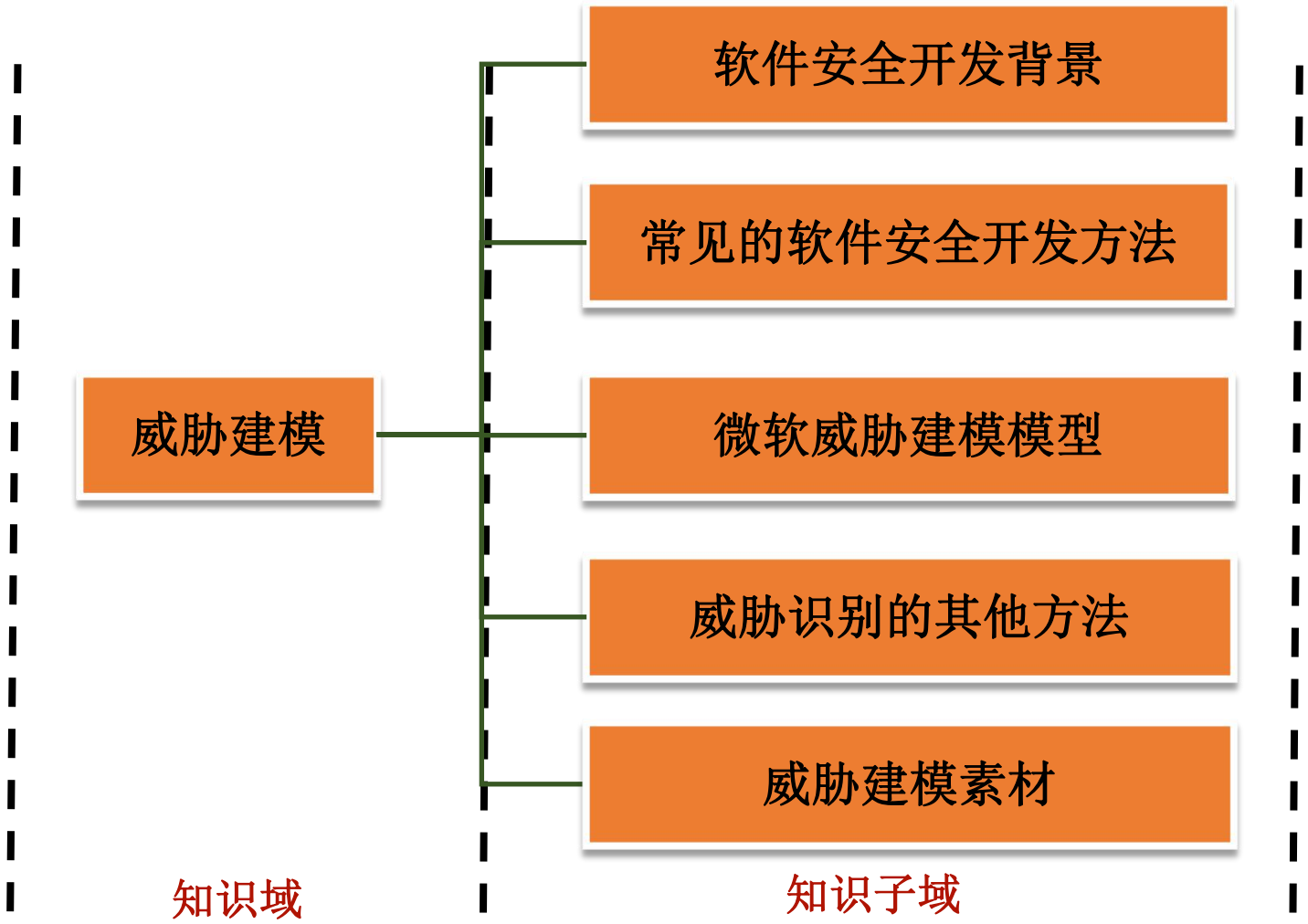
默安科技
企业信赖的安全伙伴

金融行业SDL之威胁建模实践

2020年03月27日

课程内容


威胁建模
软件安全开发背景
常见的软件安全开发方法
微软威胁建模模型
威胁识别的其他方法
威胁建模素材
知识域
知识子域

软件发展和安全问题

默安科技
企业信赖的安全伙伴

Shellshock

2014年9月，破壳漏洞首次爆发，由于没有在输入的过滤中没有严格限制边界且没有做合法化参数判断，导致在Linux等操作系统上被远程执行任意命令。包括但不限于：redhat、centos、ubuntu等平台。

系统软件问题

OWASP TOP10

自2011年以来，网上陆续披露出一些信息系统的安全漏洞，导致大量信息泄露。造成这一系列安全问题的原因是在开发过程中缺乏安全知识，导致开发出的系统存在SQL注入、密码重置、XSS等漏洞。

应用软件问题

第三方代码安全

2014年OpenSSL1.0.1-1.0.2-beta1版本发现Heartbleed心脏出血漏洞，该漏洞会暴露https服务器64KB的内存明文信息。同年7月，Struts2漏洞爆发，利用该漏洞，攻击者可对服务器进行远程命令执行。

第三方代码安全

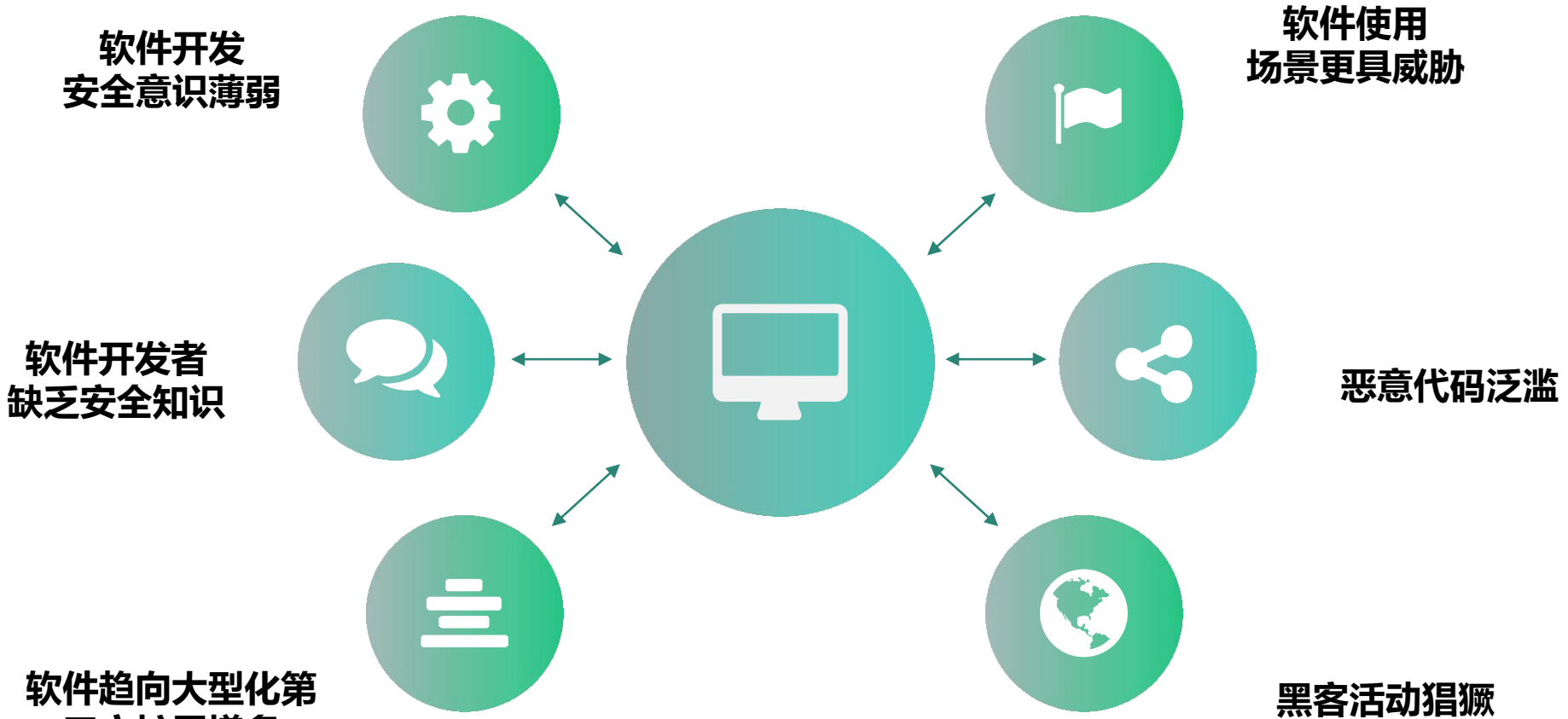
新技术安全问题

在工业生产领域，传统的工业控制系统（ICS）逐渐向网络化转变，黑客、病毒等威胁也随之像ICS扩展。如Stuxnet病毒入侵伊朗布什尔核电站，严重影响到核反应堆的正常运行。

新技术安全

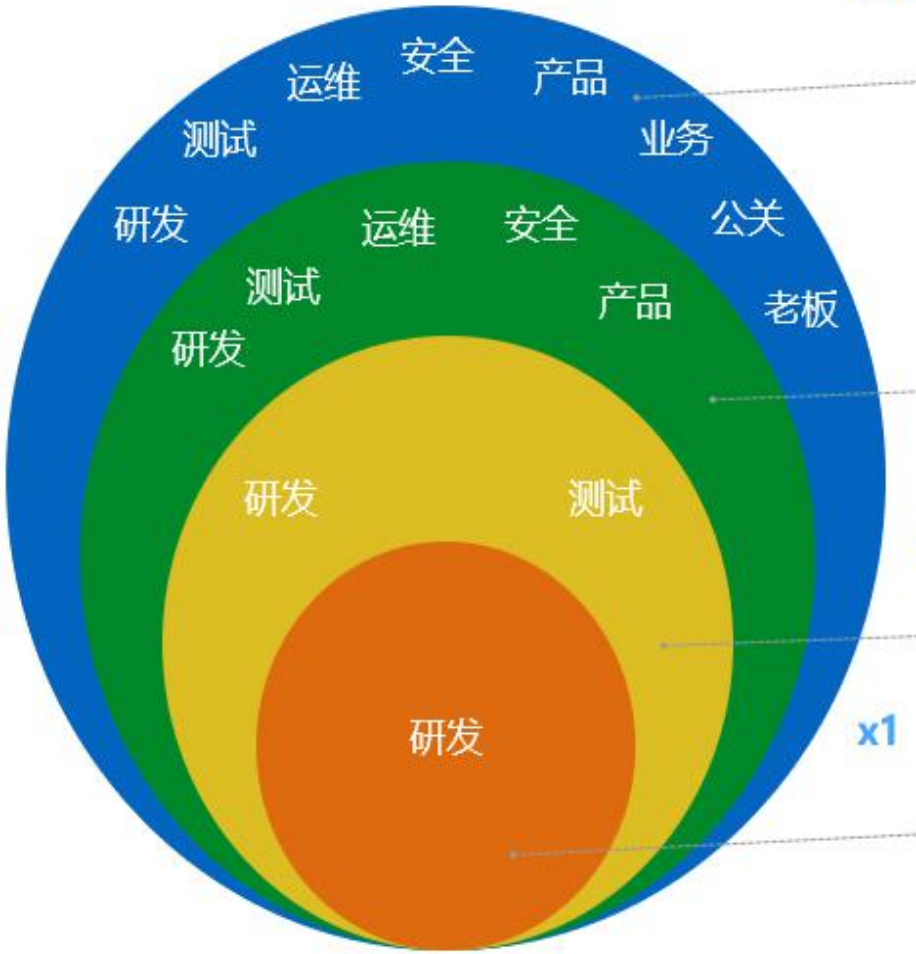
软件安全问题产生的原因

默安科技
企业信赖的安全伙伴



漏洞修复的成本

默安科技
企业信赖的安全伙伴



运行阶段

运行一段时间后，被白帽子报告发现的漏洞，需要付出额外的金钱，沟通成本高，需要再安全FIX的时间，需要运维，发布的介入，修复成本成倍数的上升，给企业带来相当大的风险和成本压力。

发布阶段

发布到线上后检测出的漏洞，需要安全人员给出方案，与研发人员沟通，由测试人员验证，也需要承受一定可能性的线上风险，相对成本较高。

测试阶段

测试阶段发现的漏洞，由测试提交给研发，需要一定的沟通成本，相对来说FIX的效率较高。

研发阶段

研发阶段发现的漏洞可以由开发直接FIX，成本底，效率高。

软件安全开发方法

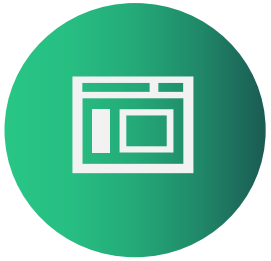
默安科技
企业信赖的安全伙伴

SDL

安全开发生命周期

BSI

内建安全



BSIMM

软件安全构建成熟度模型

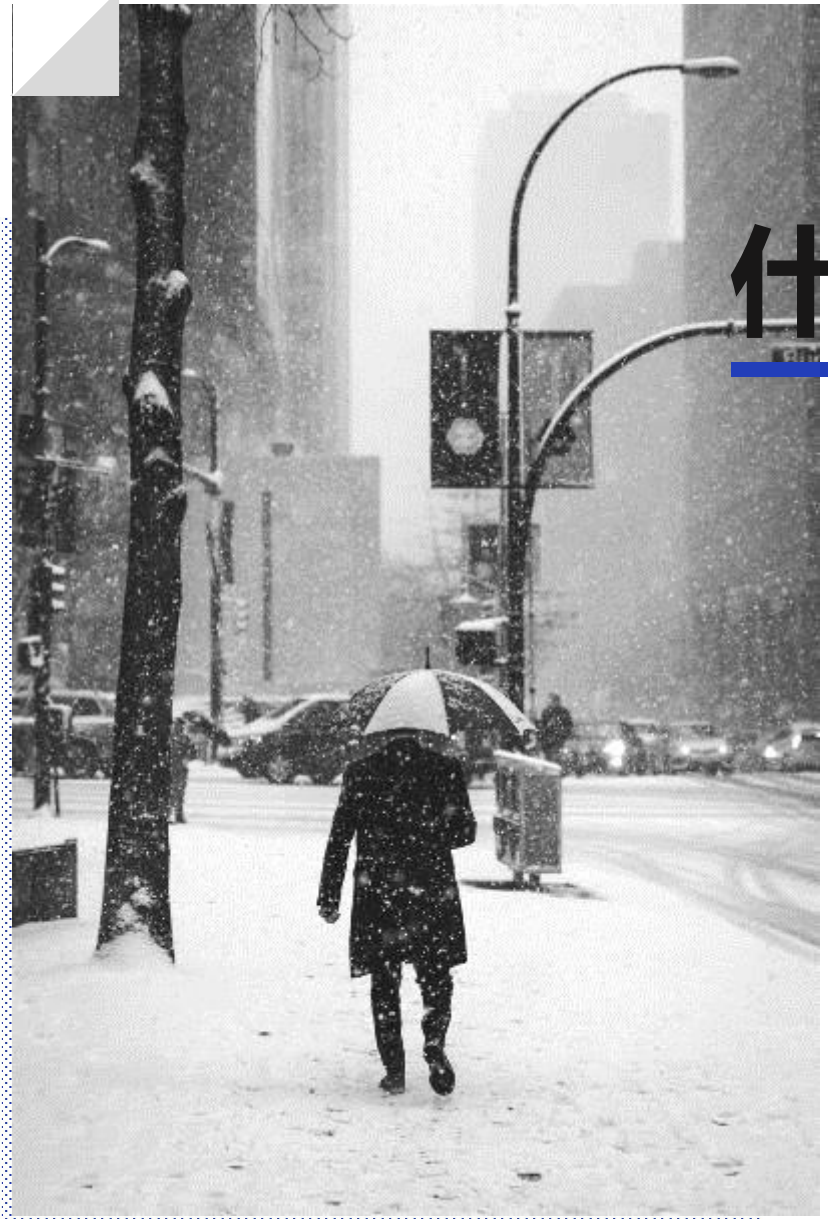
SAMM

软件保障成熟度模型

CLASP

综合的轻量应用安全过程

默安科技
企业信赖的安全伙伴



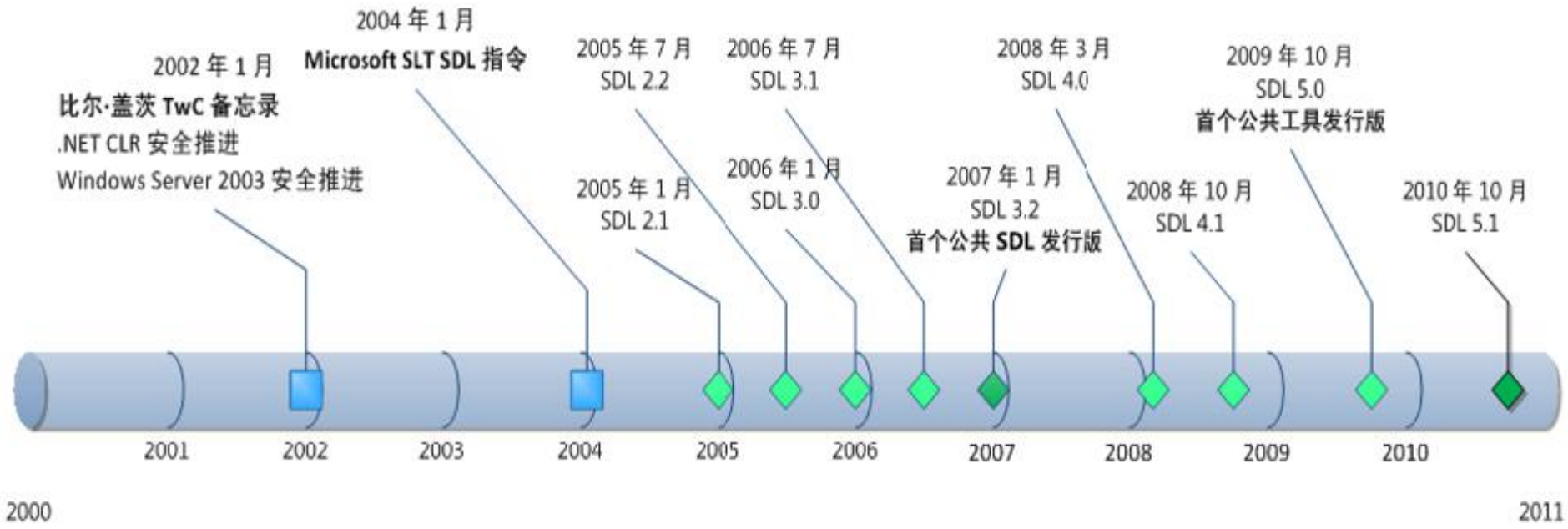
什么是SDL

Security Development Lifecycle

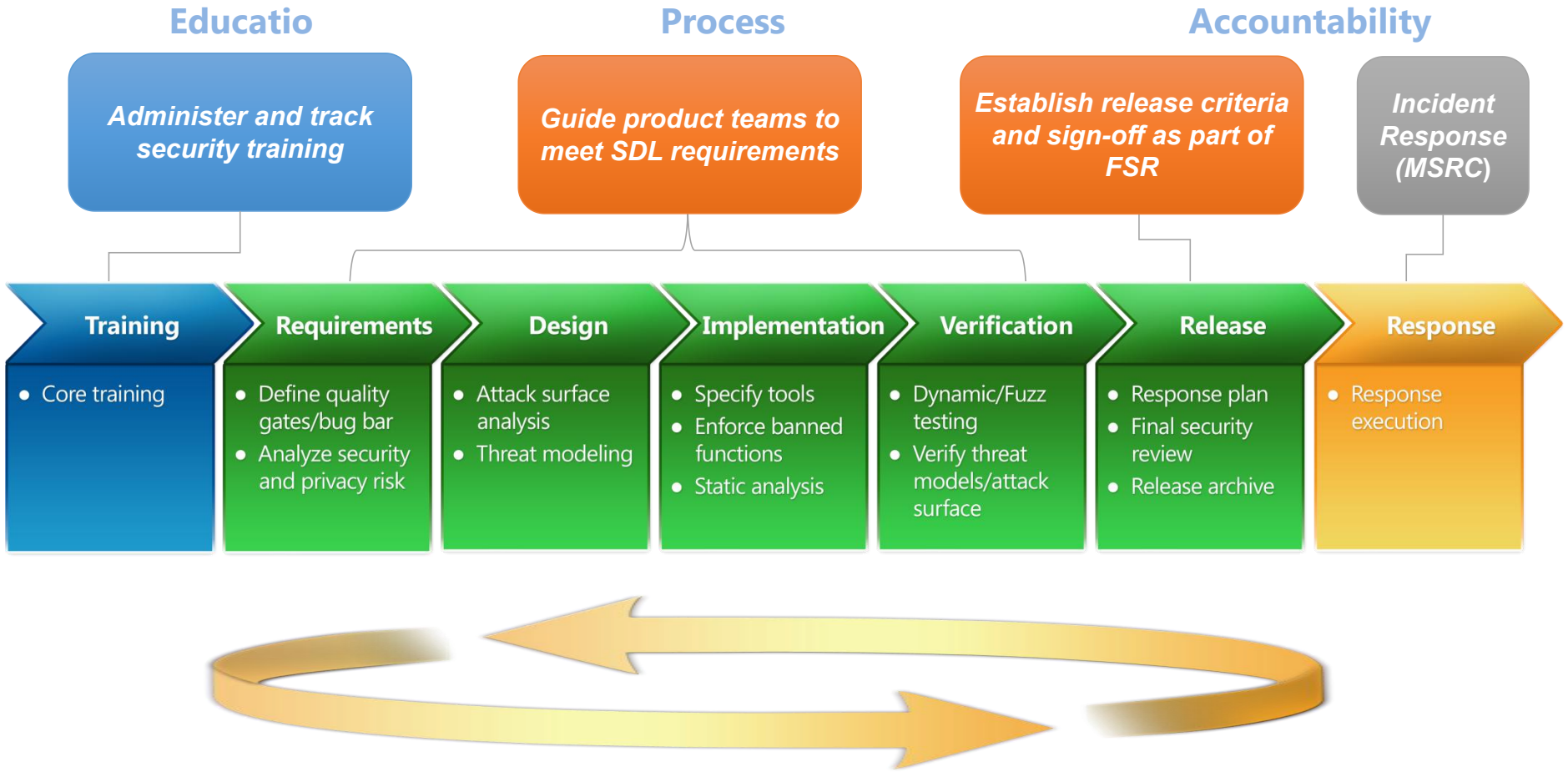
SDL是微软提出的从安全角度指导软件开发过程的管理模式。 是将设计、代码和文档等安全相关漏洞减到最少，在软件开发的生命周期中尽可能的早得发现并解决相关漏洞建立的流程框架；为了实现保证最终的用户安全，在软件开发各阶段中引入针对项目安全和用户隐私问题的解决方案。

帮助软件研发类企业在产品研发过程中减少产品的安全问题，并通过方法实践从每个阶段提高产品的整体安全级别。

微软SDL发展历史

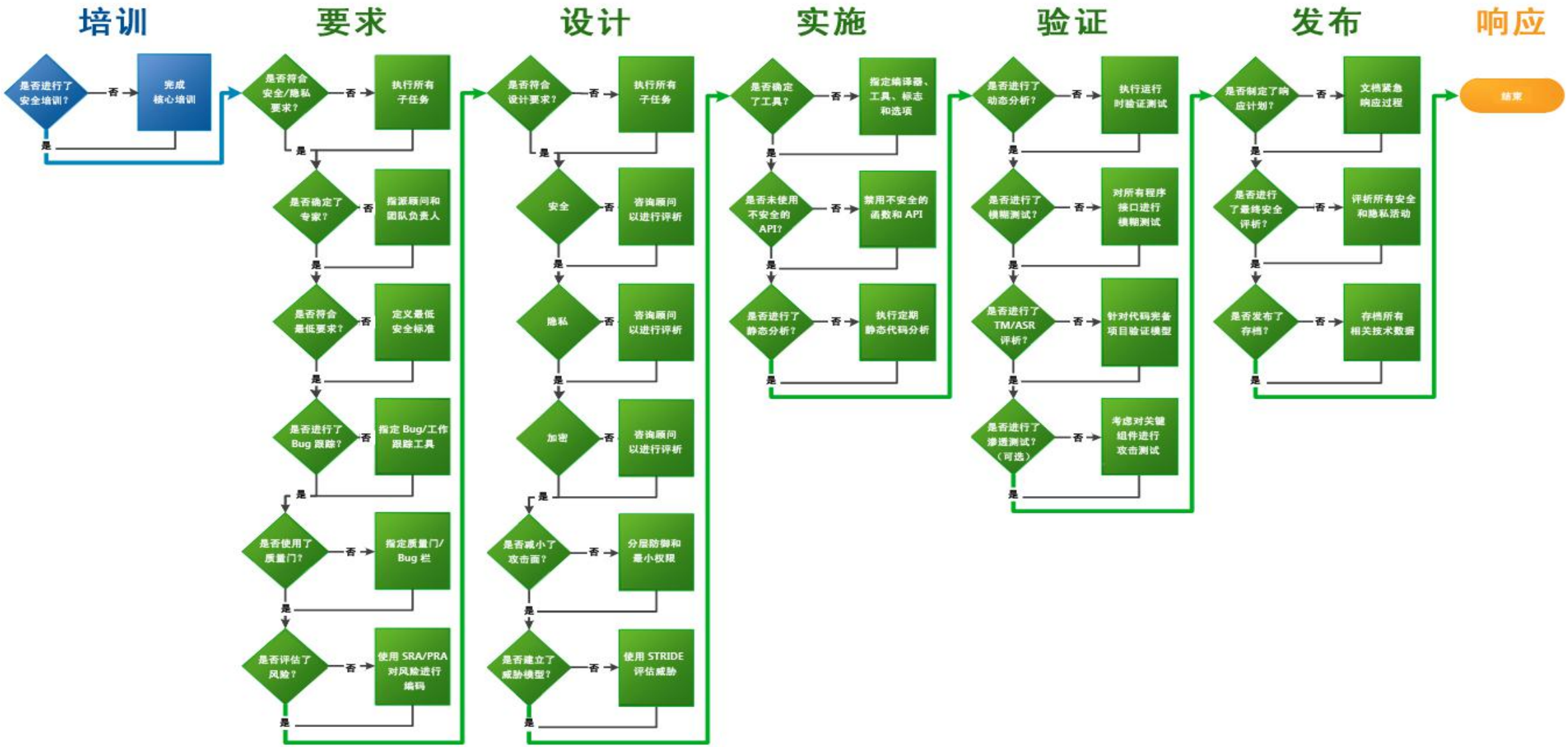

2002 年 1 月
比尔·盖茨 TwC 备忘录
.NET CLR 安全推进
Windows Server 2003 安全推进
2004 年 1 月
Microsoft SLT SDL 指令
2005 年 7 月
SDL 2.2
2006 年 7 月
SDL 3.1
2008 年 3 月
SDL 4.0
2009 年 10 月
SDL 5.0
首个公共工具发行版
2005 年 1 月
SDL 2.1
2006 年 1 月
SDL 3.0
2007 年 1 月
SDL 3.2
首个公共 SDL 发行版
2008 年 10 月
SDL 4.1
2010 年 10 月
SDL 5.1
2000
2001
2002
2003
2004
2005
2006
2007
2008
2009
2010
2011

微软SDL安全活动



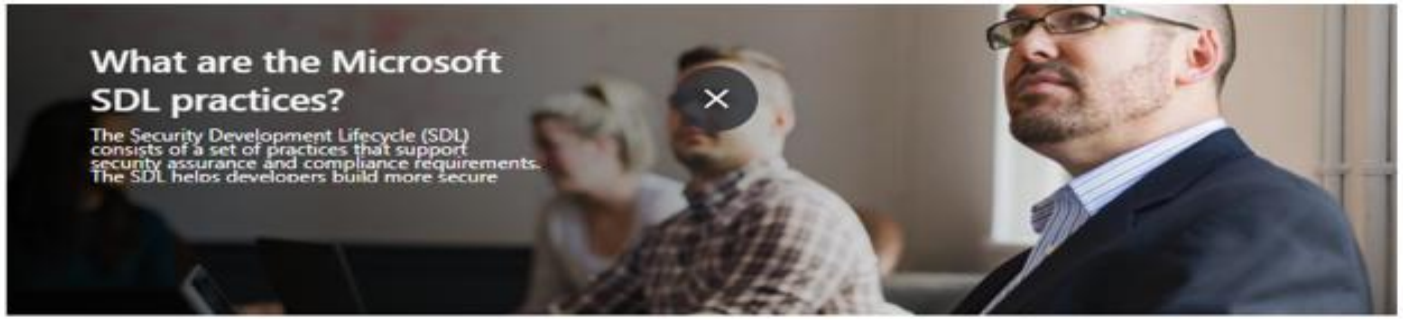
微软SDL实施流程

默安科技
企业信赖的安全伙伴



微软SDL最新活动

默安科技
企业信赖的安全伙伴



Provide Training
Ensure everyone understands security best practices.
Learn more >

Define Security Requirements
Continually update security requirements to reflect changes in functionality and to the regulatory and threat landscape.
Learn more >

Define Metrics and Compliance Reporting
Identify the minimum acceptable levels of security quality and how engineering teams will be held accountable.
Learn more >

Perform Threat Modeling
Use threat modeling to identify security vulnerabilities, determine risk, and identify mitigations.
Learn more >

Establish Design Requirements
Define standard security features that all engineers should use.
Learn more >

Define and Use Cryptography Standards
Ensure the right cryptographic solutions are used to protect data.
Learn more >

Manage the Security Risk of Using Third-Party Components
Keep an inventory of third-party components and create a plan to evaluate reported vulnerabilities.
Learn more >

Use Approved Tools
Define and publish a list of approved tools and their associated security checks.
Learn more >

默安科技
企业信赖的安全伙伴

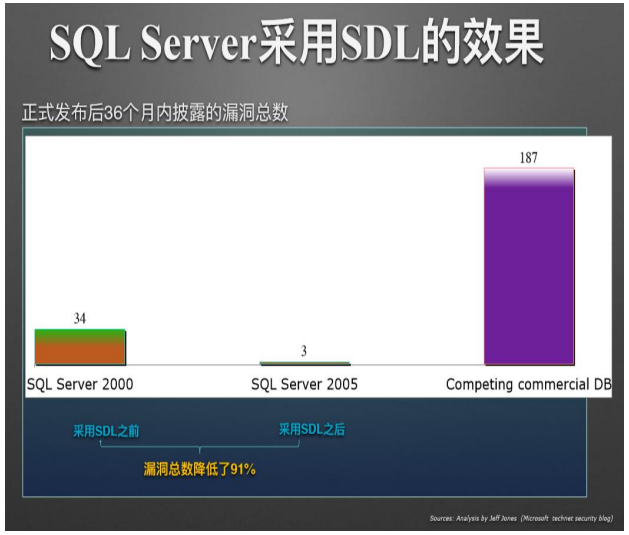
微软SDL实施效果

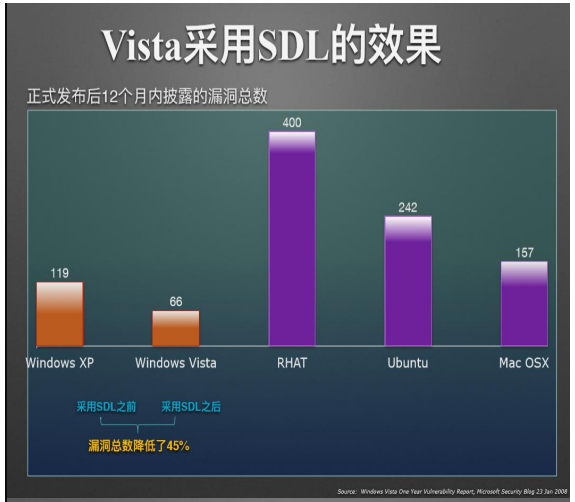
在全部已披露的漏洞中，微软产品所占的比重逐步降低

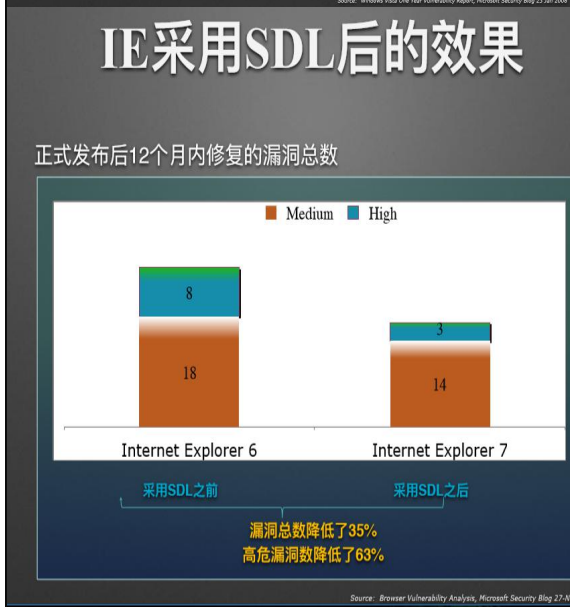
03
PHOTOS

02
PHOTOS

01
PHOTOS







软件安全构建成熟度模型BSIMM

默安科技
企业信赖的安全伙伴

区域			
 治理	 情报	 SSDL 触点	 部署
用于协助组织、管理和评估软件安全计划的实践。人员培养也是一项核心的治理实践。	用于在企业中汇集企业知识以开展软件安全活动的实践。所汇集的这些知识既包括前瞻性的安全指导，也包括组织机构威胁建模。	与分析和保障特定软件开发工件（artifacts）及流程相关的实践。所有的软件安全方法中都包含这些实践。	与传统的网络安全及软件维护组织机构打交道的实践。软件配置、维护和其他环境问题对软件安全有直接影响。
实践模块			
治理	**情报**	**SSDL 触点**	**部署**
1. 战略和指标(SM) 2. 合规性与政策(CP) 3. 培训(T)	4. 攻击模型(AM) 5. 安全性功能和设计(SFD) 6. 标准和要求 (SR)	7. 架构分析(AA) 8. 代码审查(CR) 9. 安全性测试(ST)	10. 渗透测试(PT) 11. 软件环境 (SE) 12. 配置管理和安全漏洞管理 (CMVM)

架构分析AA

默安科技
企业信赖的安全伙伴

SSDL 触点： 架构分析(AA)

架构分析包括以简明的图表来显示软件架构、应用风险和威胁列表、采用审查流程（例如 STRIDE 或架构风险分析），以及为企业制定评估和修复计划。

AA 第 1 级

[AA1.1: 103] 开展安全性功能审查。

在着手开展架构分析时，应当把这一流程的重点放在安全功能审查上。具有安全意识的审查人员首先识别出应用中的安全功能（身份验证、访问控制、密码使用，等等），然后再研究整个设计，以寻找可能导致这些功能无法按预期运行或不足以满足需求的缺陷。例如，此类审查可以同时发现因为访问控制权出现疏漏而面临权限升级攻击危险的系统，以及把 PII（个人识别信息）隐藏在本地存储器中的移动应用。某些情况下，采用企业的“通过设计保证安全”（secure-by-design）组件能够简化此流程。请注意，云服务提供商 API 及其背后的服务常为某些安全功能发挥作用提供不可或缺的支持。

[AA1.2: 29] 针对高风险应用开展设计审查。

企业可以通过观察若干引人瞩目的高风险应用的实际结果来了解架构分析（AA）的优势。审查人员必须具备执行详细设计审查的经验，还必须具备分解架构进行考虑的经验，尤其是对于新平台或新环境更是如此。在任何情况下，设计审查都应发现一系列架构缺陷并制定相应计划来补救这些缺陷。如果 SSG 尚未准备好开展深入的架构分析，可以聘请顾问来完成此项工作，但本身应积极参与。此时，可采用严重依赖专门技能的特别审查模式，但这种模式从长远角度看发展空间不大。如果审查仅聚焦于软件项目是否执行了正确的流程步骤，将不会得到预期的结果。请注意，不可能以 CI/CD 速度来完成一次足够可靠的设计评审流程。

[AA1.3: 23] 由 SSG 领导设计审查工作。

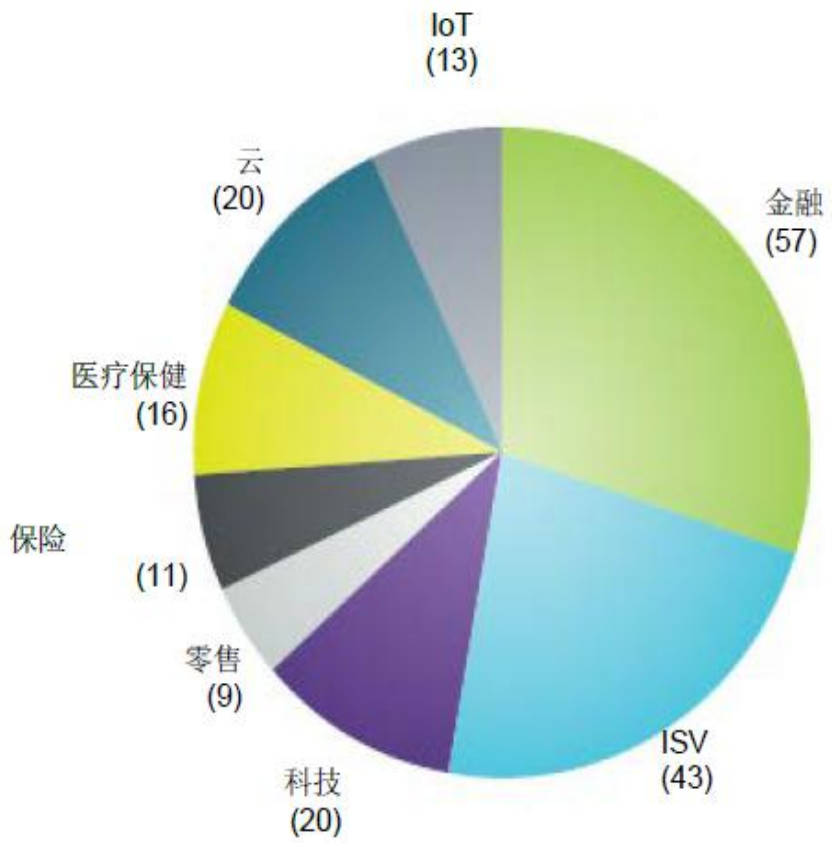
SSG 在架构分析中发挥主导作用，它通过开展设计审查来发现缺陷。分解一套架构是件非常技术性的工作，因此，SSG 在把工作移交给架构师之前必须精通于此道，而精通是需要反复演练的。SSG 也无法仅凭一己之力取得成功；它可能需要架构师或实施人员的帮助来理解设计。在清晰了解设计的基础上，SSG 在开展详细的审查时可最大限度地减少与项目组的互动。随着时间的推移，领导审查工作的责任将移交给软件架构师。处理架构分析（包括威胁建模）的方法会随时间的推移而演变，因此，不要期望设定一套流程后就可以一劳永逸地使用下去。

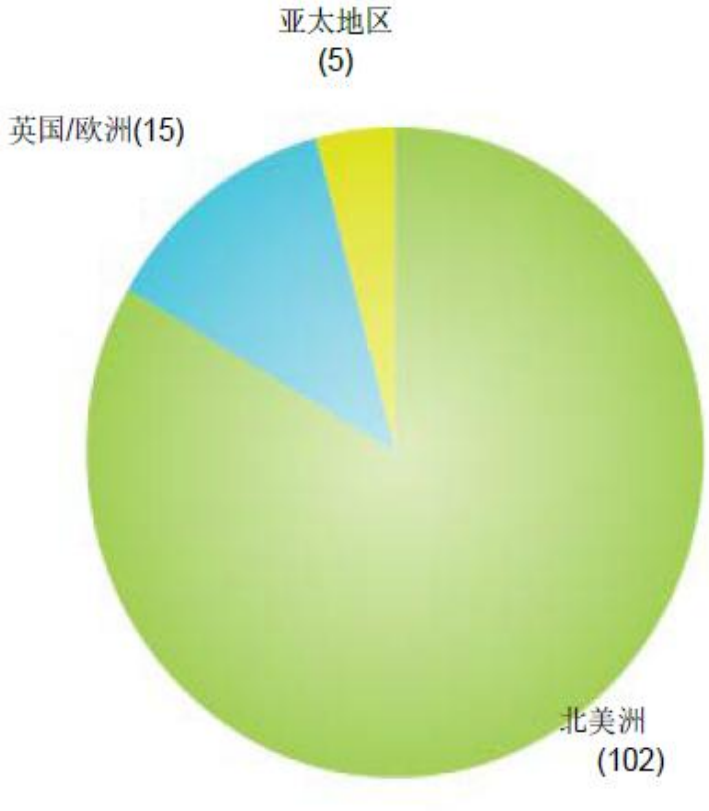
[AA1.4: 62] 利用风险问卷调查为应用排序。

为了便于开展安全功能和设计审查流程，SSG 使用风险问卷调查或类似方法 （ 无论手动还是自动 ） 来收集每个应用的信息，以便分配风险类别和优先级方案。为分配工作提供依据的信息可能包括：“该应用是采用哪种编程语言编写的？”“谁使用该应用？”或者“该应用是否部署到容器中？”等等。通常情况下，应用团队的合格成员提供此类信息，该流程应当尽可能短，以便能够在几分钟内完成。SSG 可以利用这些答案将应用划分为高、中、低风险三档。鉴于风险调查问卷可能未被认真对待，因此应当安排一些抽查，以保证有效性和准确性，这一点很重要。过度依赖自我报告或自动化可能会使此项活动失去意义。

BSIMM10 记分卡

默安科技
企业信赖的安全伙伴





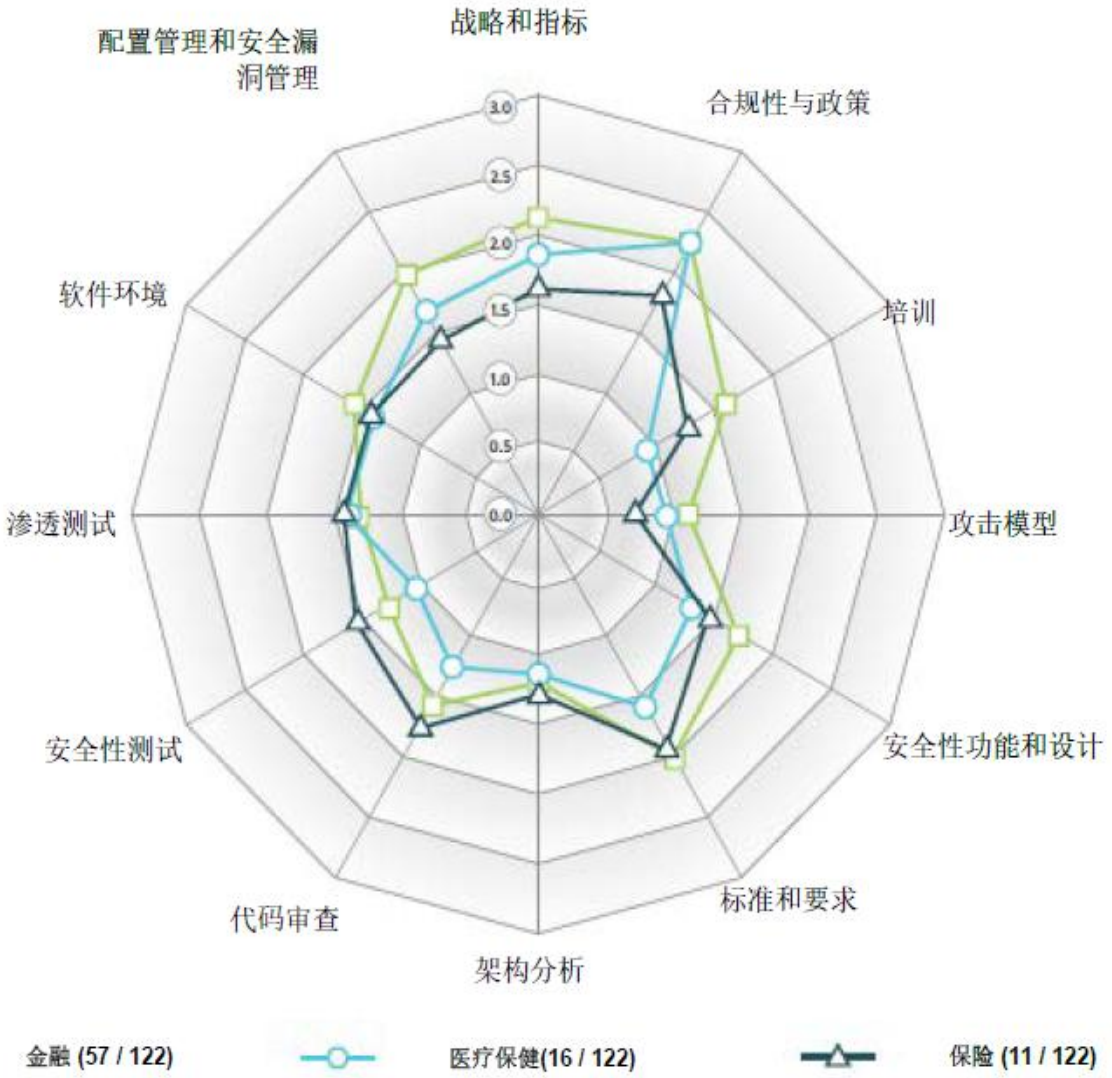
BSIMM10 记分卡

默安科技
企业信赖的安全伙伴

每个实践模块中最常见的活动	
活动	描述
[SM1.4]	确定门控位置，收集必要的工件（artifacts）。
[CP1.2]	确定个人识别信息(PII)义务。
[T1.1]	开展意识培训。
[AM1.2]	制定数据分类方案并制作数据清单。
[SFD1.1]	构建并发布安全性功能。
[SR1.3]	把合规性约束转变成要求。
[AA1.1]	开展安全性功能审查。
[CR1.4]	并行采用自动化工具和人工审查。
[ST1.1]	确保 QA 支持边缘/边界值条件测试。
[PT1.1]	聘请外部渗透测试者来寻找问题。
[SE1.2]	确保主机及网络安全性基础能力就位。
[CMVM1.1]	创建事件响应机制或者与事件响应团队交流。

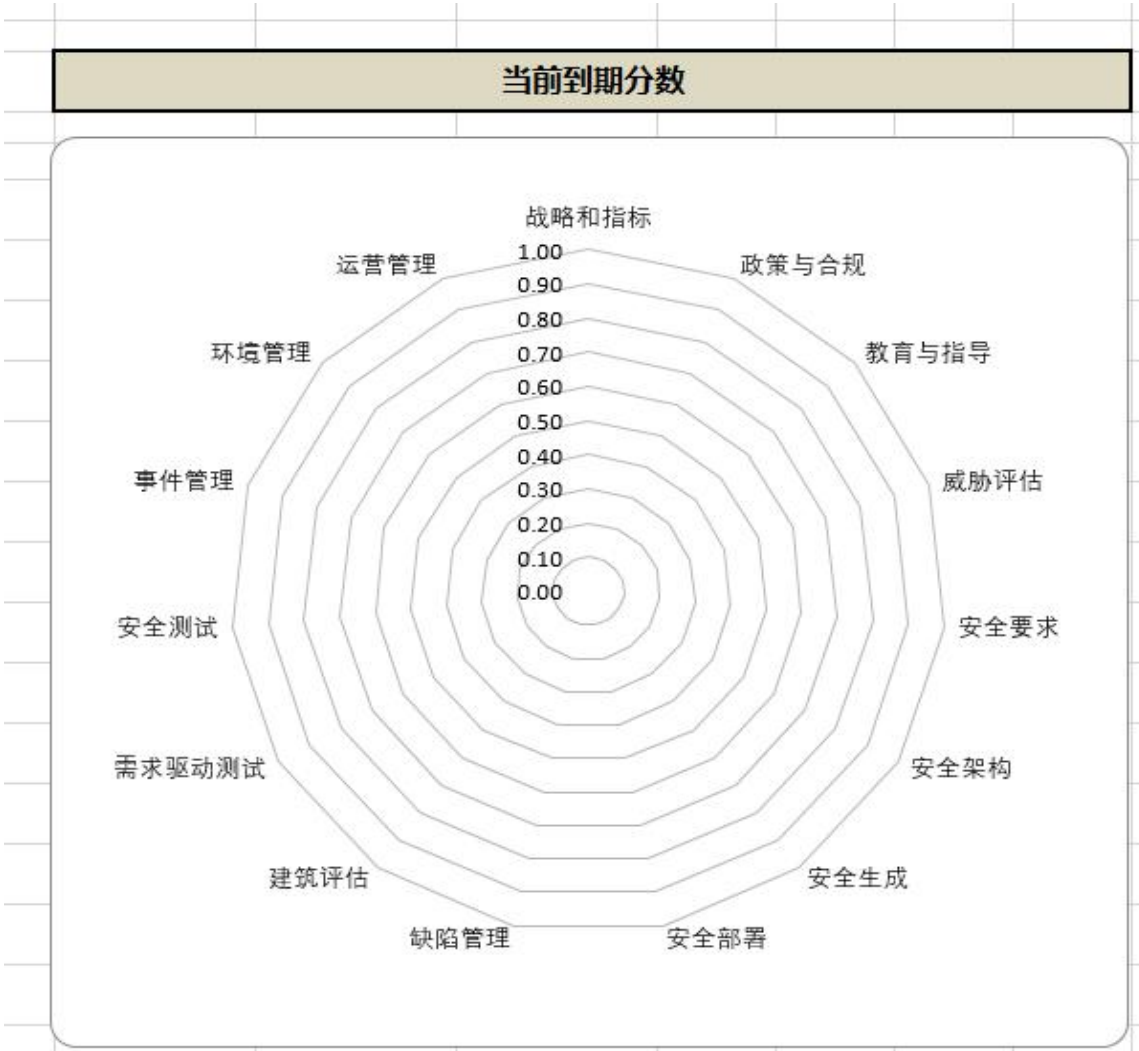
BSIMM10 记分卡

默安科技
企业信赖的安全伙伴



软件保障成熟度模型-SAMM

默安科技
企业信赖的安全伙伴



当前到期分数			
		治理	设计
治理	战略和指标	0.00	0.00
治理	政策与合规	0.00	0.00
治理	教育与指导	0.00	0.00
设计	威胁评估	0.00	0.00
设计	安全要求	0.00	0.00
设计	安全架构	0.00	0.00
实施	安全生成	0.00	0.00
实施	安全部署	0.00	0.00
实施	缺陷管理	0.00	0.00
验证	建筑评估	0.00	0.00
验证	需求驱动测试	0.00	0.00
验证	安全测试	0.00	0.00
操作	事件管理	0.00	0.00
操作	环境管理	0.00	0.00
操作	运营管理	0.00	0.00

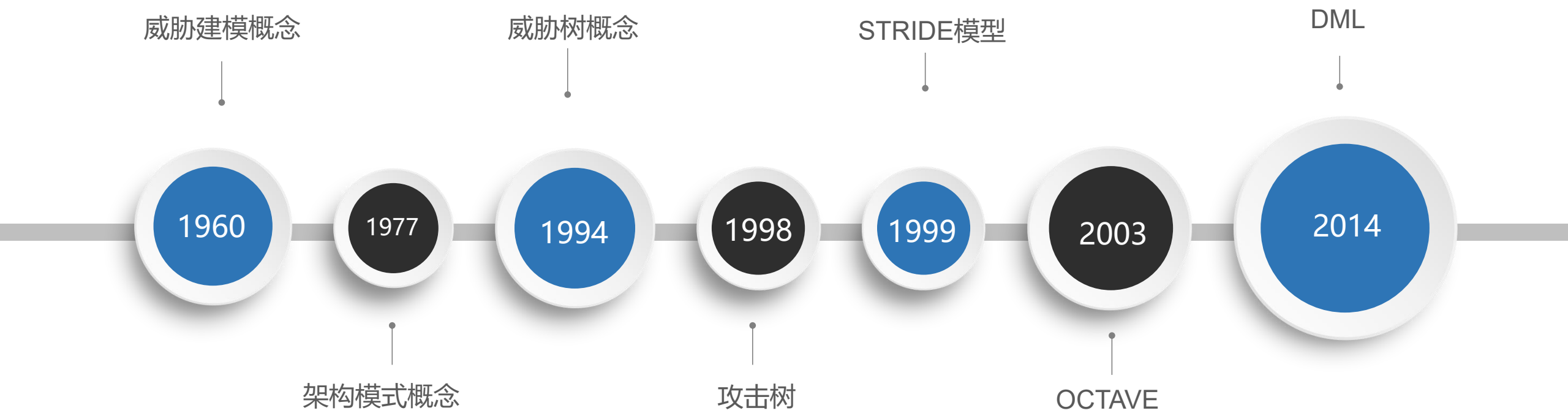
软件保障成熟度模型-SAMM

默安科技
企业信赖的安全伙伴

	设计
	威胁评估
TA1	**组织中的项目是否考虑并记录可能的威胁？**
	指导： 根据每个项目的业务风险状况，记录可能的最坏情况。 *指导：* 为每个项目创建攻击树或威胁模型，跟踪实现最坏情况所需的先决条件。 *指导：* 攻击树或威胁模型被扩展到包括当前和历史功能需求中的潜在安全故障。 *指导：* 将新功能添加到项目中时，将更新攻击树或威胁模型。
	贵组织是否了解并记录其面临的攻击者类型？
	指导： 每个项目都记录了潜在的外部威胁因素及其动机。 *指导：* 每个项目或架构类型都记录了潜在的内部威胁代理、它们的相关角色和潜在的损害。 *指导：* 在组织级别收集一组常见的威胁代理、动机和其他信息，并在项目中重用。
TA2	**项目团队是否定期分析功能需求以防止可能的滥用？**
	指导： 每个项目都从其用例中派生出滥用案例。 *指导：* 随着项目要求或特性的增加，滥用案例也会更新。
	项目团队是否使用评估威胁的方法进行相对比较？
	指导： 使用基于记录的威胁代理、利用价值、技术难度和其他因素的记录权重系统对威胁进行排序。 *指导：* 漏洞修复的优先级取决于权重系统。
	利益相关者是否意识到相关的威胁和评级？
	指导： 与项目利益相关者一起审查潜在威胁和评级。
TA3	**项目团队是否特别考虑来自外部软件的风险？**
	指导： 每个项目中使用的第三方、外部库和代码都有明确的标识和文档记录。 *指导：* 项目威胁模型根据已识别的威胁代理和第三方库和代码的动机进行更新。
	大多数保护机制和控制是否被捕获并映射回威胁？
	指导： 对每个项目进行了评估，以确定缓解控制措施，防止在攻击树或威胁模型中确定的先决条件。 *指导：* 每次引入新功能或需求或修改攻击树时，都会更新此评估。 *指导：* 在攻击树或威胁模型中记录了缓解控制。 *指导：* 每个项目都添加了缓解控制或安全要求，以解决在攻击树中仍然导致成功攻击的任何先决条件。

威胁建模发展历史

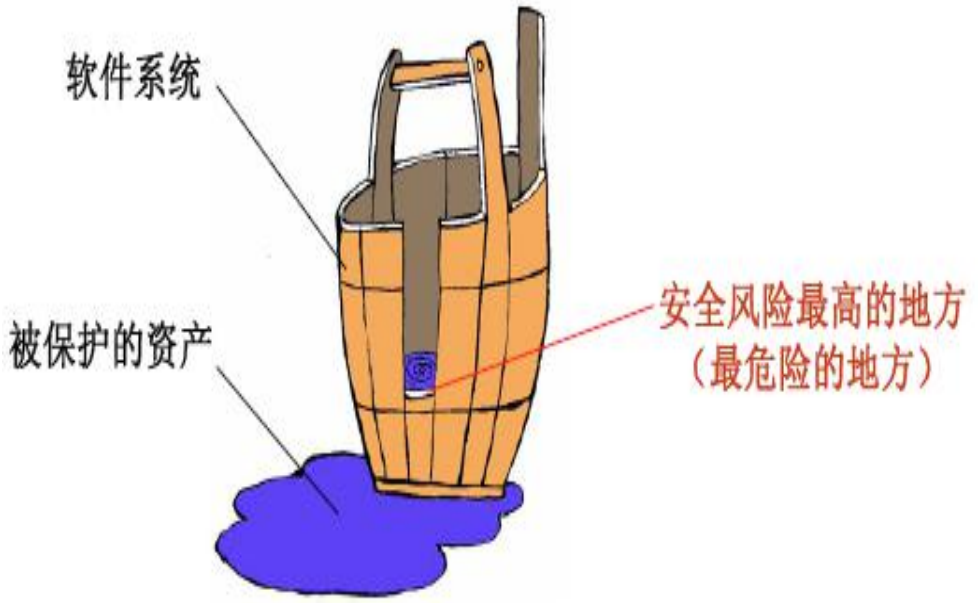
默安科技
企业信赖的安全伙伴



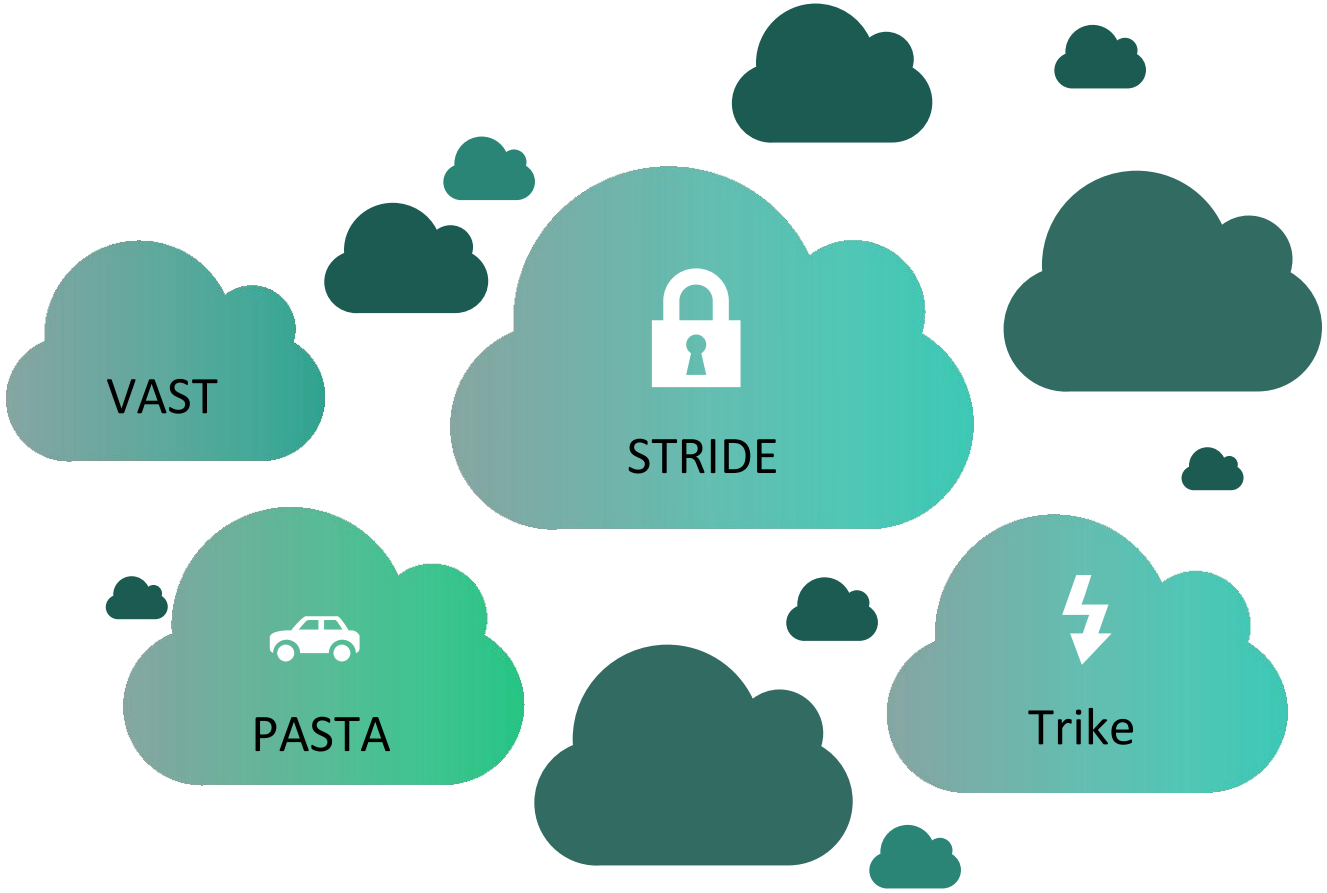
威胁建模

默安科技
企业信赖的安全伙伴

- 什么是威胁建模
  - 威胁建模就是通过结构化的方法，系统的识别、评估产品的安全风险和威胁，并针对这些风险、威胁制定消减措施的一个过程。
- 为什么要威胁建模
  - 帮助在设计阶段充分了解各种安全威胁，并指导选择适当的应对措施
  - 对可能的风险进行管理
  - 可以重新验证其架构和设计
  - 有助于软件的受攻击面降低
- 谁需要做威胁建模
  - 在产品设计阶段、架构评审阶段或者产品运行时开展



威胁建模方法



微软威胁建模模型

默安科技
企业信赖的安全伙伴

1 流程管理

第1步：标识资源；
第2步：创建总体体系结构；
第3步：分解应用程序；
第4步：识别威胁；
第5步：记录威胁；
第6步：评价威胁。

2 技术措施

STRIDE模型：威胁识别模型；
DREAD模型：威胁评价模型；
Microsoft Threat Modeling Tool：威胁建模技术工具。

3 人员组织

开发人员：威胁建模确认及处置者，利用威胁建模降低风险；
设计人员：威胁建模发起和组织者，利用威胁建模进行技术和功能方面的安全设计并进行选择决策；
测试人员：威胁建模参与者。利用威胁建模编写测试案例。

4 考量指标

威胁评价公式：危险 = 发生的概率×潜在的损失；
威胁评价表：对威胁进行定性评价，指导威胁处置优先级；
评估报告及处置建议：明确威胁及威胁后续处置建议。

微软威胁建模工具

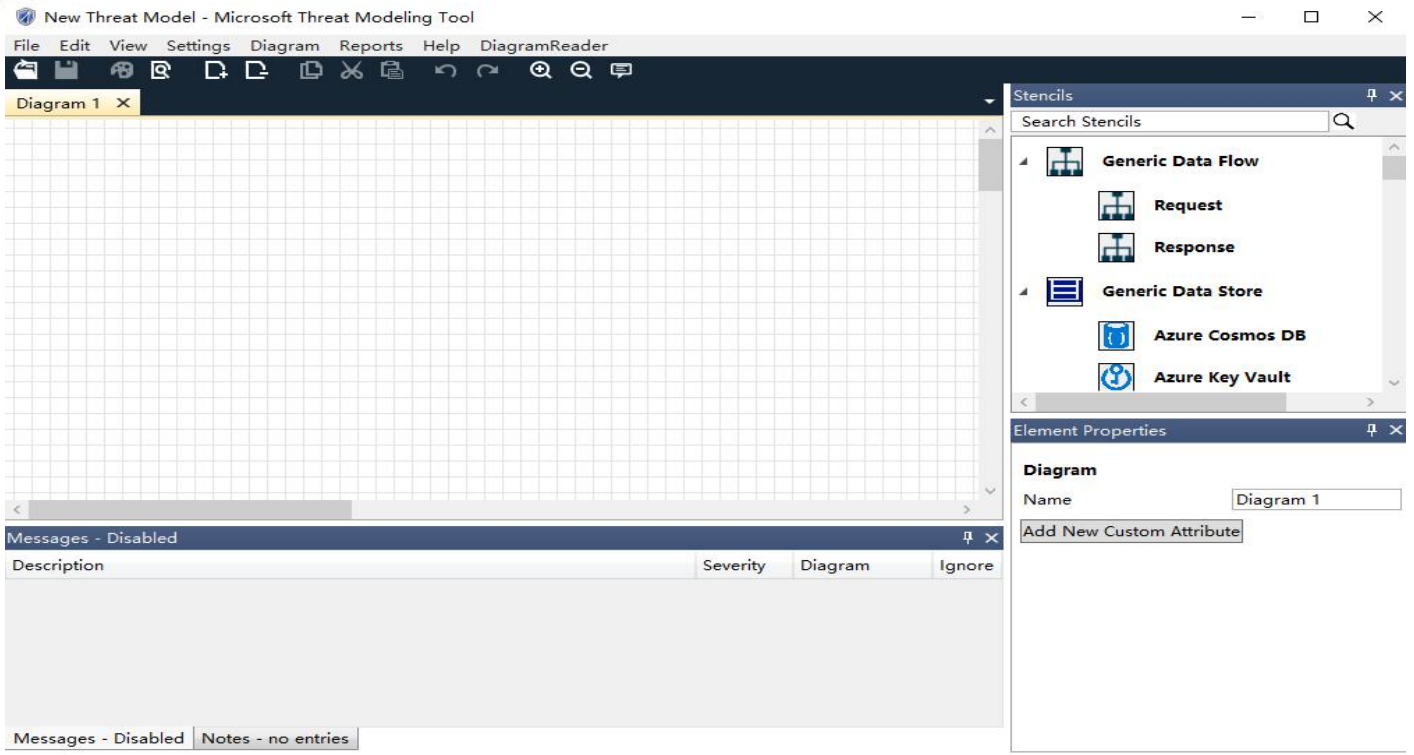
默安科技
企业信赖的安全伙伴

2004年威胁建模方法论诞生

2008年初代威胁建模工具发布

2014年二代威胁建模工具发布

2016年二代威胁建模工具更新



微软威胁建模流程

默安科技
企业信赖的安全伙伴

找出系统必须保护的有价值的资源

标识资源

分解应用程序的体系结构，包括基本的网络和主机基础结构的设计，从而为应用程序创建安全配置文件。安全配置文件的目的是发现应用程序的设计、实现或部署配置中的缺陷。

利用通用威胁模板记录每种威胁，该模板定义了一套要捕获的各种威胁的核心属性。

创建结构

利用简单的图表来记录应用程序的体系结构，包括子系统、信任边界和数据流。

分解程序

识别威胁

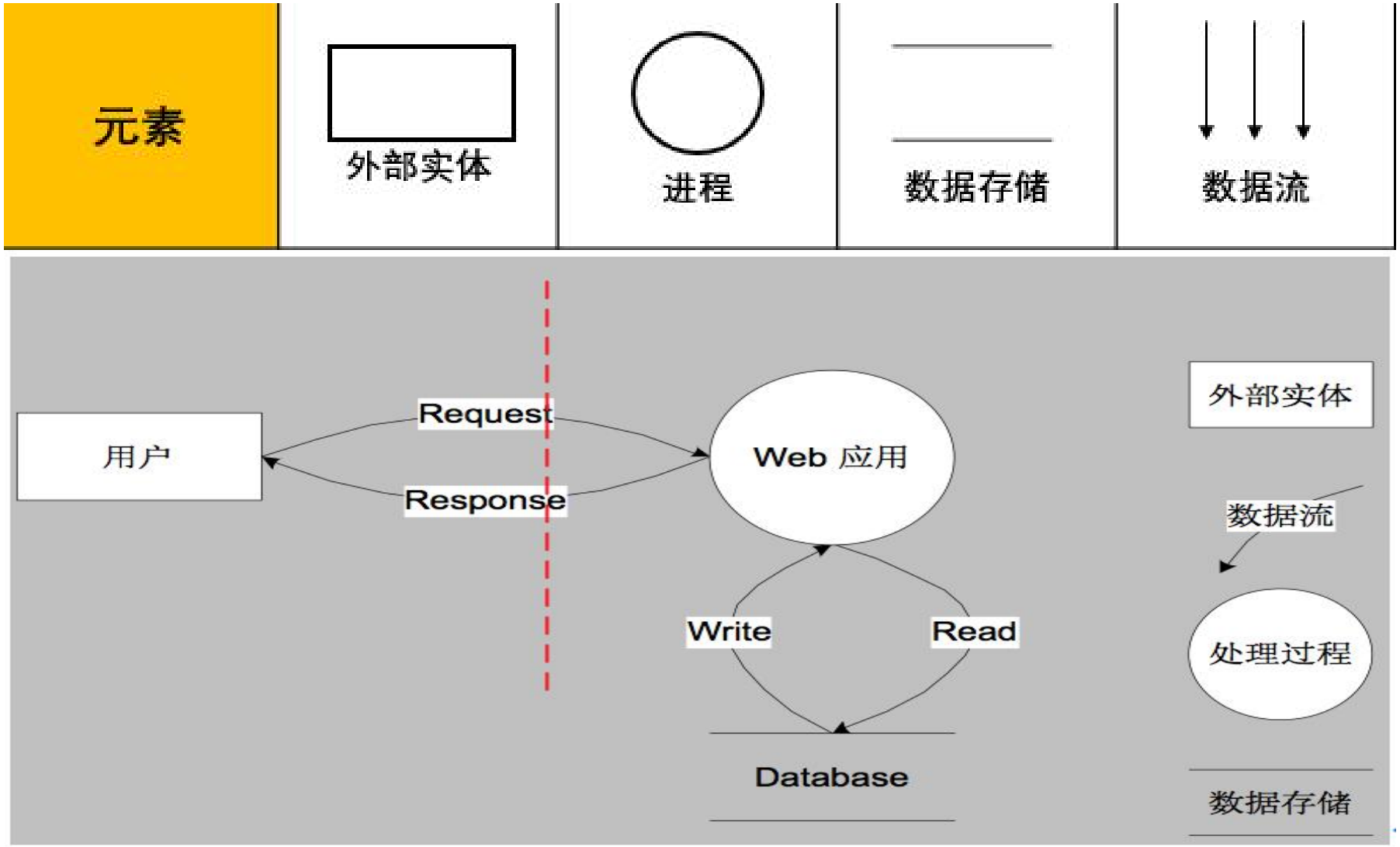
牢记攻击者的目标，利用对应用程序的体系结构和潜在缺陷的了解，找出可能影响应用程序的威胁。

记录威胁

评价威胁

对威胁进行评价以区分优先顺序，并首先处理最重要的威胁。这些威胁带来的危险最大。评价过程要权衡威胁的可能性，以及攻击发生时可能造成的危害。评价的结果可能是：通过对比威胁带来的风险与为使威胁得到减少所花费的成本，对于某些威胁采取的行动是不值得的。

威胁识别-数据流图


元素
外部实体
进程
数据存储
数据流
用户
Request
Response
Web 应用
Write
Read
Database
外部实体
数据流
处理过程
数据存储

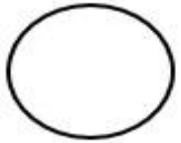
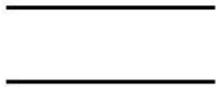
威胁识别-SRTIDE-per-Element

默安科技
企业信赖的安全伙伴

威胁	安全属性	定义	举例
欺骗（S）	认证	假装成别人或别的个体	冒充其他用户账号
篡改（T）	完整性	修改数据或代码	修改订单信息
抵赖（R）	审计	否认做过的事	不承认修改行为
信息泄露（I）	保密性	信息被泄露或窃取	用户信息被泄露
拒绝服务（D）	可用性	消耗提供服务所需的资源	DDOS 导致网站不可用
特权提升（E）	授权	未经授权获取、提升权限	普通用户提升到管理员

威胁识别-对应关系

默安科技
企业信赖的安全伙伴

元素	S	T	R	I	D	E
 外部实体	✔		✔			
 进程	✔	✔	✔	✔	✔	✔
 数据存储		✔	✔	✔	✔	
 数据流		✔		✔	✔	

记录威胁

威胁目标	Web 应用程序用户身份验证进程
威胁说明	攻击者通过监视网络获取身份验证凭据
威胁类别	I
攻击方法	利用网络监视软件
缓解措施	利用SSL提供加密通道
风险评级	

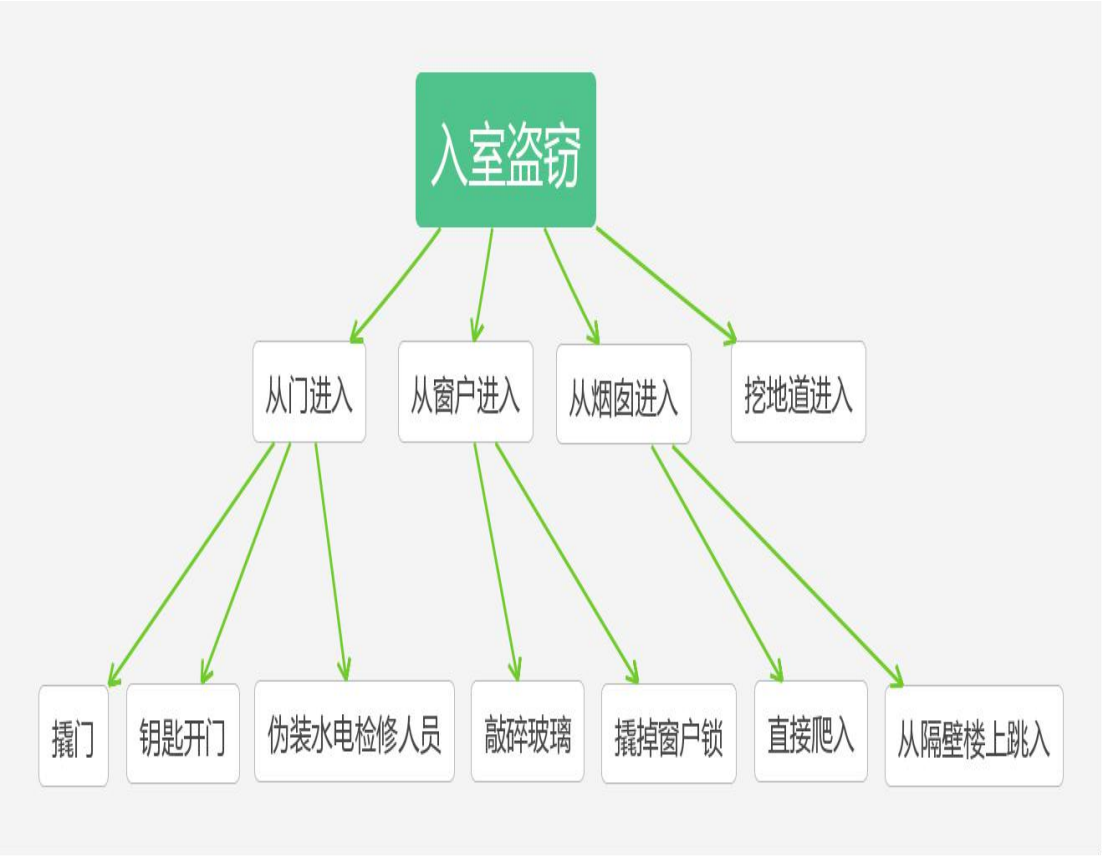
评价威胁

默安科技
企业信赖的安全伙伴

等级	高	中	低
潜在的损失 **D**	获取完全验证权限，执行管理员操作，非法上传文件	泄露敏感信息	泄露其他信息
重现性 **R**	攻击者可以随意再次攻击	攻击者可以重复攻击，但有时间限制	攻击者很难重复攻击过程
可利用性 **E**	初学者短期能掌握攻击方法	熟练的攻击者才能完成这次攻击	漏洞利用条件非常苛刻
受影响用户 **A**	所有用户，默认配置，关键用户	部分用户，非默认配置	极少数用户，匿名用户
可发现性 **D**	漏洞很显眼，攻击条件很容易获得	在私有区域，部分人能看到，需要深入挖掘漏洞	发现漏洞极其困难

攻击树

默安科技
企业信赖的安全伙伴



攻击库

默安科技
企业信赖的安全伙伴

Home | About | CAPEC List | Community | News | Search

CAPEC™ helps by providing a comprehensive dictionary of known patterns of attack employed by adversaries to exploi
nce defenses.

View the List of Attack Patterns

by Mechanisms of Attack | by Domains of Attack

Search CAPEC

ywords(s) or by CAPEC-ID Number. To search by multiple keywords, separate each by a space.

See the full CAPEC List page for enhanced information, downloads, and more.

Total Attack Patterns: 517

1000 - Mechanisms of Attack

- Engage in Deceptive Interactions - *(156)*
  - Content Spoofing - *(148)*
  - Identity Spoofing - *(151)*
  - Resource Location Spoofing - *(154)*
  - Action Spoofing - *(173)*
  - Manipulate Human Behavior - *(416)*
- Abuse Existing Functionality - *(210)*
- Manipulate Data Structures - *(255)*
- Manipulate System Resources - *(262)*
- Inject Unexpected Items - *(152)*
- Employ Probabilistic Techniques - *(223)*
- Manipulate Timing and State - *(172)*
- Collect and Analyze Information - *(118)*
- Subvert Access Control - *(225)*

3000 - Domains of Attack

- Software - *(513)*
- Hardware - *(515)*
- Communications - *(512)*
  - Exploiting Trust in Client - *(22)*
  - Man in the Middle Attack - *(94)*
  - Interception - *(117)*
  - Flooding - *(125)*
  - Excessive Allocation - *(130)*
  - Content Spoofing - *(148)*
  - Identity Spoofing - *(151)*
  - Resource Location Spoofing - *(154)*
  - Infrastructure Manipulation - *(161)*
  - Footprinting - *(169)*
  - Protocol Analysis - *(192)*
  - Communication Channel Manipulation - *(216)*
  - Resource Injection - *(240)*
  - Protocol Manipulation - *(272)*
  - Traffic Injection - *(594)*
  - Obstruction - *(607)*
  - Fault Injection - *(624)*
- Supply Chain - *(437)*
- Social Engineering - *(403)*
- Physical Security - *(514)*

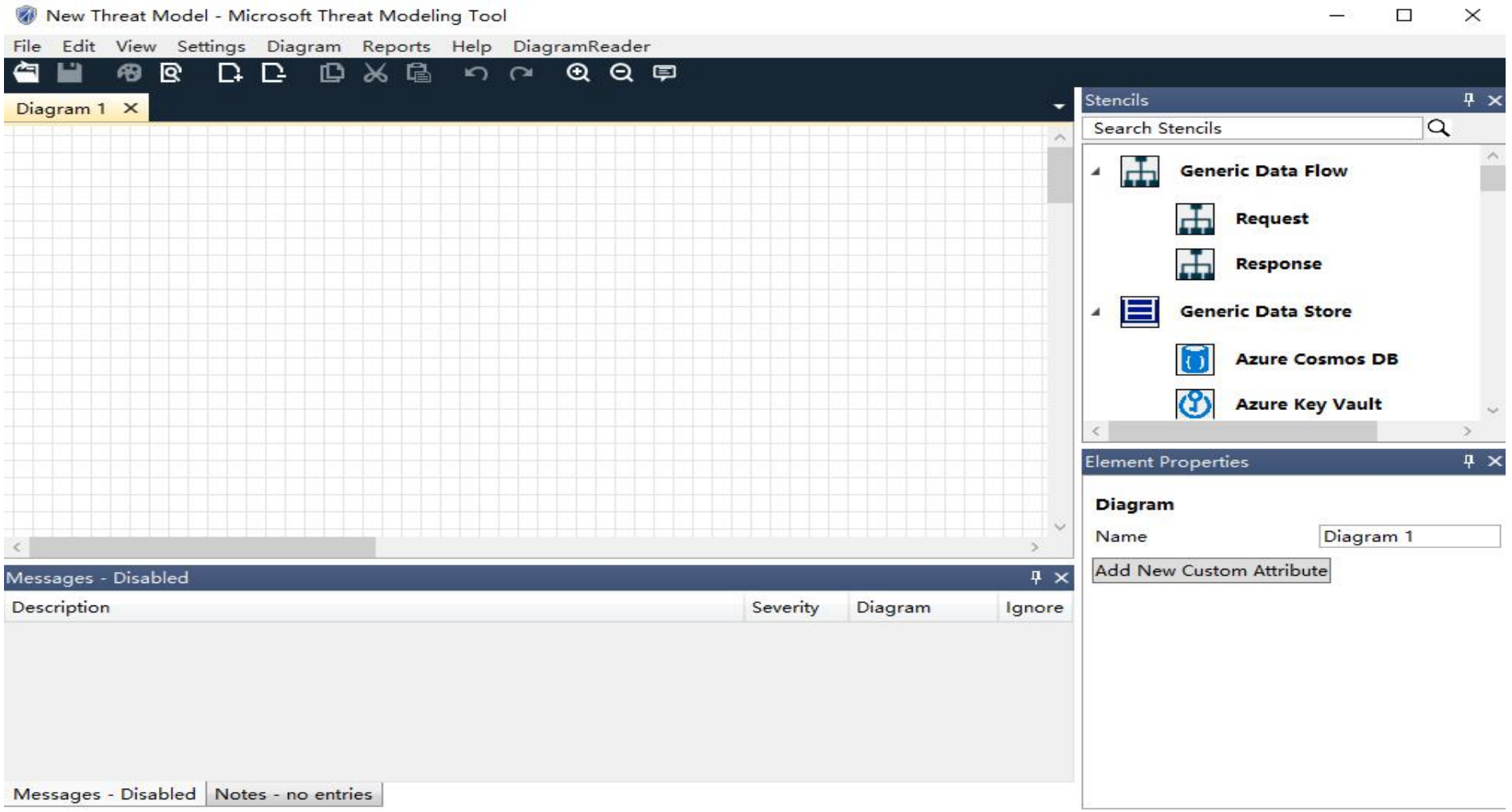
威胁建模工具

默安科技
企业信赖的安全伙伴

序号	威胁建模工具	链接
1	STAC	https://www.moresec.cn/sdl-stac.html
2	Threat Modeling Tool	https://aka.ms/threatmodelingtool（最新版下载）
3	iriusrisk	https://www.continuumsecurity.net/threat-modeling-tool/
4	ThreatModeler	https://threatmodeler.com/
5	Owasp Threat Dragon	http://docs.threatdragon.org/
6	Practical Threat Analysis	http://www.ptatechnologies.com/
7	octotrike	http://www.octotrike.org/tools
8	Seasponge	https://github.com/mozilla/seasponge
9	Seamonster	https://sourceforge.net/projects/seamonster/
10	python库	https://github.com/izar/pytm
11	java sdk	https://github.com/stevespringett/threatmodel-sdk
12	Foreseeti	https://www.foreseeti.com/
13	Tutamen	http://www.tutamantic.com/
14	Secur IT ree	https://web.archive.org/web/20120501184047/http://amenaza.com/
15	RiskTree	https://risktree.2t-security.co.uk/
16	AD Tool	https://satoss.uni.lu/members/piotr/adtool/
17	Ent	https://github.com/jimmythompson/ent

威胁建模实践

默安科技
企业信赖的安全伙伴



威胁建模资料

默安科技
企业信赖的安全伙伴

内容	链接
微软安全门户	https://www.microsoft.com/en-us/securityengineering
微软sdl	https://www.microsoft.com/en-us/securityengineering/sdl/
微软SDL流程	https://docs.microsoft.com/en-us/previous-versions/windows/desktop/cc307891(v=msdn.10)?redirectedfrom=MSDN
微软威胁建模	https://docs.microsoft.com/zh-cn/azure/security/develop/threat-modeling-tool 或 https://www.microsoft.com/en-us/securityengineering/sdl/threatmodeling内含Microsoft威胁建模工具的所有信息 https://docs.microsoft.com/zh-cn/azure/security/develop/threat-modeling-tool-releases-73002061（威胁建模工具2020年2月版本）
关于攻击面分析	实现最小特权的管理模型https://docs.microsoft.com/zh-cn/windows-server/identity/ad-ds/plan/security-best-practices/implementing-least-privilege-administrative-models#in-applications 微软攻击面分析仪2.0(2019年发布) https://www.microsoft.com/en-us/download/details.aspx?id=58105
关于BSIMM	https://www.bsimm.com/zh-cn/download.html（下载BSIMM）
关于SAMM	https://owaspsamm.org/（官网） https://github.com/OWASP/samm（SAMM最新的进展） https://wiki.owasp.org/index.php/OWASP_SAMM_Project#tab=Main（OWASP上一些SAMM的简介与资料）
STRIDE (security)	https://en.wikipedia.org/wiki/STRIDE_(security)
Attack tree	https://en.wikipedia.org/wiki/Attack_tree
威胁建模书籍	《威胁建模，设计和交付更安全的软件》
威胁缓解措施	https://docs.microsoft.com/zh-cn/azure/security/azure-security-threat-modeling-tool-mitigations
微软威胁建模	https://docs.microsoft.com/en-us/previous-versions/msp-n-p/ff648644(v=pandp.10)?redirectedfrom=MSDN

默安科技
企业信赖的安全伙伴

THANK YOU