छत्रपति शाहूजी महाराज यूनिवर्सिटी के लिए
साइबर सिक्योरिटी वोकेशनल कोर्स
C3iHub द्वारा संचालित

साइबर सिक्योरिटी वोकेशनल कोर्स के बारे में :

यह पाठ्यक्रम साइबर सुरक्षा के सबसे महत्वपूर्ण तत्वों की पड़ताल करता है जिसमे सिस्टम सुरक्षा, एप्लीकेशन सुरक्षा, नेटवर्क सुरक्षा, ऑपरेटिंग सिस्टम सुरक्षा एवं क्रिप्टोग्राफ़ी सुरक्षा शामिल है। पाठ्यक्रम पूरी तरह से ऑनलाइन है जो छात्रों को साइबर सुरक्षा का मौलिक और व्यवहारिक अनुभव प्रदान करता है। इस पाठ्यक्रम का एक अभिन्न भाग अनुकूलित प्रयोगशालाएं हैं जो आभासी प्रयोगशालाओं (वर्चुअल लैब) के माध्यम से प्रत्येक छात्र के सिस्टम पर उपलब्ध कराई जाएंगी।

सीखने के परिणाम:

1. यह प्रोग्राम आपको प्रोटोकॉल सुइट्स के सन्दर्भ में वास्तविक समय की साइबर सुरक्षा तकनीकों और विधियों का परिचय देता है और नेटवर्क सुरक्षा समाधानों पर शिक्षा देता है।
2. यह प्रोग्राम साइबरस्पेस की तकनीकी नींव और सम्बंधित साइबर मुद्दों को समझने में मदद करता है।
3. यह प्रोग्राम शिक्षार्थियों को सामान्य साइबर सुरक्षा सम्बंधित जोखिमों और कमजोरियों के मूलभूत ज्ञान से अवगत कराता है।

पाठ्यक्रम में नामांकन से छात्र को क्या मिलेगा?

- LMS (लर्निंग मैनेजमेंट सिस्टम) पर पीपीटी स्लाइड्स
- पीपीटी में उपलब्ध करायी गयी पठन सामग्री का सन्दर्भ
- लेक्चर में दी गई पठन सामग्री का अभ्यास करने हेतु वर्चुअल लैब
- LMS (लर्निंग मैनेजमेंट सिस्टम) पर व्याख्यान रिकॉर्डिंग

पाठ्यक्रम सामग्री:

1. साइबर सुरक्षा का परिचय

a. साइबर सुरक्षा का परिचय

i. बुनियादी सुरक्षा अवधारणाएं : गोपनीयता, अखंडता, उपलब्धता

ii. साइबर सुरक्षा का महत्व

b. साइबर सुरक्षा बनाम साइबर अपराध

i. आधुनिक साइबर खतरों के प्रकार: मैलवेयर, फ़िशिंग, मैन इन द मिडिल अटैक, डिनायल ऑफ़ सर्विस/ डिस्ट्रिब्यूटेड डिनायल ऑफ़ सर्विस अटैक

c. MITRE TTPs एवं साइबर किल चेन का परिचय

d. वास्तविक दुनिया के साइबर हमलों पर चर्चा

i. वास्तविक दुनिया के कुछ साइबर धोखाधड़ी व साइबर अपराध के मामले

2. साइबर खतरा परिदृश्य

a. मैलवेयर के प्रकार: वायरस, ट्रोजन्स, वर्म्स, ट्रोजन्स, रैंसमवेयर

b. फिशिंग हमले : तकनीक व रोकथाम

c. सोशल इंजीनियरिंग : सोशल इंजीनियरिंग प्रयासों को पहचानना व उनका जवाब देना

d. विभिन्न साइबर धोखाधड़ी/साइबर अपराध के तरीके

i. OTP धोखाधड़ी , डीपफेक आधारित धोखाधड़ी , वॉयस क्लोनिंग, साइबर बुलिंग, साइबर एक्सटॉर्शन

ii. विभिन्न साइबर अपराध रिपोर्टिंग नंबर व वेबसाइटे

e. साइबर युद्ध की अवधारणा व चिंता

f. IT एक्ट 2008 व् DPDP एक्ट 2023 की रुपरेखा

3. डाटा सुरक्षा एवं एन्क्रिप्शन

a. डाटा बैकअप एवं रिकवरी का महत्त्व

b. डाटा एन्क्रिप्शन : एन्क्रिप्शन तकनीकों को समझना

c. ऑनलाइन लेन देन एवं वित्तीय जानकारी को सुरक्षित करना/रखना

4. डिजिटल उपकरणों और नेटवर्क को सुरक्षित रखना

a. डिवाइस सुरक्षा: कंप्यूटर, स्मार्ट फ़ोन और टेबलेट्स की सुरक्षा करना

b. नेटवर्क सुरक्षा की मूल बातें : वाई फाई सुरक्षा, फायरवॉल इत्यादि

c. सुरक्षित वेब ब्राउज़िंग प्रथाएं

d. https, SSL certificate को समझना , अपना स्वयं का SSL certificates बनाना एवं इसकी सीमाओं को समझना ,PKI की आवश्यकता

5. एप्लीकेशन सुरक्षा

a. सुरक्षित कोडिंग सिद्धांत

b. सामान्य कोडिंग कमज़ोरियाँ : SQL इंजेक्शन, क्रॉस साइट स्क्रिप्टिंग, CSRF इत्यादि

c. OWASP Top 10, Burp Suite का परिचय

6. ऑपरेटिंग सिस्टम सुरक्षा

a. यूजर एकाउंट्स को समझना (लिनक्स एवं विंडोज)

b. फाइल एवं डायरेक्टरी की अनुमतियाँ

c. एंटी वायरस एवं उसका उपयोग

d. आवेदन एवं निष्पादन नियंत्रण

e. अपडेट एवं पैचिंग

f. DNS hijacking, DNS poisoning और सार्वजानिक वाई फाई व सार्वजनिक खुले नेटवर्क का उपयोग करने की समस्या के खतरों को समझना

LMS का उपयोग करने के निर्देश:

स्टेप 1: कृपया इंटरनेट का उपयोग करते हुए https://eictcourses.iitk.ac.in/ पर जायें

स्टेप 2: यूजर नेम में अपनी यूनिवर्सिटी का एनरोलमेंट नंबर एवं पासवर्ड में यूनिवर्सिटी का रोल नंबर प्रेषित करें

स्टेप 3: साइन इन पर क्लिक करें

स्टेप 4: “my courses” पे क्लिक करें

स्टेप 5: “Cybersecurity Vocational Course” पर क्लिक करें और कोर्स को वीडियो के माध्यम से शुरू करें

अन्य जानकारियां :

1. यह कोर्स आपको IIT कानपुर के लर्निंग मैनेजमेंट सिस्टम (LMS) द्वारा प्रदान किया जा रहा है अतः यह अति आवश्यक है कि आप इस LMS को भली भांति जानें।

2. https://eictcourses.iitk.ac.in/ पर लॉगिन करने के बाद आप “FAQs” सेक्शन में जा कर वहाँ उपलब्ध सभी वीडियो को देख लें जिसके बाद आप LMS को आसानी से उपयोग कर सकते हैं।

3. यह आपको अन्य सेक्शन के उपयोग के बारे में जानकारी देगा।

हमसे सपंर्क करें : आप हम से इस कोर्स से सम्बंधित आने वाली विभिन्न समस्याओं के लिए संपर्क कर सकते हैं, कृपया विशेष समस्या के लिए उससे सम्बंधित दिए गए नंबर पर ही संपर्क करें:

1. यदि आपको लर्निंग मैनेजमेंट सिस्टम (LMS) से सम्बंधित कोई समस्या है तो आप हमे इन नंबर व ईमेल आईडी पर संपर्क करें:

मोबाइल नंo: 9219972805, 9219972806

ईमेल आई डी: support@ifacet.iitk.ac.in

2. यदि आपको सामान्य जानकारी लेनी है एवं कोर्स सम्बंधित कोई प्रश्न है तो आप हमे इन नंबर व ईमेल आई डी पर संपर्क करें:

लैंडलाइन नंo :

0512-679-2544/2545/2126

ईमेल आई डी:

techacademy@c3ihub.iitk.ac.in

infocsjmif@csjmu.ac.in

3. लैब व तकनीकी सम्बंधित जानकारी व समस्या हेतु कृपया 0512-679-2541 पर कॉल करें।

एडिटोरियल टीम

नेहा श्रीवास्तव

Deputy Manager, C3iHub - IIT Kanpur

आदित्य सिंह गौर

Deputy Manager, C3iHub - IIT Kanpur

Contact Us

C3iHub

C3iHub
2nd Floor , Technopark
Phase 1, IIT Kanpur
UP - 208016
www.c3ihub.org

CSJMIF

Chhatrapati Shahu ji Maharaj Innovation Foundation (CSJMIF), 1st Floor, Shopping Complex, CSJMU, Kalyanpur, Kanpur, UP-208024