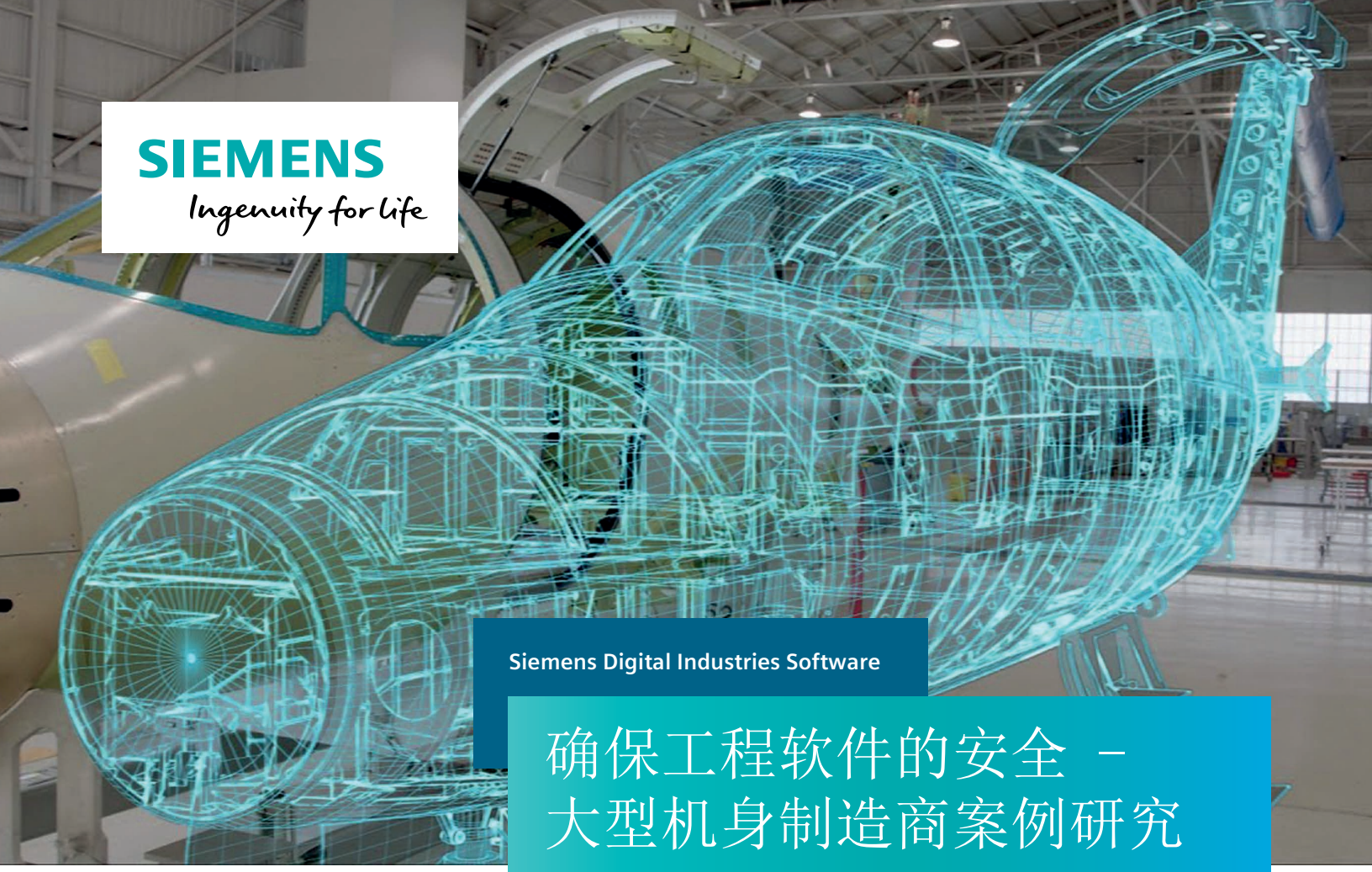

SIEMENS
Ingenuity for life

Siemens Digital Industries Software

# 确保工程软件的安全 – 大型机身制造商案例研究


**高层摘要**

放眼全球，不断增长的网络犯罪、网络间谍活动和网络恐怖主义令各公司企业苦不堪言。除了公司声誉严重受损外，安全系统被破坏，还给客户的隐私、安全和生活带来巨大威胁。上报的案件仅占每天发生攻击的一小部分。仅 2016 年，美国在线信任联盟就记录了 82,000 起网络 “安全事件”（在线信任联盟，2017 年）。然而，由于人们通常不会报告网络攻击，他们估计实际事件数量超过 250,000 起（在线信任联盟，2017 年）。随着网络犯罪的发生率逐年上升，攻击的范围和损害也在不断增加。



技术总监

阿特姆 · 科尔尼洛夫 (Artem Kornilov)

# 网络犯罪：目标与影响

图 1：F-35 战斗机信息通过一款惯用的网络安全漏洞工具被盗。

各种商业组织（尤其是拥有政府合同的商业组织）以及政府机构是最常见的网络攻击目标，因为他们手中握有宝贵的信息。最富戏剧性的是，F-35 联合打击战斗机、P-8 波塞冬巡逻机、C-130 大力神运输机、联合制导攻击武器 (JDAM) 炸弹以及澳大利亚海军未来舰船的信息于 2016 年 11 月从澳大利亚国防公司泄漏（图 1，Ars Technica，2017 年）。

网络犯罪分子攻击企业的动机多种多样。有时是为了获取敏感信息，比如意图窃取知识产权。有时是为了破坏或延迟新产品或新项目的设计流程。攻击的重点还可能是通过篡改设计的关键部分来损害产品本身的功能。例如，通过更改设计过程中某些导线外的绝缘材料，第三方便能更容易地通过电磁辐射监视最终产品的活动。设计数据也可能完全遭到破坏，使数月乃至数年的设计工作毁于一旦。

网络安全漏洞的频发和严重后果震惊了全球各大公司，迫使他们采取更完善的措施来保护整个供应链中的信息。本白皮书将探讨 Siemens Digital Industries Software 等供应商如何奋力应对各种新的严苛安全要求。

# 保护企业软件解决方案的安全

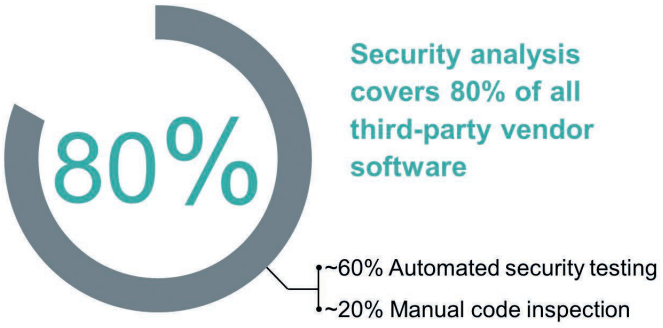


图 2：各大公司正在寻求建立统一的过程来确保其供应商软件的安全。

防范网络安全漏洞对于公司的声誉以及业务的成功运营和成长至关重要。无所作为会让企业付出高昂代价，因为安全漏洞会给公司造成巨大财务损失或者导致敏感信息泄漏。因此，世界各地的制造商已经构想并实施了多方面的安全软件开发计划，为其使用的所有软件的网络安全保驾护航。

这些计划非常重视通过测试和安全的开发实践来降低第三方软件中的安全漏洞所带来的风险和成本。安全专家团队经常与软件供应商直接合作，帮助他们将软件安全性集成到开发流程并由此受益。以这种方式与供应商合作是强化制造商系统的基本要求。

大多数安全计划都从内部软件解决方案和网络开始着手，但是，安全团队发现，黑客技术也在紧跟安全措施的改进步伐而不断演变。随着各大公司纷纷强化自己的网络和软件，黑客开始瞄准他们的供应链。对于黑客而言，供应链的攻击面往往更大，因为大型公司会使用大量第三方软件。在软件产品的开发流程和安全投资方面，每家软件供应商都有诸多不同之处，这为黑客访问公司数据提供了更多机会。一位安全专家最近指出：“只有供应商的信息安全了，我们才能安全。”

为此，各大公司纷纷扩展自己的安全计划，以便在建立统一的软件安全程序方面与软件供应商展开专项合作（图 2）。第一步通常是将对供应商产品的安全评估纳入采购流程，然后汇总评估结果并提供给公司的管理层，为他们的采购决策提供参考。

软件评估还可以包含通过独立的第三方机构对供应商的软件进行安全漏洞扫描。向供应商提供安全扫描结果的完整详细报告，而潜在客户仅会收到高度总结的结果。这种方法使供应商能够保护其知识产权，同时向关注其解决方案感的公司提供必要的可见性。供应商可以选择自己的运作程序，而制造商能够通过统一的安全评估对各供应商进行比较。

确立良好的安全报告记录后，供应商及其客户将共同评估供应商的整个安全软件开发生命周期 (S-SDLC) 流程。在某些情况下，供应商可以证明自己流程的稳健性，能够顺利交付符合安全要求的产品。而客户也将认为该供应商采用了可靠的 S-SDLC 流程，因此值得信赖，无需进行持续监督或评估。

# 供应商视角

对于当今市场上的一流工程软件而言，高级安全功能必不可少。越来越多的公司要求软件供应商系统性地验证其软件的安全性。但是，在投资更完善的产品安全性时，供应商需要考虑一些重要因素。

传统上，安全性是 IT 部门或专门安全部门的问题，并非每个软件开发团队都需要关心。安全性也与人员有关，这意味着人力资源部门将参与进来，组织并举办有关如何正确处理数据的培训。总体而言，开发更安全的软件要求各团队紧密协同，这是从前没有要求过的，因此需要新的流程。

此外，增强复杂软件的安全性也要求一种整体全面的方法。供应商必须添加各种安全功能，比如数据加密或审核跟踪，并通过发现和解决代码中的缺陷来强化软件。供应商软件中的第三方内容也必须得到保护，这样才能确保软件解决方案真正安全。这些强化措施可以提升软件的安全性与质量，实现关键且详细的代码分析，进而打造差异化优势并在市场中脱颖而出。

总之，供应商应当根据对业务可持续发展可能产生的影响来决定是否投资产品安全性。因此，他们的客户必须以不容置疑的方式来表达更好的产品安全性将如何影响自己的采购偏好、购买决定和宣传等等，这一点非常重要。制定供应商应遵循的行业安全标准后，即可根据高于最低要求多少来进行评判，从而大大简化了决策过程。决定投资产品安全性后，供应商必须考虑如何以最高效和最有效的方式实现这一目标，从而实现商业收益最大化。

# 确保投资组合的安全


图 3：Siemens Capital 软件套件为电气系统和线束的整个生命周期提供支持。

自 2011 年以来，西门子一直在安全性方面与客户开展合作。Siemens Digital Industries Software 的安全增强功能与其 IT 部门的努力密不可分。西门子 IT 部门引领了在安全性方面与各公司的整体互动，推动了企业在安全培训与安全扫描工具方面的供应商选择和预算，同时协调了西门子各部门之间的安全合作。作为互动的一部分，西门子选择了 Capital 电气系统设计和集成软件套件来参与高级安全计划。

Siemens Capital 软件套件为电气系统和线束的整个生命周期提供支持，从早期的电气和电子产品构架探索到生产设计，再到现场的生产准备和维护（图 3），可谓无所不包。Capital 解决方案可以部署在本地或云中，采用多层结构，以数据为中心，并具有基于 Web 的胖客户端。Capital 套件涵盖了广泛的常用软件技术和设计方法，堪称保护软件解决方案安全领域的典范。

在开启安全性之旅的初期，Capital 团队明确了各必要流程的目标，并获得了西门子内部高管层的支持。要确保 Capital 电气系统设计和集成套件的安全，靠一个部门的单打独斗是不可能完成的。因此，他们向西门子高管层提议让 IT 与销售部门协同合作。获得批准后，Capital 软件开发部门组建了一支安全项目团队，以期实现以下三个目标，从而确保 Capital 套件安全：

1. 解决现有安全缺陷
2. 防止引入新的安全缺陷
3. 通过培训和共享最佳实践来形成安全文化。

为了解决现有的安全缺陷，Capital 软件团队使用了基于云的解决方案来执行静态应用程序安全测试 (SAST)。选择 SAST 技术的原因是，它们提供了更大的代码覆盖范围，可以补充 Capital 软件团队已在 S-SDLC 流程中使用的动态应用程序安全测试 (DAST)。基于云的 SAST 解决方案扫描了

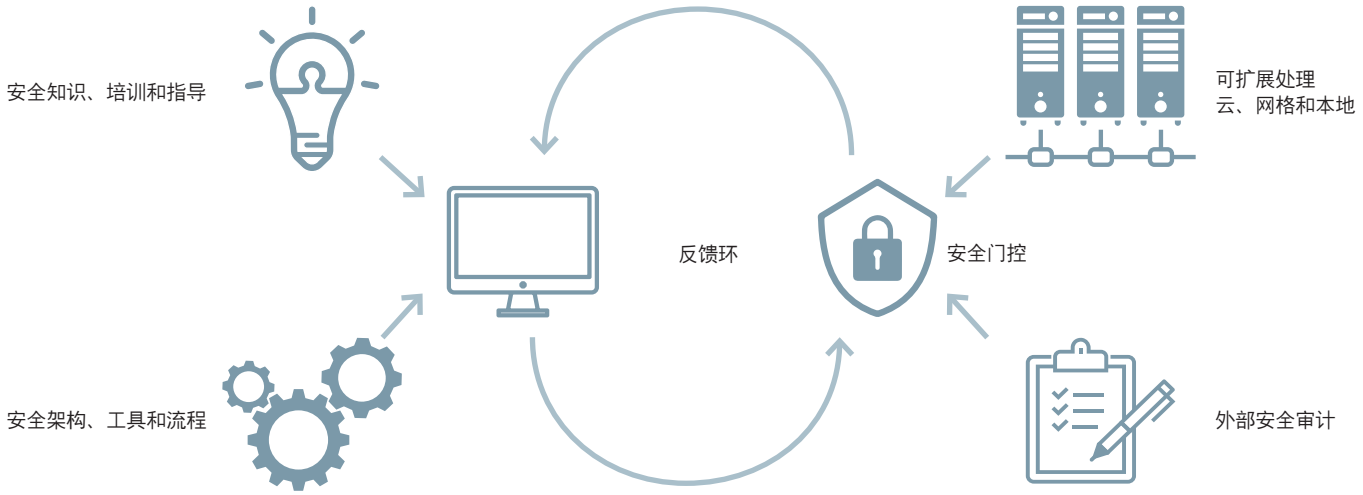


图 4：短反馈环有利于更敏捷地识别和修复缺陷。

Capital 套件的代码，并列出了现有安全缺陷的列表。他们使用此列表估算解决每个缺陷所需的工作，然后对缺陷分组并按优先顺序进行有效修复。首先解决的是具有最高潜在影响的缺陷，并一同解决了相关缺陷。这一流程直接纠正了 Capital 套件所含数百万行代码中的所有缺陷。

接下来，该团队确定了各种常规模式，并根据 Capital 套件的代码库、工具和流程制定了最佳实践。最成功的一点是 SAST 评估报告了大量误报，即在没有安全缺陷的地方识别出安全缺陷。基于云的解决方案消除了许多此类误报，但仍有大量问题需要由 Siemens Digital Industries Software 工程师解决。他们为此创建了一套用于识别误报并判断其是否需要屏蔽的方法，其中包括用于确定所识别误报之真实性的审查和批准流程。这些最佳实践首先在部门工程博客上发布，然后在定期的工程社区会议上讨论。

这些基于云的解决方案非常实用，因为它们会定期更新，从而让工具识别新型安全缺陷。这样，Capital 团队就能重新扫描先前确定为干净的代码，发现并解决新的安全缺陷。当然，要充分利用这些周期性更新，就需要可靠的扫描过程并不断投资于发现和解决安全缺陷，即便是对于已经扫描的代码也是如此。

缺陷补救情况的跟踪通过持续提交代码更改并重新运行 SAST 扫描来完成。Capital 软件团队开发了自动脚本来执行各种任务，其中包括打包用于 SAST 扫描的代码，以及将扫描结果加载到统一的代码度量平台中。为了弘扬西门子安全计划，Siemens Digital Industries Software 致力于通过不断改进代码的体系结构和设计，使安全软件的开发更加轻松顺利。这是通过定期缩小和保护应用程序的攻击面并主动管理安全风险来实现的。

SAST 技术的复杂性和 Capital 解决方案代码库的规模意味着每次扫描都需要大量时间，导致面向软件工程师的反馈环相对较长。为了缓解这种情况，Capital 软件团队采用了一套互补的工具，这些工具以 SAST 扫描覆盖范围为依托，实现了更短的反馈环（图 4）。这种最短的反馈环由专注于安全性的静态代码分析提供，该分析会在软件工程师使用的集成式开发环境中连续运行。为此，Capital 团队选择了 JetBrains ™ IntelliJ 代码检查静态代码分析引擎与开源 Find Security Bugs SAST 解决方案配对使用。

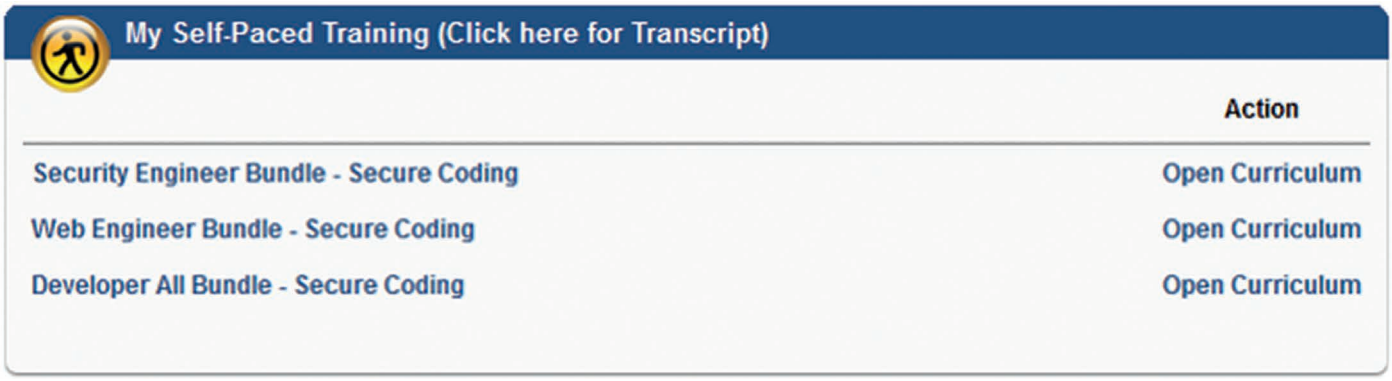


图 5：使用基于计算机的培训来增加安全知识。

除了提供更快的反馈环外，这些工具还通过检查单元测试的完成情况、单元测试的覆盖范围和代码重复情况，将安全性集成到用于控制代码和测试交付项的自动质量门控中。在工程师与团队之间以及团队与发布之间的代码传递均受到门控。这样便可将安全性根植于软件开发过程中并提高保护强度，同时无需软件工程师完成额外工作，从而达成第二个安全性目标。

对于第三个目标“形成安全文化”，Capital 团队与 IT 和 HR 合作，为软件和质量保证工程师开展了基于计算机的安全培训并进行了相应管理。他们选择了 Security Innovations ™ 作为培训提供商。培训课程针对 Capital 解决方案中的技术堆叠和各个团队的特定需求进行了量身定制。为确保及时参加培训，各部门制定了推动计划，根据截止日期对培训完成指标进行跟踪，并将安全培训整合到新员工的入职流程中。

Capital 团队采用了三种主要的安全培训方法。第一种是由讲师指导的针对安全测试的质量保证培训。这些课程的重点是 Capital 开发团队自 2011 年开始与具有安全意识的客户合作以来应用的增强和改进技术。例如，Siemens Digital Industries Software 曾使用 DAST 来评估应用程序，方法是像黑客那样发动攻击并观察结果。其次，Capital 团队通过第三方提供商 Security Innovations 进行了基于计算机的安全软件开发方面的培训。他们分别为开发人员、网络工程师和安全工程师制定了课程集。每一课程集都重点针对每种工作的安全问题（图 5）。例如，开发人员课程集中包含“创建安全 Java 代码基础知识”，“创建安全 Java 代码”和“Open Web Application Security Project 的十大威胁和缓解措施”之类的主题。最后一种方法是成立了一支安全项目团队，负责制定一系列供整个 Siemens Software 共享的最佳实践。这些最佳实践已通过 Siemens Digital Industries Software 中央 IT 组织进行共享。

# 解决开源安全问题

设计工具供应商的另一大顾虑是第三方开发商提供的开源软件 (OSS)。许多功能强大的软件解决方案（包括 Capital 套件）都包含相当一部分的 OSS。OSS 对于企业而言确实是一种宝贵的工具，可节省数天乃至数月的开发时间。但是，OSS 可能会将缺陷引入原本安全的软件解决方案中。供应商需要确保其软件解决方案中所使用的 OSS 安全无虞。

必须使用 SAST 扫描在开源软件所在的代码上下文中单独分析这些软件，然后才能将其加入供应商的产品中。发现问题后应加以解决或者说服 OSS 开发人员自行解决，这一点非常重要。公开可用的安全漏洞数据库也是此流程可以利用的重要资源。这些数据库可跟踪软件中的已知漏洞，并以可搜索的格式发布它们。其中一个典型示例便是美国国家漏洞数据库 (NVD)（美国国家标准与技术研究院，2018 年）。

然而，只关注 OSS 的安全性是不够的，必须认真考虑降低对它的依赖。每个开发团队都应检查 OSS 的使用情况，以确定是否有可能升级、删除或替换其功能。减轻 OSS 中安全缺陷风险的方法有，在供应商代码中进行变通以替换或取代 OSS 执行的功能、说服 OSS 开发人员解决检测到的问题或者改用安全性更高的其他解决方案。此外，还应制定并共享一系列 OSS 最佳安全使用实践，以帮助传播解决方案。在最终批准使用 OSS 前，必须审查其对安全性的影响。

# 主要经验教训和成就

通过系统性的培训以及开发和共享最佳安全实践，Siemens Digital Industries Software 已成功将创建安全软件产品的流程制度化。此过程已深深植入到开发生命周期中，可以确保始终如一地贯彻安全实践。

因此，西门子通过与具有安全意识的客户展开长期互动，成功实现了卓越的安全标准。这些客户对 S-SDLC 开发的热情和积极投入，向西门子展示了投资更高安全性的巨大价值。通过强化安全实践，Siemens Digital Industries Software 还获得了许多其他优势。西门子利用在安全相关活动中学到的最佳实践改进了产品开发基础设施，提高了生产力。西门子还为 Capital 电气系统设计和集成解决方案编写了具有更高质量和安全性的稳健代码，由此提高了竞争力。最后，安全培训使员工有时间专门学习重要、实用的技能，员工满意度也随之提高。

成功完成软件安全开发有几个关键步骤。首先，Siemens Digital Industries Software 进行了系统性的安全扫描和培训，识别并纠正了 Capital 电气系统设计和集成解决方案中的缺陷，从而得到一系列干净简洁的摘要报告，满足了 Open Web Application Security Project (OWASP) 及其他标准（OWASP，2018 年）。使用几种不同安全扫描产品得到的短反馈环转而又加速了缺陷的识别和解决。这是构建西门子 S-SDLC 的关键所在。其次，西门子分享了提高企业整体安全性的经验教训、知识和技能，开创了这方面的先河。

# 保障企业未来安全

如今，各大公司纷纷投资开发强大可靠的综合防护措施，用以抵御现代化环境的众多网络安全威胁。其关键原因在于网络犯罪开始将目标从大型公司扩展到他们的供应链。各大公司已经明确了软件开发安全计划应具有两大重要特征。首先是建立覆盖整个公司的组织，这一点非常关键。确保企业内所有部门都采取统一的软件安全措施对于企业安全而言至关重要。其次，安全计划确定的各供应商与公司管理层之间的合作内容必须保持一致。这样可以确保每家供应商都达到同等标准，并得到同等对待。

在提高软件安全性的过程中，西门子的 Capital 团队为安全产品和流程的响应和交付树立了达到现代化标准的标杆。在此过程中，Capital 团队还向外界证明了，像 Capital 这样功能强大的大型软件解决方案，尽管其组成非常复杂，但依然可以达到严格的安全要求。

但是，软件供应商并不是打造安全产品的唯一责任方，客户的购买决策及其 RFI 和 RFP 中包含的内容，也会对安全产品的开发产生重大影响。客户应寻求具有稳健 S-SDLC 流程和安全开发文化的供应商。RFI 和 RFP 也应强调，供应商需要对其产品中存在的第三方内容的安全性负责、应当执行 DAST 和 SAST 安全测试，并定期生成良好的安全报告。通过将软件安全作为优先要务，客户和供应商可以确保其产品和流程能够更有效地保护他们的企业。

## 参考信息


1. Gallagher, S（2017 年 10 月 13 号）。国防部确认，澳大利亚国防公司遭受黑客攻击，F-35 资料被窃。Ars Technica。检索网址为 https://arstechnica.com/information-technology/2017/10/australian-defense-firm-was-hacked-and-f-35-data-stolen-dod-confirms/
2. National Institute of Standards and Technology (2018)。美国国家漏洞数据库。检索网址为 https://nvd.nist.gov/
3. 美国在线信任联盟（2017 年 1 月 25 号）。消费者数据泄露事件趋于平稳，但其他事件呈激增态势。美国在线信任联盟。检索网址为 https://otalliance.org/news-events/press-releases/consumer-data-breaches-level-while-other-incidents-skyrocket。
4. Open Web Application Security Project (2018)。欢迎来到 OWASP。Open Web Application Security Project。检索来源 https://www.owasp.org/index.php/Main_Page。

**Siemens Digital Industries Software**

**总部**
Granite Park One
5800 Granite Parkway
Suite 600
Plano, TX 75024
USA
+1 972 987 3000

**美洲**
Granite Park One
5800 Granite Parkway
Suite 600
Plano, TX 75024
USA
+1 314 264 8499

**欧洲**
Stephenson House
Sir William Siemens Square
Frimley, Camberley
Surrey, GU16 8QD
+44 (0) 1276 413200

**亚太地区**
Unit 901-902, 9/F
Tower B, Manulife Financial Centre
223-231 Wai Yip Street, Kwun Tong
Kowloon, Hong Kong
+852 2230 3333

## 关于 Siemens Digital Industries Software

Siemens Digital Industries Software 是 Siemens Digital Industries 的一个业务部门，其致力于推动行业数字化转型，为制造商实现创新创造新机遇，可谓是全球领先的软件解决方案供应商。总部位于美国得克萨斯州普莱诺市，在全球拥有超过 140,000 个客户，并与所有规模的企业协同工作，帮助他们转变将想法变成现实的方式、产品实现方式以及使用和了解运行中产品和资产的方式。有关产品和服务的详细信息，请访问 siemens.com/plm。

**siemens.com.cn/plm**


77783-81579-C4-ZH 2/20 LOC