digicert®

TLS/SSL CERTIFICATE MANAGEMENT BEST PRACTICES CHECKLIST

When trying to increase transparency, reduce human error and eliminate rogue certificates, it pays to have a checklist.

1. IDENTIFY

- ☐ Get a baseline of all certificates issued
- ☐ Locate where all certificates are installed
- ☐ Name owners of all certificates and domains
- ☐ Identify web server O/S and application versions
- ☐ Pinpoint web server cipher suites and SSL versions

2. REMEDIATE

- ☐ Remove weak keys, cipher suites and hashes
- ☐ Control wildcard certificate issuance and distribution
- ☐ Deploy appropriate certificate types
- ☐ Control all default vendor certificates
- ☐ Ensure all web services have latest patches installed

3. PROTECT

- ☐ Standardize and automate issuance and renewal process
- ☐ Install and renew all certificates in a timely manner
- ☐ Ensure that private keys are not reused when certificates are renewed
- ☐ Install certificates and private keys in a secure manner
- ☐ Address certificate removal/revocation during decommissioning process

4. MONITOR

- ☐ Scan networks for new systems and changes
- ☐ Check Certificate Transparency (CT) logs for rogue certificates
- ☐ Use CAA to prevent unauthorized certificate requests