OWASP AppSec Asia 2016

企业应用层面临的IT安全风险与危机

何迪生
Dixon Ho

今天分享的内容 What we will share today !!!

- **安全领域的未来**

  What Security Domain will look Like in the Future
- **当前面临的最大挑战**

  Review of today’s Security Challenge
- **下一步应该做什么？**

  What should we do immediately/next step?

安全领域的未来 The future Security Realm !!!

安全领域未来的世界是什么样....

Let ‘s discuss about what the Security Domain will look like in the future......

问题：大家有没有思考过未来的安全体系会是什么样?
Question: Have you think about what will be the Security System in the future ？

公元2016年3月 围棋人机大战“历史性对决” ：李世石败给机器人 **AlphaGo**

AD March 2016 “Historic Battle" Go Man-Machine Battle results were announced: **AlphaGO win a victory** over Lee Sedol

VS
nature
THE INTERNATIONAL WEEKLY JOURNAL OF SCIENCE
At last — a computer program that can beat a champion Go player PAGE 484
ALL SYSTEMS GO

公元2016年3月，李世石在“人机大战”以 1：4 输给了AlphaGo围棋机器人！

In March 2016, Lee Sedol in “Man-Machine War" with result of 1 to 4 lost to AlphaGo Robots!

如此“智能”的AlphaGo机器人，引发了“人工智能会不会超越人类”的争论。

AlphaGo let us know that robots can already so "smart" and even give rise to “A.I. will surpass Human" argument.

- 实际上，随着2012年深度学习技术取得突破，人工智能等相关技术开始被应用，它不仅可以帮助我们造出各种聪明、可爱的机器人，还可以投入在许多不同行业。
- Indeed, as the breakthrough of deep learning technology in 2012, Artificial Intelligence-related technology has begun to apply in many areas, it’s not only help us to create all kinds of clever, cute robots, these technologies are beginning to be applied in the field of many industries.

AlphaGo是故意输一场 —— 占WHR排名？

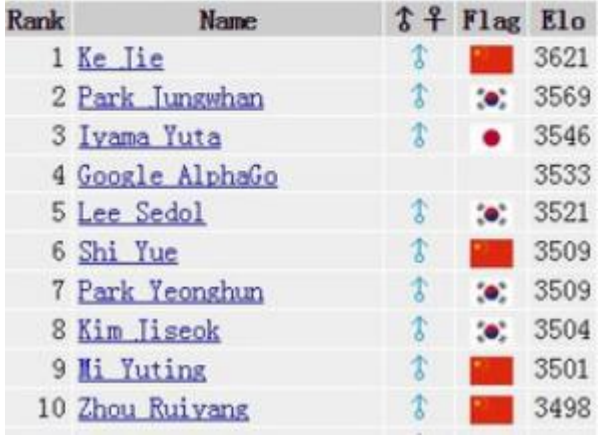
Does AlphaGo intentionally lose for an official WHR rankings?

- Google AlphaGo与李世石之间的人机世纪大战已经落下帷幕，人工智能4:1取得胜利，而且因为“终于”输了一场，AlphaGo也有了正式的WHR等级分数和排名。

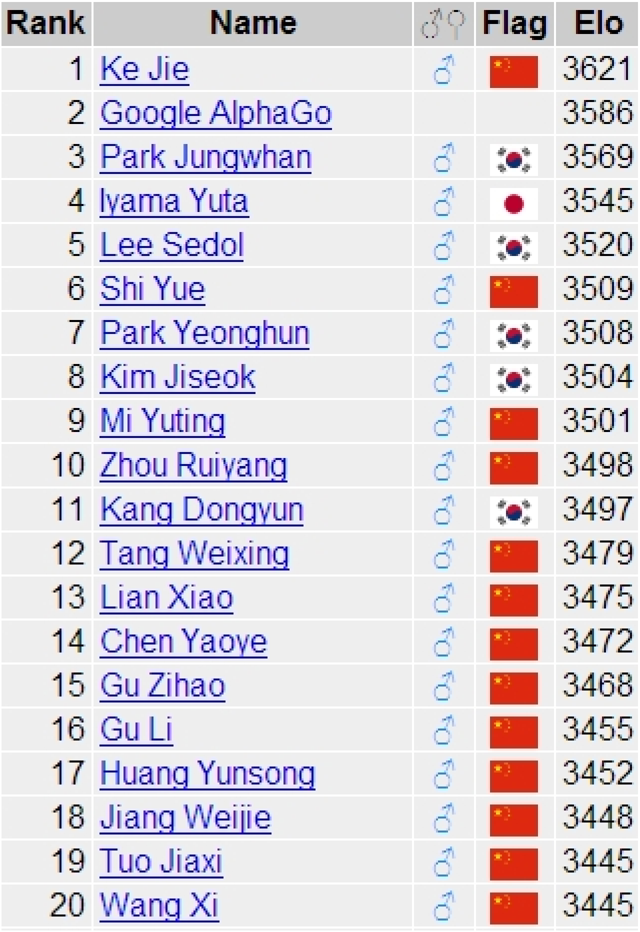
- Man-Machine war of the Century between Google AlphaGo and Lee Sedol has ended, resulting a AI 4: 1 victory, due to "finally" lost one game, AlphaGo has formally obtained the WHR rankings

- 而比赛结束后，AlphaGo凭借一场胜利，分数增加到3586，排名也超越韩国朴永训、日本井山裕太而来到第二，仅次于中国棋王柯洁(3621分)。

- After this Man-Machine war of the Century , AlphaGo obtains 3586 points, ranking above Park Jungwhan(Korea), Lyama Yuta (Japan) and came second only to the King of Go - Ke Jie from China (3621 points).



Rank	Name	♂♀	Flag	Elo
1	Ke Jie	♂	🇨🇳	3621
2	Park Jungwhan	♂	🇰🇷	3569
3	Iyama Yuta	♂	🇯🇵	3546
4	Google AlphaGo			3533
5	Lee Sedol	♂	🇰🇷	3521
6	Shi Yue	♂	🇨🇳	3509
7	Park Yeonghun	♂	🇰🇷	3509
8	Kim Jiseok	♂	🇰🇷	3504
9	Mi Yuting	♂	🇨🇳	3501
10	Zhou Ruiyang	♂	🇨🇳	3498



Rank	Name	♂♀	Flag	Elo
1	Ke Jie	♂	🇨🇳	3621
2	Google AlphaGo			3586
3	Park Jungwhan	♂	🇰🇷	3569
4	Iyama Yuta	♂	🇯🇵	3545
5	Lee Sedol	♂	🇰🇷	3520
6	Shi Yue	♂	🇨🇳	3509
7	Park Yeonghun	♂	🇰🇷	3508
8	Kim Jiseok	♂	🇰🇷	3504
9	Mi Yuting	♂	🇨🇳	3501
10	Zhou Ruiyang	♂	🇨🇳	3498
11	Kang Dongyun	♂	🇰🇷	3497
12	Tang Weixing	♂	🇨🇳	3479
13	Lian Xiao	♂	🇨🇳	3475
14	Chen Yaoye	♂	🇨🇳	3472
15	Gu Zihao	♂	🇨🇳	3468
16	Gu Li	♂	🇨🇳	3455
17	Huang Yunsong	♂	🇨🇳	3452
18	Jiang Weijie	♂	🇨🇳	3448
19	Tuo Jiaxi	♂	🇨🇳	3445
20	Wang Xi	♂	🇨🇳	3445

AlphaGo下一个对手是？
The next opponent of AlphaGo is?

3月15日，AlphaGo的世界排名也由第四名上升到了第二名，仅次于中国棋手柯洁。据说，谷歌工程师已向柯洁下了“战书”，称:“感谢输给李世石，拥有世界排名。柯洁，你准备好了吗？”对此，柯洁方面会如何应对呢？

March 15, AlphaGo’s world ranking rose from the 4th place by the 2nd, second only to Chinese player Jie Ke. It is said that Google has challenged Ke Jie with a “Gauntlet”, and says: "Thanks losing to Lee Sedol that AlphaGo can obtain a world ranking finally! Ke Jie, are you ready? “. How Ke Jie will deal with it?

中国围棋第一人怎么能咽的下这口气吗？！
Can the King of Go in China may let go this insult ?!

未来机器定能超越人脑, 会有更多的行业AlphaXXX出现吗？

…司法行业，医疗行业，安全行业…等！

Will the future machines be able to surpass the human brain,
and enable more industrialized AlphaXXX?

... says Law, Medical, Security Industries ... and so on!

Venture Radar

Artificial Intelligence Startups

Augmenting knowledge work using AI

25% of all job-based tasks will be automated by 2019
- *Forrester Research*

Many experts believe that by 2050 machines will have reached human level intelligence

Hundreds of startups are already using AI to augment knowledge work

Humans focus more on creativity, social intelligence, manual dexterity, and...

Law & Contracts

ROSS

Kelson

kira

LEGAL ROBOT

BEAGLE

DOXAI

Customer Service

FinGenius

DigitalGenius

CAPITO SYSTEMS

COGNICOR
Enabling Smarter Agreements

Wise.io

Sales

AVISO

CONVERSICA

re:infer

Personal Assistants

x.ai

Investing

VANARE

sensai

WEALTHARC

INOVANCE FINANCIAL TECHNOLOGIES

Business Intelligence, Journalism, Research

agolo

NarrativeScience

SYNAPSIFY

Audit & Compliance

AppZen

Medical & Other Image Analysis

MetaMind

clarifai

enlitic

Tractable

Other Medical

Wired Informatics

司法行业 / Law Industry：Alpha**Law?**

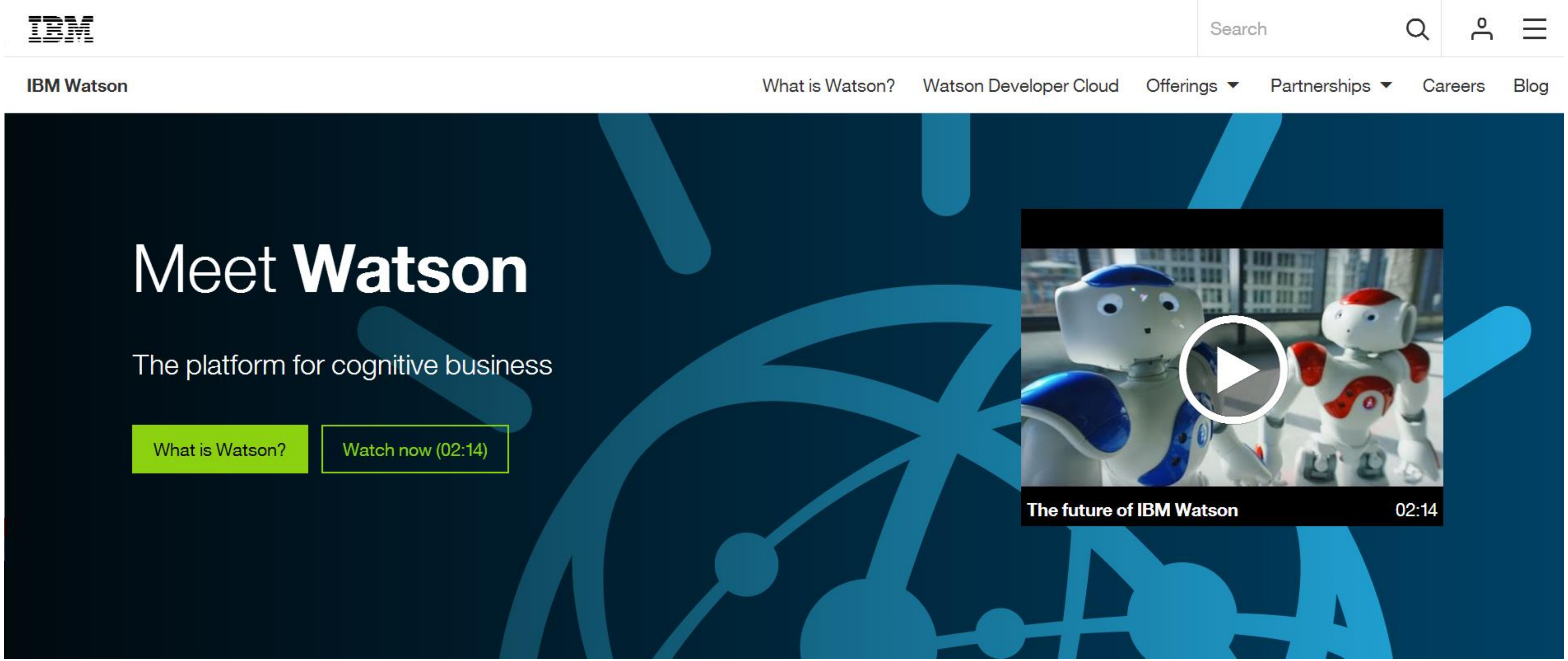
AlphaLaw 律司/法律咨询 Lawyers / Legal Advice：

- 我们的司法工作是否会被人工智能所取代？
  Will the job of our justice system be replaced by artificial intelligence?
- 有一天如果一台机器可以回答大部分的法律咨询问题，那我们法律咨询行业是否就将被终结?
  One day, if a machine can answer and handle most of the requirements of legal advice service, will it replace the traditional legal consulting service?

AlphaJudge 法官/司法裁决 Judges / judicial decisions:

- 同样，将来某一天，我们准备一千个案子，然后交给一台机器和一千名法官同时做裁决，要是最后的结果差不多，或者当事人更加认可机器的裁决，那么法官是否也会失业？
  Similarly, if one machine can handle one thousand cases that normally requiring one thousand judges to handle, with a very similar outcome in the future, will the judges lose their job?

医疗行业 / Medical Industry : Alpha**MED** → **IBM** Watson



Search

IBM Watson

What is Watson? Watson Developer Cloud Offerings ▾ Partnerships ▾ Careers Blog

Meet **Watson**

The platform for cognitive business

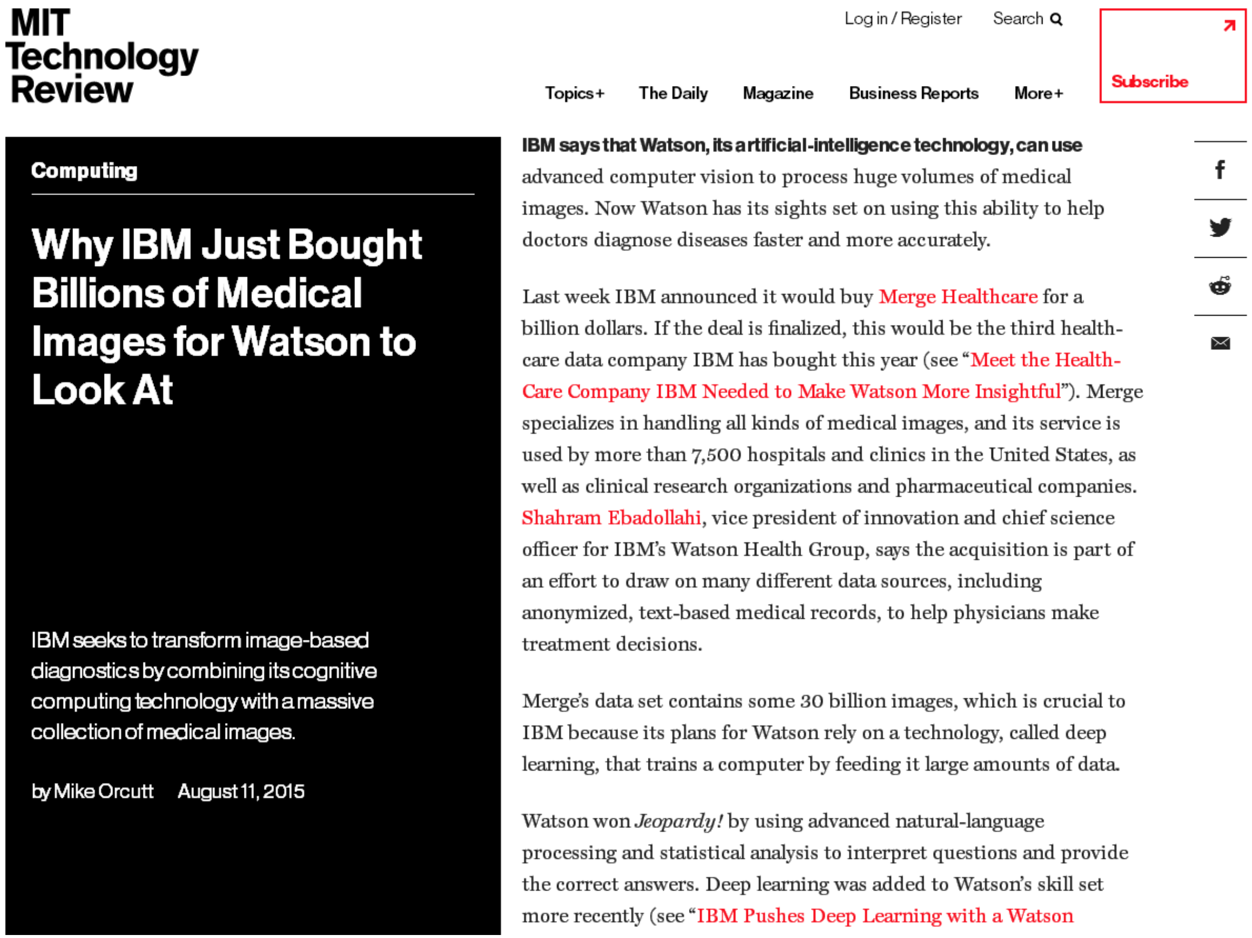
What is Watson? | Watch now (02:14)

The future of IBM Watson 02:14

IBM's Watson 'graduates' medical school in Haifa

IBM and partners use Israeli technology to transform personal health with Watson and open cloud.

By Viva Sarah Press | JUNE 16, 2015, 9:59 AM



Computing

Why IBM Just Bought Billions of Medical Images for Watson to Look At

IBM seeks to transform image-based diagnostics by combining its cognitive computing technology with a massive collection of medical images.

by Mike Orcutt August 11, 2015

IBM says that Watson, its artificial-intelligence technology, can use advanced computer vision to process huge volumes of medical images. Now Watson has its sights set on using this ability to help doctors diagnose diseases faster and more accurately.

Last week IBM announced it would buy Merge Healthcare for a billion dollars. If the deal is finalized, this would be the third health-care data company IBM has bought this year (see "Meet the Health-Care Company IBM Needed to Make Watson More Insightful"). Merge specializes in handling all kinds of medical images, and its service is used by more than 7,500 hospitals and clinics in the United States, as well as clinical research organizations and pharmaceutical companies. Shahram Ebadollahi, vice president of innovation and chief science officer for IBM's Watson Health Group, says the acquisition is part of an effort to draw on many different data sources, including anonymized, text-based medical records, to help physicians make treatment decisions.

Merge's data set contains some 30 billion images, which is crucial to IBM because its plans for Watson rely on a technology, called deep learning, that trains a computer by feeding it large amounts of data.

Watson won *Jeopardy!* by using advanced natural-language processing and statistical analysis to interpret questions and provide the correct answers. Deep learning was added to Watson's skill set more recently (see "IBM Pushes Deep Learning with a Watson

那安全领域呢... AlphaSEC?

How about the Security Industry... AlphaSEC?

- 我们会不会有安全人工智能或安全机器人？信息安全人工智能时代会实现吗？
- Will Security Artificial Intelligence Robot and/or Information Security A.I. era become reality?

Meet Microsoft's New 'RoboCop' Security Robot

By Susanne Posel – November 21, 2014 0 Comment

Knightscope have manufactured their own version of "RoboCop" to get the public ready for the future of robotic security with the K5 5', 300 pound autonomous robot.

According to the website, the company claims the "Knightscope K5 autonomous data machines predict and prevent crime in your community … with an innovative combination of large-scale robotics, predictive analytics and social engagement."

K5 is marketed by Knightscope as "a friend that can see, hear, feel and smell, that would tirelessly watch over your corporate campus or neighborhood, keep your loved ones safe and put a smile on everyone passing by. Imagine if we could utilize technology to make our communities stronger and safer."

The robot uses "a combination of autonomous technology, robotics and predictive analytics to provide a commanding but friendly physical presence while gathering important real-time on-site data with its numerous sensors."

The data collected by K5 is run through predictive analytics and corresponds with "existing business, government and crowd sourced social data sets, and subsequently assigned an alert level that determines when the community and the authorities should be notified of a concern."

The tech corporation is targeting other tech companies and shopping malls with this robot that is equipped with "non-stop security monitoring, using laser beam 3D mapping, GPS, microphones, video cameras and even license plate recognition software."

Stacy Stephens, vice president of sales and marketing for Knightscope explained that the company has "the capability of putting WMD sensing on it. Radiation, chemical, biological sensors and also airborne pathogens."

Microsoft has hired K5 to patrol their property as security guards.

Knightscope is excited to bring their robots to tech corporations: "I believe robots are the perfect tools to handle the monotonous and sometimes dangerous work in order to free up humans to more judiciously address activities requiring higher-level thinking, hands-on encounters or tactical planning."

微软的K5只是一个保安机器人！那IT系统会有安全机器人吗？
Microsoft’s K5 is just a Security Guard Robot! How about in IT System?

- 我们未来会有AlphaSEC吗？
  Do we have AlphaSEC for IT in the future?

- ITSec未来会是一个什么模样？
  What is the ITSec will look like in the future?

- 让我们一起预览....
  Let’s take a preview....

安全领域的未来方向
Future Trend Analysis in Security

- 人Human
  - Past Experience

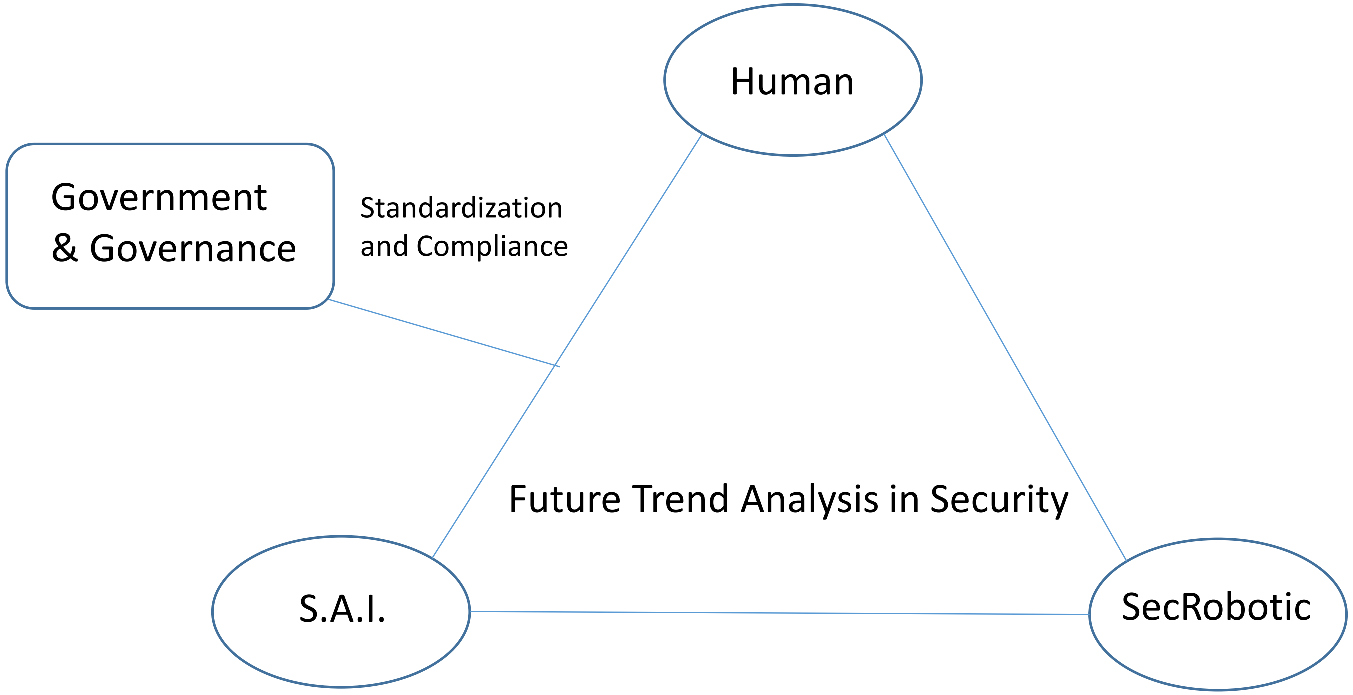
- 安全人工智能Security Artificial Intelligence (S.A.I.)
  - New Experience

- 安全机器人Security Robotic
  - Execution

安全领域的未来方向
Future Trend Analysis in Security

- 人Human
  - Design/Define/Manage + Monitor/Q.A.
- 安全人工智能Security Artificial Intelligence (S.A.I.)
  - The Core Brain - Self-Study/Build/Refine/Integrate
  - New Experience
  - Self-Study KB on Security
- 安全机器人Security Robotic
  - Leg & Arms - Execution
  - Patrol/Manage/Execute S.A.I. Model
  - Integrate through SAI API and SDSec

安全领域的未来方向
Future Trend Analysis in Security


Human
Government & Governance
Standardization and Compliance
Future Trend Analysis in Security
S.A.I.
SecRobotic

Adaptation Period:

- Tee-off at current and will mature in 2 to 5 Years

Objective:

- Enable Self-learning Adaptive Security & Threat Model to drive controlling - a set of useful analytic and decision-making techniques base on SIEM/ Sec Big Data / Threat Intelligence / Behavior Detection and Analysis/ Machine Learning (ML) / SOC / Risk Control System

Adaptation Period:

- Kicked off 8 years ago at 2008 (AISec 2008)

Objective:

- Convert the Traditional Knowledge & Experience to New Security Domain A.I.

Adaptation Period:

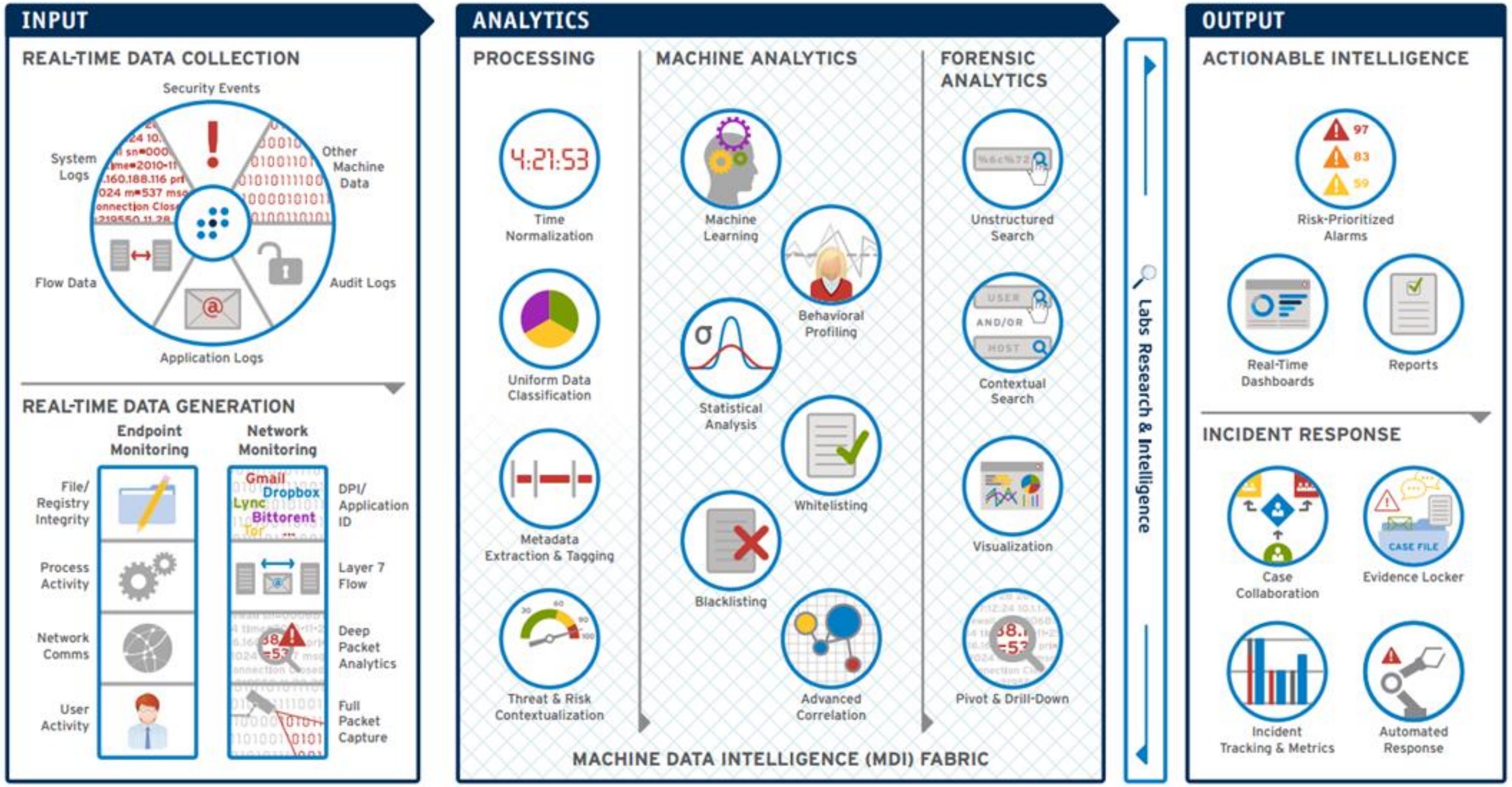
- Start to mature in 3 to 6 years from now

Objective:

- Build a S/W SecRobot based on SAI API and SDSec

安全领域的未来方向
Future Trend Analysis in Security

安全人工智能（S.A.I.）框架
Security Artificial Intelligence (S.A.I.) Framework



今天是OWASP大会，我们先从未来返回当下, 让重点放回现在面对的AppSec挑战

Today is OWASP Conference, so let’s return from the future and focus in our current AppSec challenges

安全挑战

香港航空某站SQL注入
涉及156万乘客信息/268万机票信息/八千多员工信息

中石化车e族APP存在SQL注入漏洞
可跨9个库

海尔 旗下日日顺商城SQL注入
可导致300万会员信息泄漏

邯郸市 工信办漏洞
危及大量个人信息以及金额等数据，百万用户数据

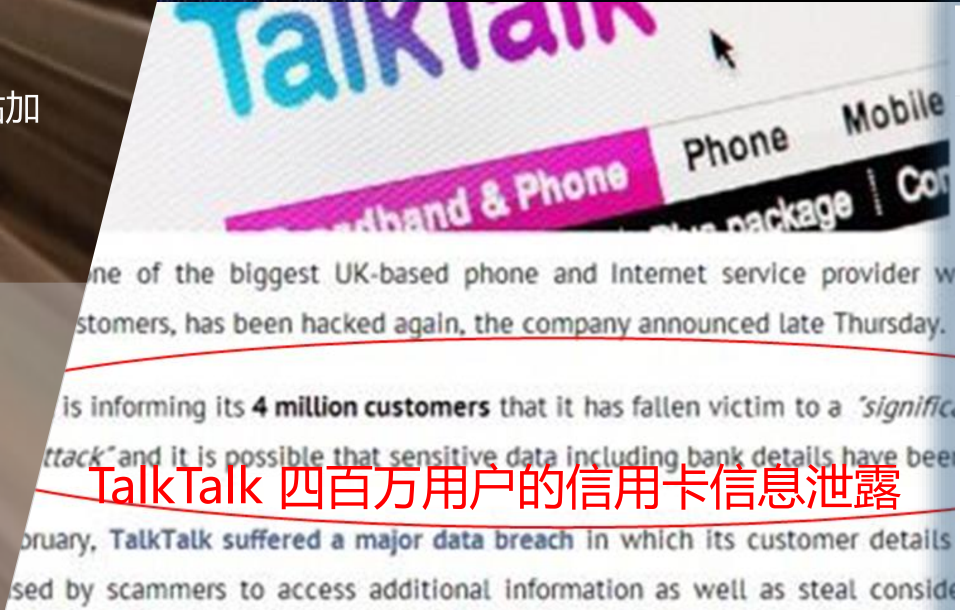
中国电信 翼支付某系统漏洞
泄露400万用户信息、支付交易明细信息（超市购物/加油站加油）以及充值等数据。

十万家用智能系统被黑客攻击

高中生入侵 中央情报局 高管的私人邮箱

More……

网络空间是一个非常危险的领域 ....

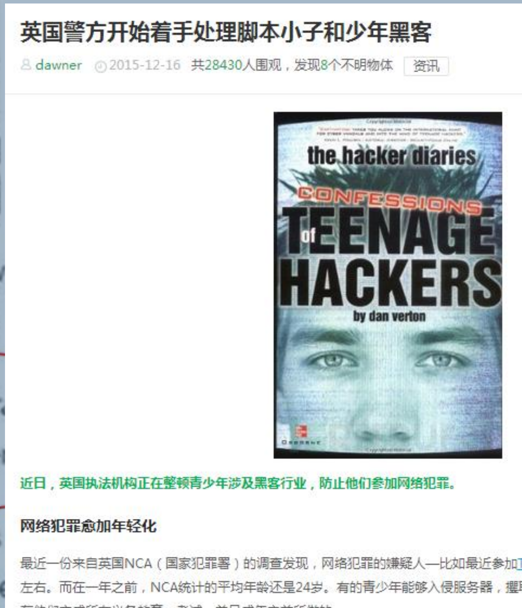


ne of the biggest UK-based phone and Internet service provider w
stomers, has been hacked again, the company announced late Thursday.

is informing its **4 million customers** that it has fallen victim to a *"significa*
ttack" and it is possible that sensitive data including bank details have bee

bruary, **TalkTalk suffered a major data breach** in which its customer details
sed by scammers to access additional information as well as steal conside

TalkTalk 四百万用户的信用卡信息泄露



英国警方开始着手处理脚本小子和少年黑客

dawner 2015-12-16 共28430人围观，发现8个不明物体 资讯

近日，英国执法机构正在整顿青少年涉及黑客行业，防止他们参加网络犯罪。

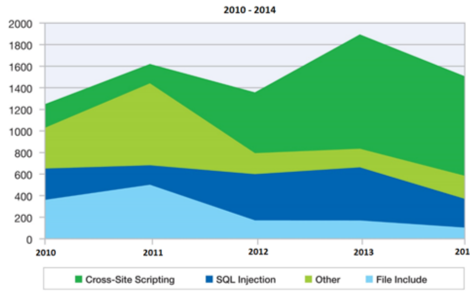
网络犯罪愈加年轻化

最近一份来自英国NCA（国家犯罪署）的调查发现，网络犯罪的嫌疑人—比如最近参加
左右。而在一年之前，NCA统计的平均年龄还是24岁。有的青少年能够入侵服务器，攫

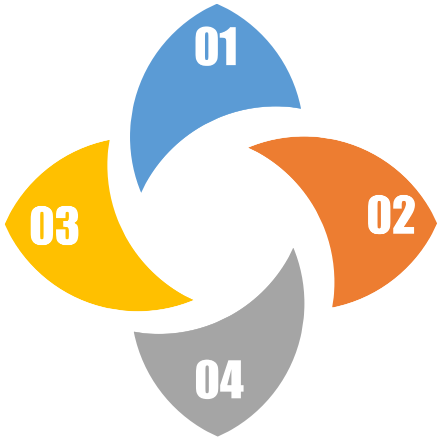
安全现状

超过80%的攻击
发生在应用层

主流漏洞攻击数据汇总



资料来源：IBM X-Force®研究与发展



相关分析报告

周界安全和应用安全投入比例为 23:1

调研员：Joseph Feiman, Gartner Analyst

调研报告主题: 让应用程序做自我保护

Sept 25, 2014

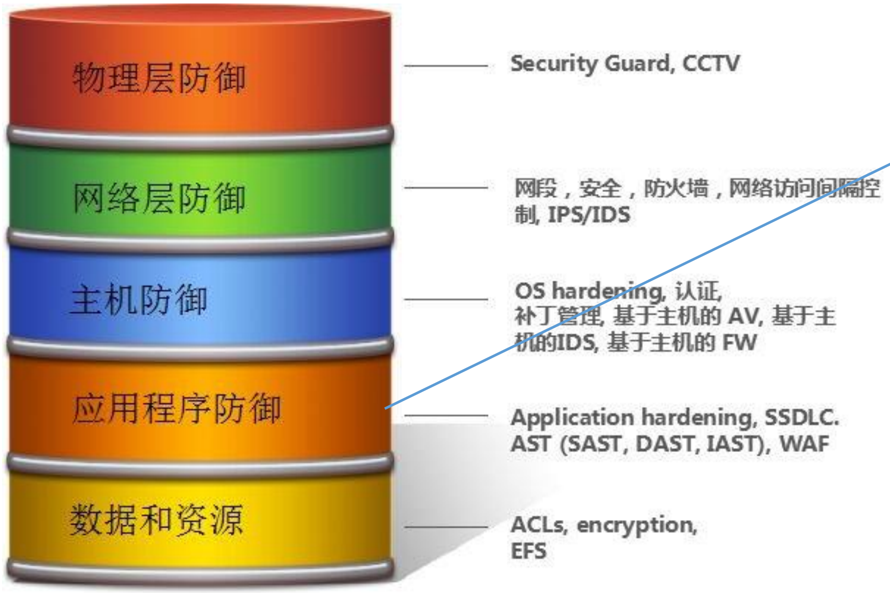
研发商在安全领
域投入少

WAF真的可以保
护应用系统安全么?

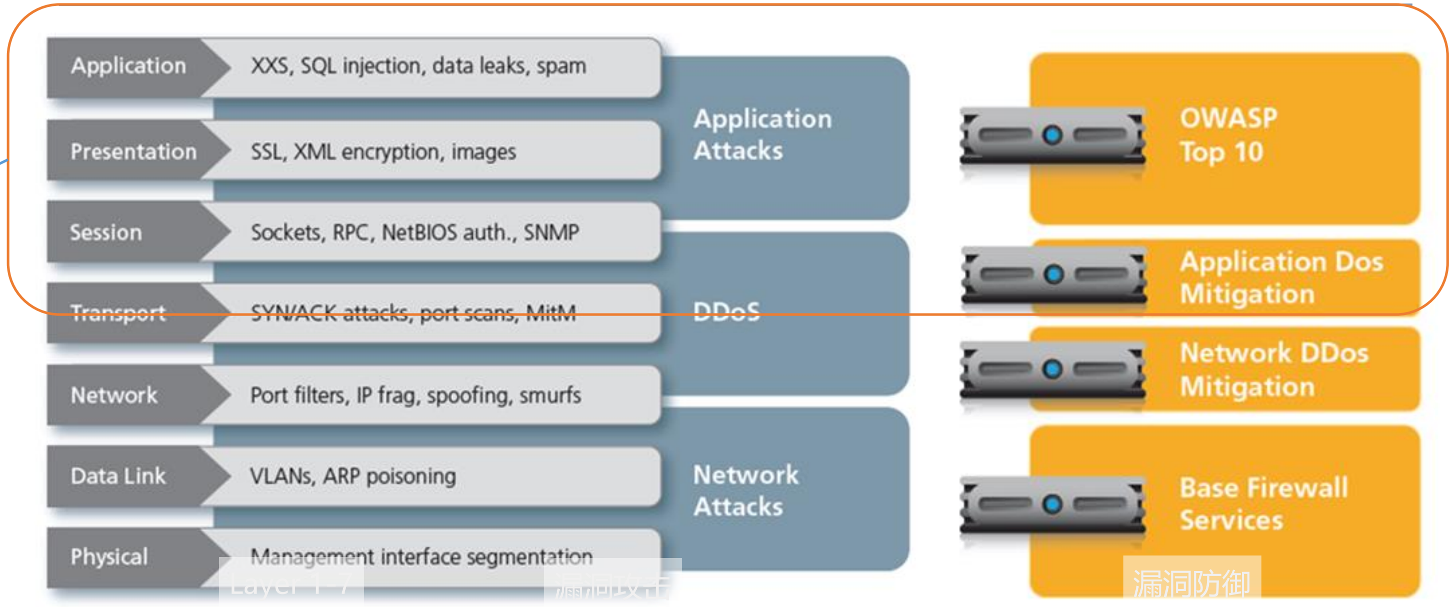
多样化的攻击越来
越难以防御

安全对策：深度安全防御模型

- 分层次防御
  - 提高攻击者被检测到的概率
  - 降低攻击者成功得手的几率

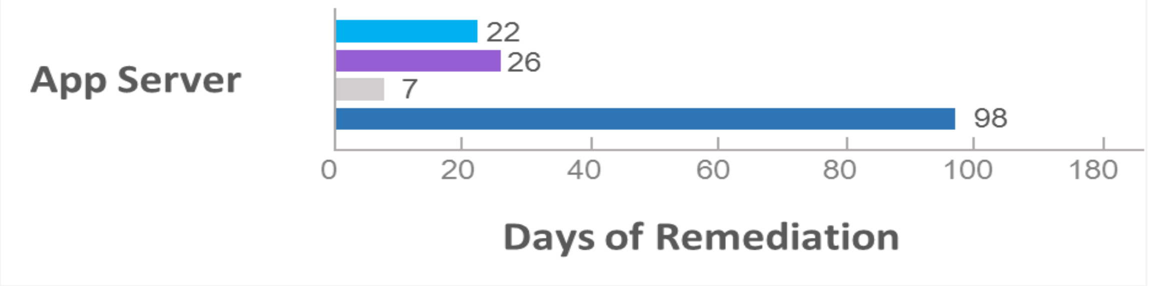

物理层防御
Security Guard, CCTV
网络层防御
网段，安全，防火墙，网络访问间隔控制, IPS/IDS
主机防御
OS hardening, 认证, 补丁管理, 基于主机的 AV, 基于主机的IDS, 基于主机的 FW
应用程序防御
Application hardening, SSDLC. AST (SAST, DAST, IAST), WAF
数据和资源
ACLs, encryption, EFS

深度防御模型


Application
XXS, SQL injection, data leaks, spam
Presentation
SSL, XML encryption, images
Session
Sockets, RPC, NetBIOS auth., SNMP
Transport
SYN/ACK attacks, port scans, MitM
Network
Port filters, IP frag, spoofing, smurfs
Data Link
VLANs, ARP poisoning
Physical
Management interface segmentation
Application Attacks
DDoS
Network Attacks
OWASP Top 10
Application Dos Mitigation
Network DDos Mitigation
Base Firewall Services
Layer 1-7
漏洞攻击
漏洞防御

常见补救措施有什么？

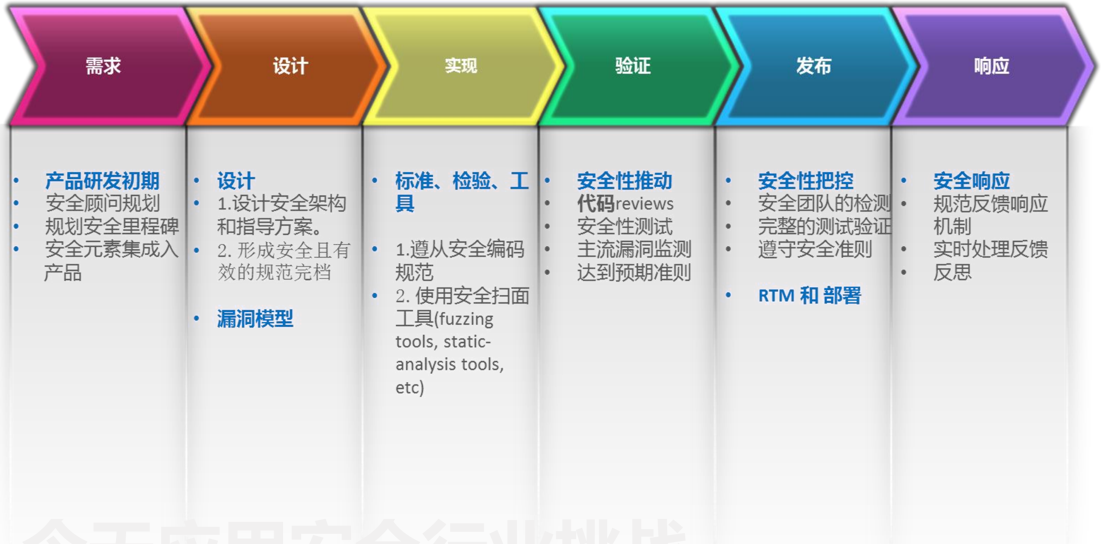
- 漏洞补救



- 发现漏洞，及时修复它，Great！☺
- 1个漏洞很快能修复；10个漏洞勉强应付；如果同时面对100个甚至1000个漏洞呢?
- 如果是一些很久远连源代码都找不到的应用漏洞....

常见的安全工具!

- 安全软件的开发生命周期
  Security Software Development Life Cycle



需求
- **产品研发初期**
- 安全顾问规划
- 规划安全里程碑
- 安全元素集成入产品

设计
- **设计**
- 1.设计安全架构和指导方案。
- 2. 形成安全且有效的规范完档
- **漏洞模型**

实现
- **标准、检验、工具**
- 1.遵从安全编码规范
- 2. 使用安全扫面工具(fuzzing tools, static-analysis tools, etc)

验证
- **安全性推动**
- **代码**reviews
- 安全性测试
- 主流漏洞监测
- 达到预期准则

发布
- **安全性把控**
- 安全团队的检测
- 完整的测试验证
- 遵守安全准则
- **RTM 和 部署**

响应
- **安全响应**
- 规范反馈响应机制
- 实时处理反馈
- 反思

今天应用安全行业挑战

安全领域的指导
人才少见

缺乏安全且有效的
流程指导文档

研发团队往往很少
考虑安全因素

怎样解决?

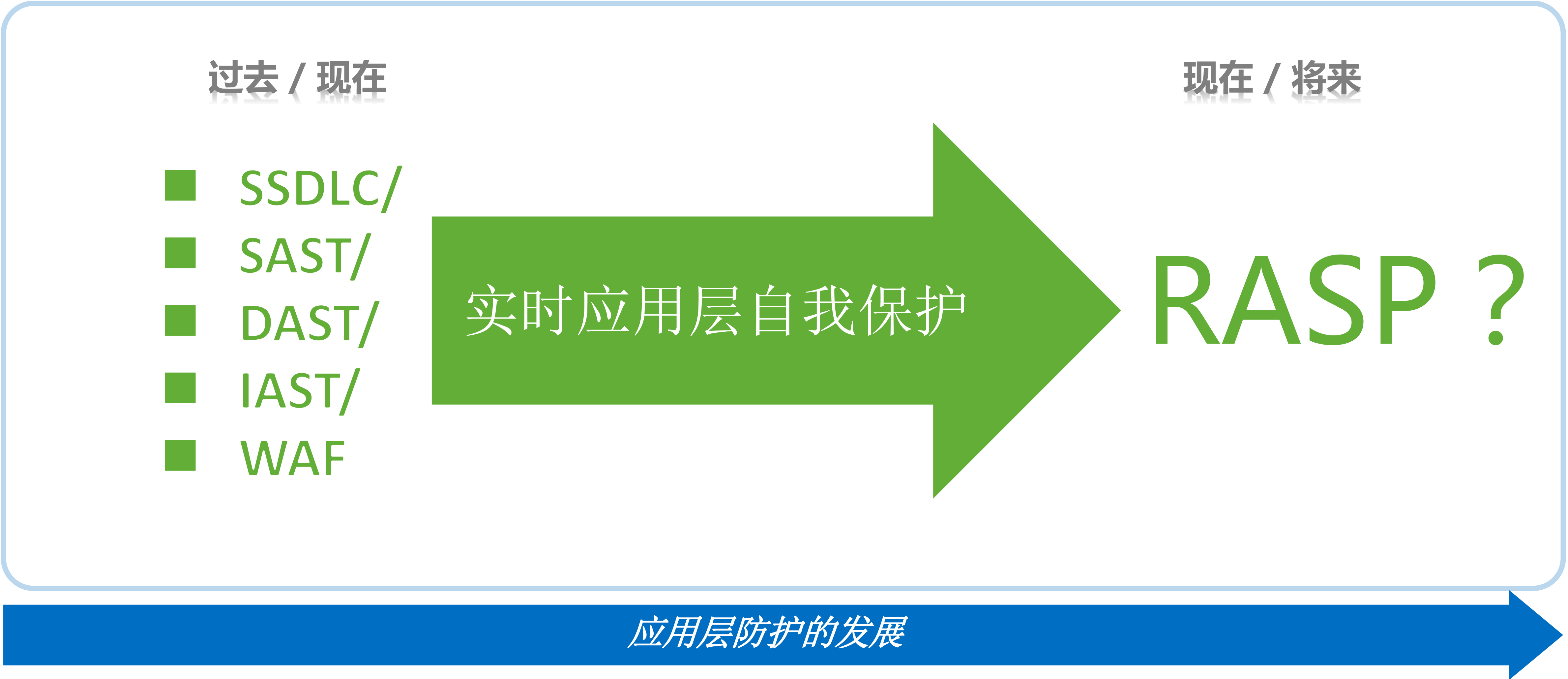
传统 到 未来 - RASP

Gartner

调研员：Joseph Feiman, Gartner Analyst

调研报告主题: 让应用程序做自我保护

Sept 25, 2014



过去 / 现在

- SSDLC/
- SAST/
- DAST/
- IAST/
- WAF

实时应用层自我保护

现在 / 将来

RASP？

应用层防护的发展

What is RASP ?

可以为软件产品提供实时保护，使其免受漏洞所累

ONE ASP RASP

(Runtime Application Self-Protect)

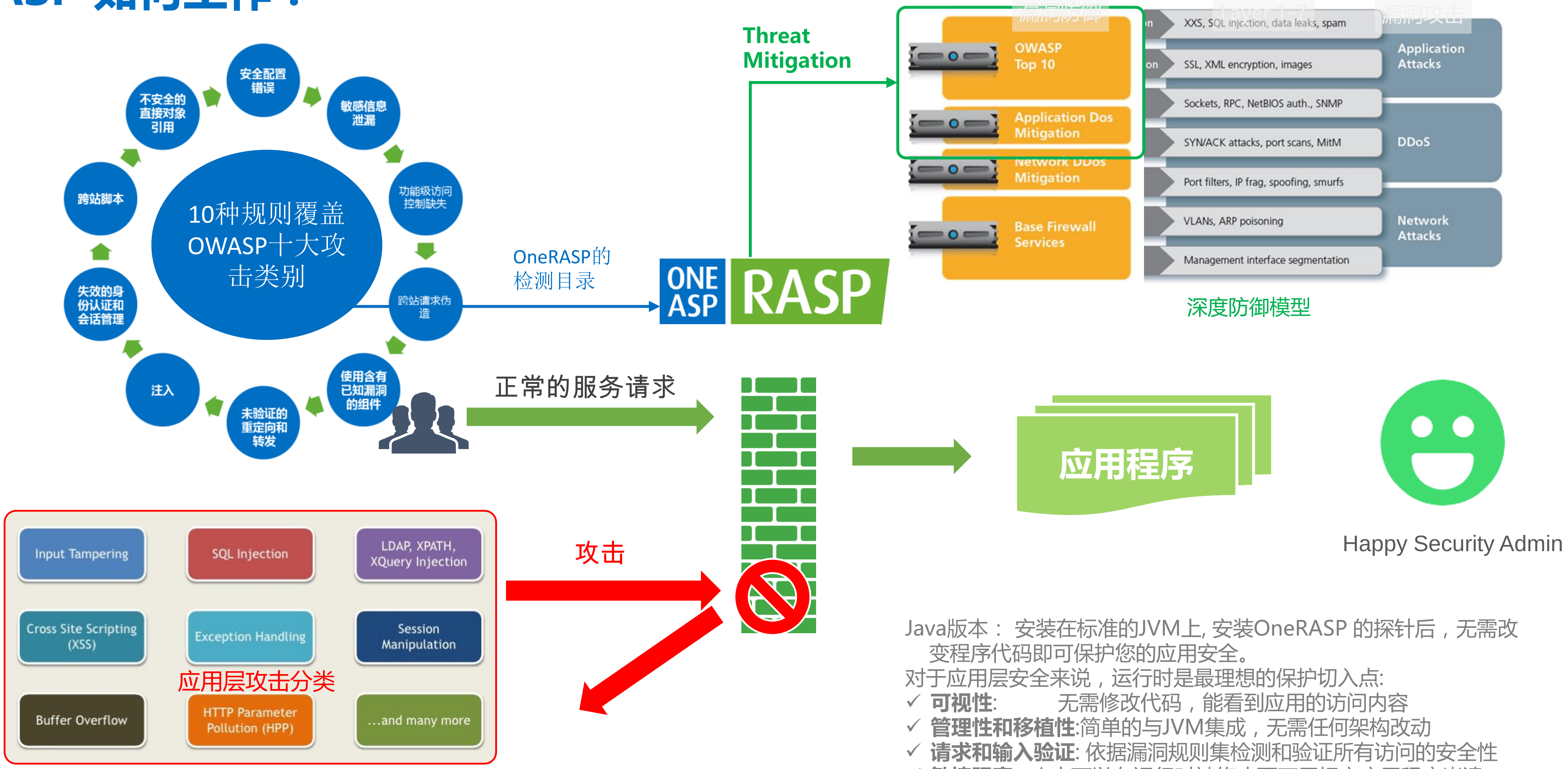
漏洞攻击抓取

实时响应，通过后台
展现给用户

漏洞攻击阻断

ONE ASP RASP

RASP 如何工作？



Java版本： 安装在标准的JVM上, 安装OneRASP 的探针后，无需改变程序代码即可保护您的应用安全。

对于应用层安全来说，运行时是最理想的保护切入点:

- ✓ **可视性**: 无需修改代码，能看到应用的访问内容
- ✓ **管理性和移植性**:简单的与JVM集成，无需任何架构改动
- ✓ **请求和输入验证**: 依据漏洞规则集检测和验证所有访问的安全性
- ✓ **敏捷阻塞**: 攻击可以在运行时被终止而不用担心应用程序崩溃

为什么我们需要RASP技术

Now！市场现状

- 超过80%的漏洞攻击发生在应用层
- 通过更改代码来修复漏洞的周期长
- 在此期间，通过补偿控制来保护你的应用程序

*企业应该通过**简化**自己的系统来抵御黑客攻击，而不是把系统修改的越发复杂。*

——Gartner 2015

更多问题

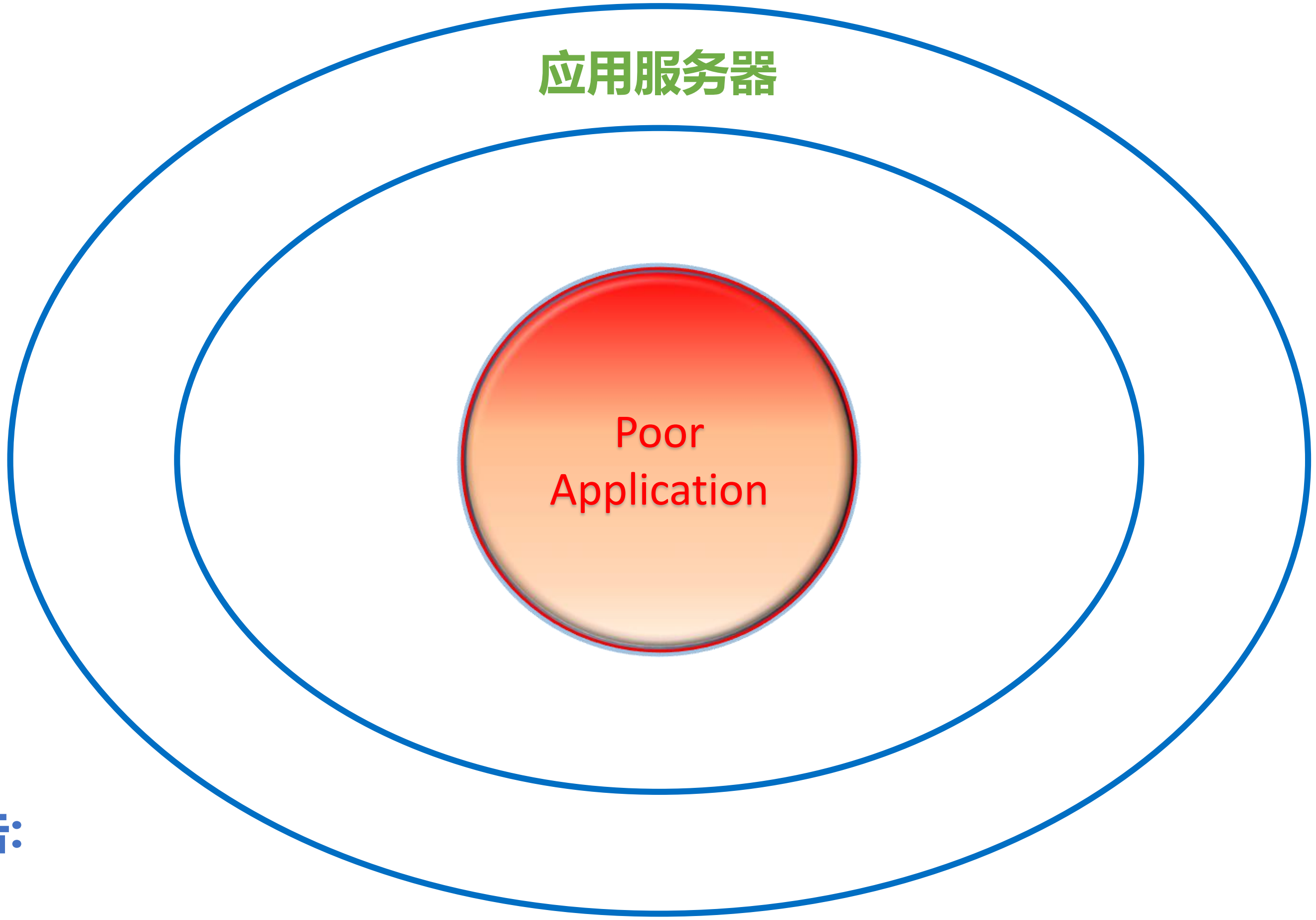
- 程序完成的太久远，找不到源代码
- 发现的应用漏洞数量太多
- 缺少安全专家去推动SSDLC
- 开发团队缺乏安全经验
- 第三方供应商的漏洞修复周期长
- 系统中存在未知的漏洞

你需要使用OneRASP产品打虚拟补丁，
来保护你的应用程序

跨站脚本攻击

周边安全体系(防火墙/IPS/AV/WAF等)

发现:已知的漏洞扫描

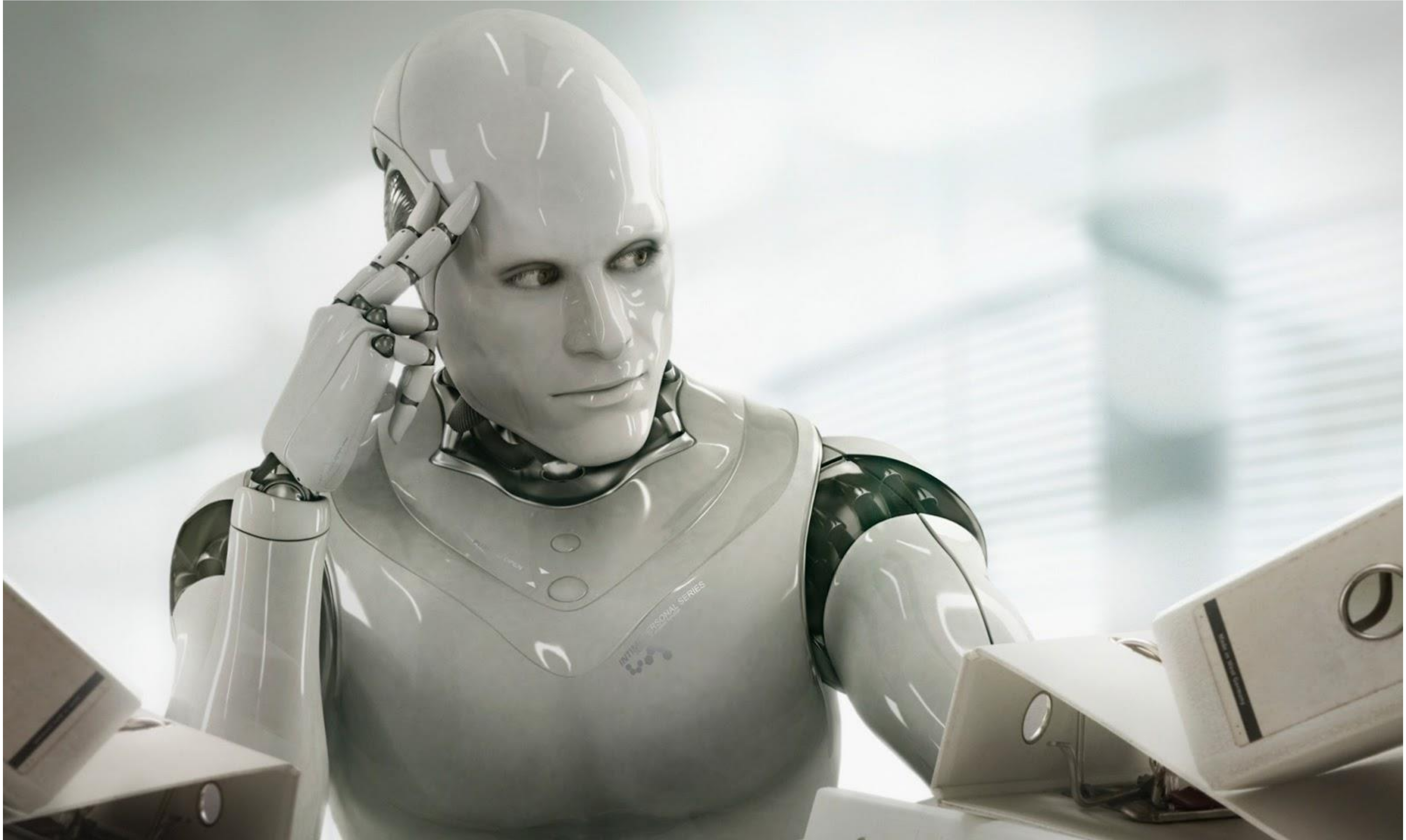


命令注入攻击

SQL注入

分布式拒绝服务攻击:
Parse Double

系统信息泄漏


PERSONAL SERIES

More details, please visit

ONE ASP RASP

www.OneASP.com

Thanks！

谢谢！