Райффайзен БАНК

Защит а API на основе Machine Learning

Нагин Павел,
АО «Райффайзенбанк»

Просто. Четко. Компетентно

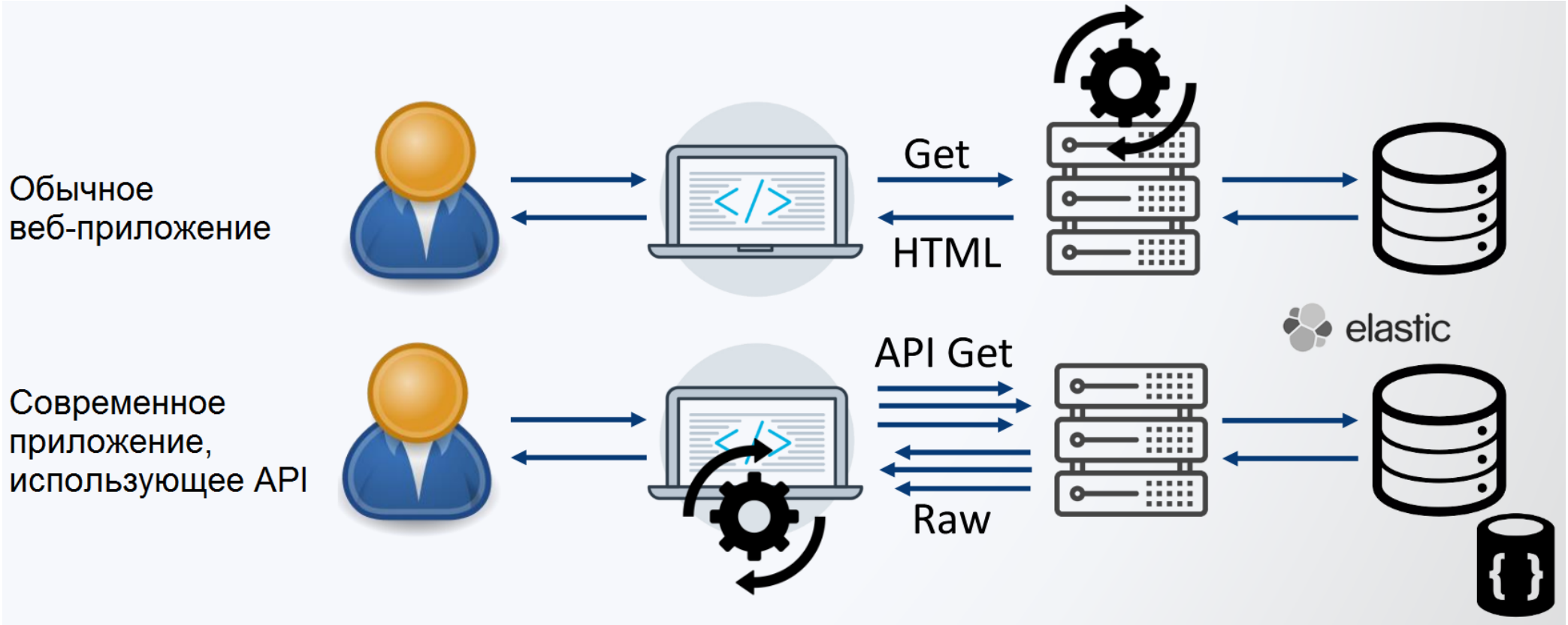
Райффайзен БАНК

Содержание

- Потенциальные угрозы
- Предпосылки к выбору решений по защите API на основе ML
- Тестируемые гипотезы

Что меняется с переходом на API?

1. API раскрывают логику и особенности реализации приложения.
2. В HTTP запросах передается большее количество параметров.
3. Другая схема предоставления доступов (JWT & API Keys)
4. Растет скорость создания и изменения новых сервисов (shadow API).



Угрозы для API

API Security TOP 10

- **A1**: Broken Object Level Authorization
- **A2**: Broken Authentication
- **A3**: Excessive Data Exposure
- **A4**: Lack of Resources & Rate Limiting
- **A5**: Broken Function Level Authorization
- **A6**: Mass Assignment
- **A7**: Security Misconfiguration
- **A8**: Injection
- **A9**: Improper Assets Management
- **A10**: Insufficient Logging & Monitoring

VS

OWASP Top 10

- **A1**: Injection
- **A2**: Broken Authentication
- **A3**:Sensitive Data Exposure
- **A4**: XML External Entities (XXE)
- **A5**: Broken Access Control
- **A6**: Security Misconfiguration
- **A7**: Cross-Site Scripting (XSS)
- **A8**: Insecure Deserialization
- **A9**: Using Components with Known Vulnerabilities
- **A10**: Insufficient Logging & Monitoring

Примеры:

A1: Получение документов другого пользователя по ID (ID=ID+1).

A2: Отсутствие защиты от brute force и credential stuffing, некорректная реализация JWT, OAuth, хранения паролей.

A3: Сервер возвращает больше данных, чем просил пользователь (паспортные данные, когда нужно только ФИО).

A4: Отсутствие ограничения на объем возвращаемых данных (/api/users?limit=999…).

Примеры из реальной жизни

1. Переборы в СБП:

From: fincert@cbr.ru <fincert@cbr.ru>
Sent: Friday
To: Raiffeisen
Subject: [ФинЦЕРТ] Запрос от ФинЦЕРТ REQ-xxx: 'Попытки массового выявления связи Идентификатор клиента — Банк/Банк по умолчанию в СБП ПС БР'

Здравствуйте!
Пожалуйста, примите к рассмотрению запрос "Попытки массового выявления связи Идентификатор клиента — Банк/Банк по умолчанию в СБП ПС БР" от ФинЦЕРТ под номером REQ-xxx.

Открыть запрос в личном кабинете: REQ-xxx

--
Автоматическая рассылка ФинЦЕРТ

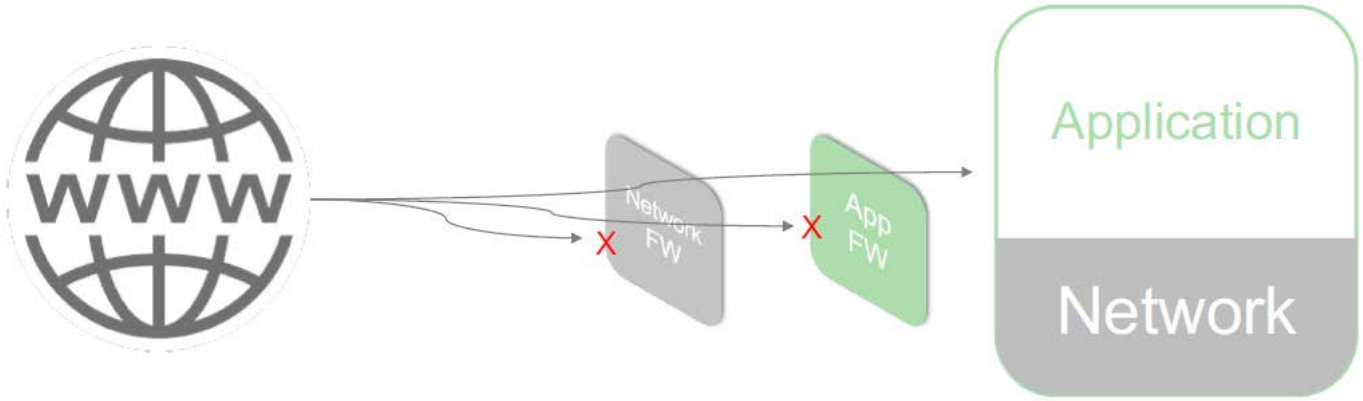
2. SMS Bomber

text 11.78 KB raw download clone embed report print

```
#!/usr/bin/python
class spymer:
        def main(self):
                import requests, random, datetime, sys, time, argparse
                from colorama import Fore, Back, Style
                print("CyberLand SMS Bomber version.1.4")
                parser = argparse.ArgumentParser(prog='spymer', description="Возможно что-то уже не работает. Только для России!")
                parser.add_argument('phonenum', metavar='phone', help='Телефонный номер жертвы (пример: 79991234455)')
                args = parser.parse_args()
                def showstatus(message, type='new'):
#                       raiffeisen = requests.get('https://oapi.raiffeisen.ru/api/sms[redacted], params=
```

Почему необходимо отдельное решение для защиты API?

Межсетевые экраны (FW) и файрволы веб-приложений (WAF) в первую очередь ориентированы на контроль и управление доступом:



В то же время при защите API необходимо ориентироваться на проверку надлежащего использования. Это очень сложно сделать с помощью набора правил, так как API имеют сложную, динамично меняющуюся структуру.

Какие преимущества может дать Machine Learning (ML)?

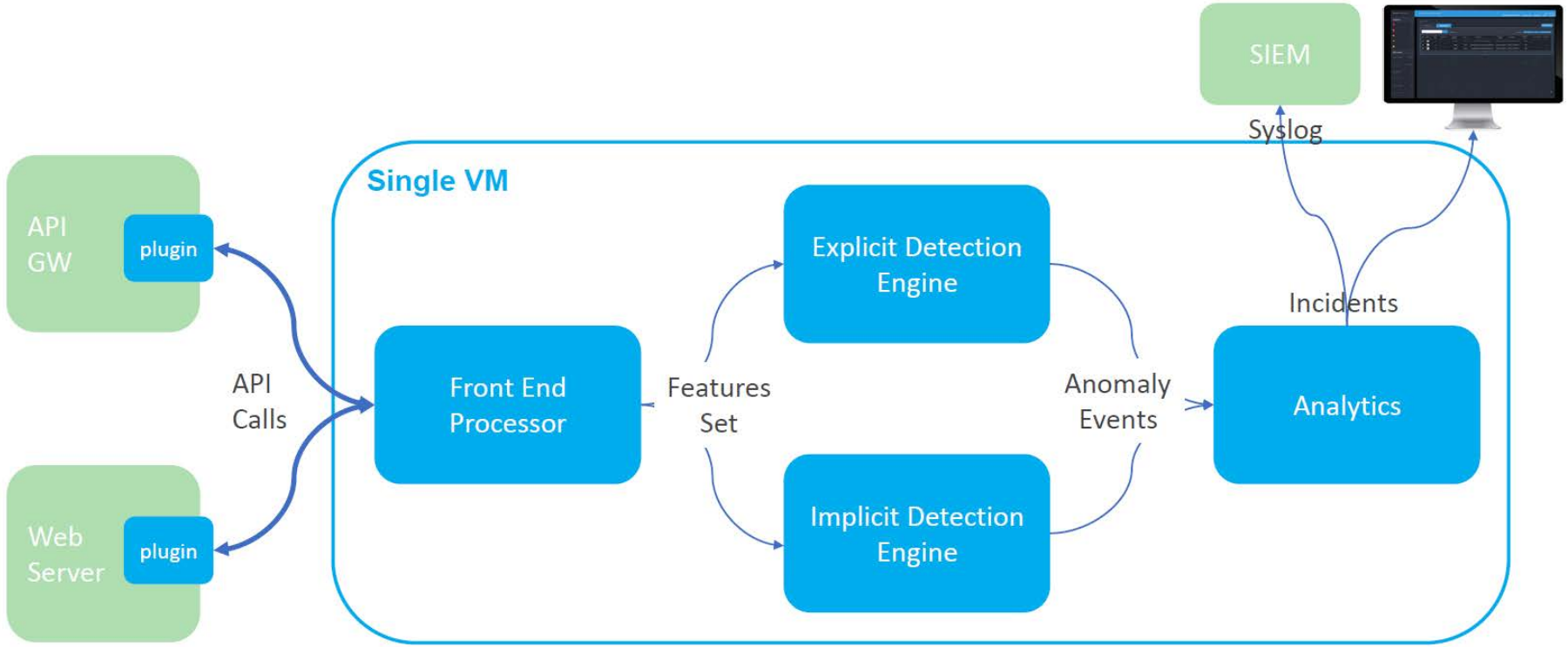
Выявлений аномалий должно помочь:

- обнаруживать неизвестные ранее атаки и уязвимости
- на раннем этапе фиксировать попытки найти уязвимости в API
- детектировать атаки на бизнес-логику

Постоянное автоматическое обучение:

- снижает затраты на первоначальное конфигурирование и администрирование
- обнаруживает новые API и изменения в уже существующих, а также ошибки конфигурирования
- упрощает встраивание в циклы разработки

Архитектура решения ImVision



Explicit Detection основано на предопределенной логике (совпадение с заданными паттернами).

Implicit Detection использует Machine Learning с предиктивной аналитикой, автоматически изучает:

- Структуру и значения API вызовов
- Взаимосвязи между значениями в API вызове
- Взаимосвязи между API вызовами

Вопросы?

Полезные ссылки:

https://www.owasp.org/images/5/59/**API_Security_Top_10_RC**.pdf

https://cheatsheetseries.owasp.org/cheatsheets/**REST_Security_Cheat_Sheet**.html

https://www.**ImVision**tech.com/