digicert®

# DETECCIÓN CRIPTOGRÁFICA DE DIGICERT®

Detección exhaustiva para elaborar un registro central

## Resumen

El objetivo de la detección es elaborar un registro central para gestionar los distintos grupos de activos. Con él, podrá aplicar políticas, identificar las vulnerabilidades, actualizar los algoritmos e integrar la automatización en los activos objetivo o las clases de certificados que se desee.

DigiCert® Trust Lifecycle Manager (TLM) ofrece visibilidad y control centralizados para el análisis, la importación y la gestión de certificados y claves criptográficas en los entornos corporativos, además de proporcionar información clave para centralizar la gestión y la planificación de la PKI y prepararse para los algoritmos resistentes a la informática cuántica.

TLM utiliza diferentes mecanismos para garantizar que ningún certificado quede sin detectar, con el fin de que las empresas no sufran interrupciones que podrían salirles muy caras.

## Cifras clave

**Más de 50 000**
Certificados de servidor empresariales

**1200**
Certificados empresariales sin gestionar

**47 %**
Porcentaje de empresas con certificados fraudulentos

**500 000 $**
Coste por hora de las interrupciones relacionadas con los certificados

## Mecanismos de detección

**Integración con CertCentral y CA Manager**
Esta integración optimiza la gestión del ciclo de vida de los certificados (CLM) desde la emisión hasta la centralización, lo que le permite detectar estos certificados fácilmente. Esta capacidad tan completa es algo que la mayoría de proveedores de CLM compatibles con cualquier CA no ofrecen.

**Integración con CA de terceros**
La mayoría de las soluciones basadas en CA no detectan aquellos certificados que no se hayan originado en ellas, un aspecto que los proveedores de soluciones antiguas compatibles con cualquier CA utilizan como argumento de venta insistentemente. Sin embargo, Trust Lifecycle Manager es diferente porque, a pesar de ser una solución basada en la CA, es compatible con cualquier CA.

**Análisis basado en puertos**
El análisis basado en puertos es el método más básico para detectar certificados que no provienen directamente de una CA. Una solución de CLM coloca un sensor en su entorno de TI y se encarga del arduo trabajo de buscar los certificados.

**Sensores que encuentran los certificados en los equilibradores de carga**
Trust Lifecycle Manager utiliza sus sensores para automatizar los certificados en los equilibradores de carga, algo que resulta esencial si tenemos en cuenta el elevado número de certificados que se suelen asociar a los equilibradores de carga.

**Herramientas de análisis basadas en agentes**
Algunos certificados, como los instalados en servidores web de Microsoft IIS o Apache, no se pueden detectar con el análisis basado en puertos. Para hacerlo, TLM recurre a agentes que recopilan información específica sobre dichos certificados.

**Herramientas de análisis de vulnerabilidades**
TLM utiliza soluciones de detección de vulnerabilidades que ya analizan cada rincón de la red para crear y mantener un inventario y mapa completos del entorno de la empresa.

# Características destacadas de DigiCert® Discovery

### Visibilidad mejorada
Obtenga una vista centralizada de todos los activos criptográficos para facilitar la gestión y la emisión de certificados en todos los entornos corporativos.

### Menos riesgos
Identifique y solucione los problemas rápidamente, como los algoritmos débiles, los archivos binarios sin firmar y los certificados que estén a punto de caducar, que sean vulnerables o que incumplan la normativa.

### Aplicación de políticas más rigurosa
Minimice la emisión de certificados de una autoridad de certificación de origen dudoso y siga de cerca el cumplimiento de la política de seguridad.

### Agilidad criptográfica
La detección de los activos es el primer paso para incorporar la criptografía poscuántica, además de proporcionar visibilidad y movimiento dinámico a los activos criptográficos de una empresa.

### Integración con Tenable
TLM es compatible con los certificados detectados en Tenable, que utiliza diversos tipos de complementos para analizar y detectar los datos.

### Integración con Qualys
Gracias a la integración entre la solución de gestión, detección y respuesta a vulnerabilidades VMDR de Qualys y los productos de DigiCert, los clientes pueden gestionar y automatizar los activos criptográficos que detecten en sus análisis de vulnerabilidades.

### AWS y Microsoft CA
A medida que avanza la migración a la nube, muchas empresas cuentan con certificados emitidos desde AWS Private CA, Microsoft CA u otras autoridades de certificación. Por eso, necesitan poder detectar certificados emitidos por estas CA, de modo que puedan importarlos a sus inventarios centrales y catalogarlos.

# Dé el primer paso hoy mismo

Empiece a disfrutar de las ventajas de los servicios de PKI de DigiCert®. Póngase en contacto con un gestor de cuentas de DigiCert o envíe un correo electrónico a sales@digicert.com.

# Acerca de DigiCert, Inc.

DigiCert es el proveedor número uno del mundo de confianza digital. Gracias a él, tanto los usuarios individuales como las empresas pueden utilizar Internet con la tranquilidad de saber que su presencia en el mundo digital está protegida. La plataforma DigiCert® ONE, garantía de confianza digital, protege los sitios web, los accesos y comunicaciones empresariales, el software, las identidades, el contenido y los dispositivos para que las empresas respondan a toda una gama de necesidades en materia de confianza pública y privada con una visibilidad y un control centralizados.

Su galardonado software y su liderazgo en el sector de los estándares, la asistencia y las operaciones convierten a DigiCert en el proveedor de confianza digital al que recurren las grandes empresas de todo el mundo. Para obtener más información, visite digicert.com/es o siga a @digicert.