IS 20 CONTROLS™

IS20 Security Controls ™

DATOS CLAVE

Nombre del curso:

General Security – Top 20 Information Systems Security Controls

Maps to SANS Security 440 & ISC2 CAP (Certification and Accreditation Professional)

Duración:

3 días

Idioma:

Español

Formato:

* Aula con instructor

Pre-requisitos:

* Conocimientos básicos en seguridad de redes y seguridad en tecnología

Track de Certificaciones:

* Mile2's ISSC (Information Systems Security Controls) & ICS2 CAP

DESCRIPCIÓN DEL CURSO

El curso IS 20 Controls de Mile2 cubre los controles probados y metodologías que son usados para ejecutar y analizar el Top 20 de los controles más críticos de seguridad. Este curso permite al profesional de seguridad ver cómo implementar controles en las redes de manera eficaz, automatizada y económica. Para la Administración, este curso es la mejor manera de distinguir cómo se evaluará si los controles de seguridad están bien implementados

VALOR DEL CURSO

Casi todas las organizaciones contienen información sensible y están implementando y adoptando los más altos sistemas de seguridad como prioridad. Estos controles fueron escogidos por el gobierno y organizaciones privadas expertas en cómo funcionan los ataques y qué es lo que se puede hacer para mitigarlos y prevenirlos. Estos expertos en seguridad eligieron lo mejor que hay en controles de seguridad para bloquear los incidentes conocidos así como paliar los daños de ataques exitosos. Por último, la implementación de este Top 20 de controles, asegurará mejores esfuerzos para disminuir drásticamente el costo total de seguridad mientras se mejoran en eficacia y eficiencia.

¿QUIÉN DEBE TOMAR EL CURSO?

- Auditores/ Gerentes de seguridad de Información
- Adminstradores e Implementadores de Sistemas
- Ingenieros en Seguridad de Redes
- Administradores de TI
- Agencias Federales
- Empresas de Seguridad en TI, consultorías

HISTORIA

Los expertos comenzaron a recopilar el llamado “Top 20 de Controles de Seguridad” (Consensus Audit Guidelines) en 2008 después de que una serie de compañías de Estados Unidos sufrieron pérdidas de información, a consecuencia de ciber ataques. Con el alza de estos ataques, muchos expertos en defensa y ciber ataques reunieron sus conocimientos de estas técnicas de ataques que fueron usadas en contra del gobierno e instancias. Esta reunión dio lugar a el “Top 20 de Controles de Seguridad” necesario para asegurar la integridad de los activos de una organización.

El proyecto CAG fue liderado por John Gilligan, quien se desempeño como Jefe de Información para la fuerza aérea de Estados Unidos y el Departamento de Energía. Alguna vez Gilligan declaró “Era obvio que las organizaciones deben implementar estos controles, también afirmó "si usted sabe que los ataques se llevan a cabo tiene la responsabilidad de dar prioridad a las inversiones en seguridad para detener esos ataques”. http://www.zdnet.com/us-dept-of-defense-lists-top-20-security-controls-3039617669/

CNSS

gs TM GENERAL SECURITY

AL CONCLUIR

El estudiante será capaz de realizar confiadamente el examen Mile2 IS20 Controls y entender el *SANS Security 440 el estudiante disfrutará de un curso en profundidad que se actualiza continuamente para mantener e incorporar el entorno de seguridad en constante cambio. Este curso ofrece los últimos estudios de casos de propiedad que se han investigado y desarrollado por los profesionales de seguridad líderes de todo el mundo.

MÓDULOS DEL CURSO

- Course Introduction
- Critical Control 1: Inventory of Authorized and Unauthorized Devices
- Critical Control 2: Inventory of Authorized and Unauthorized Software
- Critical Control 3: Secure Configurations for Hardware and Software on Laptops, Workstations, and Servers
- Critical Control 4: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
- Critical Control 5: Boundary Defense
- Critical Control 6: Maintenance, Monitoring, and Analysis of Audit Logs
- Critical Control 7: Application Software Security
- Critical Control 8: Controlled Use of Administrative Privileges
- Critical Control 9: Controlled Access Based on Need to Know
- Critical Control 10: Continuous Vulnerability Assessment and Remediation
- Critical Control 11: Account Monitoring and Control
- Critical Control 12: Malware Defenses
- Critical Control 13: Limitation and Control of Network Ports, Protocols, and Services
- Critical Control 14: Wireless Device Control
- Critical Control 15: Data Loss Prevention
- Critical Control 16: Secure Network Engineering
- Critical Control 17: Penetration Tests and Red Team Exercises
- Critical Control 18: Incident Response Capability
- Critical Control 19: Data Recovery Capability
- Critical Control 20: Security Skills Assessment and Appropriate Training to Fill Gaps