**自适应安全架构在数据中心**

**网络安全管控的实践**

随着云计算、大数据、移动互联、物联网等新技术的成熟，社交网络、电子商务、智慧城市的发展，已经使人们的生活全面走进了由网络所构建的虚拟世界。事物总是有两面性，当虚拟世界越来越丰富的时候，面临的安全威胁也随之越来越多，金融行业因其特殊背景，面临的风险更加突出。近年来，针对金融行业关键信息基础设施的网络攻击常态化且针对性强，甚至出现了具备APT特征的高技术含量攻击。在这种严峻的网络安全形势下，如何有效应对成为了各金融机构数据中心非常重要的课题，下面是招商银行信息技术部数据中心在这方面的探索和实践。

1. 安全形势分析

网络安全核心实际上是攻防双方的一种博弈，在这个博弈对局中，防御方想战胜攻击方，扭转天生的被动局面，必须对目前的博弈环境有一个充分认识。

首先是“攻击面扩大”带来的挑战。由于云计算、大数据、移动互联、物联网等新技术的发展，组织机构会充分利用无处不在的网络连接、海量分析、低成本、高扩展性的技术平台，敏捷快速成为主旋律，这样会大幅增加组织机构的受攻击面。

其次是“网络无边界”带来的挑战。随着云计算、wifi、移动互联网、远程办公等网络场景、应用场景的出现，网络访问与接入对移动性提出了前所未有的要求和挑战，“网络无边界”已经成为了必然，企业的安全边界不再是企业的网络边界，过去纵深防御机制中非常强调的边界防御（Firewall、IDS、IPS、WAF、Anti-DDOS）的适用性受到了极大的挑战。

最后是“军火民用化、攻击组织化”带来的挑战。从近期被曝出的美国总统候选人希拉里团队电脑疑遭黑客攻击事件，俄罗斯20多个政府机构被植入间谍软件，“永恒之蓝”的勒索病毒席卷全球，体现一个显著特征“军火民用化、攻击组织化”，这种形式下攻击常态化、专业化和精细化。

1. 安全应对（自适应安全架构）

传统的安全管控基本包括以下几个方面：一是安全理念是御敌于国门之外，对内部异常防范通过隔离和封堵实现；二是管理框架体系采取ISO27001；三是技术框架体系采取基于签名/特征的纵深防御机制，整个体系强依赖内部的“严”管理和外部基于签名和网络隔离的纵深防御，希望通过“事前”控制机制实现“零”风险。

传统的安全管控机制诞生在相对封闭的非互联网时代，网络经济还处于初级阶段，各种连接也比较弱，金融业务主要依赖柜台、ATM、POS，如果能够提供基于互联网的交易已经让人骄傲无比了，在这种形态下，传统的安全管控机制完全可以匹配业务的发展。但是随着科技创新涌现时代的来临，沟通、协作、万物互联是历史的趋势，一切数字化，业务也演变出各种形态，“严”管理和外部基于签名和网络隔离的纵深防御已经很难适应业务发展需求，迫切需要创新。

传统的安全管控机制由于本身技术限制，漏报误报频频，在面对爆炸式攻击时，在面对社会工程学攻击时，都举步维艰，同时攻击者越来越多的采取未知攻击手段进行渗透，依矛铸盾的攻防思路能被轻松绕过。

面对这种形式，Gartner提出面向下一代的安全体系框架--自适应安全框架（ASA），以应对云大物移智时代所面临的安全形势。自适应安全框架）从预测、防御、检测、响应四个维度，强调安全防护是一个持续处理的、循环的过程，细粒度、多角度、持续化的对安全威胁进行实时动态分析，自动适应不断变化的网络和威胁环境，并不断优化自身的安全防御机制。

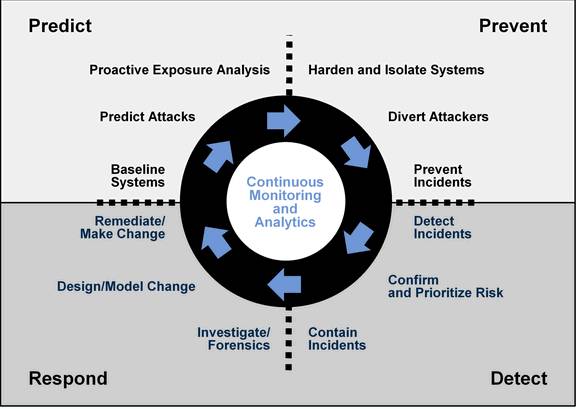


图1：Gartner自适应安全架构

Gartner预测：有针对性的高级攻击将以预防为中心的战略过时，2020年，企业需要向以信息为中心和以人为中心的安全战略转变，再结合内部普遍监控和安全情报分享，才能确保企业安全。

1. 我行数据中心自适应安全架构实践

自适应安全架构是Gartner总结的一套通用架构，它必须和组织的实际情况相结合才充分发挥其内在价值。我行根据自身实际情况，对总体自适应架构进行了少许更改形成了招商银行数据中心网络安全自适应安全架构。

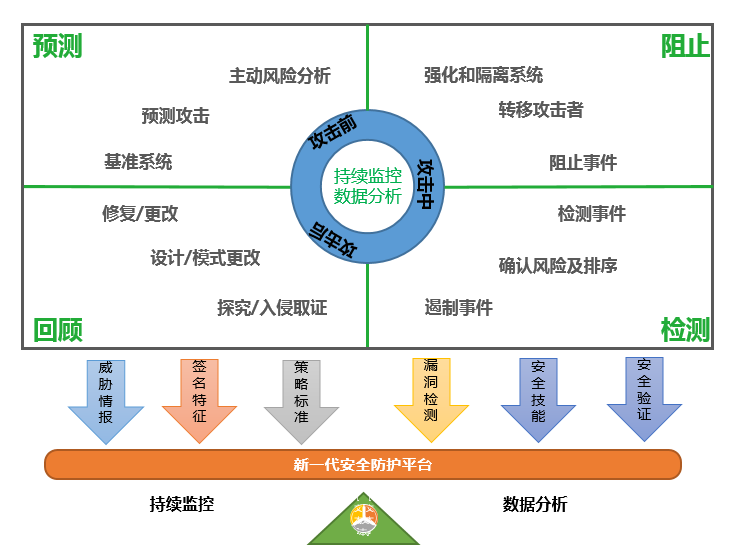


图2：招商银行自适应安全架构

下面简要介绍一下我行自适应安全架构的总体实现情况。

1. 安全理念

做什么事情，核心理念非常重要，这是我们一切工作的前提，理念符合实际了，架构和运营才能真正的落地。

第一个理念是：攻击一定会发生，而且常态化和专业化，“黑天鹅”后面都隐藏着“灰犀牛”；

第二个理念：我们的对手从个人到有组织经济犯罪，到网络战，包括黑客、异常员工、第三方、黑客集团，甚至XX国家；

第三个理念：攻击渠道覆盖所有暴露的攻击面，包括终端、渠道、设备、系统、应用、服务、第三方、员工等等；

第四个理念：漏洞一定存在，并且可能覆盖所有攻击面，所以御敌国门之外基本是奢望，所以管控重心应该在预测、检测、响应三个维度；

第五个理念：对抗最终是“数据”+“人”的对抗，所以数据行为分析是主战场。另外欺骗对欺骗在实力超过我方的对抗中会有意想不到的效果。

1. 安全定位

按照攻击者能力的不同，我行将攻击者分为以下等级：

第一级：国家行为，掌握硬件后门或0day漏洞；具备超维攻击能力，例如光缆窃听等；

第二级：黑客集团，掌握操作系统和应用0day漏洞；具备开发免杀病毒、固件病毒等高级病毒的能力

第三级：异常员工，具备内部系统、设备接入权限甚至管理权限；熟悉系统应用逻辑、代码实现

第四级：第三方，主要是通过第三方专线进入的黑客

第五级：个人黑客，只掌握已公开的操作、应用组件漏洞；主要攻击SQL注入、跨站脚本这类常见漏洞，或越权访问等业务逻辑漏洞

下图是不同维度的攻击者掌握的攻击能力分析：



综合自身能力，我行博弈对抗对手定位为：黑客集团、异常员工、第三方、个人黑客，对于国家行为的对抗至少在未来三年不考虑。

1. 安全思路和指标

基于自适应安全架构，从过去强调防御，转变为更加强调预测、检测、响应；

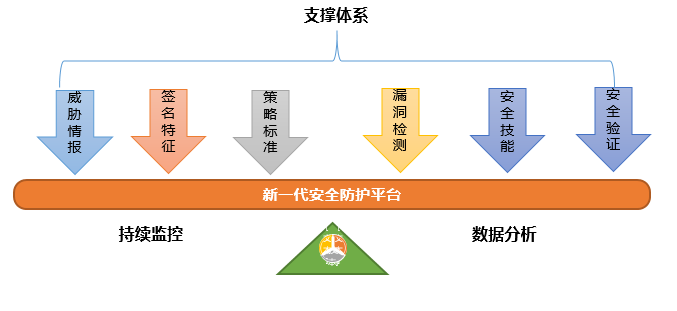
四个维度的控制重点：防御能力以降低最小攻击面为核心，检测能力以降低攻击发现时间为核心，响应能力以降低攻击持续时间和攻击强度为核心，预测能力以情报覆盖使用度为核心。

根据理念、定位和思路形成具体的安全指标：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | 防御能力 | 检测能力  MTTD | 响应能力  MTTR | 预测能力 |
| 黑客集团 | 略 | | | |
| 异常员工 |
| 第三方 |
| 黑客 |

1. 自适应安全架构建设情况
2. 支撑体系建设情况

支撑体系包括六个方面，分别是策略标准、签名特征、威胁情报、漏洞检测、安全验证、安全技能，策略主要负责系统的配置、更新、网络活动以及响应机制；签名特征主要负责安全控制组件的更新策略；威胁情报主要负责通过和内部情报结合，协助自适应架构各组件保护关键资产；漏洞检测负责攻击面按照策略实现最小化；安全验证负责建立自动化验证机制确保安全管控的有效性；安全技能负责安全人员的知识能力培养。



* 策略标准

关键词：标准化（通过工具实现自动化检查）

制定策略包括配置类、补丁类、端口应用类、敏感数据类、应急响应类，核心思想是标准化攻击面，指引自适应架构的防御组件的相关配置和运营。

配置类：网络配置规范、服务器配置规范、web服务器配置规范、数据库配置规范、第三方框架配置规范、安全设备配置规范。

补丁类：网络、服务器、应用、数据库的补丁安装策略，这一类策略的制定最大的风险就是兼顾系统和应用的可用性，所以会根据面临风险的大小来确定具体的更新频率，在实施过程中会采用灰度和分布实施策略。

端口类：互联网服务系统管理规范、外联网服务系统管理规范，这类规范主要明确对外开放的类型，限制容易出现问题的端口、应用和服务（比如ftp、struts2、后台维护界面）

敏感数据类：定义敏感数据类型，指引防御、检测的组件实施具体的防御和检测，在数据层增加一道防线。

应急响应类：制定主要攻击类型的响应机制，包括web攻击、DDOS攻击、数据攻击、内部员工异常行为。

* 签名特征

关键词：持续更新

签名特征主要负责安全控制组件的更新策略，我们基本上按照以下标准进行签名特征更新：一、旁路类安全组件更新采取实时更新机制，比如IDS、异常流量；二、在线类安全组件的更新根据风险和业务的影响程度进行更新，比如IPS、WAF、防病毒、防火墙的更新。

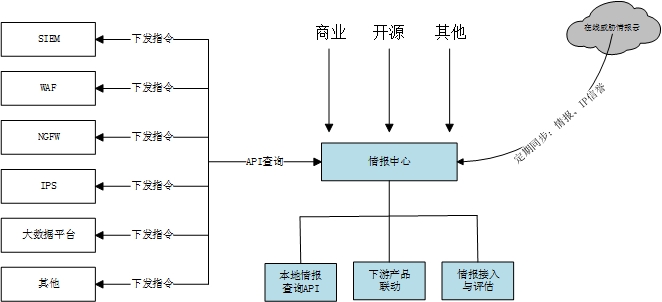
* 威胁情报

关键词：知彼

威胁情报分为战略情报和战术情报两种，战略情报主要从宏观层面指引我行整体的安全网络规划和思路的调整更新，比如每年的RSA大会和Gartner各项预测、框架、报告；战术情报是具体的攻击细节，包括IOC情报、TTP情报，具体内容包括攻击的上下文、各种信誉数据（URL、IP、MD5）等等，下面是我行情报体系：



情报的使用在我们未来的安全体系中起到非常重要的几个作用：一是通过情报共享让企业和黑客组织的战斗，由过去的单打独斗变成合成作战，在资源对抗中获得了优势；二是情报和防御、检测、响应组合一起可以极大扩充各维度的能力；三是情报和大数据的结合，让预测安全成为了可能。下面是我们情报和防御组件相结合的案例：



* 漏洞检测

关键词：知己

建立常态化的漏洞检测机制，感知攻击面，验证攻击面是否实现最小化。下面是我们对攻击面和防守面的进行了一个抽象，根据抽象形成我们的漏洞检测扫描机制：

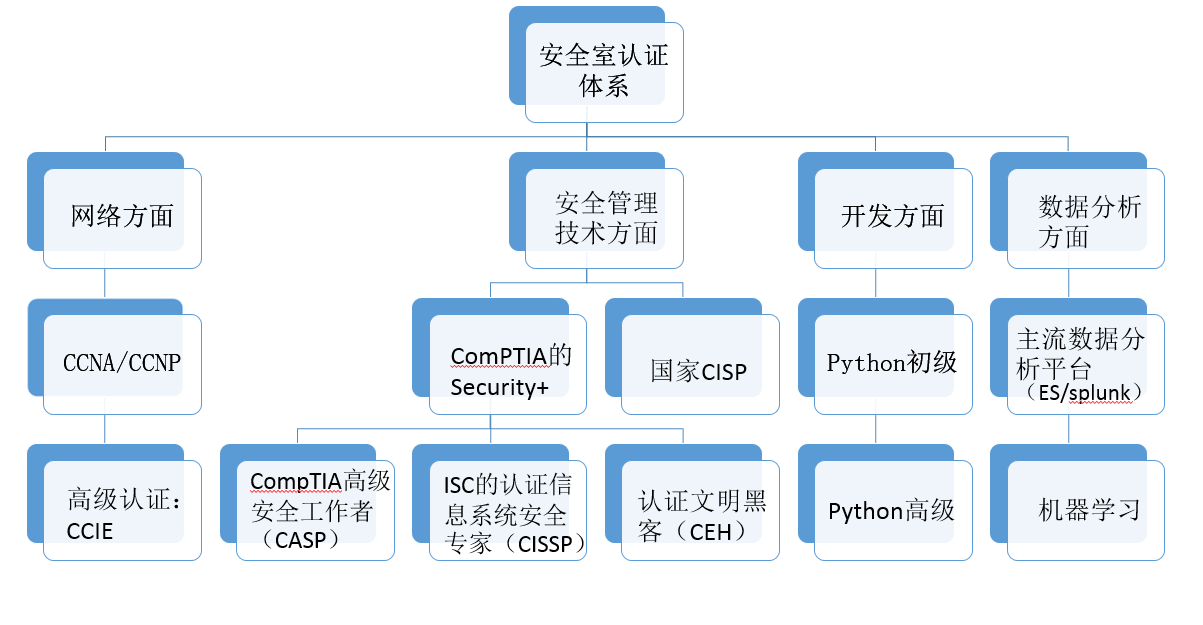
|  |  |  |  |
| --- | --- | --- | --- |
|  | 攻击面 | 防守面 | 漏洞检测机制 |
| 业务层 | 不可信交易 | 确保可信人员、可信设备和可信交易 | 常态化漏洞挖据、钓鱼网站检测系统、Github检测 |
| 数据层 | 不可信用户 | 确保非法人员 | 常态化漏洞挖据 |
| 应用层 | 不可信的应用指令 | 确保应用指令和调用合法 | 开发测试阶段：SDL  运维阶段：自建Web扫描系统、web云扫描系统、应用安全态势系统、常态化漏洞挖据 |
| 系统层 | 不可信的系统指令 | 确保系统指令合法 | 防病毒常态化扫描系统、主机层面漏扫系统、补丁检测系统 |
| 虚拟层 | 不可信的镜像和容器 | 确保镜像和容器合法 | 镜像和容器的常态化扫描系统还在建设中 |
| 网络层 | 不可信的IP | 确保IP和端口开放的最小化 | 互联网开放端口扫描系统、关键区域端口扫描系统 |
| 硬件层 | 不可信的硬件设备 | 不在讨论范围内 | |
| 物理层 | 不可信的外部人员 | 不在讨论范围内 | |

另外组建蓝军，模拟“对手”角色，实现真实对抗。目前蓝军的规模和人员使用（内部员工和外部员工的选择）还在摸索阶段。

* 安全技能

关键词：广而精

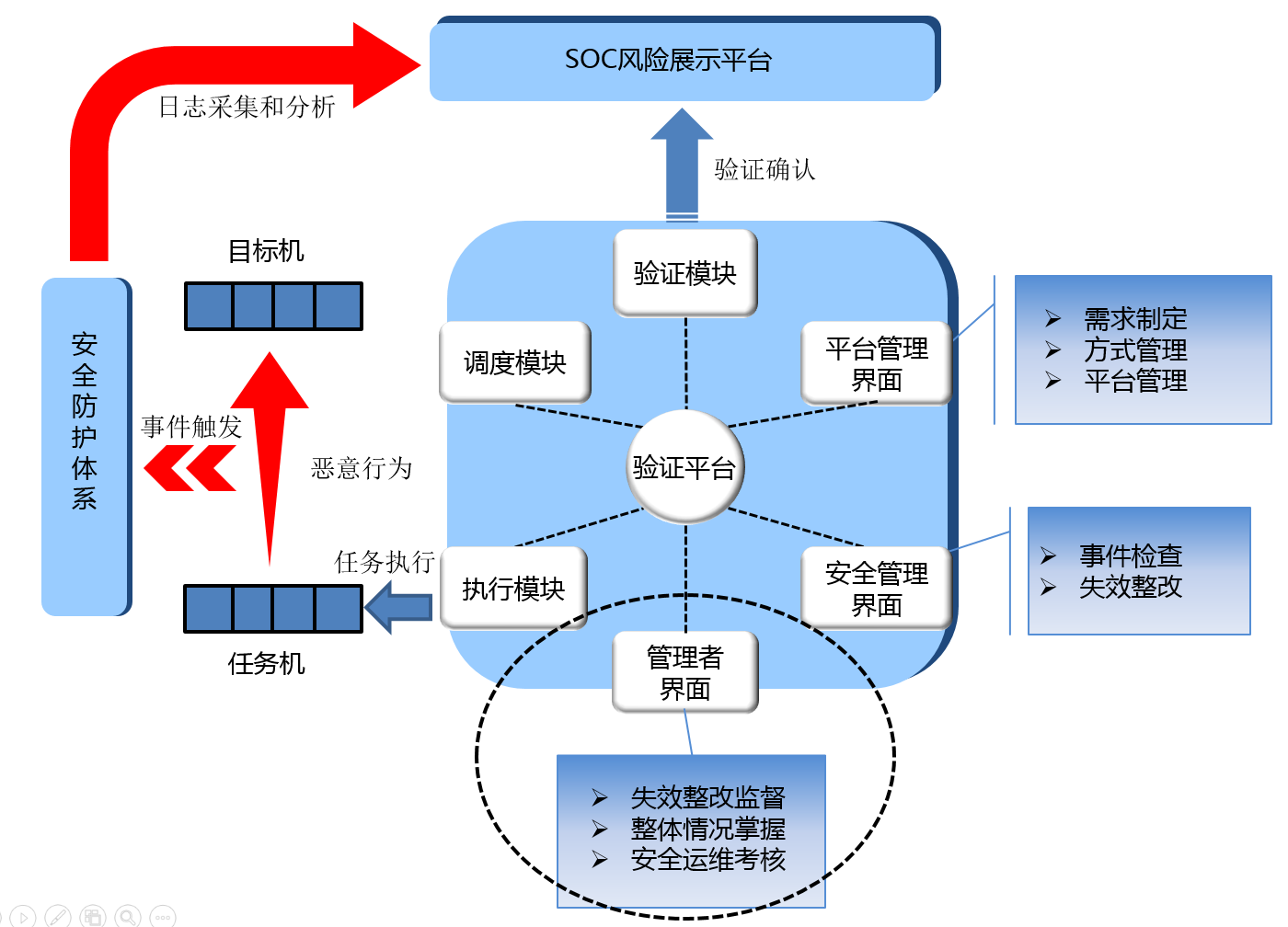
安全博弈，最终还是人和人的对抗，所以安全人员本身的技能也直接影响到这场对局，下面是我们制定的人员技能树：



* 安全验证

关键词：全覆盖

随着组织的规模扩大，安全管控措施也随之出现爆发式增长，具体表现是大量安全管控设备、安全管控工具、管控脚本的出现，有效地管理这些安全管控措施就成为了一个重要课题。我们的解决方案就是构建自动化的安全验证，通过自动构建测试案例验证安全防护功能和安全运维能力是有效、可靠的，安全验证要覆盖所有安全管控点，安全控制点出现问题，能够在24小时发现24小时解决。下图是我行的安全验证架构：



1. 防御维度的建设情况

防御维度的核心工作就是在整个协议栈将攻击面降至最小，在我们的防御体系主要承担黑客或者第三方从互联网渠道和第三方渠道通过自动化工具或者脚本发起的攻击。



* 强化和隔离系统

强化和隔离系统的功能是采用多种技术降低攻击面，限制黑客接触系统、发现漏洞和执行恶意代码的能力。

在我们这个体系中，通过防火墙、ACL只允许信任IP访问开放业务；通过防病毒、HIPS实现系统层的白名单模式；通过IPS、WAF、SDL、API可信实现应用操作的可信；通过加密（数据和通讯）实现人员的可信访问；通过风控防欺诈系统实现交易的可信。（注：HIPS是否具备拦截能力，以及API可信建设我行还在探索中）

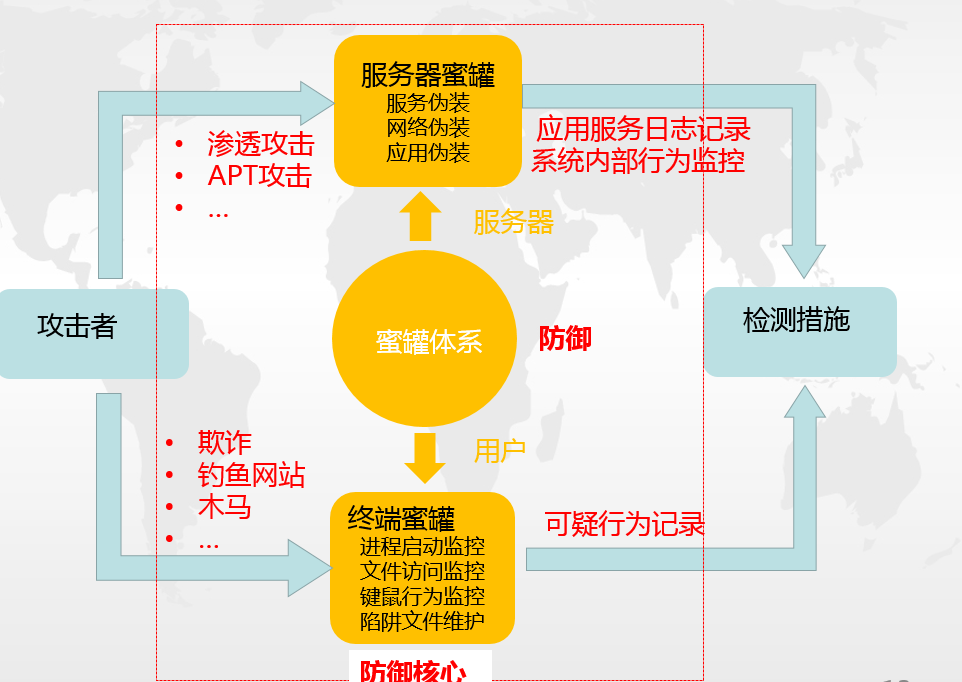
我们在实践这部分架构设计时，也参照了google对外公布的基础设施安全架构，值得我们一起学习，在这儿做个简单分享：谷歌的安全目标是实现对国家行为级别攻击的防御，因此在硬件层、物理层，谷歌均有针对性防御措施。同时，为了满足自己全球化部署、应用互联互通的需求，谷歌将纵深防御构建在应用层。详见下图。

另外DDOS防护在整个数据中心的网络安全防护中是一个很重要的方面，下面是我行针对不同类型的DDOS攻击的防护举措：



* 转移攻击者

在Garnter自适应架构中，“转移攻击者”控制点是通过技术隐藏和混淆系统，增加攻击难度和浪费黑客时间，解决黑客在时间方面拥有的不对称优势。蜜罐是一种典型技术。

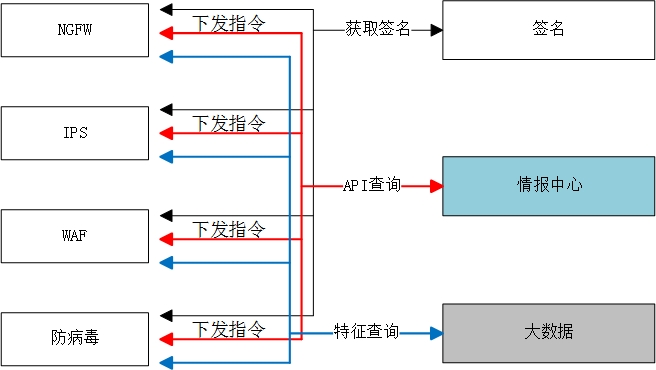
我行对“转移攻击者”的理解，认为这个控制点主要针对对象是已经攻破系统的黑客集团和本身拥有内部权限的异常员工如果简单的采用Garnter架构上的蜜罐技术（在网络层模拟真实应用）很难实现具体目标，所以我们对该架构进行了一定优化，在网络、系统、应用、指令、数据多个维度构建蜜罐体系，最终实现“转移攻击者”的目标，下图是我们蜜罐体系示意图： 

每个VLAN都有模拟各种应用的蜜罐服务器，每一台服务器都有模拟的敏感服务端口（这一功能还在进行中），每一台服务器都包含带有宏指令的蜜罐文件（这一功能还在进行中）和伪装过的蜜指令。举一个蜜指令例子，每台服务器上都一条经过包装了whoami指令，这条指令黑客经常使用，当黑客通过某种方式进入系统后，一定会对环境进行一个确认，whoami指令通常会执行，这样就会触发我们的后台监控报警。关于蜜罐体系的未来设想，我们希望实现“全民皆兵”，每一台设备都有蜜罐，让攻击寸步难行。

目前RSA创新沙盒的评选和Garnter的预测，都将蜜罐的使用都作为重点方向，除了我们“全民皆兵”这个思路，另外的思路是通过网络层将攻击流量诱因至蜜罐区域。

* 阻止攻击

阻止攻击主要是利用传统的“基于签名”的反病毒系统和基于“行为签名”的IPS系统、NGFW系统、WAF系统进行攻击拦截，另外和情报、大数据的结合是我们目前打造的主要方向。



1. 检测维度的建设情况

检测维度的建设已然成我行网络安全建设最重要的方向，也是投入最大的方向。在整个能力建设中，我们最关注的就是“异常行为”的发现，但凡走过必留痕迹，所以“看见”成为了检测最重要的能力--看见用户异常行为（UEBA）。

异常行为的主要场景：网络层（隐蔽信道、异常通讯）、系统层（异常指令、异常进程、异常用户）、应用层（攻击特征）、终端层（异常用户行为）、数据层（异常表访问、数据外泄）

下图是我们在检测维度的应对示意图：



* 检测事件

首先介绍我行整个检测体系架构：



上层检测层负责主要维度的数据收集：

|  |  |
| --- | --- |
| 网络层 | 异常流量系统：负责网络六元组的收集和简单学习分析（针对异常通讯）  网络UEBA系统（实施进行中）：负责网络流量内容识别（针对隐蔽信道和异常通讯 |
| 系统层 | socagent:负责收集系统日志  sysman\linuxagent:负责收集进程MD5、驱动、网络连接等等  flumeagent：负责收集应用日志 |
| 应用层 | IPS负责检测流量中是否有应用攻击 |
| 数据层 | 数据库安全、数据库审计：负责检测异常表访问  DLP负责边界数据泄露和指令执行 |
| 终端层 | 终端UEBA（实施进行中）：负责维护终端的行为识别 |
| 蜜罐层 | 蜜罐体系协助总体检测 |

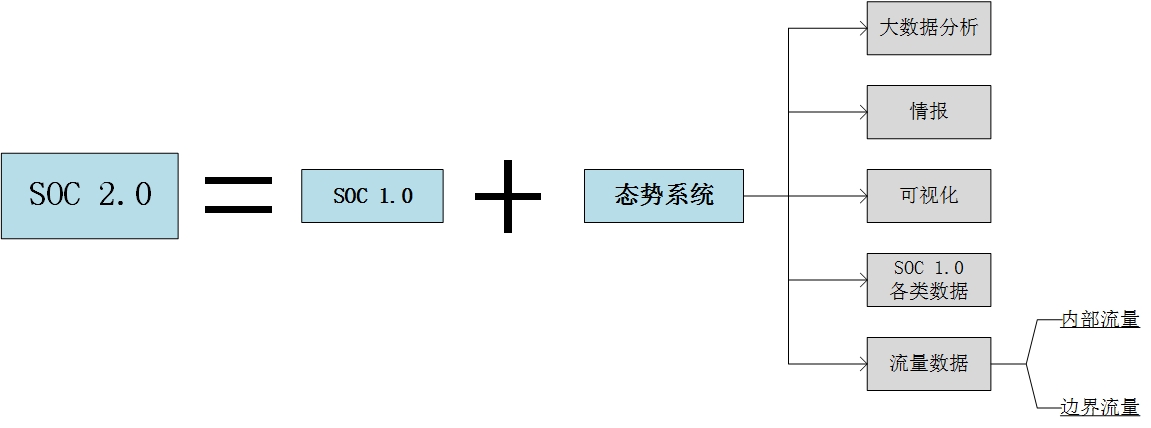
下层：就是我们的SOC系统，负责信息汇总、关联分析、风险展示和报警处置，也就是现在比较流行的态势系统。

下面我们重点介绍这个体系中几个重要支撑：

* SOC体系建设

我行SOC1.0 从2009年进行开始进行平台基础建设，2013年进行SOC运维平台和运维机制建设，2015年成体系，实现7X24小时安全事件响应和处理，建立了包含安全日志采集和监控、安全事件预警和分析、安全事件响应和处理、安全事件回顾和总结的闭环；制定和完善安全事件的响应和处理流程，明确各岗位的工作职责，建立安全事件调查知识库，通过日报、周报、月报的方式提供安全事件的调查处理过程和安全建议；建立由一线、二线、三线组成的SOC运维团队和汇报机制。

SOC1.0初步完成建设以后，面临几个问题：一是SOC平台建立在传统架构上，数据大以后出现性能瓶颈；二是可视化能力较弱；三是基于规则匹配所以精确度不够；四是缺乏上下文误报较高。所以从2016年开始我们启动了SOC2.0的建设，重点解决以上问题，具体通过态势系统实现。



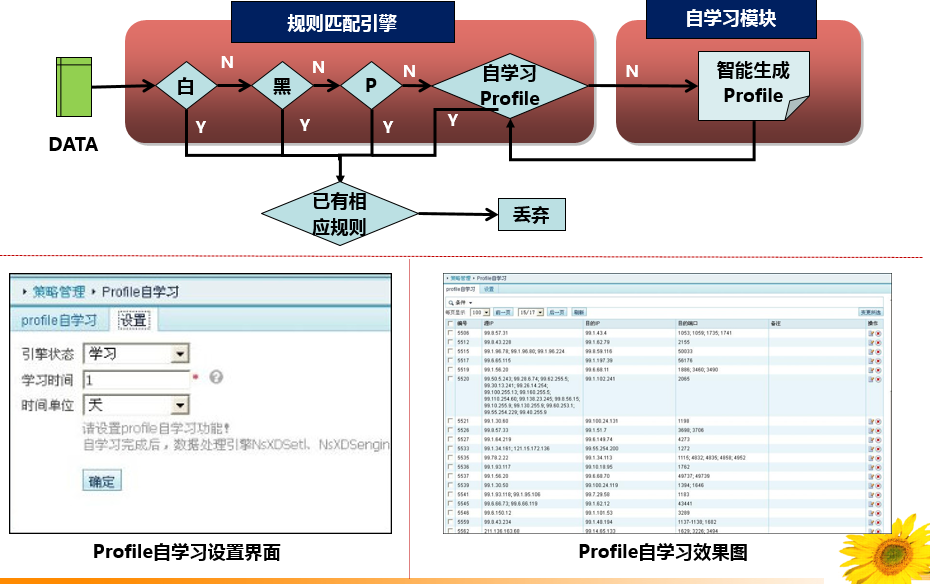
态势系统在我行数据中心未来的安全建设中处于高优先级地位，我们也设计规划了具体的发展规划图，主要思路是：传统网络安全—〉应用安全—〉业务安全，我们也希望通过这个平台建设实现真正意义的数据驱动安全和智能驱动安全。



* 异常流量系统

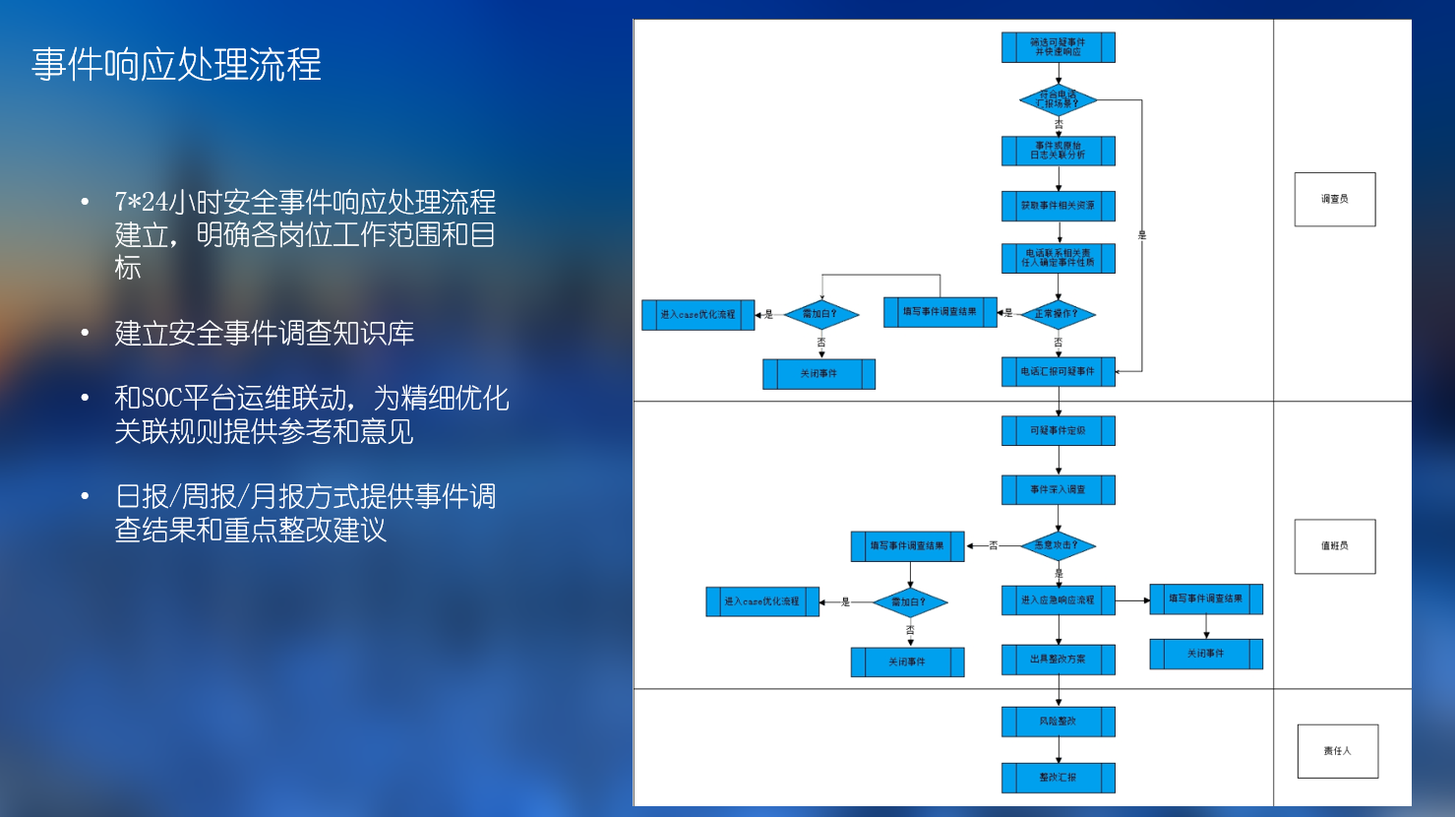
SOC1.0时代我们有一个比较有代表性的系统—异常流量系统，下面简单介绍一下。其原理是对网络流量进行镜像并分析，提取六元组（时间、源IP、源端口、目的IP、目的端口、协议）来进行分析。分析主要有两个切入点，一个是基于访问路径的异常，一个是基于访问频率的异常。按六元组来标识访问关系及统计访问频率，通过自学习模式生成白名单和profile规则，按照我们的管控规则自定义黑名单，对后续流量按照白名单、黑名单、profile规则的顺序进行匹配，对高风险事件进行实时告警。同时，针对隐蔽信道检测也进行了针对性的定制开发，对常见的icmp tunnel、dns tunnel也能发现。

经过近多年的持续运营优化与推广部署，目前已经覆盖总行与分行、分行与分行、办公与业务、进出网管区、重要互联网DMZ区等区域的流量，该系统在内部红蓝对抗中多次成功发现入侵行为，也多次发现内部人员违规访问。



* 确认风险并对风险排续

“确认风险并对风险排续”负责对检测事件的分析确认，下图是我行的确认风险的主要流程。



在老的SOC1.0体系下，由于主要依赖黑白名单和简单的行为特征进行事件的确认，所以误报率很高，进而导致运维成本（每一单事件都需要闭环关闭，邮件、电话调查事件高频使用）非常也很高，久而久之会容易让运维人员麻痹，最后导致安全事件的漏报，“狼来了”现象始终困扰着总体的安全运维。

现在SOC2.0的建设中，在引入情报后，通过对IP、域名信誉、恶意进程MD5的引入，缓解了这部分压力，但是对于内部的异常行为分析的确认风险成本收效甚微，这一部分工作是SOC2.0需要解决的问题。

* 遏制事件

“遏制事件”主要负责事件的临时处置，包括网络层的临时阻断或者隔离系统，系统层的结束进程，应用层的升级优化，数据层的文件删除。这部分我们的建设目标是实现处置自动化---一键拒绝、一键结束、一键升级、一键删除，下面是我们目前的进展情况：

一键拒绝：通过防火墙自动化、ACL自动化实现、IPS黑名单自动化

一键结束：终端层面通过EDR实现，服务器层面还在探索中

一键升级：通过自动化发布平台建设，能够对应用程序一键升级，这方面随着我行规模的扩大，需求也越来越迫切。

一键删除：删除操作很简单，但是能够及时准确发现待删除的文件目前还无法实现自动化

1. 响应维度的建设情况

响应维度偏重对事件进行调查取证，并根据取证分析来设计处理类似事件的方法并及措施，并通过实施新安全措施以避免未来事件发生。

* 探究/入侵取证

溯源能力=专家团队+威胁情报（攻击者画像）+攻击路径确认



这部分核心工作就是对每一次攻击事件的攻击者、攻击路径、攻击技术以及内部防御弱点进行确认。首先这项工作由三线安全条线（购买外部专家服务进行补充）承担，所以这项工作对三线人员的技能要求非常高，必须精通攻防两方面知识；其次对攻击者的画像，主要依赖的于外部的威胁情报平台，但是就目前的现状，外部商业威胁情报平台还只能画出的“受控端”的画像，不能真正画出攻击者的画像，还需要依赖的一些“特殊资源”；最后就是对攻击路径确认，这个主要依赖SOC2.0的检测体系，同时辅助专家团队的经验技能。

在这个维度建设中，核心两个方面：人+数据，也就是360在最近两年倡导的“数据驱动安全”+“人是安全的尺度”。数据驱动安全考验的是我们的数据分析能力，过去在这方面我们尝试利用外部资源，效果不是很好，后来我们进行了策略调整，采取自里根生模式实现安全数据分析体系的建设，整个数据分析体系建设不追求“高大上”，一切以解决问题为出发点。下图是我们的数据分析体系：

|  |  |  |
| --- | --- | --- |
| 基于简单规则 | Excel、数据库、Splunk、ES | 查询即得 |
| 基于统计分析 | Excel、数据库、Splunk、ES | 统计+人工判断 |
| 基于机器学习 | ES、Splunk、数据库+机器学习算法库（Tensorflow） | 模型+专家判断 |
| 基于人工智能 | 期待中 | |

* 设计/模式更改

明确问题后，需要解决问题，在Gartner模型中，解决问题的维度只有“防御维度”，比如是关闭端口、更新签名库、更新系统配置、更改用户权限、更改用户培训。我们对这个模型进行了一定优化，增加了“检测维度”的各项控制点的优化，是更新各层次的检测点的覆盖度或者增加新维度检测点。

* 修复/更改

修改/更改主要负责策略的下发，主要涉及防火墙、WAF、IPS以及防病毒的自动化策略下发。我们行目前的进展，实现防火墙、IPS的一键拒绝，但是WAF的自动化还未涉及。

1. 预测维度的建设情况

通过防御、检测、响应结果不断优化基线系统；通过情报逐渐精准预测未知的、新型的攻击，主动锁定对现有系统和信息具有威胁的新型攻击，并对漏洞划定优先级和定位，并反馈到预防和检测功能，从而构成整个处理流程的闭环基准系统。

核心思想是：通过情报+数据分析去提前部署防御、检测控制点；通过情报+事件结果去优化基线系统。

* 基线系统

这部分内容主要是根据情报+事件结果不断优化各个维度的基线，具体覆盖范围和支撑系统中“策略标准”一致。

我行具体实践中，对基线的更改是一个非常谨慎的事情，通常技术验证测试，流程走完，再加上具体执行是一个非常漫长的过程，投入的成本也很高，如何兼顾效率和稳定对我们是一个很大的挑战，目前来说，能做到基线一年修改一次已经非常理想了。

* 预测攻击

在Garnter自适应安全架构里面，预测攻击被定义为对黑客市场的高度关注，主动收集相关性情报（比如金融类），然后提前进行针对性管控。

目前我行的具体实践情况，估计和其他银行类似，主要依赖监管通报、安全公司预警以及安全圈社交三个方面，这方面工作能够解决全局的一些风险事件（比如struts2、wanncry、匿名组织的威胁），但是无法应对只针对我行的APT攻击，这方面的工作我们还在探索中。

另外我们对预测攻击进一步思考，认为预测攻击不是强调提前知道对手发起攻击，而是当对手关注我们还未发起攻击时，我们提前知道及时布控。所以整个管控点落脚点还是在“情报”+“数据”。

* 主动风险分析

利用内外部收集的各种新情报，及时评估相关风险。

我们目前建立的主要风险分析场景包括：互联网攻击IP的分析、互联网流量中所有IP和情报关联分析、钓鱼网站检测和情报关联分析。

未来还会对服务器进程MD5和情报关联分析、每月针对业界主要风险事件进行分析（需要联系情报厂商和大的安全公司）

1. 自适应安全架构在实践中面临的挑战

自适应安全架构非常强调数据的分析能力，所以机器学习在安全数据分析的使用无疑成为一个非常热门的话题，但从我们的实践结果看，情况不是很乐观，可能还需要在算法和观念上有突破。结合我们实践，再综合各方观点：机器学习成功案例主要在大量重复性操作上，技术性较高的工作机器学习远远达不到标准，网络安全对事件的准确性要求很高，漏报误报都非常敏感。另外机器学习基本上发生在正常人正常行为上，而我们的对手是非正常人，行为也非正常行为，如何适应这种变化，还需要大家共同的智慧。

自适应安全架构中，不管是检测分析还是溯源都对网络流量的抓取有非常大的依赖，网络流量抓取有两种模式，一种是抓取五元组，一种是全流量，但是云化后，流量获取将是一个挑战。

自适应安全架构中，服务器端agent是一类非常重要的检测点，但本身稳定性和升级策略都直接影响到决策。

1. 总结

自适应安全框架是面向当前主要威胁风险的安全体系框架，以应对云大物移智时代所面临的安全形势。自适应安全框架从预测、防御、检测、响应四个维度，强调安全防护是一个持续处理的、循环的过程，细粒度、多角度、持续化的对安全威胁进行实时动态分析，自动适应不断变化的网络和威胁环境，并不断优化自身的安全防御机制。

金融组织在自适应安全框架建设中，有几点需要注意：一是和具体场景相结合，要清楚每个场景下，博弈对手是谁，从哪儿来，怎么来，来了后做什么，怎么做；二是要和组织的具体情况相结合，每个组织的组织架构不一样，策略不一样，阶段目标不一样，所以具体实现方法和运营手段都是有差异的，关键是如何在自己现有条件下有效运营最关键；三是整个数据分析建设需要投入大的资源，不追求高大上，一切从问题出发；四是金融行业的情报建设应该纳入到日程上来，开放、共享才是未来。