

# Corso Universitario

## Analisi e Sviluppo di Malware



## Corso Universitario Analisi e Sviluppo di Malware

- » Modalità: online
- » Durata: 6 settimane
- » Titolo: TECH Global University
- » Accredimento: 6 ECTS
- » Orario: a tua scelta
- » Esami: online

Accesso al sito web: [www.techtute.com/it/informatica/corso-universitario/analisi-sviluppo-malware](http://www.techtute.com/it/informatica/corso-universitario/analisi-sviluppo-malware)

# Indice

01

Presentazione

---

*pag. 4*

02

Obiettivi

---

*pag. 8*

03

Direzione del corso

---

*pag. 12*

04

Struttura e contenuti

---

*pag. 16*

05

Metodologia

---

*pag. 20*

06

Titolo

---

*pag. 28*

# 01

# Presentazione

In un contesto digitale in cui le risorse aziendali dipendono in modo critico dalla sicurezza informatica, la costante minaccia del malware rappresenta una sfida significativa. A questo proposito, la proliferazione di attacchi maligni evidenzia l'urgenza di avere professionisti altamente qualificati in questo settore. In questo senso, il programma affronta l'esigenza prevalente di esperti che non solo comprendano la complessità delle minacce digitali, ma siano anche in grado di progettare strategie proattive per il loro rilevamento e mitigazione. Gli studenti approfondiranno quindi gli strumenti essenziali per salvaguardare l'integrità dei sistemi in un ambiente aziendale sempre più digitalizzato. Con la flessibilità della modalità 100% online, questo corso garantisce l'accessibilità e l'aggiornamento continuo necessari per affrontare le mutevoli sfide del cyberspazio.



“

*Diventa un esperto di malware con nuove tecniche di analisi dinamica grazie a questo esclusivo programma online al 100%”*

Nell'attuale panorama della sicurezza informatica, la sofisticazione delle minacce informatiche ha raggiunto livelli senza precedenti, generando una domanda crescente di professionisti specializzati nell'Analisi e nello Sviluppo di Malware. La costante evoluzione delle tattiche dannose richiede una risposta altrettanto dinamica da parte degli esperti di sicurezza informatica. In questo contesto, il presente programma universitario di TECH emerge come una soluzione completa per soddisfare queste esigenze. Progettato per fornire agli studenti conoscenze avanzate, la comprensione approfondita della natura del malware fino alla valutazione di strumenti anti-malware. Questo approccio integrato prepara ad affrontare le minacce attuali e future.

Il piano di studio del programma in Analisi e Sviluppo di Malware di TECH si pone come un solido compendio di conoscenze che abbraccia diverse dimensioni del mondo del malware. Gli studenti approfondiranno le varie forme e gli obiettivi del malware, acquisendo conoscenze avanzate sulla sua natura, funzionalità e comportamento. Il programma approfondisce l'analisi forense applicata al malware, fornendo agli studenti le competenze necessarie per identificare indicatori di compromissione (IoC) e modelli di attacco, cruciali per il rilevamento tempestivo e la risposta efficace agli incidenti di sicurezza. Inoltre, il percorso si concentra sullo sviluppo di competenze specifiche per valutare e selezionare strumenti di sicurezza anti-malware. Gli studenti impareranno a discernere l'efficacia di questi strumenti e la loro adattabilità a particolari ambienti, essenziale per attuare strategie di difesa efficaci.

Con un approccio innovativo e adattabile, questo programma universitario si presenta come una proposta di formazione unica. La modalità online al 100% e la metodologia *Relearning* garantiscono un'esperienza educativa flessibile ed efficiente, consentendo ai professionisti di progredire nella loro carriera senza interruzioni e adattarsi continuamente alle mutevoli esigenze del settore della cibersicurezza.

Questo **Corso Universitario in Analisi e Sviluppo di Malware** possiede il programma più completo e aggiornato del mercato. Le caratteristiche principali del programma sono:

Sviluppo di casi pratici presentati da esperti in Analisi e Sviluppo di Malware

- ♦ Contenuti grafici, schematici ed eminentemente pratici che forniscono informazioni aggiornate e pratiche sulle discipline essenziali per l'esercizio della professione
- ♦ Esercizi pratici che offrono un processo di autovalutazione per migliorare l'apprendimento
- ♦ Particolare enfasi sulle metodologie innovative
- ♦ Lezioni teoriche, domande all'esperto e/o al tutor, forum di discussione su questioni controverse e compiti di riflessione individuale
- ♦ Contenuti disponibili da qualsiasi dispositivo fisso o mobile dotato di connessione a internet



*Padroneggerai l'analisi delle chiamate con API in sole 6 settimane della migliore formazione online"*



“

*Affronterai la generazione di Shellcode nell'università meglio valutata al mondo dai suoi studenti secondo la piattaforma Trustpilot (4,9/5)”*

Il personale docente del programma comprende rinomati specialisti del settore, che forniscono agli studenti le competenze necessarie a intraprendere un percorso di studio eccellente.

I contenuti multimediali, sviluppati in base alle ultime tecnologie educative, forniranno al professionista un apprendimento coinvolgente e localizzato, ovvero inserito in un contesto reale.

La creazione di questo programma è incentrata sull'Apprendimento Basato su Problemi, mediante il quale il professionista deve cercare di risolvere le diverse situazioni che gli si presentano durante il corso. Lo studente potrà usufruire di un innovativo sistema di video interattivi creati da esperti di rinomata fama.

*Avrai accesso a un sistema di apprendimento basato sulla ripetizione, grazie a un insegnamento semplice e graduale durante l'intero programma.*

*Approfondirai l'offuscamento di Strings. Dai alla tua carriera la spinta di cui ha bisogno!*



# 02 Obiettivi

Questo piano di studi ha lo scopo principale di formare gli studenti nella padronanza di conoscenze avanzate su natura, funzionalità e comportamento del malware. Durante il programma, gli studenti approfondiranno le varie forme e gli obiettivi del malware, consentendo loro di analizzare e sviluppare efficaci strategie difensive nel campo della cibersicurezza. Inoltre, questo approccio olistico mira a formare professionisti in grado di affrontare le sfide emergenti nel rilevamento, analisi e mitigazione delle minacce malware in ambienti digitali complessi. Inoltre, l'utilizzo di una metodologia online al 100% rende l'apprendimento flessibile dando la possibilità di accedere in qualsiasi momento e luogo.





“

*Raggiungerai i tuoi obiettivi grazie agli strumenti didattici di TECH, tra cui video esplicativi e riassunti interattivi”*



## Obiettivi generali

---

- ◆ Acquisire competenze avanzate nei test di penetrazione e nelle simulazioni di Red Team, affrontando l'identificazione e lo sfruttamento delle vulnerabilità di sistemi e reti
- ◆ Sviluppare capacità di leadership per coordinare team specializzati nella cibersecurity offensiva, ottimizzando l'esecuzione di progetti di Pentesting e Red Team
- ◆ Sviluppare competenze nell'analisi e nello sviluppo di malware, comprendendone le funzionalità e applicando misure difensive ed educative
- ◆ Affinare le capacità di comunicazione producendo relazioni tecniche ed esecutive dettagliate, presentando i risultati in modo efficace a un pubblico tecnico ed esecutivo
- ◆ Promuovere una pratica etica e responsabile nel campo della sicurezza informatica, tenendo conto dei principi etici e legali in tutte le attività



*Vuoi sperimentare un salto di qualità nella tua carriera? Grazie a TECH acquisirai competenze nell'analisi forense applicata al malware"*





## Obiettivi specifici

---

- ◆ Acquisire una conoscenza avanzata della natura, della funzionalità e del comportamento del malware, comprendendone le varie forme e gli obiettivi
- ◆ Sviluppare competenze nell'analisi forense applicata al malware, consentendo l'identificazione degli indicatori di compromissione (IoC) e dei modelli di attacco
- ◆ Apprendere strategie per il rilevamento e la prevenzione efficace di malware, compresa l'implementazione di soluzioni di sicurezza avanzate
- ◆ Familiarizzare con lo sviluppo di malware a scopo educativo e difensivo, consentendo una comprensione approfondita delle tattiche utilizzate dagli hacker
- ◆ Promuovere pratiche etiche e legali nell'analisi e nello sviluppo di malware, garantendo integrità e responsabilità in tutte le attività
- ◆ Promuovere pratiche etiche e legali nell'analisi e nello sviluppo di malware, garantendo integrità e responsabilità in tutte le attività
- ◆ Sviluppare le competenze per valutare e selezionare gli strumenti di sicurezza anti-malware, considerando la loro efficacia e adattabilità ad ambienti specifici
- ◆ Imparare a implementare una mitigazione efficace contro le minacce dannose, riducendo l'impatto e la diffusione del malware su sistemi e reti
- ◆ Promuovere una collaborazione efficace con i team di sicurezza, integrando strategie e sforzi per la protezione dalle minacce malware



# 03

## Direzione del corso

Il programma in Analisi e Sviluppo di Malware dispone di un personale docente eccezionalmente qualificato. TECH ha selezionato esperti con una vasta esperienza e un prestigio riconosciuto in aziende leader del settore della cibersecurity. Questo personale docente, composto da professionisti di riferimento, apporta non solo la sua esperienza pratica nell'analisi e nello sviluppo di malware, ma anche il suo impegno nella formazione di futuri specialisti, garantendo un insegnamento aggiornato e allineato alle esigenze e alle sfide attuali nel campo della cibersecurity.





“

*Aggiornati sulla configurazione di macchine virtuali e snapshot con i migliori esperti del settore. Dai uno slancio alla tua carriera con TECH!”*



## Direzione



### Dott. Gómez Pintado, Carlos

- Responsabile di Cibersicurezza e Rete CIPHERBIT presso Grupo Oesía
- Responsabile *Advisor & Investor* presso Wesson App
- Laurea in Ingegneria del Software e Tecnologie della Società dell'Informazione, Università Politecnica di Madrid
- Collabora con istituzioni educative per la preparazione di cicli di formazione di livello superiore in materia di cibersicurezza



# 04

## Struttura e contenuti

Questo programma universitario fornirà agli studenti una profonda immersione nel mondo del malware, concentrandosi sul suo sviluppo a fini educativi e difensivi. Nel corso del programma, gli studenti affronteranno le complessità del malware, consentendo una comprensione dettagliata delle tattiche utilizzate dagli aggressori. A questo proposito, l'approccio equilibrato del piano di studi non solo incoraggia l'acquisizione di conoscenze avanzate nell'analisi del malware, ma consente anche agli studenti di sviluppare strategie difensive essenziali nel campo della cibersecurity.

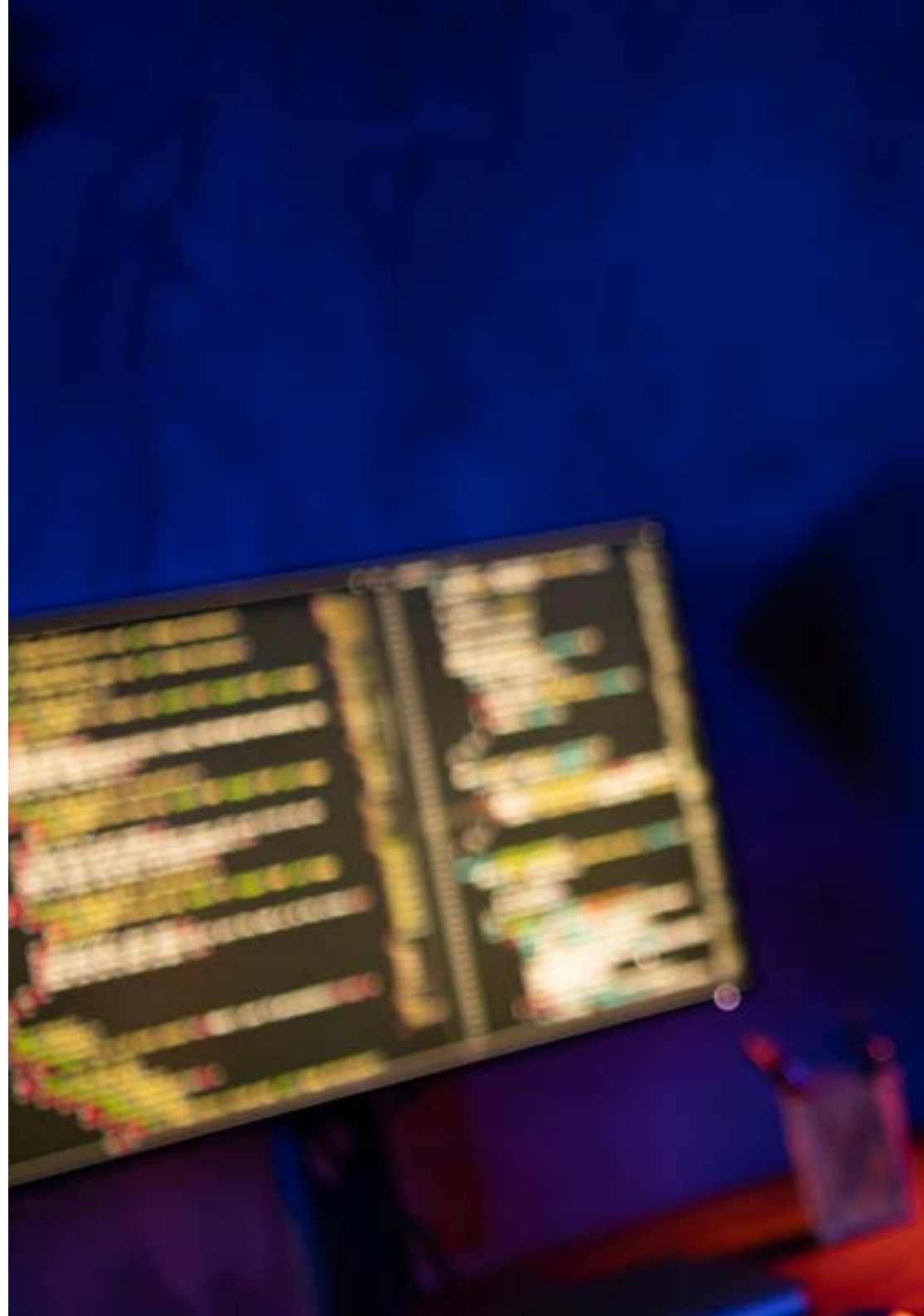


“

*Avrai accesso a un programma di studio elaborato da un personale docente di grande prestigio, che ti garantirà un apprendimento di successo”*

## Modulo 1. Analisi e Sviluppo di Malware

- 1.1. Analisi e Sviluppo di Malware
  - 1.1.1. Storia ed evoluzione di malware
  - 1.1.2. Classificazione e tipi di malware
  - 1.1.3. Analisi del malware
  - 1.1.4. Sviluppo di malware
- 1.2. Preparazione dell'ambiente
  - 1.2.1. Configurazione di Macchine Virtuali e Snapshots
  - 1.2.2. Strumenti di analisi del malware
  - 1.2.3. Strumenti di sviluppo del malware
- 1.3. Fondamenti di Windows
  - 1.3.1. Formato dei file PE (Portable Executable)
  - 1.3.2. Processo e Threads
  - 1.3.3. Sistemi di archivio e registro
  - 1.3.4. Windows Defender
- 1.4. Tecniche di malware di base
  - 1.4.1. Generazione di shellcode
  - 1.4.2. Esecuzione di shellcode su disco
  - 1.4.3. Disco vs memoria
  - 1.4.4. Esecuzione di shellcode su memoria
- 1.5. Tecniche di malware intermedie
  - 1.5.1. Persistenza di Windows
  - 1.5.2. Cartella Home
  - 1.5.3. Chiavi di registro
  - 1.5.4. Screensaver
- 1.6. Tecniche di malware avanzate
  - 1.6.1. Crittografia di shellcode (XOR)
  - 1.6.2. Crittografia di shellcode (RSA)
  - 1.6.3. Offuscamento di strings
  - 1.6.4. Iniezione di processi





- 1.7. Analisi statica di malware
  - 1.7.1. Analisi dei packers con DIE (Detect It Easy)
  - 1.7.2. Analisi delle sezioni con PE-Bear
  - 1.7.3. Decompilazione con Ghidra
- 1.8. Analisi dinamica di malware
  - 1.8.1. Analisi del comportamento con Process Hacker
  - 1.8.2. Analisi delle chiamate con API Monitor
  - 1.8.3. Analisi delle modifiche al registro di sistema con Regshot
  - 1.8.4. Analisi delle richieste di rete con TCPView
- 1.9. Analisi in .NET
  - 1.9.1. Introduzione a .NET
  - 1.9.2. Decompilazione con dnSpy
  - 1.9.3. Debug con dnSpy
- 1.10. Analisi di malware reali
  - 1.10.1. Preparazione dell'ambiente
  - 1.10.2. Analisi statica dei malware
  - 1.10.3. Analisi dinamica dei malware
  - 1.10.4. Creazione di regole YARA



*Non perdere l'opportunità di promuovere la tua carriera con questo programma innovativo”*

# 05 Metodologia

Questo programma ti offre un modo differente di imparare. La nostra metodologia si sviluppa in una modalità di apprendimento ciclico: ***il Relearning***.

Questo sistema di insegnamento viene applicato nelle più prestigiose facoltà di medicina del mondo ed è considerato uno dei più efficaci da importanti pubblicazioni come il ***New England Journal of Medicine***.



“

*Scopri il Relearning, un sistema che abbandona l'apprendimento lineare convenzionale, per guidarti attraverso dei sistemi di insegnamento ciclici: una modalità di apprendimento che ha dimostrato la sua enorme efficacia, soprattutto nelle materie che richiedono la memorizzazione”*



## Caso di Studio per contestualizzare tutti i contenuti

Il nostro programma offre un metodo rivoluzionario per sviluppare le abilità e le conoscenze. Il nostro obiettivo è quello di rafforzare le competenze in un contesto mutevole, competitivo e altamente esigente.

“

*Con TECH potrai sperimentare un modo di imparare che sta scuotendo le fondamenta delle università tradizionali in tutto il mondo"*



*Avrai accesso a un sistema di apprendimento basato sulla ripetizione, con un insegnamento naturale e progressivo durante tutto il programma.*



*Imparerai, attraverso attività collaborative e casi reali, la risoluzione di situazioni complesse in ambienti aziendali reali.*

## Un metodo di apprendimento innovativo e differente

Questo programma di TECH consiste in un insegnamento intensivo, creato ex novo, che propone le sfide e le decisioni più impegnative in questo campo, sia a livello nazionale che internazionale. Grazie a questa metodologia, la crescita personale e professionale viene potenziata, effettuando un passo decisivo verso il successo. Il metodo casistico, la tecnica che sta alla base di questi contenuti, garantisce il rispetto della realtà economica, sociale e professionale più attuali.

“ *Il nostro programma ti prepara ad affrontare nuove sfide in ambienti incerti e a raggiungere il successo nella tua carriera* ”

Il Metodo Casistico è stato il sistema di apprendimento più usato nelle migliori Scuole di Informatica del mondo da quando esistono. Sviluppato nel 1912 affinché gli studenti di Diritto non imparassero la legge solo sulla base del contenuto teorico, il metodo casistico consisteva nel presentare loro situazioni reali e complesse per prendere decisioni informate e giudizi di valore su come risolverle. Nel 1924 fu stabilito come metodo di insegnamento standard ad Harvard.

Cosa dovrebbe fare un professionista per affrontare una determinata situazione?

Questa è la domanda con cui ti confrontiamo nel metodo dei casi, un metodo di apprendimento orientato all'azione. Durante il corso, gli studenti si confronteranno con diversi casi di vita reale. Dovranno integrare tutte le loro conoscenze, effettuare ricerche, argomentare e difendere le proprie idee e decisioni.



## Metodologia Relearning

TECH coniuga efficacemente la metodologia del Caso di Studio con un sistema di apprendimento 100% online basato sulla ripetizione, che combina diversi elementi didattici in ogni lezione.

Potenziamo il Caso di Studio con il miglior metodo di insegnamento 100% online: il Relearning.

*Nel 2019 abbiamo ottenuto i migliori risultati di apprendimento di tutte le università online del mondo.*

In TECH imparerai con una metodologia all'avanguardia progettata per formare i manager del futuro. Questo metodo, all'avanguardia della pedagogia mondiale, si chiama Relearning.

La nostra università è l'unica autorizzata a utilizzare questo metodo di successo. Nel 2019, siamo riusciti a migliorare il livello di soddisfazione generale dei nostri studenti (qualità dell'insegnamento, qualità dei materiali, struttura del corso, obiettivi...) rispetto agli indicatori della migliore università online.



Nel nostro programma, l'apprendimento non è un processo lineare, ma avviene in una spirale (impariamo, disimpariamo, dimentichiamo e re-impariamo). Pertanto, combiniamo ciascuno di questi elementi in modo concentrico. Questa metodologia ha formato più di 650.000 laureati con un successo senza precedenti in campi diversi come la biochimica, la genetica, la chirurgia, il diritto internazionale, le competenze manageriali, le scienze sportive, la filosofia, il diritto, l'ingegneria, il giornalismo, la storia, i mercati e gli strumenti finanziari. Tutto questo in un ambiente molto esigente, con un corpo di studenti universitari con un alto profilo socio-economico e un'età media di 43,5 anni.

*Il Relearning ti permetterà di apprendere con meno sforzo e più performance, impegnandoti maggiormente nella tua specializzazione, sviluppando uno spirito critico, difendendo gli argomenti e contrastando le opinioni: un'equazione diretta al successo.*

Dalle ultime evidenze scientifiche nel campo delle neuroscienze, non solo sappiamo come organizzare le informazioni, le idee, le immagini e i ricordi, ma sappiamo che il luogo e il contesto in cui abbiamo imparato qualcosa è fondamentale per la nostra capacità di ricordarlo e immagazzinarlo nell'ippocampo, per conservarlo nella nostra memoria a lungo termine.

In questo modo, e in quello che si chiama Neurocognitive Context-dependent E-learning, i diversi elementi del nostro programma sono collegati al contesto in cui il partecipante sviluppa la sua pratica professionale.



Questo programma offre i migliori materiali didattici, preparati appositamente per i professionisti:



#### Materiali di studio

Tutti i contenuti didattici sono creati appositamente per il corso dagli specialisti che lo impartiranno, per fare in modo che lo sviluppo didattico sia davvero specifico e concreto.

Questi contenuti sono poi applicati al formato audiovisivo che supporterà la modalità di lavoro online di TECH. Tutto questo, con le ultime tecniche che offrono componenti di alta qualità in ognuno dei materiali che vengono messi a disposizione dello studente.



#### Master class

Esistono evidenze scientifiche sull'utilità dell'osservazione di esperti terzi.

Imparare da un esperto rafforza la conoscenza e la memoria, costruisce la fiducia nelle nostre future decisioni difficili.



#### Pratiche di competenze e competenze

Svolgerai attività per sviluppare competenze e capacità specifiche in ogni area tematica. Pratiche e dinamiche per acquisire e sviluppare le competenze e le abilità che uno specialista deve sviluppare nel quadro della globalizzazione in cui viviamo.



#### Letture complementari

Articoli recenti, documenti di consenso e linee guida internazionali, tra gli altri. Nella biblioteca virtuale di TECH potrai accedere a tutto il materiale necessario per completare la tua specializzazione.





### Casi di Studio

Completerai una selezione dei migliori casi di studio scelti appositamente per questo corso. Casi presentati, analizzati e monitorati dai migliori specialisti del panorama internazionale.



### Riepiloghi interattivi

Il team di TECH presenta i contenuti in modo accattivante e dinamico in pillole multimediali che includono audio, video, immagini, diagrammi e mappe concettuali per consolidare la conoscenza.

Questo esclusivo sistema di specializzazione per la presentazione di contenuti multimediali è stato premiato da Microsoft come "Caso di successo in Europa".



### Testing & Retesting

Valutiamo e rivalutiamo periodicamente le tue conoscenze durante tutto il programma con attività ed esercizi di valutazione e autovalutazione, affinché tu possa verificare come raggiungi progressivamente i tuoi obiettivi.





# 06 Titolo

Il Corso Universitario in Analisi e Sviluppo di Malware garantisce, oltre alla preparazione più rigorosa e aggiornata, il conseguimento di una qualifica di Corso Universitario rilasciata da TECH Global University.





“

*Porta a termine questo programma e ricevi la tua qualifica universitaria senza spostamenti o fastidiose formalità”*

Questo programma ti consentirà di ottenere il titolo di studio di **Corso Universitario in Analisi e Sviluppo di Malware** rilasciato da **TECH Global University**, la più grande università digitale del mondo.

**TECH Global University**, è un'Università Ufficiale Europea riconosciuta pubblicamente dal Governo di Andorra (*bollettino ufficiale*). Andorra fa parte dello Spazio Europeo dell'Istruzione Superiore (EHEA) dal 2003. L'EHEA è un'iniziativa promossa dall'Unione Europea che mira a organizzare il quadro formativo internazionale e ad armonizzare i sistemi di istruzione superiore dei Paesi membri di questo spazio. Il progetto promuove valori comuni, l'implementazione di strumenti congiunti e il rafforzamento dei meccanismi di garanzia della qualità per migliorare la collaborazione e la mobilità tra studenti, ricercatori e accademici.

Questo titolo privato di **TECH Global University**, è un programma europeo di formazione continua e aggiornamento professionale che garantisce l'acquisizione di competenze nella propria area di conoscenza, conferendo allo studente che supera il programma un elevato valore curriculare.

Titolo: **Corso Universitario in Analisi e Sviluppo di Malware**

ECTS: **6**

N. Ore Ufficiali: **150o.**



futuro  
salute fiducia persone  
educazione informazione tutor  
garanzia accreditamento insegnamento  
istituzioni tecnologia apprendimento  
comunità impegno  
attenzione personalizzata innovazione  
conoscenza presente qualità  
formazione online  
sviluppo istituzioni  
classe virtuale lingue

**tech** global  
university

**Corso Universitario**  
Analisi e Sviluppo di  
Malware

- » Modalità: online
- » Durata: 6 settimane
- » Titolo: TECH Global University
- » Accreditamento: 6 ECTS
- » Orario: a tua scelta
- » Esami: online

# Corso Universitario Analisi e Sviluppo di Malware