协同安全能力 共建情报生态

威胁情报生态大会

基于网络全流量及威胁情报的高级威胁检测体系建设

牟健君 中国光大银行

提纲

1 行业态势

2 高级威胁检测体系建设

3 安全生态，合作共赢

网络安全现状

- 近年来，针对金融行业关键信息基础设施的网络攻击更加常态化、专业化，针对性极强，造成了大量的经济损失。

勒索病毒持续爆发

•2017年5月，永恒之蓝WannaCry病毒在全球大规模爆发。10个小时感染74个国家的45000台主机，勒索金额13,500,000美元，直接**经济损失数十亿美元。**

APT攻击愈演愈烈

•世界范围内使用**SWIFT系统**的银行相继被曝出盗窃案件，从2015年厄瓜多尔银行损失1200万美元，10月的菲律宾银行，到16年2月孟加拉国央行曝出被盗窃8100万美元。

有组织有目的的攻击

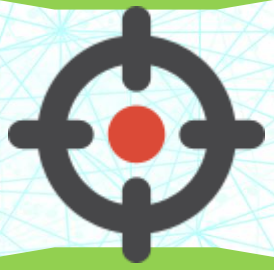
• **Anonymous（匿名者）**组织12月12日发布了攻击宣言，将针对国内银行机构进行DDOS和SQL注入攻击，目标是攻陷全球的银行业巨头，使其无法正常提供服务。

- **攻防形势，带来安全新挑战**：网络安全攻防形势的变化对网络安全提出了新的挑战；
- **技术创新，带来安全新需求**：“云大物移智”等新技术的应用，WIFI、移动互联网、远程办公等带来便利的同时也带来数据泄露风险，新技术的应用带来更多业务场景，同时也对网络安全提出了新需求；
- **监管要求，带来安全新要求**：国家和监管机构发布了“网络安全法”、"信息安全等级保护2.0"、普惠金融发展规划，对信息科技发展和网络安全建设提出了新要求，指明了发展方向；
- **能力建设**：网络安全人才建设对比同业还存在很大不足，面临招人难的问题；

APT等高级威胁一直在持续

高级(A)	可持续(P)	威胁(T)
可绕过目前的防御系统	不断尝试，直至进入目标	可造成极大危害

Gartner定义



APT攻击

具体表现

驱动力

- 地下黑客产业
- 政治利益
- 黑客行动主义
- 国家政治背景

攻击手段

- 零日攻击
- 水坑攻击
- 鱼叉攻击
- 多种逃逸技术

攻击对象

- 中小企业
- 大型企业
- 基础设施行业
- 国家机关

造成的影响

- 商业机密泄露
- 终断业务
- 破坏声誉
- 盗窃国家机密

威胁入侵途径

外部入侵	不合规软件	供应链问题	内网威胁
外网漏洞利用	第三方软件	供应链间谍	内网边界
• APT攻击； • Weblogic反序列化漏洞； • Strust2漏洞； • 暴力破解； • 勒索病毒；	• 开源软件； • 灰色软件； • 盗版软件； • 合作公司提供软件；	• 合作公司； • 外包公司； • 内部人员投放长期潜伏；	• 内网终端、服务器染毒； • 内网攻击注入； • 内部数据泄露； • 社工；

当更多的0DAY漏洞和未知威胁穿透当前的安全防御体系后，如何尽快地做出响应，锁定攻击范围，最大程度地减少损失，将成为最有价值的创新！


安全威胁是无限的
安全要解决的问题是无限的
识别网络行为，定义正常的业务行为，发现异常行为

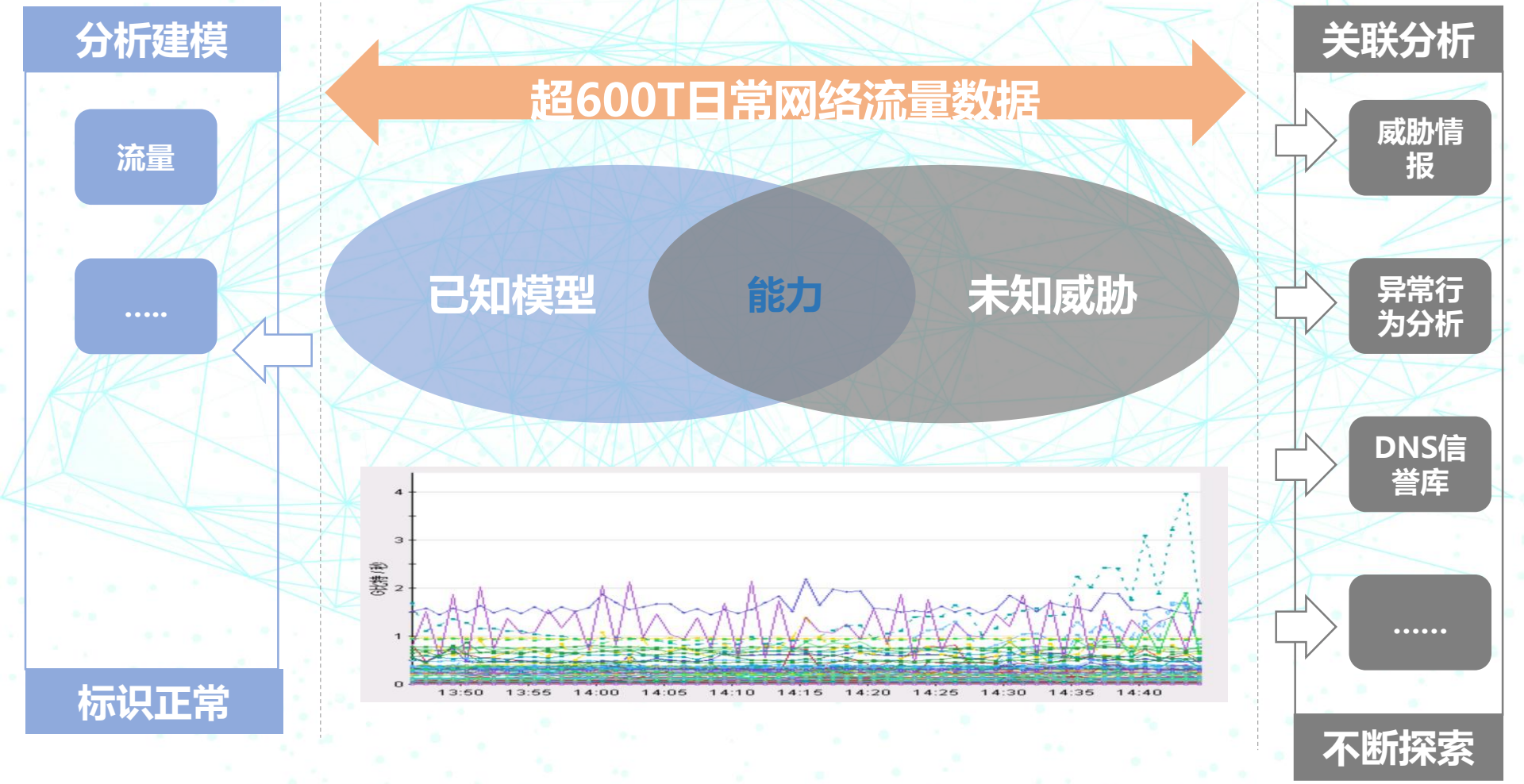
提纲

2 高级威胁检测体系建设

1. 技术架构支撑
2. 高级威胁检测方案设计
3. 其他保障方案

技术架构支撑

将日常威胁分为已知模型和未知威胁两大类，利用威胁情报、异常行为分析、DNS信誉库等手段不断探索发现更多的未知威胁，同时通过分析建模等方式定义已知，标识正常行为，减少未知。

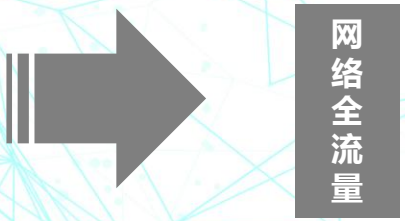


技术架构支撑

发现的手段

基于网络全流量采集、分析技术，通过对正常流量进行分析、学习、建模，识别网络“异常行为”，但凡走过必留痕，实现网络攻击可视化。

- **情报收集**：网络扫描、应用程序漏洞探测；
- **单点突破**：漏洞利用、钓鱼邮件、暴力破解；
- **命令控制**：恶意DNS请求、外联恶意互联网ip、外联服务器下载病毒或木马；
- **横向移动**：内网踩点、内网横向渗透、内网横向病毒传播；
- **数据窃取**：异常网络行为、用户行为异常、异常的数据库操作；
- **数据外传**：异常网络行为、外联异常服务器、异常通信流量；



需要的技术支撑

序号	技术支撑	部署位置
1	纯网络流量捕获、汇聚、分配探针	全网覆盖
2	异常流量检测、采集技术	互联网边界、内网环境
3	网络全流量深度威胁分析技术	互联网边界、内网环境、自助设备/物联网设备汇聚节点
4	强大的威胁情报库、DNS/IP信誉库、规则库	同上
5	大数据分析、建模、智能学习技术	同上
6	网络报文回溯、取证技术	同上
7	网络海量日志集中监控平台	态势感知平台
8	安全资产盘点展示	态势感知平台
9	系统日志与网络全流量日志关联分析技术	态势感知平台

技术架构支撑

所需产品

序号	关键产品	核心功能
1	流量采集分配交换机	用于网络流量精确采集、汇聚、分配
2	网络蜜罐系统	实时捕获异常网络流量，实现黑客攻击转移、主动发现并记录内网黑客扫描、攻击、横向渗透
3	网络全流量深度威胁分析设备	识别未知威胁、高级威胁和异常流量
4	配套的全球威胁情报库、DNS/IP信誉库、规则库	用于检测大量的已知威胁
5	配套的大数据分析、建模、AI智能学习能力	基于大数据分析和AI智能学习技术，对全网数据进行分析、学习、建模，标识正常业务行为
6	配套的大容量存储空间	用于对完整的威胁进行回溯、取证、追踪溯源
7	网络海量日志集中监控平台	平台对全网网络安全事件进行统一监控、识别和响应
8	态势感知平台	安全资产盘点和集中展示
9	态势感知平台	将主机被入侵或攻击后的日志协同网络全流量日志进行关联分析

高级威胁：攻击范围、时间、技术方式均不可预测性

防护重点过渡到**加强检测和响应 (Detection & Response)**，核心技术从依赖规则发现单一攻击，演进到通过广泛的**全流量数据采集、分析技术**对攻击的检测、分析、溯源、处置；

提纲

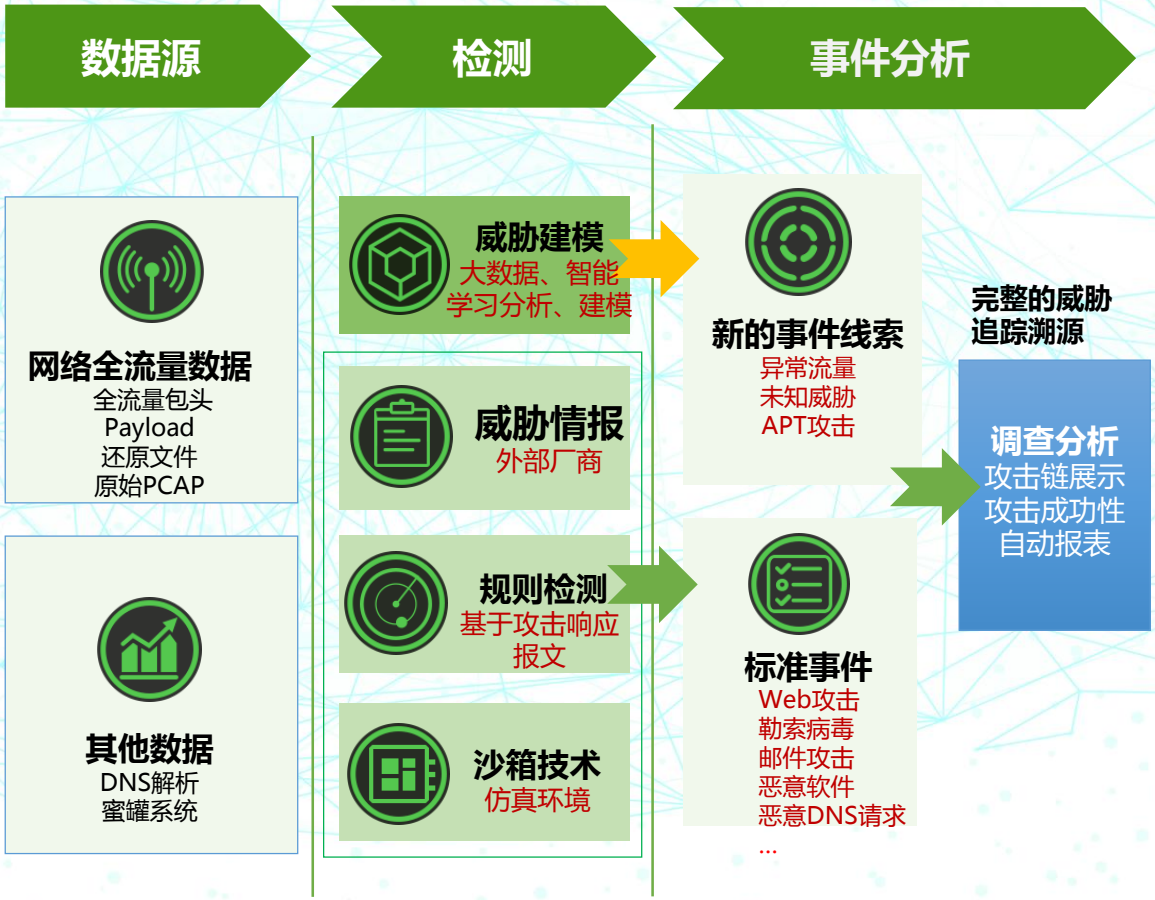
2 高级威胁检测体系建设

1. 技术架构支撑
2. 高级威胁检测方案设计
3. 其他保障方案

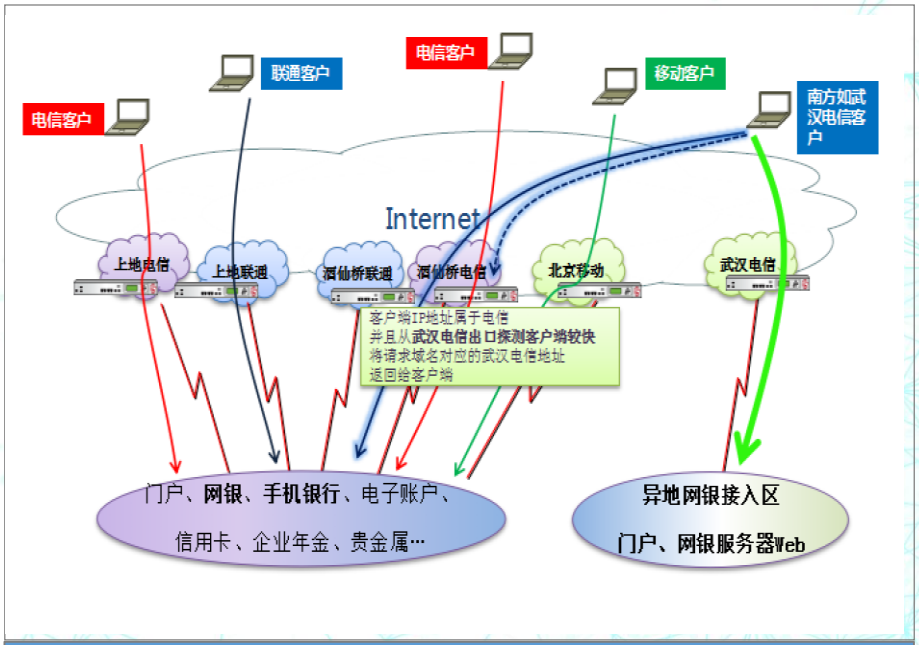
高级威胁检测方案设计

全面部署网络全流量深度威胁分析系统：

全面部署网络全流量深度威胁分析系统，根据现有技术发展趋势，基于大数据分析和AI智能学习技术，对全网数据进行分析、学习、建模，标识正常业务行为，同时结合外部威胁情报库、沙箱技术及规则检测引擎，能够识别已知威胁、异常流量和高级威胁，对攻击成功性进行跟踪，对完整的威胁进行追踪溯源。



高级威胁检测方案设计



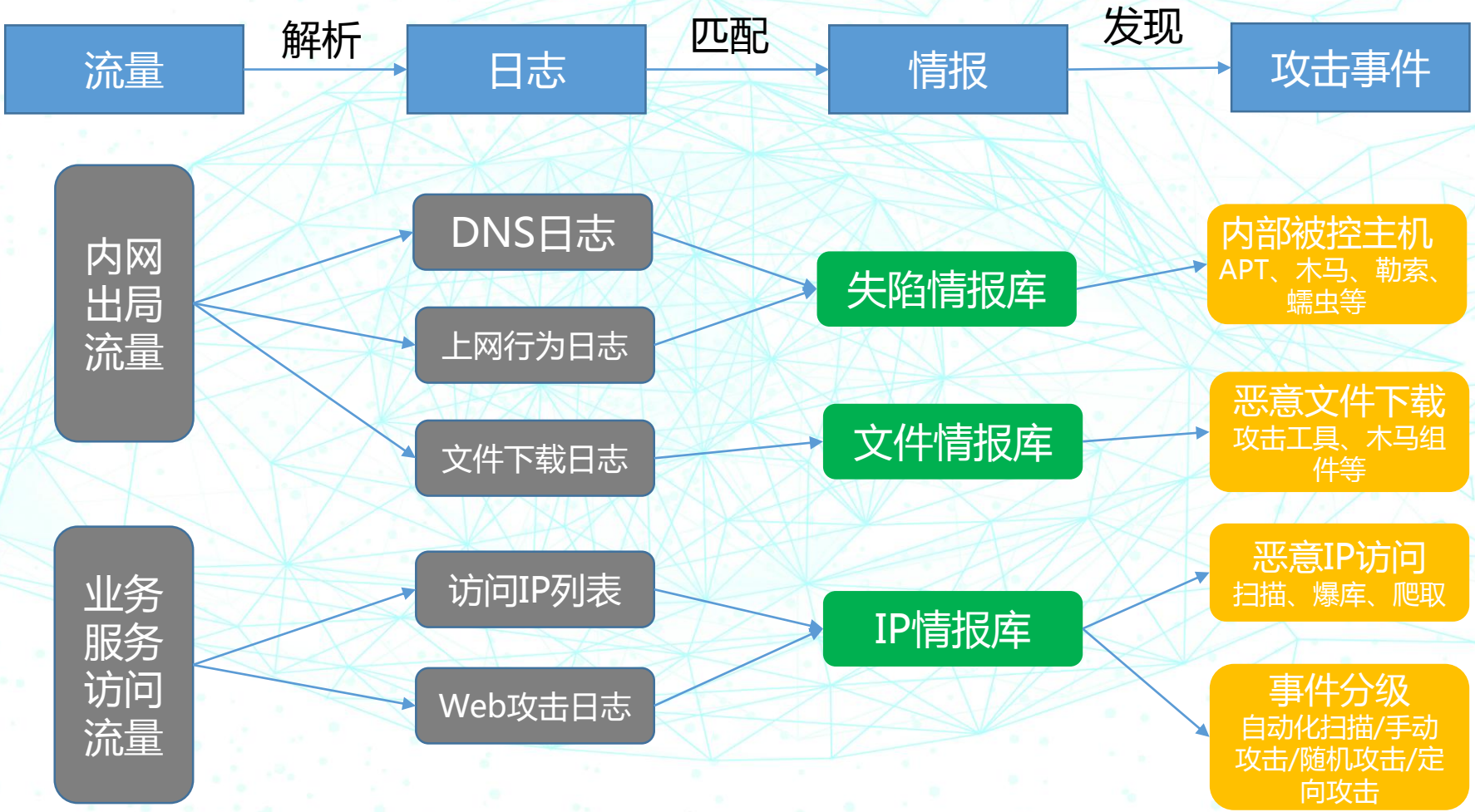
网络部署架构

Timestamp	Source Host	Destination Host	Threat Description	Det...	Protocol	Detection Severity	Attack Phase	Notable Object
2018-07-06 03:07:38	10.1.156.81	10.1.189.21	DNS response of a queried malware Com...		DNS Response	High	C&C Communication	Domain: a.vspcord.c...
2018-07-06 03:07:38	54.91.150.236	10.1.156.81	DNS response of a queried malware Com...		DNS Response	High	C&C Communication	Domain: a.vspcord.c...
2018-07-06 03:04:05	10.1.156.81	10.1.189.19	Possible CONFICKER DNS Response		DNS Response	Low	C&C Communication	Domain: hjwlkgsvrl.net
2018-07-06 03:03:29	199.127.56.82	192.168.1.226	CVE-2014-6278 - SHELLSHOCK HTTP Exp...		HTTP	Medium	Point of Entry	URL: http://106.37.1...
2018-07-06 03:03:28	199.127.56.82	192.168.1.226	CVE-2014-6278 - SHELLSHOCK HTTP Exp...		HTTP	Medium	Point of Entry	URL: http://106.37.1...
2018-07-06 03:03:21	199.127.56.82	192.168.1.226	CVE-2014-6278 - SHELLSHOCK HTTP Exp...		HTTP	Medium	Point of Entry	URL: http://106.37.1...
2018-07-06 03:03:20	199.127.56.82	192.168.1.226	CVE-2014-6278 - SHELLSHOCK HTTP Exp...		HTTP	Medium	Point of Entry	URL: http://106.37.1...
2018-07-06 03:03:18	199.127.56.82	192.168.1.226	CVE-2014-6278 - SHELLSHOCK HTTP Exp...		HTTP	Medium	Point of Entry	URL: http://106.37.1...
2018-07-06 03:03:18	199.127.56.82	192.168.1.226	CVE-2014-6278 - SHELLSHOCK HTTP Exp...		HTTP	Medium	Point of Entry	URL: http://106.37.1...
2018-07-06 03:03:17	199.127.56.82	192.168.1.226	CVE-2014-6278 - SHELLSHOCK HTTP Exp...		HTTP	Medium	Point of Entry	URL: http://106.37.1...
2018-07-06 03:03:16	199.127.56.82	192.168.1.226	CVE-2014-6278 - SHELLSHOCK HTTP Exp...		HTTP	Medium	Point of Entry	URL: http://106.37.1...
2018-07-06 03:03:14	10.1.156.82	10.1.189.19	Possible CONFICKER DNS Response		DNS Response	Low	C&C Communication	Domain: bmkrgprtiri...
2018-07-06 03:03:14	10.1.156.82	10.1.189.19	Possible CONFICKER DNS Response		DNS Response	Low	C&C Communication	Domain: bmkrgprtiri...
2018-07-06 03:03:10	199.127.56.82	192.168.1.226	CVE-2014-6278 - SHELLSHOCK HTTP Exp...		HTTP	Medium	Point of Entry	URL: http://106.37.1...
2018-07-06 03:03:09	199.127.56.82	192.168.1.226	CVE-2014-6278 - SHELLSHOCK HTTP Exp...		HTTP	Medium	Point of Entry	URL: http://106.37.1...
2018-07-06 03:03:08	199.127.56.82	192.168.1.226	CVE-2014-6278 - SHELLSHOCK HTTP Exp...		HTTP	Medium	Point of Entry	URL: http://106.37.1...
2018-07-06 03:03:08	199.127.56.82	192.168.1.226	CVE-2014-6278 - SHELLSHOCK HTTP Exp...		HTTP	Medium	Point of Entry	URL: http://106.37.1...
2018-07-06 03:03:07	199.127.56.82	192.168.1.226	CVE-2014-6278 - SHELLSHOCK HTTP Exp...		HTTP	Medium	Point of Entry	URL: http://106.37.1...

网络隐蔽信道检测

- **网络部署架构设计**：根据自适应安全体系建设思路，完成网络全流量深度威胁分析设备部署架构设计；
- **全面部署网络全流量深度威胁分析设备**：在总行互联网边界及内网关键区域全面部署网络全流量深度威胁分析设备，识别已知威胁、异常流量和高级威胁，提升网络高级威胁的检测防御能力；

高级威胁检测方案设计


流量
解析
日志
匹配
情报
发现
攻击事件
内网出局流量
业务服务访问流量
DNS日志
上网行为日志
文件下载日志
访问IP列表
Web攻击日志
失陷情报库
文件情报库
IP情报库
内部被控主机
APT、木马、勒索、蠕虫等
恶意文件下载
攻击工具、木马组件等
恶意IP访问
扫描、爆库、爬取
事件分级
自动化扫描/手动攻击/随机攻击/定向攻击

失陷主机检测

- **基于情报**
- 本地数据类型：DNS、HTTP代理、上网行为日志、
- 威胁情报类型：失陷检测（CnC）情报
- 价值—检测失陷主机：
  - APT攻击、僵尸网络、勒索软件、蠕虫木马、后门软件、黑客工具等
- 情报特点：
  - 检测精准：报警主机上基本确定有恶意软件并运行；
  - 详细上下文可以指导行动：风险级别、可信度、当前状态、Tag标记、发现时间、是否定向攻击、攻击团伙或者恶意家族的详情等；

也可以对出口报文全路径回放

基于海量报文存储、对基础设施能力有较高要求


```
"status": 10000,
"msg": "Success",
"data": [
  {
    "confidence": "high",
    "risk": "critical",
    "campaign": "APT-C-09",
    "targeted": true,
    "current_status": "active",
    "etime": "2017-04-11T15:34:39.000Z",
    "kill_chain": "c2",
    "platform": "generic",
    "alert_name": "APT-C-09 APT组织活动事件",
    "tag": [
      ""
    ],
    "ioc_category": "DOMAIN_PORT",
    "malicious_family": [
      "Unknown"
    ],
    "ioc": [
      "ciis-cn.net",
      "0",
      ""
    ],
    "id": "58ec870f2a33175de59d23a4",
    "malicious_type": "KNOWN APT"
  }
```

高级威胁检测方案设计

AV报警确认/优先级

- 本地数据类型：AV或防毒网关的报警日志（MD5、SHA1）
- 威胁情报类型：文件信誉
- 价值—报警确认：
  - 恶意的可执行文件（僵尸网络、勒索软件、 攻击利用套件、木马程序、流氓推广、 恶意病毒、后门、 间谍软件、广告软件、漏洞利用程序等）
- 情报特点：
  - 检测精准：云端多引擎、沙箱、白名单、机器学习、人工分析等多种；
  - 详细上下文可以指导行动：家族信息、恶意类型、文件类型、发现时间等；

杀链分析

- 本地数据类型：文件传输日志、主机进程链、网络行为日志
- 威胁情报类型：高级文件信誉
- 价值：威胁检测、杀链分析
  - 通过文件传输、邮件、主机进程等方式检测恶意文件；
  - 通过文件信誉中的网络行为及IOC，检测恶意软件感染面及回联通信
- 情报特点：
  - 检测精准：云端多引擎、沙箱、白名单、机器学习、人工分析等多种；
  - 更多上下文：域名解析、TCP/UDP会话、URL、IOC等

高级威胁检测方案设计

业务服务器攻击分析/响应

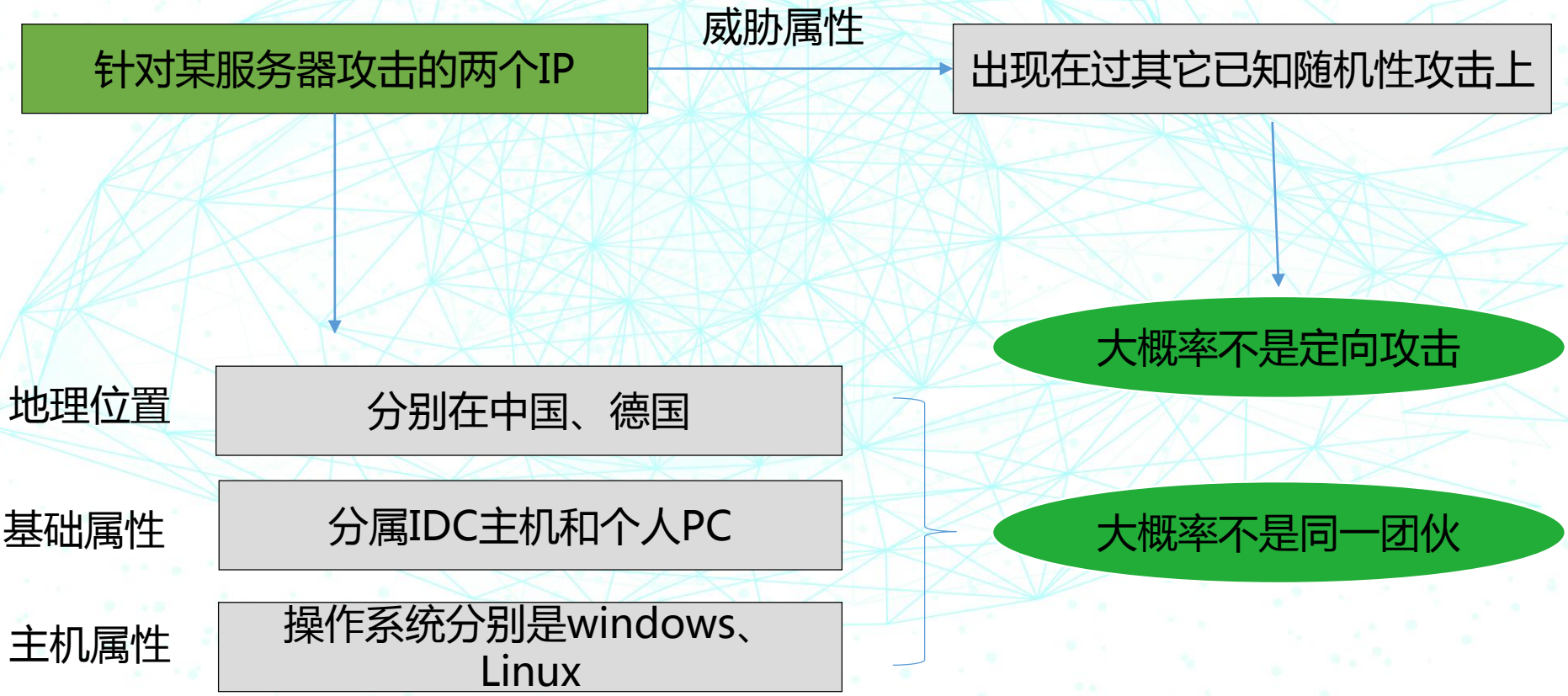
- 本地数据类型：对外业务服务器前IPS、WAF报警日志
- 威胁情报类型：IP信誉
- 价值：攻击分析、白名单
  - 对攻击性质做判断；
  - 查询基础属性，确定是否可以拦截；
- 情报特点：
  - 检测精准：10多种维度数据表述一个IP的信息；
  - 覆盖全：来源数据广

IP情报

- 地理位置，所属ASN组织；
- 僵尸主机
- 基础属性：网关、个人主机、IDC主机、未启用IP等
- 威胁属性：
  - 何时
  - 何种攻击手段
  - 相关网站行业

IP情报：分析样例

- 检测：检测或拦截已知黑IP
- 分析：



全面建设网络蜜罐体系

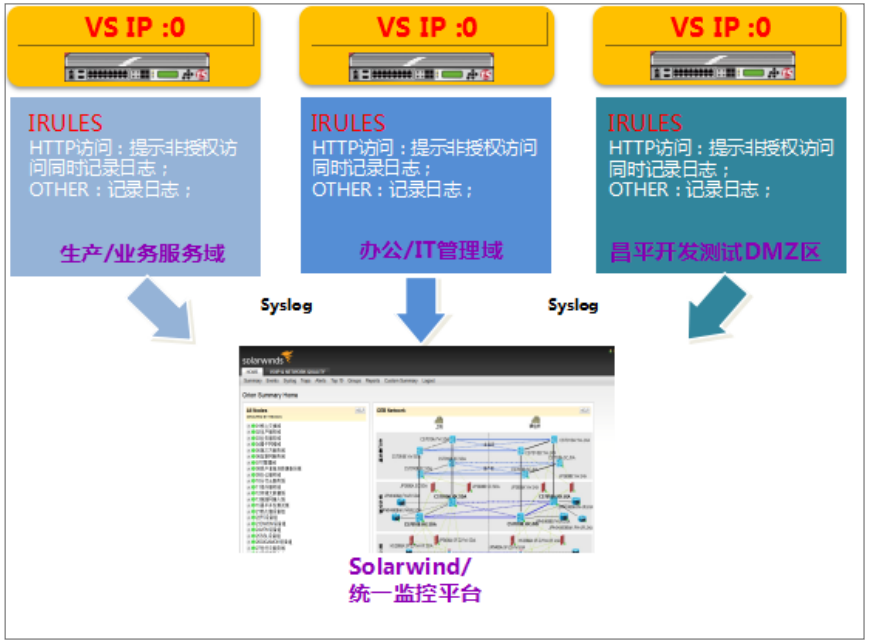
结合主动式和被动式蜜罐特点，完成数据中心**五类蜜罐体系**部署实施，实现主动发现并记录内网黑客扫描、攻击跳板、企业黑产、异常DNS请求、主机异常连接等行为。

五类网络蜜罐系统即五类不同的异常流量检测探针，目前已成为网络高级威胁发现的重要抓手，未来仍将持续探索和扩展。

F5VS蜜罐

目前在银行架构中广泛使用F5负载均衡设备，考虑到内网安全，我们**利用现有各区域F5负载均衡设备做二次开发，**通过F5将流量初级分类，实现与高交互蜜罐联动，可对扫描和精确攻击进行分类分析，实现上万种应用的持续监控，截止目前已覆盖总行10多个网络区域，检测到多次异常访问行为。

网络蜜罐体系



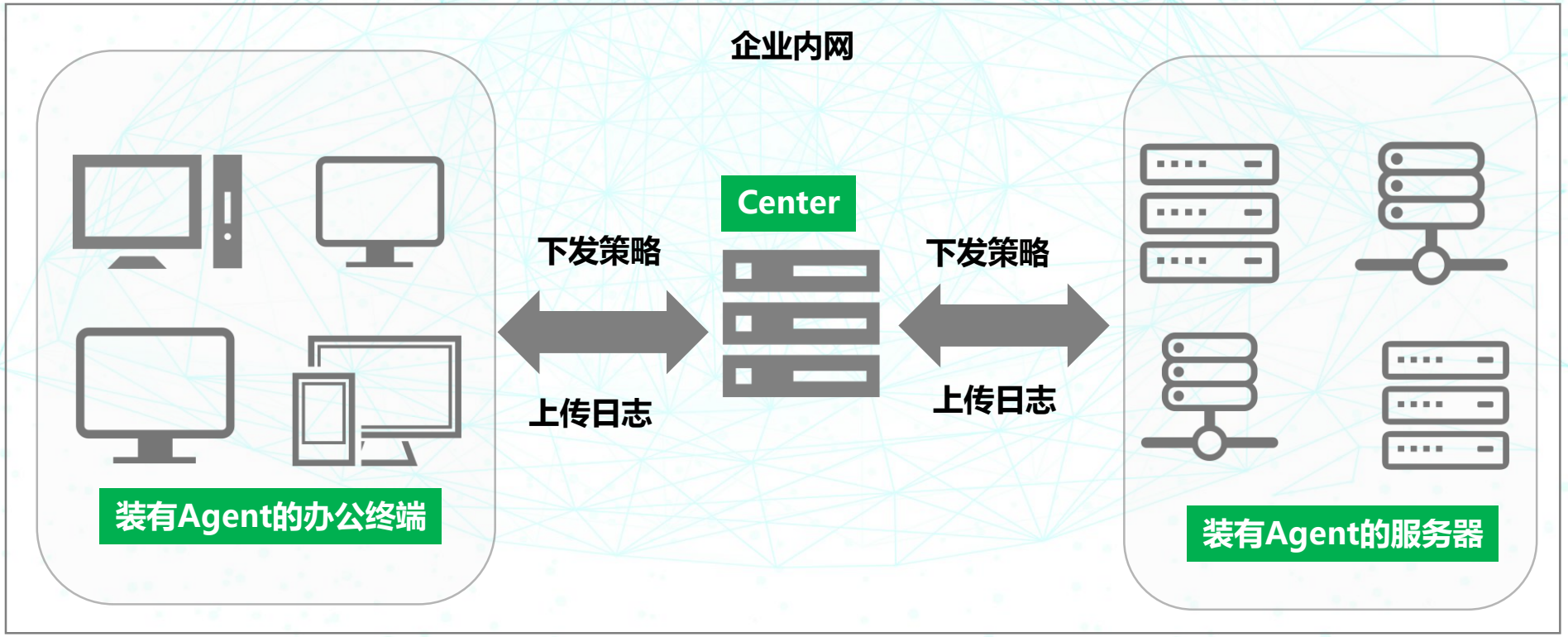
F5 VS蜜罐

检测技术及方案设计

全面部署自适应安全监测系统：

目前在互联网边界全面部署自适应安全监测系统，具备主机**微蜜罐**功能，Agent以软件形势部署在内网主机上，通过伪装多种应用服务及蜜罐文件，检测黑客对内网的渗透攻击行为；Center管理服务器端以软件形式部署在企业的内网服务器上，进行Agent行为日志的统一收集、分析和预警；

同时可作为**安全检测底线**，实现主机异常提权、反弹shell等安全入侵行为的实时监测及预警；



检测技术及方案设计

- 威胁情报和Threat Hunting
  对外业务服务器前IDS、IPS、WAF报警日志，通过匹配威胁情报中的IP信誉对攻击性质做判断；通过查询基础属性，确定是否可以拦截；

安全狩猎

52%
发现之前未检测到的威胁

74%
减少攻击面

59%
提升响应的速度和精度

来源: “Threat Hunting: Open Season on the Adversary,” Robert M. Lee, SANS Institute, 2016

提纲

2 高级威胁检测体系建设

1. 技术架构支撑
2. 高级威胁检测方案设计
3. 其他保障方案

其他保障方案

持续响应

根据目前的运维经验，提升应急响应效率，需有足够手段对发现的问题进行准确判断，依赖于大数据关联分析、安全资产梳理、主动漏洞验证及应急处置闭环流程。

大数据关联分析

面对检测发现的**海量告警**，需要态势感知平台对全网网络安全事件进行统一监控、识别和响应，依托大数据关联分析技术，实现全网安全日志的过滤筛选合并、智能关联和智能判断；

安全资产梳理

同时需要对全网安全资产进行**准确梳理和全面管理**，如IP、OS、系统进程、软件清单、中间件版本、应用版本等，展示安全资产相关的风险量化评级；

应急处置闭环流程

建立网络安全事件闭环跟踪流程，形成事件检测、响应、处置、审核的应急**处置闭环**流程；

主动漏洞验证

对于网络检测发现的异常流量事件，**主动进行漏洞验证**，验证系统漏洞情况，并制定漏洞修复计划，纳入应急处置闭环流程，规避风险隐患；

其他保障方案——态势感知平台建设

- 态势感知平台作为全网安全管理平台，可集中展现全网安全状态和全网风险预警信息；
- 结合系统部署位置、操作系统、服务协议、安全基线配置、漏洞情况、修复情况、修复周期、**外部威胁情报**及其他安全风险指标对系统运行风险进行安全量化评分、统一展示，统一视图各团队重点关注；
- 安全资产的全面管理，可直观展示安全资产的全部信息，如IP、OS操作系统、系统进程、软件清单、中间件版本、应用版本等重要资产信息，可支持一键搜索，实现安全资产信息快速定位；

其他保障方案——加强漏洞修复空档期安全保障

1、完善漏洞管理体系

漏洞修复空档期即经过评级处于高风险且在一定时间内无法修复的系统漏洞，将检测策略部署在专业安全设备/应用级检测设备上，从网络维度重点关注跟踪漏洞修复空挡期风险利用情况；

2、定制网络检测策略

--网络全流量深度威胁检测设备针对重点漏洞特征定制网络安全检测策略；
--互联网边界系统全面部署云安全监测系统，作为安全底线实现主机异常提权、反弹shell等安全入侵行为的实时监测预警；

4、建立威胁回溯机制

--基于网络报文回溯、取证技术，建立完整的威胁漏洞利用回溯、取证、追踪确认机制；
--基于攻击响应报文进行分析，对攻击成功性进行跟踪判断；
--基于专业的IP信誉库，加强对攻击源ip的分析判断，如微步在线、360应急响应中心；

3、强化安全阻断手段

--网络一线按照预案要求，第一时间封堵恶意攻击ip源地址；
--WAF应用防火墙定制安全策略实现恶意攻击的拦截阻断；

提纲

3 安全生态，合作共赢

1 行业技术局限性分析

2 安全生态，合作共赢

行业技术局限性分析

技术方面

1.误报率较高；
2.规则覆盖面不全；
3.异常流量智能捕获和存储能力较弱；
4.威胁建模、大数据分析能力不足；

运营方面

1.海量告警如何逐一响应；
2.全国推广部署后，多家厂商产品如何运营，日志如何统一分析；

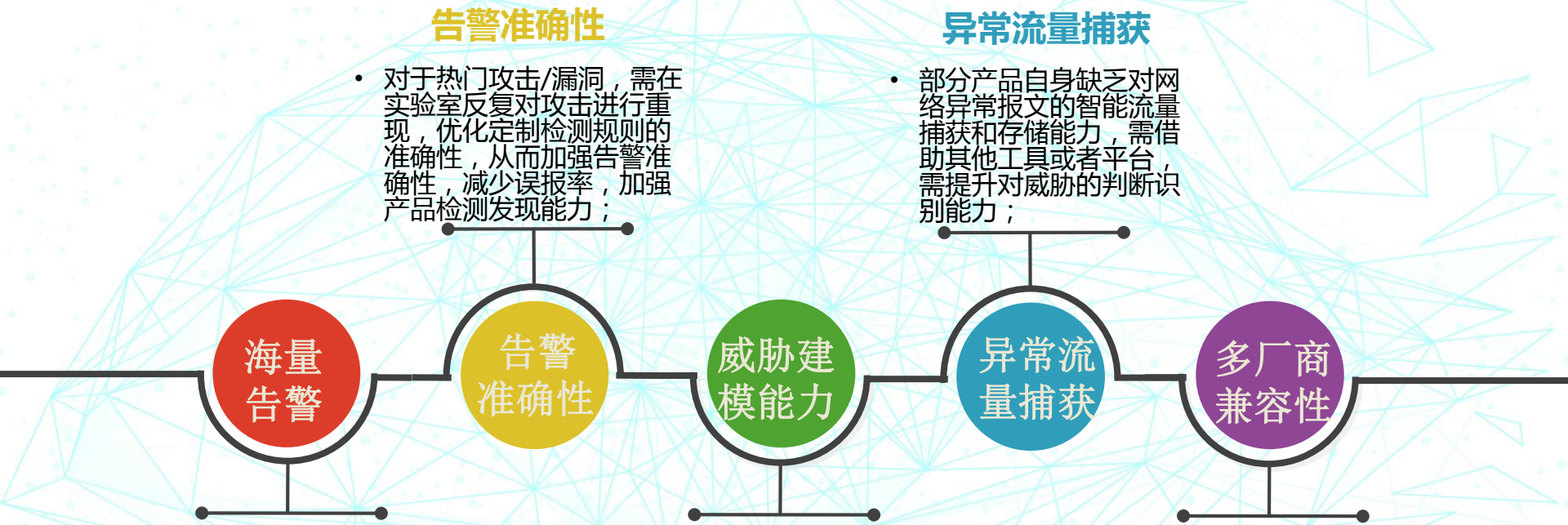
产业方面

1.各厂商没有统一标准；
2.各厂商日志格式、检测性能不统一，没有一个平台能统一加工处理；

行业技术局限性分析

技术局限性

根据日常安全运维经验，目前市面上各类高级威胁检测产品均存在一定的技术局限性，本次站在用户的角度，对行业及安全厂商提一些技术、产业相关的建议。



告警准确性

- 对于热门攻击/漏洞，需在实验室反复对攻击进行重现，优化定制检测规则的准确性，从而加强告警准确性，减少误报率，加强产品检测发现能力；

异常流量捕获

- 部分产品自身缺乏对网络异常报文的智能流量捕获和存储能力，需借助其他工具或者平台，需提升对威胁的判断识别能力；

海量告警

- 高级威胁检测不能停留在IDS层面，不能仅仅是检测到威胁就告警，应对攻击成功性进行智能判断，针对指定攻击特征报文的特定响应才触发告警；
- 同时支持对告警日志分类汇聚，优化减少日常告警数量；

威胁建模能力

- 目前厂商技术主要集中在对于异常的分析能力，应加强对正常业务的学习和建模，标识出正常业务流量；

多厂商兼容性

- 目前各厂商没有统一的标准规范，现阶段是各做各的，缺乏统一标准，没有形成合力，从而导致多厂商兼容性问题，导致各厂商日志格式、检测性能不统一，没有一个平台能统一加工处理；

提纲

3 安全生态，合作共赢

1 行业技术局限性分析

2 安全生态，合作共赢

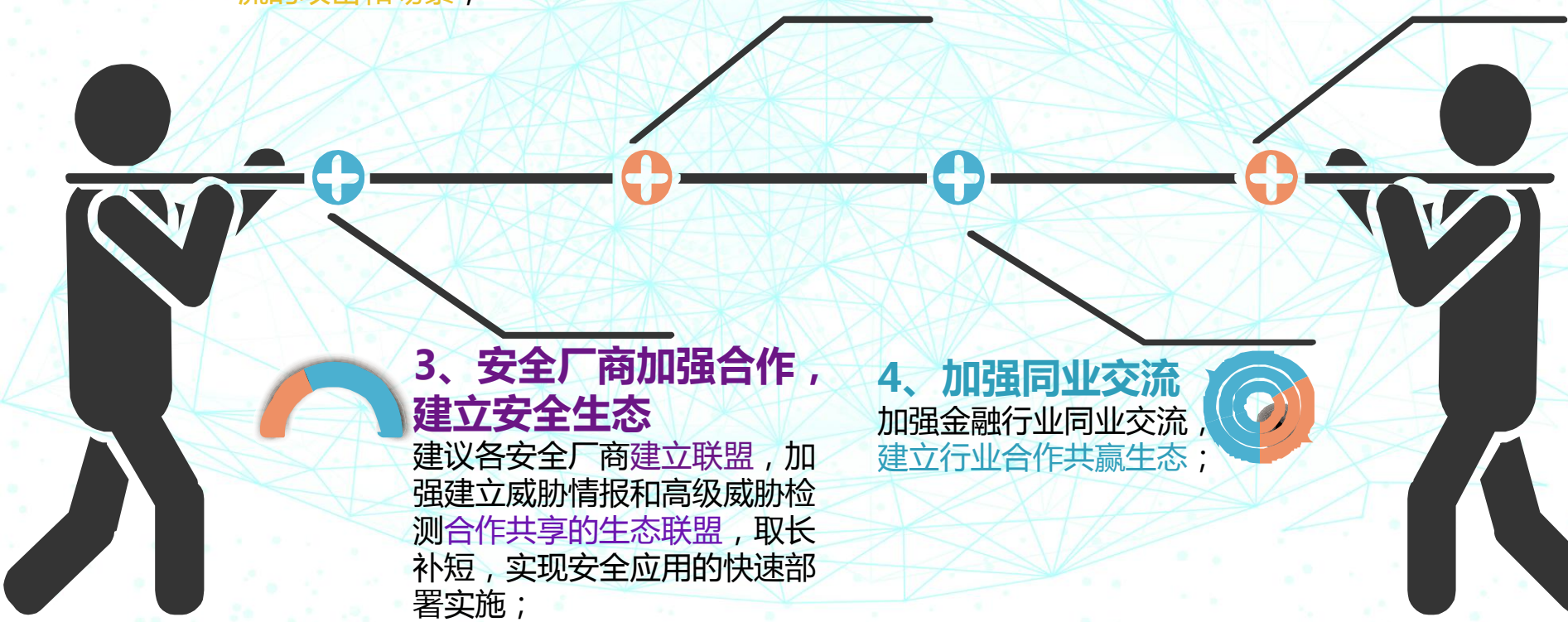
共建安全生态，合作共赢

1、加强外部厂商合作

规则库、威胁情报需定期不断更新，加强外部厂商合作，对新型的威胁进行即时更新响应，尽可能覆盖主流的攻击和场景；

2、加强企业内部合作

企业内部各部门分工明确，深入合作，实现企业内部的联防联控机制；



3、安全厂商加强合作，建立安全生态

建议各安全厂商建立联盟，加强建立威胁情报和高级威胁检测合作共享的生态联盟，取长补短，实现安全应用的快速部署实施；

4、加强同业交流

加强金融行业同业交流，建立行业合作共赢生态；

共建安全生态，合作方能共赢

创新智造 光大未来

谢谢观赏！

360威胁情报中心