迅达科技

供应商车间设备的 IT 要求

角色和职责：

- 任何供应商向迅达交付IT和OT设备，包括但不限于：服务器、计算机、网络设备、工具，以及安装在此设备上的软件和固件，或任何其他连接网络的设备或控制器（以下统称为“设备”），以用于迅达制造现场的车间，必须满足本文档註明的要求
- 在交付给迅达现场之前，必须先让迅达批准本设备的制造商、型号和技术配置
- 供应商必须能够展示完善的网络安全态势。供应商可能需要完成并提交TTM网络安全调查，说明其对NIST、ISO 27001或CMMC等相关框架的遵守情况，并详细说明其安全控制、政策和风险管理实践
    - 供应商应提交适用于其提供的产品或服务的任何行业网络安全标准认证的副本（例如ISO27001、NIST网络安全框架、CIS）
- 任何与这些标准要求的偏差都必须提前得到TTM的书面批准

一般要求：

- 交付给TTM的设备，如包含操作系统（OS），必须与包含许可証且是当前支持的OS
    - 操作系统必须是最新的，已安装的操作系统的在生命周期结束日期至少还有6个月
    - 供应商应为生命周期终止（EOL）的操作系统做出规划：
        - 如果提供的操作系统的生命周期已经终止，设备应该能够被升级到当时最新且可支持的版本;或
        - 供应商应向TTM提供最新且有支持的版本的新版本设备
- 设备交付给TTM 时，应已安装最新的，60天内的，安全补丁
- 设备和软件必须能够接受定期更新和补丁
- 设备和软件将受到TTM工具的漏洞扫描，需要有操作韧性，不受TTM扫描影响
- 防病毒 – 计算机和服务器都需要运行EDR或防病毒解决方案， 所有AV解决方案必须获得TTM IT Security的批准
- 计算机和服务器必须能够加入Microsoft Active Directory以使用Active Directory帐户执行其预期功能
- 软件必须能夠在沒有管理权限亦能正常运行
- 供应商必须向TTM提供所有设备凭证， 例如：管理员和通用访问用户名和密码
- 供应商必须提供有关其软件和系统的使用、理解和维护（如适用）的完整文档
- 供应商必须提供所有软件和许可证密钥的副本，以用于灾难恢复目的
- 如果供应商将远程提供维护，须使用BeyondTrust（TTM批准的第三方远程访问解决方案）连接
    - 任何其他远程连接方法必须由IT安全部门以书面形式审查和批准
- 在运送到TTM之前，必须从设备中移除所有后门钩和备用远程访问软件
- 处理敏感数据的设备和软件必须具有记录系统和文件访问的能力，所有设备的最短日

志保留时间为 180 天
- 必须禁用设备上的所有非必要软件、端口、协议和服务
  - 应仅启用设备正常运行所需的必要服务
  - 必须禁用或删除所有未使用的软件
- 设备必须能够对传输中和静态数据进行行业标准加密
  - 静态：Windows Server 和桌面必须能够使用经过 FIPS 验证的 Bitlocker 或其他经 TTM 批准的 FIPS 加密方法
  - Linux：LUX 或其他 TTM 批准的加密方法
  - 托管在 TTM 基础设施上的虚拟化服务器或桌面不需要支持 Bitlocker
  - 传输中：IPSEC 或其他 TTM 批准的加密

服务器：

- 新购买的硬件只可以在 2 代之内
- 必须支持 VMWare 8 或更高版本（如果已虚拟化 – OVA 等）
- 支持行业标准的数据加密方法。例如：FIPS 验证加密、TLS 等
- 禁用所有通用、来宾、维护和默认帐户（如果适用）

软件和数据库：

- 用于用户登录和用户数据输入的界面必须是安全的，并且仅使用由可靠的证书颁发机构（CA）签发的证书。示例：HTTPS / TLS / SSH
- 供应商应将系统限制为需要访问的个人，确认最低权限访问原则
- TTM 可以在集团子公司之间转让许可证
- 如果供应商向 TTM 提供定制应用程序，则必需向 TTM 提供源代码
- 任何基于 SaaS 的系统或需要云访问的系统都需要IT 安全部门的书面审查和批准
- 供应商必须及时通知 TTM 他们提供的软件中发现的漏洞，并根据 TTM SLA 中的條文，实施适当的修复或缓解措施，以确保持续的安全性和合规性：
  - 严重 – 5 天
  - 高风险 – 30 天
  - 中风险 – 60 天

网络设备：

- 提供给 TTM 的网络设备的固件必须应用最新的稳定版本
- 网络设备必须从设备制造商或制造商的授权经销商处购买

制造和测试设备：

- 制造和测试设备必须能够在离开供应商之前使用以下协议之一连接到 TTM 的工业 4.0 平台：
    - MODBUS 系列
    - OPC-UA
    - MQTT 协议
    - SECS/GEM – 供应商可能需要支付 SECS/GEM 的费用（如果使用）
    - 通过以下 PLC 驱动程序直接通信：
        - 艾伦·布拉德利
        - Omron FINS TCP/UDP 必须提供英文标签地址的 csv 导出
        - Omron NJ 驱动程序必须提供标记地址的 csv 导出
        - Siemens S7-1500， S7-1200， S7-400， S7-300 必须提供英文标签地址 其他只要满足数据流要求，即可获得 4.0 团队的批准。

注意：当车间设备由 PC 控制时，它将使用上述协议之一连接到 TTM 的工业 4.0 系统