您是否具备深度防御安全策略?

进行自我评估

1 程序安全

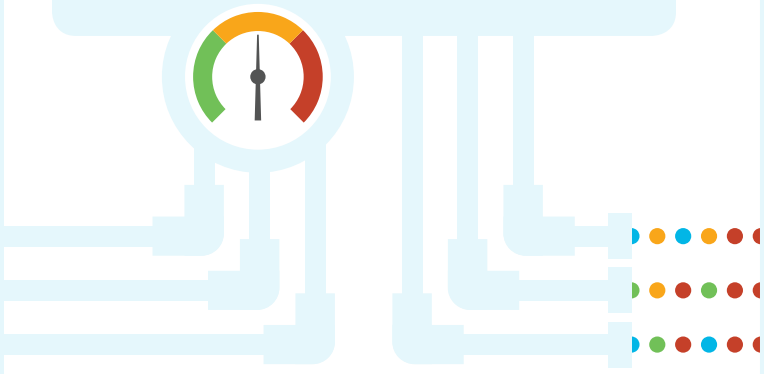
- [ ] 您的所有策略和程序是否都有相应文档记录?
- [ ] 您的员工是否已接受有关策略和程序的培训?
- [ ] 所有策略是否都已在各个站点和设施中统一实施?

2 物理安全

- [ ] 您是否使用监控技术进行实时监控?
- [ ] 您是否已详尽掌握所有机器、设备、业务系统、人员和其他资产的信息?
- [ ] 您是否已对最重要的资产进行评估、评级并确定其优先级?
- [ ] 您是否已规定哪些人有权访问哪些机器和设备?
- [ ] 您是否已限制对安全设备和关键基础设施的物理访问?

3 电子安全

- [ ] 您的生产车间是否仅使用管理型交换机?
- [ ] 您的网络是否划分为多个区域和管道?
- [ ] 您是否在工业网络和外部网络之间使用工业隔离区 (DMZ)?
- [ ] 您是否对 OT 和 IT 网络安全实施集中控制?
- [ ] 您的网络是否支持对员工、供应商和合作伙伴实施基于情景感知的接入管理?
- [ ] 您的网络边缘是否受到以下措施的保护:
  - 防火墙和入侵防御?
  - 远程接入 VPN?
  - 深度数据包检测?
  - 最新行业标准协议?
- [ ] 您是否已拥有涵盖风险评估和应对方案的补救计划?
- [ ] 您的网络能否快速调配并安全可靠地适配新的连接?



问题的回答结果与您的期望不符?

要了解思科互联工厂解决方案的更多信息，请访问：CISCO.COM/GO/MANUFACTURING。