ISC 2019 7th
第七届互联网安全大会

机器学习在云安全中的实践

孙志敏

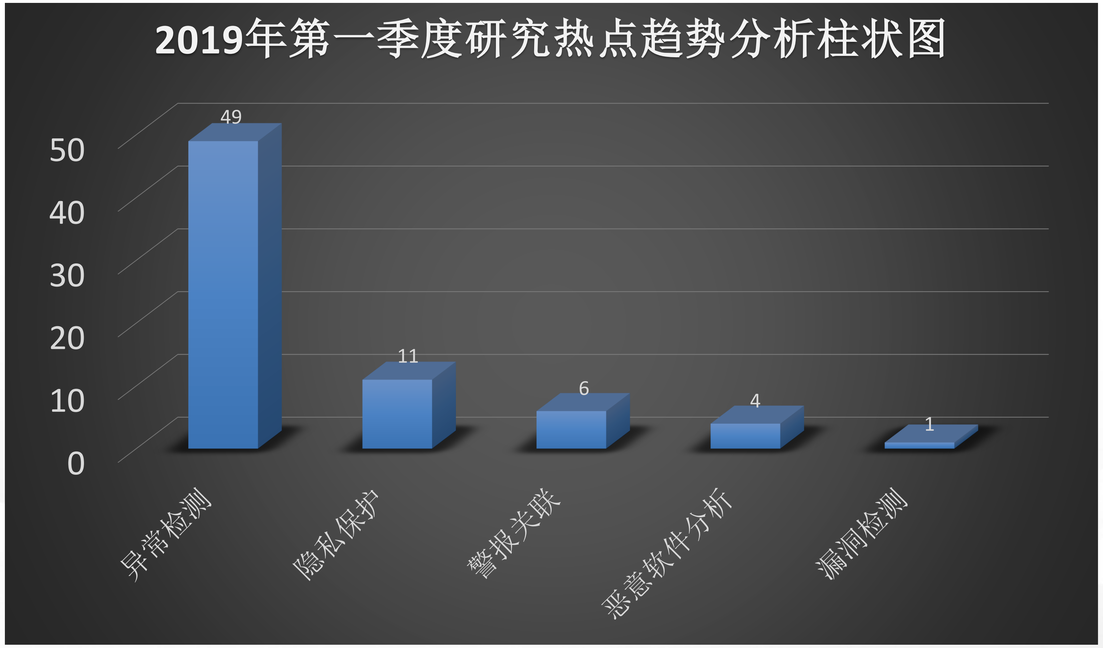
ISC 2019 第七届互联网安全大会

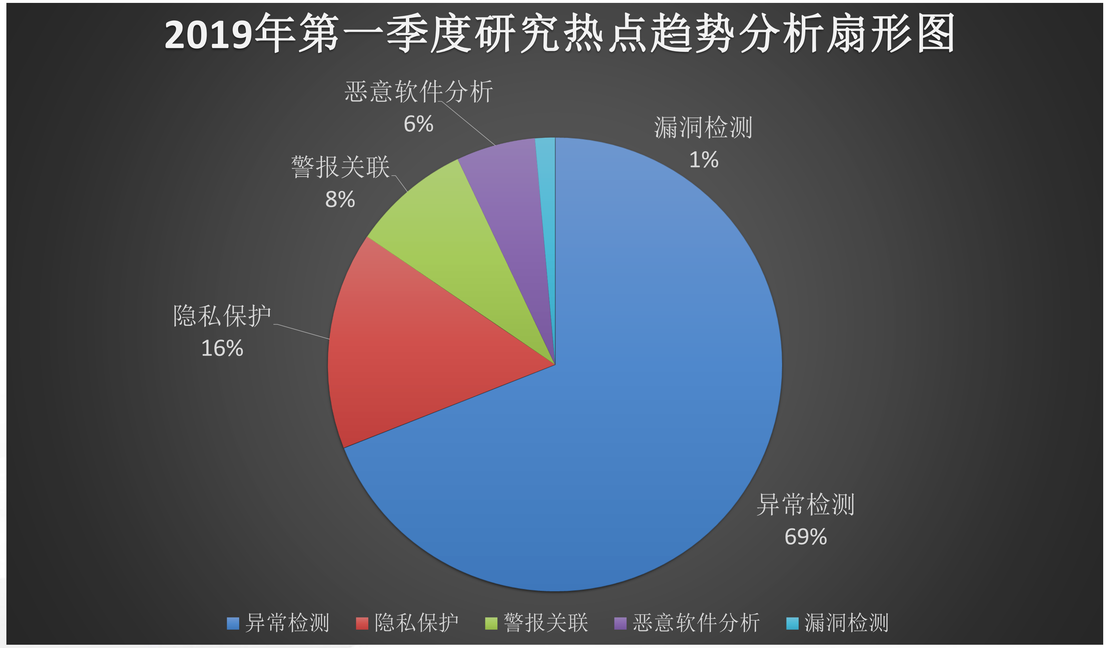
目录

- 源起
- 敏感数据发现
- 恶意软件发现
- 入侵行为发现

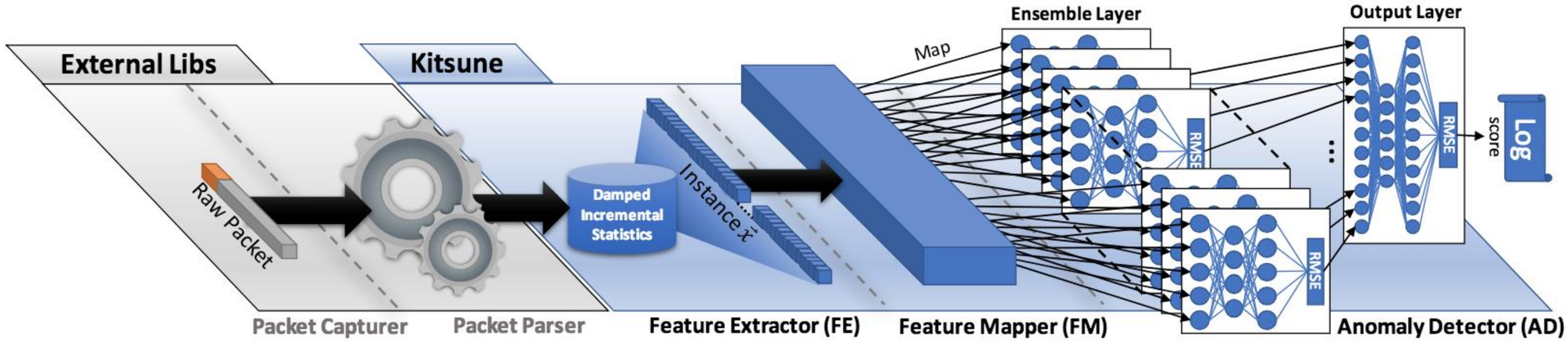
源起

- 安全由代码驱动走向数据驱动
- 传统的正则表达式遇到越来越多的挑战
- 机器学习的兴起





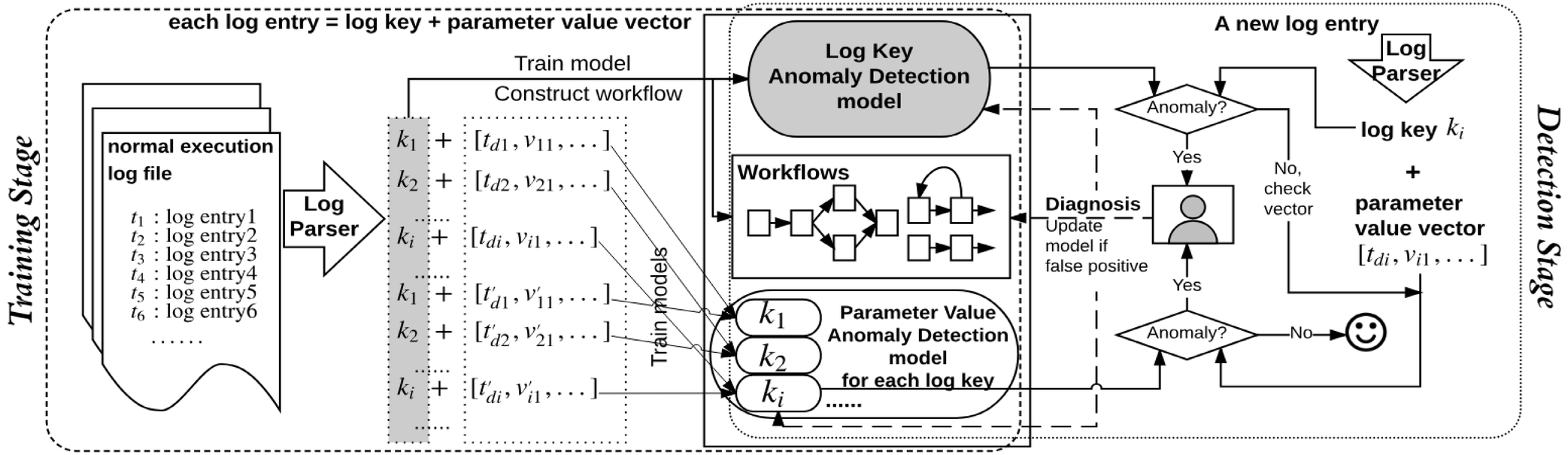
Kitsune: An Ensemble of Autoencoders for Online Network Intrusion Detection



Yisroel Mirsky, Tomer Doitshman, Yuval Elovici and Asaf Shabtai
Ben-Gurion University of the Negev

该文设计了一个在线的、无监督的网络异常检测系统
提出了基于集成AutoEncoder的异常检测模型
使用一种特征构建方式对所定义的流对象进行特征提取
通过分层聚类的方法将所提取特征进行类别划分
基于集成AutoEncoder模型的输出，使用预定义的异常阈值对流对象进行异常判断

DeepLog: Anomaly Detection and Diagnosis from System Logs through Deep Learning



- Min Du, Feifei Li, Guineng Zheng, Vivek Srikumar(School of Computing, University of Utah)
- log key异常检测模型（Log Key Anomaly Detection Model）。该模型的基本思想是把log key序列异常检测问题转化为一个多分类问题，即输入一个固定窗口大小的log key序列，输出是下一个log key的概率分布。定义 $K = \{k_1, k_2, \ldots, k_n\}$是日志生成系统生成的不同的log key集。

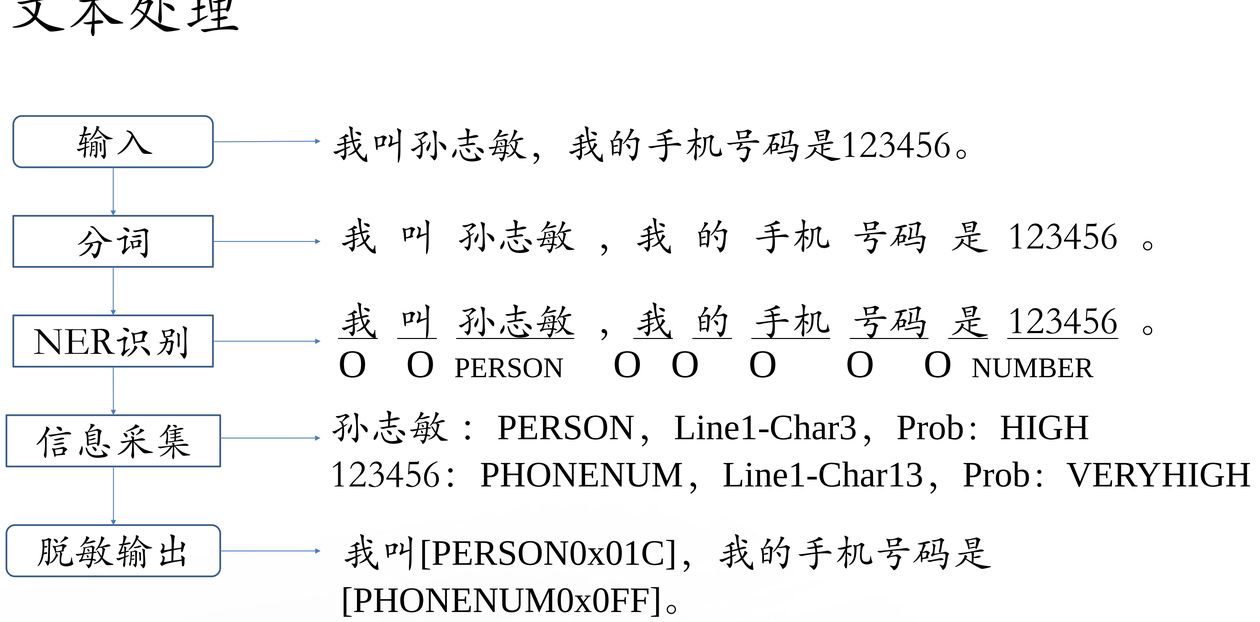
Du, Min, et al. "Deeplog: Anomaly detection and diagnosis from system logs through deep learning." ACM SIGSAC CCS, 2017.

More Paper

- 题目：Trend of Malware Detection Using Deep Learning
  - 作者：Yoon-seon Lee Jae-ung Lee（Hannam University韩国）
  - 深度学习在恶意软件检测的研究趋势。主要介绍了三种角度来实现恶意软件的检测,API特征，文件特征，指令特征—CNN 。
- 题目：Insider Threat Detection with Long Short-Term Memory
  - 作者： Jiuming Lu , Raymond K. Wong School of Computer Science and Engineering University of New South Wales Sydney, New South Wales
  - 将系统日志建模为自然结构化序列。本文的系统捕获指示用户正常使用行为的模式，以区分恶意行为的正常行为。实验表明，所提出的系统优于现有的基于对数的异常检测策略。这尤其适用于实时在线案例。

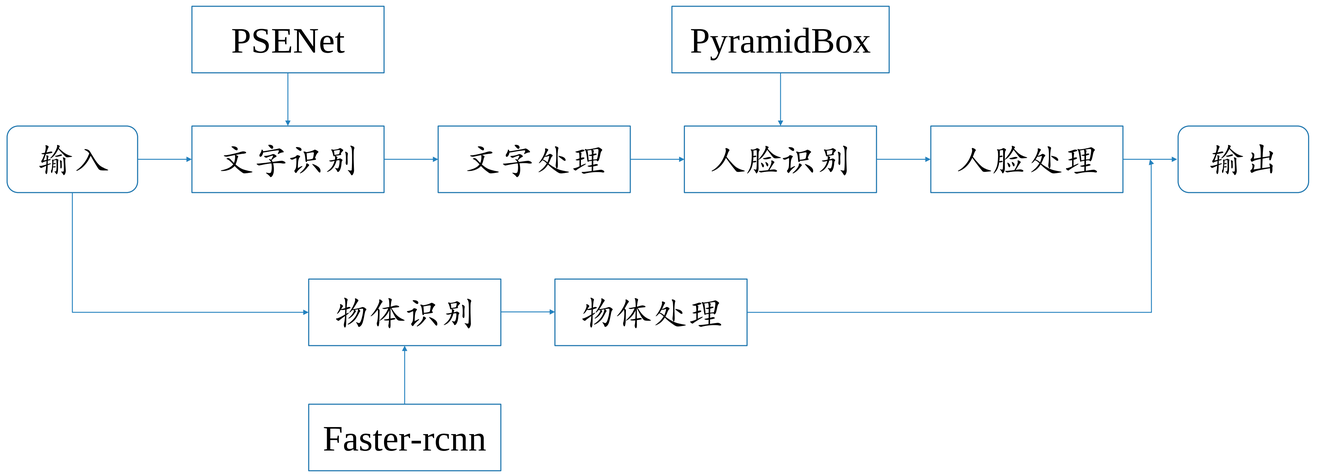
隐私数据处理-文本NLP

- GDPR要求越来越高
- 传统的正则表达式覆盖不完整
- NLP解决大部分问题，辅以正则表达式+字典
- 实际准确率约95%
- DLP应用的前景比较好



隐私数据处理—图像

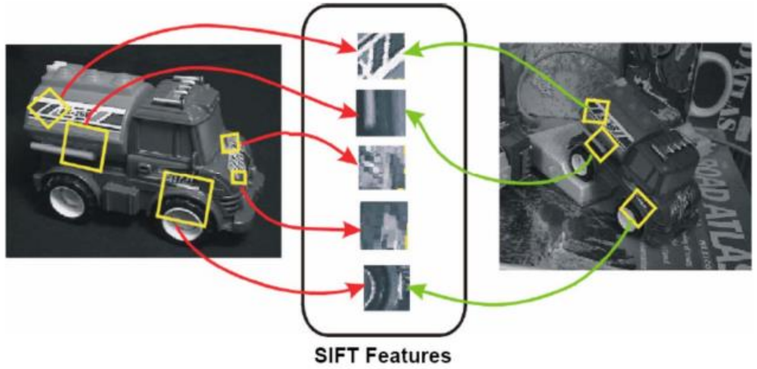
- 图片视频类占比持续上升
- PSENet, PyamidBox, Faster-rcnn在相关领域均有较好的识别能力
- 文字识别后继续走文本
- 人物，物体识别后走相关的策略

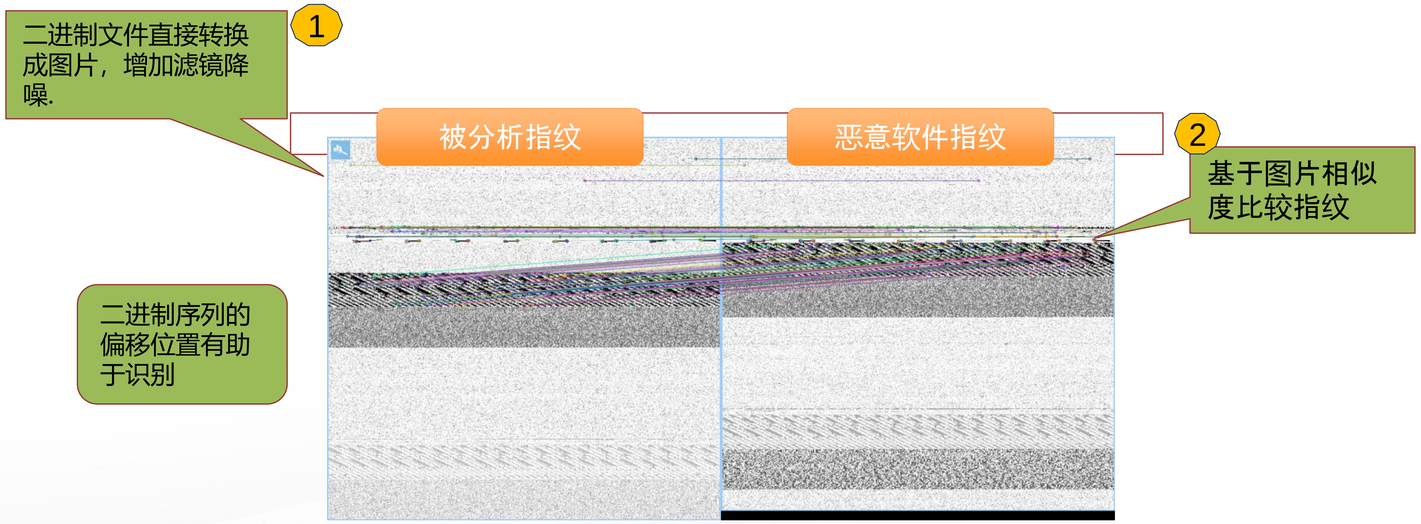


PyamidBox

VFP原理及应用

- VFP-Visual Finger Printer
- 恶意文件有家族概念，源文件变化不大，目标不同
- 从二进制文件上可以找到相似的特征
- 滤镜处理+ORB+CNN





VFP相关测试数据

- 70个家族，约1000指纹
- 每个指纹约15k
- 4万VT样本，测试准确率约93%
- 技术上有较多局限性：加壳，不在家族中，小样本不适应
- 现网运行作为杀毒软件的补充，仍然有较好作用。

网络入侵行为检测

流量数据的获取与预处理

- 公开数据集
  - McPAD
  - CICIDS2017
- 实验室数据
- 现网数据

流量数据的标注

- IDS标准数据集
- 实验室模拟干净数据
- 现网IDS检测结果
- 小部分手工标签

流量特征的构建

- 基于数据包的Payload信息
- 字符串固定长度1600个字符
- 比较ASCII码流与bit流

核心算法设计与实现

- 基于LSTM模型的检测算法
- 基于MLP模型的检测算法
- 基于CNN模型的检测算法

训练与测试

- 算法训练阶段
  - 参数配置与调整
  - 输入数据集调整
- 算法测试阶段

基于标准数据测试结果

实验方法	TPR	FPR
ASCII+MLP	0.982142857	0.021897810
Bit+ MLP	0.875000000	0.003649635
ASCII +CNN	0.892857143	0.003649635
Bit +CNN	0.875000000	0.010948905
ASCII +LSTM	0.982142840	0.007299270
1-Gram	0.892857143	0.003649635

基于McPad的测试结果

实验方法	TPR	FPR
ASCII+MLP	0.89756	0.0
Bit+ MLP	0.99745	0.0
ASCII +CNN	0.999635	0.00607
Bit +CNN	0.996354	0.001267
ASCII +LSTM	1.000000	0.0064

基于CICIDS2017的测试结果

TPR = TP / (TP + FN)
FPR = FP / (FP + TN)

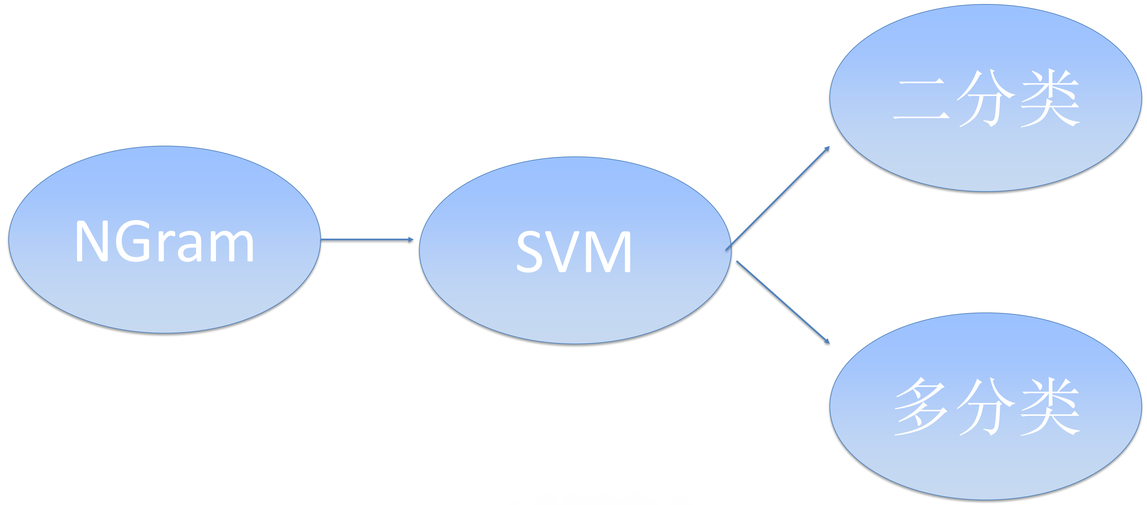
基于部分现网数据的测试结果

- 现网效果远低于模拟数据
- 需要优化的空间比较大

实验方法	TPR	FPR
Mcpad LSTM	0.4092	0.0228
Mcpad MLP	0.3819	0.0308
Mcpad CNN	0.6188	0.0903
CICI LSTM	0.0346	0.0655
CICI MLP	0.0401	0.0086
CICI CNN	0.3147	0.0657
Combine LSTM	0.9342	0.1332
Combine MLP	0.1748	0.0121
Combine CNN	0.9275	0.1607

WAF应用

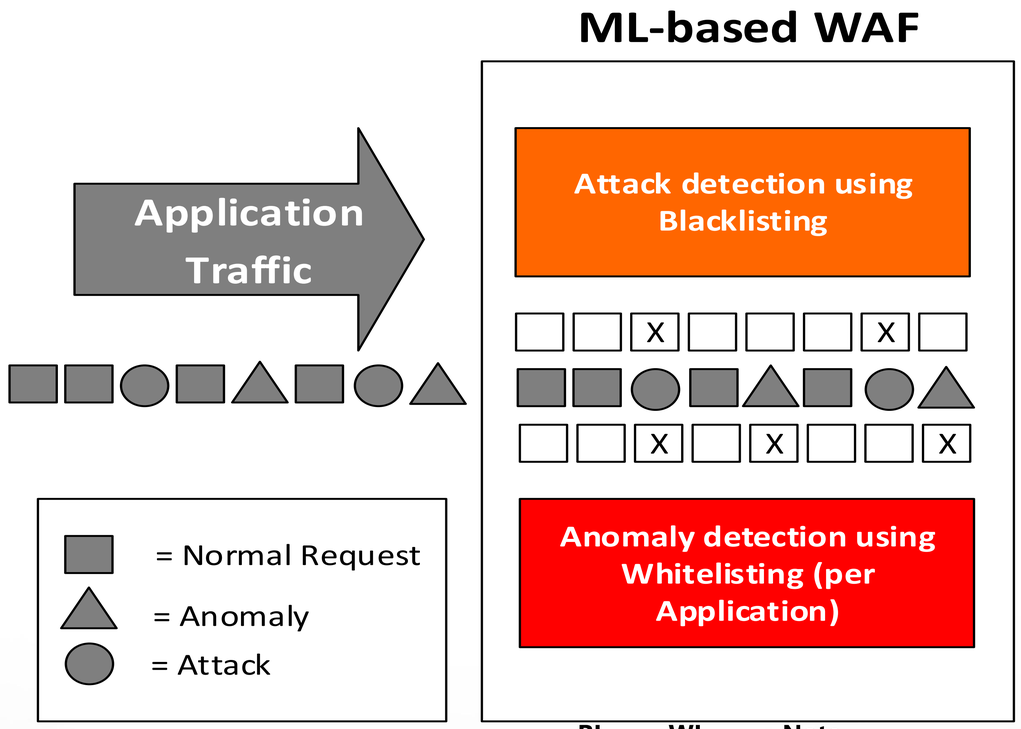
- 黑名单—已知攻击分类
  - SQL Injection (SQLi)
  - Cross Site Scripting (XSS)
  - Local/Remote File Inclusion (LFI/RFI)
  - Remote Code Execution (RCE)
  - Open Redirect (OR)
  - File/Directory browsing
- 白名单
  - 建立网站的行为分析模型
  - 基于行为异常发现
  - UEBA

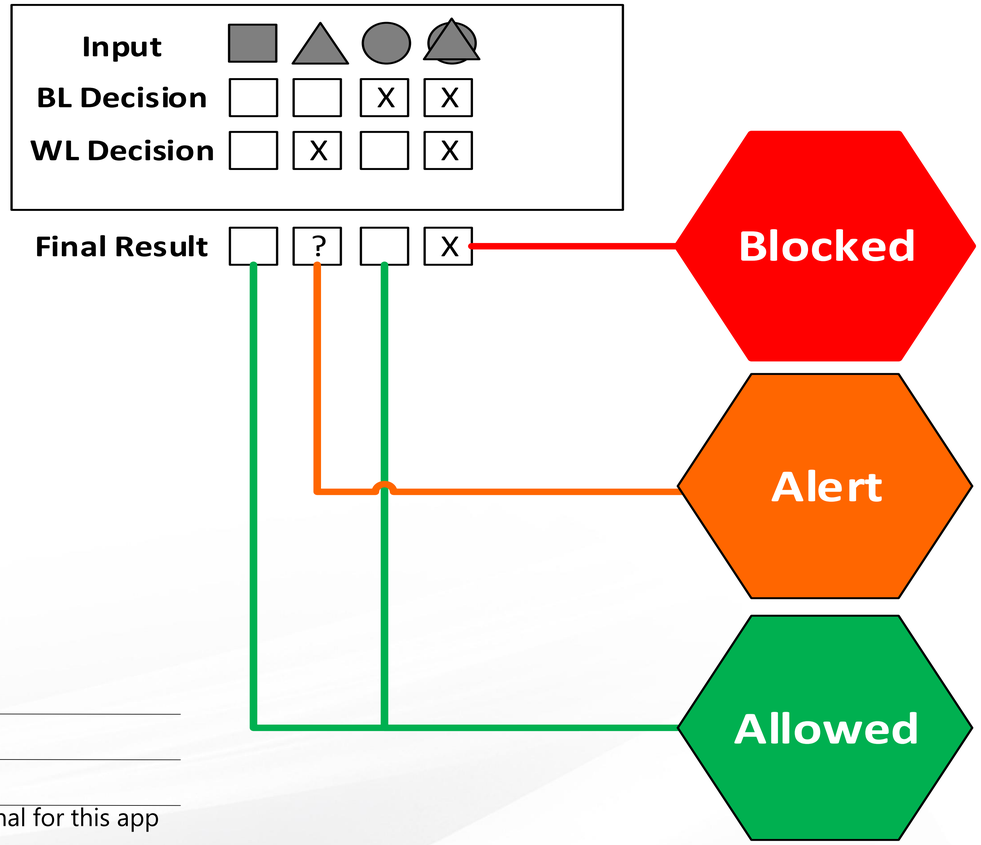


测试结果

实验方法	TPR	FPR
模拟数据二分类(N-gram over {benign, malicious} with SVM)	98%	0.04%
现网数据二分类 (N-gram over {benign, malicious} with SVM)	98%	3%
模拟数据多分类(N-gram over {benign, all classes of malicious} with SVM)	99%	0.02%
现网数据多分类 (N-gram over {benign, all classes of malicious} with SVM)	98%	2.50%
模拟数据多分类 (Smart Tokenization + N gram with XGBoost)	98%	0.001%
现网数据多分类 (Smart Tokenization + N gram with XGBoost)	98%	0.90%

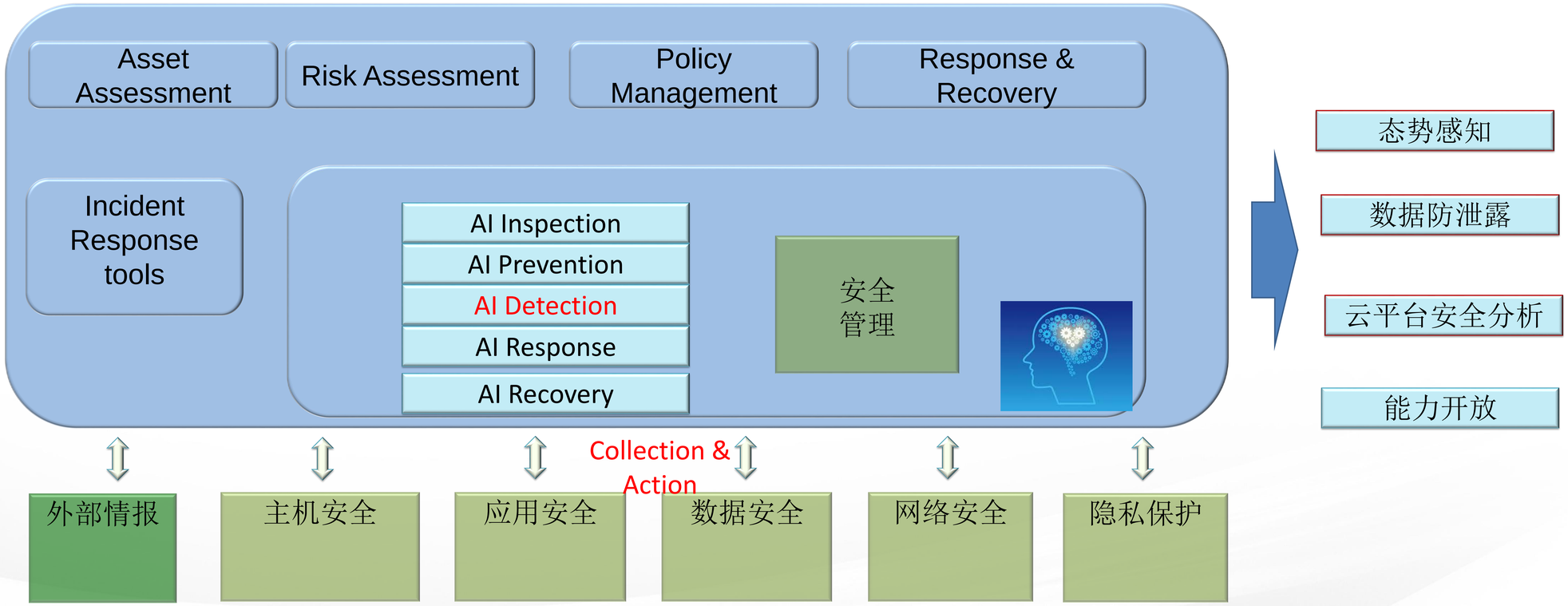
WAF的综合应用





	BL	WL	Note
Request contains price = 99.90	V	V	Normal
Request contains price = 2018-06-18	V	X	Anomaly
Request contains src = http://www.nnn.com	X	V	Looks like redirect, normal for this app
Request contains price = 99.90 and 1=1	X	X	Attack and Anomaly

面向未来


Asset Assessment
Risk Assessment
Policy Management
Response & Recovery
Incident Response tools
AI Inspection
AI Prevention
AI Detection
AI Response
AI Recovery
安全管理
Collection & Action
外部情报
主机安全
应用安全
数据安全
网络安全
隐私保护
态势感知
数据防泄露
云平台安全分析
能力开放

ISC 2019 7th
第七届互联网安全大会

THANK YOU