



*Rachel & Sean @ Switzerland  
Sep 18th, 2013*

# 从概念到实践，威胁情报的落地

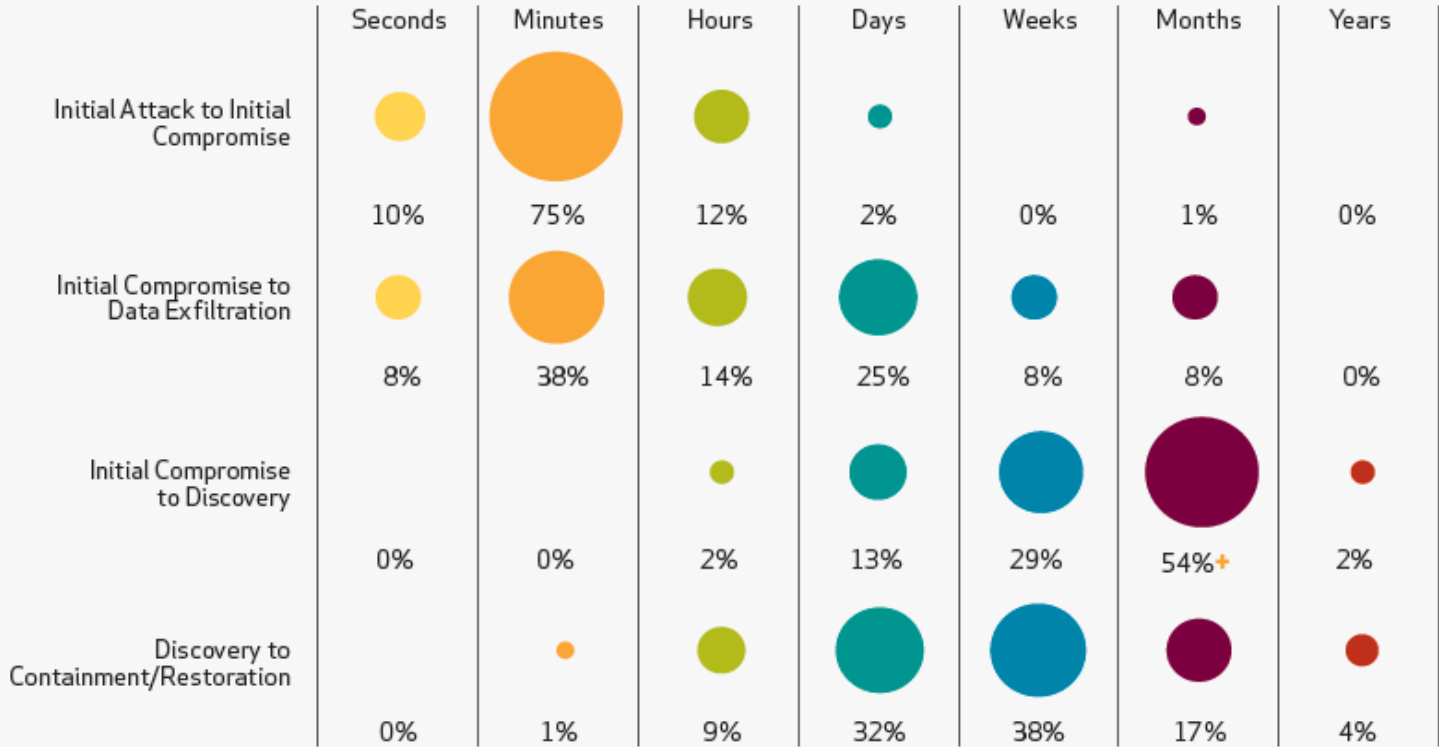
NUKE@Sec-UN

# 安全威胁情报的概念



# 当前的网络安全防护体系已落后攻击技术发展

Figure 40. Timespan of events by percent of breaches





# 对网络安全防护体系提出了更高的要求

海量安全事件中真正有价值的攻击事件的发现

识别传统安全产品难以发现的APT定点攻击

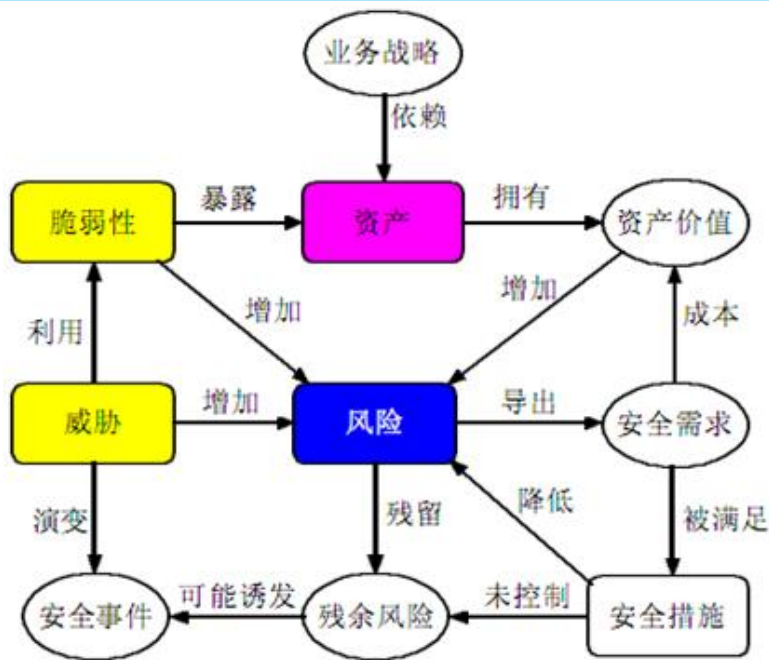
解决组织间及组织内部对攻击事件的快速协同

提供安全设备和解决方案中跨产品、跨厂家的协同



# 安全威胁情报是什么？

## 从经典“风险模型”开始



资产

脆弱性/漏洞

威胁

安全事件

安全措施

.....

# 安全威胁情报是什么？

## 安全情报/安全智能

资产情报

安全漏洞情报

安全威胁情报

安全事件情报

安全措施情报

业务战略情报

安全需求情报

威胁定义：可能导致对系统或组织危害的不希望事故的潜在起因，其属性包括主体、资源、动机、途径等。

威胁情报定义：针对一个已经存在或正在显露的威胁或危害资产的行为的，基于证据知识的，包含情境、机制、影响和应对建议的，用于帮助解决威胁或危害进行决策的知识。

# 安全威胁情报是什么？

威胁源

APT29, Sofacy, Dark Seoul, Unit 8200.....

攻击目的

Operaton Iron Tiger, Operation Russian Doll ,  
Stuxnet.....

攻击对象/与哪些事件关联

XX国家, 政府, 金融, 军队, 高科技, 电厂.....

攻击手法

鱼叉, 钓鱼, 水坑, WEB渗透, 网络植入.....

利用漏洞

CVE-2014-6352, CVE-2016-0167.....

IOCs

样本HASH, C2域名/IP, 邮箱, 跳板IP, .....

COA

预警、阻断.....

.....

.....



# 战略 vs. 战术

## 战略



- 人的对抗
- 利用人的智能
- 以人为核心的防护体系

## 战术

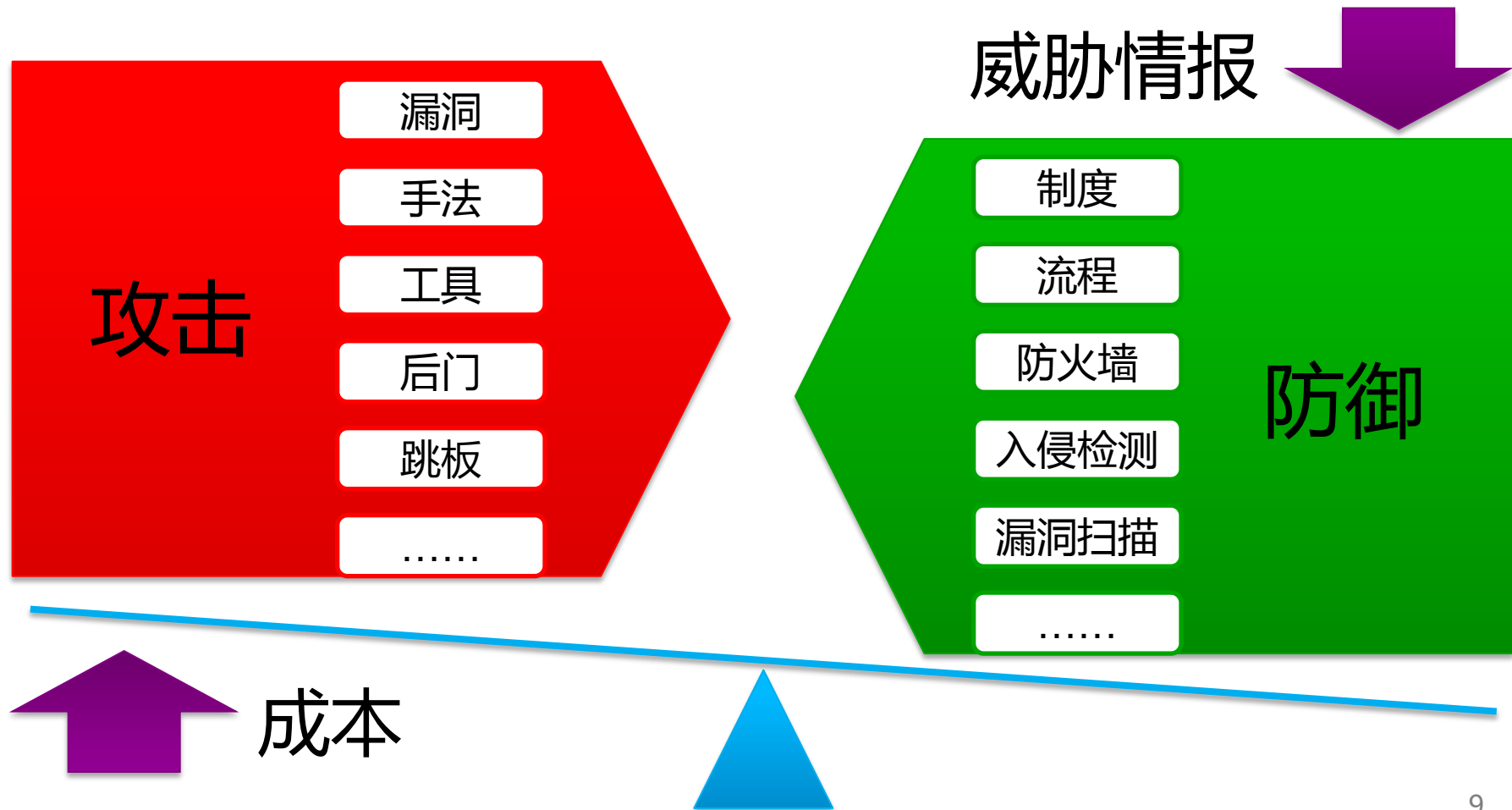


- 机器的对抗
- 利用设备的功能
- 以情报为手段的防护体系

**Intelligence**

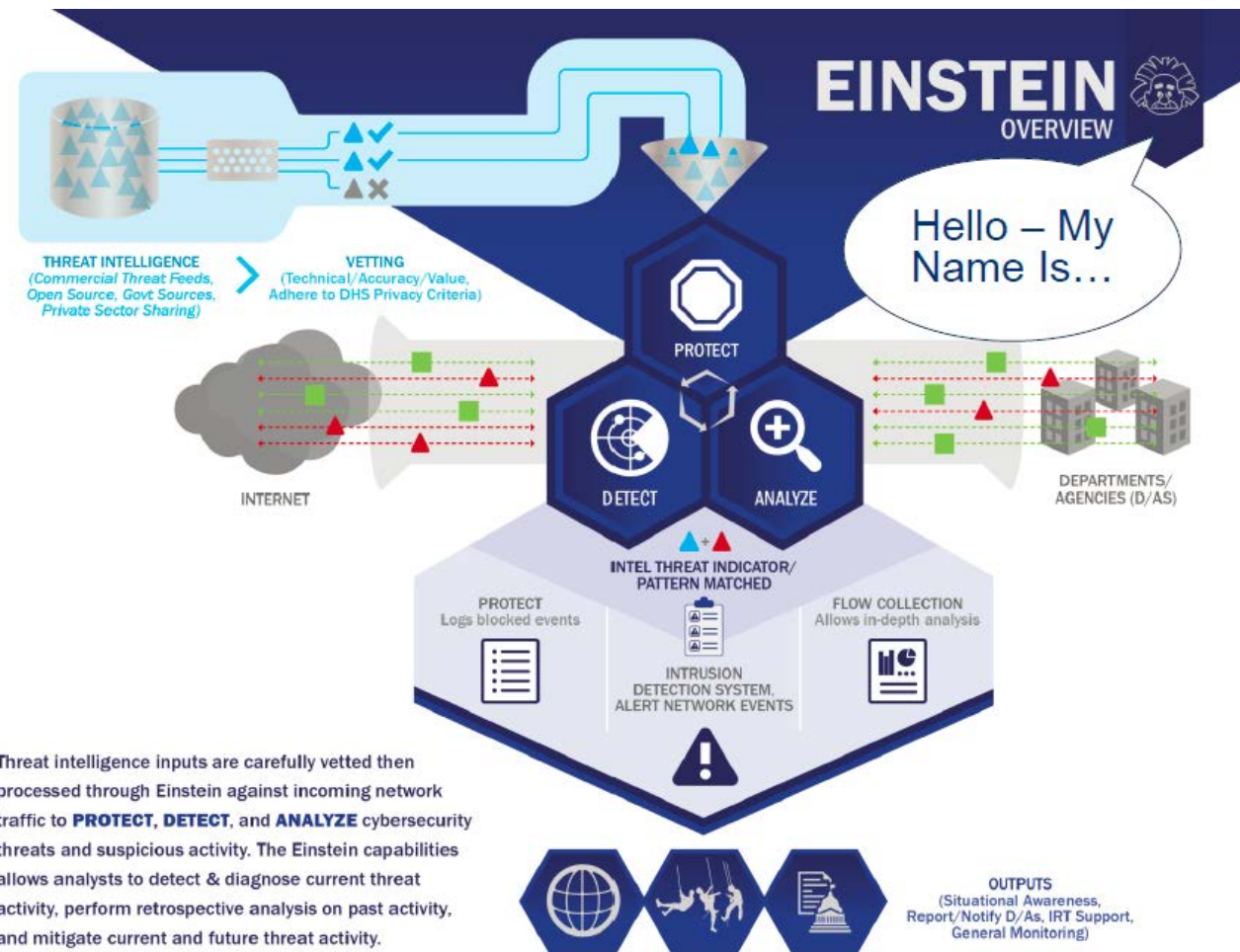


# 网络安全威胁情报是一种可能改变攻防态势的技术



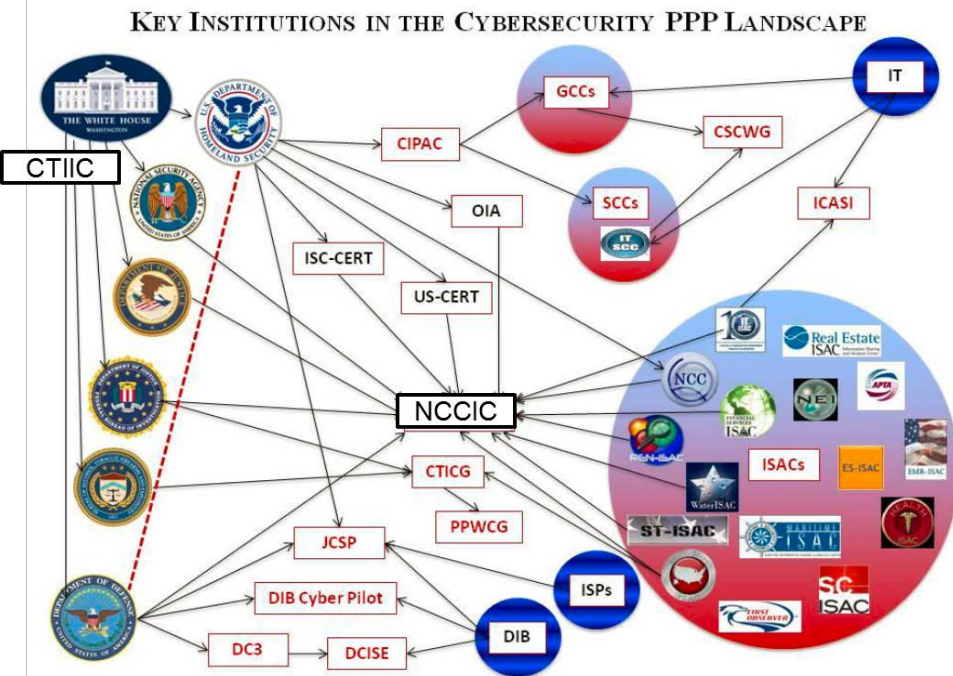
# 国际安全威胁情报的发展情况

# 国外政府层面对威胁情报的采用



- ~17B flows/day
- 300+ sensors
- 100+ organizations
- ~39M IP addresses monitored
- ~9M observed/day
- ~45M IP addresses observed/day
- ~3B IP addresses observed all-time

# 国外在政府和民营间交换威胁情报



## 网络安全信息共享法案/CISA 2015 Cybersecurity Information Sharing Act 2015

-建立一个自愿信息共享系统，该系统将由美国国土安全部管理。如果机构在其网络上检测到不寻常或可疑的活动，可将这一信息分享到安全部，安全部将给其他公司发出警报。

## 信息共享与分析中心/ISACs Information Sharing and Analysis Centers

-收集、分析、脱敏及传递来自私营企业的信息，并向行业和政府传递的中心。也可以从政府发布信息给私营企业。

## 国外在政府和民营间交换威胁情报

## Cyber Information Sharing and Collaboration Program (CISCP)

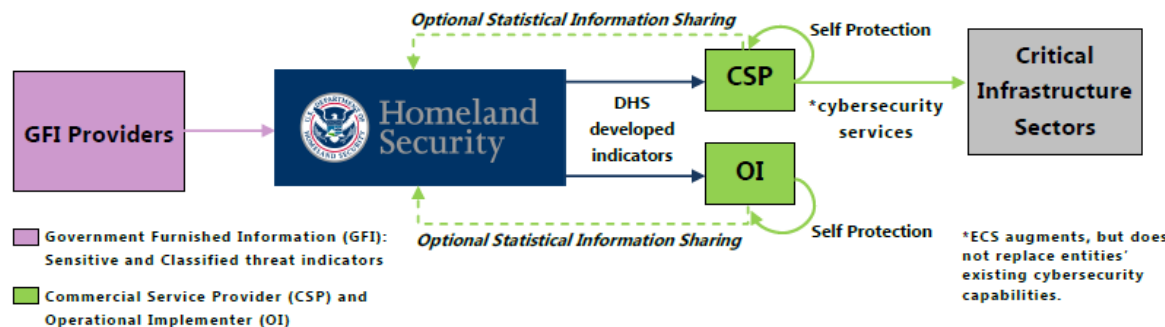


## 2012年开始

- 指示器公告、分析报告、优先告警、推荐实践
- 每周100个威胁指示器、已经产生1900份输出物和30000个威胁指示器
- 112个伙伴公司或ISACs，并额外133个存在交互

## Enhanced Cybersecurity Services (ECS)

## Enhanced Cybersecurity Services Program Model



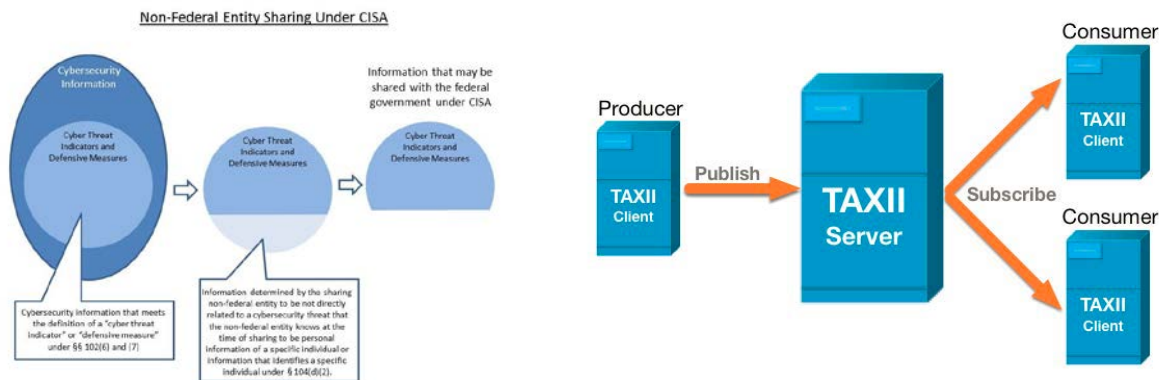
## 2013年2月的13636号总统令

- DNS Sinkholing
- E-mail Filtering

\*ECS augments, but does not replace entities' existing cybersecurity capabilities.

# 国外在政府和民营间交换威胁情报

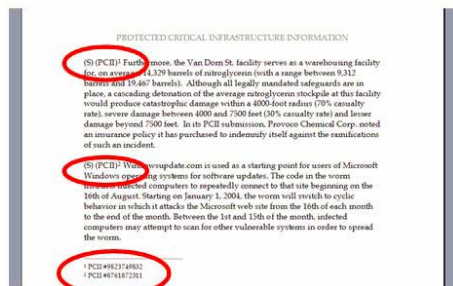
## Automated Indicator Sharing (AIS)



2015年12月的CISA法案

- Cyber Threat Indicator
- Defensive Measure

## Protected Critical Infrastructure Information Program (PCII)




2002年PCII法案  
2009年4月流程手册  
2012年1月工作产品指南



# 国外已提出建设基于威胁情报的生态系统

## Ecosystem


UNCLASSIFIED



### Achieving a Secure and Resilient Cyber Ecosystem: *A Way Ahead*

January 2016

*Continuing to strengthen the security and resilience of our nation's critical infrastructure in partnership with you...*

 Homeland Security PRE-DECISIONAL / NOT FOR DISTRIBUTION UNCLASSIFIED

UNCLASSIFIED

### Cyber Ecosystem



Secure Cyber Ecosystem

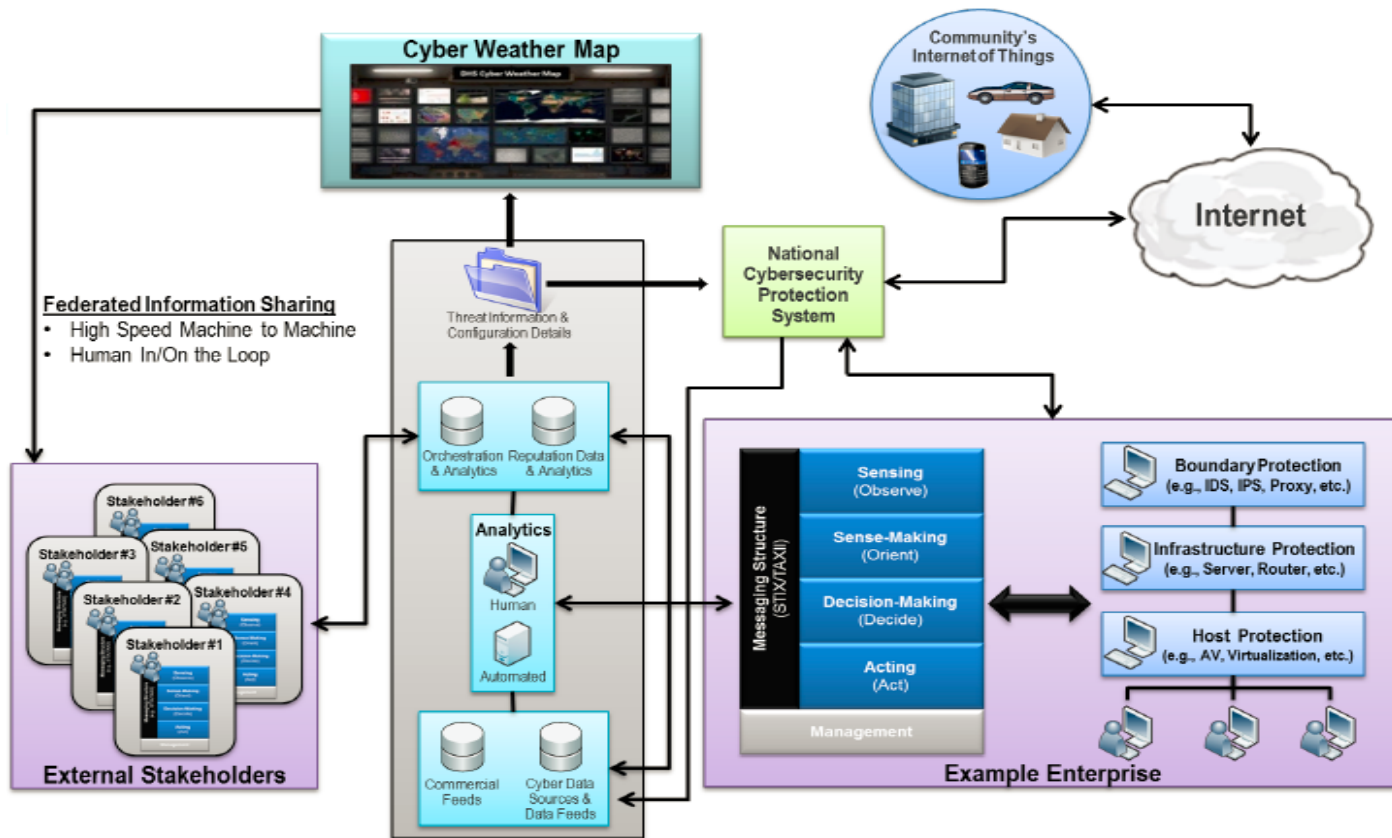
 Homeland Security PRE-DECISIONAL / NOT FOR DISTRIBUTION UNCLASSIFIED

15

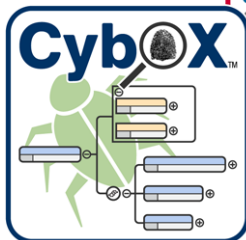


# 国外已提出建设基于威胁情报的生态系统

## DHS Secure and Resilient Cyber Ecosystem Example Architecture



# 美国在威胁情报标准方面早已布局，正推向国际标准



# 国外一线组织和厂家已经普遍支持威胁情报标准



最新清单见 <http://stixproject.github.io/supporters/>

# 威胁情报的实践与落地

# RSA 2015 vs. RSA 2016



# 2015

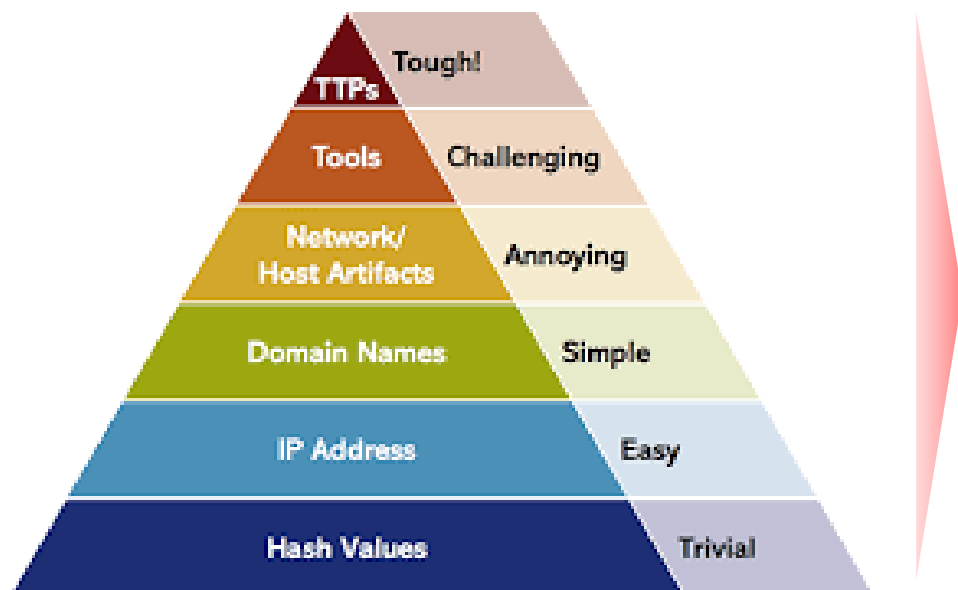


# 2016

## 热词趋势

DATA	CYBER	RISK	CLOUD
THREAT	INTELLIGENCE	MOBILE	MANAGEMENT
LEARN	PRIVACY	NEW	DEVICES
SMART	INFRASTRUCTURE	IOT	THING

# 从威胁情报到协同响应



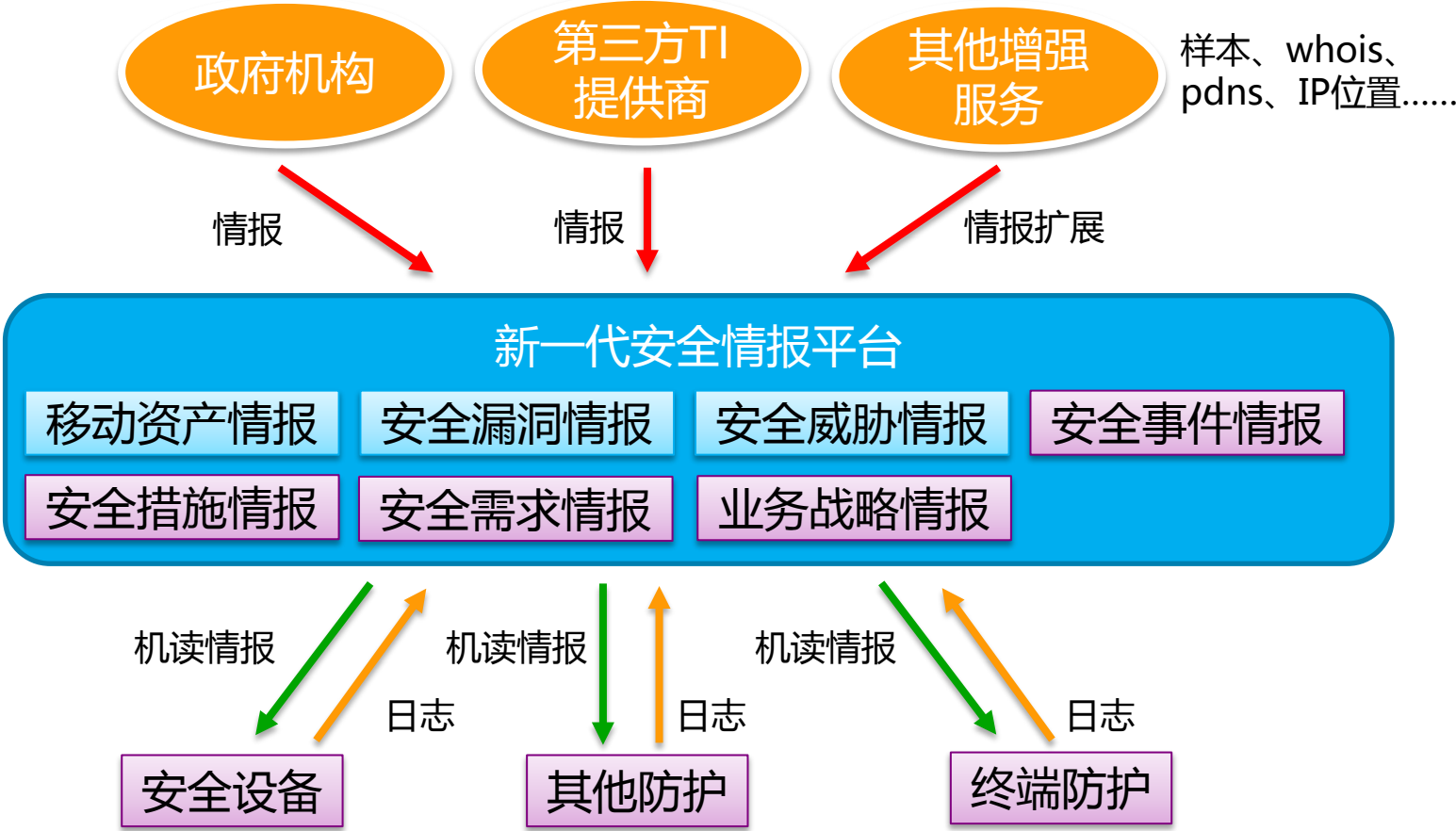
Source: David J. Bianco, personal blog

**有病！**



**有药！**

# 新一代基于情报的安全体系





# 威胁情报对安全体系的价值

事后	分析	<ul style="list-style-type: none"><li>✓ SIEM、FW等日志的信息扩展</li><li>✓ 威胁（源）分析</li><li>✓ 攻击溯源</li><li>✓ .....</li></ul>
事中	检测/响应	<ul style="list-style-type: none"><li>✓ FW、IPS、AV等基于IOC的阻断</li><li>✓ SIEM、IDS、FW等基于IOC的检测</li><li>✓ 应急响应</li><li>✓ .....</li></ul>
事前	预警	<ul style="list-style-type: none"><li>✓ 跨组织、跨设备的信息共享</li><li>✓ 基于情报的预测</li><li>✓ 与资产、漏洞等结合的告警</li><li>✓ .....</li></ul>



---

# 讨论!

