金睛云华 AI驱动安全

CSA GCR cloud security alliance GREATER CHINA REGION

亚信安全

CSA研讨会

XDR的无限可能

数字时代

金睛云华
AI 驱动安全
CSA GCR cloud security
GREATER CHINA REGION alliance
亚信安全

AI驱动的XDR解决方案及安全运营服务

演讲人：北京金睛云华科技有限公司 胡文友

讲师介绍

胡文友　　金睛云华联合创始人&市场 副总裁

- 20年网络安全从业经验，对网安行业有深刻理解
- 历任启明星辰天清汉马FW/UTM第一任产品经理
- 华为-赛门铁克安全产品线中国区行销代表
- 华为全球解决方案部CTO Office首席安全顾问
- 华为与建行、海关总署战略合作安全领域总技术负责人

金睛云华
AI驱动安全

CONTENTS

01 痛点分析

02 解决方案

03 安全服务

04 核心技术

05 成功案例

金睛云华
AI驱动安全

/01 痛点分析

Pain points analysis

痛点一：传统安全产品越来越无效

金睛云华
AI驱动安全

未知威胁层出不穷

- 零日漏洞公开叫卖，高级逃逸躲避手段日新月异
- 传统基于签名的检测技术对未知威胁失效

道高一尺，魔高一丈

APT挑战安全极限

- 手段组合，长期潜伏，迂回渗透，无孔不入
- 对整个安全体系构成全面、长期、艰巨的挑战

不怕贼偷，就怕贼惦记

加密流量越来越多

- 黑客常常利用加密技术进行网络通讯
- 流量一旦被加密，传统基于特征检测的安全产品全部失效

传统安全手段越来越无效

IDS误报率居高不下

- IDS与FW联动技术在实际应用中很少有人敢启用
- IPS的默认响应方式大多为只报警不阻断

狼来了”的故事重复上演

安全成为性能瓶颈

- 安全设备对硬件的开销要远高于网络设备
- 串联多个安全设备无异于拒绝服务攻击

没有效率的安全不是好安全

被动防范落后于人

- 安全技术发展总是落后于威胁技术发展
- 被动防范只能是坐以待毙，亡羊补牢

落后就要挨打

痛点二：“人”成为最大的成本及短板

金睛云华
AI驱动安全

安全分析人员的培养时间长，当前人才缺口极大

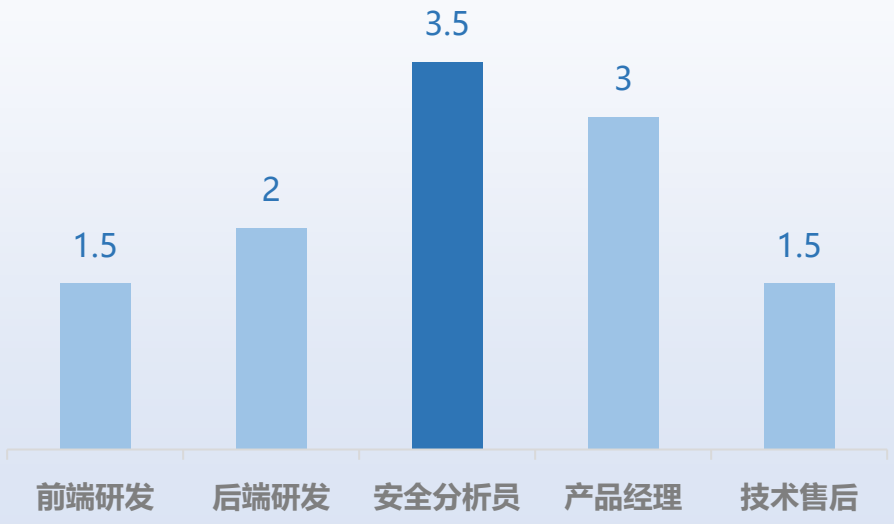
- 根据2021年《网络信息安全产业人才发展报告》，我国网络安全专业人才缺口超140万人，而目前每年全国高校网络安全相关专科、本科和研究生培养人才数量不足2万人；
- 根据教育咨询机构麦可思的研究报告，自2014届开始，信息安全反超建筑学成薪资最高专业，并连续七年成为本科主要专业中月收入最高的专业；
- 安全分析人员总量长期匮乏，势必造成总体薪资价格/成本偏高。

安全分析方向分类多，各有专精，很难配齐

- 攻防渗透工程师、漏洞分析员、二进制逆向分析员、安全运维分析员……约十余个细分类别；
- 安全厂商与甲方客户，都难以配齐全部类型的安全分析人才，造成安全能力的瓶颈和短板。

如下图行业普遍情况所示

安全分析人员是最大的成本单元



安全人员平均月薪（万元）

金睛云华
AI驱动安全

/02 解决方案

solution

AI驱动的XDR解决方案&安全运营服务

金睛云华
AI驱动安全

智慧安全运营
AISecOps

赋能 反哺

扩展检测与
响应XDR解决方案

赋能 反哺

核心能力

云托管检测与响应服务（CMDR）

MSSP-SOAR
托管安全服务平台-精密编排的快速恢复补救

检 测

高级威胁发现

- **ATD** (NDR)
  高级威胁检测系统
- **ADS** (NDR)
  智能欺骗系统
- **HTD** (EDR)
  终端威胁检测&取证

可疑威胁

分 析

安全运营事件管理

- **MSSP-CIC** (MDR)
  托管安全服务平台
  托管检测与响应模块

高级威胁分析

- **CTI**
  威胁情报平台

网络取证

- **TFS** (NDR)
  全流量威胁取证系统

主机取证

- **HTD**
  终端威胁检测与取证

响 应

网络响应

- **AI-FW** (生态合作)
  AI防火墙

主机响应

- **HTD** (EDR)
  终端威胁检测与取证

AI算法模型与海量网安数据

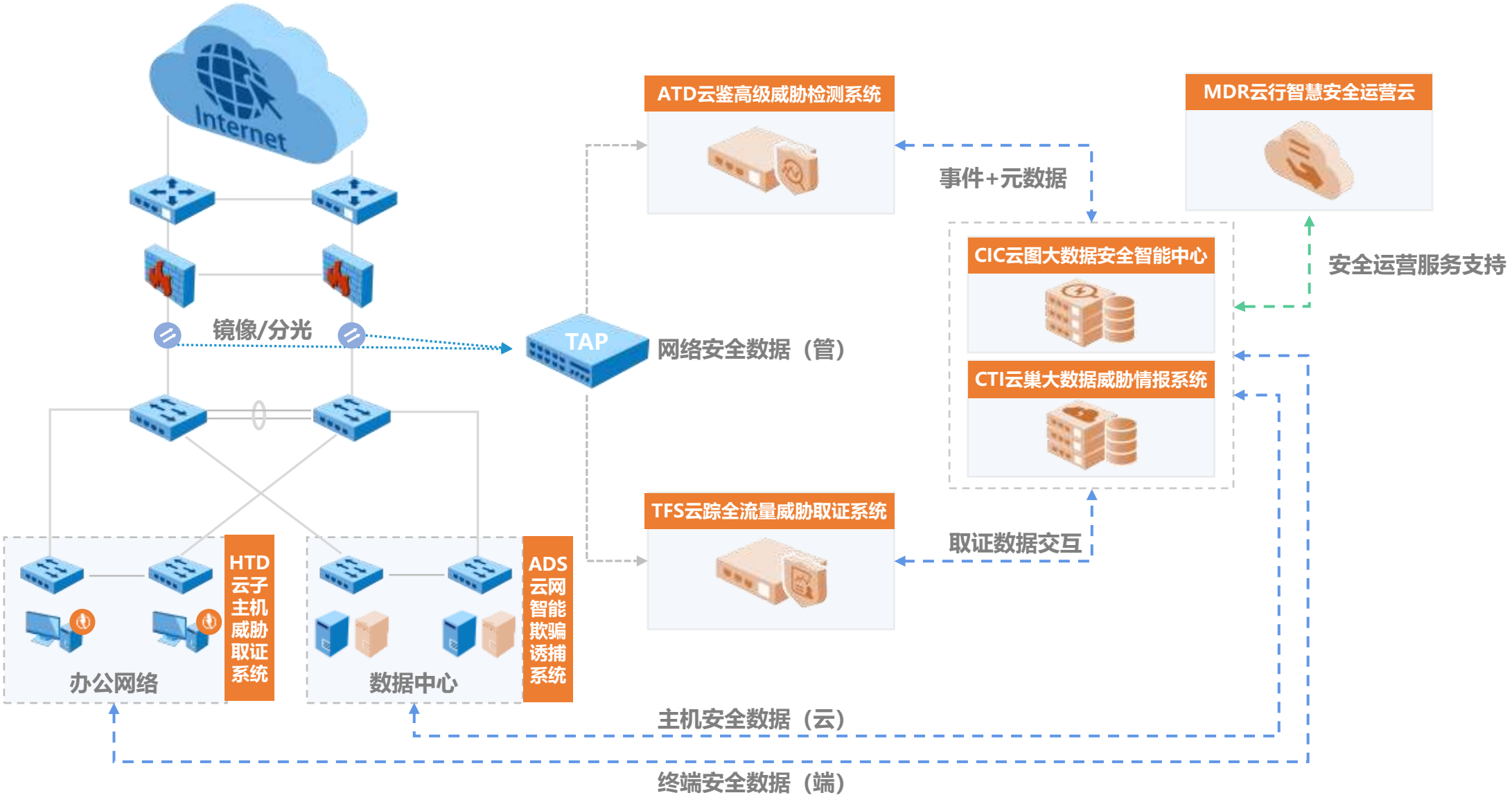
流量与文件威胁检测能力

流量引擎与全包存储能力

大数据处理与关联分析能力

XDR部署方案

金睛云华
AI驱动安全



XDR的核心是用机器学习替代特征签名技术

金睛云华
AI驱动安全

资产	**网络**	**主机**
传感器	**流量**	**终端**
需求	等保合规-->可服务性-->覆盖率	
	IDS-->NTA-->NDR	AV-->EPP-->EDR
方法论基石	以特征签名为基石的传统网络安全防御体系，本质上，依靠一个小团队对抗全球的攻击者？	

Gartner

Gartner：Market Guide for Network Detection and Response

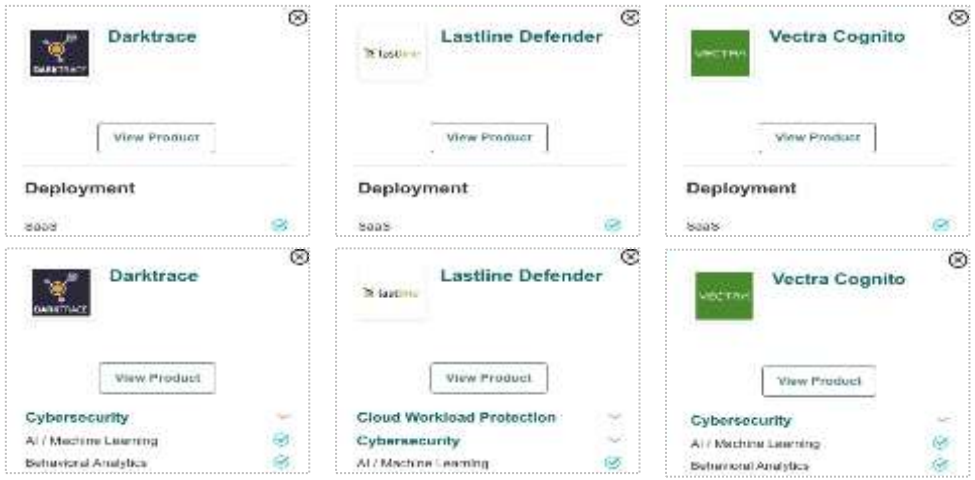
Market Definition

This document was revised on 6 April 2022. The document you are viewing is the corrected version. For more information, see the Corrections page on gartner.com. NDR solutions primarily use non-signature-based techniques (for example, machine learning or other analytical techniques) to detect suspicious traffic on enterprise networks.

Gartner：Market Guide for Extended Detection and Response

Modern security is a data-heavy exercise,and competent XDR providers will have extensive and cost-effective data storage,analytics and machine learning(ML) capabilities.

国外友商



NDR演进分析

金睛云华
AI驱动安全

IDS/IPS

基于签名特征库的网络实时流量检测

单一的流量检测产品
（等保合规）

NTA

① 基于签名特征库的网络实时流量检测；
② 应用层协议解析元数据提取；
③ 情报检测；
④ 文件还原&威胁检测；
⑤ 汇聚、关联和分级等；
⑥ 异常行为检测。

综合的流量检测产品
（可服务性和覆盖性）

NDR

① 可服务性和覆盖性；
② 以AI检测为主，重点检测威胁变种和未知威胁；
③ 响应，强调检测能力闭环和联动阻断。

NTA+AI
（强调检测威胁变种和未知威胁）

EDR演进分析

金睛云华
AI驱动安全

AV

基于签名特征库的病毒查杀

单一的杀毒产品

EPP

① AV
② 情报
③ 终端防火墙
④ 数据丢失保护
⑤ 数据加密

综合的终端防护产品

EDR

① 轻终端（CPU、内存、IO、网络带宽等），重平台；
② 以AI检测为主。

AI+轻终端+重平台

金睛云华
AI驱动安全

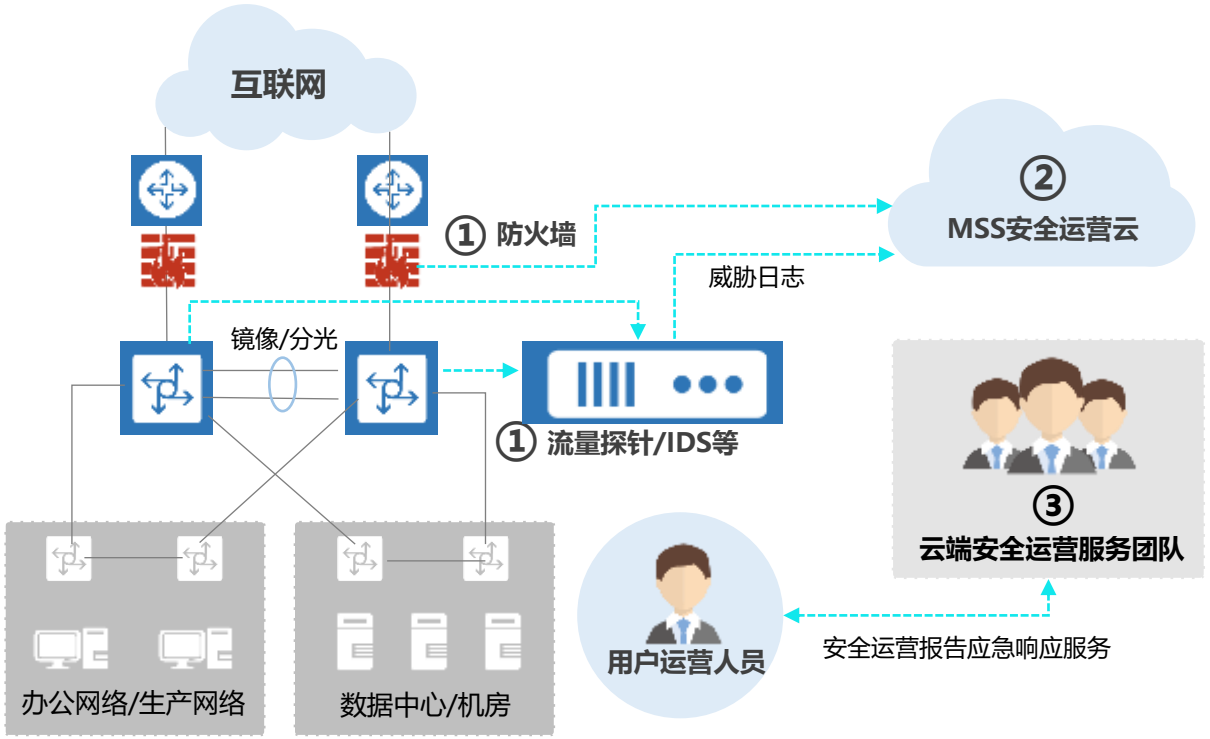
/03 安全服务

security service

AISecOps-1：托管安全服务（MSS）

金睛云华
AI驱动安全

托管安全服务（Managed Security Service）借助于用户侧多种网络安全设备与系统的日志数据与MSSP云端托管安全运营服务平台能力，实现对用户网络安全运营工作的托管运营，减轻用户安全运营负担，提升用户网络安全风险事件的响应与处置能力。

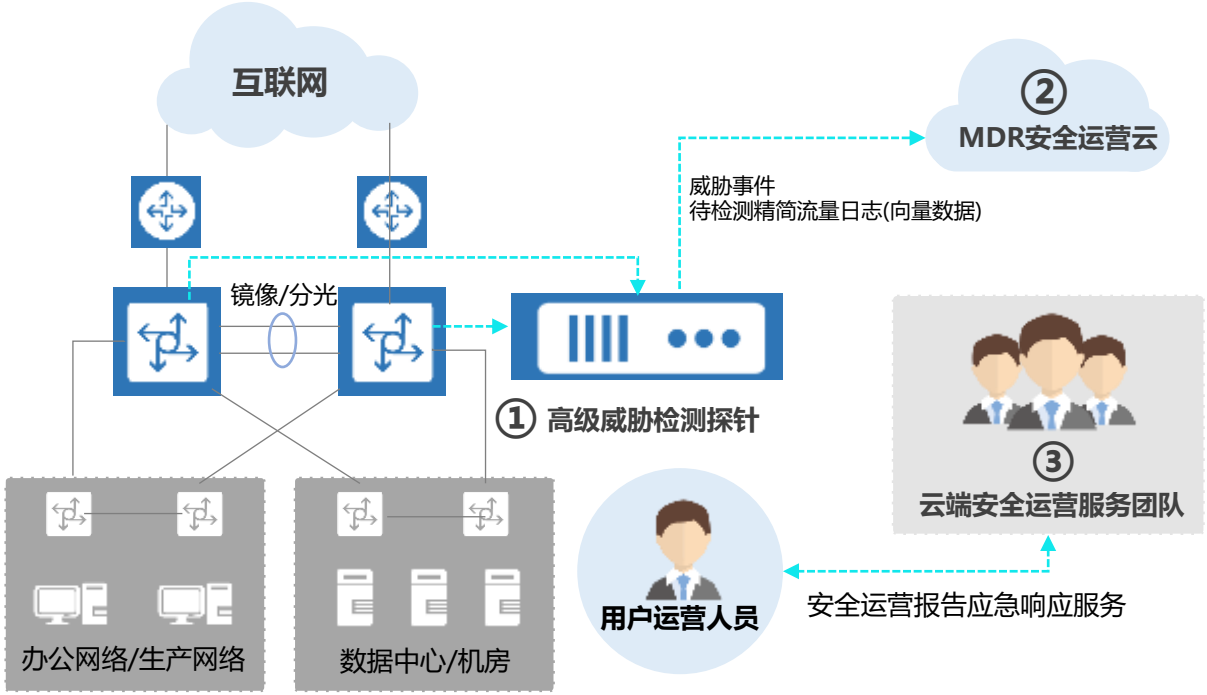


- 利旧现有网络安全数据
- 整合多元数据，洞悉风险
- 全网资产安全态势可视
- 云端全面及时的服务
- 多租户环境及数据安全
- 平滑扩展至MDR服务

AISecOps-2：托管检测与响应服务（MDR）

金睛云华
AI驱动安全

托管检测与响应（Managed Detection and Response），Gartner将其描述为企业希望获得7x24小时连续不间断的网络安全事件监测和分析，快速发现威胁与有效响应的托管安全服务。大多数MDR服务是通过主机层与网络层的威胁监测与分析技术，生成、收集安全事件以及上下文数据，结合安全运营平台的数据分析技术和安全运营专家的技术力量共同完成。金睛云华托管检测与响应服务（MDR-as-a-Service）借助于多功能融合的高级威胁检测探针与云端托管运营能力，为用户提供实战化的威胁检测与响应运营服务。



- 高度集成化的高级威胁检测探针
- 基于复杂攻击场景和APT攻击链的关联分析
- 云端全面及时的服务
- 精准的威胁事件监测与运营分析
- 云上，云下全网资产安全态势可视
- 隐私数据安全

AISecOps-3：云托管检测与响应服务（CMDR）

金睛云华
AI驱动安全

云托管检测与响应服务（Cloud Managed Detection and Response）借助于用户在公有云多种环境中的网络安全设备与系统的日志数据与CMDRP云托管检测与响应服务平台能力，实现对用户在公有云中的网络安全运营工作的托管运营，减轻用户安全运营负担，提升用户公有云中业务系统的网络安全风险事件的响应与处置能力。

- 针对公有云提供丰富的网络安全运营服务
- 为公有云环境的自研安全工具及平台
- 基于最佳实践的自动化加固与评估
- 规范的安全运营流程
- 专业的服务运营团队提供服务

/04 核心技术

core technology

核心技术--AI驱动的高级威胁检测分析

金睛云华
AI驱动安全

机器 … 学习

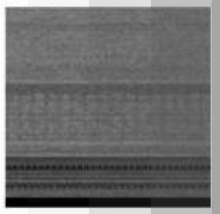
1. 恶意文件映射

APT28-Kazy

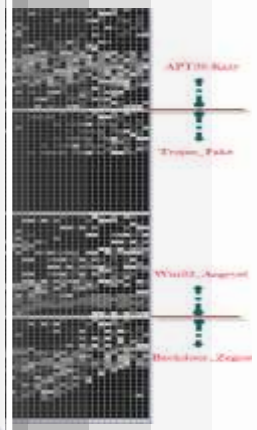
010101010000101101…… + 1

01010101, 00001011, … +

85 11 67 26 132 32 54 … +



样本4



3. 其他安全数据

- **Web攻击载荷**

  /law/list.asp?keywords=

- **网络钓鱼URL**

  https://kuljitrehal.com/b

- **沙箱行为日志**

  {"I":59,"C":2088965442,"F

  leHandle","h"],"HandleN

  m8=","$type":"00"}]}

- **DGA域名**

  dksmdvjfgpwt.net; dksmdvjfgpwt.ru; dns.msftncsi.com; ebcfuwemulkk.com; ebcfuwemulkk.in; ehidpbbpxxxs.in; ehidpbbpxxxs.net

a7 \x84

gs":["is_success","retval",["Fi

,"$type":"00"},{"$binary":"b

速报，微软英特尔联手给恶意软件拍"X光"？

零日情报局

最近，微软和英特尔合作开展了一个新的安全研究项目——STAMINA（STAtic Malware-as-Image Network Analysis），将未知软件转化为图像，通过图像扫描法进行检测分析。简单点说，就是给疑似恶意软件拍"X光"，然后专家们可以根据这张"X光片"判断是不是真的恶意软件，以及是哪种恶意软件。

首先，将未知软件转换为简单的01010像素流；

接着，按照软件的原始数据流，转换成一张图片，图片尺寸随文件大小而变化；

然后，有了图片版的软件，就可以把他们丢进神经网络(DNN)进行"X光"扫描；

再然后，经过全方位透视的扫描，图像版软件就被神经网络(DNN)划分为干净和已感染两大类；

最后，分类完毕之后，就是生成该软件的"X光"分析以及专家后期的人工分析。到这一步就可以确定，可疑软件是不是真恶意软件，以及是什么种类的恶意软件，并提供包括准确性、误报率、召回率、F1分数和接收器工作曲线的详细分析。

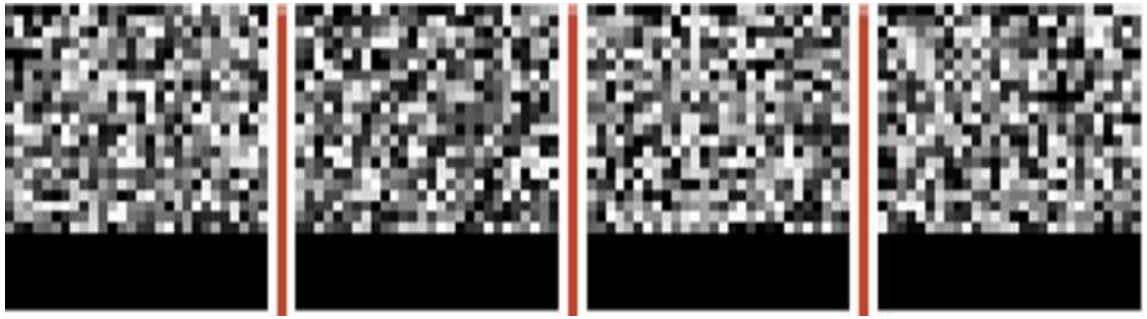
明白了微软英特尔给可疑恶意软件拍X光的全流程，再说说STAMINA技术把可疑软件从.exe变.jpg中，一个值得注意的隐藏亮点。

那就是这种技术处理可疑软件时，不需要全尺寸，逐像素的重建，这对处理大型可疑恶意软件是个好消息，当然现阶段技术还没有完全成熟到这种程度。不过，从目前超过99.07%的分类准确率，以及低于2.6%的误报率来看，STAMINA堪称全能恶意软件"X光扫描机"。

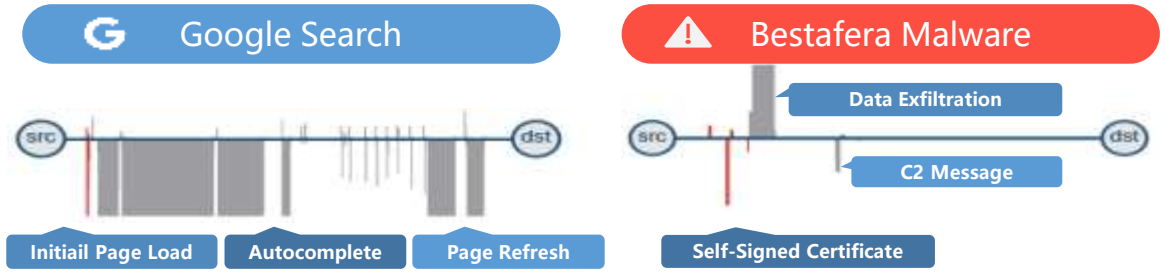
（可疑恶意软件重建图片尺寸调整方法）

核心技术--AI技术做恶意加密流量分析

金睛云华
AI驱动安全



恶意加密流量的流量基因指纹是随机的，加密算强度越高随机熵值就越高。因此，对加密流量Payload的特征检测和流量基因检测都会失效



合法加密流量和恶意加密流量在网络行为上差异较大，主要表现在3层包行为、TLS握手特征和行为，以及应用层协议关联行为等方面

基于恶意代码通讯模块建模的理念，提出步态指纹概念，实现的检测模型：

① 恶意加密流量检测模型
② VPN流量以及业务识别模型
③ Tor流量以及业务识别模型
④ 翻墙流量以及业务识别模型
⑤ 其他定制化的模型

竞争优势：大数据+人工智能+网络安全

金睛云华
AI驱动安全

No.	应用	AI技术	交叉验证准确率
1	文件基因图谱检测	基于基因图谱及深度学习模型检测恶意代码变种	97.77%
2	流量基因图谱检测	基于基因图谱及深度学习模型检测未知协议恶意流量	98.12%
3	恶意加密流量检测	采用集成学习模型检测恶意程序的加密通讯行为	98.23%
4	暗网（Tor）通信检测	采用步态指纹技术以及深度学习模型检测暗网通信行为	99.12%
5	ShadowSocks通信检测	采用步态指纹技术以及深度学习模型检测Shadowsocks通信行为	96.54%
6	VPN通信检测	采用步态指纹技术以及深度学习模型检测VPN通信行为	96.63%
7	DNS隐秘隧道检测	采用集成学习模型对于DNS隧道数据外泄进行检测	99.83%
8	ICMP隐秘隧道检测	采用集成学习模型对ICMP隧道数据外泄进行检测	97.45%
9	HTTP隐蔽隧道检测	采用集成学习模型对于HTTP隧道数据外泄进行检测	96.18%
10	HTTPS隐蔽隧道检测	采用集成学习模型对于HTTPS隧道数据外泄进行检测	95.21%
11	动态沙箱恶意行为模式库构建	采用频繁项集挖掘算法构建沙箱恶意行为模式库	不涉及
12	DGA域名检测	采用集成学习模型对于DGA域名进行检测	98.94%
13	仿冒域名检测	采用距离和异常模型对仿冒域名进行检测	93.21%
14	Web攻击检测--XSS攻击	基于深度学习及强化学习框架对XSS攻击进行持续建模和检测	96.11%
15	Web攻击检测--SQL注入	基于集成学习及强化学习框架对SQL注入进行持续建模和检测	96.89%
16	Web攻击检测--Webshell	基于深度学习及强化学习框架对Webshell进行持续建模和检测	96.20%
17	命令执行攻击检测	利用深度学习对混淆的命令执行进行建模检测	99.13%
18	代码执行攻击检测	利用深度学习对混淆的代码执行进行建模检测	98.59%
19	Cobalt Strike的通信检测	基于集成学习的CS渗透测试工具识别模型	99.42%
20	知识图谱挖掘	基于知识图谱挖掘的攻击组织发现	不涉及
21	操作系统指纹识别	基于集成学习的旁路操作系统指纹识别	内部孵化中
22	自适应的蜜罐	基于强化学习的智能自适应蜜罐框架	内部孵化中

实战效果

- 2016年浙江移动G20安保一鸣惊人
- 2018年某中心网络流量分析引擎比赛第一名（总共19家参赛）
- 2019年深信服产品线测试评价“业界第一”
- 2020年360攻防产品线测试评价“比其他厂商好很多”
- 2020工业互联网安全技术大比拼活动，支持合作伙伴获得第一名
- 2020年国家电网恶意代码监测系统专项，支持合作伙伴获得第二名
- 2021年深圳市测评中心网络安全监测预警服务综合排名第一
- ……

2020年ISC创新独角兽沙盒大赛，荣获“最强发展力项目”奖项！

评委会评语：是安全圈里最懂大数据人工智能，而在大数据人工智能圈里最懂安全。站在技术前沿，凭借独特的产品理念，成为人工智能与安全领域的双料优胜者！

金睛云华
AI驱动安全

/05 成功案例

successful case

客户案例：超过1000+，现网运行系统3500+

金睛云华
AI驱动安全

WJ

- AI课题1
- AI课题2
- AI课题3
- 研制项目1
- 研制项目2

运营商

- 中国联通
- 中国移动
- 北京移动
- 浙江移动
- 广东电信
- 江西电信
- 重庆移动
- 黑龙江移动
- 广东省通信管理局

GA

- AI课题1
- XX市XX局
- XX市XX中心

公安

- 公安部
- 北京市公安局
- 上海市公安局
- 大连市公安局
- 广东省公安厅
- 安徽省公安厅
- 湖北省公安厅
- 厦门市公安局
- 福州市公安局
- 杭州市公安局
- 温州市公安局
- 潮州市公安局
- 惠州市公安局
- 无锡市公安局
- 日照市公安局
- 临沂市公安局
- 聊城市公安局

网信

- 河南网信办
- 深圳网信办
- 宁夏网信办

政府

- 国务院办公厅
- 国家税务总局
- 北京市国税局
- 国家质检总局
- 国家铁路局
- 北京市铁路局
- 国土资源部
- 北京城市副中心
- 北京市国资委
- 北京市商委
- 天津滨海新区政府
- 山东省政务云
- 广州海关
- 深圳海关
- 海关总署广东分署
- 黑龙江海事局
- 广东省人社厅
- 深圳智慧城市
- 南京市政府
- 铜陵市政府
- 南京软件园
- 贵州省安监局
- 河南省检察院
- 河南省人社厅

保密局

- 新疆保密局
- 河南保密局
- 吉林保密局

金融

- 上海证券交易所
- 北京产权交易所
- 中国银行
- 光大银行
- 红塔证券
- 红塔期货
- 高瓴资本

能源

- 中石油新疆油田
- 中石油长庆油田
- 北京市热力集团
- 北京市燃气集团
- 京能集团
- 京煤集团
- 蒙能集团

电力

- 国家电网
- 南方电网
- 国家能源集团
- 青海电力
- 黑龙江电力
- 陕西电力
- 山东省电力

广电

- 中央电视台
- 浙江华数
- 安徽广电
- 上海东方有线

大型活动安保

- 2016~2018贵阳
- 2016年G20会议
- 2017年金砖五国
- 2018年互联网大会
- 2019年数字中国
- 2021年护网行动

教育

- 清华大学
- 兰州大学
- 中山大学
- 北方工业大学
- 北京信息科技大学
- 南通大学
- 广东省教育厅
- 青岛市教体局
- 安庆市教育局

互联网

- 新浪
- 58到家
- 酒仙网

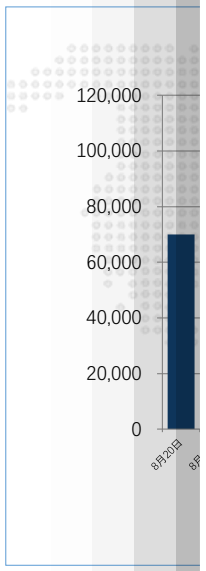
大企业/医疗/地产

- 中国中车集团
- 长春一汽集团
- 昆明市烟草公司
- 福清市医院
- 龙湖地产
- 中海地产

2016年浙江移动G20安保

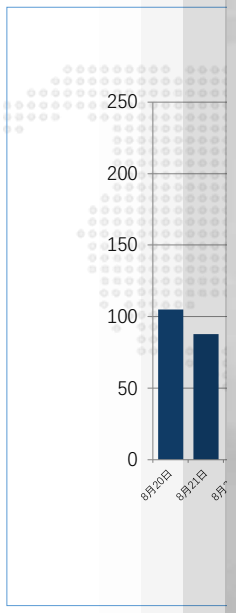
金睛云华
AI驱动安全

监



攻击次数众多：
方式组合使用：
主要呈现问题：
威胁性质确定：
TCP会话劫持和D

监测



病毒木马发现：
病毒木马种类：
侵入方式：特种
威胁性质确定：

G20 2016 CHINA

感谢信

北京金睛云华科技有限公司：

金秋九月，举世瞩目的二十国集团(G20)杭州峰会在钱塘江畔顺利召开。为顺利完成这一光荣的保障任务，你们与我部门同心协力、共同奋斗，在峰会网络完全保障工作中，做出了显著的成绩，我们由衷地感谢你们所有的努力和付出，感谢你们在峰会期间对安全保障工作的重视，尤其是在对各种病毒木马和威胁攻击的安全监测中表现优异。虽然保障工作夜以继日，但你们毫无怨言，全力支持我们的工作，这一切都令我们深深感动。

峰会已经结束，但是我们之间良好的合作却将长久延续，愿我们在今后的工作合作中密切配合、携手前进。

此致

敬礼！

中国移动通信集团浙江有限公司
信息技术部
2016年9月8日

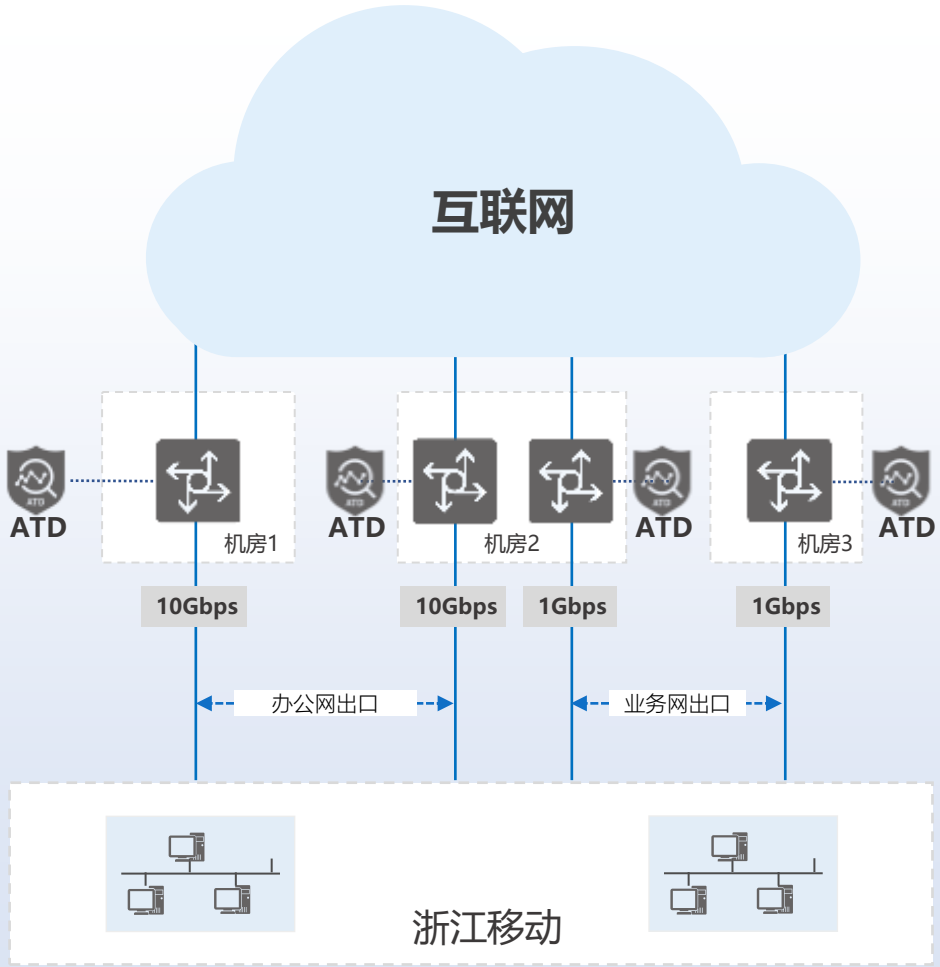
危木马病毒及其它威胁统计及危害

种类	次数	成功入侵或感染后危害
木马	50	直接破坏资料数据，抢占系统资源，占用磁盘空间，严重影响计算机运行速度或致死机，会传染其它设备；盗取账号、信息和数据，下载主程序安装、隐藏黑客活动、横向渗透、完全被控制、DDoS攻击。
钓鱼	5	伪装成合法的工具或软件等诱骗受害人，敏感信息泄露（口令、密码、账户等）。
变种	6	直接破坏资料数据，抢占系统资源，占用磁盘空间，严重影响计算机运行速度或致死机。
木马	19	盗取账号、信息和数据，下载主程序安装、隐藏黑客活动完全被控制、DDoS攻击、攻击特定对象。
漏洞	0	利用零日漏洞可以远程执行任意代码，获得最高权限。
/躲避	8	木马实现隐匿的行为，可以自我销毁、更名，捆绑在文件或程序中，修改图标等等。难以发现和查杀。

王90个左右，G20期间每日上升至180个左右。
横向渗透，到直接控制设备或僵尸网络等等。
较容易实现入侵。
而确认病毒木马及其威胁行为。

2016年浙江移动G20安保

金睛云华
AI驱动安全



安全挑战

- G20期间浙江移动办公网及业务网面临全球黑客/组织的高级持续性威胁（APT）攻击，而现有传统安全产品对这种高级持续性威胁基本是无效的

解决方案

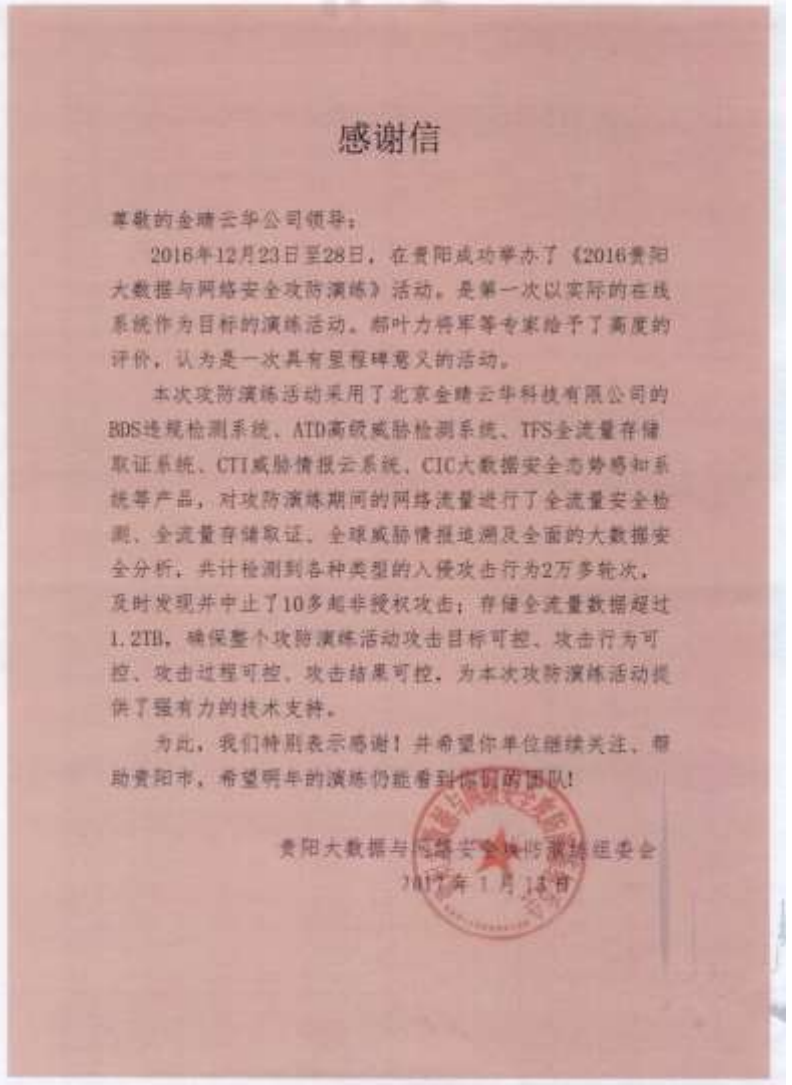
- 通过部署ATD高级威胁检测系统，对互联网出口流量进行全面的安全监测：
  - 办公互联网出口1部署一套万兆ATD高级威胁检测系统
  - 办公互联网出口2部署一套万兆ATD高级威胁检测系统
  - 业务互联网出口1部署一套千兆ATD高级威胁检测系统
  - 业务互联网出口2部署一套千兆ATD高级威胁检测系统

客户价值

- 实现对办公网及业务网潜在的高级持续性威胁检测，包括威胁情报检测、用户&实体行为分析、网络入侵检测、已知威胁多AV特征检测、威胁变种基因图谱检测、未知威胁沙箱行为检测等

2016~2021年贵阳大数据与网络安全攻防演练

金睛云华
AI驱动安全



感谢信

尊敬的金睛云华公司领导：

2016年12月23日至28日，在贵阳成功举办了《2016贵阳大数据与网络安全攻防演练》活动，是第一次以实际的在线系统作为目标的演练活动。邬叶力将军等专家给予了高度的评价，认为是一次具有里程碑意义的活动。

本次攻防演练活动采用了北京金睛云华科技有限公司的BDS违规检测系统、ATD高级威胁检测系统、TFS全流量存储取证系统、CTI威胁情报云系统、CIC大数据安全态势感知系统等产品，对攻防演练期间的网络流量进行了全流量安全检测、全流量存储取证、全球威胁情报追溯及全面的大数据安全分析，共计检测到各种类型的入侵攻击行为2万多轮次，及时发现并中止了10多起非授权攻击；存储全流量数据超过1.2TB，确保整个攻防演练活动攻击目标可控、攻击行为可控、攻击过程可控、攻击结果可控，为本次攻防演练活动提供了强有力的技术支持。

为此，我们特别表示感谢！并希望你单位继续关注、帮助贵阳市，希望明年的演练仍能看到你们的团队！

贵阳大数据与网络安全攻防演练组委会

2017年1月14日

2018年CNCERT年会网络安全引擎比赛

金睛云华
AI驱动安全

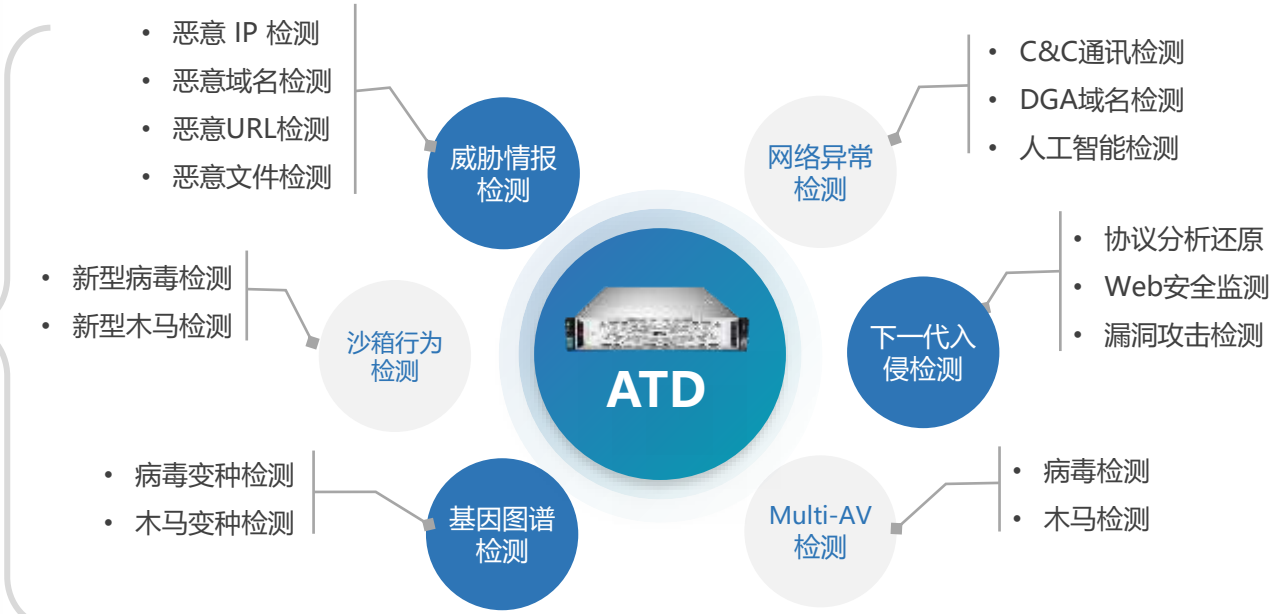
国家互联网应急中心CNCERT

（一）网络安全引擎比赛

网络安全引擎比赛选定"恶意代码分析引擎"与"网络流量分析引擎"两项比赛科目，使用真实网络安全业务数据与业务场景，对网络安全引擎的功能、性能及业务数据实战分析能力进行测试，由离线分析测试与现场答辩两部分组成。

比赛吸引了19家国内安全企业报名。自2018年7月26日起，经过16天紧张的离线检测分析与企业自证环节，每项比赛前8名脱颖而出。本场赛事进行了激烈的专家评审答辩环节，对比赛结果、创新性、应用场景进行评判。最终的比赛结果将综合离线分析测试得分与现场答辩得分，经终审之后进行公布。

1、“网络流量分析引擎”比赛



2、“恶意代码分析引擎”比赛

DNS隐蔽隧道数据外泄检测实例

金睛云华
AI驱动安全

DNS隧道源主机	DNS隧道域名	DNS服务器	次数	隧道信息举例
XX.135.190.245 北京联通	xzviz.com xzjfz.com xzcwa.com	173.201.76.9 美国	13.5w	za8a4seb ssehxa38 6wdrkf54 a2fp272k 3ickzp5y hd3maf3h tspsxxcd dy52zsst
XX.135.190.246 北京联通		173.201.76.9 美国	13.5w	
XX.108.250.232 北京联通		216.69.185.9 美国	1.5k	
XX.108.250.233 北京联通		216.69.185.9 美国	1.5k	
XX.108.250.234 北京联通		216.69.185.9 美国	1.5k	

DNS隐蔽隧道数据外泄检测实例

金睛云华
AI驱动安全

xzviz.com	xzjfz.com	xzcwa.com
ea65hd7b.xzviz.com	fm6i2nhf.xzjfz.com	p6nbna7y.xzcwa.com
si5hh7tb.xzviz.com	sasdnzjp.xzjfz.com	zscnrhnc.xzcwa.com
zfmx76e2.xzviz.com	64k5fkdr.xzjfz.com	5f6zbsdh.xzcwa.com
pcp5fi7r.xzviz.com	r7x3w48a.xzjfz.com	6emy8j4y.xzcwa.com
kaxe7hke.xzviz.com	72f6hnyj.xzjfz.com	ht8jr6na.xzcwa.com
pxe53tb6.xzviz.com	26jdm6r5.xzjfz.com	ds4e2mkt.xzcwa.com
pcrdpnb5.xzviz.com	pi3r8pmp.xzjfz.com	kpmtaiec.xzcwa.com
5skdmyer.xzviz.com	n6d3ybic.xzjfz.com	wfefb8he.xzcwa.com
czwezai5.xzviz.com	chmf54as.xzjfz.com	ja5aszb3.xzcwa.com
bt4fn42b.xzviz.com	zjr8rwtf.xzjfz.com	sjz4jse2.xzcwa.com
2iiht252.xzviz.com	cps8jzyn.xzjfz.com	re63bpm2.xzcwa.com
ebwrym2x.xzviz.com	dcrt482t.xzjfz.com	krskma5w.xzcwa.com
3freiad6.xzviz.com	b7y7czdk.xzjfz.com	cez22yb7.xzcwa.com

DNS隐蔽隧道数据外泄检测实例

金睛云华
AI驱动安全

```
ea65hd7bsi5hh7tbzfmx76e2pcp5fi7rkaxe

y xAE xB9 x85 xDE ۲.a x87 xBB [ xCD xF9 xB1 □ xA5 xCA y~.둬^
```

分析：

① 上述域名的子域名长度均为8个字符，且只包含数字和英文字母，应是Base64编码后的内容；

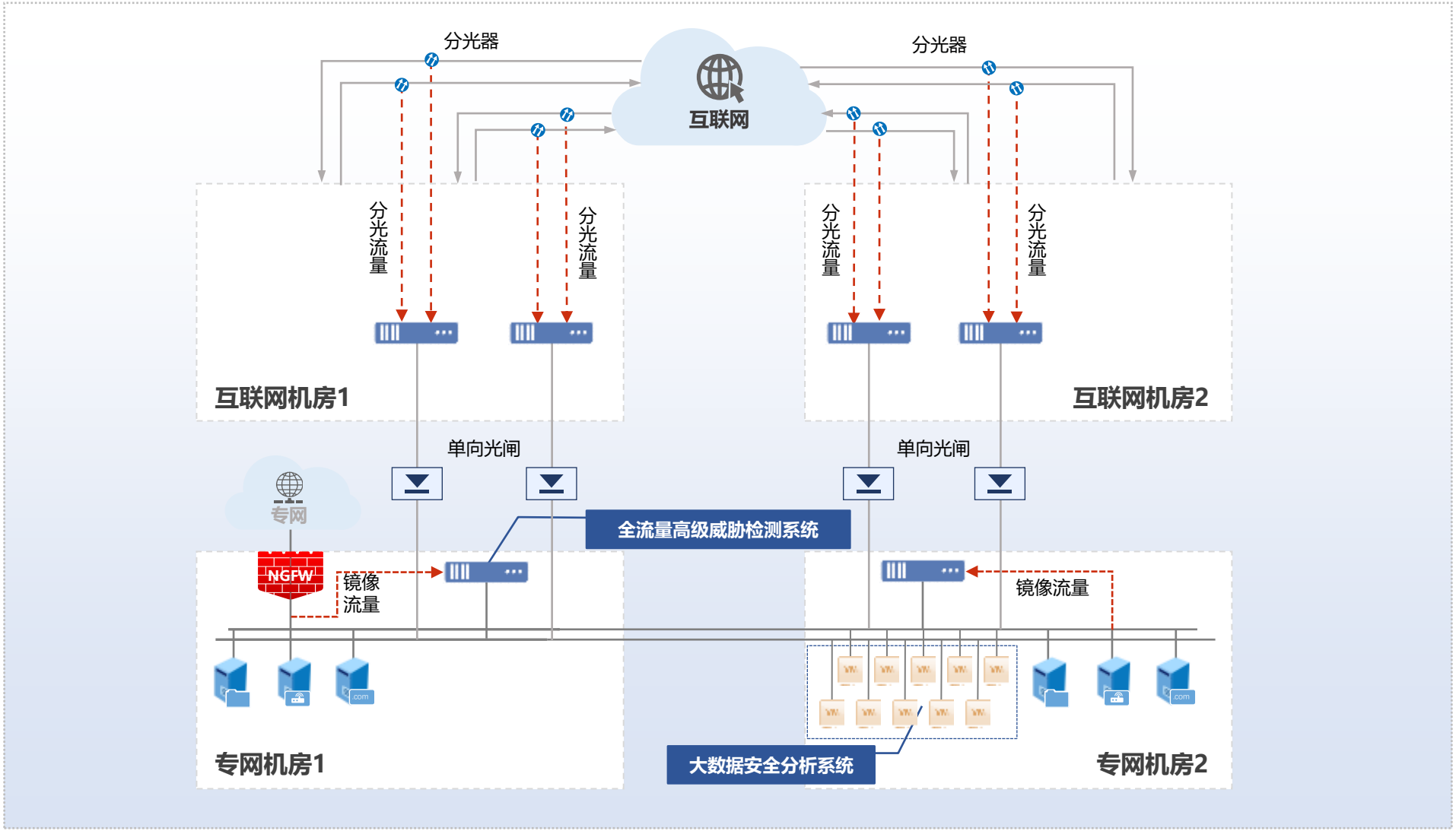
② 摘取xzviz.com的部分数据，通过Base64成功解码，解码后得到包含16进制数据，如上图所示；

③ 分析解码后的数据包含16进制内容，肯定不是文本文件，猜测可能是Word(Office)文档或者PDF或者加密后的内容等；

④ 如果按序获取完整的DNS隧道子域名数据，解码后经过进一步处理或者解密能得到外传的完整数据。

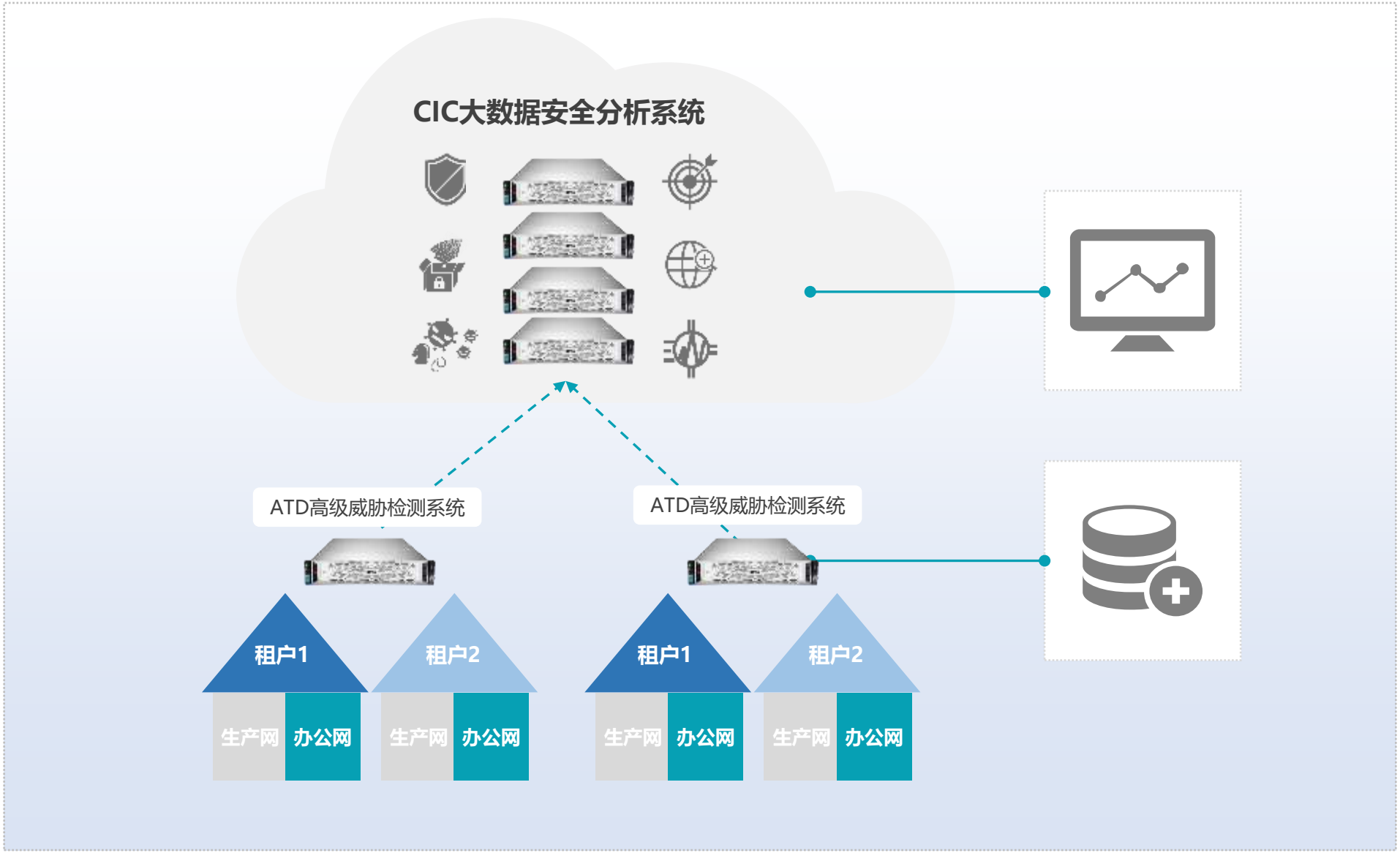
某部委大数据安全态势感知系统

金睛云华
AI驱动安全



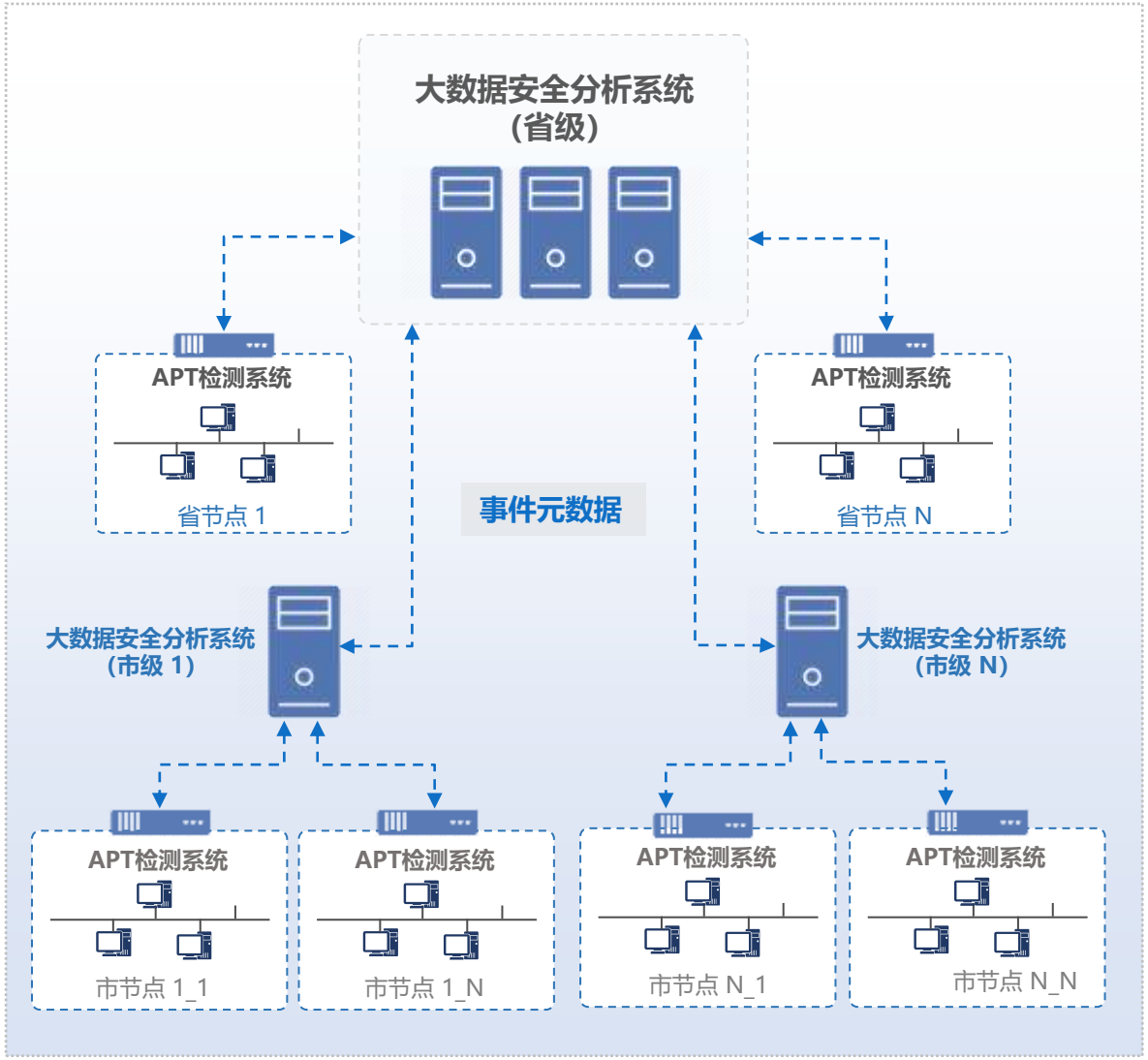
多租户安全运营解决方案

金睛云华
AI驱动安全



某省网安大数据安全态势感知系统

金睛云华
AI驱动安全



客户需求

某省重要网络节点安全监测，市级-省级，多层节点

解决方案

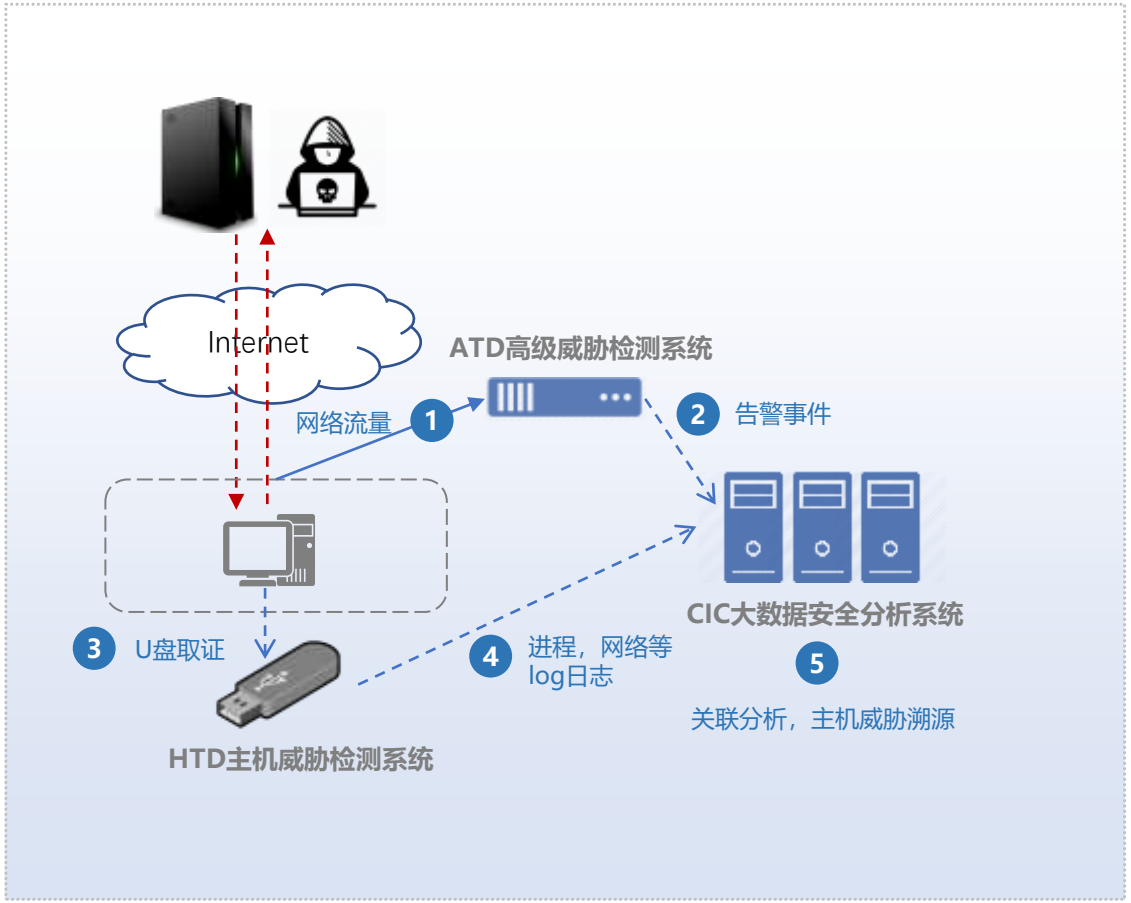
以多市节点APT检测系统作为探针采集器，实现对重点用户的互联网数据流量进行全面的检测，监控可疑网络威胁行为。探针通过将检测后事件与元数据传输至地市大数据安全分析系统，进行进一步的海量数据实时处理、分布式数据存储，长时间窗离线关联分析、人工智能模块威胁检测等。地市的数据及省探针数据传输至省大数据安全分析系统进行进一步地市的海量数据处理与分析。

客户价值

- 有效检测APT等高级可持续性威胁
- 了解全省安全态势，采取合理预防措施
- 融合安全设备，具备威胁情报检测、用户&实体行为分析、下一代入侵检测、多AV检测、基因检测和沙箱行为检测等多种安全能力，有效减少客户投资及运维工作
- 长时间窗关联分析，有效防止长时间间隔的APT攻击
- 通过U盘自动取证技术实现网络威胁关联到主机的自动取证

网络威胁在主机侧自动溯源取证

金睛云华
AI驱动安全



产品构成

- HTD主机威胁检测系统（U盘形式，运行即可，无需安装）
- ATD高级威胁检测系统/CIC大数据安全分析系统

取证流程

① 检测到网络威胁

② 告警事件上送至CIC

③ 在可疑受害主机上接上U盘，运行HTD，持续实时监测系统非白名单的进程、网络连接、系统服务等异常信息，并保存log日志在U盘中，可根据需要，运行24小时或更久

④ 在取证结束后，将U盘接在CIC，将主机log数据提交给CIC分析

⑤ 在CIC关联分析检测到的网络威胁事件和主机log数据，可以实现主机恶意进程及恶意文件定位

THANKS