端玛科技 Dumasoft

GooAnn gooann.com 谷安天下

谷安天下免费在线讲座系列之

《代码安全审计》

讲师：徐瑞祝

2012年7月13日

- 感谢您参加谷安天下举办的信息安全免费在线讲座系列之《代码安全审计》

关于谷安天下免费在线讲座的更多信息欢迎关注：
http://px.gooann.com/mfjz.aspx
或登录安帮网www.sec580.com消息的新帖子处关注我们活动的相关信息

您还可通过以下任一方式与我们联系，及时获得关于讲座的信息：
TEL　：010-51626887
QQ群 ： 236986704

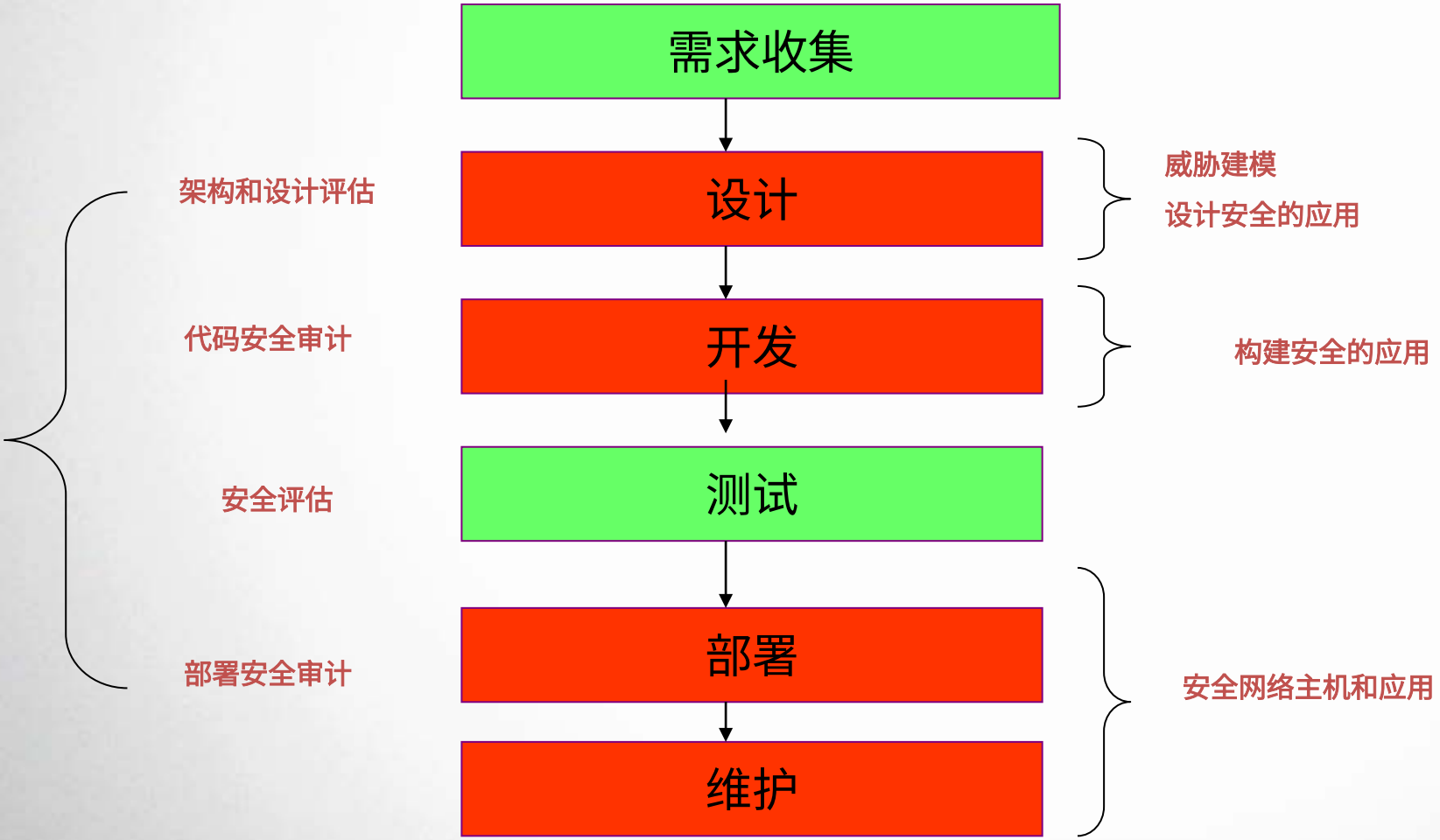
内容

- 代码审计介绍
- 代码审计的标准
- 代码审计方法
- 代码审计工具
- Checkmarx CxSuite静态源代码扫描工具介绍

代码审计介绍

- 通过分析，读源码去发现漏洞
- 为了发现实现上的漏洞和缺陷
  - 内存泄露
  - 注入型漏洞（SQL注入）
  - 错误的字符串比较
  - …

代码审计介绍



代码审计介绍

- 代码审计是一项沉闷与繁琐的工作
- 很难去估算需要的时间
- 需要对开发的语言非常熟悉
- 对开发的业务有一定的了解

代码审计的标准

- 信息安全等级保护基本要求
- 萨班斯法案
- 信息安全管理体系要求（IDT ISO/IEC27001：2005）
- 支付卡行业数据安全标准（PCI DSS）
- 电子银行业务管理办法及电子银行安全评估指引

代码审计方法

- 了解应用程序
  - 查看开发设计相关文档，大概了解业务内容
  - 检查攻击面
  - 根据攻击面，定义目标组件

选择检查点

- 用户输入数据相关的代码路径
- 安全机制
- 复杂的处理，协议，数据管理
- 提示业务比较复杂和困难的注释
- 拼写错误
- FIXME，TODO等注释
- 找到错误代码的开发人员，看在其它地方有无重现

读代码

- 要读懂一些设计复杂的代码非常困难和令人沮丧
- 要了解一个组件需要联系上下文
- 跳过一些不重要的组件
- 关注一些重点：
  - 拷贝或移动数据
  - 执行输入/输出验证
  - SQL语句拼接
  - 硬编码
  - 使用未初始化变量

代码审计工具

- 编辑查看代码的工具
  - 跟踪变量在哪里定义
  - 跟踪方法在哪里被实现
  - 方法的调用点
  - 搜索
  - Source Navigator, Eclipse, Source Insight,VSS
- 模式匹配工具
- 静态源代码扫描工具
- 渗透测试工具

Checkmarx CxSuite静态源代码扫描工具介绍

- Checkmarx CxEnterprise静态源代码安全漏洞扫描和管理工具是以色列Checkmarx 公司在分析全球静态分析技术的优缺点后,结合全球安全组织和安全专家多年的软件安全咨询的经验而研发出的新一代源代码安全扫描方案,旨在从根源上识别、跟踪和修复源代码的技术和逻辑上的安全缺陷。该方案独创以查询技术定位代码安全问题,克服了传统静态分析工具误报率（False Positive）高和漏报（False Negative）的缺陷.
- 主要提供的功能:
  - 源代码安全漏洞的扫描、结果分析和管理
  - 源代码技术和逻辑缺陷调查、分析及规则自定义。
  - 扫描团队和用户权限管理
  - 扫描自动化及任务调度管理
  - 私有/公有虚拟云服务

主要客户

- 部分主要客户
  - 中国信息安全认证中心
  - 中国信息安全测评中心
  - 北京市信息安全测评中心
  - 清华大学
  - 北京大学
  - 武汉大学
  - 北京邮电大学
  - 上海市信息安全测评中心
  - 上海软件测评中心
  - 国家电力科学研究院
  - 华为
  - 国家开发银行
  - 深圳大运会
  - 国家信息技术研究中心

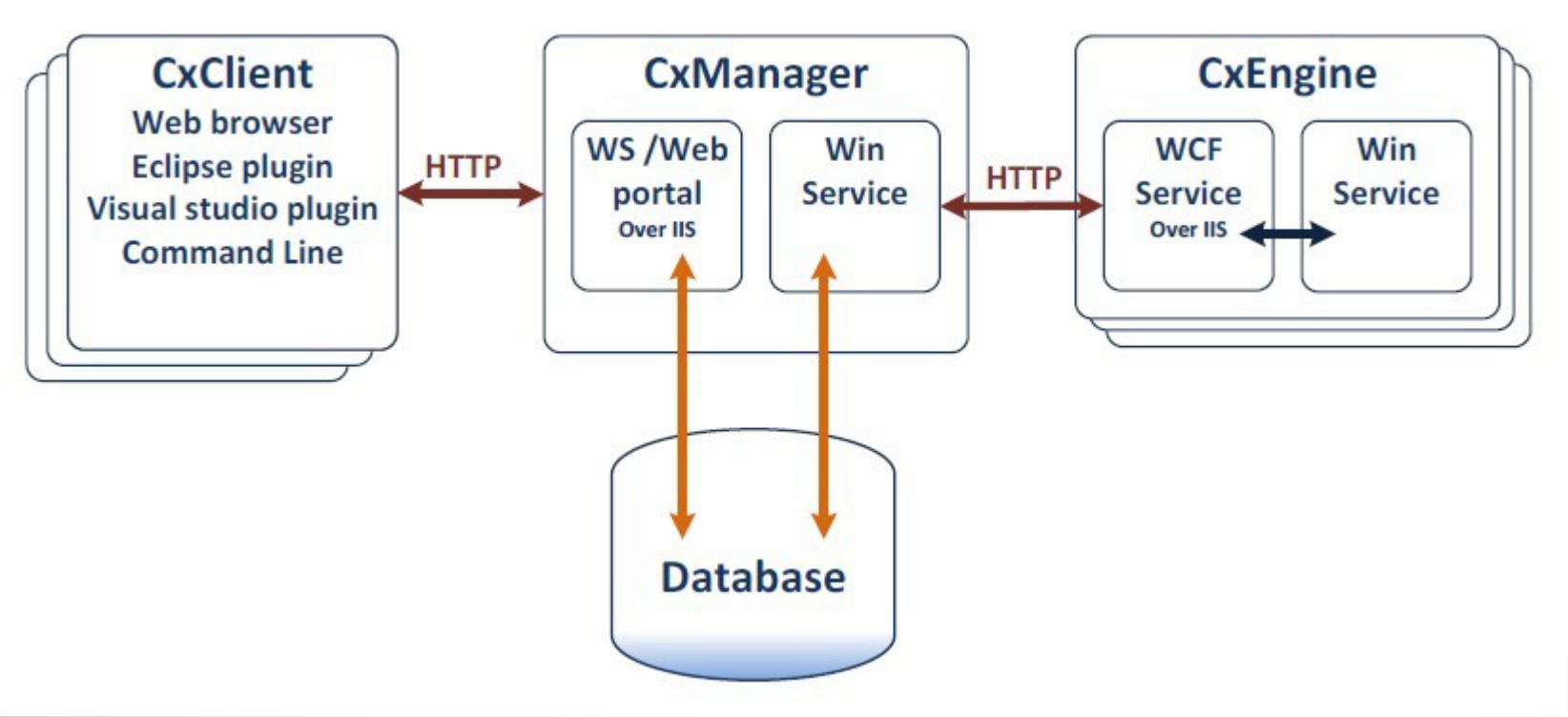
15.04.2010 Checkmarx Named "Cool Vendor" by Leading Analyst Firm-Gartner

- Checkmarx Cxsuite其无与伦比的准确性和方便的企业部署和实施的特性赢得了全球众多客户的青睐。比如Salesforce.Com、道琼斯（新闻集团）、雅高、NDS公司、美国陆军、阿姆多克斯等都在采用这种新一代的静态分析技术做源代码安全检测和风险评估。至今，Checkmarx的客户量数目庞大，其中包括涉及电信、金融银行、保险、汽车、媒体娱乐、软件、服务和军事等行业的财富1000的企业。2010年4月15日Checkmark被全球领先的行业分析公司Gartner评为“2010年度最酷应用安全供应商”
- “ Checkmarx is the first code analysis company that can inspect and summarize application security risk quickly, non-intrusively and with tremendous accuracy 。 ”
  - 摘自Gartner “ Cool Vendors in Application Security, 2010”报告。

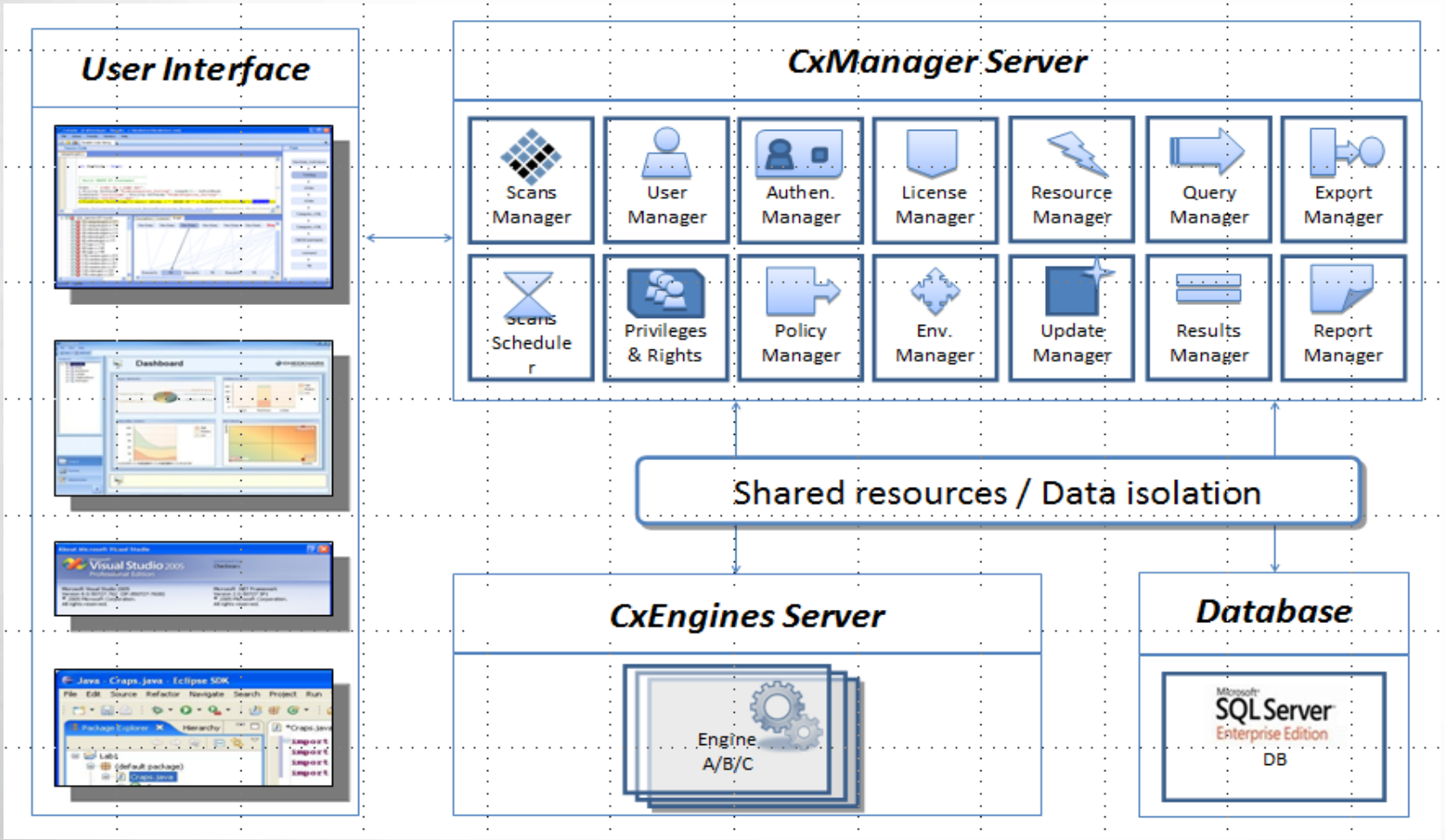
Checkmarx CxEnterprise 产品的基本组件

- CxScanEngine
  - CxScanEngine安装在指定的服务器上，引擎服务负责扫描和查询的任务。
- CxManager
  - CxManager安装在指定的服务器上，负责管理用户、项目、扫描任务等。
  - CxManager 与 CxScanEngine 通信。
- CxClient
  - 轻量级的客户端组件，安装在客户端的机子上。
  - CxClient 通过WCF 与 CxManager 通信。
- CxWebPortal
  - CxManager的一个Web方式的客户端，用以替换CxClient.

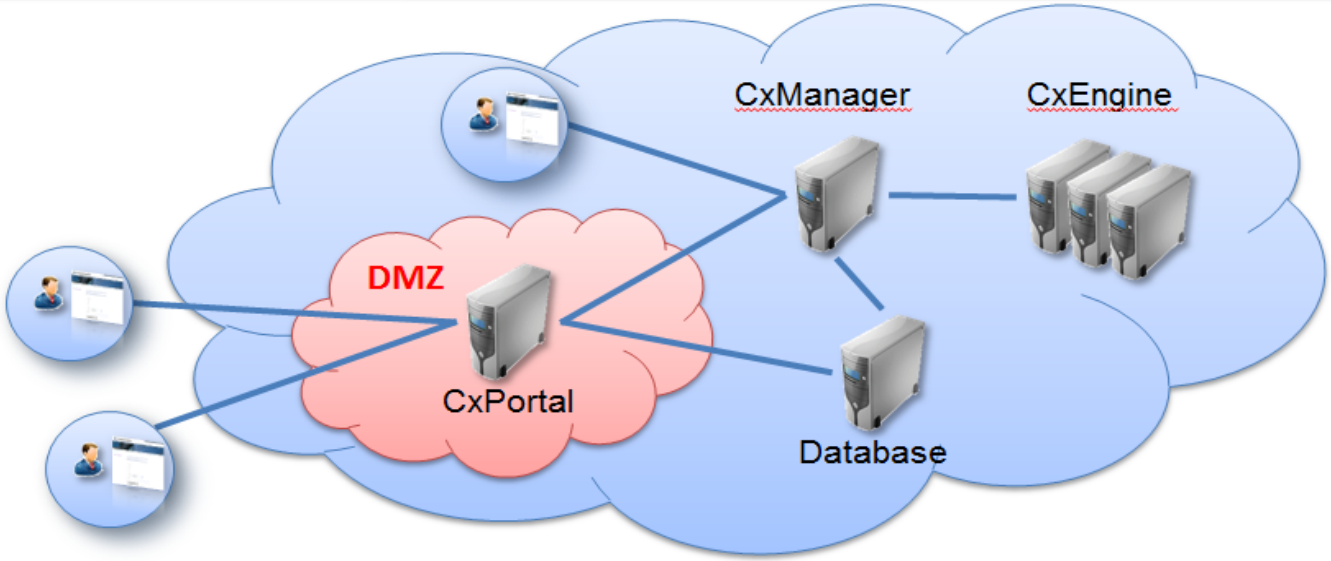
Checkmarx CxEnterprise 产品的基本组件



Checkmarx CxEnterprise 的基本架构（C/S）



Checkmarx CxSuite CxEnterprise Portal 架构



Manager Server's specification:

RAM	4 GB
Processor	Dual Core
Hard Disk	250GB
OS	Win Server 2008
Software	.Net 3.5 SP1, IIS7

Database Server's specification:

RAM	4 GB
Processor	Dual Core
Hard Disk	100GB
OS	Win Server 2008
Software	SQL Server 2008[*]

[*] Management Studio is required

Engine Server's specification[*]:

RAM	32 GB
Processor	8 Core s
Hard Disk	250GB
OS	Win Server 2008
Software	.Net 3.5 SP1, IIS 7

[*] Allowing 8 concurrent scans of 500K LoC projects

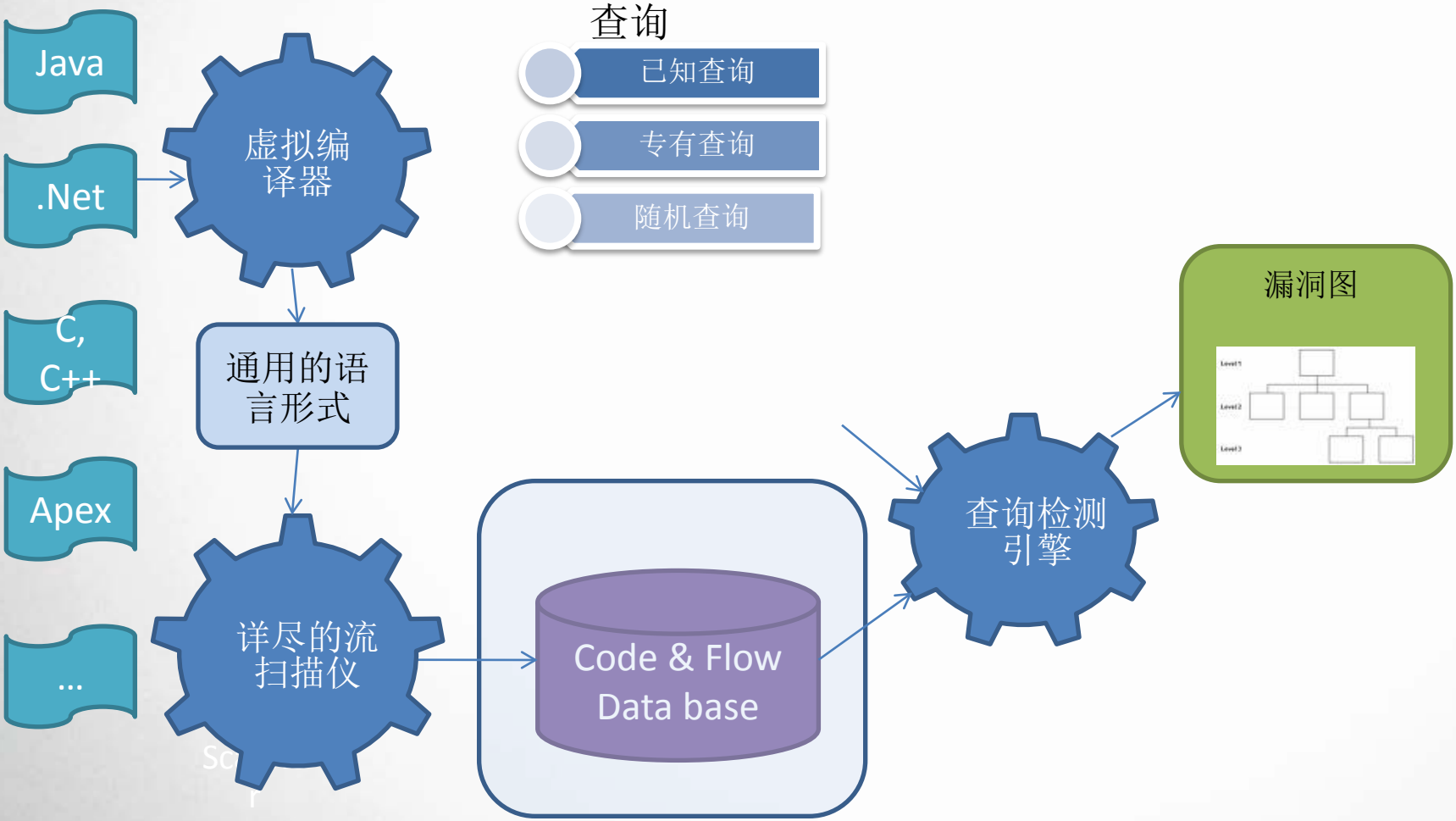
Portal Server's specification:

RAM	4 GB
Processor	Dual Core
Hard Disk	250GB
OS	Win Server 2008
Software	.Net 3.5 SP1, IIS 7

CxEnterprise 客户端的访问形式

- *CxClient*
- Web *browser*
- Eclipse plugin and Visual Studio

Checkmarx Cxenterprise 静态源代码扫描原理



Checkmarx CxSuite 产品演示

- Checkmarx CxEnterprise （C/S）演示
  - 角色介绍、创建和权限管理
  - 客户端远程登录到服务器
  - 扫描项目和扫描任务的建立
  - 报表生成。
  - 查询规则的自定义。
- Checkmarx CxEnterprise Portal Base（B/S）演示

Checkmarx CxSuite 主要功能及特性

- 操作系统独立
  - CxEnterpris企业服务下的代码扫描不依赖于特定操作系统，只需在在企业范围内部署一台扫描服务器，就可以扫描其它操作系统开发环境下的代码，包括但不限于如下操作系统Windows、Linux 、AIX，HP-Unix, Mac OS, Solaris。
  - 不需要购买额外的硬件服务器和操作系统- Linux 、AIX，HP-Unix, Mac OS, Solaris
- 编译器独立、开发环境独立，搭建测试环境简单快速且统一
  - 由于采用了独特的虚拟编译器技术，代码扫描不需要依赖编译器和开发环境，无需为每种开发语言的代码安装编译器和测试环境，只需要通过CxClient登录到CxManager Application服务器，提供本地代码扫描代码的目录、远程代码目录、和版本管理代码目录（Subversion、CVS，ClearCase即可，扫描代码无需通过编译过程。搭建测试环境快速简单，无需像其它的静态分析工具，必须在相应的操作系统上安装相应的工具软件包，安装众多开发工具和代码依赖的第三方库及软件包、调试代码通过编译，方可进行测试。CxSuite CxEnterprise安装一次，即可扫描Java代码、C/C++代码、.NET代码JSP、JavaSript 、VBSript、 .、C# 、 ASP.net 、VB.Net、 VB6、 、ASP 、Apex Visual Force 、PHP … 等各种语言代码，并且不管这些代码是在windows平台、Linux平台或者其它平台的
  - 无需购买各种语言的开发环境和编译器,大大节约试验室扫描代码环境的搭配.
- 工具学习、培训和使用的成本少，最小化影响开发进度：
  - 由于编译器、操作系统和开发环境独立，使用者无需去学习每种平台下如何去编译代码，调试代码、如何扫描测试代码，无需去看每种平台下繁琐的使用手则。因为Checkmarx CxEnterprise服务只需要提供源代码即可扫描，并给出精确的扫描结果

Checkamrx CxSuite 主要功能及特性(续)

- 低误报:
  - CxSuite 企业服务在扫描过程中全面分析应用的所有路径和变量。准确的分析结果，验证可能的风险是否真正导致安全问题，自动排除噪音信息，扫描结果几乎就是最终的分析结果，其误报率（False Positive）几乎为零。极大的减少了审计分析的人工劳动成本，极大的节省了代码审计的时间，为开发团队赢得更多的开发时间。
- 安全漏洞覆盖面广且全面 (低漏报):
  - 数以百计的安全漏洞检查适合任于何组织，支持最新的OWASP 、CWE、SANS、PCI、SOX等国际权威组织对软件安全漏洞的定义。漏洞覆盖面广，安全检查全面，其自定义查询语言CxQL可以让用户灵活制定需要的代码规则，极大的丰富组织特定的代码安全和代码质量的需要 。

Checkamrx CxSuite 主要功能及特性(续)

- 安全查询规则清晰且完全公开实现：
  - 规则定义清晰，并完全公开所有规则的定义和实现让用户清楚知道工具如何去定义风险、如何去查找风险，透明各种语言风险。让用户知道工具已经做了那些工作，没有做那些该工作。而不是给用户一个黑匣子，用户无法了解工具的细节和缺陷，无法在代码审计过程中规避工具的风险（比如漏报和误报），比如利用人工或者其它手段查找工具不能定位的问题。
  - 可以移植该工具库的知识到其他工具里去,完善其他工具的能力
- 安全规则自定义简单高效
  - 由于公开了所有规则实现的细节和语法，用户可以快速修改规则或者参考已有的规则语句自定义自己需要规则，规则学习，定义简单高效。能快速实现组织软件安全策略。
  - 可以累积试验室的安全研究成果,把实验室的成果转换成查询规则,然后用自动化的方式去验证试验室的安全知识对实际系统的应用情况.

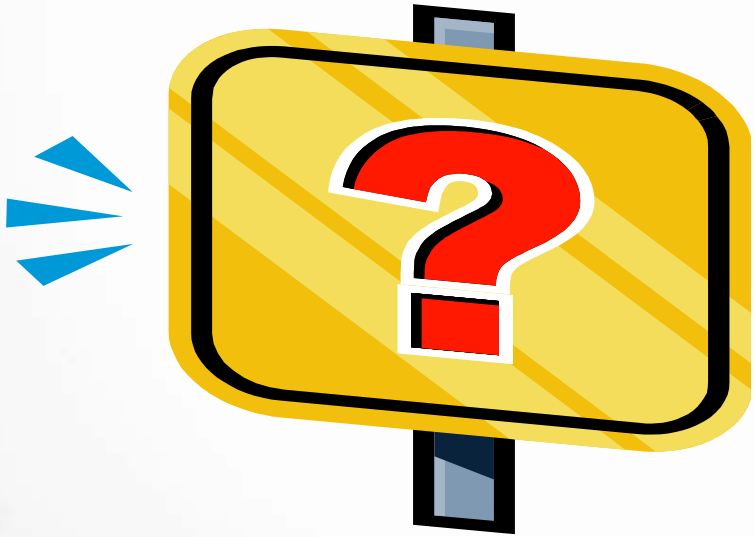
Checkamrx CxEnterprise 主要功能及特性(续)

- 业务逻辑和架构风险调查:
  - Checkmarx CxSuite服务可以对所有扫描代码的任意一个代码元素（词汇）做动态的数据影响、控制影响和业务逻辑研究和调查。分析代码逻辑和架构特有的安全风险，并最后定义规则精确查找这些风险。这是目前**唯一能动态分析业务逻辑和软件架构的静态技术**。
- 服务独立，全面的团队扫描支持
  - 作为服务器运行。开发人员、管理人员和审计人员都可以凭各自的身份凭证从任何一处登录服务器，进行代码扫描、安全审计、团队、用户和扫描任务管理。
- 高度自动化扫描任务
  - 自动集成版本管理（SubVersion、CVS、ClearCase、TFS）、SMTP邮件服务器和Windows账户管理，实现自动扫描代码更新、自动扫描、自动报警和自动邮件通知…等

Checkamrx CxEnterprise 主要功能及特性(续)

- Checkmarx CxSuite目前支持主流语言
  - Java、JSP、JavaSript、 VBSript、 .NET 、C# 、 ASP.net 、VB.Net、VB6、 C/C++ 、ASP 、Apex 、VisualForce、 PHP， API to 3rd party languages
- 支持的主流框架（Framework）
  - Struts 、Spring、Ibatis、GWT、Hiberante 、Enterprise Libraries、Telerik 、ComponentArt 、Infragistics、 FarPoint ， Ibatis.NET、Hibernate.Net [*] 、MFC，并可针对客户特定框架快速定制支持。
- 支持多任务排队扫描、并发扫描、循环扫描、按时间调度扫描。
- 云服务实现：支持跨Internet实现源代码安全扫描“云服务”

Q&A

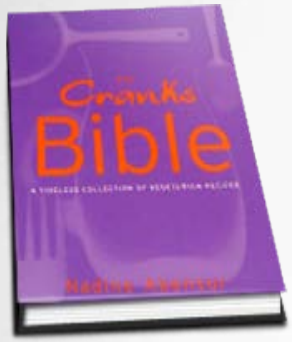


附：谷安天下安全开发框架

需求分析	设计	开发编码	测试	实施上线
•业务安全分析 •隐私安全分析 •合规性分析 •业务安全建模 •需求评审	•威胁建模 •攻击面分析 •系统安全建模 •设计评审	•安全编码培训 •安全编码规范 •Peer Code Review •静态代码分析 •单元测试 •代码评审	•测试用例评审 •单元测试 •集成测试 •系统功能测试 •可接受性测试 •静态代码分析 •模糊测试 •渗透测试 •代码动态分析 •错误注入测试 •测试评审	•用户安全意识培训 •系统安全管理与操作培训 •临时账户管理 •系统安全交付 •数据安全迁移 •上线评审

安全开发管理（配置安全管理 漏洞管理 安全培训管理，……）

附：谷安天下安全信息系统安全开发服务介绍



安全开发咨询

现场指导客户进行安全需求分析，安全设计，安全开发，安全测试，以及安全实施上线，实施相关培训，建立各种相关规章制度，体系文档以及内在持续改进机制。为客户建立起全面的安全开发管理体系

安全开发培训

全方位的安全开发培训服务，为客户建立起完备的安全开发能力，包括安全意识培训，安全编码培训，黑客技能培训，渗透测试培训……

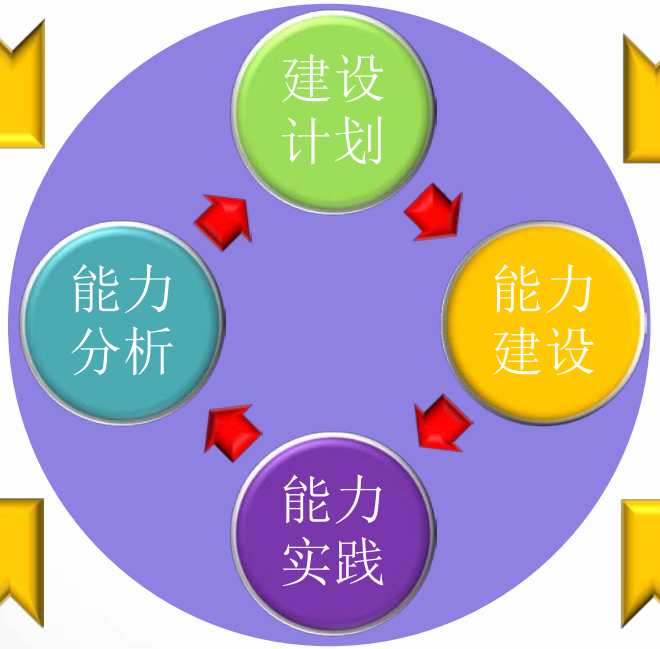
安全开发技术服务

为客户实施各种安全测试和代码审计服务，如渗透测试，模糊测试，代码动态分析等，为客户解决人才短缺，知识储备不足，花费昂贵等问题

附：安全开发咨询服务实施办法与指导原则

实施过程

安全开发现状调研 → 全面风险评估与差距分析 → 安全开发体系架构设计 → 安全开发体系建立 → 体系试运行 → 后续跟进持续改善



完善的指导文档

资深顾问现场咨询辅导

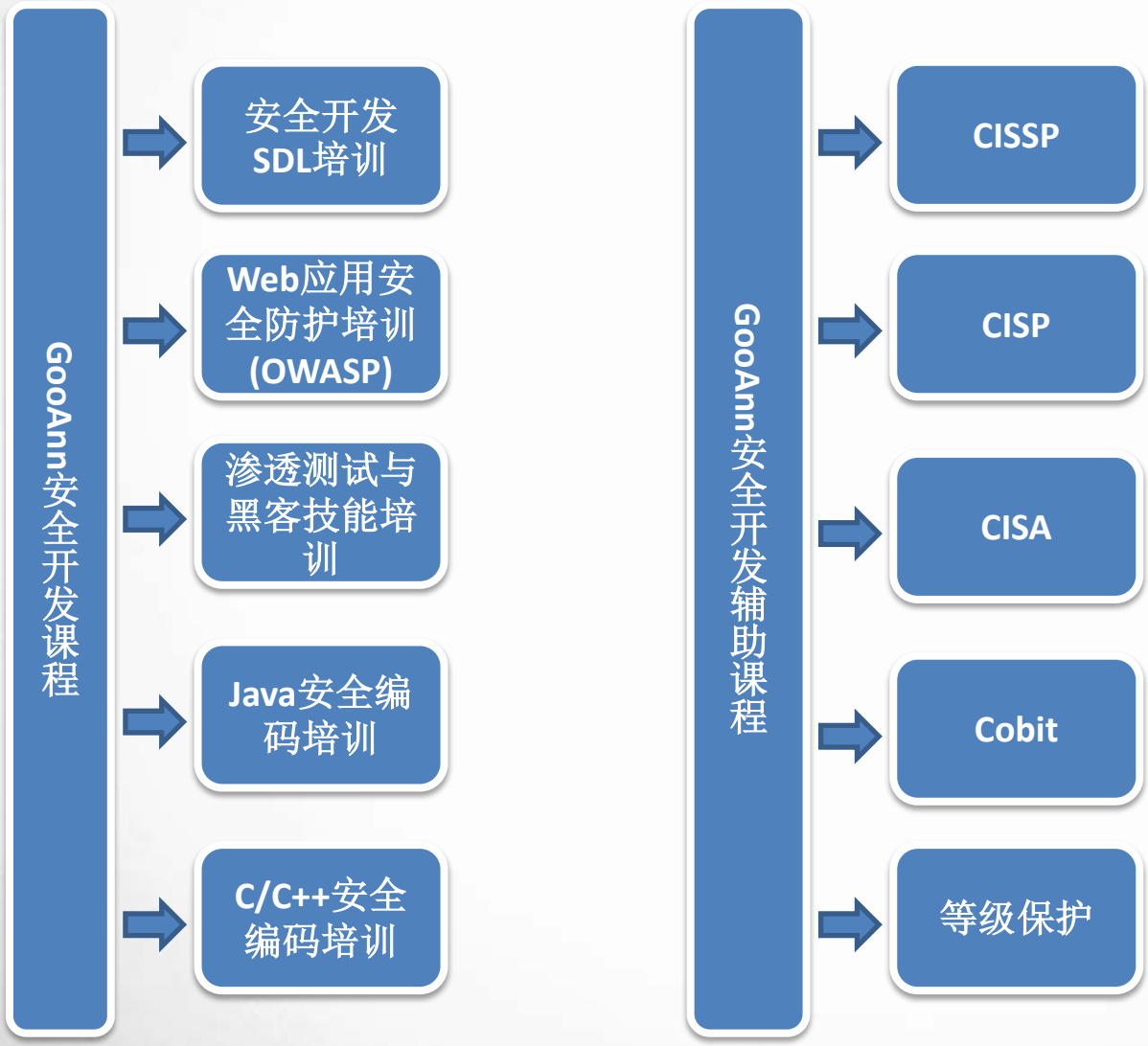
全方位安全意识、技能与工具培训

保障能力建设准则
循序渐进
持续改进

持续支持

附：咨询成果交付

附：谷安天下安全开发培训服务－课程体系



附：谷安天下安全开发技术服务