为安全防护与合规性实现自动化

帮助国防承包商满足、维护并验证合规性

红帽解决方案，帮助实现安全防护和合规性自动化：

- 红帽企业 Linux
- 红帽 Ansible 自动化平台
- 红帽智能分析
- 红帽智能管理
- 红帽 OpenShift
- 红帽 Kubernetes 高级集群管理
- 红帽 Quay

国防承包商面临的安全挑战

美国国防部 （DoD） 承包商面临许多紧迫的挑战，具体包括以下内容：

- **完善网络安全态势。**为了领先于快速发展的网络威胁，必须更深入地了解整体风险状况。
- **验证网络安全控制和流程的实施情况。**这些标准对于持续检测和修复配置偏移并减少人为错误非常必要。
- **在增加功能的同时满足成本限制。**在不显著增加成本的前提下，满足、维护和持续验证合规性并不容易。
- **采用全面的安全防护方法。**机构需要从线性瀑布式项目管理和手动安全检查逐渐过渡到更为敏捷的 DevSecOps 和自动诊断并化解风险。

根据技术要求来验证合规性并保护信息

保护敏感信息仍然是 DoD 和公共部门的重中之重。新兴的网络安全模式通过以下方式应对这一挑战：

- **衡量网络安全风险。**某些信息比其他信息更为敏感，需要加强安全控制。
- **采用更全面的安全防护方法。**网络的边界不断延伸，而仅仅依靠网络安全措施并不能将威胁挡在边界之外。标准化的流程和注重安全的行为对于保护信息至关重要。
- **通过第三方评估验证持续合规性。**机构可能会要求其供应链中的公司通过独立的第三方验证活动来证明合规性。

为什么选择红帽?

- **安全性更强。**我们的解决方案符合严格的美国联邦安全要求。
- **成本更低。**我们的订阅成本低于专有软件许可证的成本，并支持政府项目。
- **合作伙伴生态系统。**红帽维护着包含数千种产品和服务的合作伙伴生态系统，其中的内容经过测试和认证并受到支持，可以使用红帽® 技术进行部署。
- **开源领导者。**我们是开源软件的主要支持者和开发者，我们与开源社区密切合作，提供解决方案，帮助企业或机构取得成功。
- **经验丰富。**我们拥有丰富的专业知识，与美国各地的政府机构合作，助其实现应用开发流程的现代化。

红帽官方微博　红帽官方微信

构建有效的自动化安全防护和合规性策略

红帽技术可带来可见性并增强控制，有助于简化、加速合规流程并降低合规成本。[1]红帽提供值得信赖、经过认证、稳定可靠且受到支持的企业开源软件。为简化集成，我们还与广泛的云、网络和存储生态系统公司合作。红帽产品组合中的工具可以帮助满足技术安全要求，并保持与开源产品的合规性，具有已知的生命周期。

不断变化的网络安全局势要求采取更全面的安全方法，而自动化是安全防护和合规性战略的关键部分。

红帽技术可以帮助您满足并保持与安全要求相关的合规性。

基础架构软件

红帽企业 Linux® 提供了一个以安全为中心的操作系统，其中包含有助于保护环境的内置工具，并符合安全内容自动化协议（SCAP）要求。自 2008 年以来，红帽一直引领开源社区，为 SCAP 定义和构建工具，[2]已获得美国国家标准与技术研究院（NIST）认证，是适用于操作环境的安全强化解决方案。SCAP 附带了**预构建**的安全配置文件，可帮助您遵守 PCI DSS、DISA STIG 和 HIPAA 等行业标准，[3]并支持构建自定义配置文件。

红帽企业 Linux 是稳定可靠的自动化基础，包含安全增强型 Linux（SELinux），定义了系统用户、应用、进程和文件的访问控制。

支持通过一种通用语言来配置网络及各种安全防护和网络工具。

自动化和管理

红帽 Ansible® 自动化平台为系统、应用、工具和流程等各种环境提供简单、灵活、无代理的自动化语言。例如，您可以控制谁有权限来更改配置，并可轻松查看由谁在何时进行了更改。无需替换您现有的安全解决方案和工具，Ansible 自动化平台可以将这些内容连接在一起。Ansible 自动化平台有助于在混合多云环境中集成安全技术并实现互操作性。

红帽智能分析会主动评估红帽企业 Linux 环境，以识别运维风险和安全风险，并提供针对性建议，以在发生更大问题之前快速解决这些风险。

红帽智能管理将红帽智能分析与红帽卫星的强大功能（可提供完整的生命周期管理）与图形用户界面（GUI）相结合，帮助您更安全地管理受红帽企业 Linux 支持的物理机和混合多云等所有环境。

容器平台

适用于 Kubernetes 的红帽 OpenShift® 和红帽高级集群管理通过标准化的部署、升级、修补和安全审计工作流，为管理全球分布式应用平台提供支持。

红帽 Quay 容器镜像仓库提供存储功能，并帮助您构建、分发和部署加密签名的容器。通过自动化、身份验证和授权系统，提高镜像存储库的安全性。

[1] 红帽概述，“借力红帽和 OpenSCAP，改善并实现合规自动化”，2019 年 10 月。

[2] 红帽博客，“红帽正在评估 OpenSCAP，以满足 SCAP 1.2 NIST 标准”，2013 年 3 月 13 日。

[3] 支付卡行业数据安全标准（PCI DSS）、国防信息系统局（DISA）安全技术实施指南（STIG）、健康保险可携性与责任法案（HIPAA）。

服务与支持

我们还为受到严格监管和注重安全的客户提供培训、支持和咨询服务。这些服务可帮助您充分发挥技术投资的价值。

了解更多

自动化、容器化、基础架构生命周期管理和主动操作环境评估可以帮助 DoD 承包商应对合规性挑战。

请访问 redhat.com/gov，进一步了解红帽将如何帮助维护系统的安全性、隐私性和稳定性。

其他资源：

红帽 ATO 路径

用于“合规即代码”的红帽官方 Ansible 角色

红帽知识库中包含通用标准、FIPS 140-2、STIG、USGCB、USGV6 （DoD IPv6）、Section 508 等内容

红帽安全数据，包括开放式漏洞与评估语言（OVAL）定义

销售及技术支持
800 810 2100
400 890 2100

红帽北京办公地址
北京市朝阳区东大桥路 9 号
侨福芳草地大厦 A 座 8 层
邮编: 100020
8610 6533 9300

红帽官方微博　红帽官方微信

关于红帽

红帽是世界领先的企业开源软件解决方案供应商，依托强大的社区支持，为客户提供稳定可靠而且高性能的 Linux、混合云、容器和 Kubernetes 技术。红帽帮助客户集成现有和新的 IT 应用、开发云原生应用，在业界领先的操作系统上开展标准化作业，并实现复杂环境的自动化、安全防护和管理。凭借一流的支持、培训和咨询服务，红帽成为《财富》500 强公司备受信赖的顾问。作为众多云提供商、系统集成商、应用供应商、客户和开源社区的战略合作伙伴，红帽致力于帮助企业做好准备，拥抱数字化未来。

O-F26829