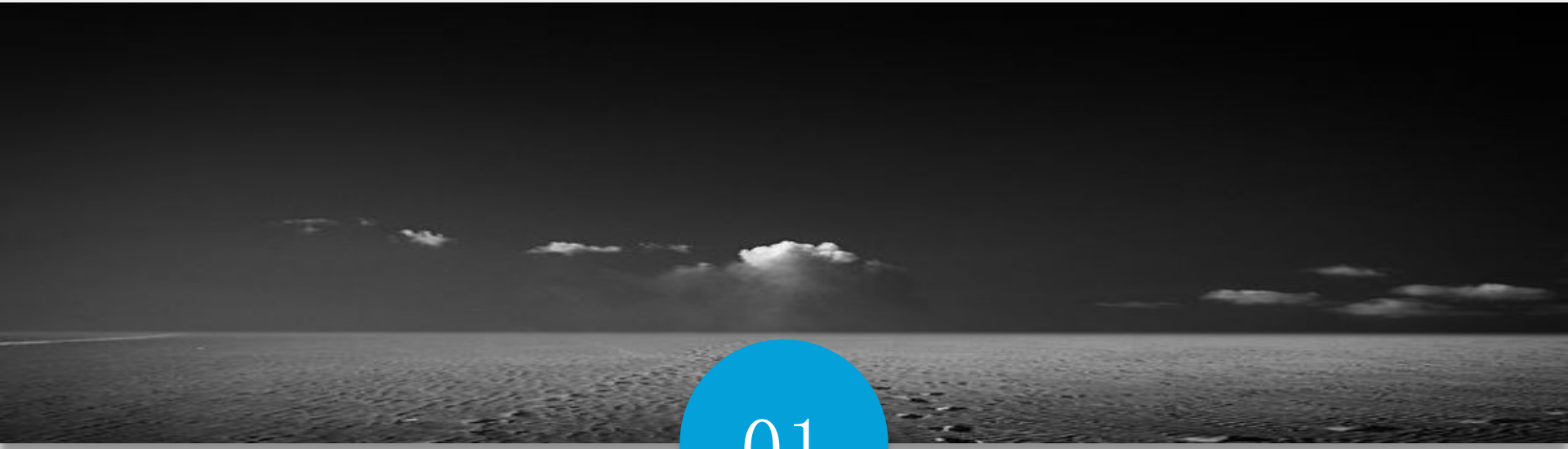
# APT检测及安全智能技术探讨

2017年10月

# 目录

CONTENT



01

# 传统安全面临的挑战

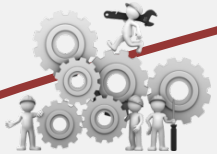
# 威胁发展趋势

APT

有组织/国家背景：
商业/政治诉求，监听/窃取/破坏

黑 客 实 力 及 动 机

产业链：
经济利益，偷窃/破坏



Hacking as Organized Crime

0-Day

Hacking as Business

极少数派：
扬名/炫耀，恶搞

Hacking as Display

社工、0day漏洞：
有针对性的APT攻击

Advanced
Cyber Attack

移动威胁

WEB脆弱性：
主动的WEB攻击、拒绝服务攻击

Web威胁

僵尸网络

互联网接入：
随机的病毒/木马感染

蠕虫

木马

病毒

Motiveless
Cyber Attack

Ordinary Targeted
Cyber Attack

攻 击 手 段 及 目 标

# APT成为网络攻击“新常态”

- 数字资产价值越来越大，觊觎数字资产的黑客组织越来越多
- 传统安全机制无法对抗APT等高级威胁
- 巨大的利益驱使产业组织，乃至政府组织投入大量资源资助和发展黑客组织

**定向（80%恶意代码只用一次）**
针对锁定的价值目标，黑客组织收集信息，利用社工等高级手段投放定制“武器”

**隐蔽**
针对锁定目标的防御体系定制复杂的高级的“武器”，传统安全机制无法发现

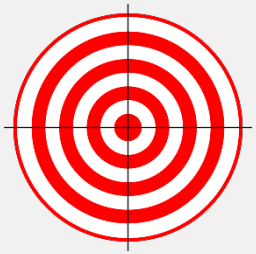
**长期（APT被发现前平均潜伏320天）**
潜伏之后，持续窥探价值目标，找到并获利后才打扫战场

# 什么是APT？

Advanced Persistent Threat：高级持续性威胁

定向

锁定目标
有针对的渗透攻击



持续攻击，长期潜伏
直到达成目标

长期

APT

组合

结合各种技术
形成更高级的攻击手段


隐蔽

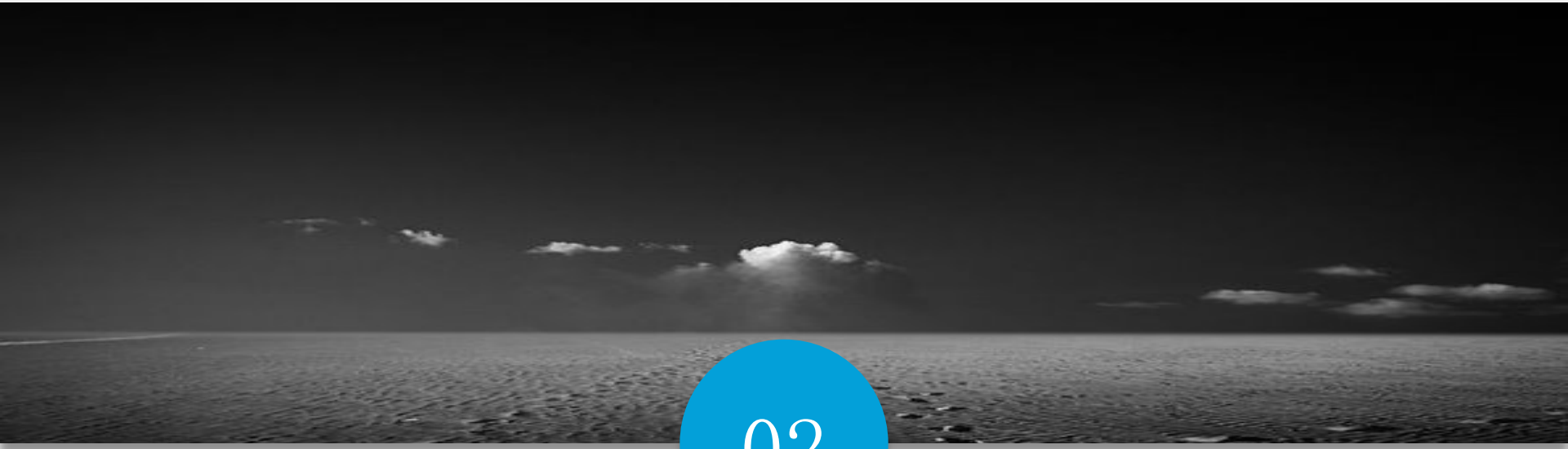
你已经被感染
只是你不知道

①扫描探测 ②网络钓鱼 ③初步感染 ④木马下载 ⑤远程控制 ⑥横向渗透 ⑦行动收割

# 传统安全面临的挑战

黑客组织化/国家化；攻击手段高级化，组合化，长期化；目标明确

**APT防不胜防：不怕贼偷，就怕贼惦记！**



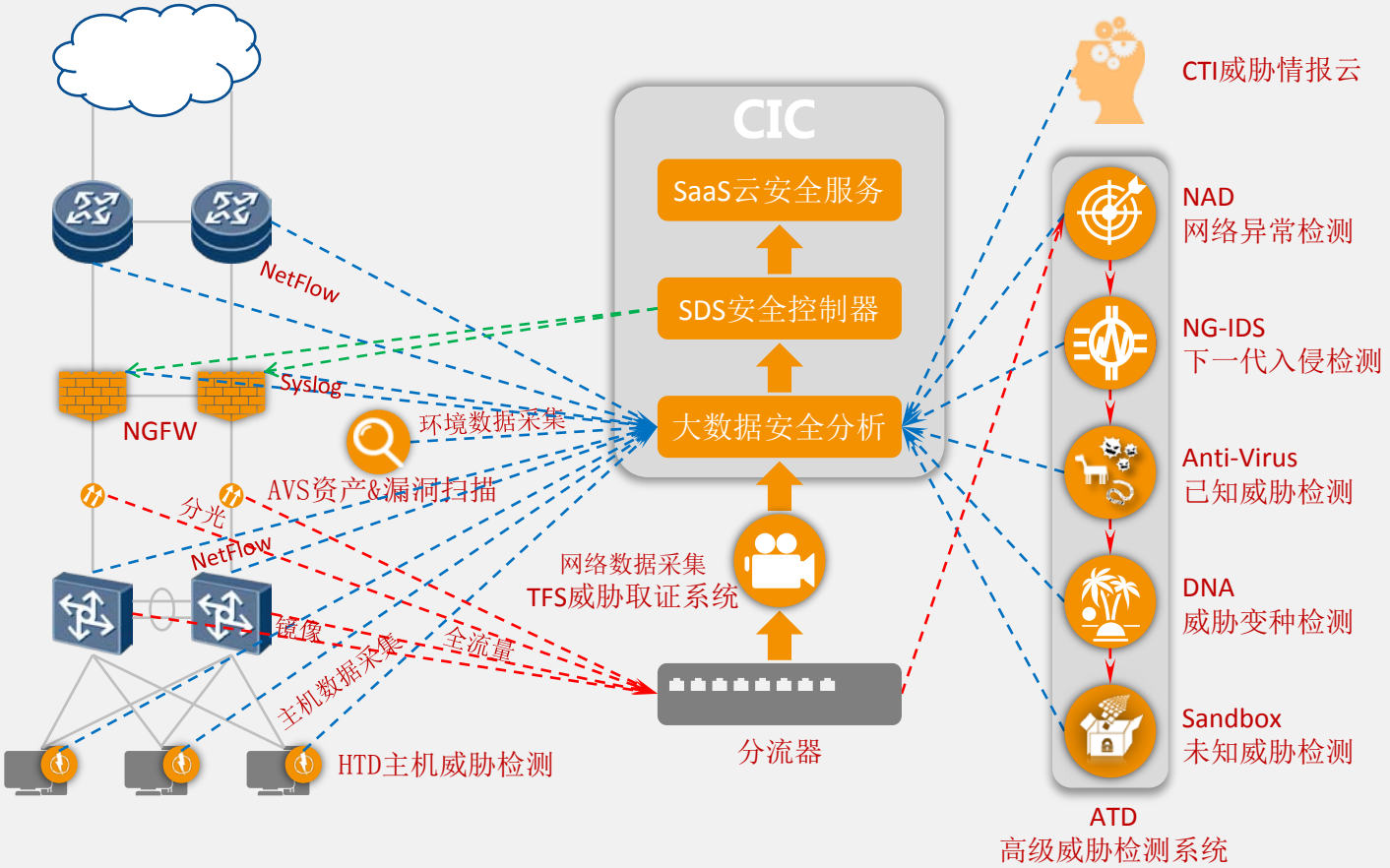
02

# 基于攻击链的APT解决方案

# APT攻击链检测模型

| KILL CHAIN | 扫描探测 | 网络钓鱼 | 漏洞利用 | 木马下载 | 远程控制 | 横向渗透 | 行动收割 |
|---|---|---|---|---|---|---|---|
| 网络异常检测 | ✓ | | ✓ | | ✓ | ✓ | ✓ |
| 下一代入侵检测 | ✓ | | ✓ | | | ✓ | |
| Multi-AV检测 | | ✓ | | ✓ | | | |
| 基因图谱检测 | | ✓ | | ✓ | | | |
| 沙箱行为检测 | | ✓ | ✓ | ✓ | | | |
| 威胁情报检测 | ✓ | ✓ | | ✓ | ✓ | | ✓ |
| 大数据关联分析 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |

# 解决方案


CIC
SaaS云安全服务
SDS安全控制器
大数据安全分析
CTI威胁情报云
NAD
网络异常检测
NG-IDS
下一代入侵检测
Anti-Virus
已知威胁检测
DNA
威胁变种检测
Sandbox
未知威胁检测
ATD
高级威胁检测系统
NetFlow
Syslog
NGFW
环境数据采集
AVS资产&漏洞扫描
分光
NetFlow
镜像
主机数据采集
全流量
HTD主机威胁检测
网络数据采集
TFS威胁取证系统
分流器

# 方案特点

## 全面

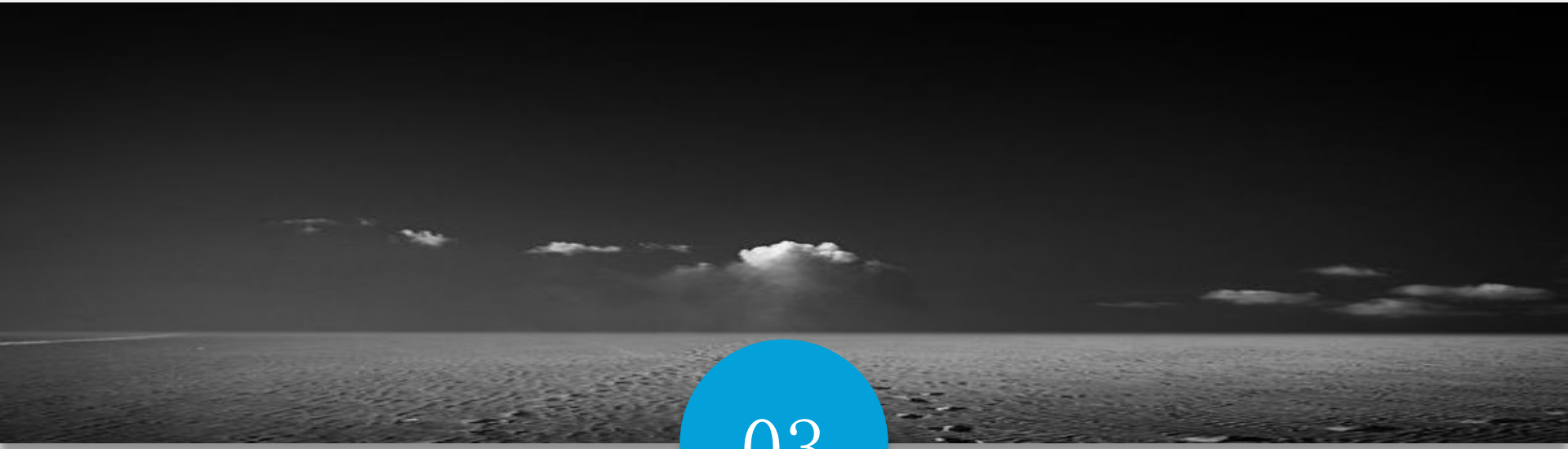
- 数据采集全面
  - 网络数据
  - 环境数据
  - 主机数据
  - 情报数据
- 检测技术全面
  - **网络异常检测**
  - 下一代入侵检测
  - 病毒木马检测
  - **基因图谱检测**
  - **沙箱行为检测**
  - 主机威胁检测

## 智能

- 机器学习/深度学习
  - 安全建模
  - 业务建模
- 异常检测
  - 异常流量检测
  - 异常行为检测
- 大数据关联分析
  - 实时数据分析
  - 历史数据分析
- 自适应安全控制
  - 软件定义安全
  - 头脑发达，四肢简单

## 主动

- 行为激活/内容引爆
  - 未知威胁检测
  - 防躲避/逃逸
- 安全态势感知
  - 实时威胁监测
  - 安全趋势走向
  - 威胁情报共享
- 主动检测防护
  - 资产漏洞扫描
  - APT攻击链检测
  - 全局协同防护
  - 按需分配资源



03

# 人工智能检测APT技术探讨

# 大数据人工智能安全分析平台

**DeepInsight**

**AI 安全模型**

| | | | |
|---|---|---|---|
| 钓鱼检测 | Web攻击检测 | 基因检测 | DGA检测 |
| 行为模式库生成（沙箱） | 协议与应用识别（DPI） | 网络异常检测 | 攻击成功判定 |

**AI 算法引擎**

| | |
|---|---|
| 深度学习训练模块 | 机器学习训练模块 |
| TensorFlow | MLlib（Spark） |

**Panku（盘古）安全大数据平台**

| | | | |
|---|---|---|---|
| 实时关联引擎 | 异常检测引擎 | 任务调度引擎 | 存储管理引擎 |
| CDH | HDP | FusionInsight | Apache |

# DGA域名深度学习检测Fast-Flux僵尸主机

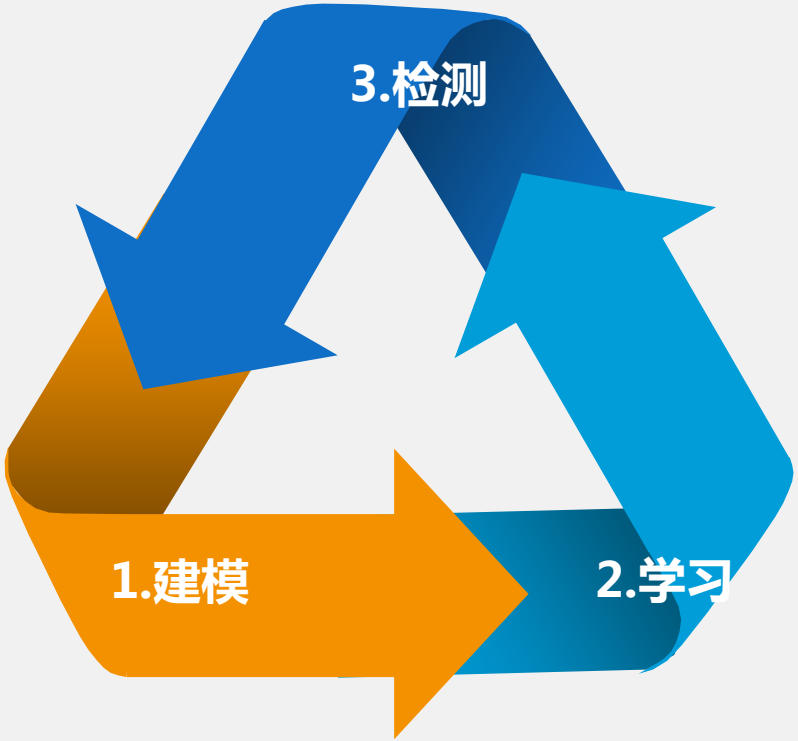
Fast-Flux是在DNS RR上设定非常短的TTL，并以循序的方式在一个IP集合中做频繁替换，这些IP集合表示受控主机集合，在Fast-Flux技术中作为proxy角色

DGA域名生成算法(Domain Generation Algorithm)是设计思想是，malware代码里不写入域名字符串，而是使用一个私有的随机字符串生成算法，按照日期或者其他随机种子，每天生成一些随机字符串然后用其中的一些当作C&C域名

我们将采用静态及动态特征相结合的DGA域名识别系统（LSTM深度学习模型），捕捉防护目标网络内的DNS查询，经系统的三层分析后给出是否是恶意域名的判断，相关结果提供给用户作为决策参考

# DGA域名深度学习检测Fast-Flux僵尸主机

网络异常检测引擎分析捕捉到网络流量中的域名信息后，将之输入深度学习模型进行识别，深度学习模型输出该域名是否为DGA生成的域名




建立针对DGA生成域名的长短期记忆神经网络LSTM深度学习模型

用海量的各种类型的DGA生成的域名，以及海量的正常域名对深度学习模型进行训练，训练完成之后，深度学习模型就具备了识别能力

# DGA域名深度学习检测Fast-Flux僵尸主机实例

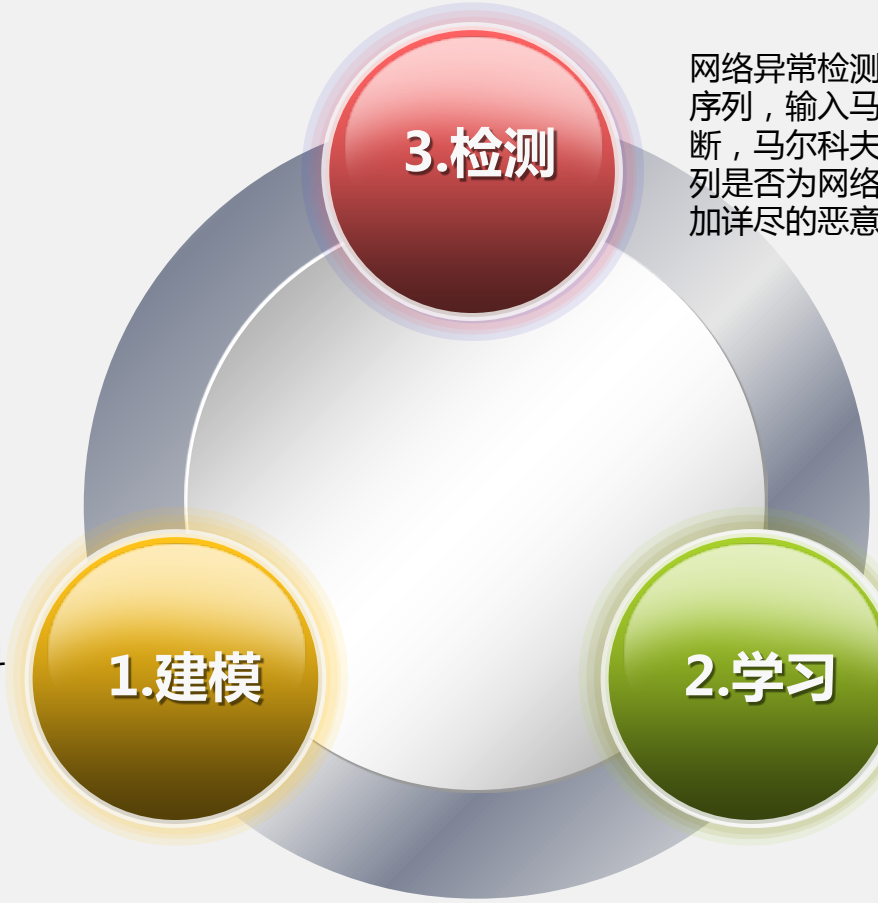
## 部分数据统计

| 威胁名称 | 疑似被控制主机IP | DNS查询内容 | 次数 |
|---|---|---|---|
| DGA::可疑恶意域名发现 | 172.16.11.112 | buweogh.org 查询类型:A | 4 |
| | | ixggjysd.ws 查询类型:A | 4 |
| | | tclghjkf.com 查询类型:A | 3 |
| | | tukcjmufmjk.cn 查询类型:A | 3 |
| | | cvjuyiwx.cn 查询类型:A | 3 |
| | | dzptbcpwmm.ws 查询类型:A | 3 |
| | | eezlupsw.cc 查询类型:A | 3 |
| | | eupebvn.biz 查询类型:A | 3 |
| | | fejbqiuz.org 查询类型:A | 3 |
| | | fxecjael.cc 查询类型:A | 3 |
| | | fzpfkmumv.cc 查询类型:A | 3 |

## 尝试访问


可以看出，IP为172.16.11.112的主机大量访问疑似C&C域名，且其中某些域名(如tukcjmufmjk.cn)目前正在工作。猜测该主机已经被攻击者控制。

# 马尔科夫链模型（机器学习）检测网络异常行为



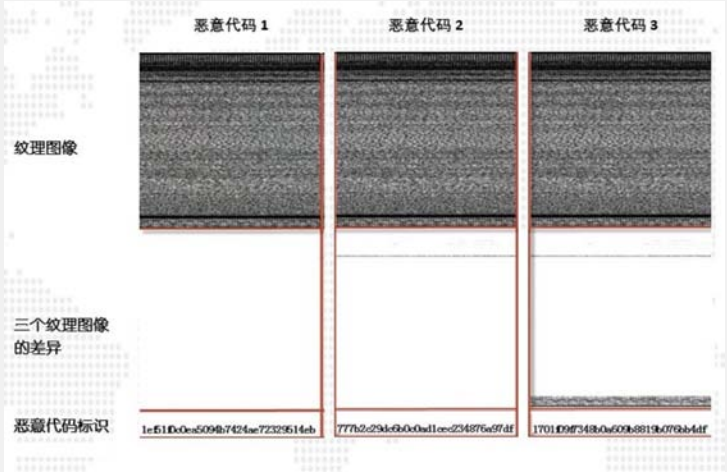

网络异常检测引擎分析提取网络行为序列，输入马尔科夫模型进行分类判断，马尔科夫模型输出该网络行为序列是否为网络异常行为模式，以及更加详尽的恶意行为类别等信息

建立恶意代码网络行为的马尔科夫模型（机器学习）

利用海量的恶意代码的网络行为对马尔科夫模型进行机器学习训练，训练成功后的模型就具备了网络异常行为模式的分类能力

# 恶意代码基因图谱深度学习检测威胁变种

**灰度图像样例**




恶意代码Worm.Win32.WBNA 3个家族成员内容纹理差异实例

**检测方法**

01 将恶意代码映射为灰度图像，并提取其灰度图像特征

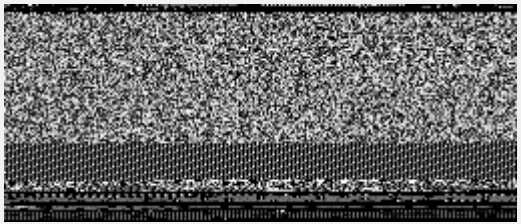
02 利用恶意代码灰度图像特征进行聚类，并将聚类结果进行恶意代码家族标注

03 建立卷积神经元网络CNN模型，并设置网络结构参数和训练参数

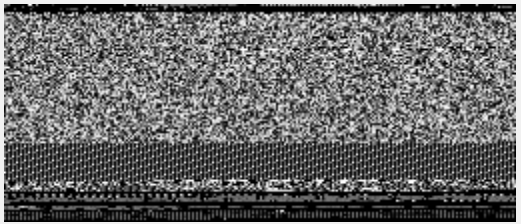
04 利用恶意代码家族灰度图像集合训练卷积神经元网络，并建立检测模型

05 利用检测模型对恶意代码及其变种进行家族检测

# 恶意代码基因图谱深度学习检测威胁变种

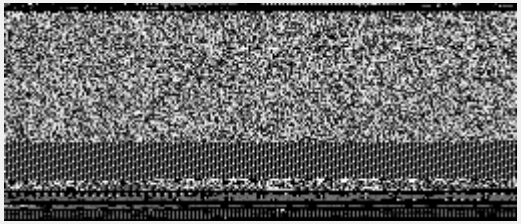


da72e369c3f0d5a5e0f0fa8435c36a86

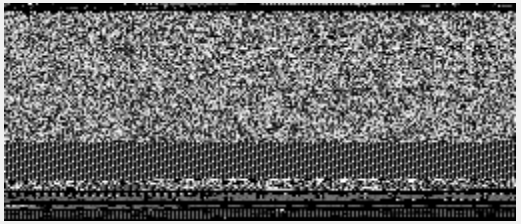


da76adbd6e500150542cf8081113fdc5

变种

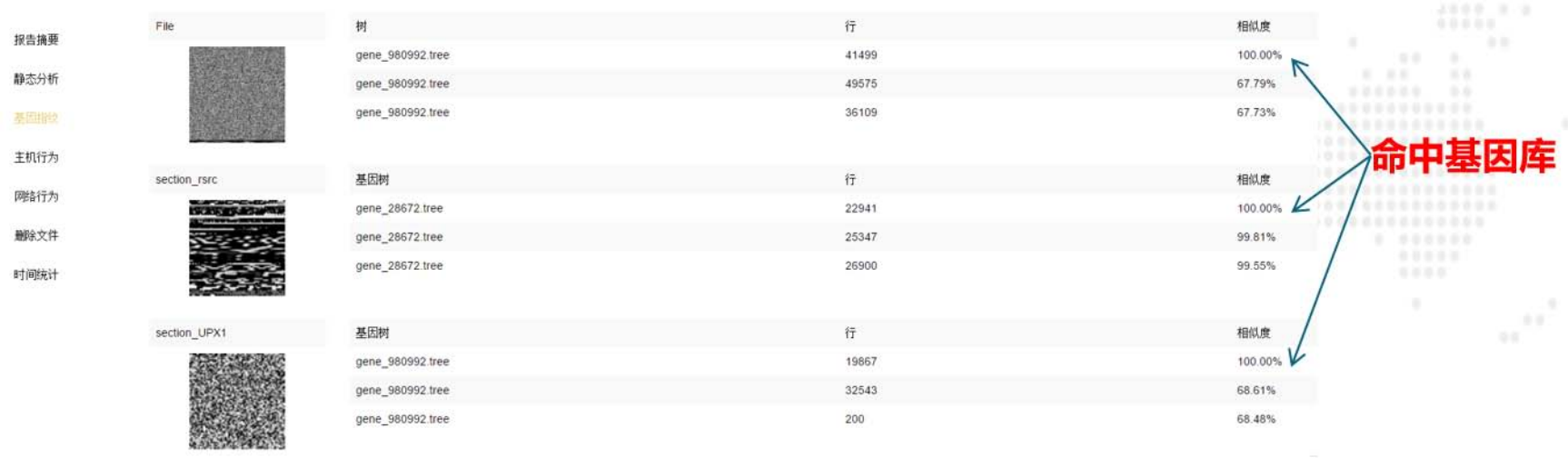


da80c62bc648433a75b364b2643c7f49



da83bf6d4a776b4171546748498453d6

# 恶意代码基因图谱深度学习检测威胁变种实例




恶意代码家族是有具有明显特征的恶意代码种类，是由很多拥有共同特性的恶意代码个体组成，共同特性通常包括相同的代码，图案，应用特征及相似的行为方式。恶意代码家族中的个体成员之间差异较小，而且它们的基因结构也比较相近，犹如物种在进化过程中基因变化一样。

# 频繁项集挖掘算法（深度学习）提取沙箱行为模式库

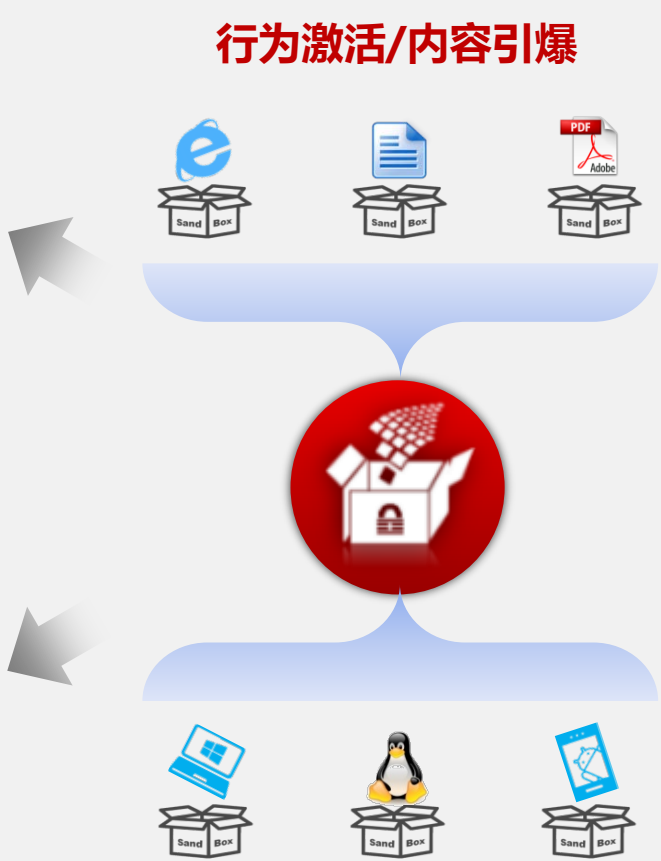

建立针对恶意代码沙箱行为的频繁项集挖掘算法模型

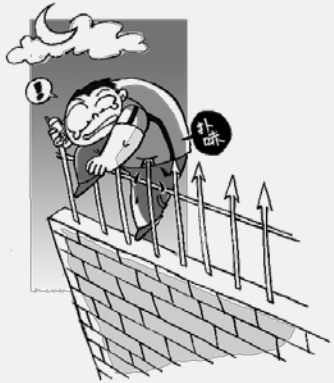
用海量的恶意代码沙箱行为数据输入频繁项集挖掘算法模型，生成高频的沙箱行为模式库

安全专家团队分析排查频繁项集挖掘算法模型生成的沙箱行为模式库，去除无效和失真部分，保留所有有效条目进而建立用于商用检测的恶意行为模式库

1、极大提高了恶意行为模式库生成效率
2、显著提升了恶意行为模式库的数量和质量，进而实现高检出和低误报

# 沙箱恶意行为模式匹配检测未知威胁




# WannaCry加密勒索软件检测实例

| | |
|---|---|
| 等级: | 高危 |
| 沙箱: | xp1 |
| 开始: | 2017-05-13 11:58:51 |
| 持续: | 62 秒 |

## 行为签名

| | | | | |
|---|---|---|---|---|
| 异常读行为：试图从文件自身二值图像中读取数据 | 可信度 | 30 | 危险等级 | 1 |
| 反沙箱行为：检测到脚本定时器窗口，疑似采用sleep方式躲避沙箱捕获其行为 | 可信度 | 100 | 危险等级 | 2 |
| 隐匿行为：进程创建了一个隐藏的窗口 | 可信度 | 100 | 危险等级 | 2 |
| 异常的文件行为：疑似在文件系统中创建 55 个可执行程序 | 可信度 | 100 | 危险等级 | 2 |

## 相关文件

- r.wnry
- Blue hills.jpg.WNCRY
- New Stories (Highway Blues).wma.WNCRY
- s.wnry
- 4.WNCRYT
- Water lilies.jpg.WNCRY
- m_norwegian.wnry
- XLog_20161103094440_2516_3.txt.WNCRY
- 2.WNCRYT
- Winter.jpg.WNCRY
- c.wnry

04

# 关于金睛云华

# 公司简介

- 北京金睛云华科技有限公司成立于2015年，注册资金1000万
- 创始人及核心团队主要来自于华为、启明星辰、联想等公司

**使命** 让网络空间更安全

**愿景** 成为国际一流、国内领先的大数据安全分析及云安全服务提供商

# 核心团队

## 研发总监：曲武

- 北京科技大学硕士&博士，清华大学博士后（十多项专利发明人，数十篇论文作者，曾经一年发表6篇SCI论文）；
- 超过十年大数据&网络安全领域研究和实践经验，掌握国内领先的APT检测及大数据安全分析核心技术
- 历任启明星辰核心技术研究院高级研究员（启明星辰云SOC原型设计者）、华为网络安全产品线高端安全专家（华为大数据安全分析产品首席架构师）

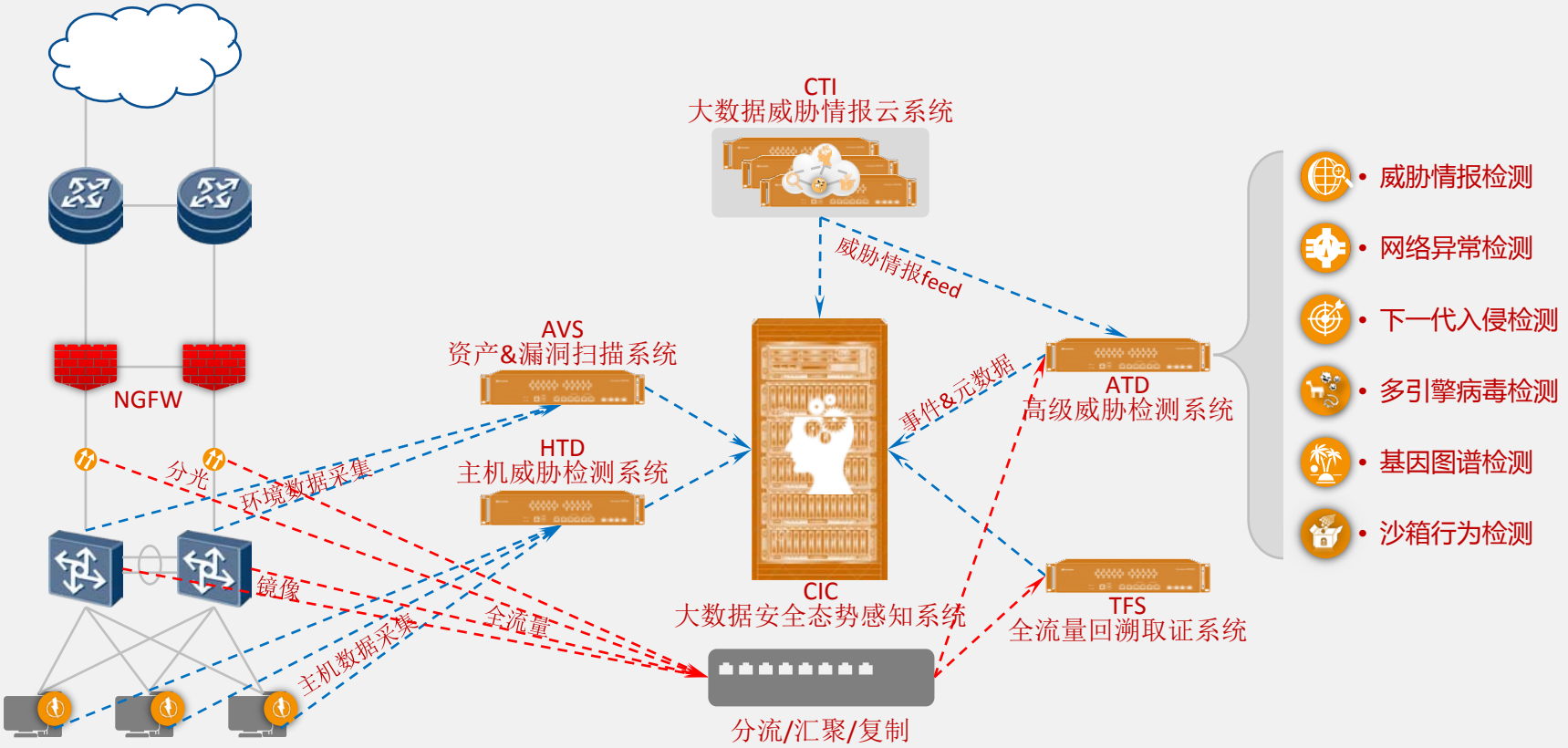
## 市场总监：胡文友

- 超过十五年网络安全行业经验；历任启明星辰高级产品经理（号称“天清汉马防火墙之父”）、华为赛门铁克安全行销代表（华赛中国区安全行销第一人）、华为全球解决方案部CTO Office首席安全顾问
- 与建行、海关总署等客户战略合作安全领域总体技术负责人（当年安全产品在建行销售额超过网络设备及IT设备）

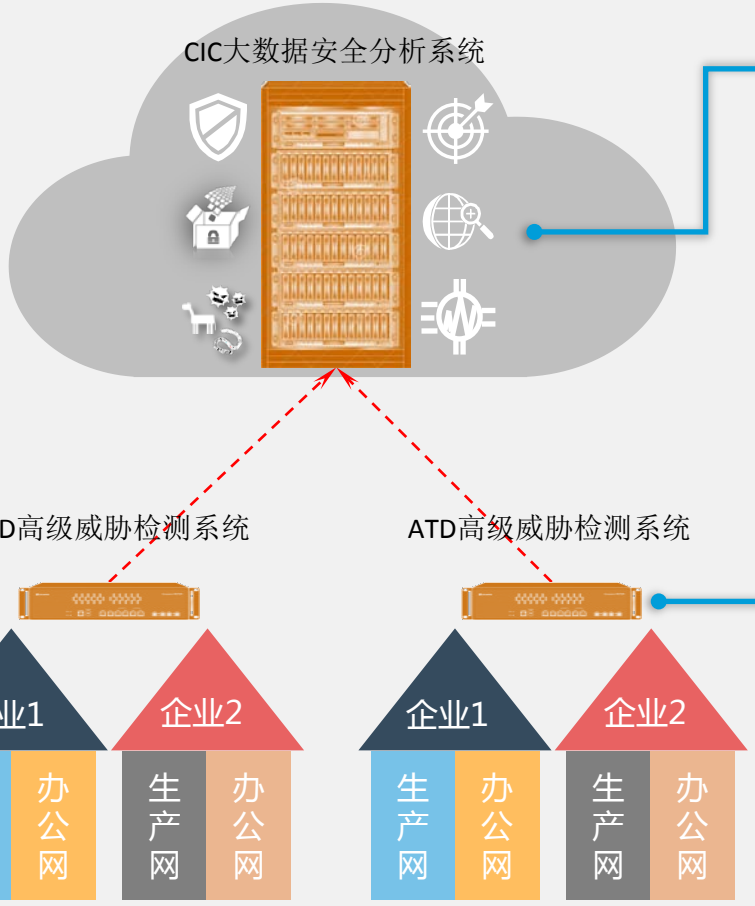
## 技术总监：赵立久

- 北京大学数学系学士&硕士，十七年华为工作经验，历任华为公司开发工程师、项目经理、研究部经理、以太网核心交换机开发代表、以太网交换机产品领域总经理、华为企业BG中国区商业产品与解决方案销售部部长等职务。

# 产品方案


CTI
大数据威胁情报云系统
威胁情报feed
AVS
资产&漏洞扫描系统
HTD
主机威胁检测系统
NGFW
分光
环境数据采集
镜像
全流量
主机数据采集
CIC
大数据安全态势感知系统
事件&元数据
ATD
高级威胁检测系统
TFS
全流量回溯取证系统
分流/汇聚/复制
威胁情报检测
网络异常检测
下一代入侵检测
多引擎病毒检测
基因图谱检测
沙箱行为检测

# SaaS服务



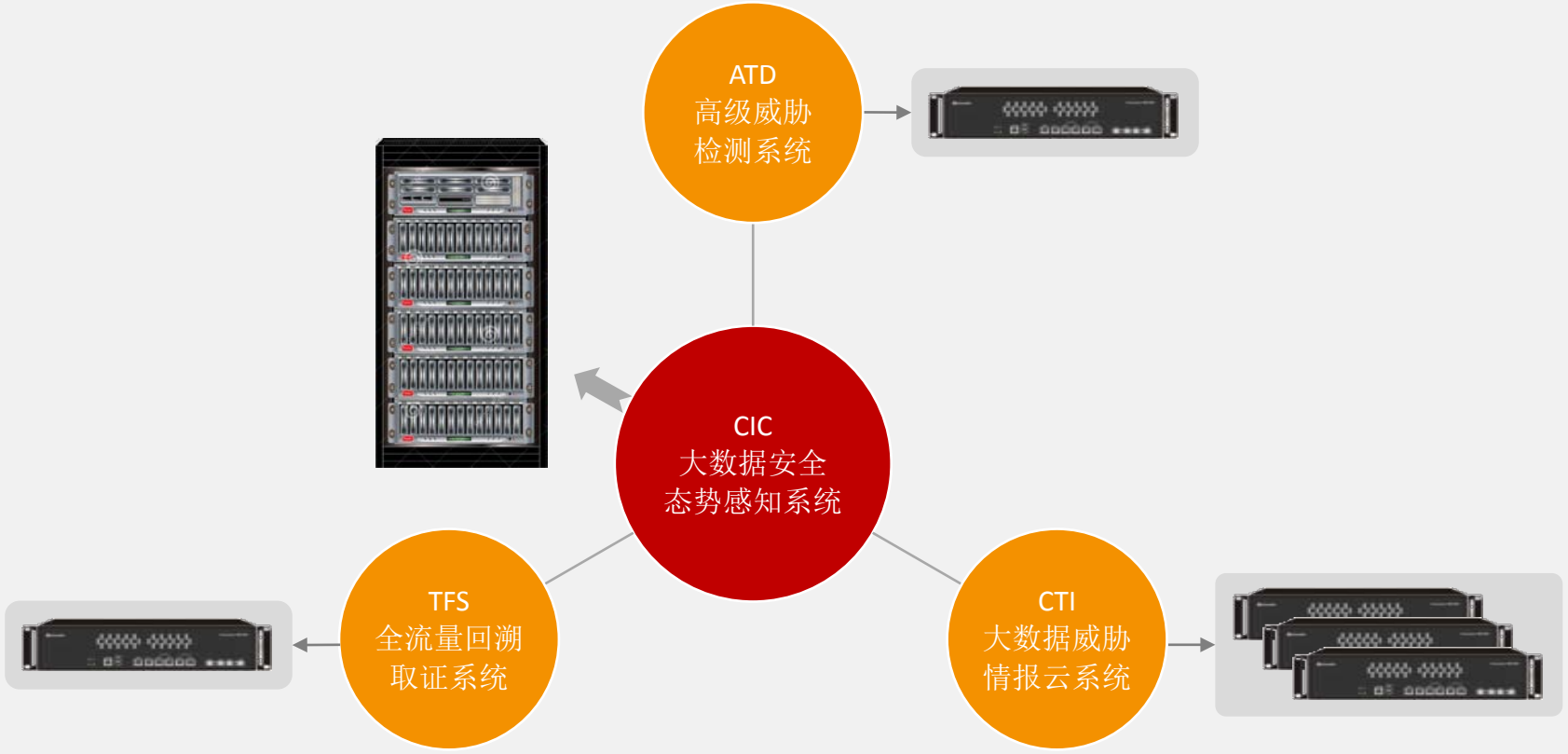

**解决方案支持多租户独立使用与管理：**

- 方案1：企业1，企业2，企业N……
- 方案2：企业1生产网，企业1 办公网，企业2生产网，企业2办公网，……

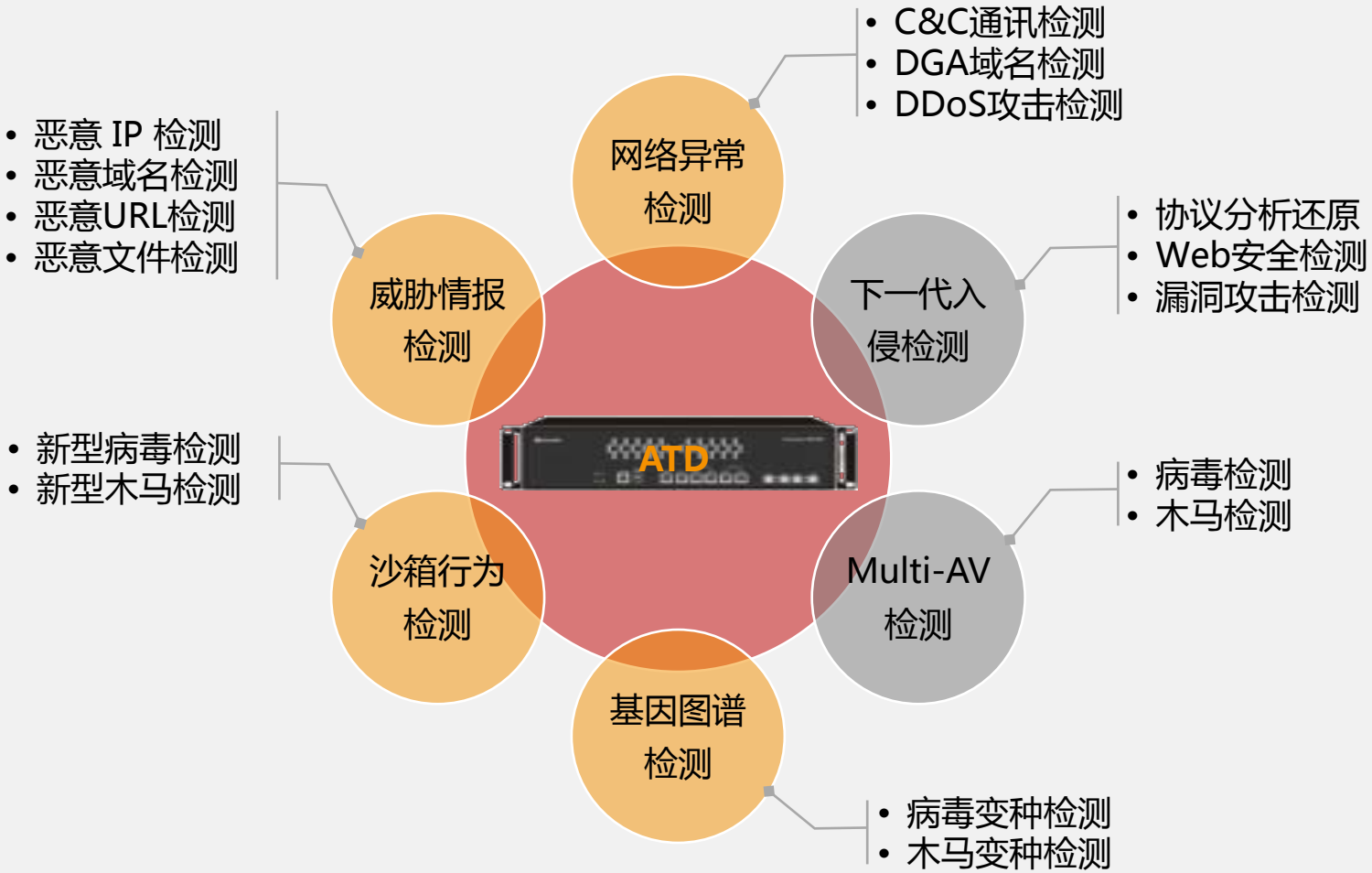
**多租户隔离方案：**

- 方案1：ATD标识 + 网络接口标识
- 方案2：ATD标识 + 网络接口标识 + 子网标识
- 第三方设备对接：设备标识 + 自定义标识（可选）

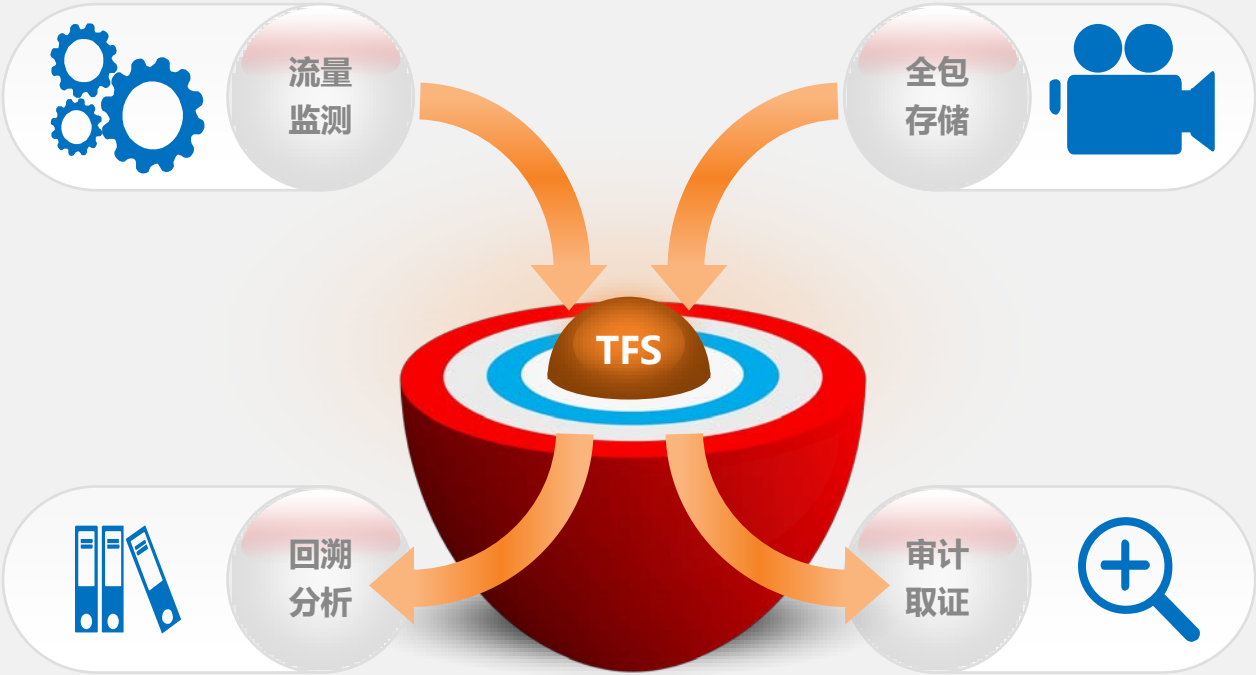
# 核心产品


ATD
高级威胁
检测系统
CIC
大数据安全
态势感知系统
TFS
全流量回溯
取证系统
CTI
大数据威胁
情报云系统

# 高级威胁检测系统（ATD）

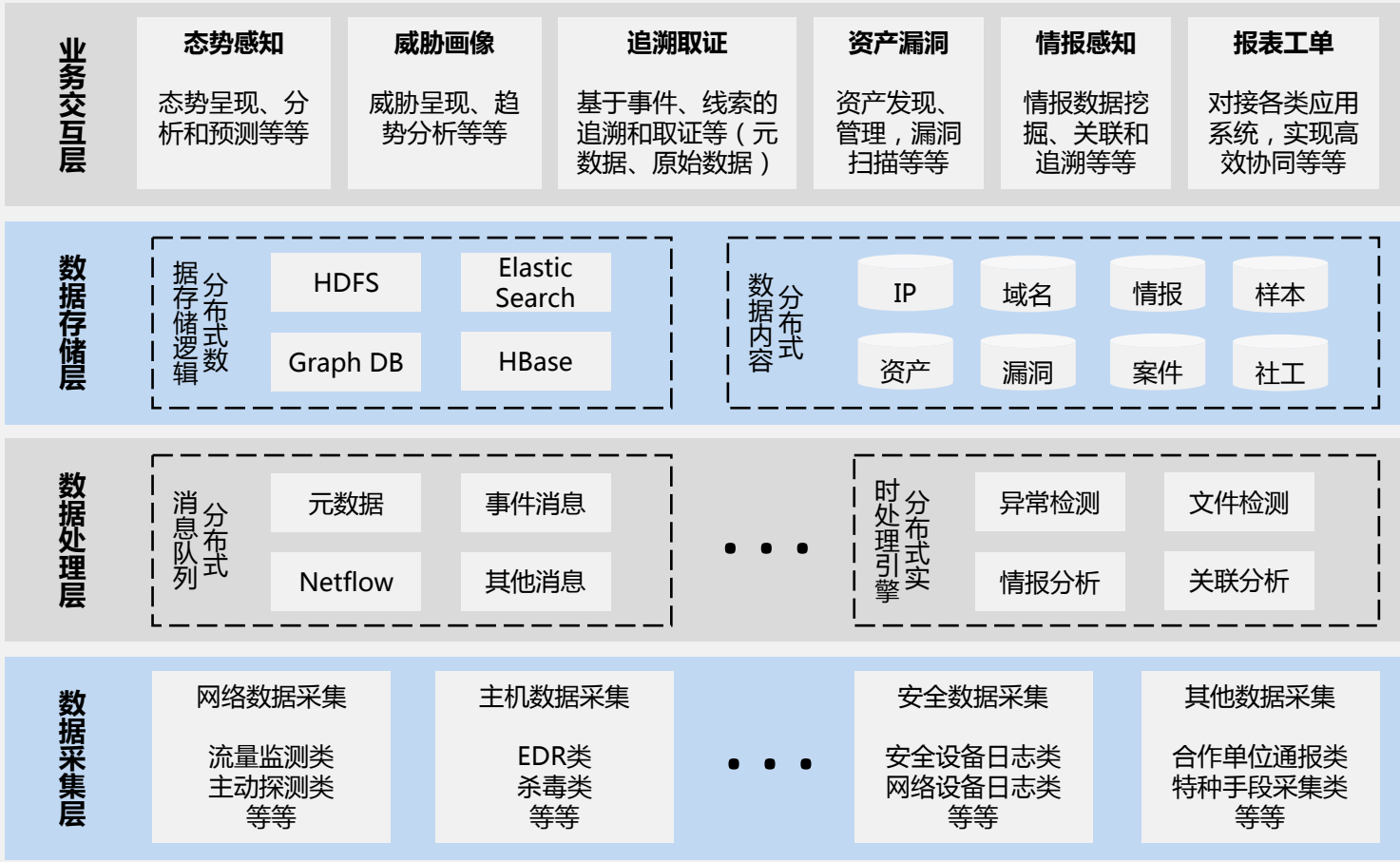


# 全流量回溯取证系统（TFS）



# 大数据威胁情报云（CTI）

# 大数据安全智能分析系统（CIC）



# 核心技术

业界唯一产品化的基于**机器学习/深度学习**的恶意代码变种**基因图谱检测**技术


业界领先的基于**机器学习/深度学习**的**Fast-Flux（DGA）僵尸网络主机**C&C通讯检测技术

业界领先的基于**机器学习/深度学习**的恶意代码频繁行为模式挖掘及**未知威胁检测**技术

业界领先的基于**分布式图挖掘**的全球**威胁情报关联分析及追溯取证**技术

人工智能技术专利

011721191-E

# 中华人民共和国国家知识产权局

100192

北京市海淀区学清路 8 号 B 座 1601A
北京安信方达知识产权代理有限公司 李红爽(82730790),李丹
(82730790)

发文日：

2017 年 07 月 06 日

申请号或专利号：**201710543651.9**　　发文序号：**2017070600285070**

## 专利申请受理通知书

根据专利法第 28 条及其实施细则第 38 条、第 39 条的规定，申请人提出的专利申请已由国家知识产权局受理。现将确定的申请号、申请日、申请人和发明创造名称通知如下：

申请号：201710543651.9

申请日：2017 年 07 月 05 日

申请人：北京金睛云华科技有限公司

发明创造名称：一种恶意代码家族的训练和检测方法及装置

011721277-E

# 中华人民共和国国家知识产权局

100192

北京市海淀区学清路 8 号 B 座 1601A
北京安信方达知识产权代理有限公司 李红爽(82730790),李丹
(82730790)

发文日：

2017 年 07 月 26 日

申请号或专利号：**201710619576.X**　　发文序号：**2017072601783260**

## 专利申请受理通知书

根据专利法第 28 条及其实施细则第 38 条、第 39 条的规定，申请人提出的专利申请已由国家知识产权局受理。现将确定的申请号、申请日、申请人和发明创造名称通知如下：

申请号：201710619576.X

申请日：2017 年 07 月 26 日

申请人：北京金睛云华科技有限公司

发明创造名称：一种僵尸主机检测方法和装置

# 权威认证

国家计算机病毒应急处理中心计算

## 检验报

| | |
|---|---|
| 产品名称 | 高级威胁检测系统 SecureCloud V2.0 |
| 生产单位 | 北京金睛云华科技有限公司 |
| 委托单位 | 北京金睛云华科技有限公司 |
| 检验依据 | 公信安[2014]786 号《高级可持续价方法(试行)》 |
| 检验结论 | 经检验，该产品为增强级。 |
| 备注 | / |
| 审批 | 主检：徐超　　审核： |

计算机信息系统安全专用产品

# 销售许可证

证书编号：XKA11215

有效期：自 2017年 08月 25日

至 2019年 08月 25日

中华人民共和国公安部监制

北京金睛云华科技有限公司

根据公安部《计算机信息系统安全专用产品检测和销售许可证管理办法》及有关规定，经审查，准许你单位生产的(代理)

高级威胁检测系统 SecureCloud V2.0 (V2.0)

APT 安全监测产品(增强级)　　安全专用产品进入市场销售，特发此证。

2017年 08月 25日

# 典型用户

借贷宝

中华人民共和国公安部
The Ministry of Public Security of the People's Republic of China

中共中央网络安全和信息化领导小组办公室
Office of the Central Leading Group for Cyberspace Affairs

国家税务总局
State Administration of Taxation

中国移动通信
CHINA MOBILE
浙江移动通信有限责任公司

上海科技网
STNC

中国·南京
www.nanjing.gov.cn
网站群

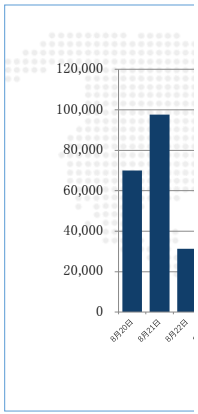
北京市商务委员会
BEIJING MUNICIPAL COMMISSION OF COMMERCE

北京信息科技大学
Beijing Information Science & Technology University

国家安全生产监督管理总局
State Administration of Work Safety

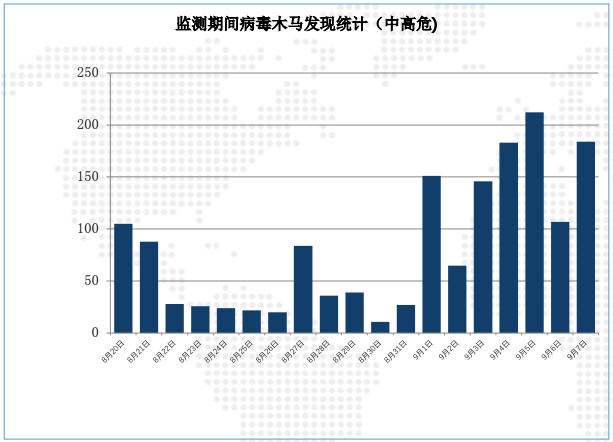
# 浙江移动G20安保

## 监测情




**攻击次数众多**：共计发
**方式组合使用**：监测其
**主要呈现问题**：内网设
**威胁性质确定**：通过详
TCP会话劫持和DDoS等

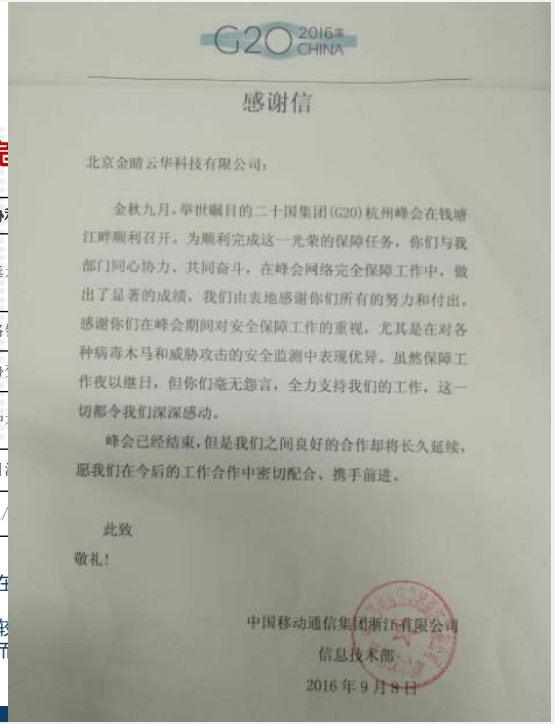
## 监测情况概述




**病毒木马发现**：监测期间共计发现中高危病毒木马1600次，20/21/27日平均每日在
**病毒木马种类**：种类繁多，有外连恶意IP、下载程序、盗取私密信息、发送数据、
**侵入方式**：特种木马采用组合攻击方式，同时有些有明显的逃逸和躲避行为，比较
**威胁性质确定**： BDS沙箱发现高危病毒木马后，结合云图、HTTP详细日志等，从而

高危

| 威胁 |
| --- |
| 病毒 |
| 网络 |
| 威胁 |
| 特种 |
| 零日 |
| 逃逸/ |



G20 2016 CHINA

感谢信

北京金暗云华科技有限公司：

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

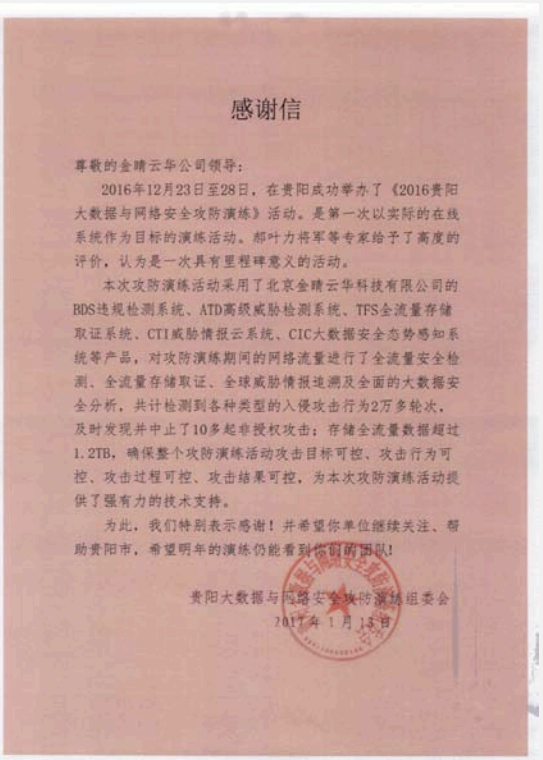
敬礼！

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

# 贵阳大数据与网络安全攻防演练

感谢信

尊敬的金晴云华公司领导：

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。郝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晴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15日


THANK YOU