☑ **CCDC Checklist**

---

0 – Pre-Game

- ☐ Confirm all team roles and communication channels
- ☐ Identify scored services and assign watchers (scoring engine may appear as an unknown user)
- ☐ Define credential change plan and change order
- ☐ Prepare inject submission templates and documentation format

---

Startup (First 15 Minutes)

- ☐ Change all default and weak passwords, preserving scored connectivity
- ☐ Enable host firewalls to allow only scored ports and management access
- ☐ Disable all non-scored and unnecessary services
- ☐ Enable system logging and auditing on every host
- ☐ Terminate suspicious or unnecessary sessions without impacting scoring
- ☐ Record initial host state: hostname, IPs, services, and abnormalities

---

1 – Assessment

- ☐ Inventory all systems and running services
- ☐ Map network connectivity (no VLAN segmentation)
- ☐ Capture configs, startup tasks, and scheduled jobs
- ☐ Restrict management access paths and enforce access control

---

2 – Access Control

- ☐ Audit all user accounts, groups, and privileges
- ☐ Treat unknown accounts as potentially scored; avoid deletions without validation
- ☐ Apply strong password and lockout policies
- ☐ Review administrative access (sudo, Administrators, SSH keys, tokens)

---

3 – Services & Persistence

- ☐ Disable all non-essential or redundant services
- ☐ Review configurations for all scored services
- ☐ Locate and remove persistence mechanisms (cron, systemd, WMI, startup tasks)

---

4 – Network

- ☐ Verify open ports align with the scoreboard

- [ ] Configure firewalls for default-deny inbound; allow only scored and management traffic
- [ ] Inspect routing tables, ARP cache, and gateways for anomalies
- [ ] Secure network shares and restrict anonymous access

---

5 – File System

- [ ] Identify dangerous permissions, SUID/SGID files, and recent unauthorized changes
- [ ] Clean webroots of shells, backdoors, or unsafe upload handlers
- [ ] Verify file permissions across critical directories

---

6 – Logging & Monitoring

- [ ] Enable and centralize logs
- [ ] Configure log rotation and retention
- [ ] Monitor authentication and service activity continuously
- [ ] Track configuration and service changes

---

7 – System Hardening

- [ ] Apply patches to critical and remotely exploitable services
- [ ] Enforce secure OS and service defaults
- [ ] Disable insecure protocols and legacy features (e.g., SMBv1, Telnet)

---

8 – Application Security

- [ ] Harden web and database configurations
- [ ] Enforce strong credentials and principle of least privilege
- [ ] Rotate all application and database secrets
- [ ] Disable dangerous functions, directory listings, and sample apps

---

9 – Backup & Recovery

- [ ] Create live backups of configurations and critical data
- [ ] Verify backup integrity and storage location security
- [ ] Maintain a quick-restore process for scored systems

---

10 – Continuous Operations

- [ ] Continuously verify all scored services remain operational
- [ ] Monitor for new IOCs and block malicious IPs
- [ ] Maintain real-time change and incident logs
- [ ] Communicate status updates and submit inject reports promptly

---

Incident Response

- [ ] Maintain service availability while responding to incidents
- [ ] Isolate compromised systems through host or network controls
- [ ] Capture volatile data and logs before remediation
- [ ] Identify IOCs, remove persistence, rotate credentials
- [ ] Restore affected services and verify scoring functionality
- [ ] Document all findings and report to the white team

Every 15 Minutes

- [ ] Confirm all scored services are green
- [ ] Review logs and detect new IOCs
- [ ] Check inject assignments and progress
- [ ] Update team log with current system changes and handoffs