Los 18 controles críticos de seguridad

Los Controles de Seguridad Cítricos (CIS) de CIS son un conjunto prescriptivo, priorizado y simplificado de mejores prácticas que puede usar para fortalecer su postura de ciberseguridad.

Esta última versión, CIS Controls v8.1, incluye una alineación actualizada con los estándares y marcos de la industria en evolución, las clases de activos revisadas y las descripciones de Salvaguardia, así como la adición de la función de seguridad de “Gobernanza”.

CIS Control 1: Inventario y control de activos empresariales

Administre activamente (inventario, seguimiento y correcto) todos los activos empresariales (dispositivos de usuario final, incluidos los dispositivos portátiles y móviles; dispositivos de red; dispositivos que no son de computación / Internet de las cosas (IoT); y servidores) conectados a la infraestructura física, virtual, remota y aquellas dentro de los entornos de nube para conocer con precisión la totalidad de los activos que deben ser monitoreados y protegidos dentro de la empresa. Esto también apoyará la identificación de activos no autorizados y no administrados para eliminar o remediar.

CIS Control 2: Inventario y control de activos de software

Administre activamente (inventario, seguimiento y corrección) todo el software (sistemas operativos y aplicaciones) en la red para que solo se instale y pueda ejecutar software autorizado, y que el software no autorizado y no administrado se encuentre y se impida la instalación o ejecución.

CIS Control 3: Protección de datos

Desarrollar procesos y controles técnicos para identificar, clasificar, manejar, retener y disponer de datos de forma segura.

CIS Control 4: Configuración segura de activos y software empresariales

Establecer y mantener la configuración segura de los activos empresariales (dispositivos de usuario final, incluidos los portátiles y móviles; dispositivos de red; dispositivos no informáticos/IoT; y servidores) y software (sistemas y aplicaciones de operación).

CIS Control 5: Gestión de Cuentas

Utilice procesos y herramientas para asignar y administrar la autorización a credenciales para cuentas de usuario, incluidas las cuentas de administrador, así como las cuentas de servicio, a los activos y el software de la empresa.

CIS Control 6: Gestión de control de acceso

Utilice procesos y herramientas para crear, asignar, administrar y revocar credenciales y privilegios de acceso para las cuentas de usuario, administrador y servicio de los activos y software de la empresa.

CIS Control 7: Gestión Continua De La Vulnerabilidad

Desarrollar un plan para evaluar y rastrear continuamente las vulnerabilidades en todos los activos empresariales dentro de la infraestructura de la empresa, con el fin de remediar y minimizar la ventana de oportunidad para los atacantes. Monitorear fuentes de la industria pública y privada para obtener nueva información sobre amenazas y vulnerabilidades.

CIS Control 8: Gestión de registro de auditoría

Recopile, alerte, revise y retenga los registros de auditoría de eventos que podrían ayudar a detectar, comprender o recuperarse de un ataque.

CIS Control 9: Protección de correo electrónico y navegador web

Mejore las protecciones y detecciones de amenazas de correo electrónico y vectores web, ya que estas son oportunidades para que los atacantes manipulen el comportamiento humano a través del compromiso directo.

Control 10 de la CEI: Defensas contra malware

Prevenir o controlar la instalación, propagación y ejecución de aplicaciones, código o scripts maliciosos en los activos empresariales.

Control CIS 11: Recuperación de datos

Establecer y mantener prácticas de recuperación de datos suficientes para restaurar los activos empresariales integrados a un estado preincidente y de confianza.

CIS Control 12: Gestión de infraestructura de red

Establecer, implementar y administrar activamente (rastrear, informar, corregir) dispositivos de red, con el fin de evitar que los atacantes exploten los servicios de red vulnerables y los puntos de acceso.

CIS Control 13: Monitoreo y Defensa de Red

Opere procesos y herramientas para establecer y mantener un monitoreo y defensa integrales de la red contra las amenazas de seguridad en toda la infraestructura de red y la base de usuarios de la empresa.

CIS Control 14: Concienciación sobre seguridad y capacitación en habilidades

Establecer y mantener un programa de conciencia de seguridad para influir en el comportamiento entre la fuerza laboral para

ser consciente de la seguridad y debidamente capacitado para reducir los riesgos de ciberseguridad para la empresa.

CIS Control 15: Gestión de proveedores de servicios

Desarrollar un proceso para evaluar a los proveedores de servicios que tienen datos confidenciales, o son responsables de las plataformas o procesos críticos de TI de una empresa, para garantizar que estos proveedores estén protegiendo esas plataformas y datos de manera adecuada.

CIS Control 16: Seguridad del software de aplicación

Administre el ciclo de vida de seguridad del software interno desarrollado, alojado o adquirido para prevenir, detectar y remediar las debilidades de seguridad antes de que puedan afectar a la empresa.

CIS Control 17: Gestión de la respuesta a incidentes

Establecer un programa para desarrollar y mantener una capacidad de respuesta a incidentes (por ejemplo, políticas, planes, procedimientos, roles definidos, capacitación y comunicaciones) para preparar, detectar y responder rápidamente a un ataque.

Control CIS 18: Pruebas de penetración

Pruebe la efectividad y la resiliencia de los activos empresariales a través de la identificación y la explotación de debilidades en los controles (personas, procesos y tecnología) y la simulación de los objetivos y acciones de un atacante.


CONTROL 01
Inventory and Control of Enterprise Assets
5 Safeguards
IG1 2/5
IG2 4/5
IG3 5/5
CONTROL 02
Inventory and Control of Software Assets
7 Safeguards
IG1 3/7
IG2 6/7
IG3 7/7
CONTROL 03
Data Protection
14 Safeguards
IG1 6/14
IG2 12/14
IG3 14/14
CONTROL 04
Secure Configuration of Enterprise Assets and Software
12 Safeguards
IG1 7/12
IG2 11/12
IG3 12/12
CONTROL 05
Account Management
6 Safeguards
IG1 4/6
IG2 6/6
IG3 6/6
CONTROL 06
Access Control Management
8 Safeguards
IG1 5/8
IG2 7/8
IG3 8/8
CONTROL 07
Continuous Vulnerability Management
7 Safeguards
IG1 4/7
IG2 7/7
IG3 7/7
CONTROL 08
Audit Log Management
12 Safeguards
IG1 3/12
IG2 11/12
IG3 12/12
CONTROL 09
Email and Web Browser Protections
7 Safeguards
IG1 2/7
IG2 6/7
IG3 7/7
CONTROL 10
Malware Defenses
7 Safeguards
IG1 3/7
IG2 7/7
IG3 7/7
CONTROL 11
Data Recovery
5 Safeguards
IG1 4/5
IG2 5/5
IG3 5/5
CONTROL 12
Network Infrastructure Management
8 Safeguards
IG1 1/8
IG2 7/8
IG3 8/8
CONTROL 13
Network Monitoring and Defense
11 Safeguards
IG1 0/11
IG2 6/11
IG3 11/11
CONTROL 14
Security Awareness and Skills Training
9 Safeguards
IG1 8/9
IG2 9/9
IG3 9/9
CONTROL 15
Service Provider Management
7 Safeguards
IG1 1/7
IG2 4/7
IG3 7/7
CONTROL 16
Applications Software Security
14 Safeguards
IG1 0/14
IG2 11/14
IG3 14/14
CONTROL 17
Incident Response Management
9 Safeguards
IG1 3/9
IG2 8/9
IG3 9/9
CONTROL 18
Penetration Testing
5 Safeguards
IG1 0/5
IG2 3/5
IG3 5/5