EzeCastle INTEGRATION

CYBERSECURITY CHECKLIST

Levels of Protection **Aligned with the Center for Internet Security (CIS) Controls** *CIS Controls provide actionable ways to prevent cyber threats*	**Standard** *baseline protection*	**Advanced** *Next-level protection*
Control #1: Inventory and Control of Hardware Assets		
• Automated Hardware Inventory	●	●
• Quarantine or Removal of Unauthorized Assets	●	●
• Certificate Based Hardware Authentication		●
• Switch Port Level Access Control		●
• Network Admission Control		●
Control #2: Inventory and Control of Software Assets		
• Automate Software Inventory	●	●
• Removal of Unauthorized Software	●	●
• Application Whitelisting		●
Control #3: Continuous Vulnerability Management		
• Continuous External Vulnerability Scanning	●	●
• Continuous Internal Vulnerability Scanning		●
• Automated Software Patching	●	●
Control #4: Controlled Use of Administrative Privileges		
• Restricted Use of Administrative Privileges	●	●
• Centralized Logging of Administrative Permission Use	●	●
• Inventory of Privileged Accounts	●	●
• Privileged Account Management		●
Control #5: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers		
• Deploy Standard Configurations	●	●
• Manage/Enforce Configurations	●	●
• Security Baselining Tools		●

Levels of Protection	Standard *baseline protection*	Advanced *Next-level protection*
Control #6: Maintenance, Monitoring and Analysis of Audit Logs		
• Centralized Logging	●	●
• Security Information and Event Management (SIEM)		●
Control #7: Email and Web Browser Protections		
• Next-Generation Firewalls	●	●
• Email Filtering & Anti-Phishing Service	●	●
• Anti-Phishing Training Campaigns	●	●
• DNS Level Filtering	●	●
• Email Attachment Sandboxing	●	●
Control #8: Malware Defenses		
• Anti-Virus/Anti-Malware	●	●
• Endpoint Protection	●	●
• Malware Sandboxing & Detonation		●
• Anti-Exploit Technologies		●
Control #9: Limitation and Control of Network Ports, Protocols and Services		
• Regularly Validate Open Network Resources	●	●
• Host-based Firewalls	●	●
• Application Firewalls		●
Control #10: Data Recovery Capabilities		
• Perform Regular Secure Encrypted Backups	●	●
• Regularly Test Backup Integrity	●	●
• Ensure Backups are Inaccessible Using OS Protocols	●	●

Levels of Protection	Standard *baseline protection*	Advanced *Next-level protection*
Control #11: Secure Configurations for Network Devices (Firewalls, Routers and Switches)		
• Maintain Standard Network Documentation	●	●
• Centralize Management with Policy	●	●
• Use Dedicated Administration Systems	●	●
Control #12: Boundary Defense		
• Encryption in Transit	●	●
• Multi-factor Authentication	●	●
• Next-Generation Firewalls	●	●
• Network Intrusion Detection Systems		●
Control #13: Data Protection		
• Data Inventory Systems	●	●
• Endpoint Protection Systems	●	●
• Whole Disk Encryption	●	●
• Removable Media Restrictions	●	●
• Data Classification Systems		●
Control #14: Controlled Access Based on the Need to Know		
• Host-based Firewalls	●	●
• Encryption in Transit	●	●
• Implement Microsegmentation		●
• Data Loss Prevention		●
Control #15: Wireless Access Control		
• Ensure WiFi Networks are Subject to Security Policies, Strong Authentication, Encryption, Firewalls, IDS, etc.	●	●
• Segment Guest and Privileged Networks	●	●
• Centralize Management	●	●

Levels of Protection **Aligned with the Center for Internet Security (CIS) Controls** *CIS Controls provide actionable ways to prevent cyber threats*	**Standard** *baseline protection*	**Advanced** *Next-level protection*
Control #16: Account Monitoring and Control		
• Inventory/Document Accounts	●	●
• Password Vaults	●	●
• Disable Accounts in Timely Fashion	●	●
• Centralize Account Management	●	●
• Single Sign-on		●
• Security Information and Event Management		●
Control #17: Implement a Security Awareness and Training Program		
• Security Awareness Training	●	●
• Social Engineering/Anti-Phishing Training	●	●
Control #18: Application Software Security		
• Code Review		●
• Vulnerability Testing		●
Control #19: Incident Response and Management		
• Written Information Security Plan (WISP)	●	●
• Incident Response Plan	●	●
• Tabletop Exercises	●	●
Control #20: Penetration Tests and Red Team Exercises		
• Penetration Testing		●
• Red Team Exercises, which simulate the actions of an attacker		●

Contact Us:

P: 1-800-752-1382 or +44 207 071 6802 | **E:** sales@eci.com | **W:** www.eci.com/contact

Learn more: www.eci.com/cybersecurity