CompTIA

Security+

CompTIA Security+ es la principal certificación global que establece las habilidades esenciales necesarias para las funciones de seguridad esenciales y para una carrera profesional en seguridad informática. Demuestra las capacidades de los profesionales para proteger redes, aplicaciones y dispositivos, garantizando la integridad, confidencialidad y disponibilidad de los datos. CompTIA Security+ se centra en habilidades prácticas para afrontar los desafíos del mundo real. Al ser la credencial más reconocida, es fundamental para progresar en el dinámico campo de la ciberseguridad.

Objetivos del curso

Conceptos generales de seguridad (12%)

- **Controles de seguridad:** comparación de controles técnicos, preventivos, gerenciales, disuasorios, operativos, detectivos, físicos, correctivos, compensatorios y directivos.
- **Conceptos fundamentales:** resumen de confidencialidad, integridad y disponibilidad (CIA); no repudio; autenticación, autorización y contabilidad (AAA); confianza cero; y tecnología de engaño/disrupción.
- **Gestión de cambios:** explicación de procesos de negocio, implicaciones técnicas, documentación y control de versiones.
- **Soluciones criptográficas:** uso de infraestructura de clave pública (PKI), cifrado, ofuscación, hash, firmas digitales y blockchain.

Amenazas, vulnerabilidades y mitigaciones (22%)

- **Actores de amenazas y motivaciones:** comparación de estados-nación, atacantes no calificados, hacktivistas, amenazas internas, crimen organizado, TI en la sombra y motivaciones como la exfiltración de datos, el espionaje y las ganancias financieras.
- **Vectores de amenaza y superficies de ataque:** explicación de redes no seguras basadas en mensajes, ingeniería social, archivos, llamadas de voz, cadena de suministro y vectores de software vulnerables.
- **Vulnerabilidades:** explicación de las vulnerabilidades basadas en aplicaciones, hardware, dispositivos móviles, virtualización, sistemas operativos (SO), específicas de la nube, basadas en la Web y en la cadena de suministro.

- **Actividad maliciosa:** análisis de ataques de malware, ataques de contraseñas, ataques de aplicaciones, ataques físicos, ataques de red y ataques criptográficos.
- **Técnicas de mitigación:** uso de segmentación, control de acceso, aplicación de configuración, refuerzo, aislamiento y aplicación de parches.

Arquitectura de seguridad (18%)

- **Modelos de arquitectura:** comparación de instalaciones locales, en la nube, virtualización, Internet de las cosas (IoT), sistemas de control industrial (ICS) e infraestructura como código (IaC).
- **Enterprise infrastructure:** applying security principles to infrastructure considerations, control selection, and secure communication/access.
- **Data protection:** comparing data types, securing methods, general considerations, and classifications.
- **Resilience and recovery:** explaining high availability, site considerations, testing, power, platform diversity, backups, and continuity of operations

Security operations (28%)

- **Computing resources:** applying secure baselines, mobile solutions, hardening, wireless security, application security, sandboxing, and monitoring.
- **Asset management:** explaining acquisition, disposal, assignment, and monitoring/tracking of hardware, software, and data assets.
- **Vulnerability management:** identifying, analyzing, remediating, validating, and reporting vulnerabilities.
- **Alerting and monitoring:** explaining monitoring tools and computing resource activities.
- **Enterprise security:** modifying firewalls, IDS/IPS, DNS filtering, DLP (data loss prevention), NAC (network access control), and EDR/XDR (endpoint/extended detection and response).
- **Identity and access management:** implementing provisioning, SSO (single sign-on), MFA (multifactor authentication), and privileged access tools.
- **Automation and orchestration:** explaining automation use cases, scripting benefits, and considerations.
- **Incident response:** implementing processes, training, testing, root cause analysis, threat hunting, and digital forensics.
- **Data sources:** using log data and other sources to support investigations.

Security program management and oversight (20%)

- **Security governance:** summarizing guidelines, policies, standards, procedures, external considerations, monitoring, governance structures, and roles/responsibilities.
- **Risk management:** explaining risk identification, assessment, analysis, register, tolerance, appetite, strategies, reporting, and business impact analysis (BIA).
- **Third-party risk:** managing vendor assessment, selection, agreements, monitoring, questionnaires, and rules of engagement.
- **Security compliance:** summarizing compliance reporting, consequences of non-compliance, monitoring, and privacy.
- **Audits and assessments:** explaining attestation, internal/external audits, and penetration testing.
- **Security awareness:** implementing phishing training, anomalous behavior recognition, user guidance, reporting, and monitoring.

Habilidades aprendidas

- Identificar varios tipos de amenazas, ataques y vulnerabilidades, incluido malware, ingeniería social y ataques de aplicaciones.
- Utilice tecnologías y herramientas de seguridad, como firewalls, sistemas de detección de intrusiones y seguridad de puntos finales, para proteger los sistemas.
- Diseñar arquitecturas de redes seguras, implementar sistemas seguros y aplicar protocolos seguros para la arquitectura y el diseño.
- Gestionar los conceptos de identidad y acceso, incluida la autenticación, la autorización y la contabilidad, para garantizar un control de acceso seguro.
- Evaluar y gestionar el riesgo mediante análisis de riesgos, estrategias de mitigación y planificación de la continuidad del negocio.
- Aplicar conceptos de criptografía, incluidos algoritmos de cifrado, infraestructura de clave pública (PKI) y firmas digitales, para proteger datos.
- Implementar medidas de cumplimiento y seguridad operativa, incluidas políticas de seguridad, procedimientos y mejores prácticas.