

安世加

"Face the challenge, Embrace the best practice"

EISS-2020 企业信息安全峰会 之上海站

2020年11月27日





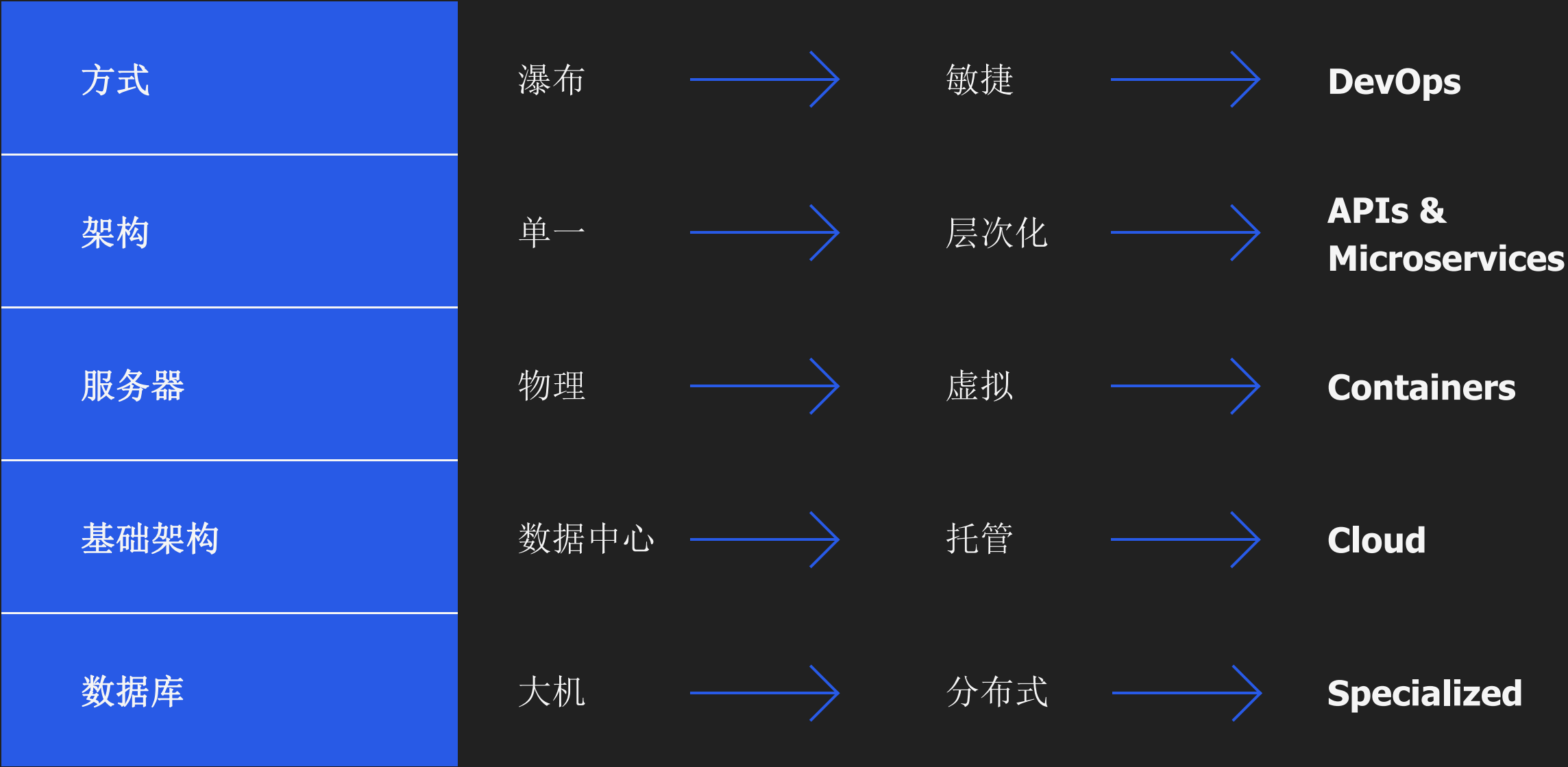
imperva

现代数据库环境下的 安全思考

刘沛旻

Imperva中国区技术经理

现代企业环境的变化



66%

上云最大的顾虑是数据安全问题，之后才是计算资源的功能和数据可视等方面¹

41%

最大的数据库安全风险还是来自于内部特权用户的操作和访问²

11%

很少的人认为DBaaS可以提供足够完善的安全措施和手段²

84%

大多数管理者关注数据安全方案能给他们带来多少价值，而不仅仅是数据可视²

1.Reproduced from CloudTech Report: *Why more than three quarters of enterprise workloads will be in the cloud by 2020* (L. Columbus)

2. Imperva sponsored research - AWS Re:Inforce 2019 (n=142)

传统数据库安全建设



现代数据库环境下的挑战

安全覆盖

针对 **DBaaS** 环境
针对定制化数据库平台
针对混合部署环境

价值

输出有价值的报告、
视图、分析

成本

管理和运维成本
其他资源成本

合规高要求

超大数据检索、查询、存储
信息补充

如何覆盖更多现代数据库安全需求

覆盖更多的现代数据库形态

流量分析的方法可能无法覆盖所有现代数据形态，利用原生日志来做补充

DBaaS的全面覆盖

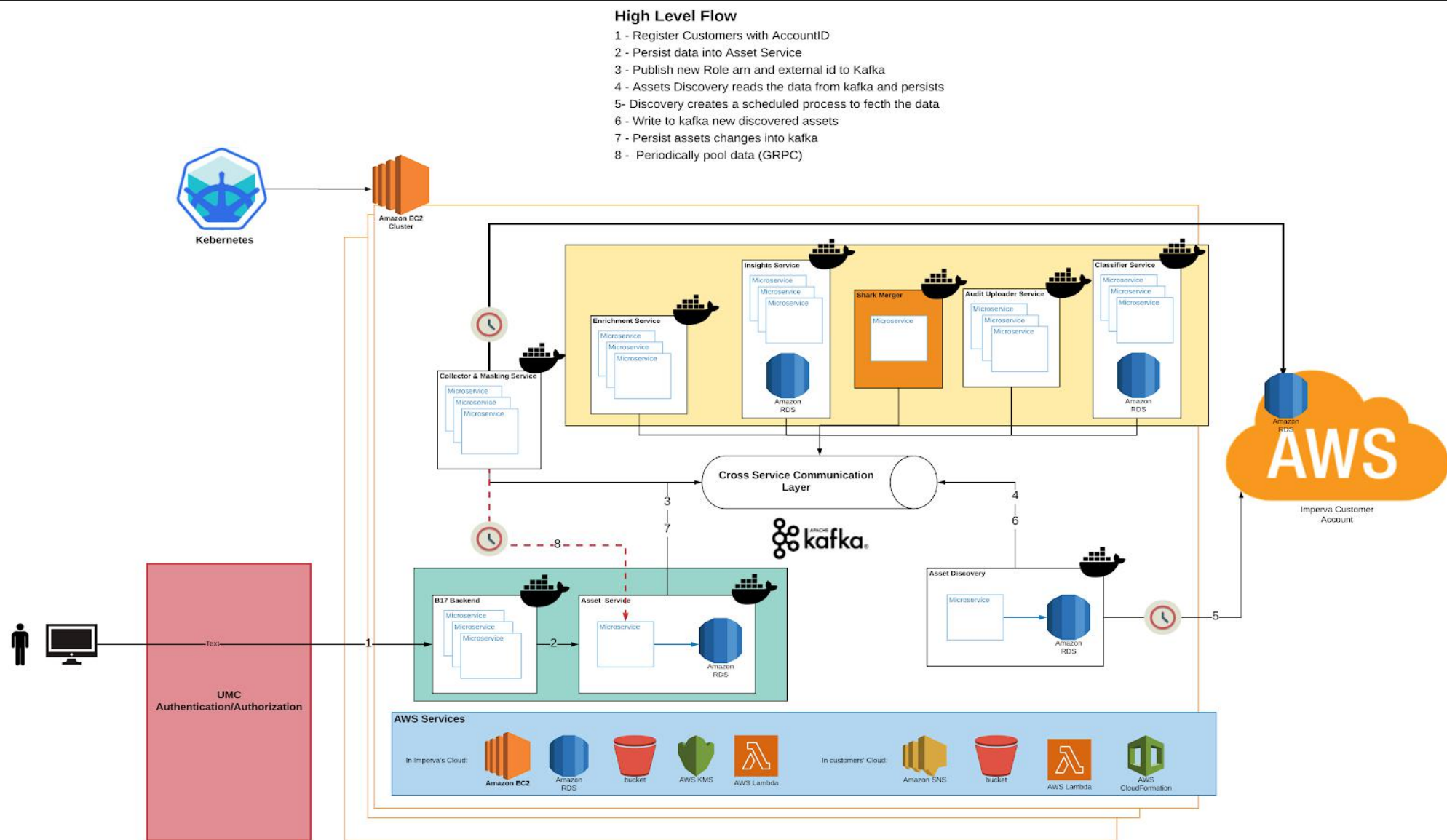
云端的数据安全是未来的焦点，新手段和新技术的涌现

补充完整信息

CMDB、VA、IAM等相关信息的补全



Cloud Database Security 创新技术



如何进行超大数据的存储和检索

Table			
	Country	Product	Sales
Row 1	India	Chocolate	1000
Row 2	India	Ice-cream	2000
Row 3	Germany	Chocolate	4000
Row 4	US	Noodle	500

Row Store	
Row 1	India Chocolate 1000
Row 2	India Ice-cream 2000
Row 3	Germany Chocolate 4000
Row 4	US Noodle 500

Column Store	
Country	India India Germany US
Product	Chocolate Ice-cream Chocolate Noodle
Sales	1000 2000 4000 500

Row-based				
Row ID	Date/ Time	Material	Customer Name	Quantity
1	845	2	3	1
2	851	5	2	2
3	872	4	4	1
4	878	1	5	2
5	888	2	3	3
6	895	3	4	1
7	901	4	1	1

Column-based				
Row ID	Date/ Time	Material	Customer Name	Quantity
1	845	2	3	1
2	851	5	2	2
3	872	4	4	1
4	878	1	5	2
5	888	2	3	3
6	895	3	4	1
7	901	4	1	1

行存储 vs 列存储

怎样让安全数据有价值和降低成本？

提供风险分析智能

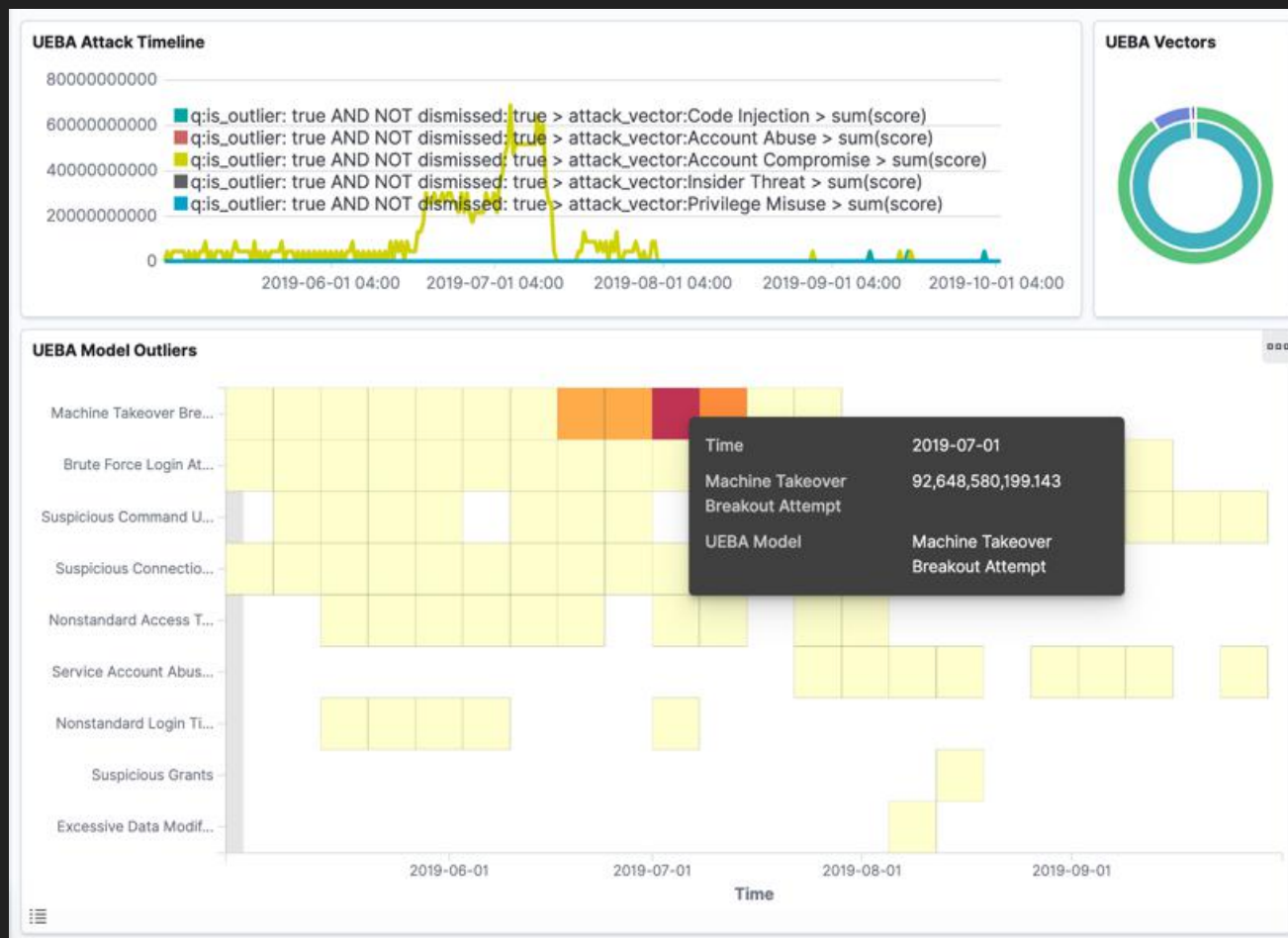
利用无监督学习的**UEBA**机制，
将原始的审计数据变成有价值的
风险分析信息

安全数据服务化

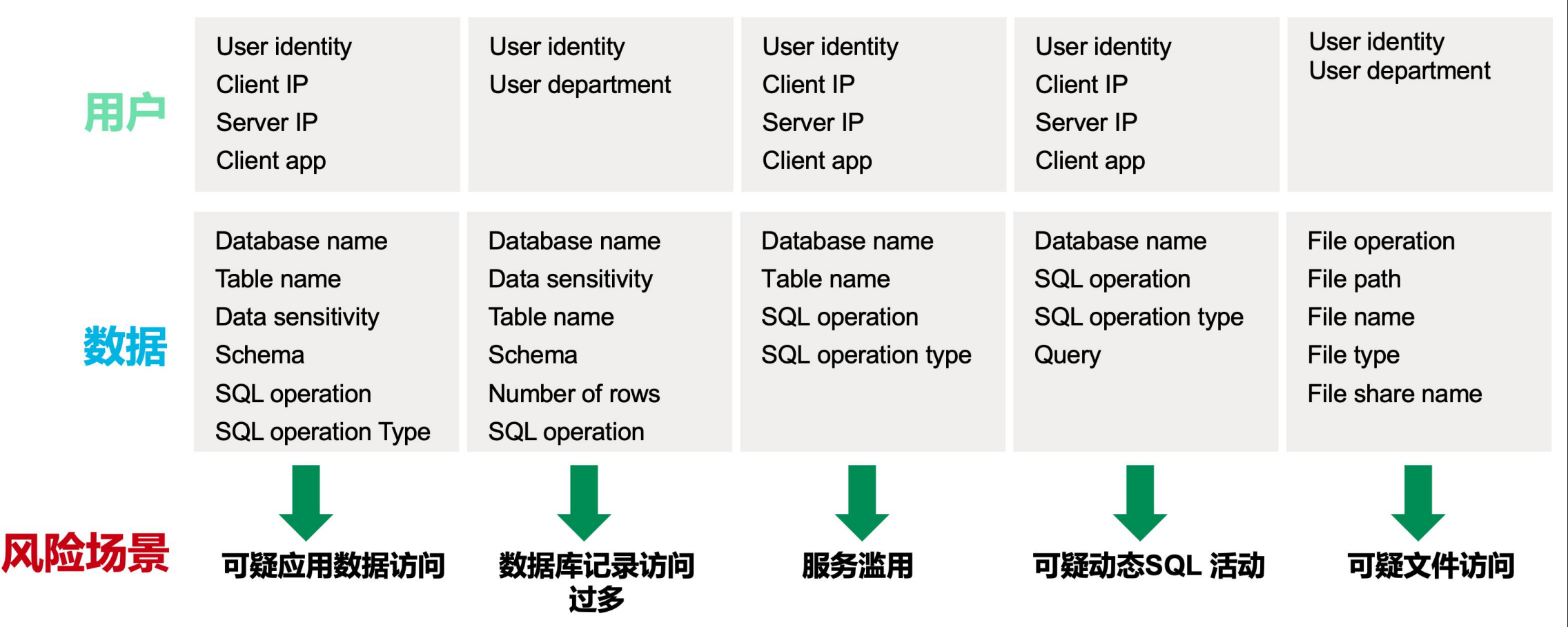
为各种团队提供安全数据服务，
提供全面、完整和统一的数据
库安全相关的数据

自动化编排和响应

除了数据存储和处理成本之外，
安全运维成本是巨大的开销，
自动化运维势在必行



针对数据安全的UEBA



让安全数据服务化

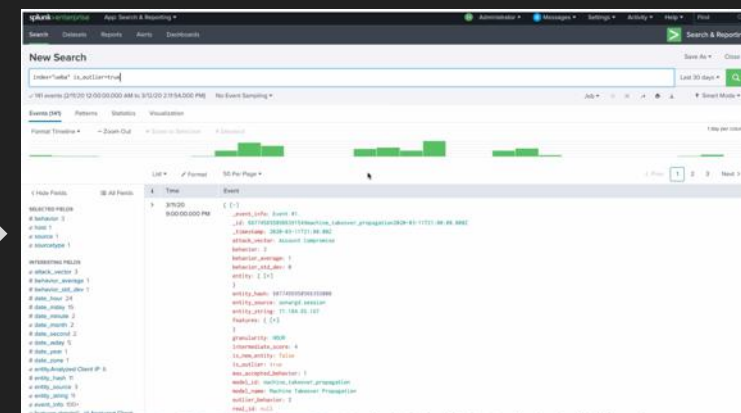
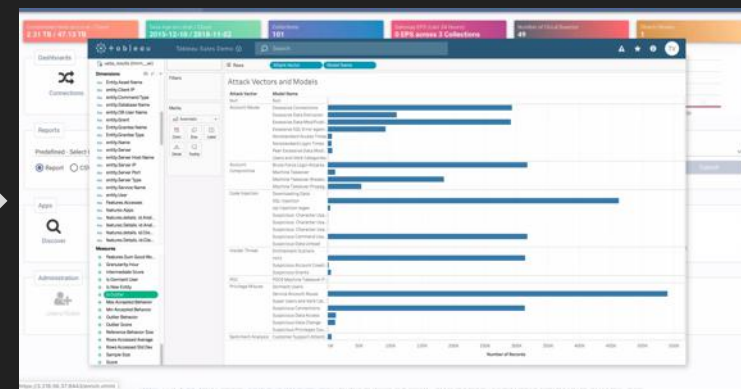
Any Team, Any Tool

SOC	Splunk
Audit	BI Tools
Data Scientist	R, SciKit
DBA	SQL
Forensi	Kibana

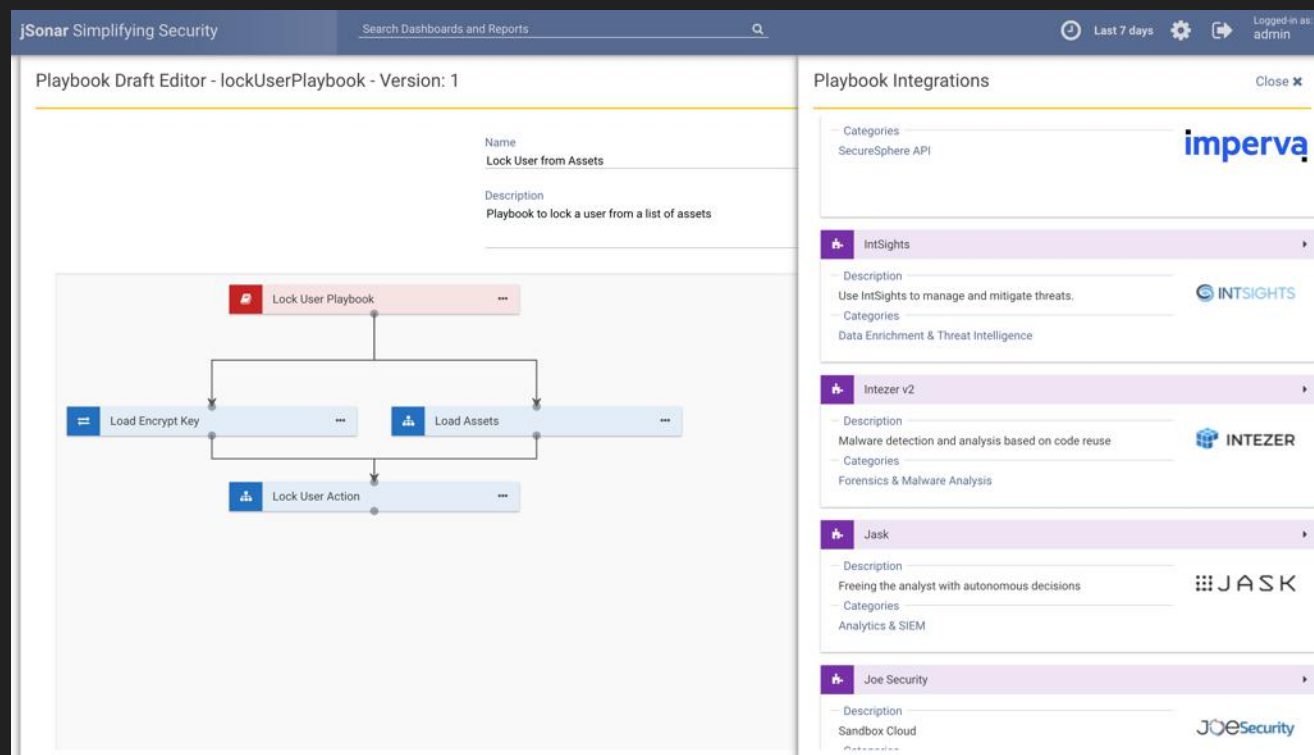
Role-based
Access
Control

Audit via
Tableau

SOC via
Splunk



数据库安全自动化编排和响应



数据库安全SOAR

建立以数据库为中心的自动化和响应平台

- 基于UEBA的分析结果来进行下一步的行动
- 避免大量的重复数据处理工作
- 定制数据安全Playbook

数据库安全中台？



统一数据接口
避免“重复造轮子”



获取数据效率低、质量差
避免“烟囱式立项”



挖掘数据的价值
数据服务化



数据拥有成本
增长过快



企业级数据库安全服务平台

现代企业数据库安全智能平台

数据展现

交互式数据探索	统一企业视图	数据处理流程自动化
多年数据保存	自助报告	SOC优化

数据智能

统一数据模型	数据富集与关联	数据风险分析	可扩展UEBA	数据SOAR
--------	---------	--------	---------	--------

通用采集

数据采集

扫描结果

发现	漏洞评估
分类	用户权限管理

活动监测源

代理监控	无代理监控
云	DAM解决方案

其他数据源

上下文元数据 (IAM、变更控制、CMDB等等)
任何工具 (Qualys、Tenable、Varonis等等)

Imperva 全球公认领先的应用数据安全及云安全供应商，提供世界一流的数据、应用、API、云端安全解决方案。公司成立于2002年，总部位于美国加州红木海岸，在全球100多个国家拥有超过6000+直接客户和超过550+合作伙伴。



安世加