确保测试系统的安全

- 测试系统与其他工业设备一样，非常容易受到网络攻击。
- 应用分阶段的网络安全方法，消除最有可能的威胁
- 与供应商交流，理解供应链中的上游威胁。

在如今的数字时代，存在安全隐患的测试系统可能会对组织的声誉和销售额造成严重影响，但是确保测试系统的安全并不容易。如果想保护测试系统的安全，又不确定如何开始，那么请参考下面的方法，该方法包含三个阶段。

阶段1. 谨慎将IT的做法应用于测试系统

首先，使用泄露数据可帮助您确定测试系统应借鉴哪些IT安全措施。此数据可让您与IT安全人员一起探讨测试系统存在的风险。2016年Verizon数据泄露调查报告（DBIR）显示，黑客一般会利用供应商发布补丁程序的时间和计算机安装补丁的时间之间的时间差侵入到系统中。系统漏洞通常发生在广泛使用的软件发布补丁后两到七天内，而大多数测试系统无法在该时间段内重新认证。为了尽可能降低风险，请删除不必要的软件，启用尽可能多的实用操作系统安全功能，并将测试系统与IT网络隔离开来。

第二，大多数测试系统并非为处理动态隔离文件或高吞吐量网络数据而设计。在将它们应用于测试系统之前，请仔细评估IT安全技术行为。

第三，利用测试系统特定的安全功能来补充传统的IT安全措施以解决测试系统独有的风险。例如，考虑到数据校准、参数测试和测试序列对于保证测试质量的重要性，您可以使用专为您的测试系统配置的文件完整性监控和校准完整性监控等技术。

阶段2. 评估供应链

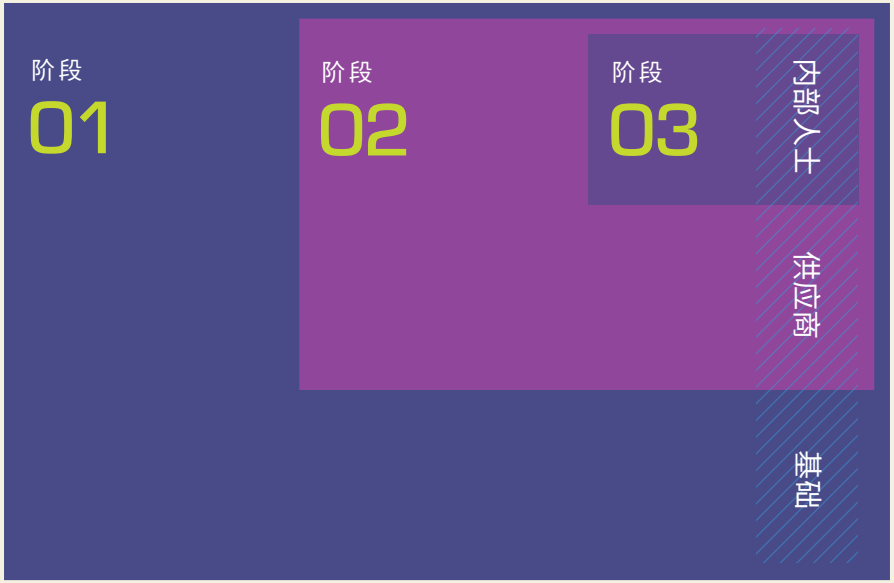
测试系统的完整性依赖于在其整个生命周期中所有组件的完整性多个供应商的合作，降低了仅依赖单一供应商来设计的系统所带来的安全风险。但是这样并不能够弥补由员工学习成本和管理供应商关系带来的长期成本问题。

规范供应链之后，确保系统安全的最重要步骤就是与供应商交流。询问其供应链信息，以及他们如何在开发、制造和执行订单的过程中保护产品的完整性。了解以上流程中的缺漏之处可以帮助您降低供应链受到安全威胁的风险，并有助于您的供应商加强安全措施。如果发现漏洞，请确保您的供应商会对其进行检测，并明确回复应对措施。如果缺少此类对话，则双方可能会因沟通不畅而做出没有依据的决定。

阶段3. 防范内部威胁

众多的相关报道使得内部威胁听起来风险十足，但2016年Verizon DBIR表示内部威胁发生的概率并不高。在2015年超过64,000起网络安全事件报告中，只有172起涉及内部人士滥用特权。75%以上的内幕事件都是由内部原因造成不存在任何外部协助或内部勾结。

克服内部威胁是一个多方面的挑战，仍然需要重点研究。无论是员工还是开发人员，任何可以访问关键测试系统的人员都需多加防范。另外，还需明确业务的最关键部分、参与人员以及权限分配。最重要的步骤是将关键功能的权限授予至少两个人员，这样任何个人都无法危及整个测试系统。



首先消除可能性最高的威胁，然后再采取措施防止公司遭受影响较广的内部威胁。

案例学习

IT做法

2016年，一个资产达数十亿美元的某家公司的制造系统在三个月内多次瘫痪。PLC一直因不明原因而无法运行，直到调查发现了根本原因：IT最近将安全扫描范围扩展到测试系统设备，并且数据包速率超出了PLC的承受范围。不了解测试系统的独特需求将会带来数百万美元的经济损失。

供应链

2014年，Energetic Bear黑客攻击了三家不同的软件供应商，这些供应商在网站上提供了其行业控制系统软件的下载。黑客获取网站上的文件之后，通过插入恶意软件来更改合法的供应商软件安装程序，然后将文件保存在网站上的原始位置。之后客户下载了木马软件并进行安装。这给软件供应商和客户带来的经济影响是无法估量的。

内部威胁

Omega Engineering公司的Timothy Lloyd由于在1996年进行一些威胁公司内部安全的行为变得臭名昭著。当他在车间现场被罢免了系统管理人员的职务时，他安装了一个软件定时炸弹，在他的控制下将系统内所有的制造软件全部删除。这件事给Omega Engineering公司造成了数百万美元的经济损失，导致80人失业，使公司陷入濒临破产的境地。