RSA CONFERENCE
CHINA 2012

RSA信息安全大会2012

THE GREAT CIPHER

MIGHTIER THAN THE SWORD

伟大的密码胜于利剑

下一代安全的战略思考 – 应对下一代威胁

Strategic Thinking on Next Generation Security in Cloud Era

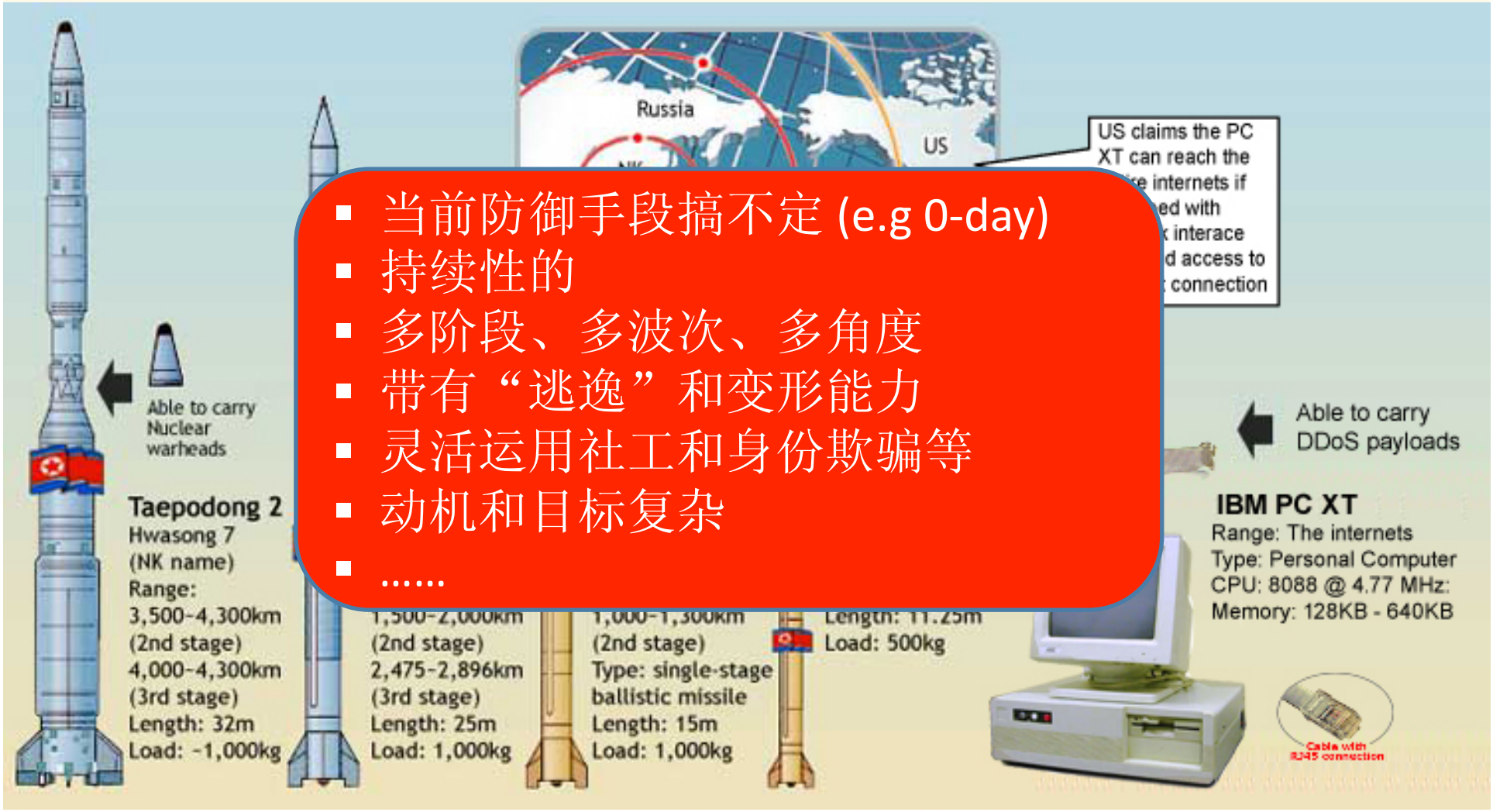
赵粮

richard.zhao@nsfocus.com

绿盟科技

RSA CONFERENCE CHINA 2012

“下一代”威胁



- 当前防御手段搞不定 (e.g 0-day)
- 持续性的
- 多阶段、多波次、多角度
- 带有“逃逸”和变形能力
- 灵活运用社工和身份欺骗等
- ……

“当代”安全设备力不从心

业务越来越复杂，新应用太多，用户位置多变，终端BYOD多样化并且很难规范化

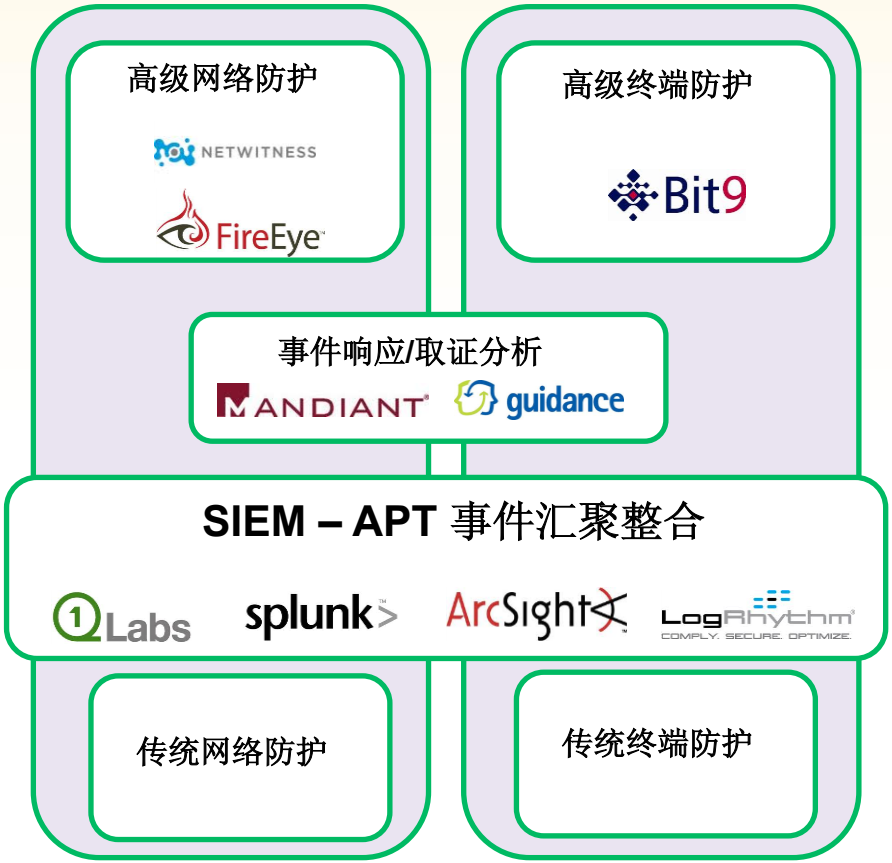
- 端口失效 - > Applications
- IP地址失效 -> Users
- 数据包层面的检查失效 -> Content

- 攻击变化太快，现有的黑名单机制总是更新不及时
- Advanced Malware,
- Zero-Day,
- Targeted APT Attacks

AV

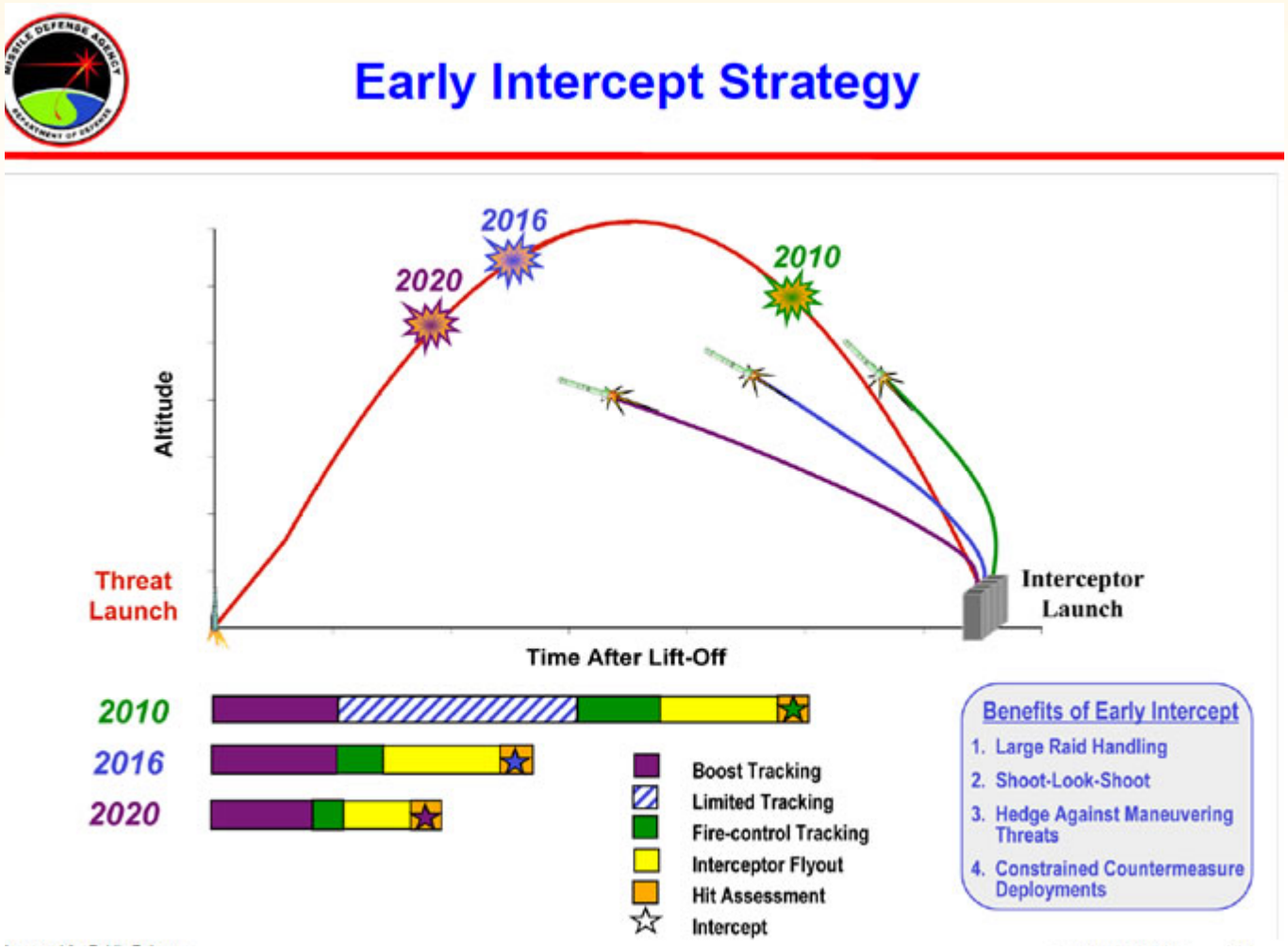
- 病毒样本不胜其多，反病毒程序消耗计算机资源不胜其负
- 病毒样本库更新太慢
- “特征”匹配很容易被“躲避”
- …

针对下一代，千帆竞渡、各显神通



Early Intercept Calls For Kills At Extended Range

RSA CONFERENCE CHINA 2012



http://defense-update.com/20101118_aegis_ng_early.html

三个假设及其推论

假设1： 攻击者正在转向经济目的，攻击者和防守者之间的竞争关键是成本。获得成本优势的一方将会获得“战场”上的优势态势。

假设2：为了降低成本，攻击者必须尽可能地重复使用（Reuse）其攻击代码、工具、僵尸、技术和手法等。

推论1：一般来说，一种威胁或攻击会出现在多个场合，在一些场合中检测出来并证明为威胁或攻击的行为有非常大的概率在另外的场合下也是威胁或攻击。

推论2: 重用越少，意味着成本越高，越难以检测

假设3：为了降低成本，防守者必须重构防御体系，将部分密集的、重复性的计算转移到“云”中进行，而将计算产生的“智能”（Intelligence）推送到防御功能点（Defense Function Point）。

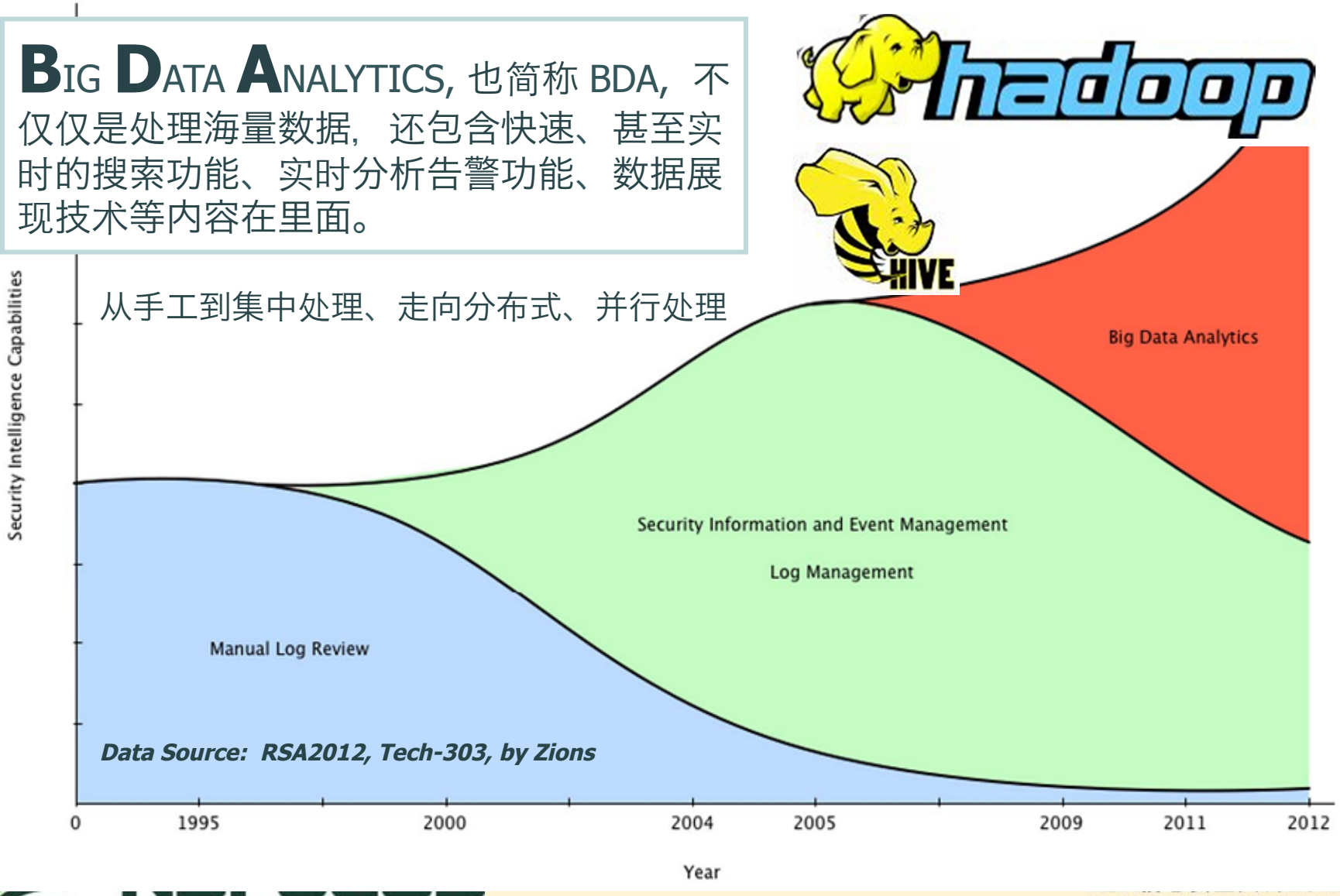
推论3: 覆盖越大的“云”检测能力相对更强

推论4: 生产成本相对固定，越能多次使用越能降低成本

From SIEM to BIG DATA & Intelligence

BIG DATA ANALYTICS, 也简称 BDA，不仅仅是处理海量数据，还包含快速、甚至实时的搜索功能、实时分析告警功能、数据展现技术等内容在里面。

从手工到集中处理、走向分布式、并行处理



大数据不仅仅是数据

定理1：大数据需要数据

定理2：大数据需要安全攻防知识

定理3：大数据需要抽象和数学建模能力

定理4：大数据需要长时间的、大范围的运营和积累

攻防

数据

建模

智能

手法|模式|信誉|规则|态势|趋势…

安全智能是下一代安全的关键能力

RSA CONFERENCE CHINA 2012

Signature + Behavior + Reputation

Global &
Cross Enterprise

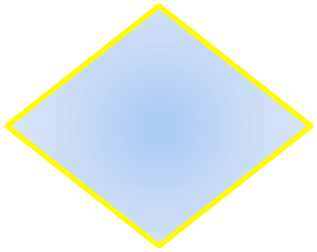
Enterprise

Device

Session

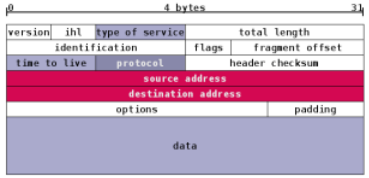
Packet

Intelligence



Self-Healing

More business
Awareness



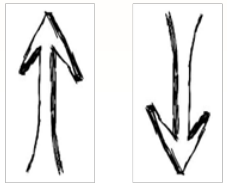
Data → Decision Making Engine → Action

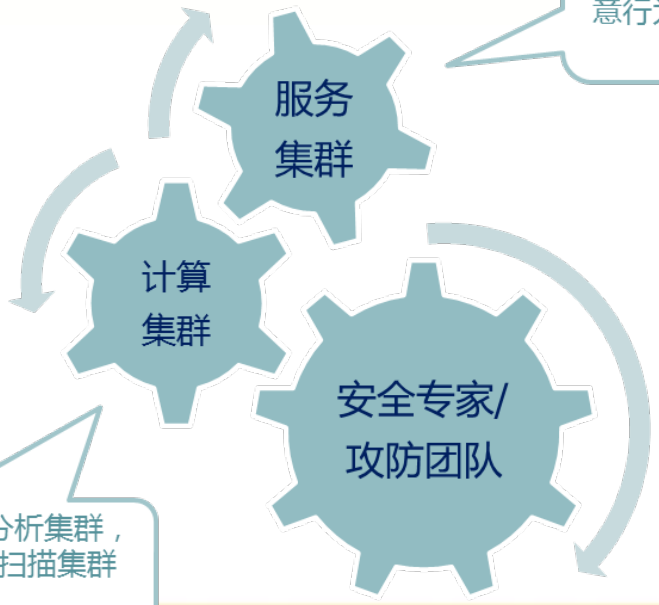
NSFOCUS

RSA信息安全大会2012

智能驱动的下一代安全图像

业务识别能力
信息获取能力
处理逻辑和规则分离
快速升级能力
灵活部署能力

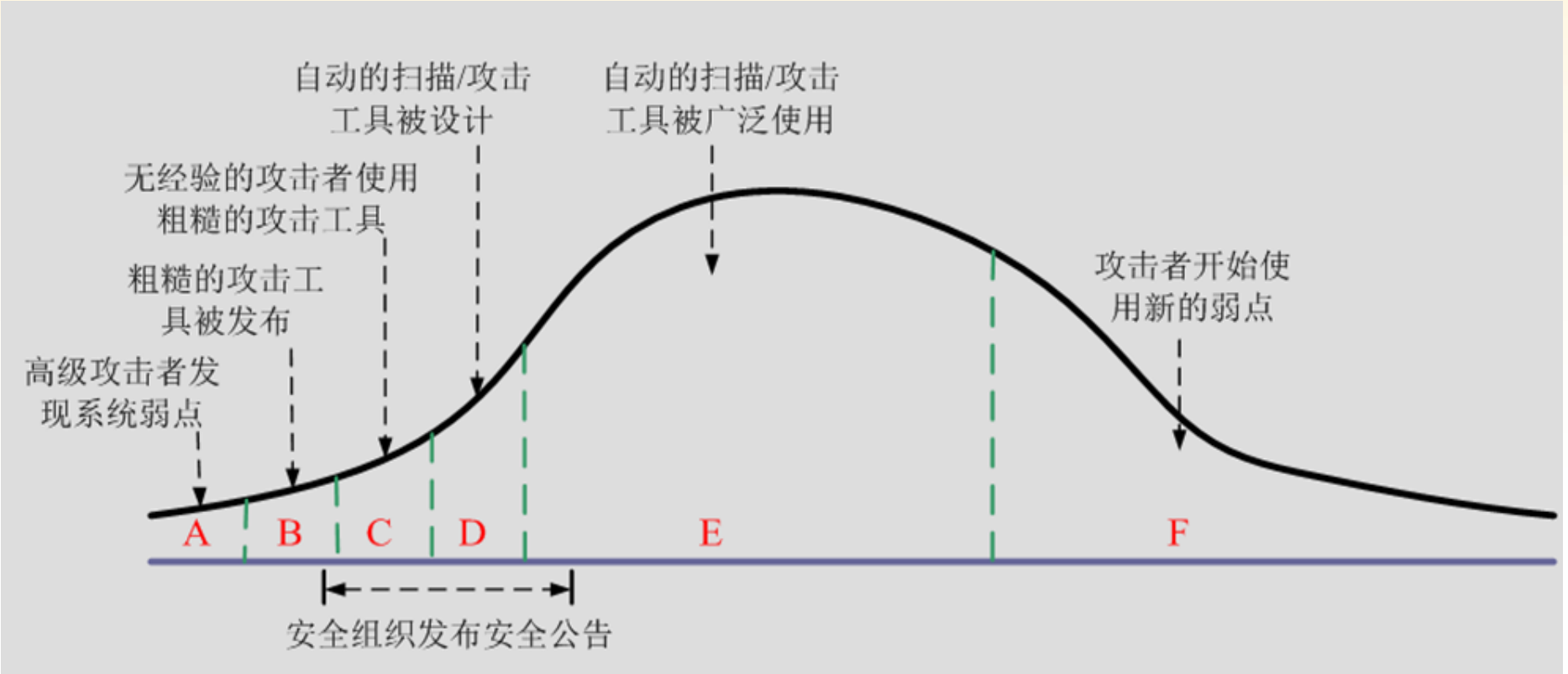




IP信誉/文件信誉/域名信誉/URL信誉/恶意行为/安全漏洞/攻击手法/...

页面爬取集群，页面内容分析集群，恶意代码分析集群，漏洞扫描集群
智能挖掘集群

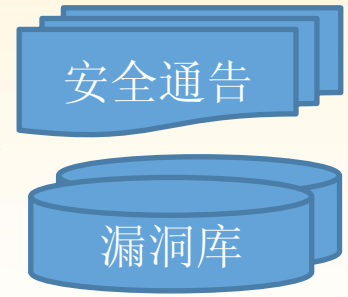
漏洞威胁指数曲线



- 每个漏洞都有各自的生命周期
- 生命周期的不同阶段，威胁大小不同。
- 参考当前威胁指数及变化趋势，可以做出漏洞管理的决策

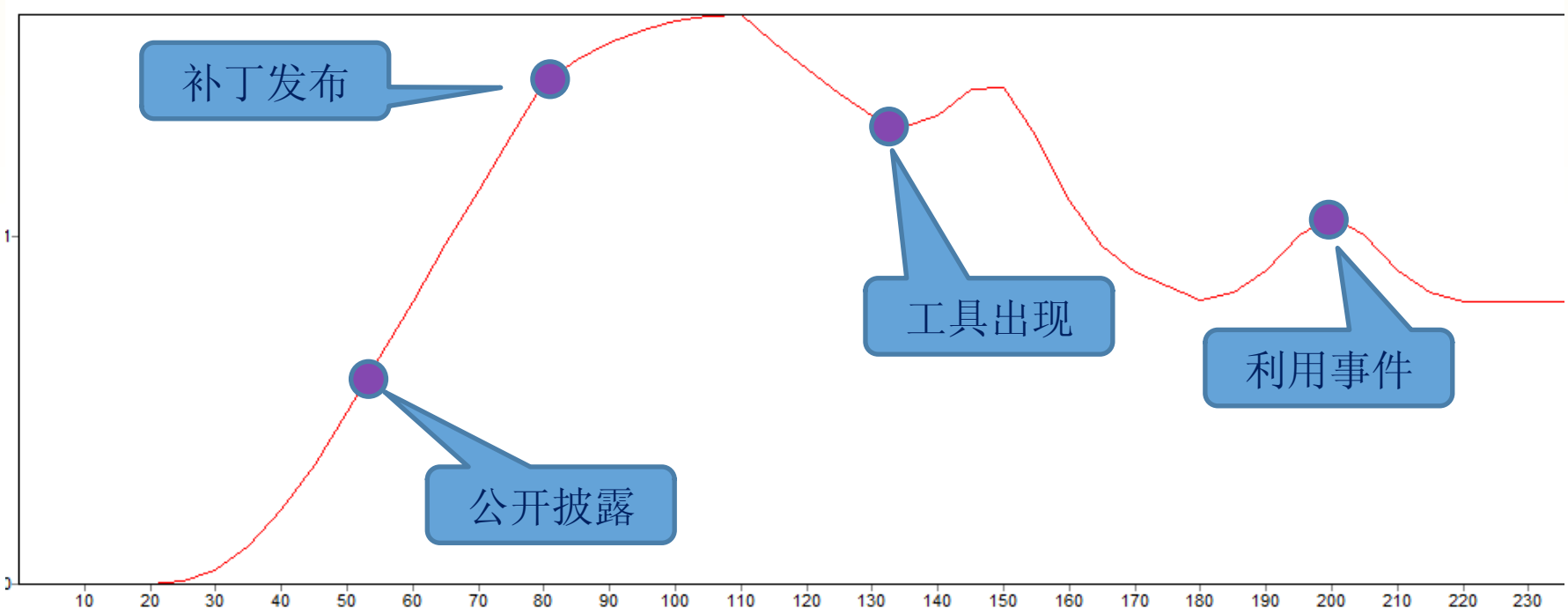
漏洞威胁指数曲线

- CERT
- 安全厂商
- 政府机构
- 安全组织



分析计算

I_T (漏洞威胁指数)



- 每个漏洞生命周期里程碑事件影响威胁的大小
- 不同的漏洞，里程碑事件的出现顺序不尽相同

Google Hacking, OSINT and …

RSA CONFERENCE CHINA 2012

SearchDiggity

SearchDiggity 2.5 is the primary attack tool of the Google Hacking Diggity Project. It is Stach & Liu's MS Windows GUI application that serves as a front-end to the most recent versions of GoogleDiggity, BingDiggity, Bing LinkFromDomainDiggity, Google CodeSearchDiggity, DLPDiggity, FlashDiggity, and MalwareDiggity. It includes:

- GoogleDiggity
- BingDiggity
- FlashDiggity

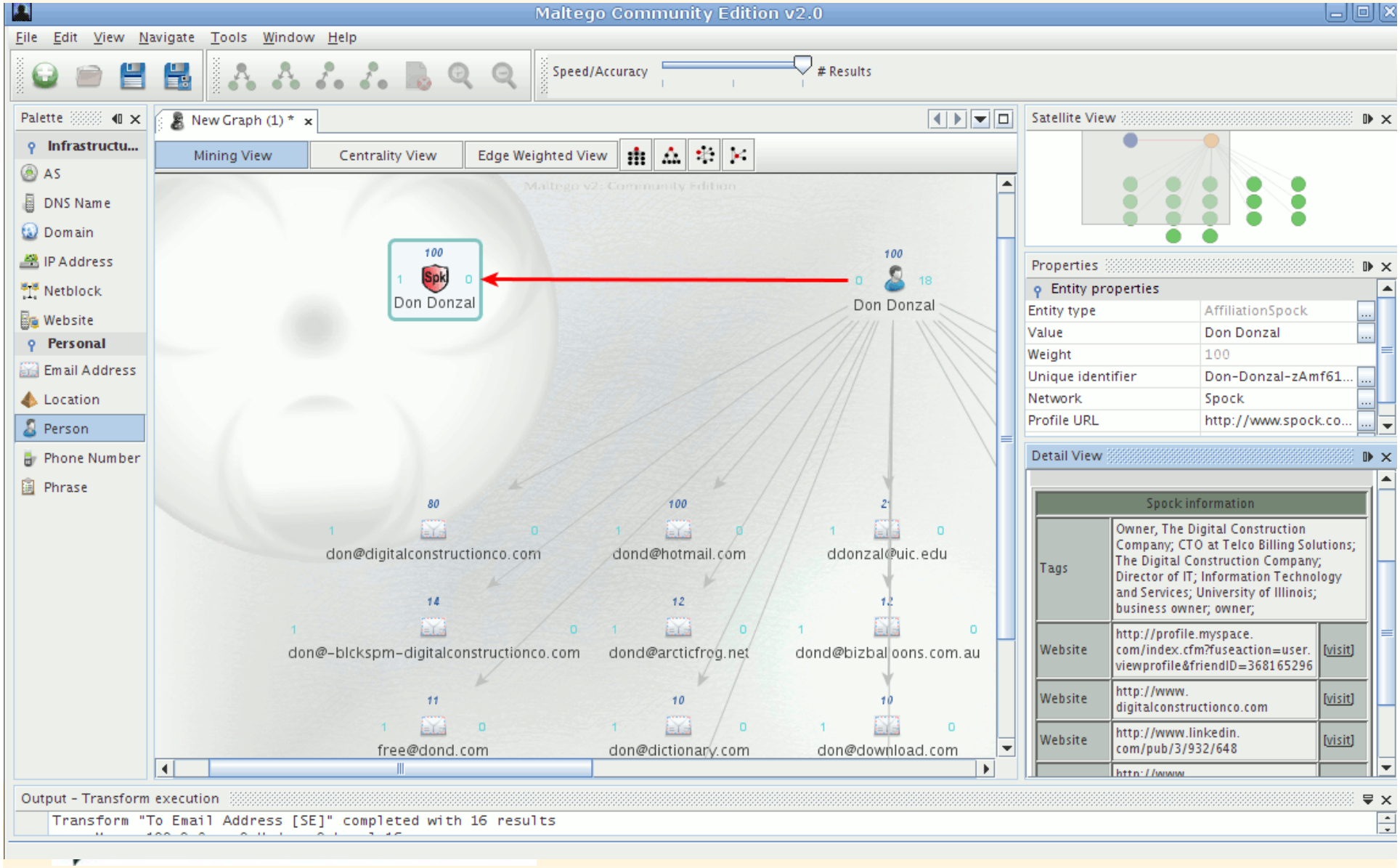
Description	
Vulnerability	Sensitive Information Disclosure via Google
Description	This scan is based on search result on google and may generate false positive. Google is a very popular search engine. By editing search conditions, you can get some documents and sensitive information from a website through Google, including documents of doc, ppt, xls, vsd, prj, ini formats.
Solution	Enumerated documents in the search result include non-public information. You are suggested to restrict access privilege to these documents.
Risk Value	3
Dangerous Plugin(s)	No

NSFOCUS WSM

http://www.stachliu.com/resources/tools/google-hacking-diggity-project/attack-tools/

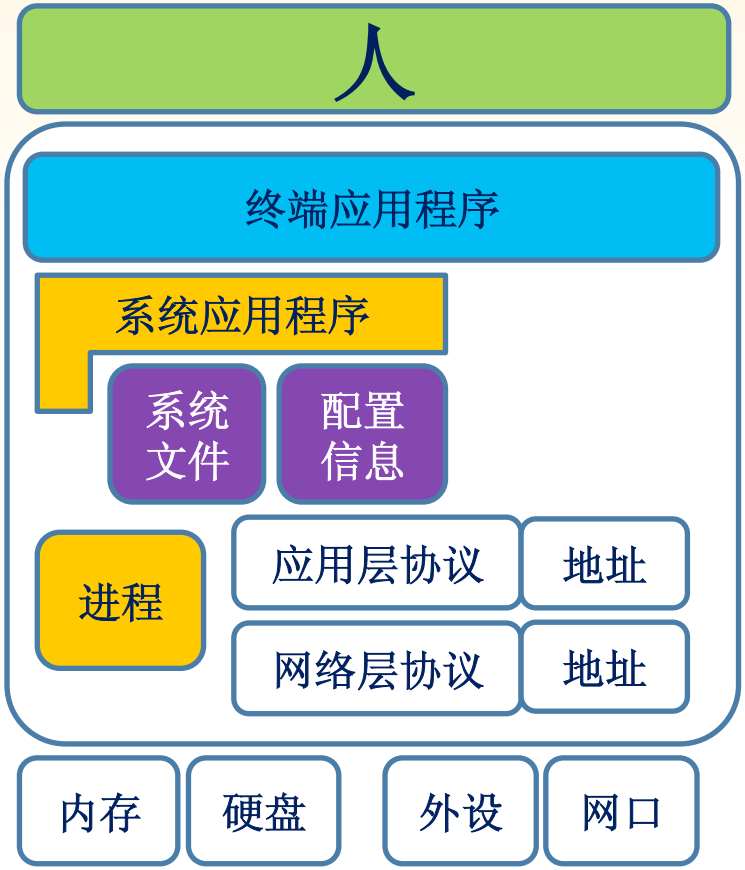
Maltego

RSA CONFERENCE CHINA 2012

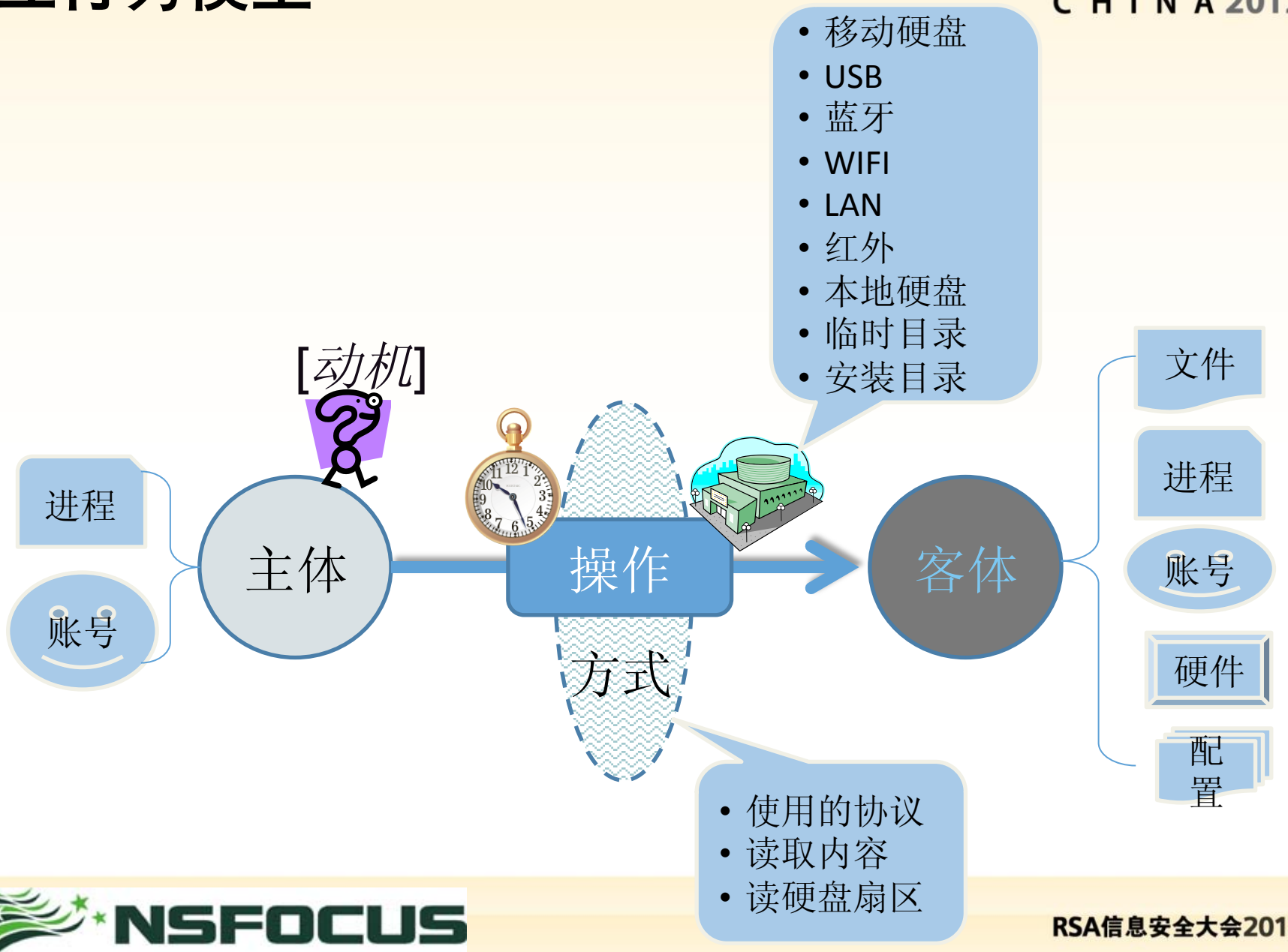


关于行为和行为异常发现

- 什么是“行为”？
  - 行为是分析目标和信息系统产生互动、引起信息系统发生某些改变的过程。行为可以由一个或多个信息系统的记录来描述。
- 什么是“异常”？
  - “当然了，不正常吗，就是异常了”…
- 怎么发现“异常”？
  - 把“正常”得拿出去了…

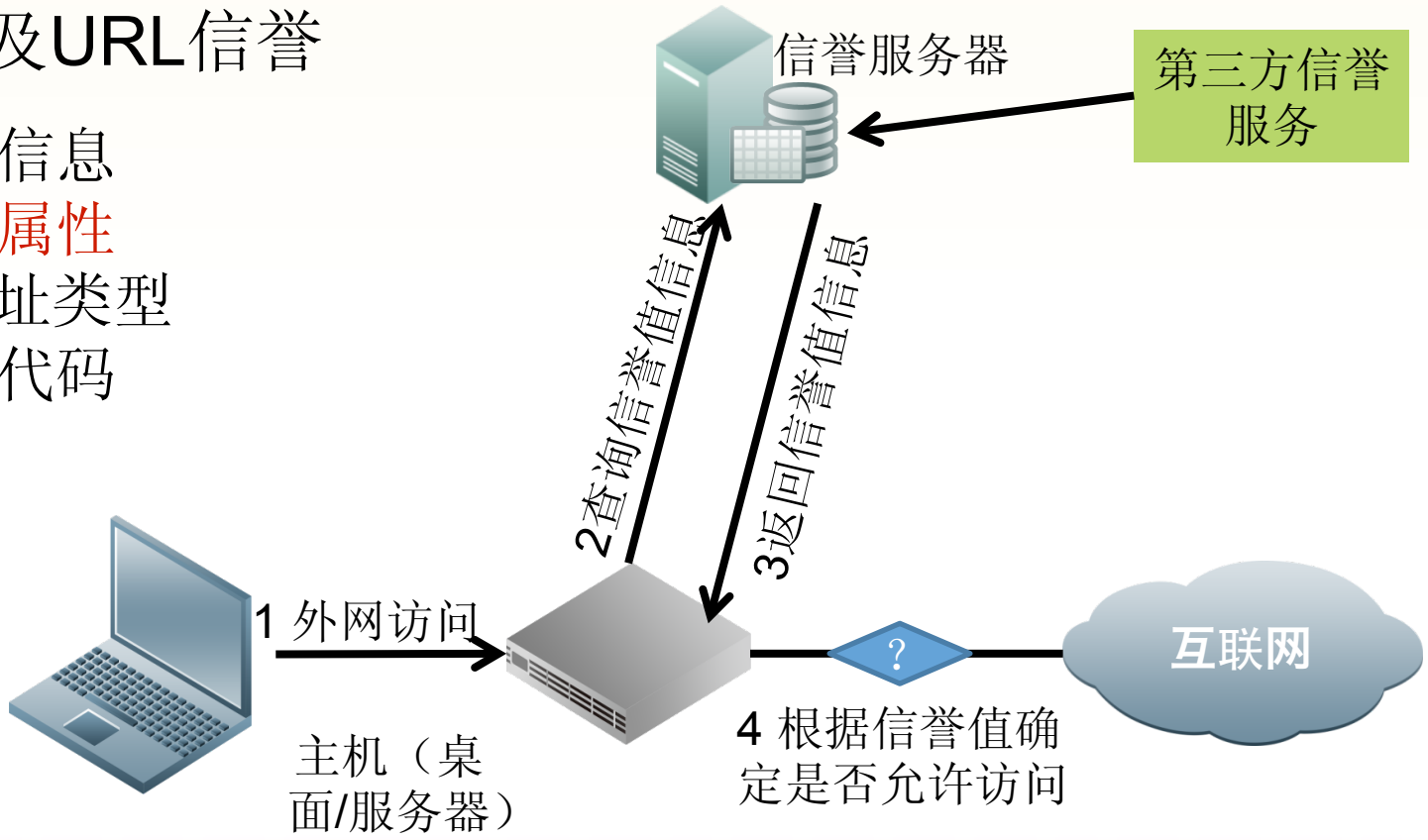


建立行为模型


• 移动硬盘
• USB
• 蓝牙
• WIFI
• LAN
• 红外
• 本地硬盘
• 临时目录
• 安装目录
[动机]
进程
账号
主体
操作
方式
客体
文件
进程
账号
硬件
配置
• 使用的协议
• 读取内容
• 读硬盘扇区

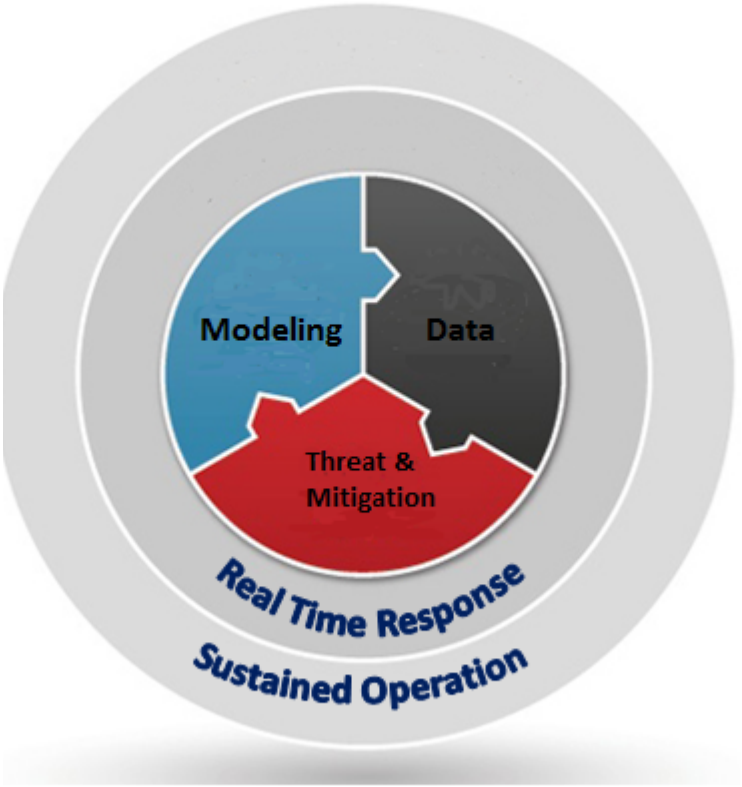
网络层面的各种“信誉”体系

- 对IP地址和URL建立信誉评价
- IP地址及URL信誉
  - ✓ 漏洞信息
  - ✓ 域名属性
  - ✓ IP地址类型
  - ✓ 恶意代码



针对下一代威胁，下一代安全需要…

- 前端地位将会下降，”云“端重要性逐渐凸显
- 基于异常和信誉的检测和防护方法重要性凸显
- 攻防、数据、建模、实时响应、持续运营五个因素缺一不可



谢谢

Richard.zhao@nsfocus.com

RSA CONFERENCE
CHINA 2012