digicert®

Early detection, remediation and compliance: 3 top reasons CT log monitoring is critical to your website's security

Certificate Transparency (CT) logs are publicly visible records that are maintained by several large Certificate Authorities (CAs) like DigiCert, or Internet Service Providers (ISPs). These records provide insight into the TLS/SSL certificate ecosystem by allowing anyone to access information about the issuance and existence of a certificate.

Similar to registering your vehicle at the DMV, CAs are required to register their digital certificates to CT logs the minute they are issued in order to track domain ownership and prevent malicious actors from illegally obtaining control of a web domain or website.

CT logs make websites and internet transactions more secure for everyone by providing legitimacy to CAs and the roots certificates are issued from.

1 DETECT VULNERABILITIES FIRST:

Monitoring CT logs can help you detect unauthorized certificates in a few hours—instead of days, weeks, or months.

2 QUICKER REMEDIATION:

CT logs help you identify certificates that need to be revoked, allowing you to quickly communicate with the issuing Certificate Authority (CA) and shorten the process of removing them.

3 .GOV COMPLIANCE:

.Gov Compliance: Starting in early 2019, per an emergency directive from the cybersecurity branch of Department of Homeland Security (DHS), all domains ending with .gov must be monitored by CT logs to avoid Domain Name System tampering.

Ready to start monitoring your certificates with CT log monitoring? Get DigiCert Secure Site Pro—which includes CT log monitoring—and start tracking your certificates today. Reach out to a DigiCert sales representative to get Secure Site Pro or learn more here.