The Top CIS critical security controls

If your customers aren't familiar with the CIS controls, make them aware of them and discuss how you can assist with the implementation.

Basic CIS controls

1 **Inventory and control of hardware assets—**
identifying the systems and devices that need to be secured

2 **Inventory and control of software assets—**
identifying, tracking and accounting for all the software in a network

3 **Continuous vulnerability management—**
identifying what the vulnerabilities are and how to address them

4 **Controlled use of administrative privileges—**
limiting and managing administrator access (through methods such as multifactor authentication)

5 **Secure configurations for hardware and software on devices, laptops, workstations and servers—**
disabling unused services and ports, changing default accounts, updating protocols and examining other methods of reducing the devices' attack surfaces

6 **Maintenance, monitoring and analysis of audit logs—**
ensuring the accurate and timely logging of all security events

Foundational CIS controls

7 **Email and web browser protections—**
focusing on the security of web browsers and email clients, which are vulnerable to attack vectors

8 **Malware defenses—**
concentrating on the steps to implement a strong defense against malware intrusions

9 **Network posts, protocols and services controls and limitations—**
ensuring that the process and tools employed aren't intrusive and don't impact the availability or reliability of the system

10 **Data recovery capabilities—**
implementing the processes for performing system backups for data recovery capability

11 **Secure configurations for network defenses—**
making sure firewalls, routers and switches are configured to deny by default and that there's redundancy

12 **Boundary defense—**
managing information flow between networks, especially those with different degrees of security

13 **Data protection—**
enabling encryption of all sensitive data

14 **Controlled access based on the need to know—**
making sure devices that directly impact mission-critical operations are logically and physically segmented from general-purpose workstations

15 **Wireless access control—**
securing all wireless access points; keeping software security patches and product upgrades current throughout the wireless infrastructure

16 **Account monitoring and control—**
managing user access to systems on the network (through authentication)