BOOM CYBERSECURITY

BOOM

powered by CRIF

COSA CI DICE IL CONTESTO ESTERNO?

Uno sguardo al 2025

- Circa il **50% delle aziende investe in formazione** per migliorare le competenze in cybersecurity, **con il 43% che supporta ulteriormente i dipendenti nel conseguimento di certificazioni per validare le loro conoscenze.**

- Il **56% delle aziende** riconosce la necessità di **formazione** per colmare le lacune nelle competenze dei dipendenti. La richiesta riguarda **non solo competenze tecniche ma anche soft skill per una migliore gestione del rischio.**

- **Nel 2025, l'intelligenza artificiale guiderà sia gli attacchi che le protezioni.** Gli attori delle minacce utilizzeranno l'IA per generare attacchi di phishing altamente personalizzati e malware adattivi in grado di imparare dai dati in tempo reale per evitare il rilevamento.

- Le aziende utilizzeranno l'AI per automatizzare la risposta agli incidenti, monitorare le reti e prevedere le minacce future. Circa il **41% delle aziende sarà impegnato in programmi pilota o implementazioni iniziali di AI generativa per migliorare le operazioni di sicurezza.**

- Con **32 miliardi di dispositivi IoT previsti entro il 2025**, la **protezione** di questi sistemi interconnessi diventerà fondamentale.

(FONTE: STATE OF CYVERSECURITY, 2024 - CompTIA)

I progetti formativi BOOM più significativi sviluppati in ambito di CYBERSECURITY

BOOM

powered by CRIF

#1 Il Progetto

Laboratorio aperto

In **collaborazione con il Nuovo Circondario Imolese**, è emersa l'esigenza di supportare le PMI locali per diffondere la conoscenza su tematiche come l'**Intelligenza Artificiale**, l'**Innovazione Tecnologica**, la **Cybersecurity** e la **Sostenibilità-ESG;** aree che sono sempre più determinanti per rimanere competitivi in un contesto economico in rapido cambiamento.

48 ore di formazione totali

80 partecipanti coinvolti

2 Workshop Sulla Cybsercurity

2 Testimonianze aziendali in ambito Cybersecurity

I workshop hanno trattato **i concetti base della cybersecurity e della mitigazione delle minacce informatiche. È stato presnetato il quadro normativo attuale,** con un focus sull'importanza della cybsersecurity in ambito smart manufacturing e industry 5.0. Sono stati condivisi i principali **trend tecnologici**, **i sistemi IoT e l'integrazione dell'AI nei processi produttivi**, e come queste tecnologie influenzano infrastrutture, competenze digitali e processi aziendali.

Feedback dai protagonisti

«Un'esperienza formativa molto interessante grazie anche alla presentazione di casi pratici e testimonianze da parte delle aziende.»

«È stato molto utile poter approfondire ii concetti base della cybsercurity. È fondamentale oggi essere a conoscenza dei rischi che corriamo.»

#2 Il Progetto

Master In CyberSecurity “From Design To Operations”

IN PARTNERSHIP CON ALMA MATER STUDIORUM – UNIVERSITÀ DI BOLOGNA

ALMA MATER STUDIORUM UNIVERSITÀ DI BOLOGNA

Questo **Master di I livello** è stato sviluppato per i **professionisti dell'ICT** che vogliono accelerare il loro percorso di carriera, **così come per i neolaureati** che vogliono specializzarsi nel campo della cybersecurity. Il Master offre competenze avanzate per l'analisi delle criticità esistenti e per il design, la progettazione, l'integrazione e il deployment delle soluzioni di sicurezza, sia a livello applicativo che di rete, in tutte le fasi operative delle infrastrutture e dei processi.

Al termine del master i partecipanti acquisiranno le seguenti competenze:

- **Tecniche di protezione dei dati per mezzo di algoritmi/protocolli crittografici**
- **Incident Response**
- **Configurazione delle infrastrutture per minimizzarne le vulnerabilità**
- **Mitigazione dei Rischi**
- **Tecniche di rilevazione degli attacchi cyber**

PROFILO PROFESSIONALE

ICT Security Specialist, Web Security Expert, Mobile Security Expert, Penetration tester e Security Incident Analyst and Responder.

DIDATTICA

Il master prevede la frequenza di **304 ore d'aula** distribuite su **otto mesi** con **formula weekend.**

*«Il Master, giunto alla sua **seconda edizione**, ribadisce la **sua forza nella collaborazione tra il mondo accademico e le aziende specializzate in cybersecurity**. La didattica fornita da docenti universitari con una significativa esperienza di ricerca sarà integrata dalla testimonianza diretta di esperti del mondo delle imprese e della Pubblica Amministrazione, e la capacità di applicare i concetti appresi sarà consolidata attraverso uno stage di 500 ore in una delle aziende partner, tutte con divisioni specializzate.”* **Prof. Marco Prandini del Dipartimento di Informatica e Ingegneria dell'Università di Bologna.**

#3 Il Progetto

HACK-IN-TOWERS

Hack-in-Towers è un **Hackathon dedicato alla Cybersecurity**, un evento innovativo e dinamico che riunisce esperti del settore, studenti, professionisti e appassionati di tecnologia.

L'Hack-in-Towers **si rivolge a diplomati tecnici, laureandi e neolaureati in Informatica e Ingegneria Informatica** delle principali università dell'Emilia Romagna e alle aziende che desiderano investire nell'ambito della Cybersecurity.

VANTAGGI PER LE AZIENDE: PERCHE' PARTECIPARE

SELEZIONE CANDIDATI

Il team di BOOM si occuperà di selezionare i giovani talenti che prenderanno parte alla challenge promossa dalle aziende Main Sponsor.

Numero massimo di partecipanti per ogni Azienda: 6.

FORMAZIONE DEI MENTORS

Formazione ai Business Mentors da parte di esperti BOOM per guidare con successo i team nello sviluppo di dee innovative.

VISIBILITÀ, MATERIALI ED EMPLOYER BRANDING

- Inserimento del **logo e del nome aziendale** in tutte le **comunicazioni** ufficiali BOOM.
- **Condivisione di una selezione di 40 foto e video intervista** di un rappresentate dell'azienda con cui promuovere l'iniziativa sui propri canali e sui canali.
- **Presentazione aziendale** ai presenti durante le due giornate finali. (2 rappresentati aziendali tra figure HR e di Business)

EVENTO FINALE IN BOOM

- Supporto gestione trasporti
- Catering esclusivo e a KM0
- Sala per i colloqui di gruppo o singoli
- Auditorium da 105 posti a disposizione

IN PARTENZA DA APRILE 2025

IN COLLABORAZIONE CON:

ALMA MATER STUDIORUM UNIVERSITÀ DI BOLOGNA

Università degli Studi di Ferrara

UNIMORE UNIVERSITÀ DEGLI STUDI DI MODENA E REGGIO EMILIA

UNIVERSITÀ DI PARMA

IN LAVORAZIONE IL PATROCINIO DI:

RegioneEmilia-Romagna

CITTÀ METROPOLITANA DI BOLOGNA

Offerta Formativa Boom

BOOM

powered by CRIF

PERCHÈ INVESTIRE NELLA CYBERSECURITY?

La cybersecurity non è più un optional, ma **una necessità per ogni impresa**, indipendentemente dalle sue dimensioni.
Un attacco informatico può causare gravi danni economici, la perdita di dati sensibili, la compromissione della reputazione aziendale e l'interruzione delle attività.

ECCO COSA VUOL DIRE INVESTIRE IN CYBERSECURITY:

- **Prevenire perdite finanziarie:** un attacco ransomware può costare milioni di euro e paralizzare un'azienda.
- **Mantenere la fiducia dei clienti:** una violazione dei dati può erodere la fiducia dei clienti e danneggiare la reputazione dell'azienda.
- **Evitare sanzioni per non conformità:** Regolamenti come il GDPR e il CCPA impongono multe sostanziali in caso di cattiva gestione dei dati dei clienti.

LE SFIDE PER LE PMI

Per le grandi aziende, la cybersecurity è una componente fondamentale della strategia aziendale, mentre per le PMI rappresenta una sfida critica che richiede soluzioni efficaci e accessibili. **L'Italia è il quarto paese al mondo per numero di rivendicazioni Ransomware e il primo in Europa**. Questo dimostra come il nostro paese sia un **bersaglio privilegiato per gli attacchi informatici:** solo **nel primo semestre del 2023 si è registrato un +85,7%** di attacchi rispetto all'anno precedente.
E le Pmi, in particolare le piccole micro-aziende, si sono confermate il target preferito degli hacker. (SI MOLTIPLICANO GLI ATTACCHI DEGLI HACKER, PMI NEL MIRINO, 2024 - IL SOLE24ORE)
Le piccole e medie imprese affrontano quindi **sfide uniche in termini di cybersecurity**.
Spesso dispongono di risorse limitate e di personale non specializzato, rendendole vulnerabili agli attacchi informatici. Tuttavia, esistono **soluzioni accessibili** che possono migliorare significativamente la sicurezza, **in primo luogo la formazione del personale sui rischi informatici.**

BOOM powered by CRIF

L'OFFERTA FORMATIVA BOOM

I percorsi e le pillole formative BOOM offrono una formazione approfondita sulle principali **tematiche legate alla cybersecurity**, fornendo alle aziende le competenze necessarie per anticipare, affrontare e mitigare i rischi informatici in maniera efficace.

Obiettivi dei nostri percorsi formativi:

- **Fornire formazione approfondita e mirata a tutti i dipendenti per renderli più consapevoli e pronti a fronteggiare le continue minacce digitali.**
- **Formare personale dedicato per sviluppare competenze pratiche nella protezione di informazioni sensibili, riducendo il rischio di attacchi informatici e migliorando la capacità di risposta.**

I NOSTRI PERCORSI FORMATIVI:

OGNI PERCORSO FORMATIVO OFFRE UN NUMERO VARIABILE DI WORKSHOP AL SUO INTERNO

01 CYBERSECURITY AWENESS: Proteggersi nell'era digitale

Percorso per distinguere i principali rischi informatici, adottando buone passi di sicurezza e utilizzare in modo sicuro le piattaforme cloud, con focus per i team leader sulla gestione consapevole e sicura dei dati.

02 CYBER SECURITY E DATA PROTECTION

Il percorso formativo combina teoria e pratica per fornire una comprensione approfondita della sicurezza informatica. Verranno condivise informazioni sulla protezione dei dati, sulla gestione degli incidenti informatici e sui riferimenti normativi, con linee guida applicabili al contesto aziendale.

03 CYBERSECURITY PER IL MANUFACTURING: Difendere la produzione nell'Industria 4.0

Il percorso, pensato per il settore manifatturiero, ha l'obiettivo di fornire le competenze per prevenire, riconoscere e mitigare le minacce che possono compromettere la produttività aziendale.

04 CLOUD SECURITY STRATEGY

Il percorso formativo offre una visione chiara e pratica delle principali sfide di sicurezza per dati e infrastrutture in ambienti cloud. Strutturato in moduli multi-target, mira a fornire una comprensione approfondita dei rischi e delle minacce specifiche dell'ambiente cloud.

BOOM powered by CRIF

L'OFFERTA FORMATIVA BOOM

01 CYBERSECURITY AWERNESS: PROTEGGERSI NELL'ERA DIGITALE

Il percorso, pensato per professionisti e **dipendenti di qualsiasi settore o ruolo (non tecnici)**, fornisce una **panoramica sui rischi informatici più comuni** e sulle **buone prassi per proteggere sé stessi e l'azienda.**
I partecipanti, attraverso esempi pratici e use case imparano a riconoscere le **principali minacce online** e a **utilizzare in sicurezza le piattaforme di collaborazione su cloud** (OneDrive, Google Drive, SharePoint, Dropbox).
Il programma include inoltre un modulo di approfondimento dedicato ai team leader, con casi pratici e linee guida per coordinare il proprio team in modo sicuro e consapevole.

Contenuti del Percorso

MODULO 1: Introduzione alla Cybersecurity – 2h
Panoramica sul contesto attuale e sulle minacce digitali più comuni (phishing, smishing, frodi) e come affrontare i rischi nelle comunicazioni come email e transazioni.
Analisi di use case di attacchi reali di cybersecurity per comprendere le dinamiche e le possibili conseguenze di una violazione.

MODULO 2: Protezione della Privacy – 2h
Principi fondamentali della privacy online e sicurezza dei dati. Utilizzo sicuro di dispositivi mobili, Wi-Fi pubblici e strumenti di collaborazione online (OneDrive, Google Drive, SharePoint, Dropbox e altre piattaforme di collaborazione).

MODULO 3: Strumenti per Team Leader – 2h
Creare una cultura della sicurezza: diffondere le best practice di cybersecurity all'interno dei gruppi di lavoro.
Analisi di scenari reali su come affrontare comportamenti rischiosi del team.

BOOM powered by CRIF

CYBERSECURITY: Formazione Aziendale

L'OFFERTA FORMATIVA BOOM

02 CYBER SECURITY E DATA PROTECTION

Un programma avanzato **pensato per professionisti ICT e sistemisti** che desiderano rafforzare le proprie competenze tecniche e strategiche per affrontare le sfide della sicurezza informatica in ambito aziendale. Il percorso combina una solida base teorica con un approccio pratico, approfondendo le tecniche per la corretta gestione dei dati e la gestione degli incidenti informatici.

Le competenze che si acquisiranno con questo percorso:

- ✓ Valutazione dei Rischi
- ✓ Amministrazione e Sicurezza di Rete
- ✓ Incident Response
- ✓ Sicurezza dei Dati
- ✓ Mitigazione dei Rischi

Il percorso formativo si articola in **tre moduli, per un totale di 16 ore**, e offre una panoramica completa sulla sicurezza informatica, fornendo competenze direttamente applicabili nel contesto lavorativo.

MODULO 1 – 6 ORE
Minacce, Vulnerabilità e Strategie di Sicurezza

Attori di minaccia (interni/esterni) e analisi degli scenari di attacco più comuni.

Minacce AI-driven: Esempi di attacchi automatizzati o potenziati dall'AI.

Tecniche di prevenzione & hardening: procedure di messa in sicurezza per workstation, server e dispositivi mobili.

Segmentazione e architettura Zero Trust

MODULO 2 – 8 ORE
Gestione dell'incidente informatico

Vulnerability Assessment e Penetration Testing

Tecniche di mitigazione e recovery: backup, disaster recovery e business continuity.

Incident response: creazione di piani di risposta e gestione delle crisi.

Simulazioni di risposta agli incidenti: analisi delle criticità emerse e definizione di azioni migliorative

MODULO 3 – 2 ORE
Accenni su policy e conformità aziendali

Introduzione alle normative principali: GDPR, e Privacy, direttive NIS.

Compliance aziendale: obblighi per la protezione dei dati e la gestione della sicurezza.

BOOM powered by CRIF

L'OFFERTA FORMATIVA BOOM

03 CYBERSECURITY PER IL MANUFACTURING: DIFENDERE LA PRODUZIONE NELL'INDUSTRIA 4.0

Il percorso, progettato specificamente per il settore manifatturiero, approfondisce la sicurezza informatica in relazione alle tecnologie di **Industria 4.0**, con un'attenzione particolare ai **sistemi IoT e OT.**

I workshop che compongono il percorso mirano a fornire le competenze per **prevenire**, **riconoscere** e **mitigare** le **minacce** che possono compromettere la continuità produttiva, la sicurezza dei sistemi industriali e la protezione dei dati aziendali.

Il percorso, dalla durata di **16 ore,** è adatto, sia alle aziende in **fase di transizione verso l'IoT** che desiderano sensibilizzare la propria forza lavoro, sia a quelle che vogliono consolidare le proprie conoscenze in materia di **sicurezza informatica industriale.**

I WORKSHOP DEL PERCORSO

01 **SPECIFICITÀ DELLA CYBERSECURITY NEL MANUFACTURING – 4H**

- Panoramica dell'Industria 4.0: connessione tra IT e OT (Operational Technology).
- Rischi associati all'Industrial Internet of Things (IIoT) e ai sistemi SCADA.
- Analisi dell'impatto di un attacco informatico sulla continuità operativa e sui processi produttivi

02 **TIPOLOGIE DI ATTACCHI NEL SETTORE – 4H**

- Tipologie di attacchi più comuni: ransomware, sabotaggi industriali, attacchi DDoS.
- Vulnerabilità specifiche dei sistemi industriali: PLC, sensori e reti industriali.
- Case study su attacchi reali nel settore manifatturiero.

03 **STRATEGIE DI PROTEZIONE PER IL MANUFACTURING – 4H**

- Esempi di implementazione di soluzioni di segmentazione della rete e monitoraggio continuo
- Le principali strategie di difesa per infrastrutture industriali

04 **TECNOLOGIE DIGITALI E CYBERSECURITY – 4H**

- Intelligenza artificiale e ruolo della protezione dei dati industriali: sfide e rischi
- Come viene integrata l'AI nei contesti OT/IoT
- Vantaggi e Rischi del Digital Twin per la gestione della sicurezza informatica

L'OFFERTA FORMATIVA BOOM

04 CLOUD SECURITY STRATEGY

Il percorso si sviluppa in **moduli multi-target** e prevede:

- **due moduli dedicati a professionisti ICT e sviluppatori**, con l'obiettivo di approfondire i rischi e le minacce nell'ambiente cloud, nonché di comprendere la suddivisione delle responsabilità tra provider cloud e cliente.
- **un modulo aggiuntivo rivolto a manager e team leader**, focalizzato sulla corretta gestione dei dati nel cloud, con cenni alla conformità normativa, suggerimenti organizzativi e strumenti per promuovere una cultura della sicurezza all'interno dei propri team.

I WORKSHOP DEL PERCORSO:

MODULO 1: Fondamenti di Cloud e Sicurezza – 4h
PER TEAM IT E DEVELOPER

- Benefici e rischi della migrazione al cloud dal punto di vista della cybersecurity
- Shared Responsibility Model: comprensione delle responsabilità tra provider cloud e cliente.

MODULO 2: Rischi e Minacce nell'Ambiente Cloud – 4h
PER TEAM IT E DEVELOPER

- Phishing e social engineering legati al cloud: tecniche di attacco e difesa.
- Rischi legati alle API non sicure.

MODULO 4: Strumenti di Sicurezza Cloud *
PER TEAM IT E DEVELOPER

- Panoramica delle soluzioni di sicurezza offerte dai principali provider cloud (AWS, Azure, Google Cloud).
- Firewall e protezioni perimetrali in ambiente cloud.
- Come riconoscere e prevenire le truffe legate al cloud.

MODULO 3: Protezione dei Dati nel Cloud - 4h
PER MANAGER/ TEAM LEADER

- Protezione delle informazioni sensibili e classificazione dei dati.
- Principali rischi legati alla protezione dei dati
- GDPR e cloud: gestione dei dati personali e conformità normativa.

*** Su richiesta moduli specifici (a partire da 8h)** su architetture cloud sicure su: AWS; GCP, Azure che si concentrano sugli strumenti offerti dai provider

BOOM powered by CRIF

L'OFFERTA FORMATIVA BOOM

Le pillole di CyberSecurity

Le **pillole e-learning** hanno la durata dai **30 minuti** ai **60 minuti** ciascuna, hanno un taglio informativo e possono essere fruite da tutte le figure professionali presenti all'interno dell'organizzazione.

CYBERSECURITY – 60 min

Il corso accompagna i partecipanti nella scoperta dei potenziali rischi e pericoli sulla rete per i dati aziendali e personali, tra cui gli attacchi hacker, il phishing e i tentativi di frode.

Contenuti:

- Conoscere minacce come cyber crime e phishing è essenziale per proteggere dati personali e aziendali.
- Identificare vulnerabilità, formare il team e usare strumenti adeguati rafforza la difesa.
- La sicurezza informatica richiede collaborazione tra dipendenti e partner.

CYBER SECURITY: I PRIMI PASSI – 60 min

Il corso fornisce elementi e competenze utili a contrastare gli attacchi informatici basati su tecniche di social engineering

Contenuti:

- La cybersecurity svela un mondo segreto, spiegando minacce come il phishing e le truffe su bonifici.
- Comprendere l'anatomia degli attacchi e proteggere i pagamenti è fondamentale nel nuovo panorama digitale.

CYBER SECURITY: NON SONO IN UFFICIO – 60 min

Il corso affronta i temi della «cybersecurity personale» a casa, in famiglia e lontano dal luogo di lavoro. Il percorso è orientato a favorire i corretti comportamenti in contesti di smart working e lavoro da remoto

Contenuti

- Manipolazione del dispositivo di lavoro prestato al figlio
- Truffa attraverso mail di addebito per fine abbonamento di prova a servizio web
- Smart phone in manutenzione fornisce l'occasione a uno stalker

CYBERSECURITY: EVOLUZIONE DELLA SPECIE – 30 min

Il corso affronta le tecniche di attacco più sofisticate e propone scenari di rischio connessi alle nuove tecnologie legate al mondo dell'internet delle cose e dei «deep fake».

La proposta punta a preparare il personale ad affrontare scenari di attacco attuali e di un prossimo futuro

Contenuti:

- Attacco a un azienda tramite USB, truffa via PEC, Attacco malware attraverso combinazione di smishing e phishing, Truffa attraverso falso QRCode, Truffa attraverso video falsificato dell'amministratore delegato.

RICHIEDI INFO

I corsi multi-azienda BOOM

I corsi **multi-azienda** organizzati da BOOM offrono **formazione su argomenti innovativi a dipendenti delle aziende di tutti i settori.**
Questi momenti permettono non solo di acquisire nuove competenze, ma anche di **confrontarsi con esperienze e best practice di altre realtà**, creando un ambiente di apprendimento condiviso e sempre aggiornato.

CORSI IN PARTNERSHIP CON bi-rex

Big Data Innovation & Research Excellence

INTERNET OF THINGS
20 E 21 GENNAIO

ISCRIVITI SUBITO!

BIG DATA E DATA VISUALIZATION PER 5.0
30 GENNAIO

ISCRIVITI SUBITO!

LEAN MANUFACTURING
11GENNAIO

ISCRIVITI SUBITO!

DIGITAL TRANSFORMATION
12 e 14 FEBBRAIO
12 e 14 MARZO

ISCRIVITI SUBITO!

GREEN SOFTWARE E AGILE MANAGEMENT
4 e 11 MARZO

ISCRIVITI SUBITO!

CYBERSECURITY
24 e 31 MAZRO
7 APRILE

ISCRIVITI SUBITO!

MANUTENZIONE PREDITTIVE E INTELLIGENZA ARTIFICIALE
10 APRILE

ISCRIVITI SUBITO!

Contattaci per richiedere maggiori informazioni e sviluppare un progetto per lo sviluppo della Cybersecurity nella tua azienda

info@bo-om.it

051 417 6111