Hoy en día, los cibercriminales envalentonados están recurriendo a legítimos recursos en línea. Lixivian la capacidad del servidor, roban datos y exigir rescates de las víctimas en línea cuya información tienen rehén. El crecimiento explosivo en el tráfico de Internet impulsado en gran parte por velocidades más rápidas de móviles y la proliferación de en línea

Los dispositivos trabajan a su favor ayudando a expandir el ataque, superficie. Afrontar los crecientes desafíos de la ciberdelincuencia, ciberespionaje, amenazas internas y amenazas persistentes avanzadas.

Las organizaciones están estableciendo equipos de seguridad SOC profesionales que pueden monitorear, detectar y responder rápidamente a incidentes de seguridad antes de que causen daños.

Obtenga habilidades de seguridad cibernética listas para la carrera
“Se espera que la demanda de profesionales de la ciberseguridad aumente a 6 millones a nivel mundial para 2019.” (Un millón de ofertas de trabajo en ciberseguridad en 2016, Forbes). Los estudiantes pueden obtener listo para este mercado de trabajo en demanda al obtener conocimientos de seguridad cibernética listos para la carrera y habilidades del currículo de Operaciones de Ciberseguridad de CCNA.

El plan de estudios de Operaciones de Ciberseguridad de CCNA proporciona un primer paso para adquirir conocimientos y habilidades necesarios para trabajar con un equipo SOC, y puede ser una parte valiosa de comenzando una carrera en el emocionante y creciente campo de las operaciones de ciberseguridad. El plan de estudios ayuda a preparar a los estudiantes para las oportunidades de carrera de ciberseguridad de nivel de entrada y está alineado con el examen Comprender los aspectos fundamentales de la seguridad cibernética de Cisco (210-250 SECFND) e implementación del examen de Cisco Cybersecurity Operations (210-255 SECOPS) llevando a la certificación de operaciones de ciberseguridad de Cisco CCNA.

El curso proporciona habilidades prácticas, relevantes y listas para el trabajo alineadas estrechamente con las Tareas específicas esperadas de los profesionales de SOC a través de los siguientes componentes:

- Contenido interactivo, multimedia.
- Actividades, laboratorio práctico virtual, actividades de Packet Tracer que refuerzan el aprendizaje
- Enlaces a artículos y sitios web para mejorar el aprendizaje sobre temas específicos
- Pruebas y exámenes para verificar que los estudiantes comprendan la información.

MÓDULO	OBJETIVOS DE APRENDIZAJE
Capítulo 1. La ciberseguridad y la Operaciones de seguridad Centrar	● Explicar el rol del Analista de Operaciones de Ciberseguridad en la empresa. ● Explicar por qué las redes y los datos son atacados. ● Explicar cómo prepararse para una carrera en ciberseguridad operaciones.
Capítulo 2. Windows Sistema operativo	● Explicar las características del sistema operativo Windows y Características necesarias para soportar los análisis de ciberseguridad. ● Explicar el funcionamiento del sistema operativo Windows. ● Explicar cómo asegurar los puntos finales de Windows.
Capítulo 3. Linux Sistema operativo	● Explicar las características y características del funcionamiento del Sistema de Linux . ● Realizar operaciones básicas en el shell de Linux. ● Realizar tareas básicas de administración de Linux.
Capítulo 4. Red Protocolos y Servicios	● Analizar el funcionamiento de los protocolos y servicios de red. ● Explicar cómo los protocolos Ethernet e IP soportan la red comunicaciones y operaciones. ● Explicar cómo los servicios de red habilitan la funcionalidad de red.
Capítulo 5. Infraestructura de la Red	● Explicar las topologías de red y el funcionamiento de la red. ● Explicar cómo se utilizan los dispositivos y servicios para mejorar la seguridad de la infraestructura red. ● Explicar cómo los dispositivos de red permiten cableado e inalámbrico la red de comunicacion.
Capítulo 6. Principios de Seguridad de la red	● Clasificar los distintos tipos de ataques a la red. ● Explicar cómo se atacan las redes. ● Explicar los distintos tipos de amenazas y ataques.
Capítulo 7. Red Ataques: Una mirada más profunda	● Usar herramientas de monitoreo de red para identificar ataques contra protocolos y servicios de red. ● Explicar el monitoreo del tráfico de red. ● Explicar cómo las vulnerabilidades de TCP / IP habilitan los ataques de red. ● Explicar cómo las aplicaciones y servicios de red comunes son vulnerable al ataque.

MÓDULO	OBJETIVOS DE APRENDIZAJE
Capítulo 8. Protección la red	● Usar varios métodos para prevenir el acceso malicioso a la computadora, Redes, hosts y datos. ● Explicar enfoques para la defensa de la seguridad de la red. ● Usa varias fuentes de inteligencia para ubicar la seguridad actual amenazas
Capítulo 9. Infraestructura de la criptografía y la clave pública	● Explicar los impactos de la criptografía en la seguridad de la vigilancia de la red. ● Usar herramientas para cifrar y descifrar datos. ● Explicar cómo la infraestructura de clave pública (PKI) soporta la seguridad de red.
Capítulo 10. Punto final Seguridad y análisis	● Explicar las vulnerabilidades de punto final y la investigación del proceso de ataques. ● Usar herramientas para generar un informe de análisis de malware. ● Clasificar información de evaluación de vulnerabilidad de punto final.
Capítulo 11. Monitoreo de la Seguridad	● Evaluar las alertas de seguridad de la red. ● Explicar cómo las tecnologías de seguridad afectan el monitoreo de seguridad. ● Explicar los tipos de archivos de registro utilizados en la supervisión de seguridad.
Capítulo 12. Intrusión y Análisis de los datos	● Analizar datos de intrusión de red para identificar hosts comprometidos y vulnerabilidades. ● Explicar cómo se recopilan los datos relacionados con la seguridad. ● Analizar datos de intrusión para determinar la fuente de un ataque.
Capítulo 13. Incidente, Respuesta y Manejo.	● Explicar cómo se manejan los incidentes de seguridad de red CSIRTs. ● Aplicar modelos de respuesta a incidentes, como NIST 800-61r2 a un incidente de seguridad. ● Use un conjunto de registros para aislar a los actores de amenazas y recomendar una plan de respuesta a incidentes.