ONE ASP RASP

企业如何构造安全防护堡垒

孙政豪

目录

安全事件概览

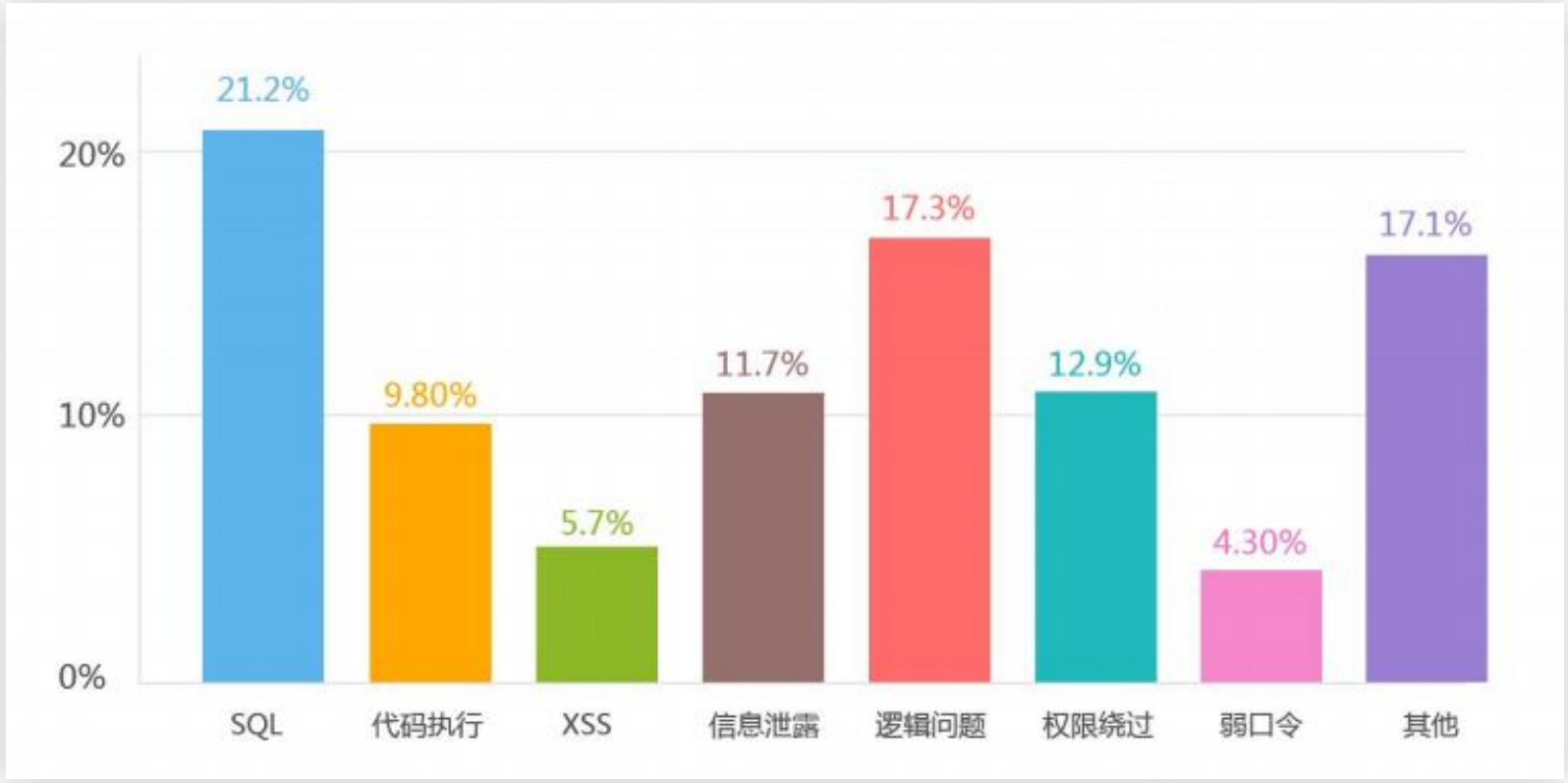
2014年全球十大安全事件四起在中国 电商网站安全漏洞堪忧

《报告》披露,2014年,各类网站存在后门的比例和绝对数量大幅攀升。统计发现,截至2014年11月30日,在164.2万个各类网站中,存在安全漏洞的网站为61.7万个,占被扫描网站总数的37.6%;存在高危安全漏洞的网站共有27.9万个,占扫描网站总数的17.0%;在后门检测中,约3465台服务器存在后门,占比41.2%,比2013年增加了7.4个百分点。

《报告》还总结了2014年全球范围内的十起网站安全事件,包括"openssl心脏出血漏洞"、"ebay数据泄露"、"索尼被黑客攻击"等,在去年的网站安全事件中"121中国互联网dns大劫难"、"携程漏洞事件"、"中国快递1400万条信息泄露"、"12306用户数据泄露"四起发生在中国。

Web安全的现状

- 超过80%的攻击发生在应用层
- 多样化的攻击越来越难以防御
- Web系统开发商在安全领域投入少



常见的攻击方式

常见的网络层DOS攻击方式

- Teardrop
- Ping of Death
- Flood
- Land
- Smurf
- 分布式拒绝服务攻击

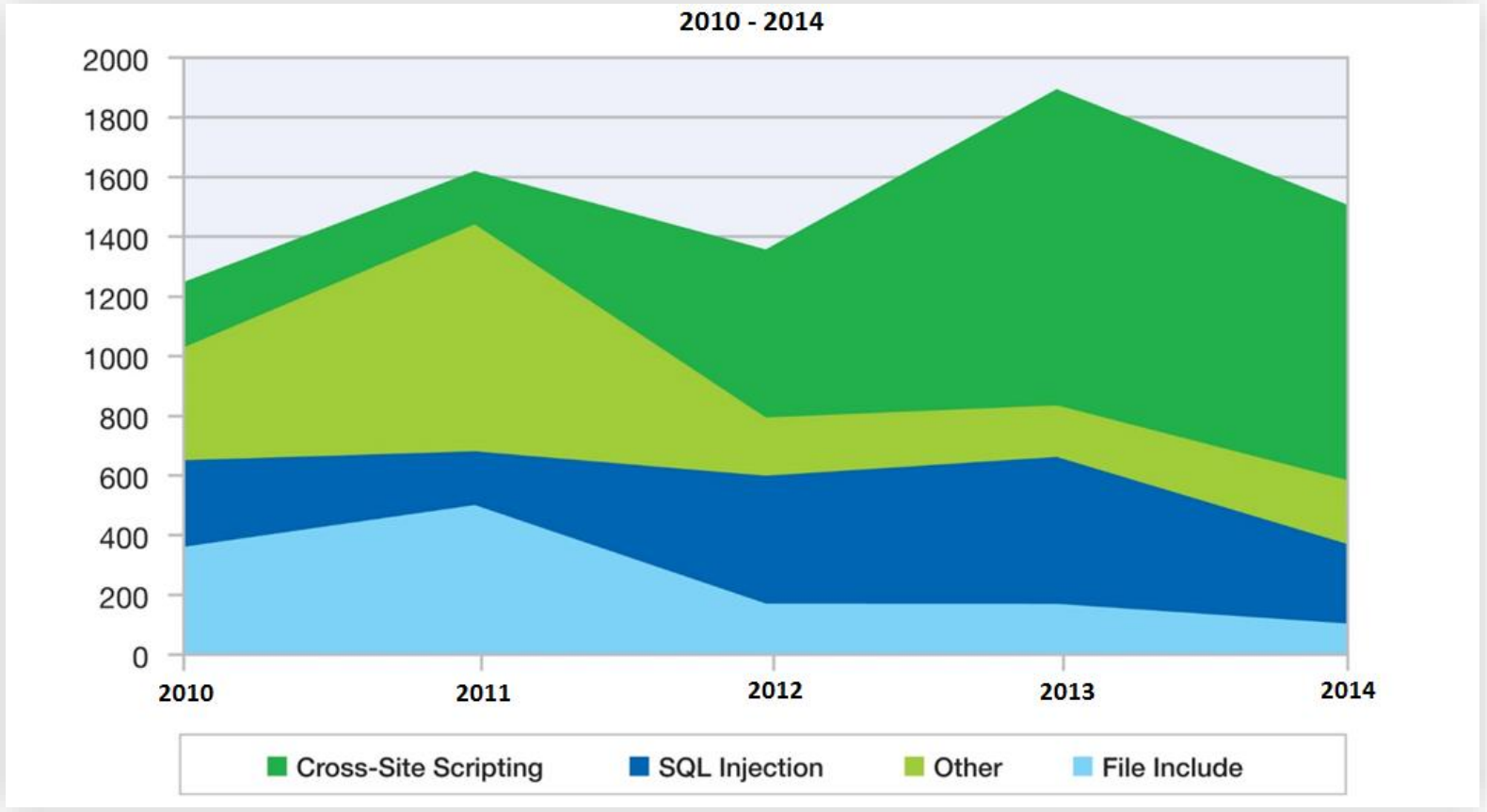
常见的主机层攻击方式

- 漏洞攻击
- 病毒攻击
- 木马攻击

常用的应用层攻击方式


Input Tampering
SQL Injection
LDAP, XPATH, XQuery Injection
Cross Site Scripting (XSS)
Exception Handling
Session Manipulation
Buffer Overflow
HTTP Parameter Pollution (HPP)
...and many more

主流的Web攻击方法



资料来源：IBM X-Force®研究与发展

OWASP（开发Web应用安全项目） Top 10

OWASP Top 10 – 2010 （旧版）	OWASP Top 10 – 2013 （新版）
A1 – 注入	*A1 – 注入*
A3 – 失效的身份认证和会话管理	*A2 – 失效的身份认证和会话管理*
A2 – 跨站脚本（XSS）	*A3 – 跨站脚本 （XSS）*
A4 – 不安全的直接对象引用	*A4 – 不安全的直接对象引用*
A6 – 安全配置错误	*A5 – 安全配置错误*
A7 – 不安全的加密存储 – 与A9合并成为→	*A6 – 敏感信息泄露*
A8 – 没有限制URL访问 – 扩展成为→	*A7 – 功能级访问控制缺失*
A5 – 跨站请求伪造（CSRF）	*A8 – 跨站请求伪造（CSRF）*
<合并在A6 – 安全配置错误>	*A9 – 使用含有已知漏洞的组件*
A10 – 未验证的重定向和转发	*A10 – 未验证的重定向和转发*

防护方法剖析

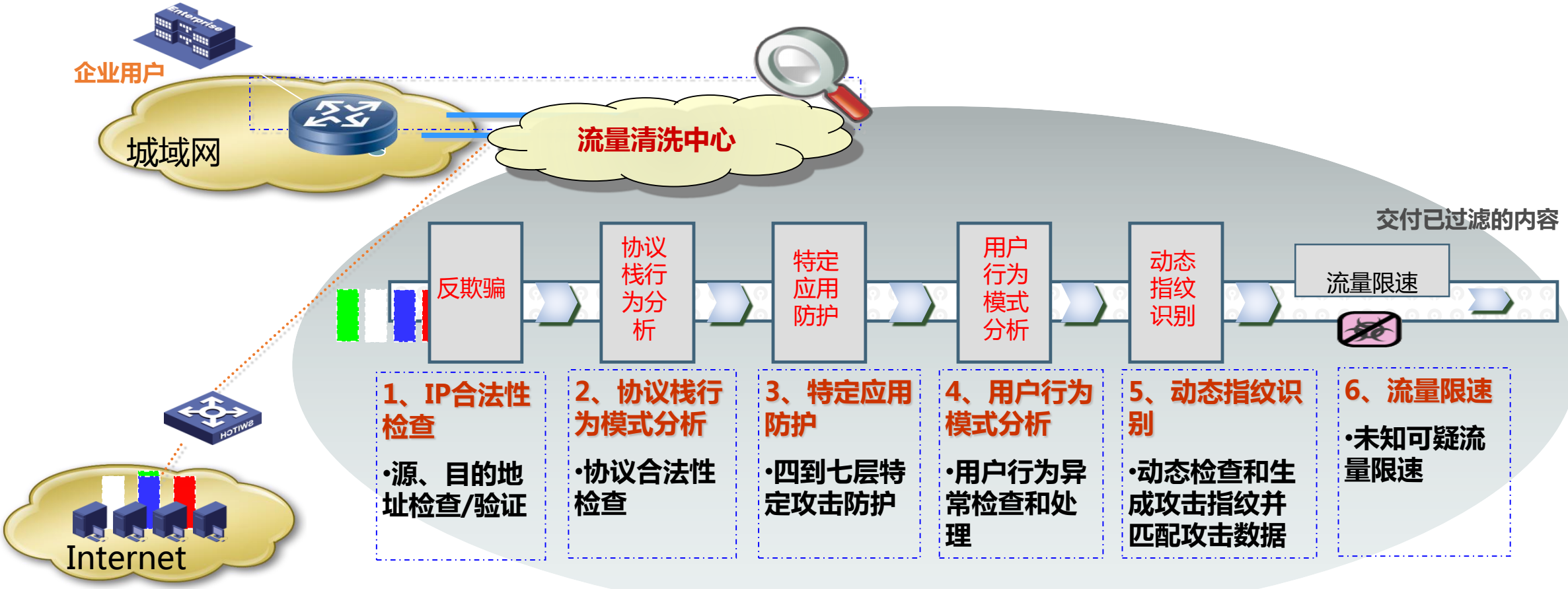
纵深安全防御模型		
	传统防御方式	新型防御方式
物理层防御	Security Guard，CCTV	
网络层防御	网段，安全，防火墙，网络访问间隔控制，IPS/IDS	
主机层防御	OS hardening ，认证，补丁管理，基于主机的 AV ，基于主机的 IDS ，基于主机的 FW	应用EDR技术的高级威胁防护系统
应用程序防御	Application hardening，SSDLC，AST(SAST，DAST，IAST), WAF	RASP（运行时应用自我保护）
数据和资源	ACLs，encryption，EFS	

常见的防护方法：纵深安全防御模型

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

流量清洗工作原理


企业用户
城域网
流量清洗中心
交付已过滤的内容
反欺骗
协议栈行为分析
特定应用防护
用户行为模式分析
动态指纹识别
流量限速
Internet
1、IP合法性检查
•源、目的地址检查/验证
2、协议栈行为模式分析
•协议合法性检查
3、特定应用防护
•四到七层特定攻击防护
4、用户行为模式分析
•用户行为异常检查和处理
5、动态指纹识别
•动态检查和生成攻击指纹并匹配攻击数据
6、流量限速
•未知可疑流量限速

常见的防护方法

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

新型主机防御：首个成熟应用EDR技术的高级威胁防护系统

- Windows XP/VISTA/7/8/8.1/10
- Windows Server 2003/2008/2012
- Linux kernel 2.6 及以后
  - Red Hat/Debian及其衍生版本

高级威胁防护
公有云

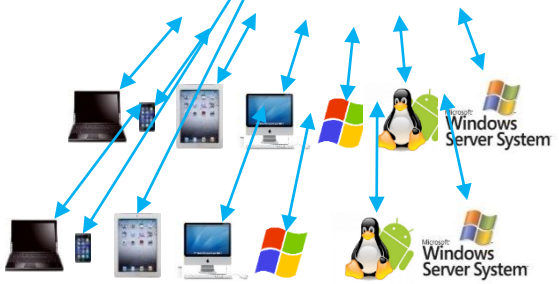
- 部署简单灵活
- 终端与服务器全程使用SSL加密链接
- WEB管理模式，随时随地管理企业安全

高级威胁防护公有云

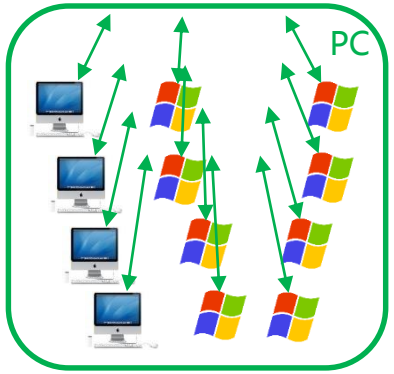
高级威胁防护私有云

SaaS安全控制中心

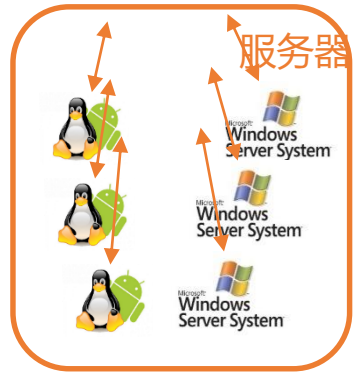
安全控制中心



中小企业



大型企业



终端检测与响应

“找不同”

- 掌握EDR核心科技
  - 操作系统级行为检测，全网终端横向比较
    - 系统调用监控
      - 是否释放可疑文件
      - 是否创建可疑进程或线程
      - 是否修改注册表
    - 内存、指令监控
      - 是否在栈上执行了二进制代码
      - 是否在堆上执行了二进制代码
      - 是否在数据区执行了二进制代码
- 已知攻击或漏洞无论如何变换都可以有效防护

ATP攻击的初期目标一般是针对少量的终端，传统的特征检测很难发现它。

“找不同”的创新检测方法可以快速发现异常，在ATP的早期就感知到可疑状况并快速响应。

“少添乱”

- 轻量无感知探针
  - 不扫描用户磁盘和网络访问，不收集用户个人信息，对终端使用零干扰
  - 仅检测系统异常行为并分析日志
  - 批量工具静默安装，终端用户无感知
  - 黑白名单结合，批量策略下发，分时扫描，极小资源消耗
- 旁路部署
  - 安全控制中心旁路部署，无需串接在网络出口

	系统行为	资源消耗
服务器	*策略下发*	*1KB*
服务器	*样本库（增量）*	*1KB*
客户端	*心跳信息*	*0.1KB*
客户端	*行为检测及日志*	*1KB*
客户端	*云防护*	*0.5KB*

传统主机防护“全家桶”易让终端不堪重负，串接在出口处的网关式部署易引发连通性问题。
“少添乱”的创新设计思想，在ATP防护的部署上更简单、更考虑使用者的体验、更容易在企业内部实行。

“快且准”

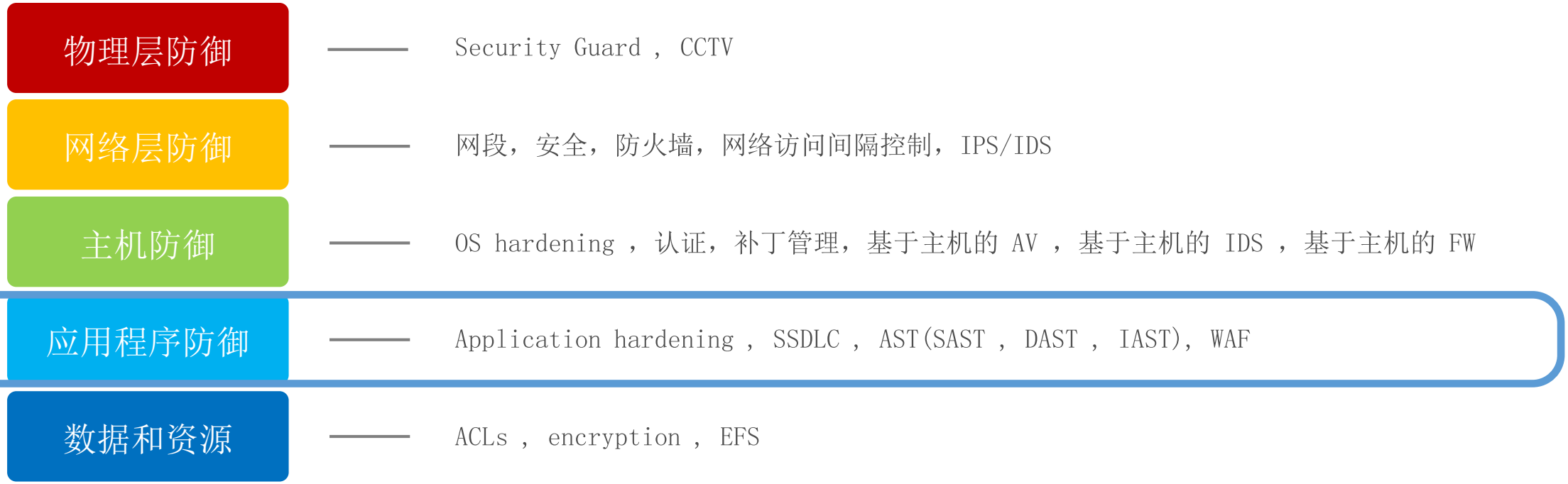
- 实时检测与防护
  - 实时检测系统状态，探针上实时执行黑/白名单策略
  - 横向对比行为异常，实时提示管理员可疑行为和文件
- 智能沙箱
  - 精确查杀PE文件格式的未知恶意软件
  - 数十亿的样本库
  - 通过时钟调速技术，有效避免针对沙箱的延时逃逸
  - 通过大数据挖掘找出正常、恶意两类软件最具有区分度的特征
  - 建立机器学习模型，使用机器学习算法得到恶意软件的识别模型

实时性和准确性往往很难平衡，效率和精度是传统安全方案无法逾越的问题。
“快且准”的平衡，通过EDR技术保障，守住企业信息安全的源头。

常见的防护方法

分层次防御

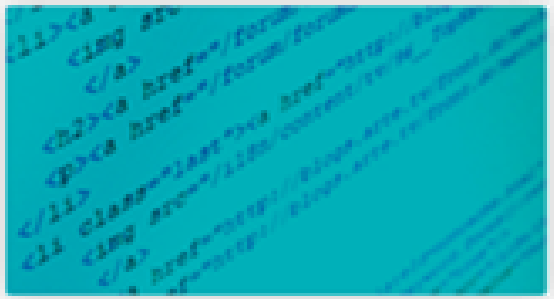
- 提高攻击者被检测到的概率
- 降低攻击者成功得手的几率



安全软件开发生命周期-SSDLC

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

Web应用防火墙

Web应用防火墙（WAF）是部署在Web服务器的入口

检测所有进入服务器的报文通过正则表达式的方式匹配报文的特征字段，来判断是否为攻击。

降低数据泄露风险

用精炼的规则对攻击实施过滤，加上HTTP协议合规检查、状态码过滤等机制，降低数据泄露风险。

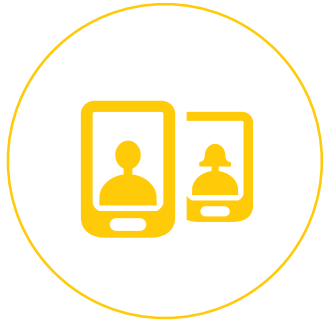
支持Web服务可用性

集成DDoS防护功能，与SQL注入防护等功能一起使用，提供多层次攻击过滤，支撑Web服务可用性。

控制恶意访问

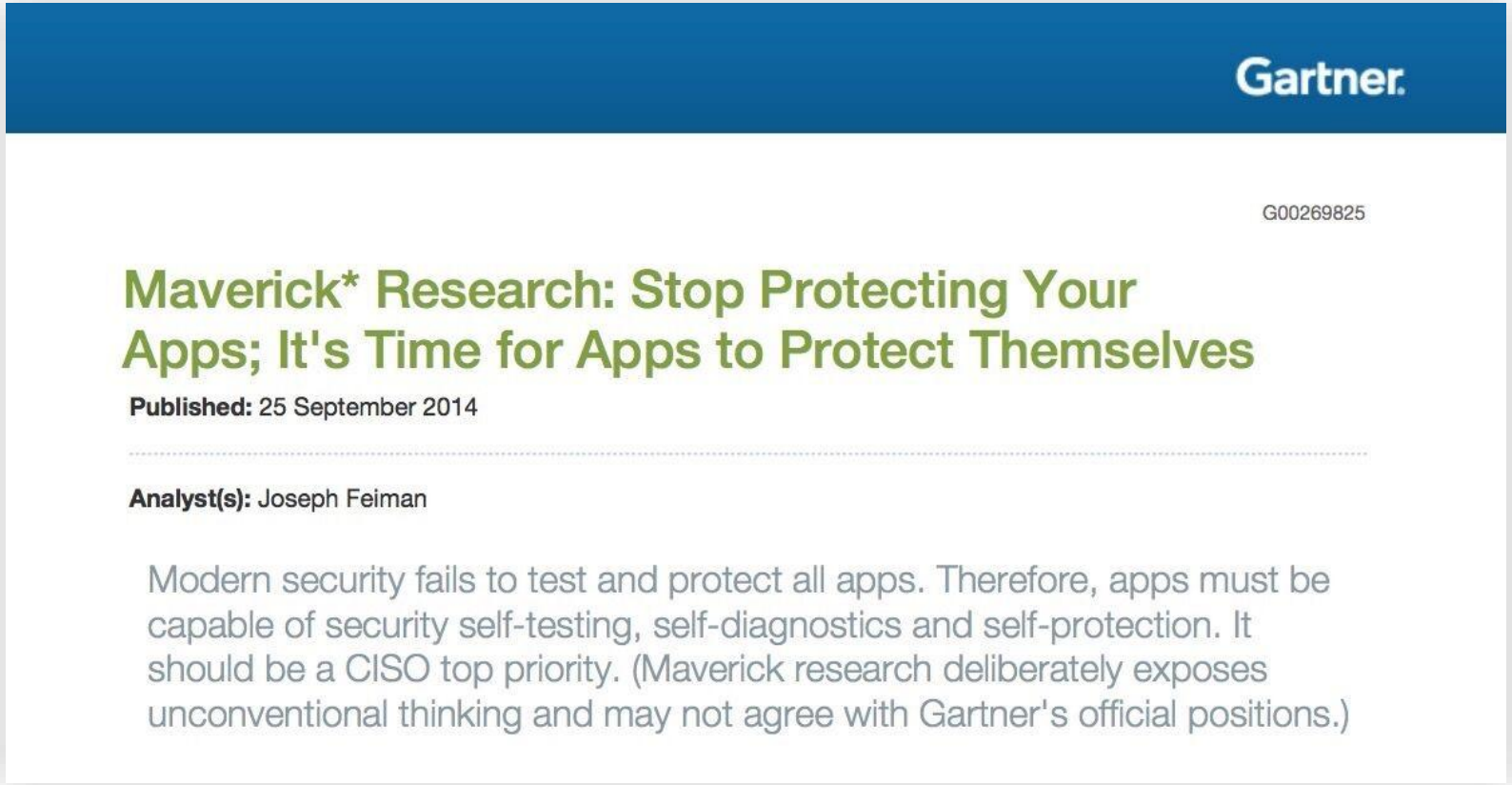
支持多种Web访问控制，包括HTTP访问控制、自动化攻击工具识别、控制非法文件上传和下载、阻止盗链和爬虫等。

保护Web客户端



提供CSRF防护、XSS防护、Cookie签名和加密等安全策略，保护Web客户端。

新型应用层防御技术：RASP（运行时应用自我保护）



Gartner

G00269825

Maverick* Research: Stop Protecting Your Apps; It's Time for Apps to Protect Themselves

Published: 25 September 2014

Analyst(s): Joseph Feiman

Modern security fails to test and protect all apps. Therefore, apps must be capable of security self-testing, self-diagnostics and self-protection. It should be a CISO top priority. (Maverick research deliberately exposes unconventional thinking and may not agree with Gartner's official positions.)

实时应用自我保护技术（Runtime Application Self - Protection）也称RASP技术，是2014年9月Gartner的调研员Feiman提出的一种全新概念。

报告指出，网络的边界逐渐在消失，同时诸如WAF这类的“边界保护”技术也无法深入应用内部，对应用的逻辑数据流理解不全面，由此带来的误杀率高的现象时有发生。

为什么需要RASP技术

- 程序完成的太久远，找不到源代码
- 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

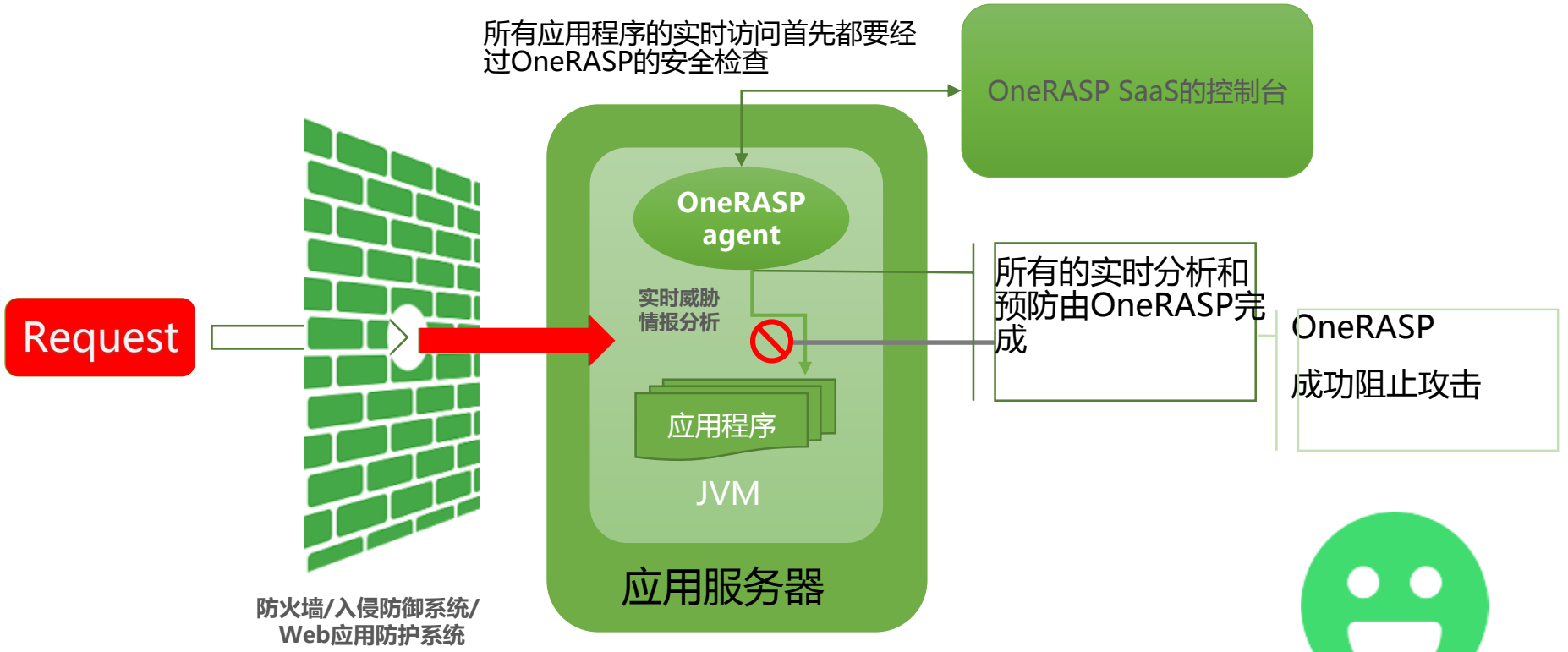
所以，你需要使用RASP技术打**虚拟补丁**，来保护你的应用程序

它像一剂疫苗注入到应用中，与应用一起运行，对外提供服务

结合应用的逻辑和数据流，在运行时对访问应用的代码进行检测

对于已知漏洞，相当于为其打了虚拟补丁，起到补偿控制后的作用

OneRASP请求实例图

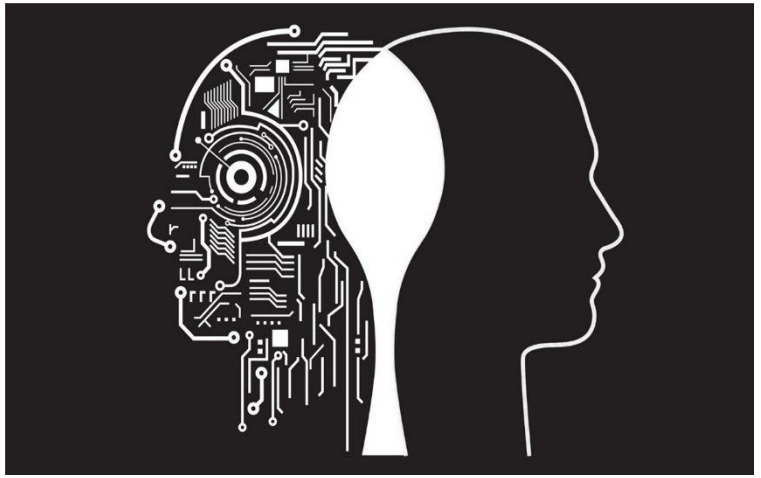


安全领域的未来

未来的安全领域是什么样的？？？

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 ！

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。



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。

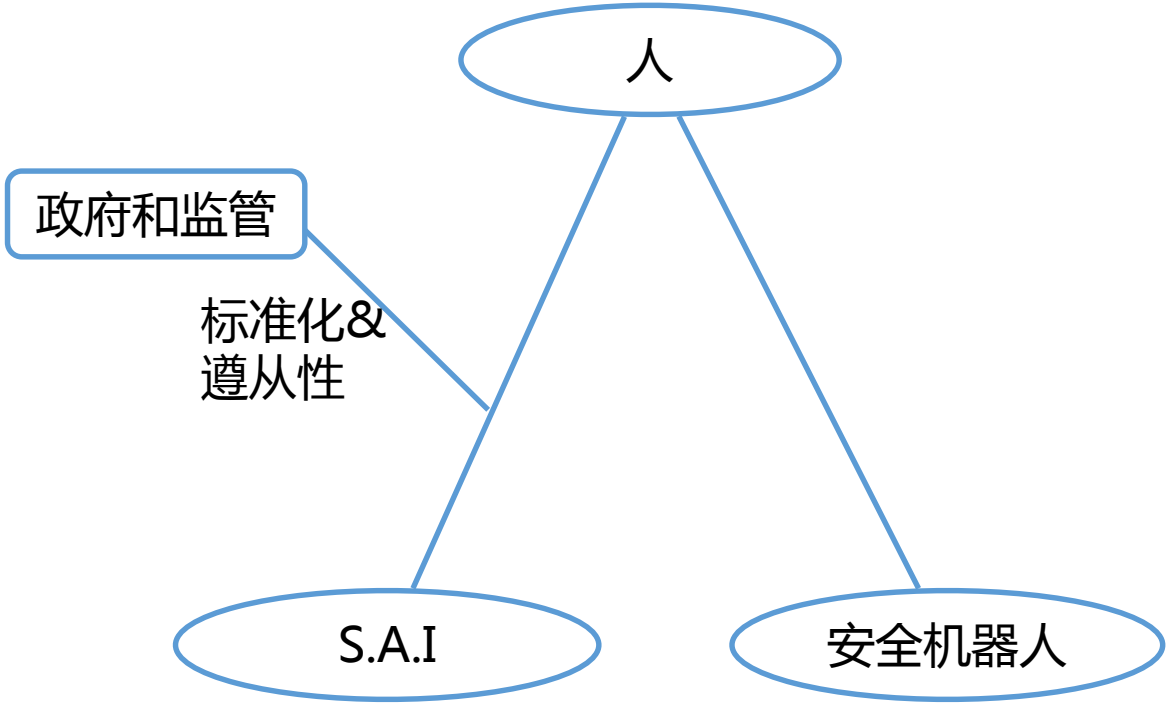
安全领域呢... AlphaSEC?

- 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？
- 我们未来会有AlphaSEC吗？
- ITSec未来会是一个什么模样？

安全领域的未来方向

- 人
  - 规则
  - 设计/定义/管理+监督/Q.A.
- 安全人工智能(S.A.I.)
  - 新规则
  - 大脑-自我学习/自我构建/自我定义/自我集成
  - 自我学习安全知识库
- 安全机器人
  - 处理执行
  - 监察/管理/执行 S.A.I. 模型
  - SAI API 和SDSec 集成

安全领域的未来方向

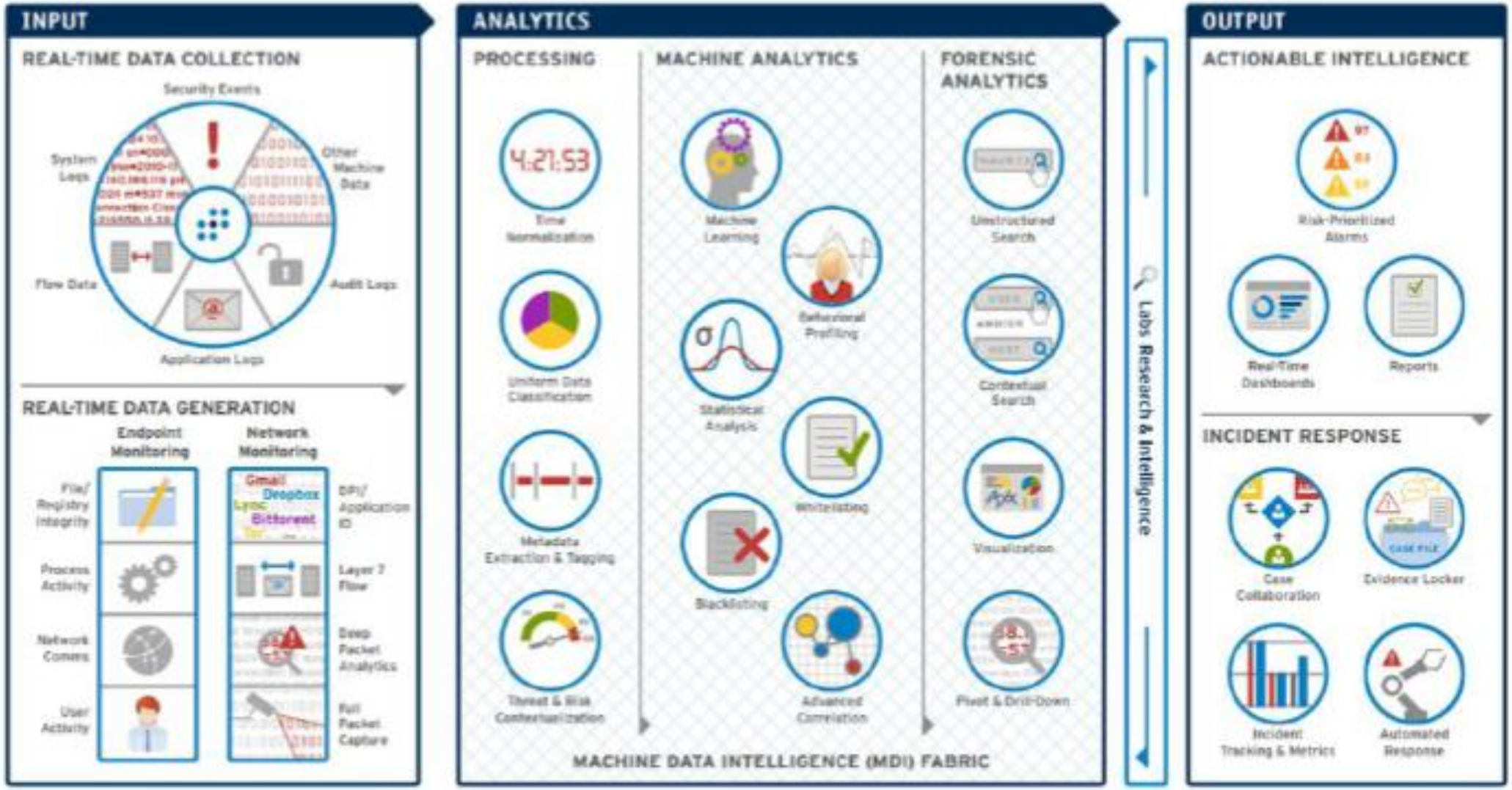


适应期：
• 刚刚兴起，未来2到5年成熟
目标：
• 赋予人工智能自我驱动自我学习的能力——一系列基于SIEM、大数据安全、智能威胁、行为检测和分析、机器学习、SOC和风控系统的实用分析和决策技术。

适应期：
• 早在8年前即2008年就已兴起（AISec 2008）
目标：
• 传统的知识和经验发展成新的安全领域——人工智能

适应期：
• 未来3到6年成熟
目标：
• 应用SAI API 和SDSec 打造S/W安全机器人

安全人工智能（S.A.I）框架

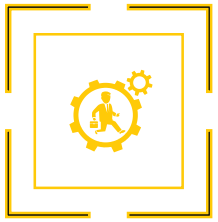


对企业安全的建议

树立安全防护意识

这个世界上一共有两种公司：一种被「黑」过，另一种，不知道自己被「黑」过。

安全防护工作，不能存在任何侥幸心理。



谨慎选择安全防护方案

市面上的安全防护方案鱼龙混杂，很大部分已经完全不适应如今的网络威胁形势，两点建议：

1. 不要试图通过让系统变复杂来换取安全，越复杂越容易暴漏缺陷。
2. 充分考察解决方案的合理性，预防因方案漏洞引入了新的威胁。

没有一劳永逸的方案

黑客攻击手段越来越先进，安全防护方案不可能是一成不变的，

持续关注安全防护的发展方向，时刻做最有效的调整。

谢谢！