HongKe 虹科

数据表CMMC合规性

CMMC合规

CMMC结合了各种网络安全标准和最佳实践，并将这些控制和流程映射到从基本网络卫生到高级网络卫生的多个成熟度级别。

对于给定的CMMC级别，相关的控制和流程在实施后，将降低针对特定网络威胁的风险。

CMMC的工作建立在现有法规(DFARS 252.204-7012)的基础上，该法规基于信任，通过添加关于网络安全需求的验证组件。

目标是使CMMC具有成本效益，并且小型企业可以在较低的CMMC级别上实现。

授权和认可的CMMC第三方评估机构(C3PAOs)将在适当级别对国防工业基地(DIB)公司进行评估并颁发CMMC证书。

C001

C002
C004

C007

C008
C009
C010

C017

访问控制

定义访问要求

使用Lepide识别哪些用户可以访问敏感数据，并限制只有授权用户才能访问。

限制数据访问

识别具有过多权限的用户。确保只有正确的用户可以访问敏感数据，并从解决方案中撤销过多的权限。

审计与问责制

定义审计要求

使用Lepide审计和记录用户操作、事件和更改，以便跟踪和调查用户操作。

执行审计

使用Lepide对系统、权限、配置和数据所做的更改进行持续审计、监控和警报。

事件响应

检测和报告事件

检测异常或不需要的事件异常检测，实时警报和预定义的报告。

执行事件后检讨

分析事件和所做的更改，以确定事件是如何、在何处以及由谁引起的。

风险管理

识别和评估风险

通过分析安全状态和发现可能导致更高风险的权限、配置或数据的更改，评估数据的风险。

C018

C031

HongKe 虹科

虹科电子科技有限公司

www.haocst.com
network@hkaco.com

广州市黄埔区开泰大道30号佳都PCI科技园6号楼1-7层

T （+86）400 - 999 - 3848
M （+86）135 3349 1614

各分部：广州 | 成都 | 上海 | 苏州 | 西安 | 北京 | 台湾 | 香港 | 日本 | 韩国 | 美国硅谷

版本：V1.0 - 23/09/10

联系我们

获取更多资料

haocst.com