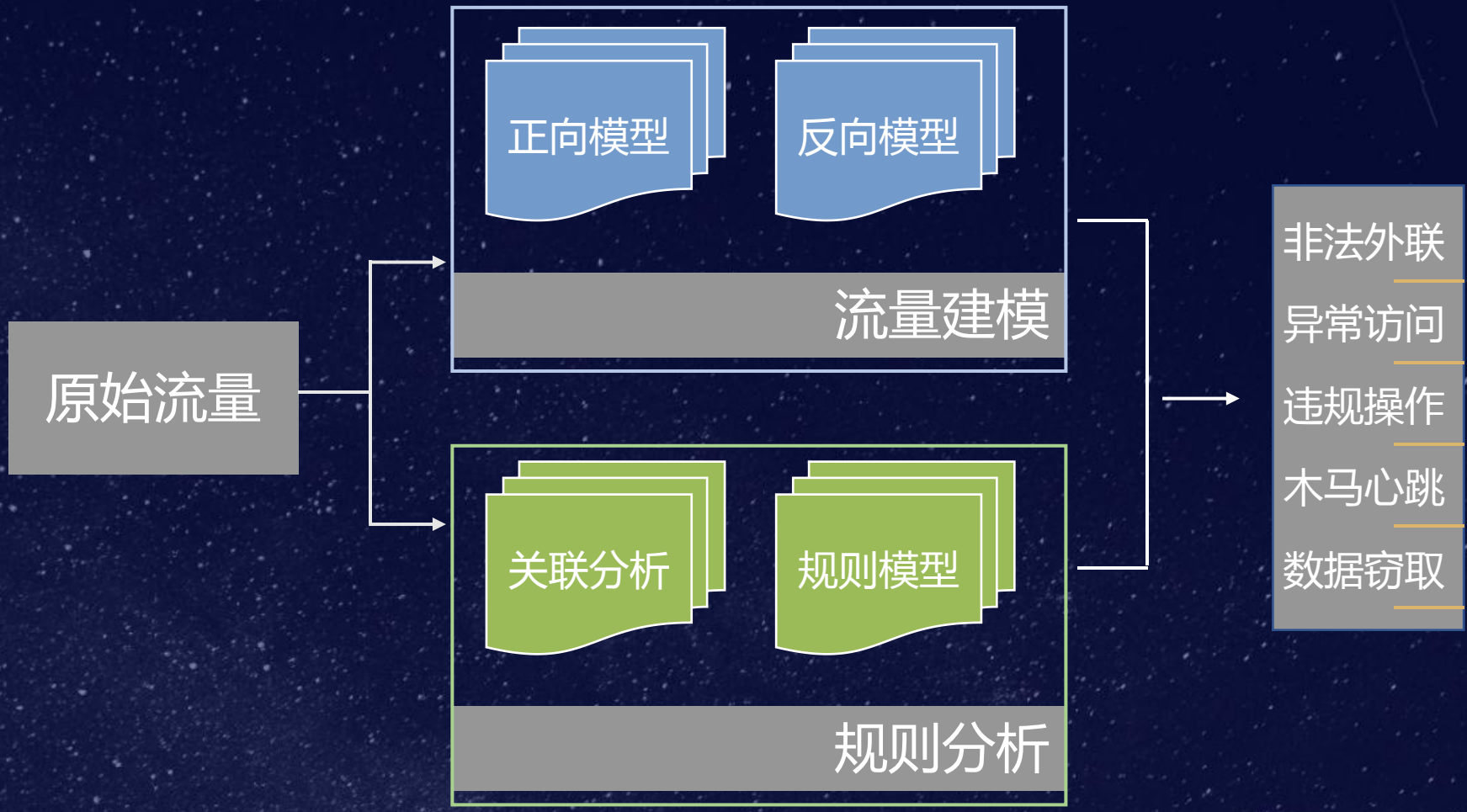
▾文件日志

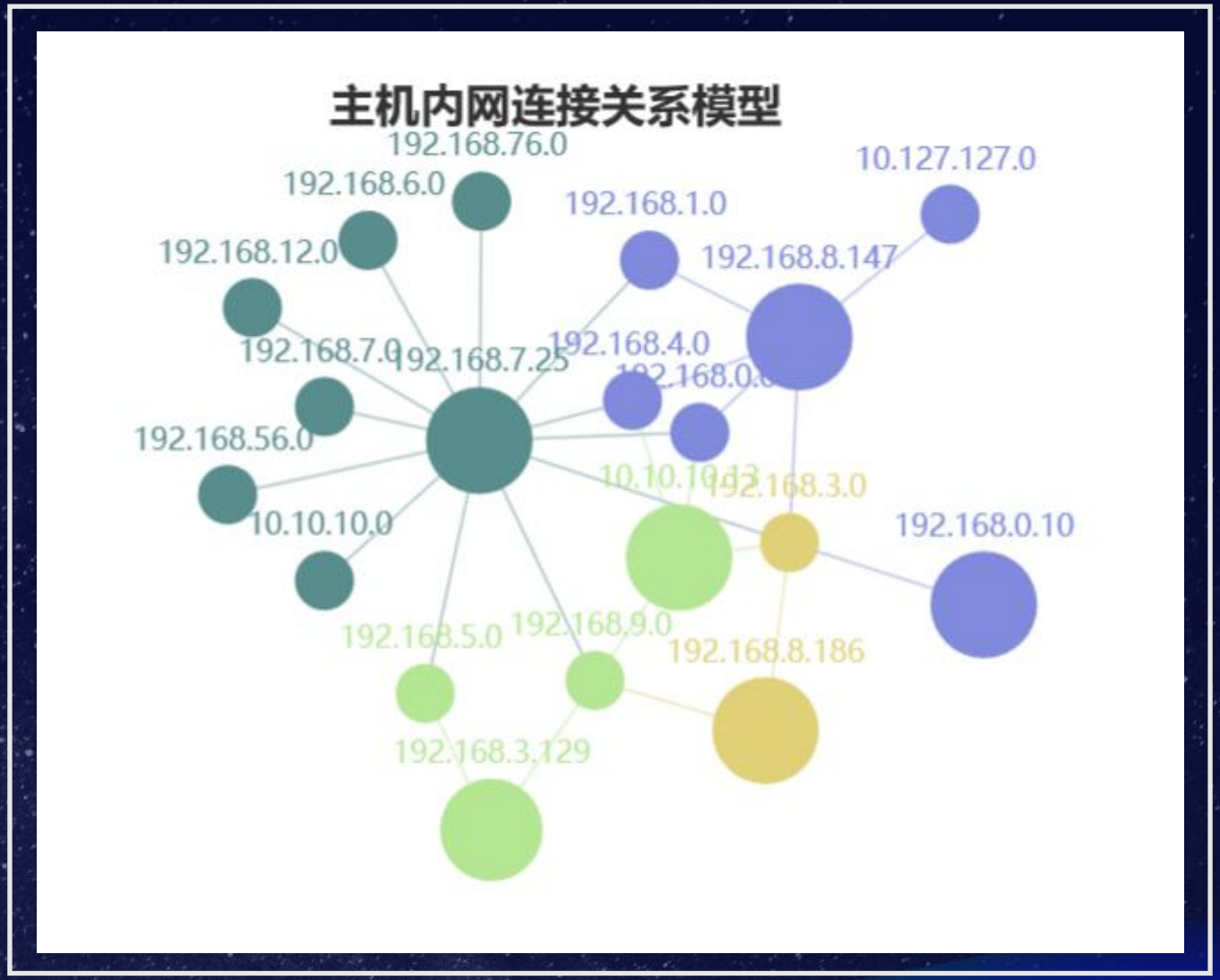
网络操作 | 进程相关操作 | 注册表相关操作 | 内存操作 | 所有日志

威胁类型 注入

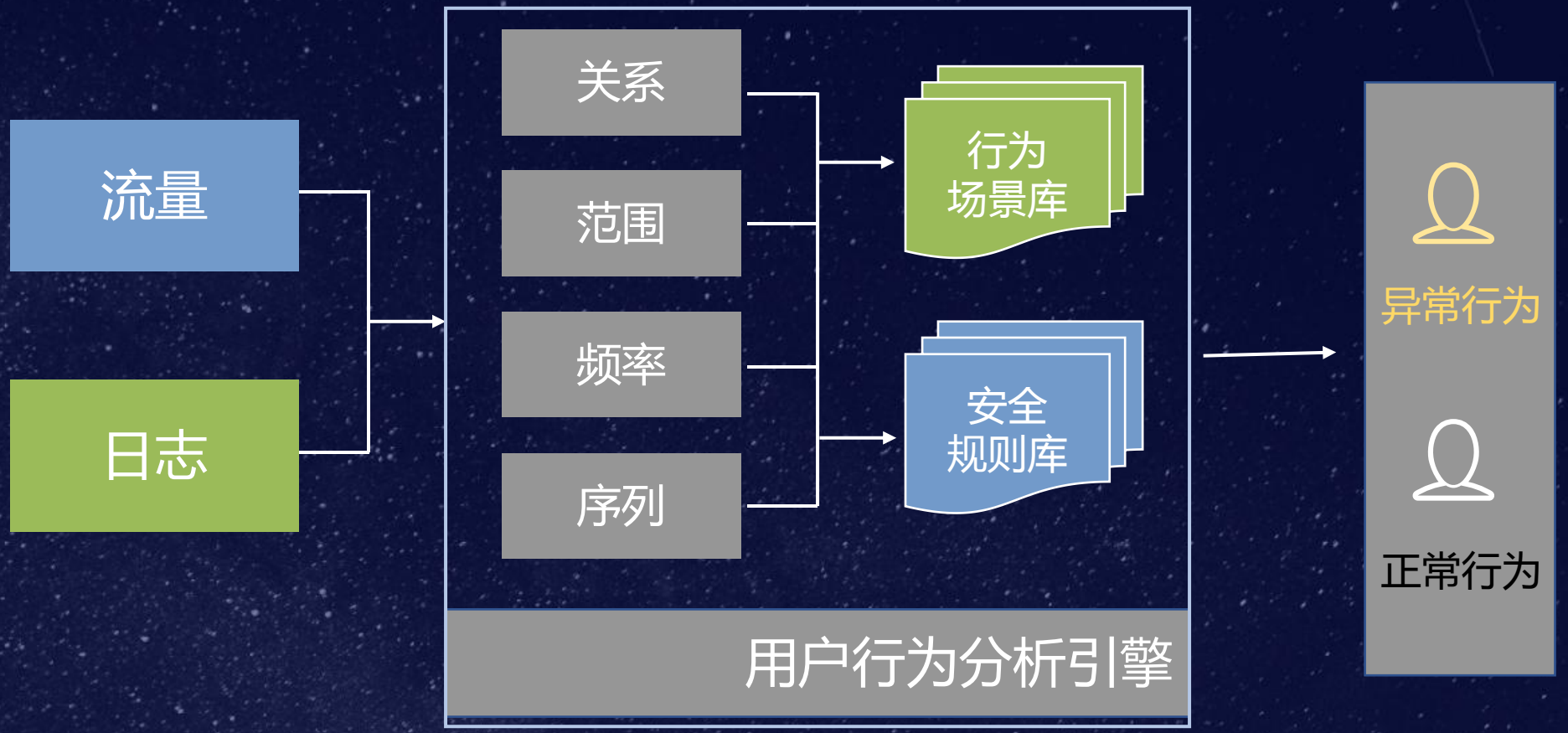
威胁描述 通过在其他进程内开辟新线程并将线程回调函数设置为LoadLibrary函数，并将其参数设置为恶意的DLL动态库文件的路径，新线程运行后会将恶意DLL库加载从而达到注入的目的

网络流量分析(NTA)

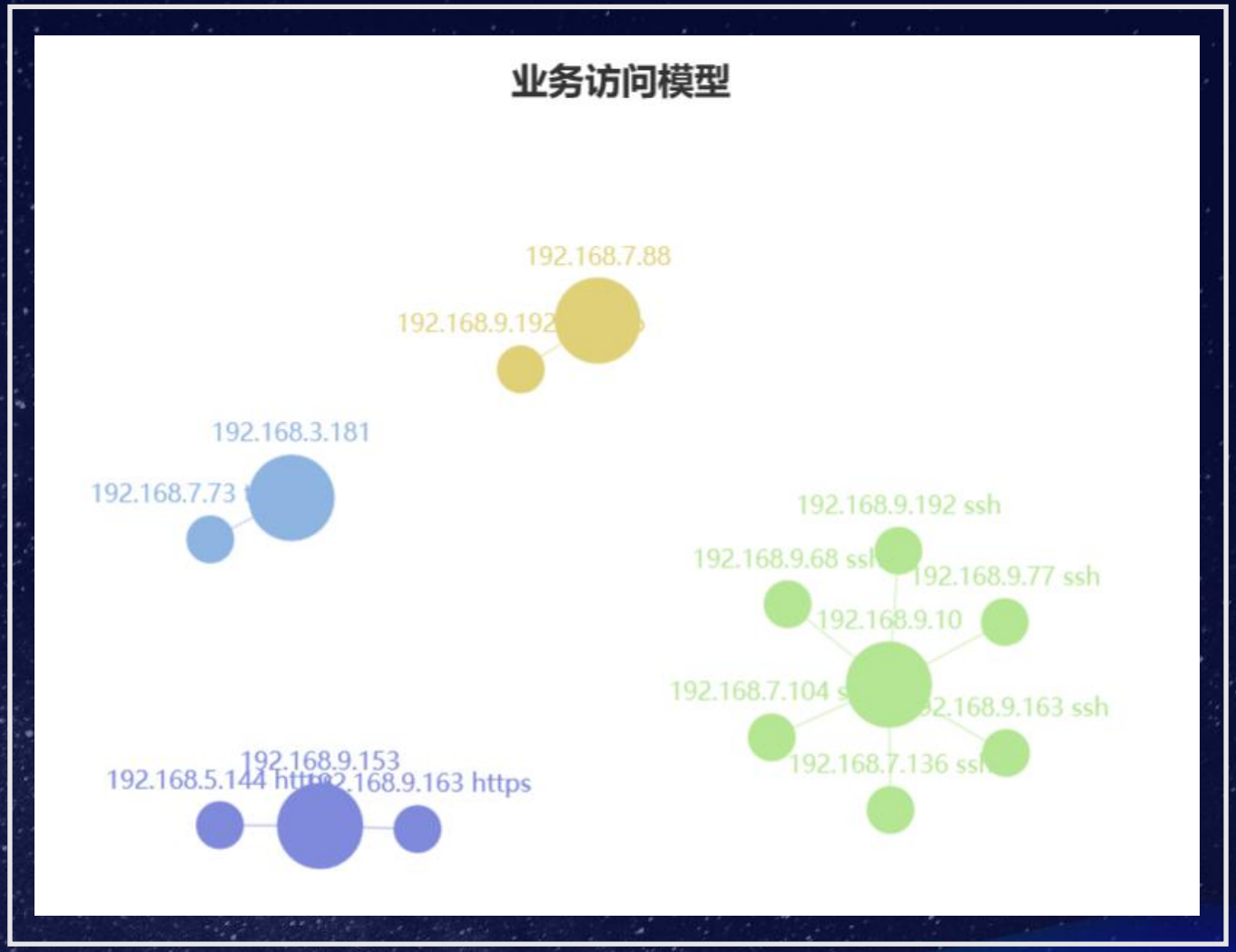




用户行为分析（UBA）



用户行为分析（UBA）



端点检测及响应技术（EDR）

01 监控操作系统级行为和可疑进程

02 发现威胁行为及时响应、阻断

端点检测及响应技术（EDR）

资产管理

手动录入、文件导入、主动扫描、被动识别

资产发现

闲置资产智能判断

价值评估

资产价值科学评估

资产管理

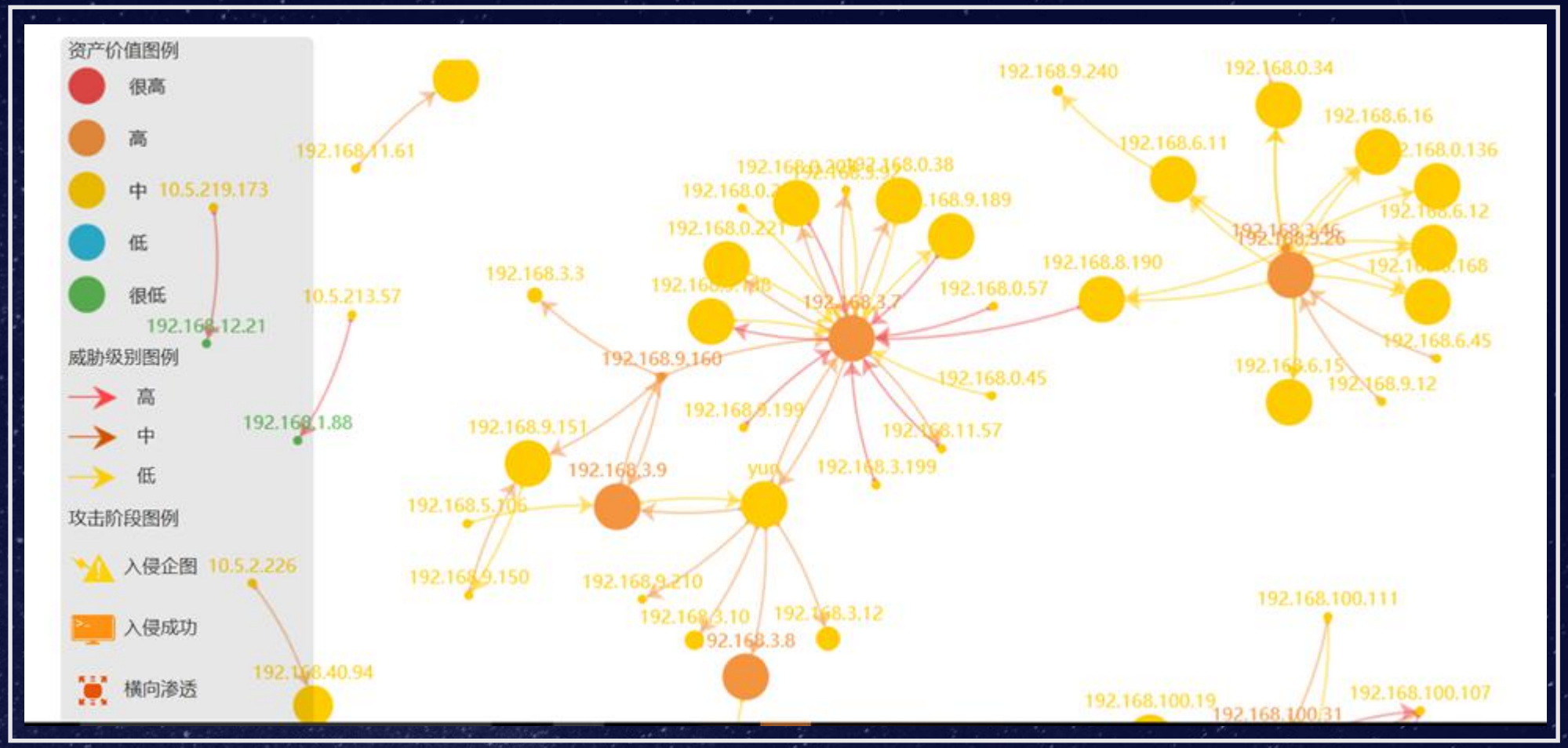
资产详情 | 运行服务 | 安装软件 | 威胁事件 | 资产漏洞 | 配置管理

详情

名称	
IP	192.168.8.157
MAC	F4:31:C3:B2:45:71
状态	在线
位置	null
拥有者	null
设备类型	PC机
设备型号	null
资产编号	null
操作系统	null
生产厂商	null
数据来源	自动采集
资产描述	null
URL	
用户名	

风险评估 很低

安全事件分析的威胁全景图



谢谢

北京兰云科技有限公司