

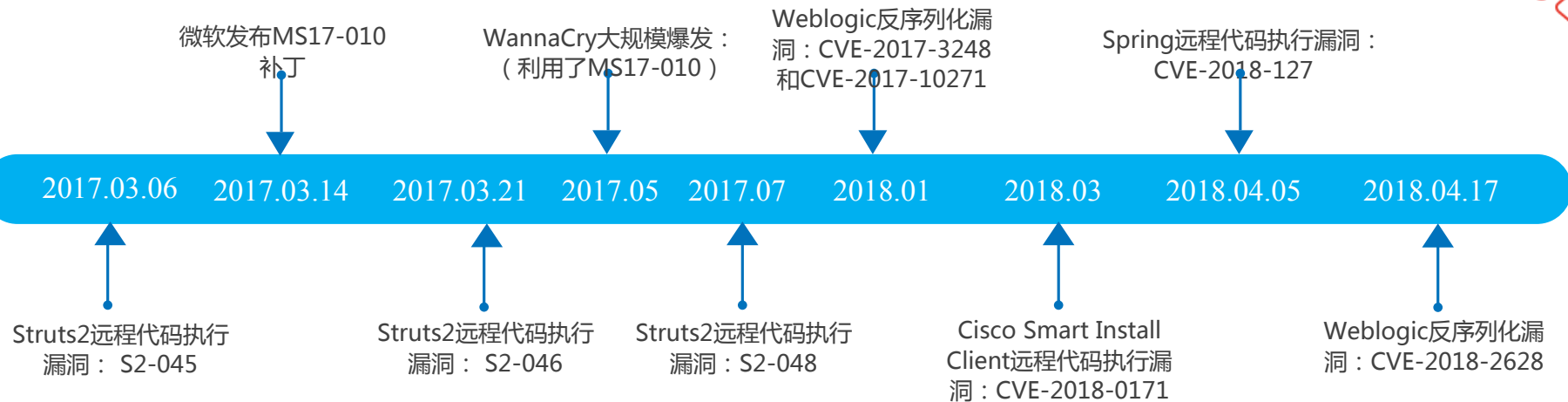
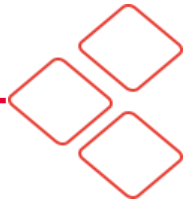


# 互联网资产管理与漏洞运营实践 &安全产品线

安全技术团队

HUATAI  
SECURITIES

# 最近一年的重大漏洞



## 漏洞检测能力

应对不断爆发的高危漏洞，需要全面、持续和高频率的漏洞检测能力。

## 互联网资产管理

企业应该精确掌握其互联网资产，特别是Struts2、Weblogic这些漏洞大户的使用情况。

## 补丁管理

基于资产的补丁管理，而不是漏洞响应。  
WannaCry的爆发在微软发布MS17-010补丁发布2个月后。

# “知己知彼，百战不殆” ——精细化的互联网资产管理



“某IP地址的某端口存在RCE漏洞，这个IP和端口是谁在用？”

“情报显示新爆发了struts2漏洞，我们是否用到了struts2框架？”

“这个有漏洞的服务器/应用我早就不用了，可以随时下线”

“这个页面是后台管理页面，不需要暴露在互联网的”

落实IP地址、端口与人的对应关系

精确了解线上系统高危组件和框架的使用情况。

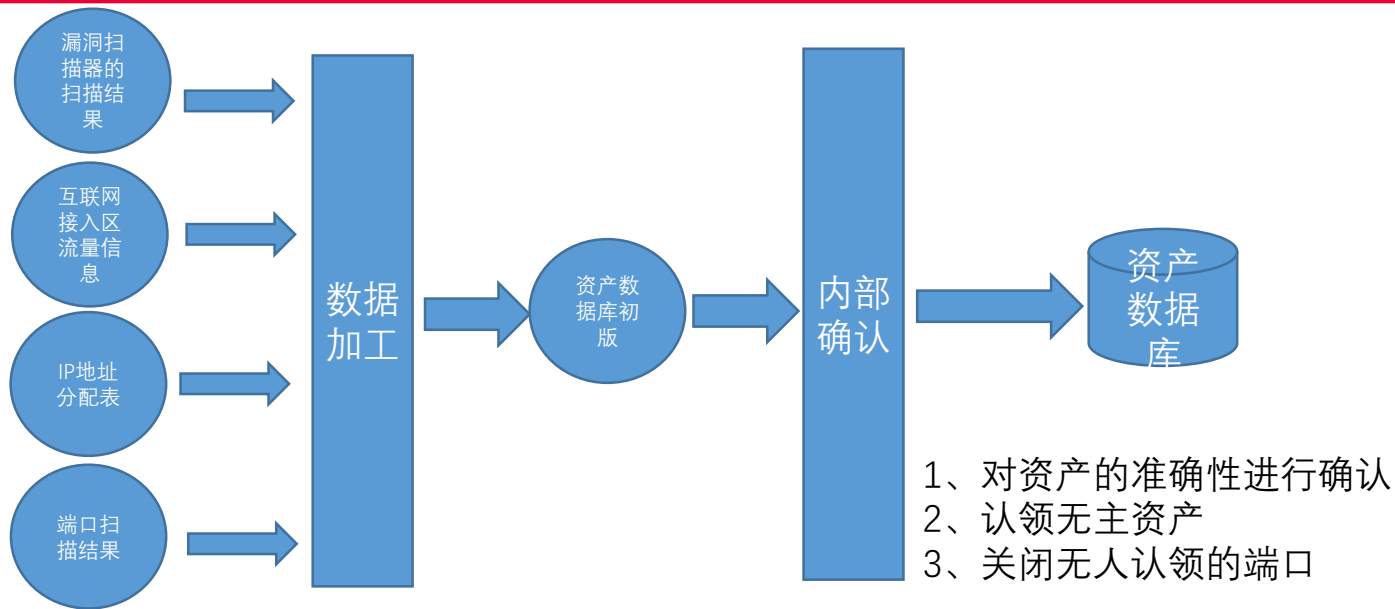
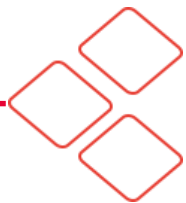
下线无用的服务器、清理多余的服务。

梳理Web应用URL和API，关闭本不该暴露在互联网端口



## 如何建立互联网资产数据库？

# 互联网资产数据的构建过程



**Nmap** : 端口、协议

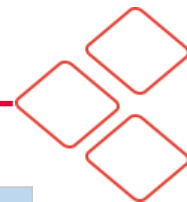
**WebInspect** : 端口、协议、是否web

**Nessus** : 端口、协议、web server、web container、SSL version等

**AWVS** : web server

**互联网接入区流量** : 所有动态的web接口。

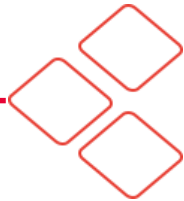
# 互联网资产的组成



IP (Internet)	IP (Mgmt)	IP (Internal)	FQDN	URL	ITSO	IT Team	Protocol (4)	Protocol (7)	Port
218. X. X. X	168. X. X. X	192. 168. X. X					TCP	HTTPS	443

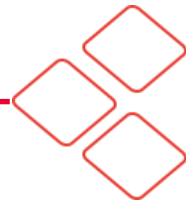
OS Type	OS Version	Web Port Y/N	Web (App) Server Type	Web Server Version	SSL/TLS Y/N	SSL/TLS Version	SSL Service Version	Runtime	Runtime Version	Database	Database Version
windows	2008 R2 SP1	Y	Nginx	1.20.0	Y	TLS 1.2	openssl 1.1.0e	PHP	5.6.7	SQL Server	2012 SP3
centos	6.9		Apache					JDK	1.7	MySQL	xxx
...	...		Tomcat					Java SE		Oracle	11g

SSH Y/N	SSH Version	SSH Service Version	Other Remote Mgmt Y/N	RM Version	RM Service Version	SNMP Y/N	SNMP Version	Nessus Agent Y/N	SEP Y/N	SEP Version	Sysmon Y/N	Sysmon Version	Reboot Required Y/N
Y	1	openSSH 7. x. x	Telent				1						



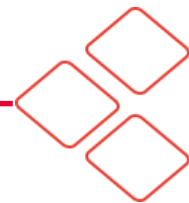
## 如何开展漏洞运营？

# 漏洞运营过程中的痛点

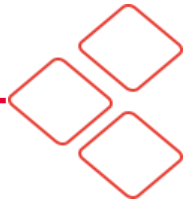




# 我们的实践



# 持续、全面和高频率的漏洞检测



Forrester : A new security vulnerability is identified approximately every

**90** minutes

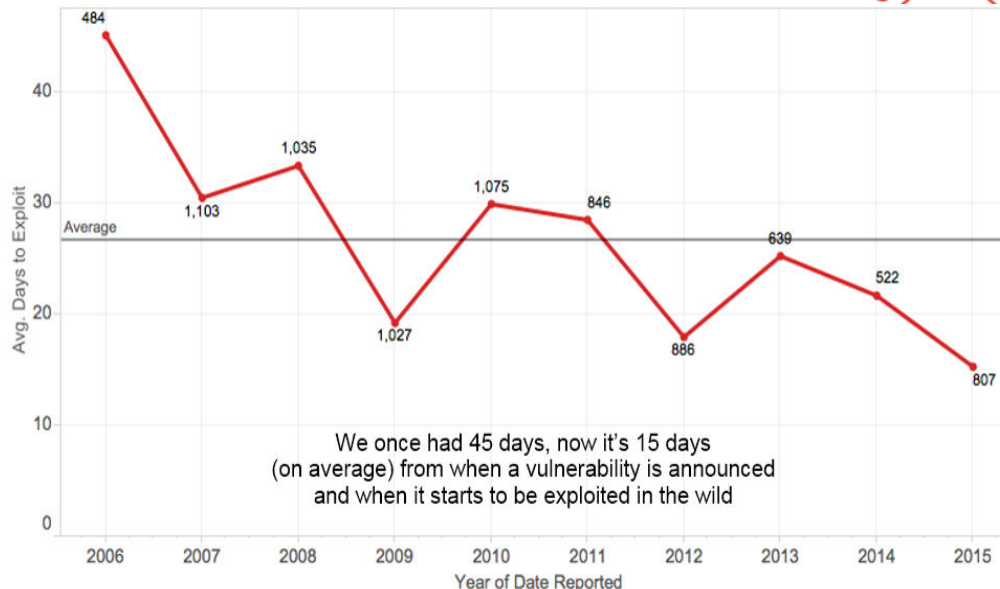
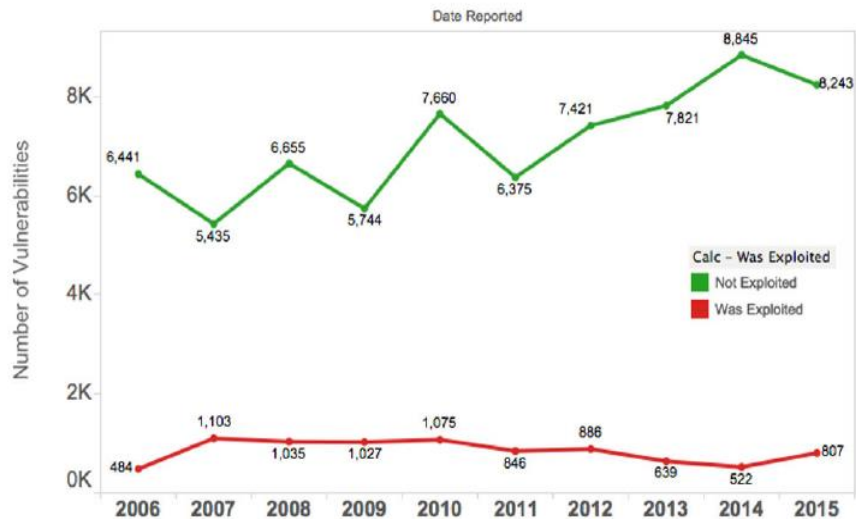


华泰证券漏洞检测手段现状				
漏洞检测手段	检测方式	检测频率	扫描目标	工具
互联网侧主机层漏洞扫描	网络扫描	每周三次	全网互联网IP地址	Tenable Nessus
互联网web应用层漏洞扫描	网络扫描	每周一次	全网互联网web应用URL	Acunetix WVS
内网侧主机层漏洞扫描	网络扫描 +Agent扫描	每周一次	核心网所有IP地址	Tenable Nessus
外部渗透测试	人工	每两个月一次	公司所有互联网应用，含APP应用	第三方渗透测试平台

# 关于漏洞修复Gartner怎么说？



Figure 3. The Number of Vulnerabilities That Have Been Exploited



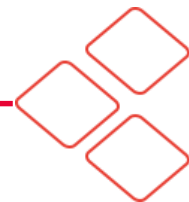
Gartner :

1、 During the past decade, on average, **only about 12.5%** of disclosed vulnerabilities have been exploited with public verification.

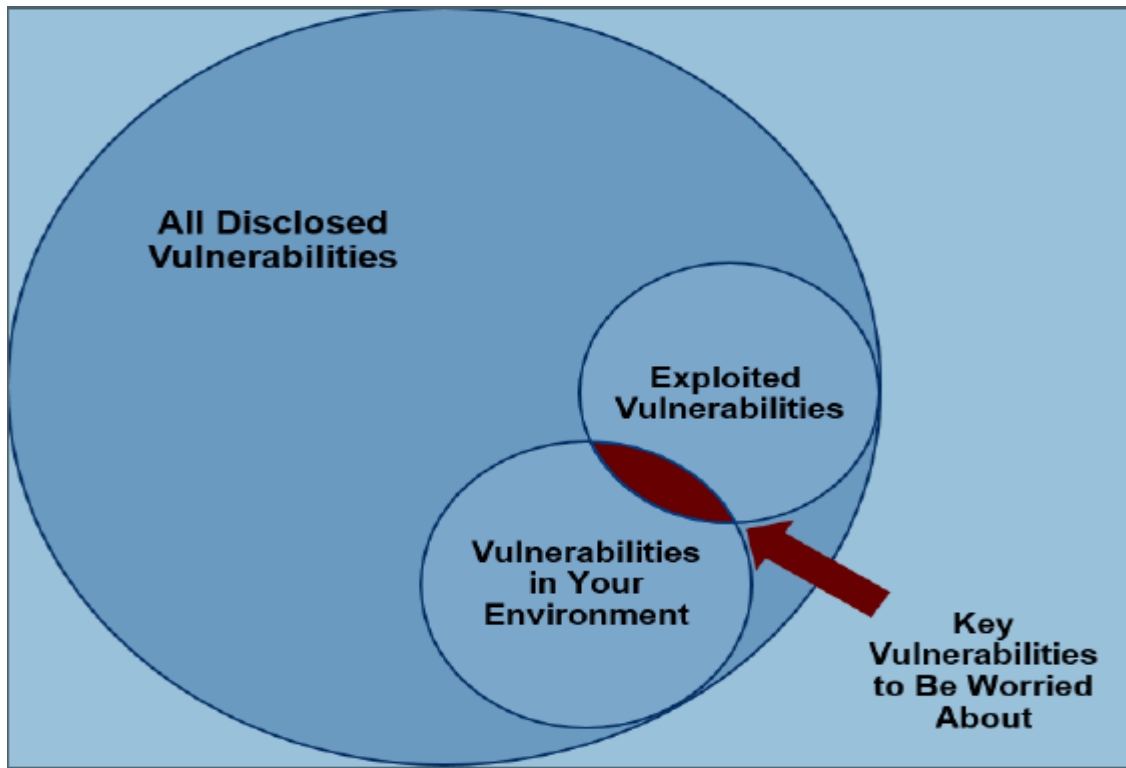
2、 If a vulnerability is not exploited in roughly the first 15 to 90 days of it being announced, it is then statistically quite rare (but still possible) that it will not be exploited in the wild. It would then fall into the

roughly **87.5%** of all vulnerabilities that are **not exploited** in the wild.

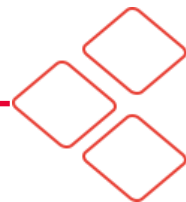
# 关于漏洞修复Gartner怎么说？（续）



The Primary IT Security Risk to Manage to Prevent a Breach



# 高收益的漏洞修复策略



漏洞类型	举例	修复优先级
已被exploited的RCE (远程命令执行) 漏洞	Struts2 S-045、S-046、S-048、Oracle WebLogic Server Java Deserialization Remote Code Execution、MS17-010 等等，常用于直接拿下互联网边界的一台服务器，再做进一步渗透或横向移动。	极高
其他已被exploited的远程利用漏洞	Struts2 S2-049等一些可导致拒绝服务攻击，服务器信息泄漏类型的漏洞。	高
已被exploited的本地利用漏洞	多用于提权，如Nginx的本地提权漏洞CVE-2016-1247	中高
其它漏洞	SSL自签证书、SSL版本低，SSL证书不被信任等	中低

如何确定漏洞是否已被exploited  
远程利用or本地利用？

- 1、漏洞扫描报告；
- 2、厂商修复公告；
- 3、CVSS官网，CVSS V3.0；
- 3、第三方威胁情报。

Base Score metrics to generate score

**Attack Vector (AV)**

Network (N) Adjacent (A) Local (L)

Physical (P)

**Attack Complexity (AC)**

Low (L) High (H)

**Privileges Required (PR)**

None (N) Low (L) High (H)

**User Interaction (UI)**

None (N) Required (R)

**Scope (S)**

Unchanged (U) Changed (C)

**Confidentiality (C)**

None (N) Low (L) High (H)

**Integrity (I)**

None (N) Low (L) High (H)

**Availability (A)**

None (N) Low (L) High (H)

## Vulnerability Information

CPE: cpe:/o:microsoft:windows

Exploit Available: true

Exploit Ease: Exploits are available

Patch Pub Date: March 14, 2017

Vulnerability Pub Date: March 14, 2017

In the news: true

## Exploitable With

Metasploit (MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption)

CANVAS 0

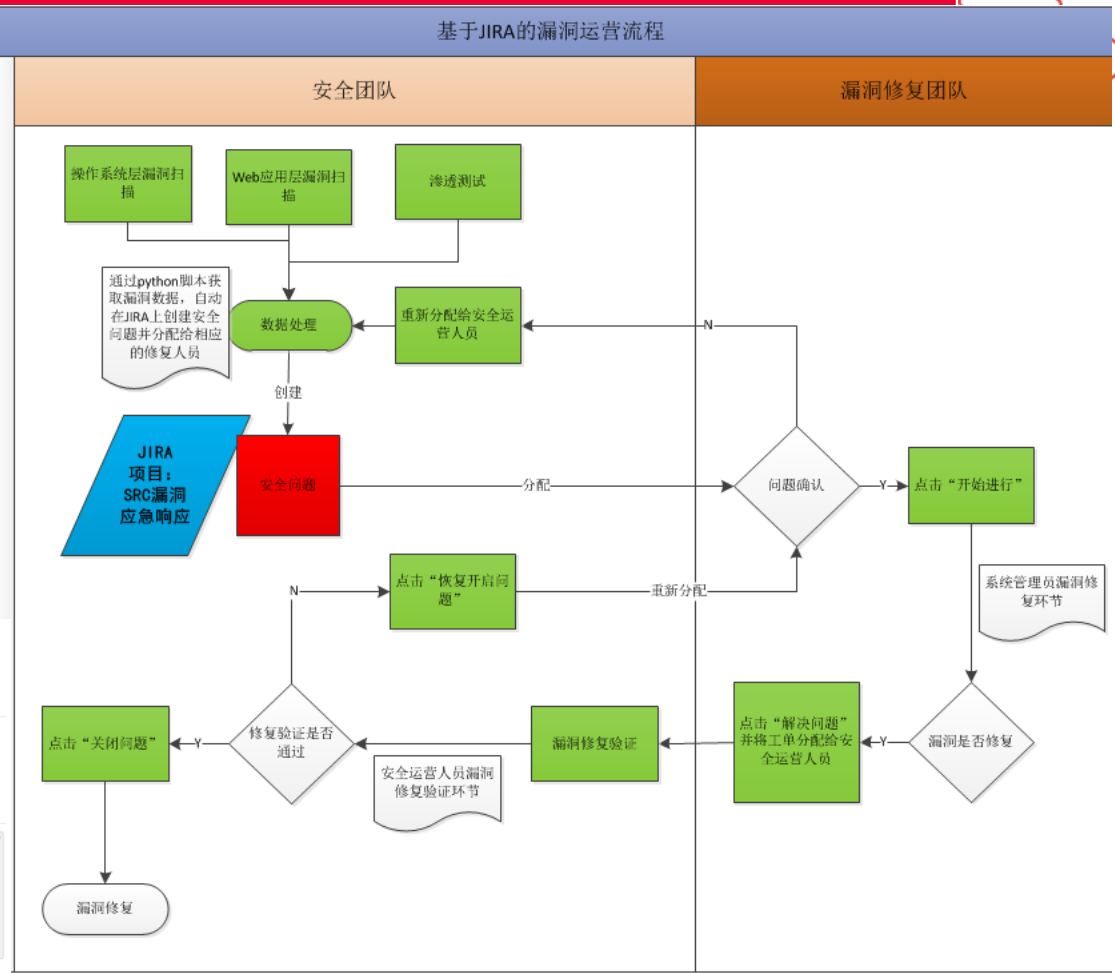
Core Impact

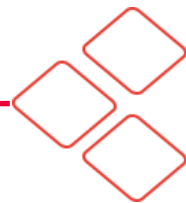
# 可视化的跟踪

工具：JIRA

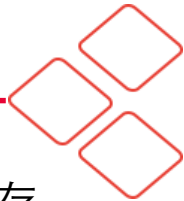
过程简介：


- 1、在JIRA上建立项目“SRC漏洞应急响应”
- 2、为每个漏洞新建“安全问题”类型的task并分配给相应的系统管理员。
- 3、系统管理员在JIRA通过“开始进行”确认漏洞，并组织修复。  
“开始进行”表明系统管理员已经确认该漏洞，并已经开始组织修复。  
“解决问题”表明系统管理员已经修复该漏洞
- 4、系统管理员修复完成后，点击“解决问题”变更task状态为“已解决”，并将task分配给安全运营人员进行修复验证。
- 5、安全运营人员收到task后组织修复验证，验证通过则通过点击“关闭问题”按钮关闭该安全问题，否则会将该安全问题重新分配给系统管理员。
- 6、漏洞状态连续三周末变化则自动添加该系统管理员的上级领导为该task的关注人。
- 7、提供看板功能给各个团队经理，用于查看各团队下所有漏洞的状态。





# “泰坦” 人工智能安全态势感知平台



 **TITANS** 基于**大数据技术**，对企业全面的安全信息进行集中采集、存储和分析，利用流式计算、**智能分析引擎**、和**可视化**等手段，结合丰富的**威胁情报**，对企业面临的外部攻击、内部违规行为进行检测，为企业建立快速有效的威胁检测、分析、处置能力和全网**安全态势感知**能力，使得企业的信息安全可知、可见、可控。



大数据



智能分析引擎



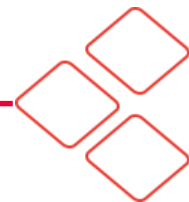
威胁情报



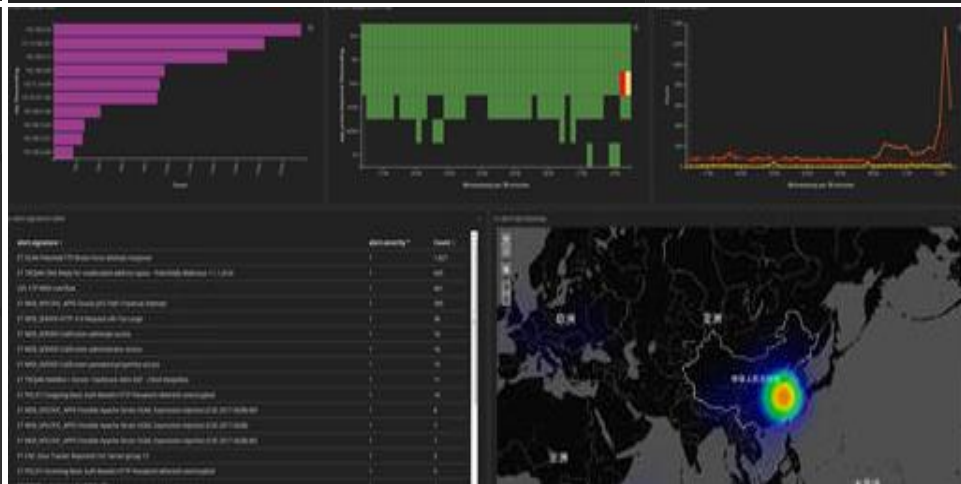
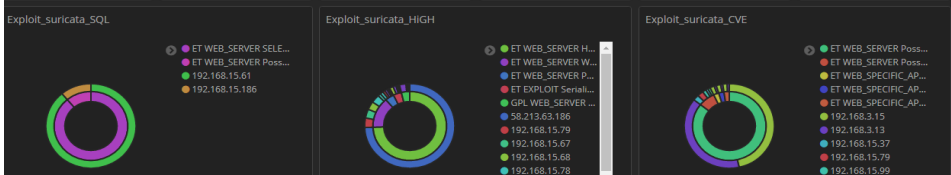
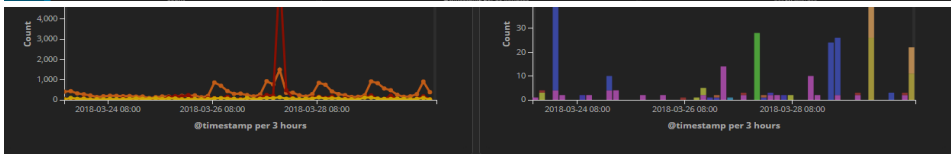
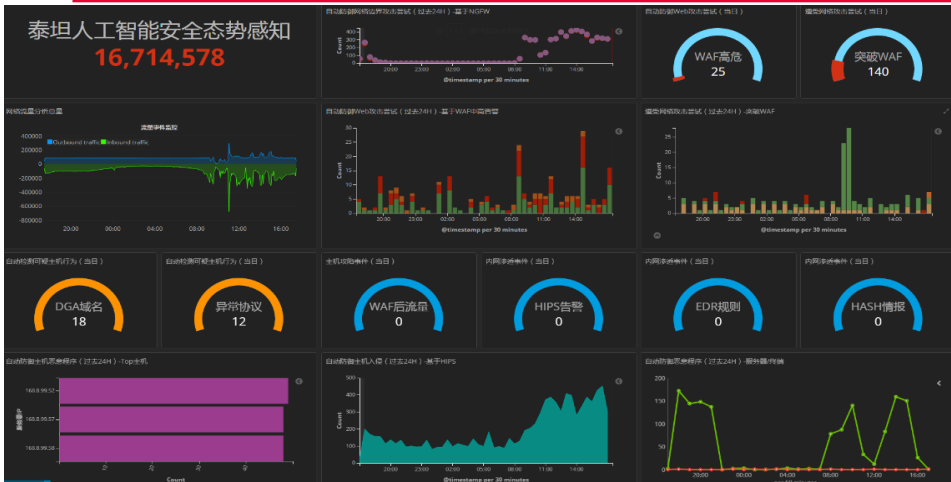
可视化



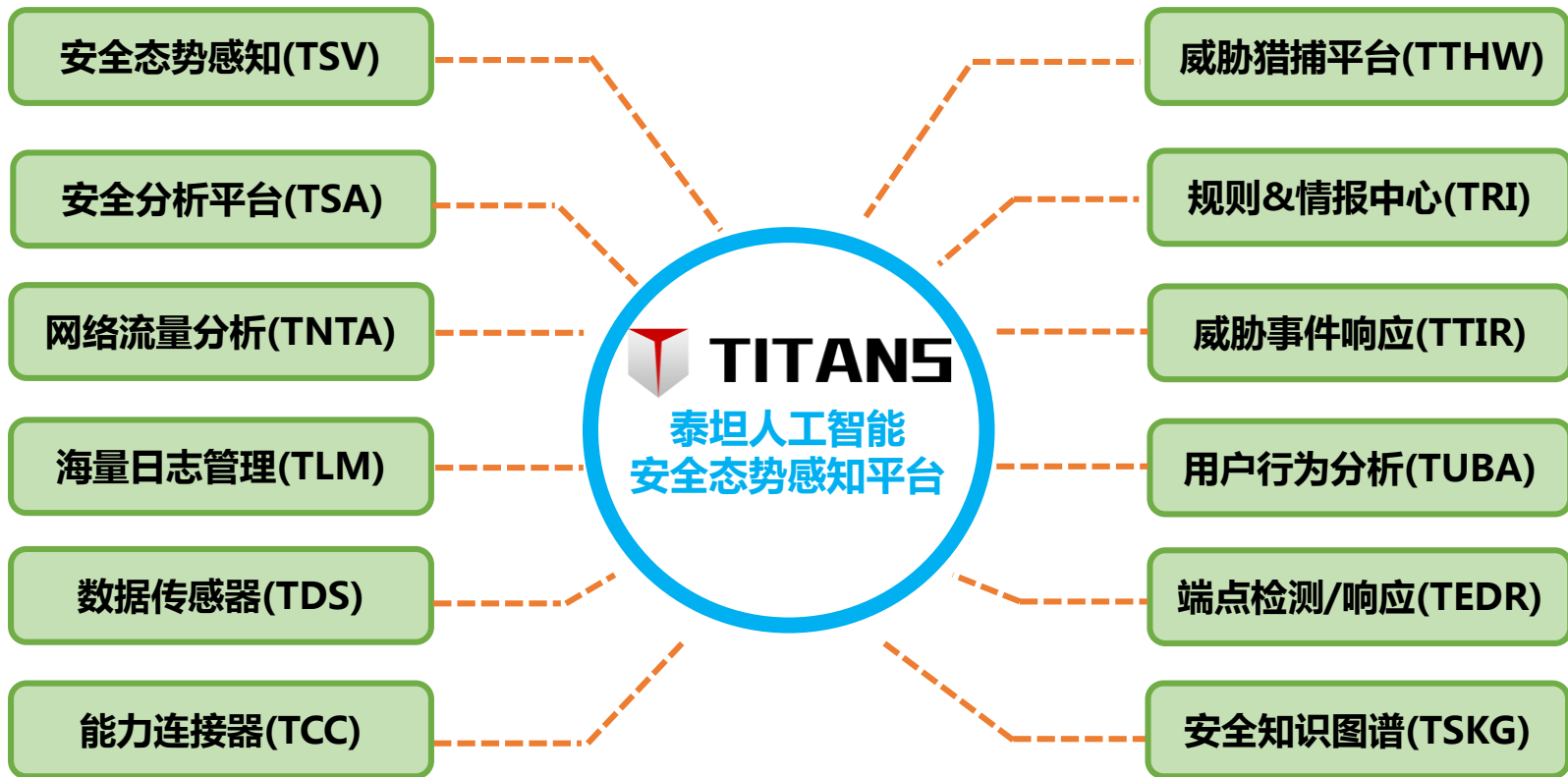
# 泰坦 - 系统架构



# 泰坦 - 安全可视化



# 泰坦 – 功能模块





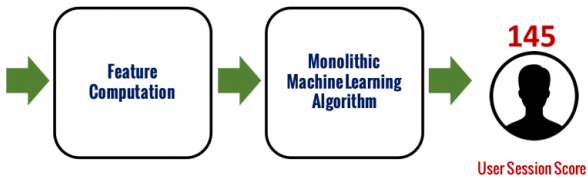
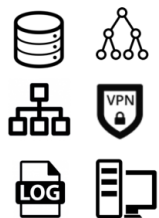
---

 **PRISM** 用户行为分析平台

# 棱镜UEBA用户行为分析平台

**PRISM 棱镜** 通过机器学习、

算法和规则模型，以用户为主体从时间序列、行为序列等建立**多维度行为基线**，对用户的行为进行**智能化分析**，建立**用户风险画像**，实时检测异常行为和隐藏的威胁，及时发现**内部用户**违规行为



AD, VPN, Database, Endpoint Logs...



## DIVERSE DATA SOURCES

LOGS Firewall, VPN, Web Proxy, DNS, AD, DHCP, Endpoint, DLP, HR, Badge  
TRAFFIC Packets, Flows, Files  
3<sup>rd</sup> PARTY Alerts, Threat Feeds

## DISTILL & INTEGRATE

DATA REDUCTION  
USER, HOST, AND DEVICES

## MACHINE LEARNING

SUPERVISED  
UNSUPERVISED  
SEMI-SUPERVISED

## CONTINUOUS MONITORING

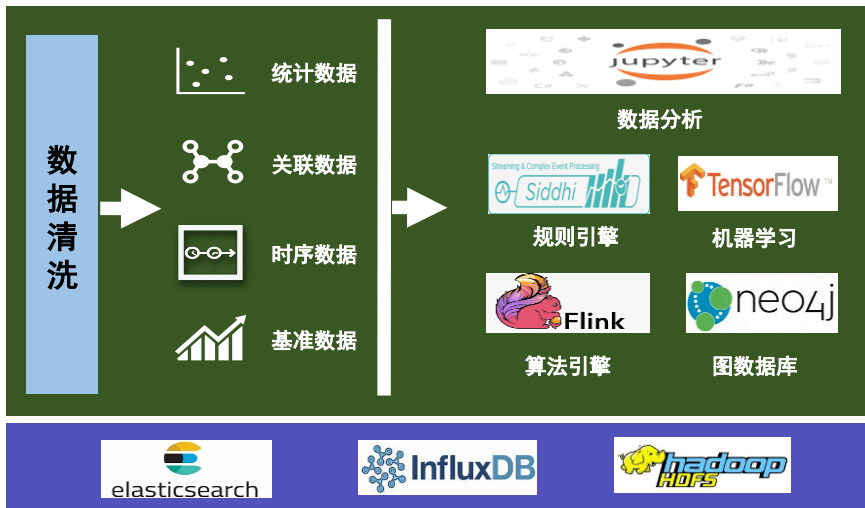
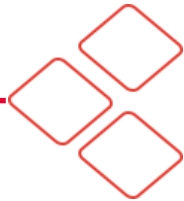
DYNAMIC RISK ASSESSMENT  
ADAPTIVE LEARNING WITH  
ANALYST FEEDBACK

## ENTITY360 | USERS, HOSTS & DEVICES

Compromised Users/Hosts/Devices  
Negligent/Malicious Insiders  
Partner Network Monitoring  
Alert Prioritization  
Incident Investigation  
Assessment

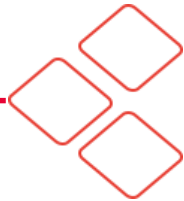
FORENSICS

# 棱镜 - 系统架构



# 棱镜 - 用户风险画像





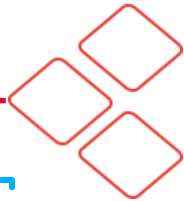
**TRIDENT**

**安全自动化测试平台**

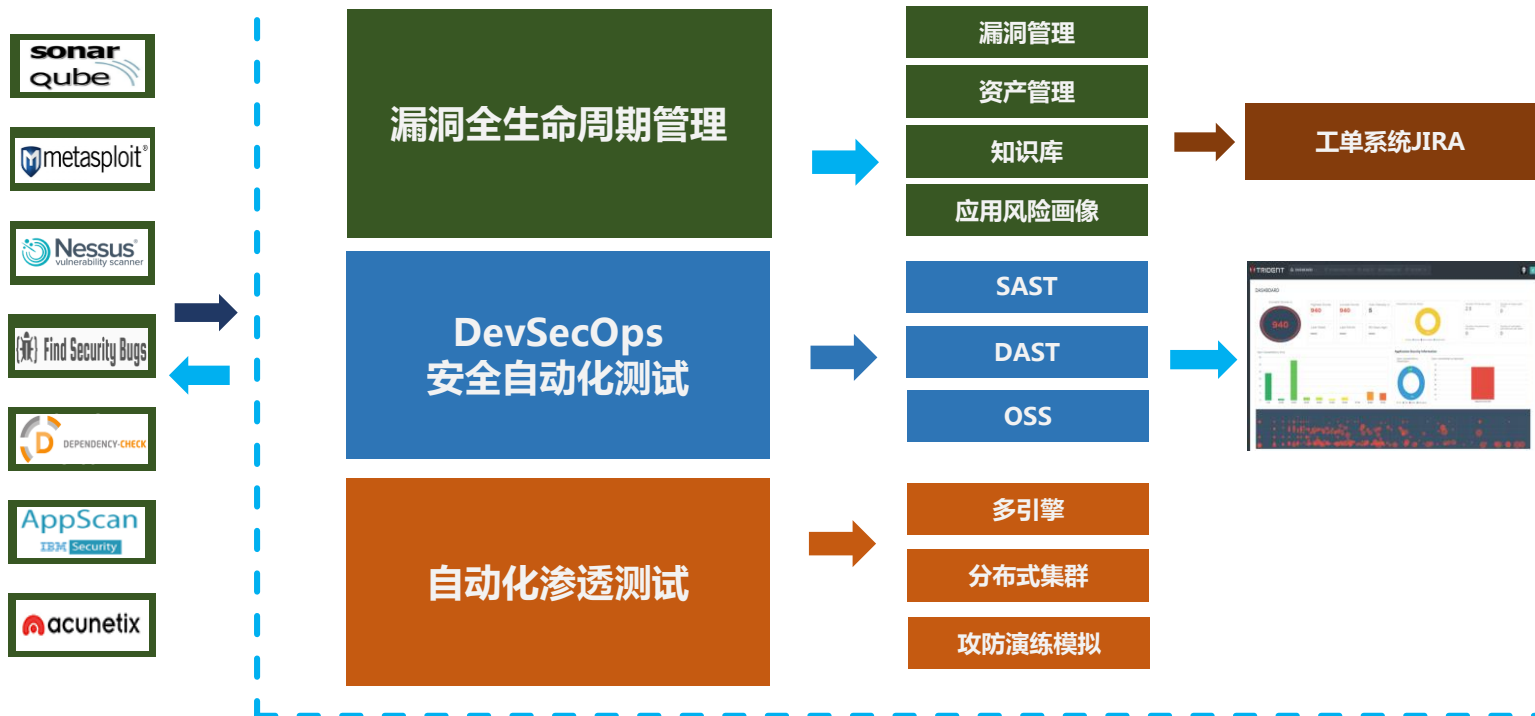


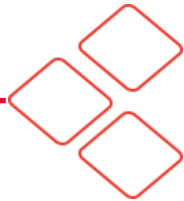


# 三叉戟 - 系统架构



## TRIDENT





# Q&A