QCon[上海站]
全球软件开发大会2016

RASP技术解读

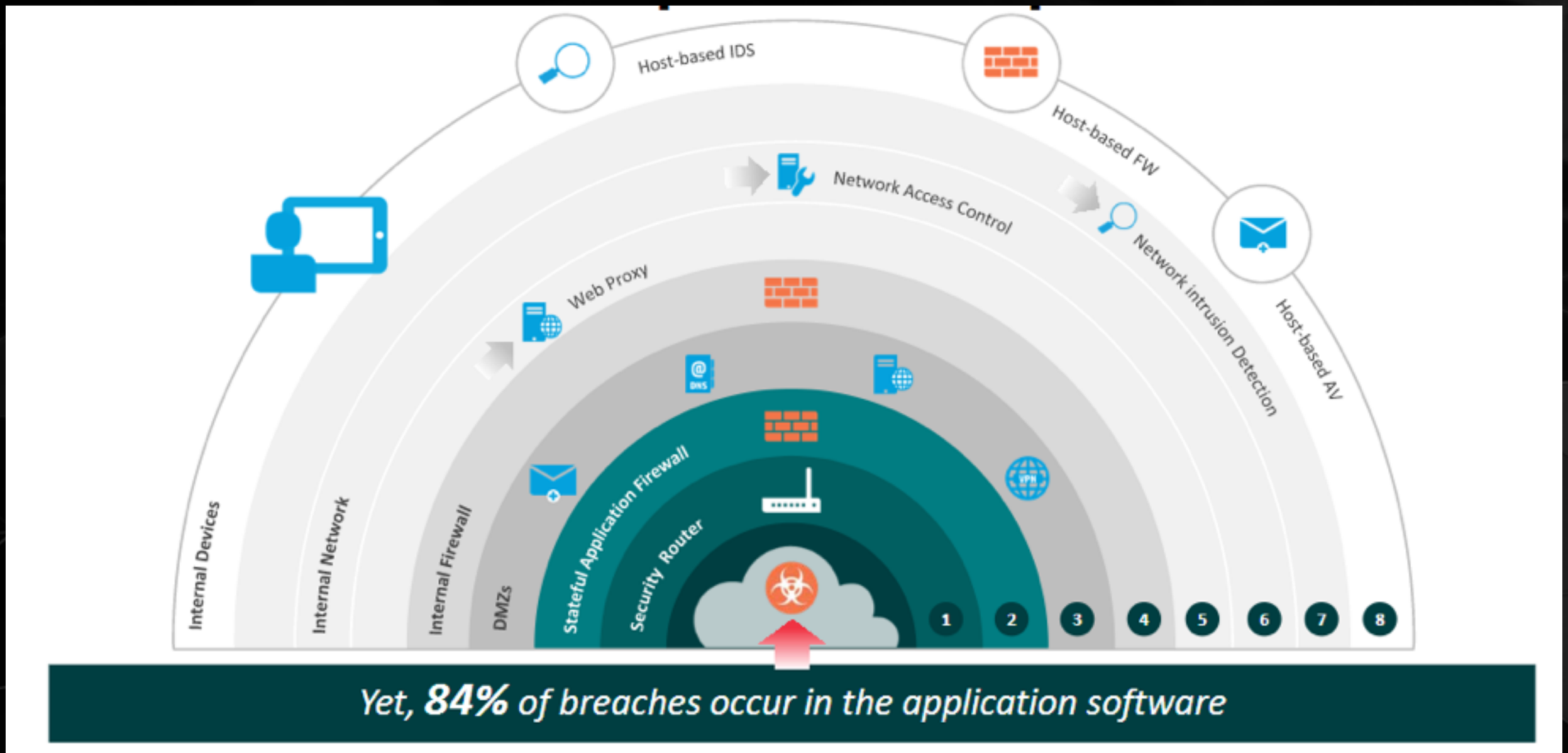
Java探针技术在应用安全领域的新突破

SPEAKER

CTO 刘再耀

主办方 Geekbang. 极客邦科技 InfoQ

- 当前安全防护现状


Host-based IDS
Host-based FW
Network Access Control
Network intrusion Detection
Host-based AV
Web Proxy
DNS
VPN
Internal Devices
Internal Network
Internal Firewall
DMZs
Stateful Application Firewall
Security Router
1
2
3
4
5
6
7
8
Yet, 84% of breaches occur in the application software

• 代码安全 -- SSDLC

需求

- **产品研发初期**
- 安全顾问规划
- 规划安全里程碑
- 安全元素集成入产品

设计

- **设计**
- 设计安全架构和指导方案
- 形成安全且有效的规范文档
- 漏洞模型

实现

- **标准、检验、工具**
- 遵从安全编码规范
- 使用安全扫描工具(fuzzing tools, static-analysis tools, etc)

验证

- **安全性推动**
- 代码reviews
- 安全性测试
- 主流漏洞监测
- 达到预期准则

发布

- **安全性把控**
- 安全团队的检测
- 完整的测试验证
- 遵守安全准则
- **RTM 和 部署**

响应

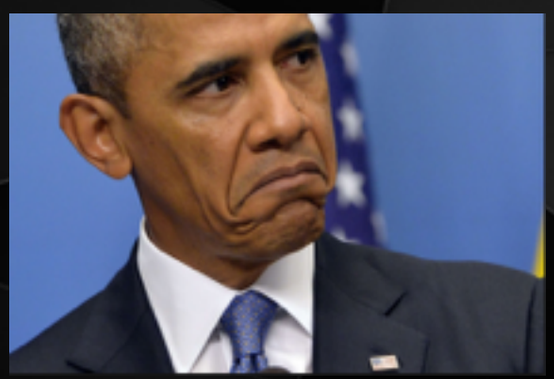
- **安全响应**
- 规范反馈响应机制
- 实时处理反馈
- 反思

- 代码安全 -- 第三方代码


自定义业务逻辑
(WARs, EJBs, JARs)
第三方库
服务器和框架
(JEE)
Java APIs
(JRE)
大部分应用代码都来自企业外部，这些外部代码或多或少都会存在已知、未知缺陷
应用各层的风险
80+%
外部代码
75% 的CIO们都没有意识去控制这些外部风险
不存在风险的代码是传说

- 代码安全 -- WAF

WEB 应用防火墙示意图



- 代码安全新方案 – **RASP**

Runtime Application Self Protection - RASP

"We need to look at new technologies which enable applications to defend themselves, known as Runtime Application Self Protection."

"Investment in RASP should be prioritized over the $12bn per annum spent on WAF, NGFW, IPS."

RASP is unlike previous security technologies because:

"[RASP] sees all data coming in and out of the application, all events affecting the application, all executed instructions, and all database access"

In other words, RASP has complete contextual awareness of all application execution which means it sees 100% of application execution information!

Joseph Feiman, VP and Gartner Fellow

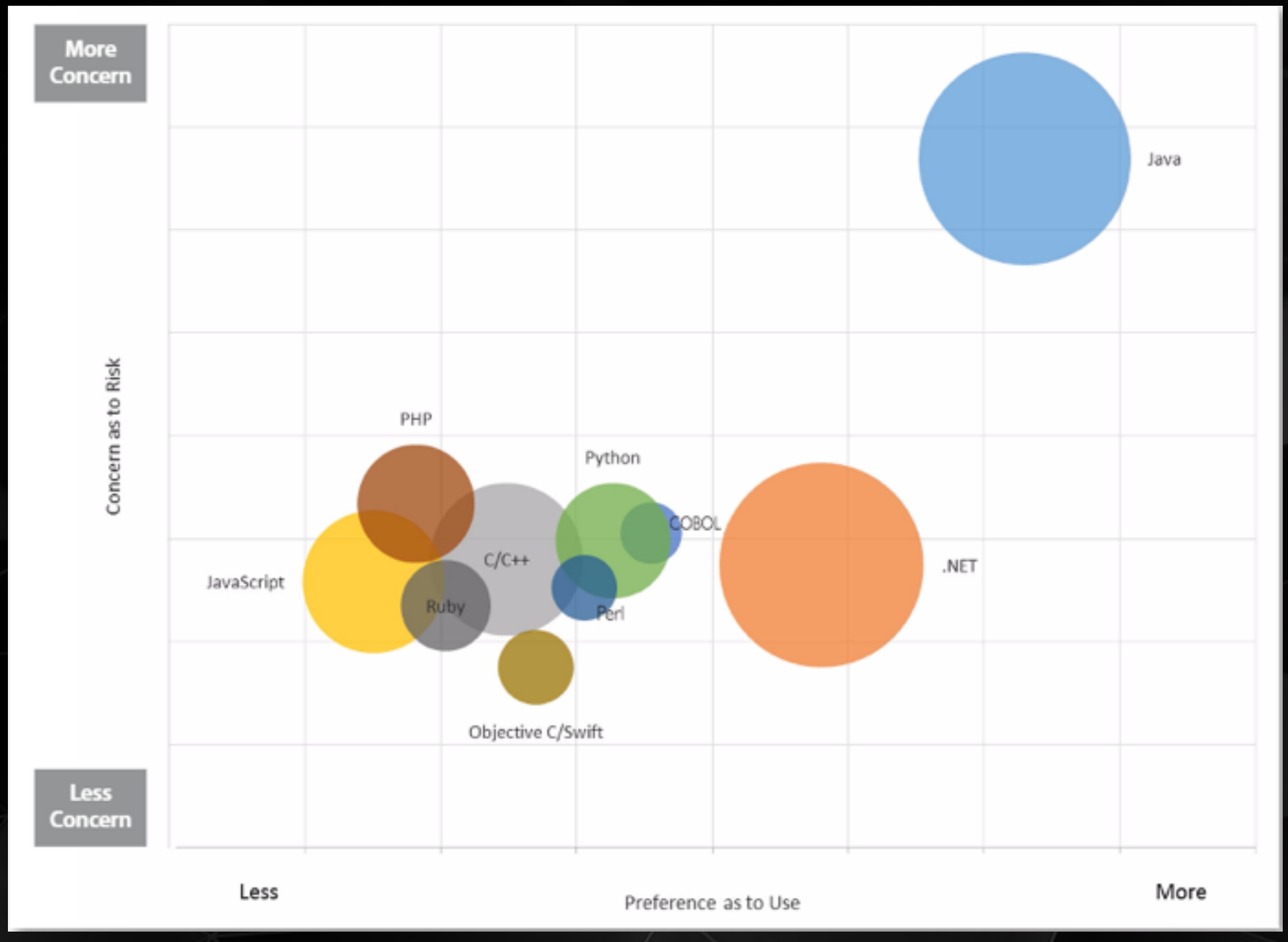
Gartner

RASP防护要求

- 基本要求
  - 能防护OWASP Top10攻击， CWE常见漏洞
  - 支持私有化和SaaS部署方式
  - 自适应各种网络部署方式和规模大小

- 独特要求
  - 高精度：接近零误报和零漏报
  - 无需改变任何代码，将安全防护和业务代码完全隔离
  - 自己保护自己，防护代码不能有漏洞
  - 保护应用各层级安全：JVM、容器、第三方组建及开源库以及业务逻辑
  - 高性能，不能随着规则集增加而对性能有大的影响
  - 能保护遗留的应用程序安全
  - 能详细展示攻击的过程和细节

- **Java应用是黑客攻击重点**

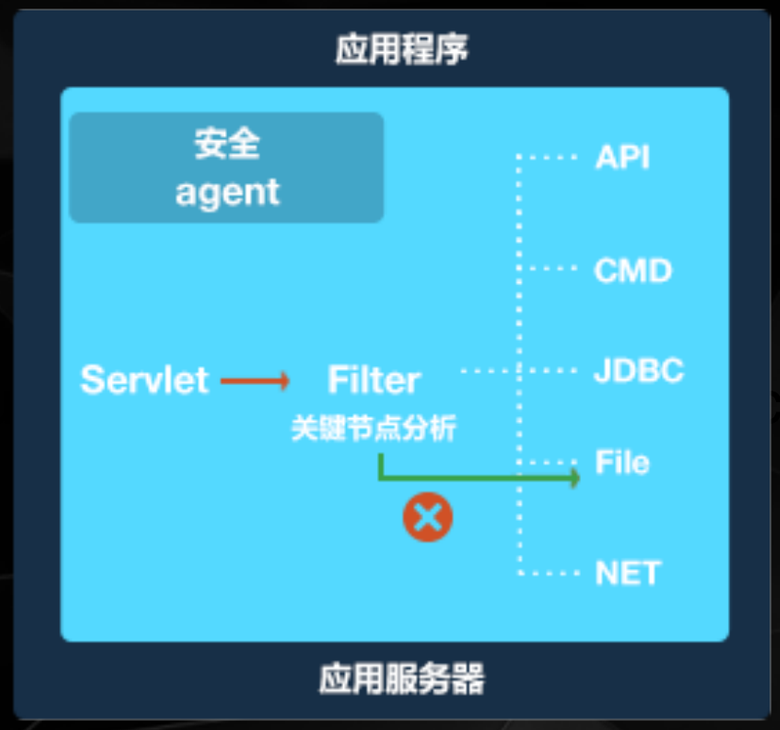


SANS State of application security 2015

- # RASP Java语言实现方式

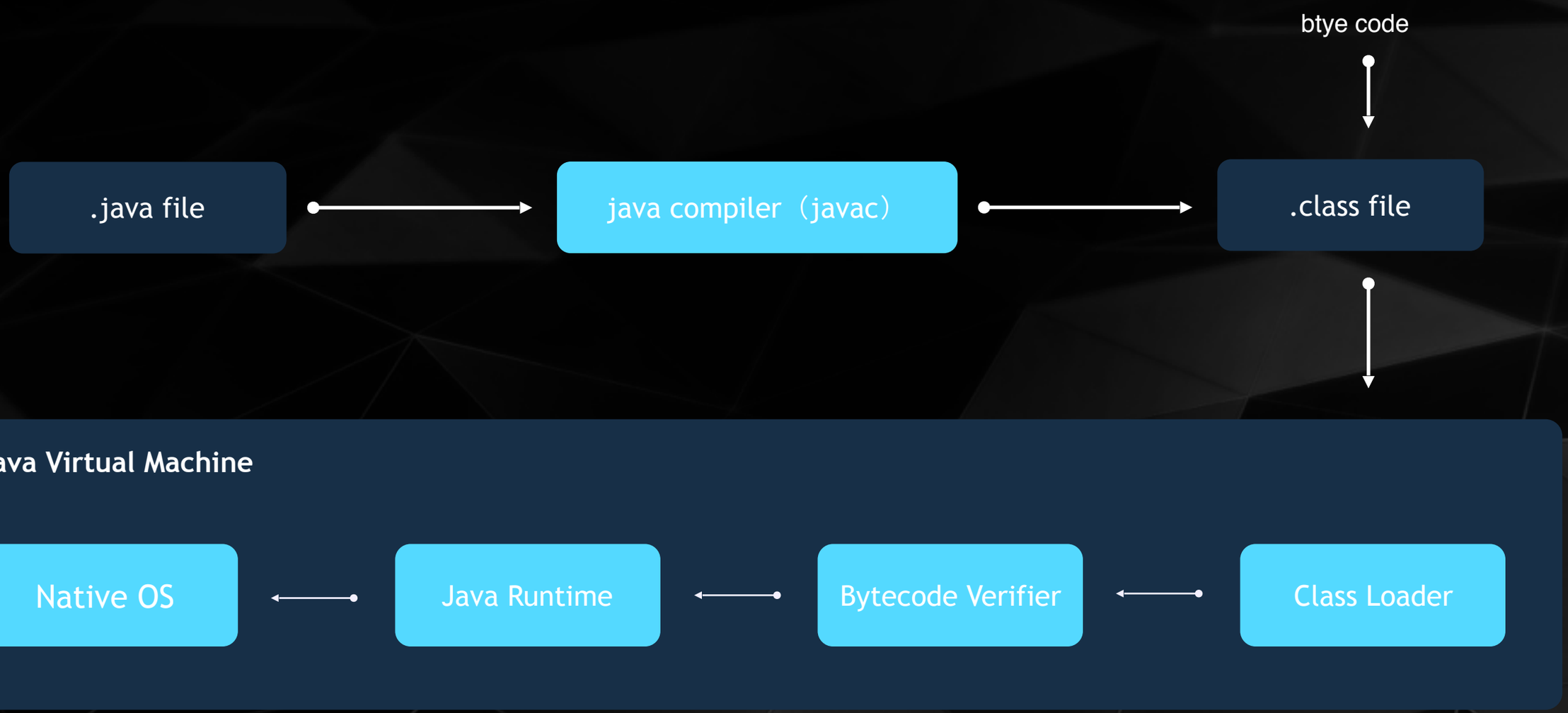
Servlet Filter

Java Instrument

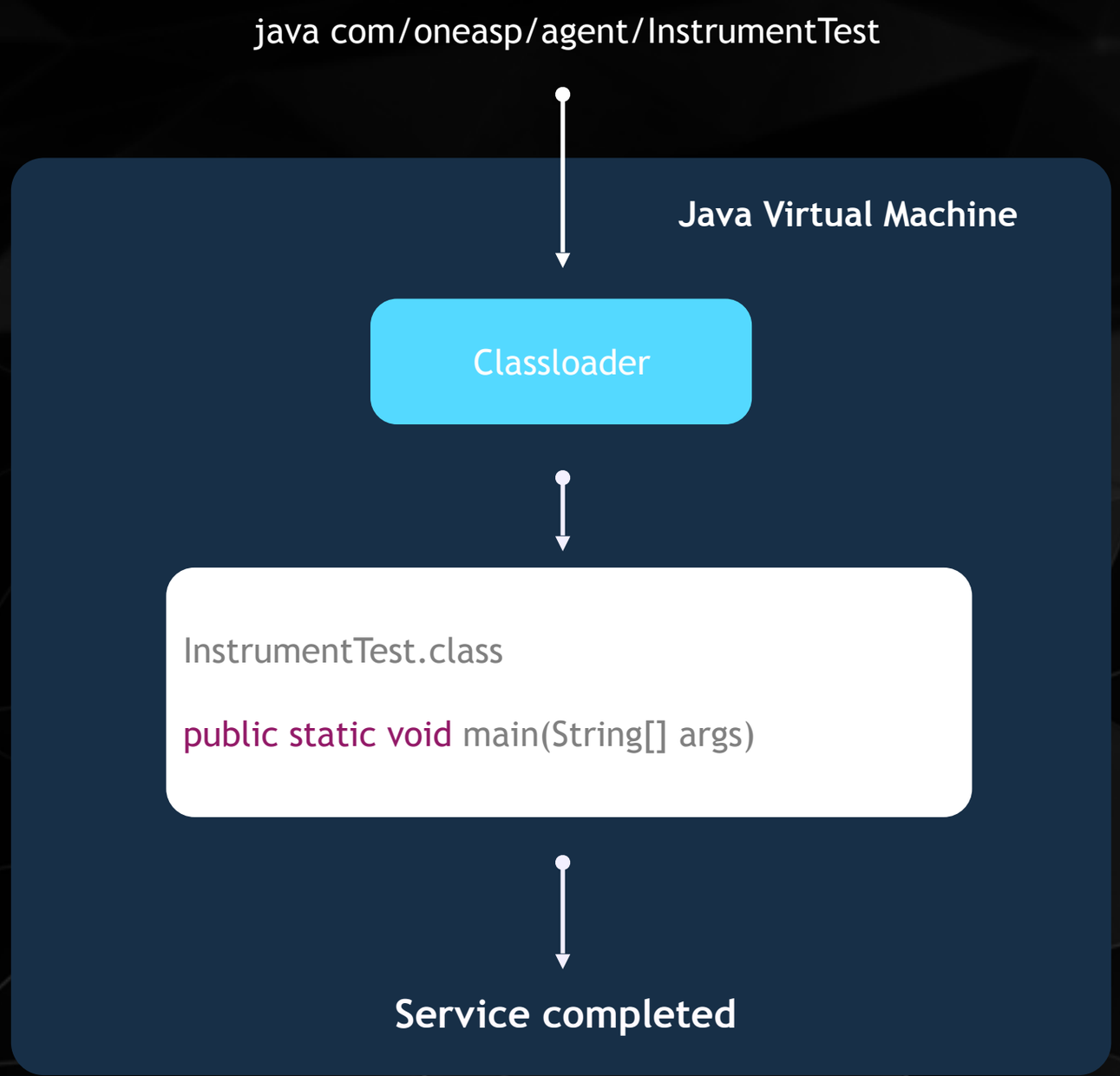


JVM重构

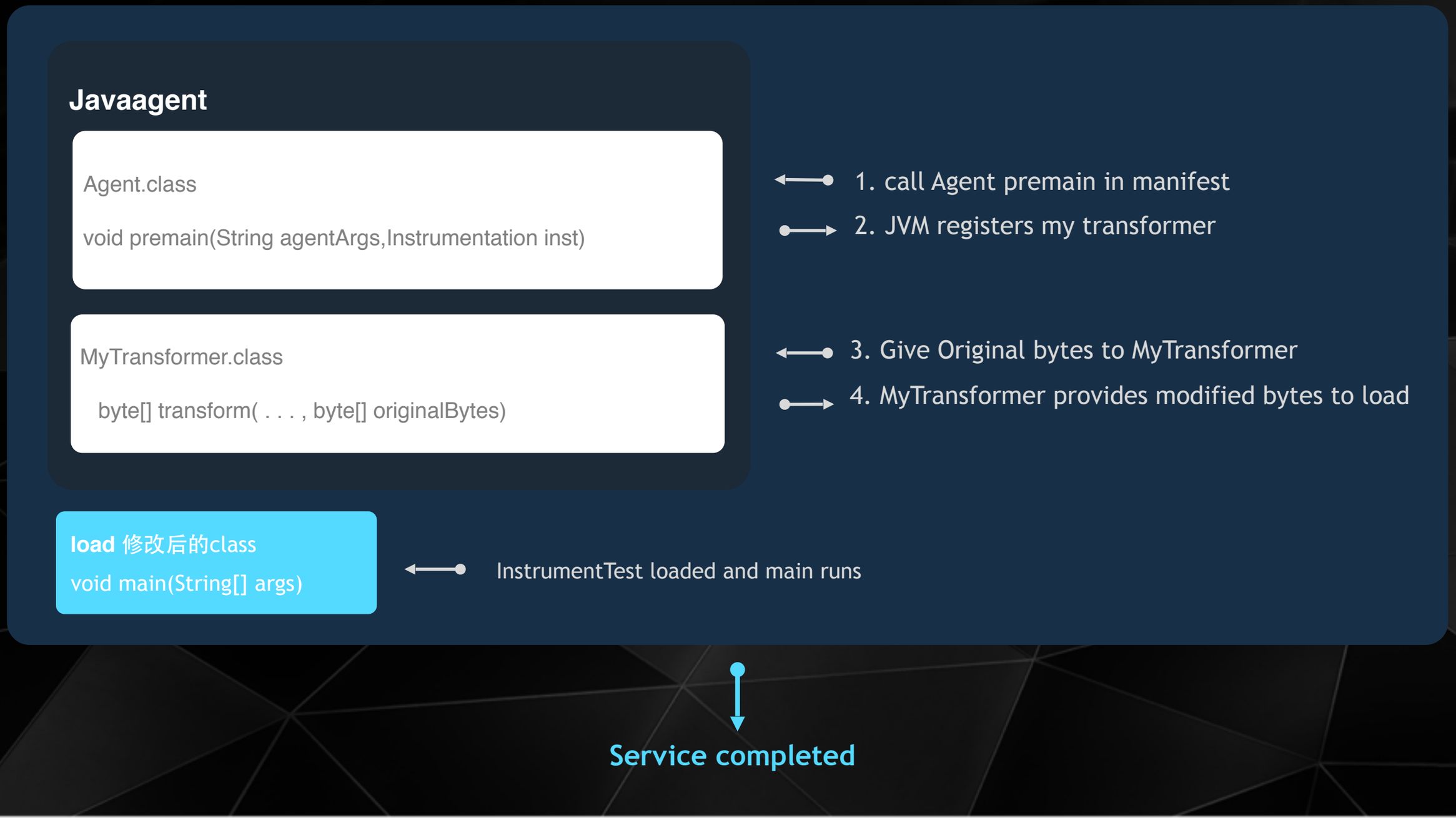
- **Instrument实现 – 字节码**



- **Instrument实现 – Java程序运行**



- **Instrument实现 – 代码注入过程**



- **Instrument实现 – 字节码操纵框架**

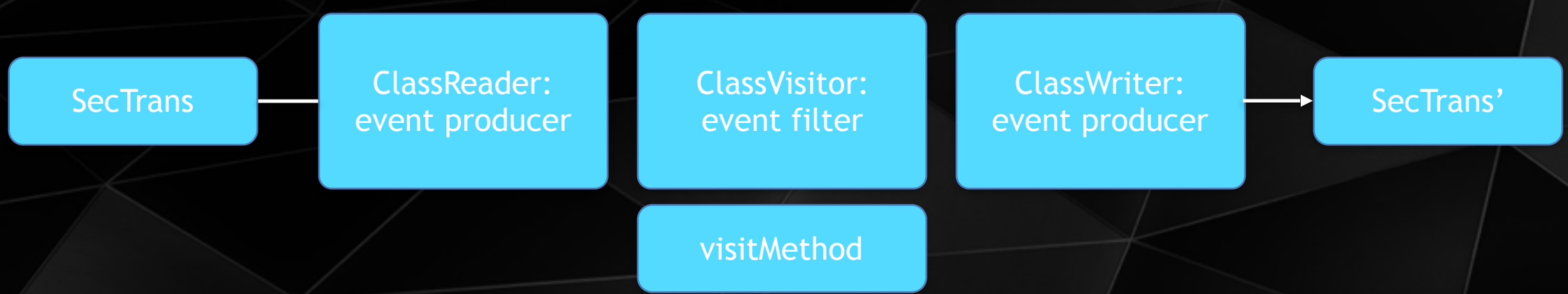
- ASM: http://asm.ow2.org
- BCEL: http://commons/apache/org/proper/commoms-bcel
- CGLib: http://github.com/cglib/cglib
- Javassist: http://www.csg.ci.i.u-tokyo.ac.jp/~chiba/javassist
- Serp: http://serp.sourceforge.net

- **Instrument实现 – ASM原理**

ClassReader： given a byte[],parses a compiled class

ClassVistor: delegates class events,event filter
visitAttribute visitField visitMethod visitInnerClass visitEnd

ClassWriter:produces output byte[]



- **OneASP实践 - 配置**

```
<Rule>
 <ProPoints>
   <ConRefer id="DbQuery"/>
   <ConRefer id="Hib2Query"/>
   <ConRefer id="Hib3Query"/>
   <ConRefer id="JpaQuery"/>
   <ConRefer id="JdoQuery"/>
 </ProPoints>
 <ProPoint id="DbQuery">
          <Method>
              <Class>java\.sql\.Statement</Class>
              <Name>addBatch|execute(Query|Update)?</Name>
              <Paras>
                  <ParaType type="java\.lang\.String"/>
                  <Ell/>
              </Paras>
          </Method>
          <Capture>
              <This id="stmt"/>
              <Argument id="sql" index="0"/>
          </Capture>
 </ProPoint>
 <Filters>
   <FilterSpec
       class="com.asp.filter.SQLProtect" ID="3A8F96C6-B2E4-4113-B0C3-740F1E0CA9CE">
          <Attributes>
              <Attribute name="type">SQLi</Attribute>
              </Attributes>
              <Config>
                  <Prop name="Trigger">
                      <Value>%{Input}</Value>
                  </Prop>
              </Config>
                  <Patchs>
                      <Patch name="Input" capture-ref="sql"/>
                      <Patch name="Stmt" capture-ref="stmt"/>
                      <Patch name="Conn" capture-ref="conn"/>
                  </Patchs>
   </FilterSpec>
 </Filters>
</Rule>
```

- **OneASP实践 - 代码**

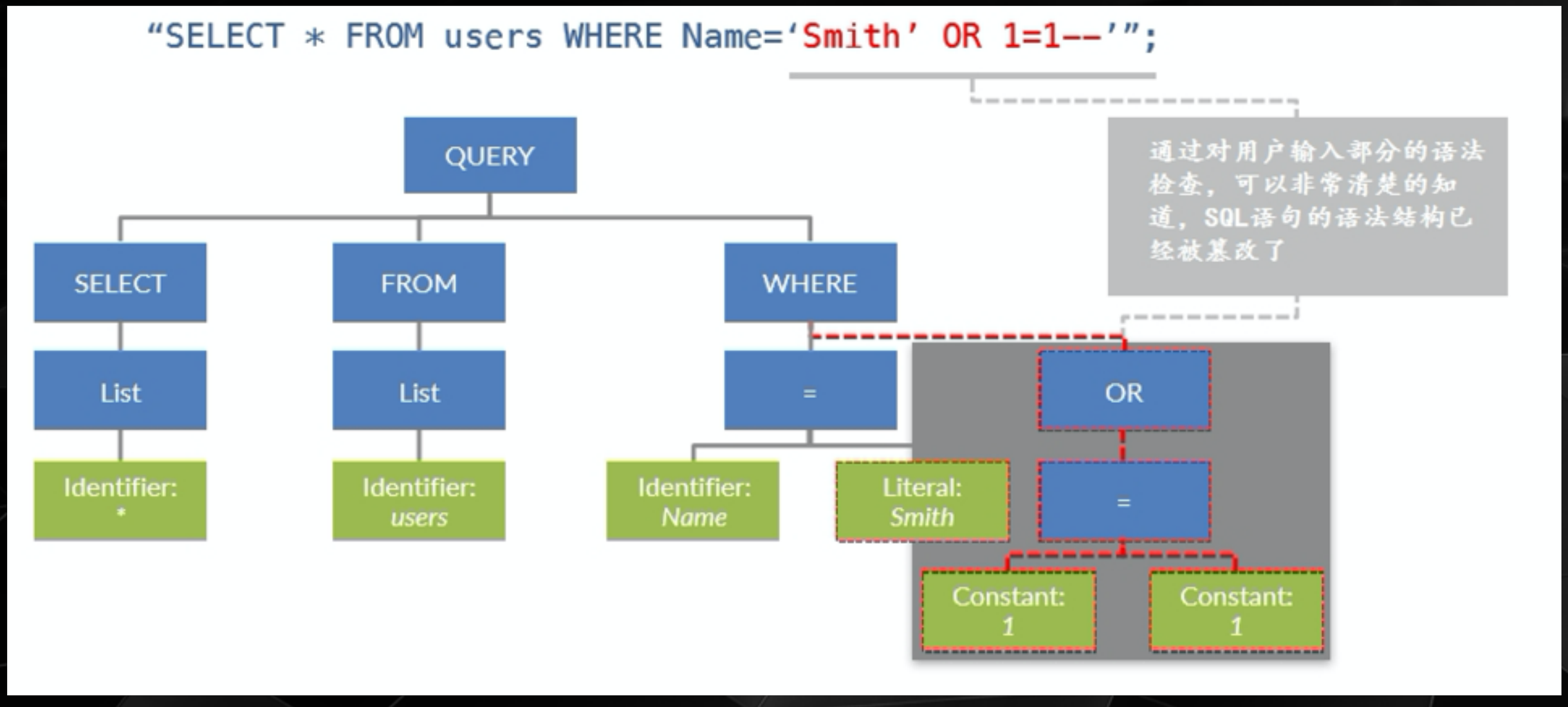
```
@Monitor
public class SQLProtect
{

    public void before() throws FilterException {
        final HttpRequest req = RaspUtil.getActiveRequest();
        if (null == req) {
            return;
        }
        if (null == this.sql) {
            return;
        }
        this.isMySql = DbUtil.isMySql();

        parseSQL(this.sql.toString().toLowerCase());
        isAttack = ;//CheckParameters CheckCookies CheckHeaders
        isAttack = DBUtil.isSQLInjection(this.sql);
        if(isAttack)
           //do action
        }
        else {
            SQLProtect.log.debug(this.sql + "is not sqli"));
        }
    }

    public void after() throws MonitorException {
        if (this.shouldAddToCache && null != this.normalSql && null != this.cache) {
            this.cache.add(this.normalizedSql);
            SQLProtect.Log.debug("Add Normalized SQL: " + normalSql));
        }
    }
}
```

- **OneASP实践 - SQL注入检测**



- RASP现状和未来

CONTRAST SECURITY

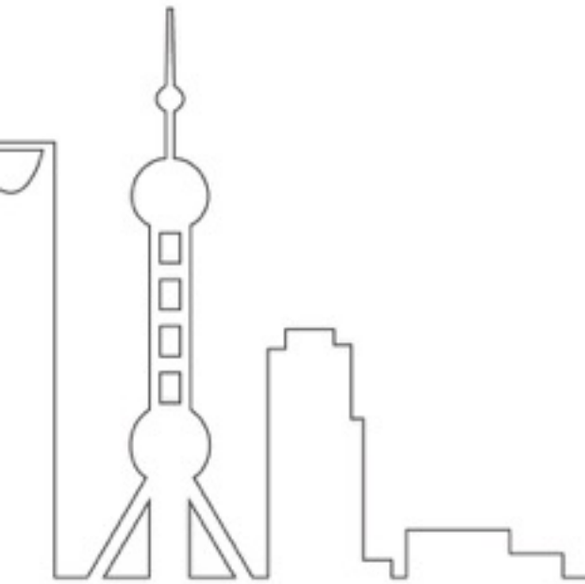
waratek

ONE ASP

PREVOTY

Hewlett Packard Enterprise

- **Question**



Thanks!

International Software Development Conference

主办方