大型企业应用安全方案

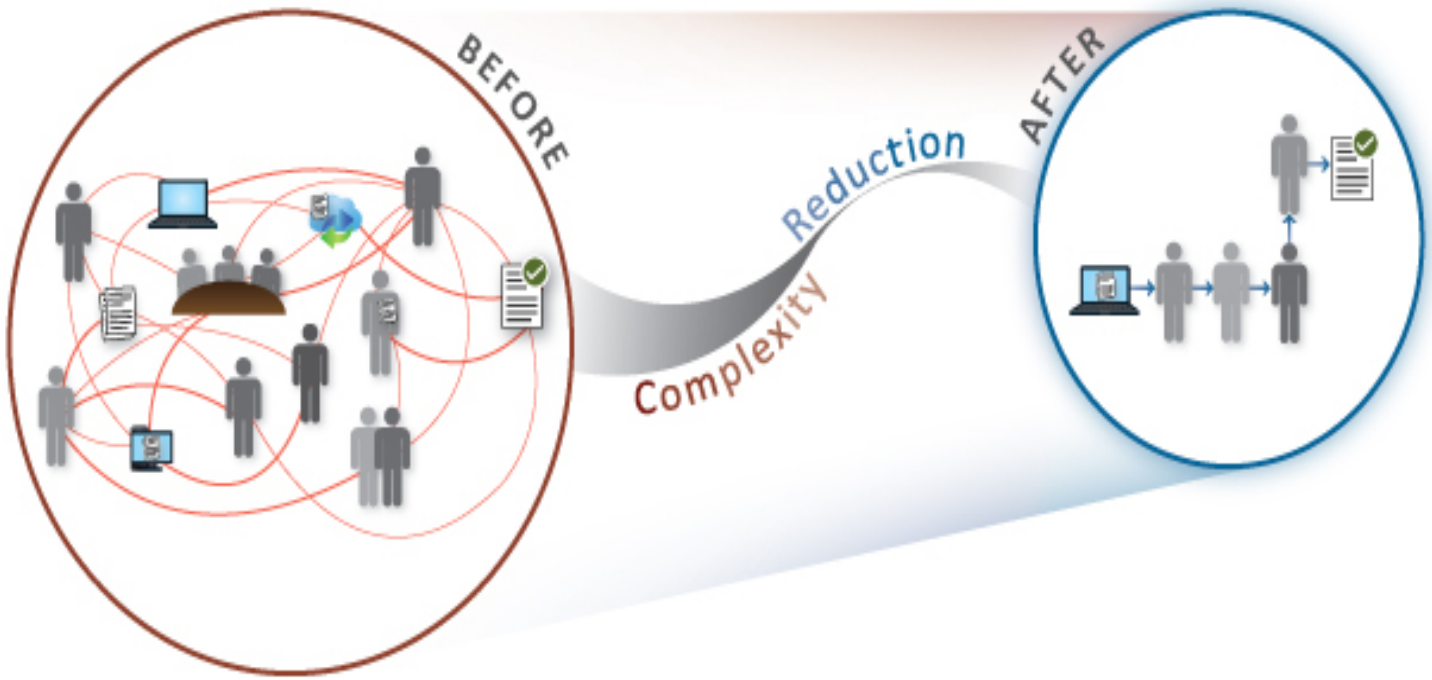
钟卫林 OWASP 亚洲峰会 深圳 2017年7月

大型企业应用安全的挑战

- 规模 (Scalability)
  - 应用数量
  - 代码数量
  - 开发人员数量
  - 团队／业务数量

大型企业应用安全的挑战

- 复杂度(Complexity)
  - 应用类型
  - 编程语言类型
  - 技术类型
  - 编译环境
  - 团队架构和文化



大型企业应用安全的挑战

- 效率 (Efficiency)
  - 扫描速度
  - 扫描容量
  - 系统资源
  - 工具安装
  - 工具使用
  - 流程集成

大型企业应用安全的挑战

- 效用 （Effectiveness）
  - 结果质量
  - 准确度
  - 从发现到修复
  - 与现有环境流程的集成

大型企业应用安全的挑战

- Governance 治理
  - 策略和法规
  - 流程和规则
  - 团队建设
  - 检测和监测
  - 指标 (metrics)
  - 变化 (trending)
  - 报告 (dashboards)

解决方案?

金融，政府，传统行业：

- 授人与鱼，不如授人与渔
- 重防御，早发现
  - An ounce of prevention is worth a pound of cure

解决方案?

新型互联网公司:

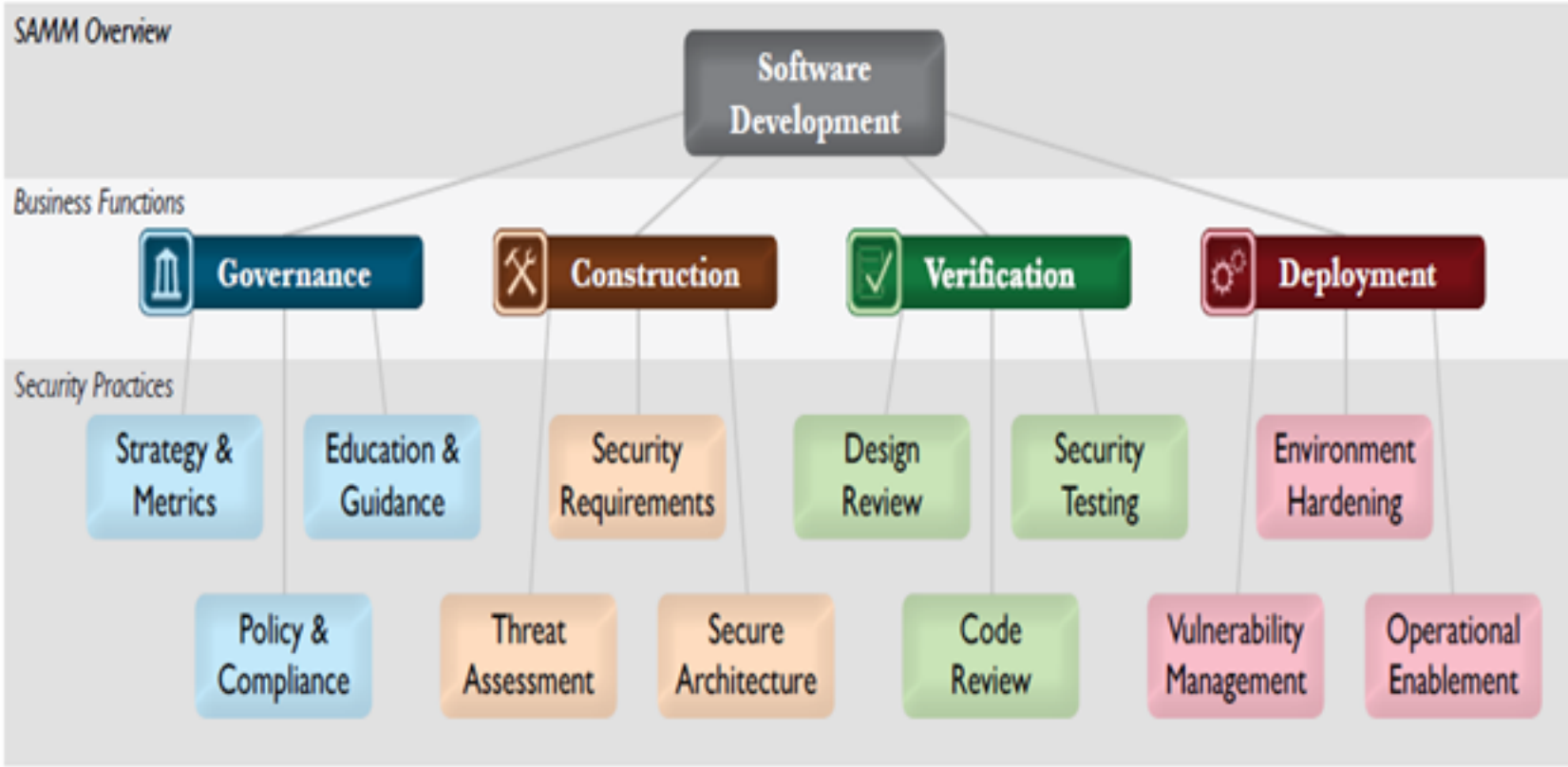
- 轻流程，重监测，快反应
- 安全问题交给专家解决

解决方案的三大要素

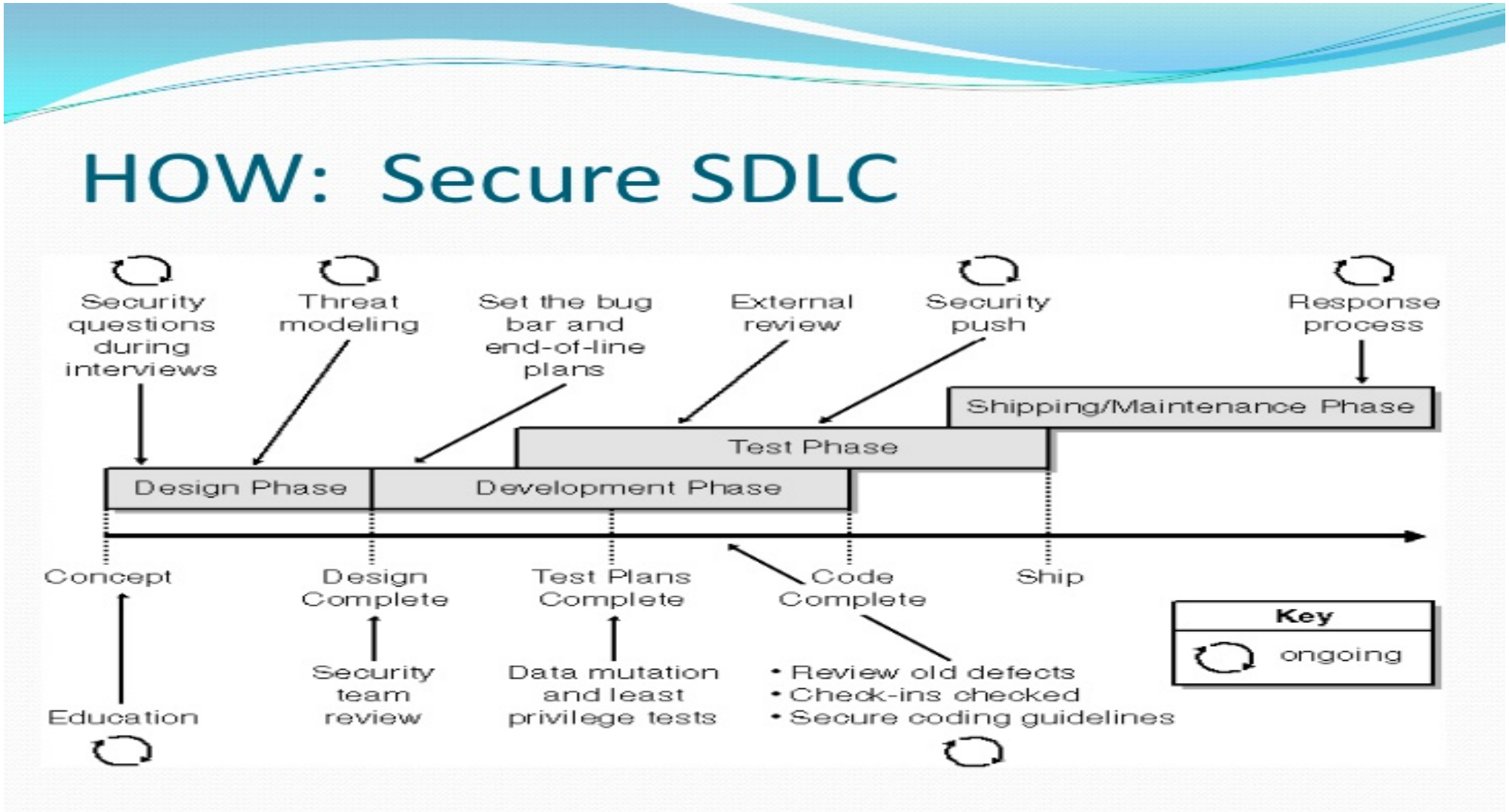
- 人：文化
- 技术：资源
- 流程：管理

大型企业应用安全框架

- 策略和法规
- 培训和指南
- 分析和检测
- 流程和管控
- 操作和执行
- 风险分析和控制



应用安全流程集成


HOW: Secure SDLC
Security questions during interviews
Threat modeling
Set the bug bar and end-of-line plans
External review
Security push
Response process
Shipping/Maintenance Phase
Test Phase
Design Phase
Development Phase
Concept
Design Complete
Test Plans Complete
Code Complete
Ship
Education
Security team review
Data mutation and least privilege tests
• Review old defects
• Check-ins checked
• Secure coding guidelines
Key
ongoing

应用开发安全实践

1. TRAINING	2. REQUIREMENTS	3. DESIGN	4. IMPLEMENTATION	5. VERIFICATION	6. RELEASE	7. RESPONSE
1. Core Security Training	2. Establish Security Requirements	5. Establish Design Requirements	8. Use Approved Tools	11. Perform Dynamic Analysis	14. Create an Incident Response Plan	
	3. Create Quality Gates/Bug Bars	6. Perform Attack Surface Analysis/ Reduction	9. Deprecate Unsafe Functions	12. Perform Fuzz Testing	15. Conduct Final Security Review	17. Execute Incident Response Plan
	4. Perform Security and Privacy Risk Assessments	**7. Use Threat Modelling**	10. Perform Static Analysis	13. Conduct Attack Surface Review	16. Certify Release and Archive	

Microsoft Security Development Lifecycle

应用安全策略和法规

- 策略和法规
  - 安全法规
    - PCI, HIPPA, 网络安全法，密码法
  - 安全政策
    - 数据分级
    - 交易风险分级
    - 应用分级
    - 批准的加密算法和实现 (Approved Crypto & Impl
    - 批准的工具 (Approved Tools)
    - 批准的库 (Approved Libraries)
  - 安全标准和指南

应用安全培训和指南

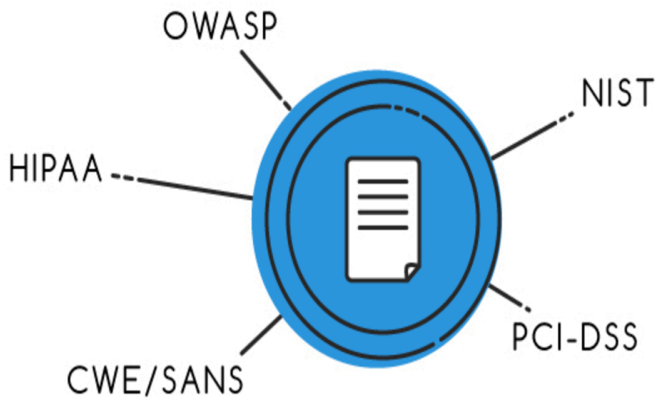
- 课程
  - 核心安全培训
  - 安全代码标准和基准
  - 不安全功能
  - 威胁建模
  - 安全设计
  - 代码检测和静态分析
  - 动态检测和入侵测试
  - 安全检测
  - 其他相关安全课程
- 培训方式

应用安全设计分析和检测

- 分析和检测
  - 安全需求
  - 风险建模
  - 安全设计
  - 同行代码检测
  - 静态分析
  - 动态分析
  - 攻击面分析
  - 关联程序库安全分析

设计检测工具与定制

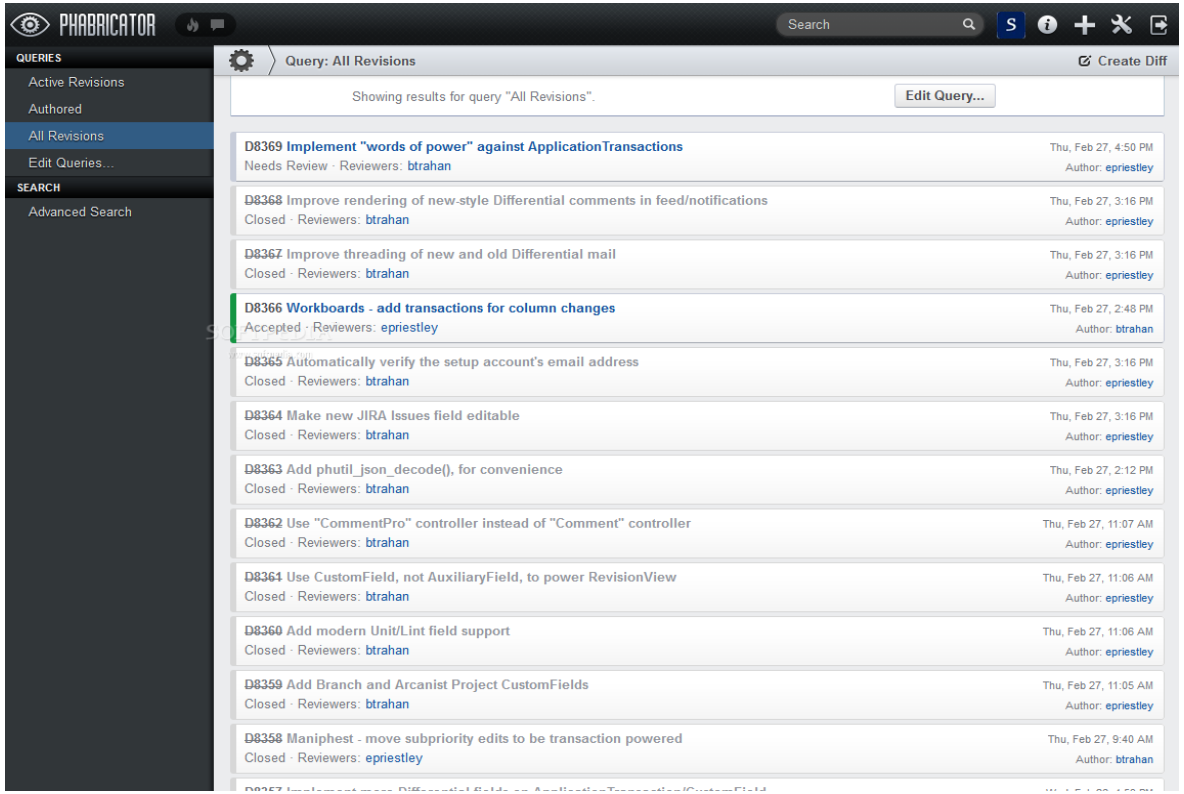
- 安全行为
  - 安全需求
  - 风险建模
  - 安全设计
- 工具
  - 应用画像 （Questionnaire/Profiling)
  - 专家系统 （应用需求设计风险）
  - 安全规则
  - 安全checklist
  - 漏洞管理
  - 整体流程集成



同行安全代码评测工具与定制

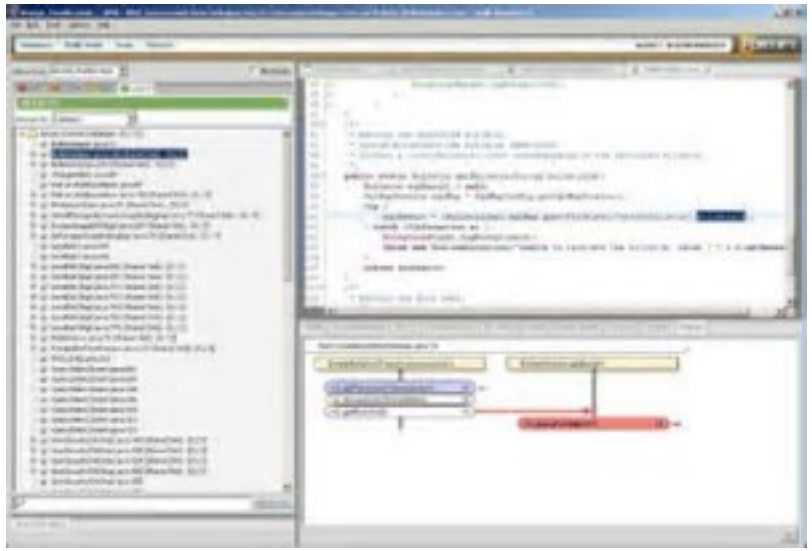
- 同行代码检测(Secure Peer Review)

PHABRICATOR



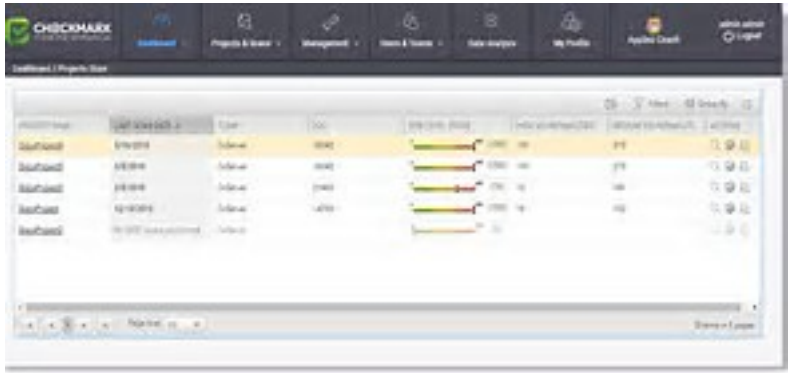
静态分析工具与定制

FORTIFY
An HP Company



扫描二进制代码，传统语言支持，传统架构，规则难改

CHECKMARX
choose what developers use



扫描源代码，新语言，新架构，规则易改

其他静态分析工具

coverity
a higher code

SYNOPSYS

codiscope

动态测试工具


AppScan
IBM Security


HP WebInspec


BURPSUITE
PROFESSIONAL

应用安全分析工具SAAS模式

VERACODE

动静态结合工具举例

- 动静态结合安全测试 Integrated Application Security Testing (IAST)
- 实时应用安全防护 Runtime Application Self-Protection (RASP)

关联程序库安全分析

Open Source Security

Find, fix and manage
open source vulnerabilities

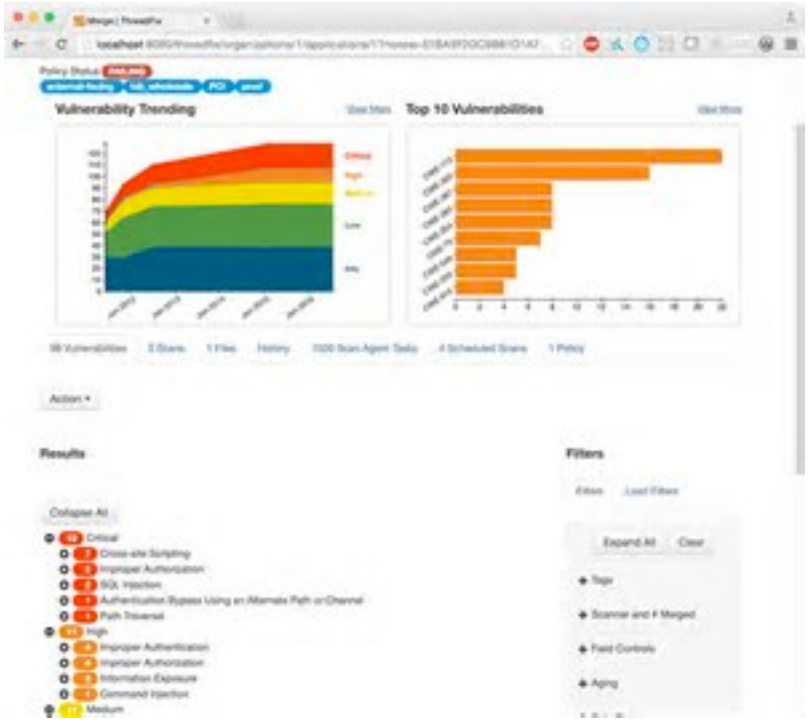
SRC:CLR

流程和管控工具与定制

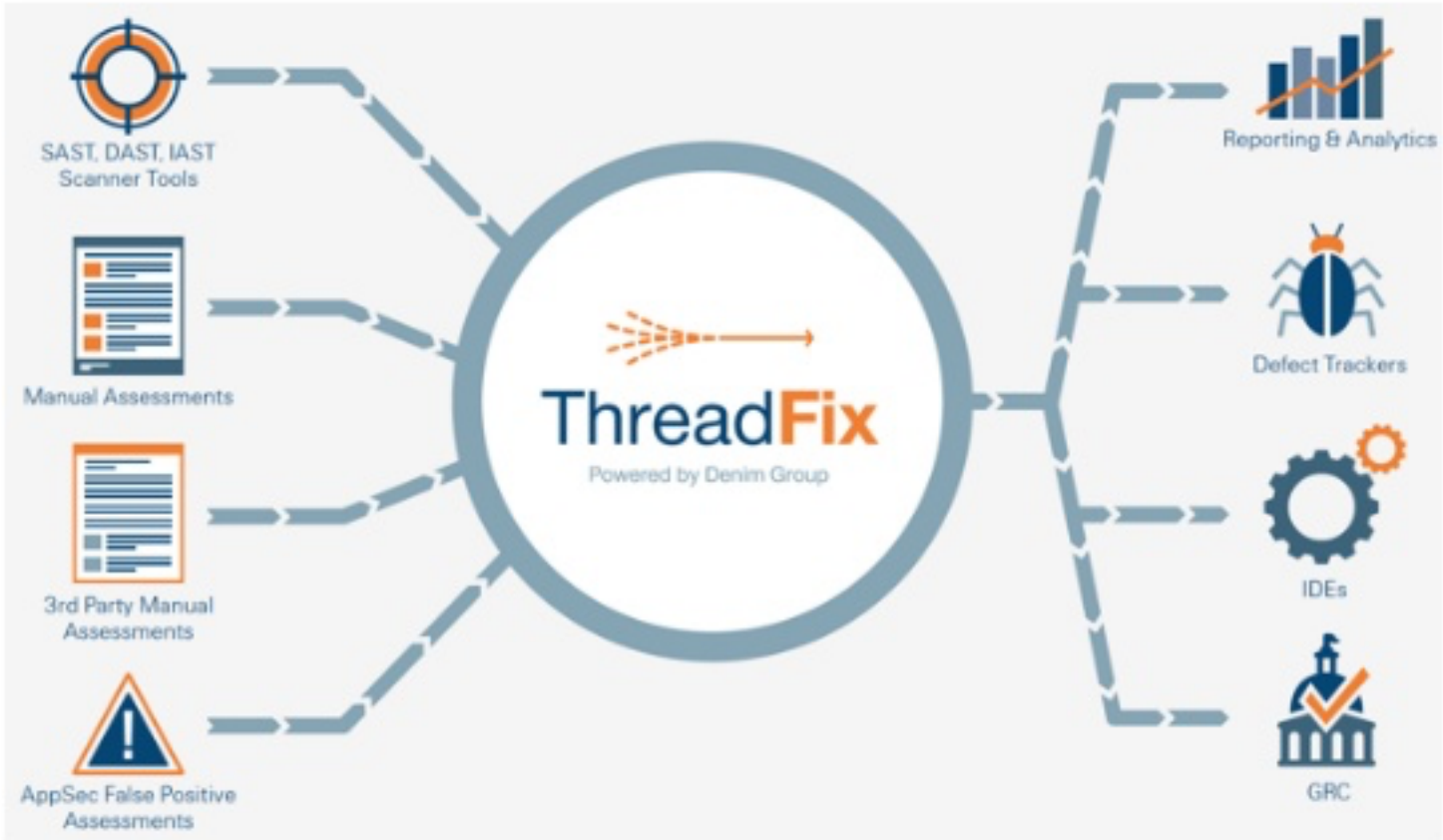
- 安全流程实现策略
- 软件开发流程集成
- 安全漏洞条
- 外部软件供应商安全规范
- 数据和报告
- 企业应用建库管理

风险分析和控制

- 风险分析
- 安全问题排级
- 企业整体安全报告
  - 实时，全面，一目了然
  - 及时调整安全策略
- 相关工具



ThreadFix Overview



DENIM GROUP

操作和执行

- 应用安全中心集中定义流程
  - Center of Excellence (COE)
- 业务线执行团队
  - Satellite Operation Teams (Application Security Champions)
- 服务和咨询
- 应急反应
- 安全自动化

应用安全新趋势

- 新技术趋势
  - 云－安全外包，数据保护，容器安全
  - 移动－认证，病毒，个人信息和隐私
  - 大数据－用户行为，信用体制
  - 人工智能 －　机器学习和深度学习
    - 发现新漏洞
    - 减低误报率
    - 降低或者替代人工分析
    - 检测异常行为和恶意攻击
    - 建立可靠的保护隐私的信用体制
    - 自动产生安全规则
    - 安全自动化

应用安全新趋势

- 挑战和机遇共存
  - 建立安全生态
  - 输出安全服务