大数据分析在企业信息安全中的最佳实践

北京站/3.29

推动研发创新

提升产品品质

秉承优质服务

拓展伙伴关系

集团概况

- 创立于1996年，现有员工3600余人，其中海外员工288人
- 始终专注于医疗健康领域，为患者提供优质产品与服务

纳通

耳鼻喉科 | 颌面外科 | 齿科 | 运动医学 | **骨科** | 器械 | VSD | IVD | 第三方物流 | 医疗服务

研发 生产 销售 供应链 医疗服务

纳通医学科技研究院 IRENE 正天 威联德 世龙路得 德尔康尼 DCN Orthopaedic

杰西慧中 JXHZ BLBC 北京莱顿 金兴达 LINK INION AIVDE 艾威德 AIVDE MEDICAL 吉泰医疗

集团产业

- 纳通产品和服务已覆盖医用内植入物全产业链
- 聚焦骨科，不断拓展医用内植入物及周边领域
- 正天、金兴达商标被认定为天津市著名商标

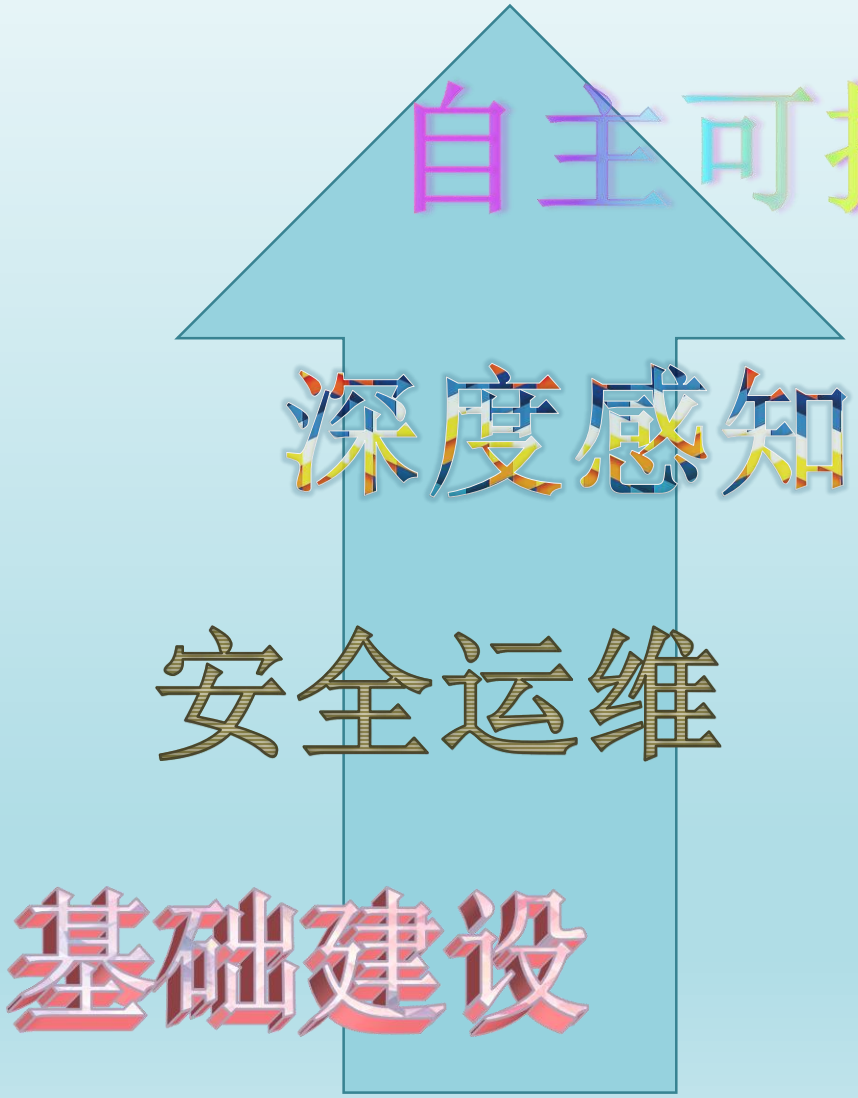
肖寒 信息安全经理

13年信息安全从业经历

CISP、PMP

主要负责企业的信息安全规划、建设与管理

1、企业信息安全发展规划



安全即服务

- 组建自有的专业安全服务职能团队，如：安全研究、安全合规、应急响应中心、研发安全防护产品等
- 安全深度合作，与各大安全平台、企业致力于安全研究与信息共享
- 安全服务对外输出

风险驱动

- 具备对未知威胁以及定向攻击防御手段，进一步提升安全防护水平
- 全面提升安全体系管理与审计工作的自动化能力

业务驱动

- 全面提升安全事件漏洞，问题主动发现能力
- 对信息安全体系文件进行可量化、可落地并贯彻执行

合规与事件驱动

- 建立纵深防御体系，具备一定的安全防护能力
- 建立信息安全制度体系，提供信息安全工作标准

2、数据安全，是企业发展的核心

数据安全保护与应用

访问控制

- ❖ **网络安全隔离**
- 不同业务数据的访问进行网络隔离
- 访问控制列表和安全组限制资源访问
- ❖ **帐号权限控制**
- 账号权限最小化（承担任务所需的最小权限）和权限分离（根据用户角色划分权限）

身份认证

- ❖ **运维安全与审计**
- 采用堡垒机进行运维安全授权与审计
- ❖ **账号密码安全策略**
- 密码复杂度、有效期
- 账号密码重置安全
- ❖ **双因子验证**
- 重要操作多种身份验证机制，如应用系统修改密码等进行短信验证码校验
- ❖ **接口认证**
- 跨信任网络且重要的业务接口进行身份认证、访问控制、加密传输

数据加密&脱敏

- ❖ **数据传输加密**
- 应用层采用SSL传输加密协议
- 重要信息数据采用加密算法进行加密传输
- ❖ **数据加密存储**
- 重要数据加密存储
- ❖ **秘钥保护**
- 使用加密机或密钥托管服务（KMS）管理用户主秘钥和数据秘钥
- ❖ **数据脱敏**
- 重要数据采用查询脱敏、导出脱敏

数据机密性保障

容灾备份/恢复

- ❖ **数据备份/容灾**
- 采用多副本存储策略
- 每天全备份、增量备份
- 实时多可用区、异地容灾
- 增量备份
- ❖ **数据恢复**
- 数据在任一副本出现故障时可快速迁移和恢复
- 系统故障时可迅速切换到正常服务器
- 定期开展数据恢复演练
- ❖ **重要服务器采用双机备份、网络出口双线路冗余**

持续服务能力保障

安全审计

- ❖ **日志审计**
- 收集主机、网络设备、数据库、应用系统日志进行分析
- ❖ **应用系统用户活动**
- 账号登陆、登出、修改密码等，登入后查询、导入、导出等
- ❖ **操作系统、数据库活动**
- 系统配置参数的修改
- 对业务的加载、卸载
- 账户的命令非查询操作
- ❖ **日志内容**
- 时间、用户ID、IP地址
- 事件类型、访问资源等
- ❖ **运维监控：硬盘、内存、CPU、网络等资源使用**

全面监控与溯源能力保障

全面防护

- ❖ **基础安全防护**
- 木马检测、暴力破解防护、漏洞扫描等基础防护功能
- 高防系统的DDoS防护
- ❖ **专业的技术能力**
- 代码安全审计
- 渗透测试
- 安全配置检查
- 应急保障、预警监控
- ❖ **完善的边界防护**
- 入侵监测与防御
- 恶意代码防护
- 网络防火墙
- 应用防火墙

全面安全防护

3、技术实现

3.1 访问控制

涉及数据相关的访问控制需要进行网络隔离、用户进行细粒度授权、访问进行认证，访问控制涉及对象包括操作系统、数据库、中间件、应用程序甚至网络设备等访问。

（一）**网络控制：**主要通过 ACL来实现，对源地址、目的地址、源端口、目的端口和协议的访问进行控制。

（二）**权限控制：**基于角色的权限访问控制。

PA-Traffic	
Receive Time	Time
Type	Drop / End
Form Zone	Zone 01
To Zone	Zone 02
Source	Src_ip
Source User	账号
Destination	Dest_ip
To Port	
Application	Dns / web-browsing / mysql /snmpv2
Action	Deny / Allow
Rule	Zone 01 to Zone 02
Session End Reason	
Bytes	

PA-Threat	
Receive Time	Time
Type	Drop / End
Name	威胁名称
Form Zone	Zone 01
To Zone	Zone 02
Attacker	Src_ip
Attacker Name	账号
Victim	Dest_ip
To Port	
Application	Dns / web-browsing / mysql /snmpv2
Action	Deny / Allow
Severity	Information High critical

3、技术实现

3.2 身份认证

（一）单点登录和双因素认证

1. 单点登录：在多个业务系统中，用户只需要登录一次就可以访问所有相互信任的业务系统。使用单点登录，在带来便利的同时也会引入新的安全风险：用户仿冒和单点故障。
2. 双因素身份认证：解决只有授权用户才能访问系统平台与服务的问题，主流的身份认证手段包括：静态密码、动态口令、密码技术或生物技术等。

PA-VPN	
Time	
src_ip	源IP
user	用户
Private IP	转换后IP
Client OS version	
Device name	
event_id	globalprotectgateway-config-succ globalprotectgateway-auth-succ globalprotectportal-auth-fail globalprotectgateway-auth-fail

ISE	
Time	
Device IP Address	
UserName	用户
NAS-IP-Address	
Called-Station-ID	链接的哪个
Calling-Station_ID	MAC
NAS-Identifier	
action	Success failure

DB日志	
Id	
Time	时间
IP	源IP
UserName	用户
Operatetype	Login Update Down Built delete
Operate	Success fail
information	Password error Username error Locking Username unknown ……

3、技术实现

3.3 数据加密&脱敏

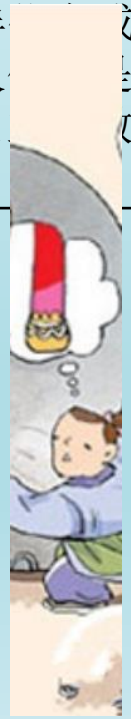
（一）数据加密

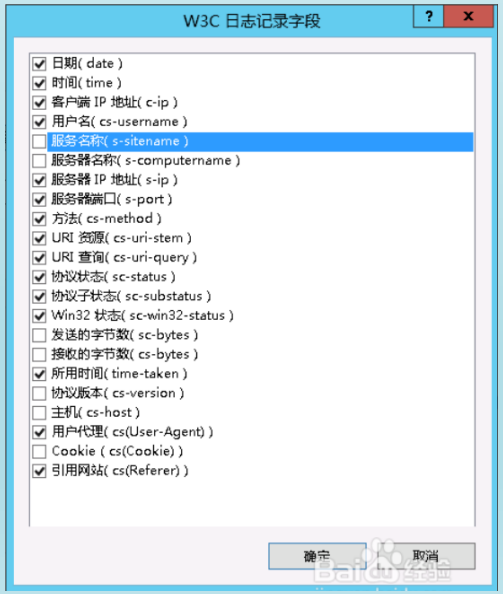
内容加密：通常采用对称加密算法，数据库中常用的加密算法AES或MD5+盐；

传输通道加密：通常采用非对称加密算法，如：SSL加密数据通道采用RSA（非对称加密）、VPN采用RSA、SSH key采用RSA。

（二）数据脱敏

企业拥有的敏感数据，包括商业秘密、知识产权、关键业务信息、业务合作伙伴[illegible]户信息等。其中涉及个人隐私的用户个人[illegible]信息系统中最重要最广泛的敏感信息。（[illegible]据与操作数据、登陆数据分离）





数据库审计日志
用户
源IP地址
数据库对象（数据库用户、表、字段）
操作时间
SQL操作命令
返回的记录数或受影响的行数
关联表数量
SQL执行结果
SQL执行时长
报文内容
告警信息

3、技术实现

3.4 全面防护
（一）基础安全防护
终端安全（杀毒）
应用安全（WAF）
垃圾邮件（反垃圾邮件）
运维监控分析（zabbix、solarwinds等）

WAF日志
TIME
alertType=特征码
alertName=HTTP 特征码违规
severity=高
act=阻止
Dst_ip
Src_ip
User
Policy
Description

反垃圾邮件日志
Time
发件人
收件人
主题
状态：quarantined spam virus

病毒日志
timestamp
AutoID
signature
threat_type
file_name
vendor_action
user
dest_nt_host
os
process

3、技术实现

3.5 安全审计：分类、分组

什么	已经完成哪些活动
为什么	为什么必须执行这些活动
谁	谁执行活动
哪里	在哪里执行这些活动
何时	何时和频率
如何	如何，根据哪些程序，信息和文件

IT运维分析师

SOC管理者

站点可靠性工程师

电子商务业务分析师

制造工程师

信息安全管理

4、产品选型

SIEM

安全需求

能支持多种数据类型

运维能获取的数据很多，包括机器数据、系统数据、应用服务器数据和数据库数据。

稳定、性能高

要能提供稳定的运营能力，整体架构要简单，技术人员能快速上手，计算速度快，扩容简单。

使用简单方便

技术人员使用、维护成本低，能快速上手。

ELK方案是我们最早选型的方案，但当时我们内部技术团队技术储备有限，也没有更多的人员编制来扩充，自己建立、掌握这个平台的时间周期较长。

具备ELK平台的优势特性，产品成型，有技术支持，价格便宜，但技术短板也同样存在，比如需要提前标记字段，报表自助定制需要开发，实时调取数据需要刷新整个页面等。

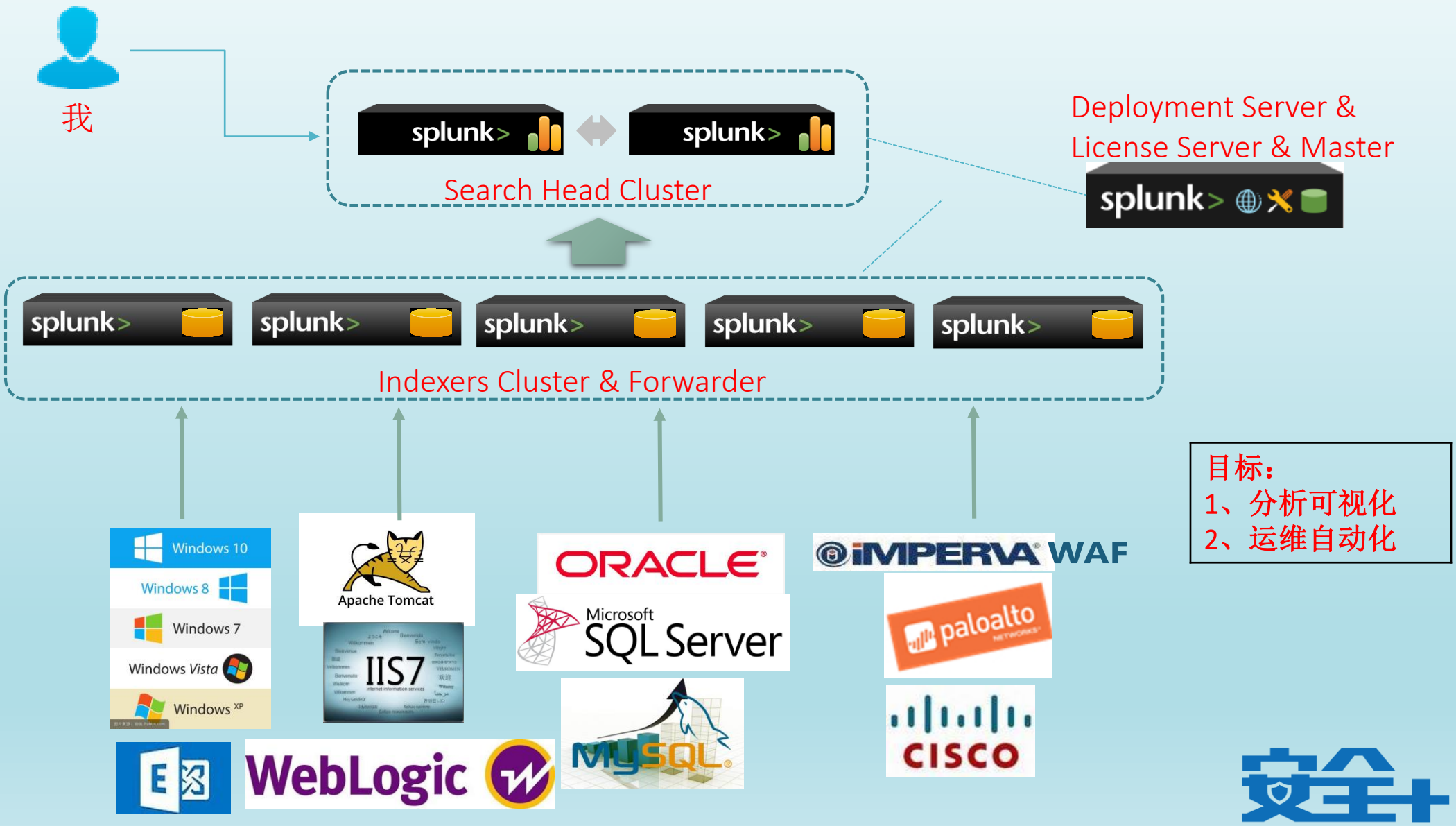
Splunk具备很多成功的APP工具，对商业化软件使用较多的企业，很容易创建易用的报表。实时报表太过酷炫。对输入数据比较随意。

ELK

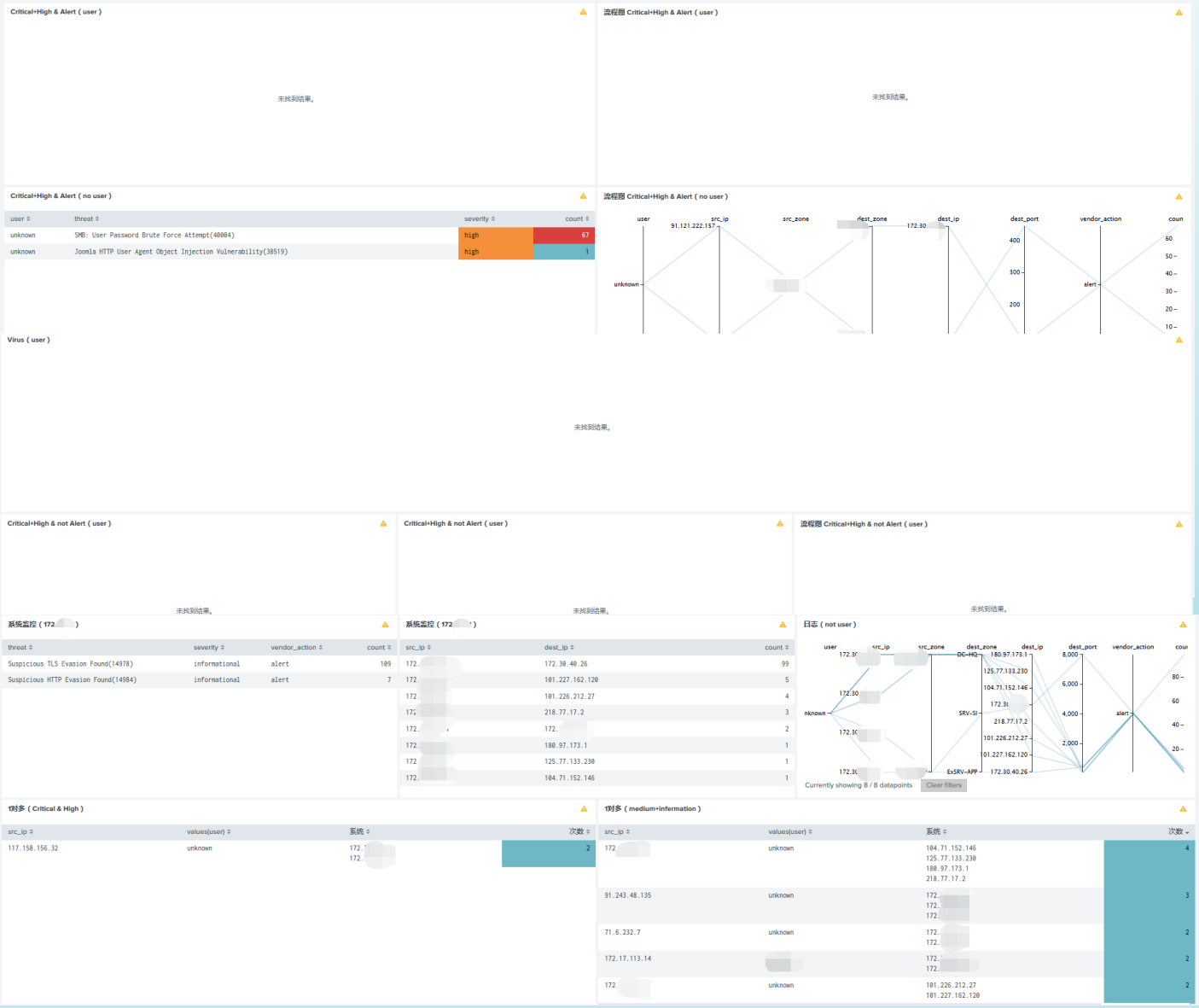
基于开源平台的创业公司产品

Splunk

5、架构部署


我
splunk>
splunk>
Search Head Cluster
Deployment Server &
License Server & Master
splunk>
splunk>
splunk>
splunk>
splunk>
splunk>
Indexers Cluster & Forwarder
Windows 10
Windows 8
Windows 7
Windows Vista
Windows XP
Apache Tomcat
IIS7
ORACLE
Microsoft
SQL Server
MySQL
iMPERVA WAF
paloalto
CISCO
WebLogic
目标：
1、分析可视化
2、运维自动化

6、模型案例分析-安全防护模型



主要日志来源：（FW、IPS、WAF）

难点：

1、多认证日志组合；

2、通过唯一参数串联各类日志（user、IP）

价值：

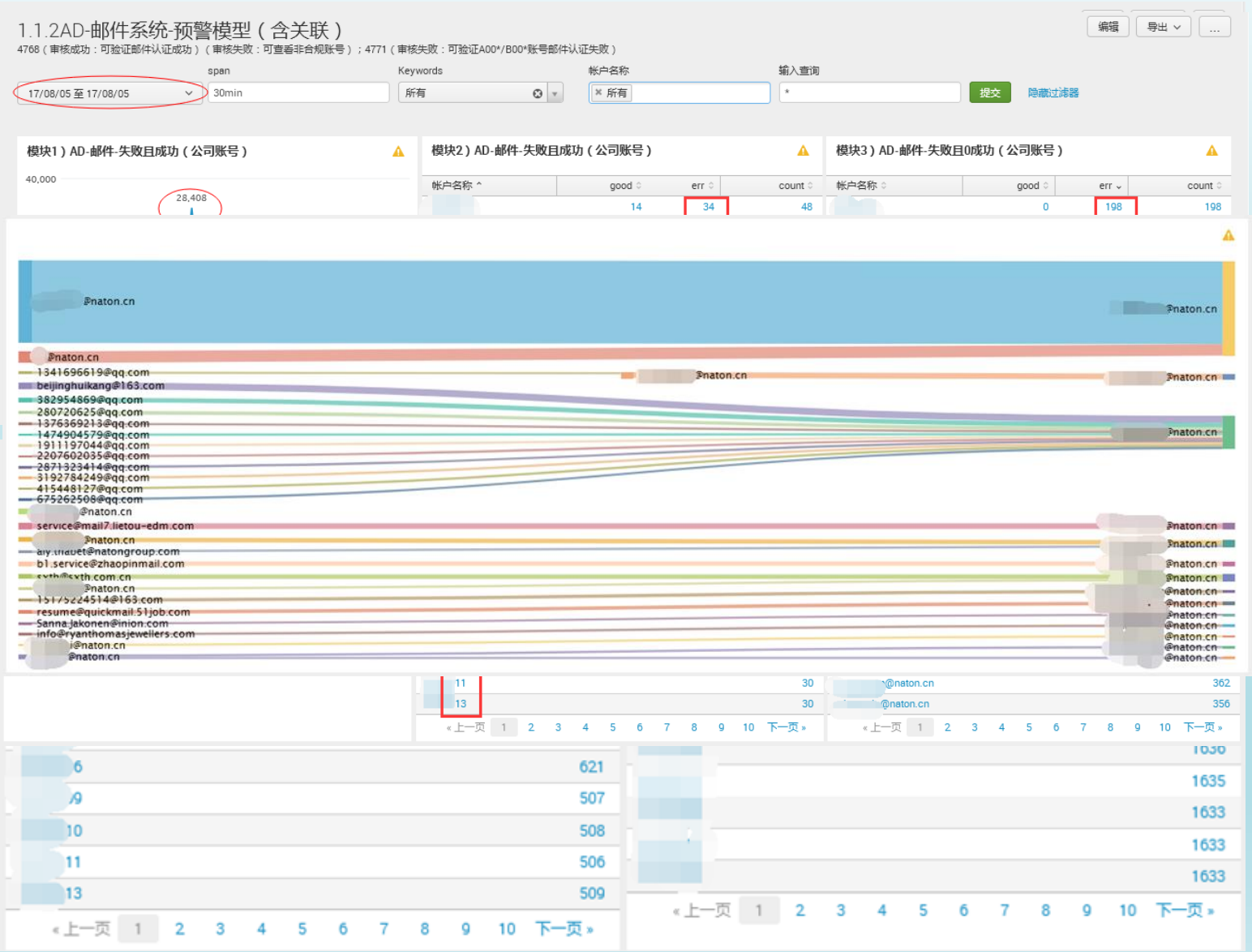
1、快速发现——威胁事件；

2、联动防火墙——自动更新封堵策略；（企业性质）

3、联动防火墙——自动封堵攻击IP；（企业性质）

4、联动威胁情报

6、模型案例分析-邮件安全模型



主要日志来源：（邮件、AD、反垃圾邮件）

难点：

1、多认证日志组合；

2、通过唯一参数串联各类日志（user、IP）

价值：

1、快速发现——威胁事件；

2、联动防火墙——自动更新封堵策略；（企业性质）

3、联动防火墙——自动封堵攻击IP；（企业性质）

4、联动威胁情报

6、模型案例分析-终端安全模型

"挖矿"病毒 加域用户 TOP10

正在等待数据...

"挖矿"病毒 非加域用户 TOP10

dest_nt_host	file_name	src_ip	detected_timestamp	count
admin	C:\windows\appdiagnostics\svchost.exe	172	2019-01-02 09:31:18.0	1
admin	C:\Windows\AppDiagnostics\svchost.exe	172.	2019-01-10 06:48:57.0	1
admin	C:\Windows\AppDiagnostics\svchost.exe	172.	2019-01-08 10:59:54.0	1
admin	C:\Windows\AppDiagnostics\svchost.exe	172.	2019-01-08 10:21:21.0	1
admin	C:\Windows\AppDiagnostics\svchost.exe	172.	2019-01-08 08:21:37.0	1
admin	C:\Windows\AppDiagnostics\svchost.exe	172.	2019-01-08 04:11:18.0	1
admin	C:\Windows\AppDiagnostics\svchost.exe	172.	2019-01-08 02:11:07.0	1
admin	C:\Windows\AppDiagnostics\svchost.exe	172.	2019-01-08 00:11:56.0	1
admin	C:\Windows\AppDiagnostics\svchost.exe	172	2019-01-07 10:00:04.0	1
admin	C:\Windows\AppDiagnostics\svchost.exe	172.	2019-01-03 09:16:38.0	1

病毒事件（ Critical or High ） TOP10 域用户 未删除

病毒事件（ Critical or High ） TOP10 非域用户 未删除

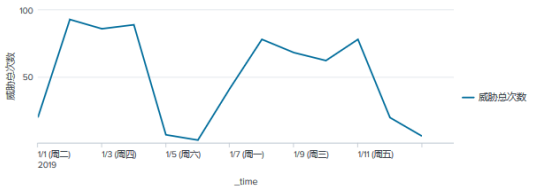
病毒事件（ Critical or High ） TOP10 域用户 已删除

dest_nt_host	file_name	event_description	count	DEPTNAME	F_EMPNAME	F_JOBNAME
	HKLM\SOFTWARE\CLASSES\WOW6432NODE\CLSID\{B164E929-A1B6-4A06-B104-2CD0E90A88FF}\	检测到并阻止了访问保护规则违规	37			
	HKLM\SOFTWARE\CLASSES\CLSID\{B164E929-A1B6-4A06-B104-2CD0E90A88FF}\	检测到并阻止了访问保护规则违规	3			
	C:\users\ .appdata\roaming\snda\sdupdate\sddupdatesvc.dll	找到感染文件	10			
	HKLM\SOFTWARE\CLASSES\WOW6432NODE\CLSID\{B164E929-A1B6-4A06-B104-2CD0E90A88FF}\INPROCSERVER32\	检测到并阻止了访问保护规则违规	10			
	HKLM\SOFTWARE\CLASSES\WOW6432NODE\CLSID\{0EBBBE48-BAD4-4B4C-8E5A-516ABECAE064}\INPROCSERVER32\	检测到并阻止了访问保护规则违规	10			
	HKLM\SOFTWARE\CLASSES\PROTOCOLS\HANDLER\SACORE\	检测到并阻止了访问保护规则违规	10			
	HKLM\SOFTWARE\CLASSES\PROTOCOLS\HANDLER\DSSREQUEST\	检测到并阻止了访问保护规则违规	10			
	HKLM\SOFTWARE\CLASSES\CLSID\{B164E929-A1B6-4A06-B104-2CD0E90A88FF}\INPROCSERVER32\	检测到并阻止了访问保护规则违规	10			
	HKLM\SOFTWARE\CLASSES\CLSID\{0EBBBE48-BAD4-4B4C-8E5A-516ABECAE064}\INPROCSERVER32\	检测到并阻止了访问保护规则违规	10			
	C:\PROGRAM FILES (X86)\ADOBE\READER 10.0\READER\ACRORD32.EXE	尝试并阻止了漏洞利用	6			

病毒事件（ Critical or High ） TOP10 非域用户 已删除

dest_nt_host	file_name	event_description	src_ip	count
BF-20180629YAAA	HKLM\SOFTWARE\CLASSES\WOW6432NODE\CLSID\{B164E929-A1B6-4A06-B104-2CD0E90A88FF}\	检测到并阻止了访问保护规则违规	10.	19
BF-20180629YAAA	HKLM\SOFTWARE\CLASSES\CLSID\{B164E929-A1B6-4A06-B104-2CD0E90A88FF}\	检测到并阻止了访问保护规则违规	10.	19
admin	C:\Windows\AppDiagnostics\svchost.exe	已感染文件已删除	172	8
admin	C:\Windows\AppDiagnostics\svchost.exe	已感染文件已删除	172.	7
admin	C:\windows\system32\snmpstorsrv.dll	找到感染文件	172.	3
NATON-20171116W	C:\PROGRAM FILES (X86)\ADOBE\READER 10.0\READER\ACRORD32.EXE	尝试并阻止了漏洞利用	172.	3
DESKTOP-QI7I2PO	HKLM\SOFTWARE\CLASSES\WOW6432NODE\CLSID\{B164E929-A1B6-4A06-B104-2CD0E90A88FF}\INPROCSERVER32\	检测到并阻止了访问保护规则违规	10.	3
DESKTOP-QI7I2PO	HKLM\SOFTWARE\CLASSES\WOW6432NODE\CLSID\{0EBBBE48-BAD4-4B4C-8E5A-516ABECAE064}\INPROCSERVER32\	检测到并阻止了访问保护规则违规	10.	3
admin	C:\windows\system32\snmpstorsrv.dll	找到感染文件	172.	2
admin	C:\Windows\AppDiagnostics\spoolsv.exe	找到感染文件	172	2

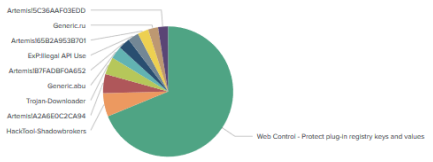
终端杀毒威胁事件总数趋势



威胁分类 TOP 用户 10

dest_nt_host	count
admin	86
	78
	62
	46
BF-20180629YAAA	40
DESKTOP-QI7I2PO	32
	25
171116W	18
	18
	17

威胁分类 TOP 10



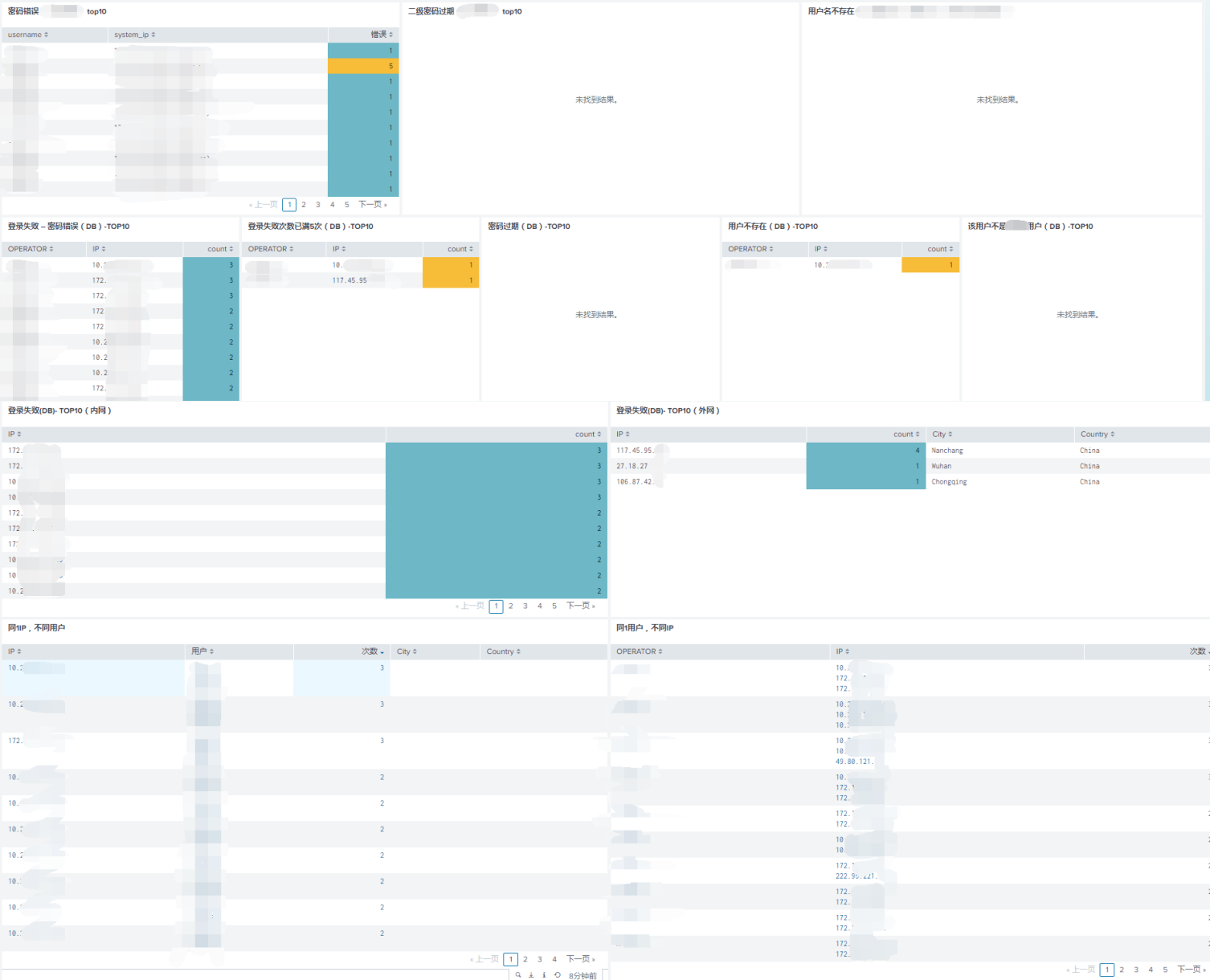
主要日志来源：（杀毒软件）

价值：

1、快速定位——挖矿病毒；

2、全面了解——终端安全病毒情况；

6、模型案例分析-业务安全模型



主要日志来源：（业务系统DB日志）

前提：日志完整、数据清洗。（NO）

如果模糊或者代理模式：

DB + 中间件日志 + 认证日志 + OA信息 + WAF（拆解包）+FW

难点：

1、多认证日志组合；

2、通过唯一参数串联各类日志（user、IP）

价值：

1、快速发现——暴力破解事件；

2、快速定位——异地登陆；（多点登录）

3、快速推动——账号解锁；

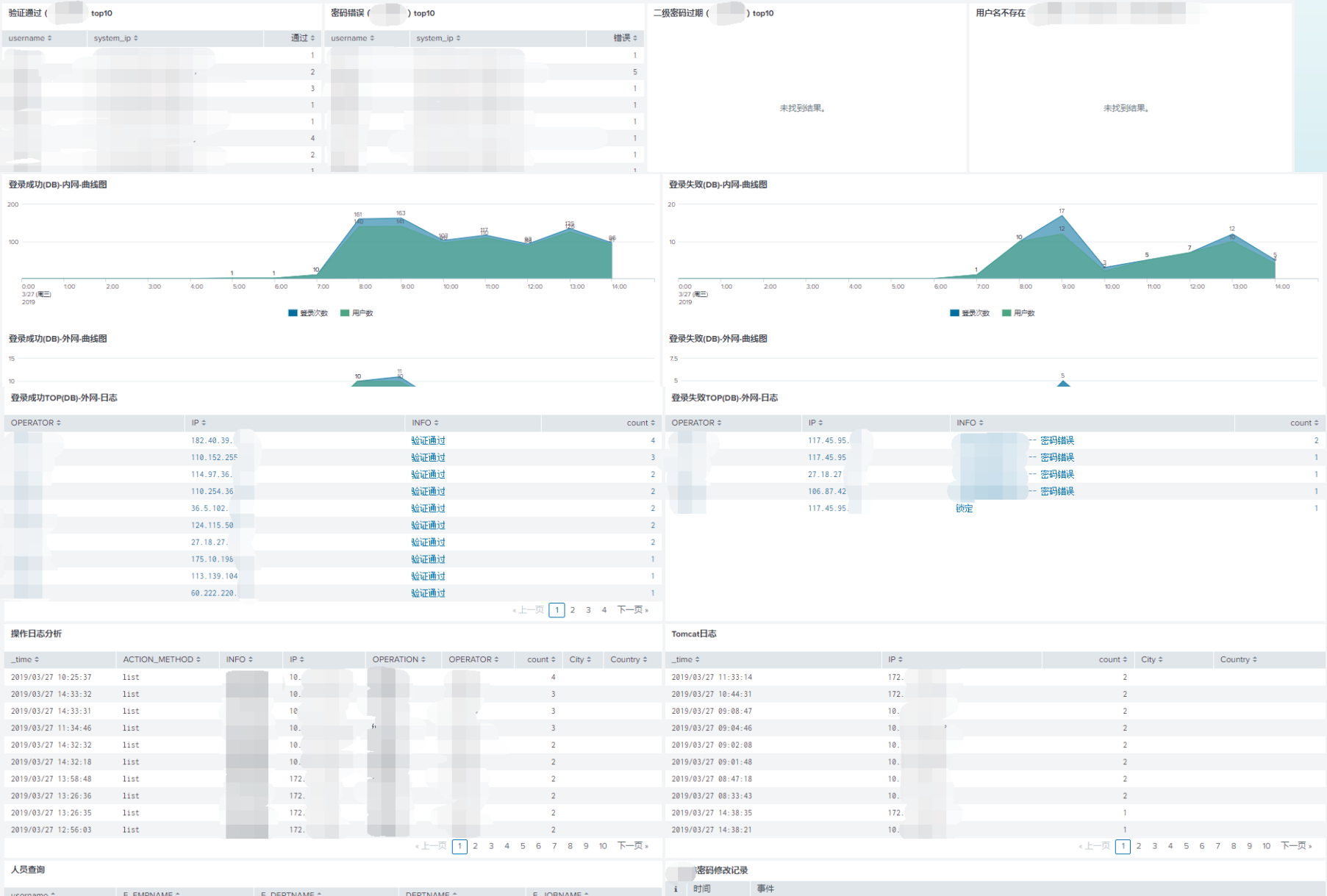
4、联动防火墙——封堵攻击IP；

附赠价值：

1、进行系统登录的代码层校验（丰富安全评估手段）

2、推动统一验证系统的企业落地

6、模型案例分析-业务安全模型



价值：

1、快速定位具体事件；

2、安全取证；

7、迎接新的挑战

Software-defined Network（软件定义网络）

为了加快企业IT服务，企业正在逐步将数据中心转变为一个可计算、可存储的联网资
这就叫做软件定义数据中心（SDDC）。SDDC的主要目标就是实现敏捷性，在不同网
架构的云中，让IT服务运行、扩展地更快、更透明。

第一阶段，保护软件定义数据中心（Software-defined DataCenter）

对企业来说，转变为SDDC的第一步就是开发软件定义网络（SDN）。SDN可以利用基
拟网络控制器），以及新的网络协议（如VXLAN）；还能保护可编程基础架构的APIs
但由于SDN无法保证L3-L7的信息安全服务，如恶意软件检测、应用控制、应用防火墙
信息安全服务能够精确地集成、交互和理解SDN。

第二阶段，集成软件定义基础设施（Software-defined Infrastructure）

信息安全控制措施必须意识到周边基础设施的变化。这些基础设施的核心是：信息安
户和群组应该可以链接到（或不能链接到）某种应用软件。否则，软件定义基础设施

由于每个SDN组都有自己的逻辑网络，在L3用路由或防火墙进行分段的做法已经落伍
网映射、制定数据包格式。这会影响安全控制措施的部署、威胁基础分段和传统安全

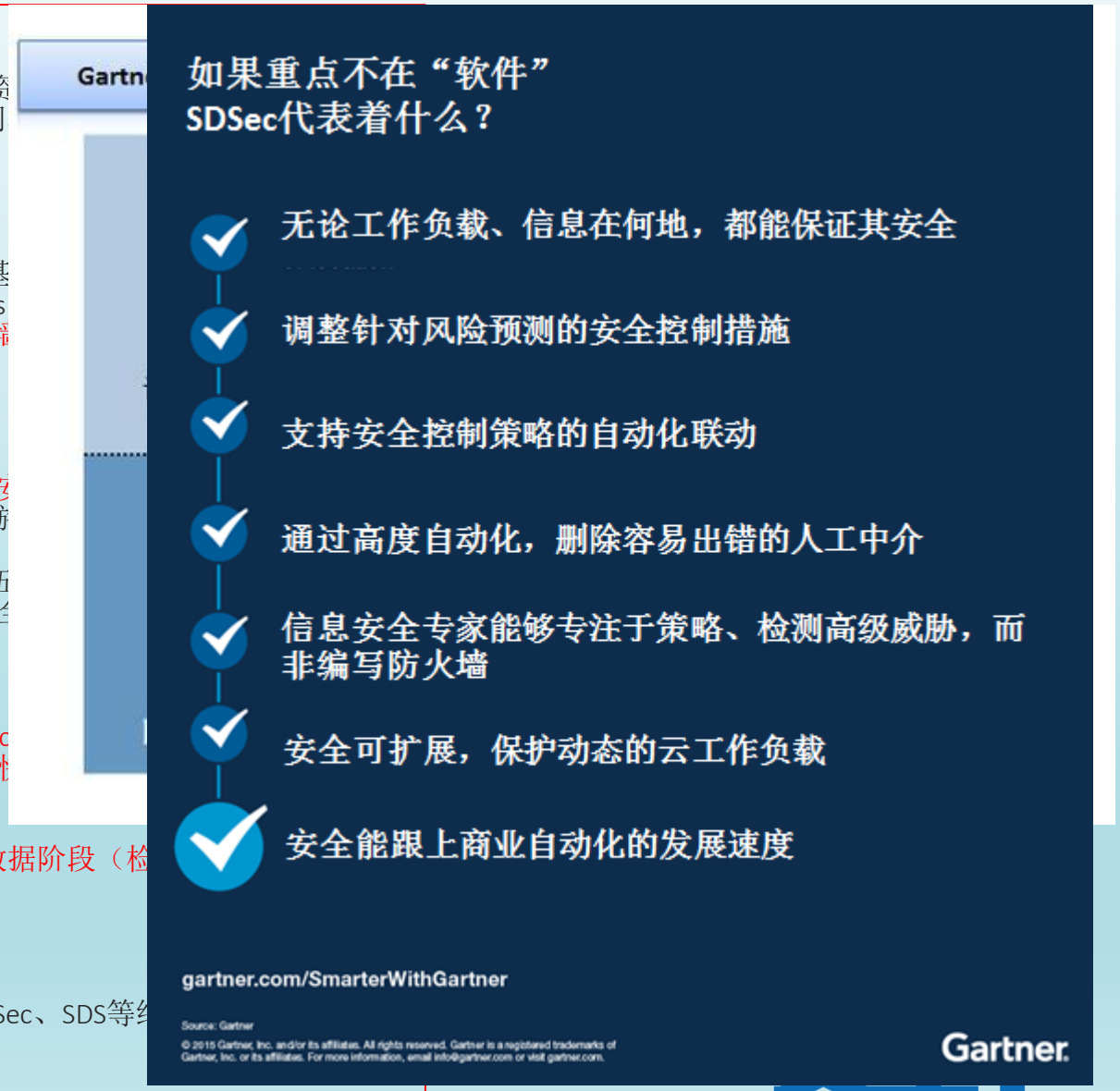
第三阶段，开发软件定义安全（Software-defined Security）

Gartner认为安全和数据中心基础架构一样，需要由软件定义。软件定义安全（SDSec
在本地还是公有云上运行，都能不断防御新型威胁、保证软件控制措施自动到位、
规要求。

但同时，我们应该看到硬件在软件定义安全（SDSec）中仍然发挥着作用，如安全数据阶段（检
仍然得益于硬件的处理能力。

小结：

软件定义一切是2014年Gartner提出的趋势之一，但到今年，已经具体到了SDN、SDSec、SDS等
60%的企业私有云部署中，信息安全控制将实现自动化。



谢谢！