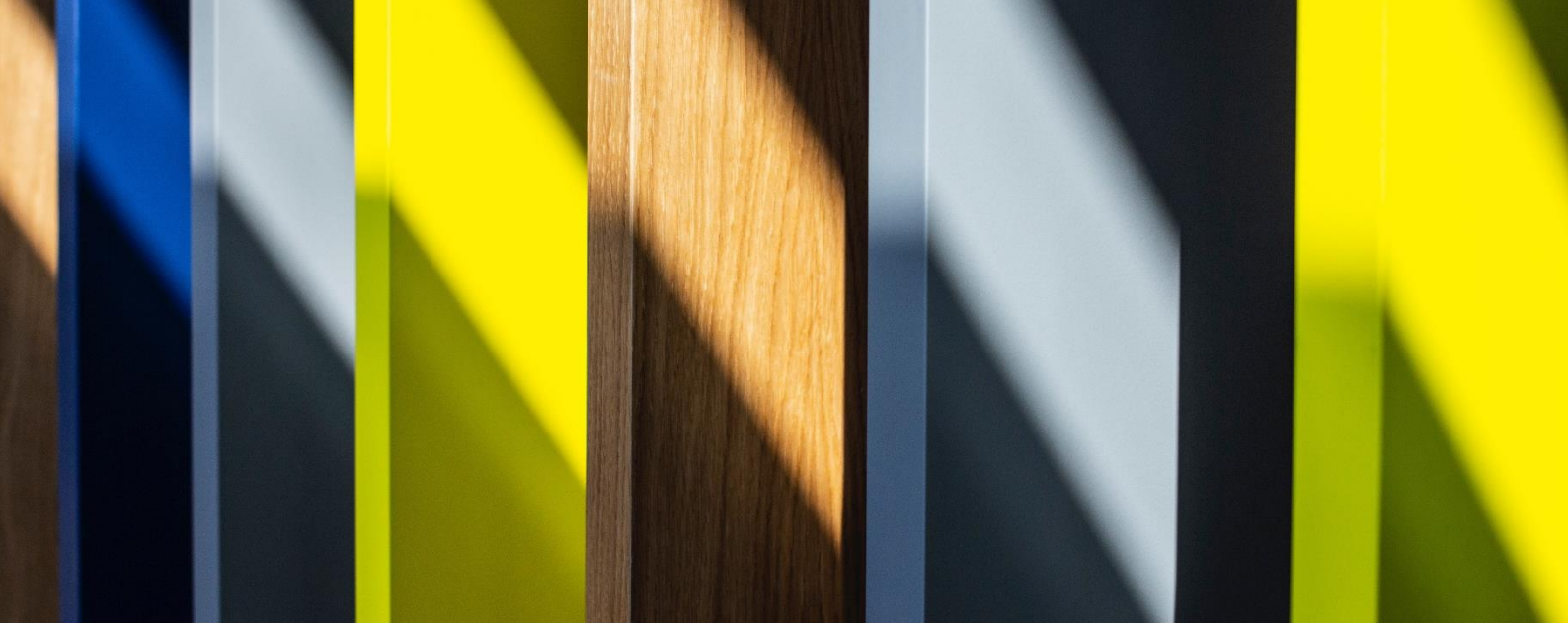


Percorso di Alta Formazione

INFORMATION SECURITY MANAGEMENT

14^ EDIZIONE

Marzo – Luglio 2019

Cefriel
POLITECNICO DI MILANO

MIP
POLITECNICO DI MILANO
GRADUATE SCHOOL
OF BUSINESS

Con il Patrocinio di

aipsa
Associazione Italiana Professionisti Security Aziendale

In collaborazione con

AIEA

Information Security Management

Cefriel e MIP Politecnico di Milano presentano la **14^ edizione del percorso di alta formazione in Information Security Management**, che si propone di formare esperti a 360° nella progettazione e gestione del sistema preposto alla tutela della sicurezza del patrimonio informatico ed informativo di un'azienda.

Il percorso di **16 giornate** è strutturato **2 stream** principali e consecutivi al fine di soddisfare il fabbisogno formativo di diverse tipologie di figure professionali in relazione all'effettivo coinvolgimento in aspetti gestionali dell'Information Security.

Al termine del percorso i partecipanti riceveranno l'**attestato di partecipazione**.

La frequenza ad ogni modulo consente il riconoscimento di 15,6 ore di credito nell'ambito del **CISA, CISM, CGEIT, CRISC Continuing Education (CPE) di ISACA**.

Per informazioni sui crediti ISACA http://bit.ly/2fz2zbI

Obiettivi

Comprendere e valutare la complessità delle problematiche di sicurezza che impattano sull'ICT aziendale, anticipandole con un approccio proattivo.

Progettare, valutare, implementare e gestire un Information Security Management System integrato con il core business aziendale, in accordo ai principali standard di riferimento, favorendo un'efficace gestione dei rischi noti o prevedibili ed anticipando l'insorgenza dei nuovi.

Stimare i costi e i benefici delle diverse soluzioni, valutare il ritorno degli investimenti in sicurezza e comprendere i risvolti organizzativi dell'Information Security.

Target

Il percorso è rivolto a responsabili dei sistemi informativi, di reti e di organizzazione di piccole, medie e grandi imprese industriali, di servizi e della Pubblica Amministrazione, nonché a tutti gli specialisti che operano nel campo della consulenza e della gestione in outsourcing di reti e di sistemi informativi che devono affrontare il contrasto al cybercrime e la compliance alla normative di settore.

È il percorso ideale per chi è destinato ad assumere il ruolo di Information Security Manager o Chief Information Security Officer.

Cefriel - MIP

Cefriel crea e ripensa prodotti, servizi e processi valorizzando e sviluppando le tecnologie digitali. Un team multidisciplinare, autorevole e appassionato di oltre 130 persone con un mix di competenze tecniche, di business e di design.

Fondato nel 1988 dal Politecnico di Milano, Cefriel è oggi un centro di eccellenza per l'innovazione digitale che include come soci altre tre università, Regione Lombardia e 18 imprese multinazionali.

Cefriel è una società consortile not for profit in cui il vero dividendo è l'impatto sull'economia, sulla società e sul territorio, la creazione e la promozione di nuove professionalità e competenze.

Fondato nel 1979 come Consorzio tra il Politecnico di Milano e numerose istituzioni ed aziende, oggi MIP è una società consortile per azioni senza scopo di lucro. MIP integra il know-how specialistico della componente accademica con la concretezza e la professionalità del mondo industriale e dei servizi.

Insieme al Dipartimento di Ingegneria Gestionale, fa parte della School of Management del Politecnico di Milano che accoglie le molteplici attività di ricerca e formazione nel campo del management, dell'economia e dell'industrial engineering. Attraverso la collaborazione Università-Impresa, la nostra

business school sviluppa molteplici attività nella formazione continua post-laurea e/o post esperienza, rivolta a singoli, imprese, istituzioni pubbliche e private. Un impegno costante, portato avanti nella nuova sede del Campus Bovisa: uno spazio di oltre 3.800 mq di superficie, immerso in uno dei più importanti centri accademici e scientifici internazionali.

Direzione

Raoul Brenna

Responsabile della Security Practice di Cefriel

Si occupa di sicurezza informatica da svariati anni, promuovendo in tutte le sue attività un approccio costantemente rivolto alla sperimentazione, come importante veicolo di consapevolizzazione a tutti i livelli.

Nel tempo ha affrontato la sicurezza informatica sia da un punto di vista "tradizionale“ (assessment tecnologici e di processo, elaborazione di linee guida, definizione di policy, security governance), sia toccando ambiti maggiormente innovativi (studio dei nuovi trend di attacco e minaccia, identificazione di rischi e opportunità legati a nuove tecnologie, sicurezza del fattore umano, sicurezza IoT, e ambienti SCADA/ICS, tecniche e approcci di Data Visualization applicate all'information security).

Paolo Maccarone

Professore Associato presso la School of Management dal Politecnico di Milano

È titolare del corso Accounting, Finance and Control, nell’ambito del Master of Science in Management Engineering (Ingegneria Gestionale).

Insegna Accounting and Performance Management, nonché Sustainability Strategy and Governance in diversi Master e corsi di formazione “custom” per le aziende di MIP Graduate School of Business.

Le sue attività di ricerca riguardano il controllo di gestione e la misurazione delle prestazioni nelle imprese “for profit”, la gestione strategica della CSR e il performance measurement and management nell’ambito dell’information security.

E’ attualmente direttore dell’Osservatorio Energy Cybersecurity (iniziativa dell’Energy&Strategy Group della School of Management). In passato è stato condirettore dell’Osservatorio congiunto Cefriel-MIP sull’Information Security Management.

Faculty

Raoul Brenna
Cefriel

Teodoro De Giorgio
Cefriel

Gabriele Faggioli
MIP - Membro direttivo Clusit

Esther Ferruccio
Cefriel

Marco Festa
Cefriel

Enrico Frumento
Cefriel

Andrea Ghirardini
BE.iT SA

Sara Grilli
Cefriel

Paolo Maccarrone
MIP

Massimo Manara
Aglea

Luca Mastrangelo
Cefriel

Giulio Perin
Cefriel

Roberto Spigolon
Cefriel

Stefano Testoni
Cefriel

Enzo Maria Tieghi
ServiTecno

Federico Valentini
Cefriel

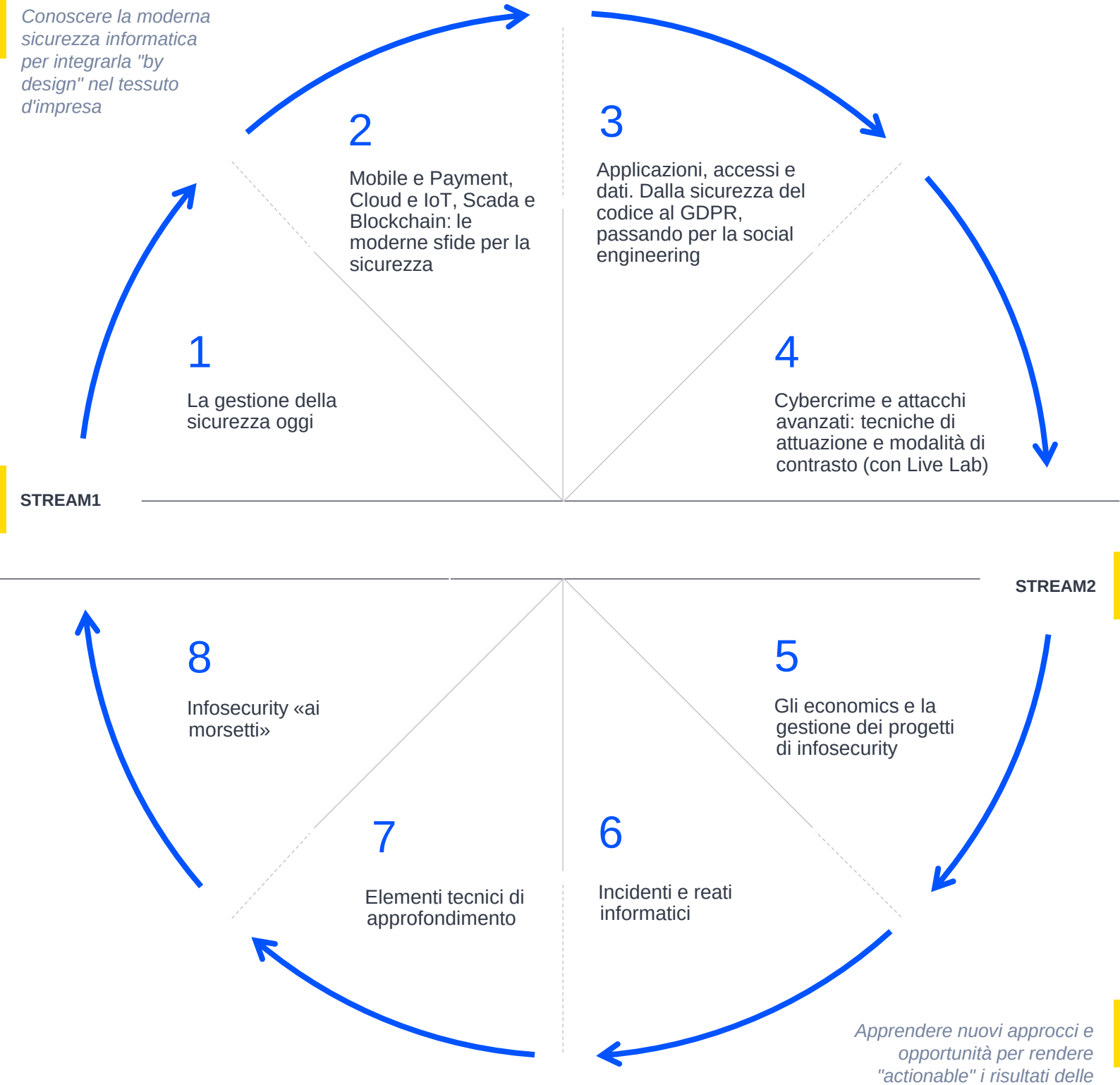
Approccio

I contenuti del percorso sono sviluppati con una prospettiva multidisciplinare, che coniuga le soluzioni **tecnologiche con i risvolti organizzativi e le implicazioni di natura legale**, sempre con la massima attenzione agli **hot topic** del momento e ai temi emergenti, in modo da anticipare i cambiamenti futuri.

Underlying technology & hot topics	Aspetti legati alle infrastrutture fisiche, la sicurezza delle applicazioni, la disponibilità dei servizi, le verifiche di conformità, fino alla governance. L'obiettivo è quello di fornire gli strumenti metodologici per attuare un'efficace protezione del patrimonio informativo aziendale, raccogliendo le sfide e le tendenze di un ambito in continua e rapida evoluzione.
Organization and management	Aspetti organizzativi ed economico-gestionali legati alle configurazioni organizzative della/delle unità di info-security, ai cicli di governance (dalla risk analysis alla messa a punto del piano di interventi, alla gestione della fase di implementazione dei progetti di info-security, alla misurazione delle performance) e alle relative metodologie (analisi costi-benefici e valutazione economico-finanziarie delle alternative decisionali).
Legal	Problematiche di carattere giuridico-legale connesse alla creazione, alla conservazione e alla circolazione dei dati e delle informazioni, in internet e nelle aziende. Le tematiche legali sono affrontate dal duplice punto di vista della compliance, con occhio di riguardo alla Privacy e al GDPR e della protezione dagli illeciti interni ed esterni.

Struttura

Conoscere la moderna sicurezza informatica per integrarla "by design" nel tessuto d'impresa



STREAM1

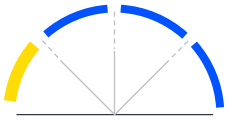
STREAM2

Apprendere nuovi approcci e opportunità per rendere "actionable" i risultati delle iniziative di sicurezza informatica e agevolare la generazione di business value

Stream1

1 La gestione della sicurezza oggi

07-08 Marzo 2019



Il modulo si propone di offrire una panoramica sugli aspetti caratteristici dei moderni attacchi informatici, inquadrando le nuove tendenze e offrendo una panoramica sulle necessità di un framework strutturato di gestione della sicurezza informatica in azienda, nonché di una conoscenza delle principali aree normative di riferimento.

Verranno affrontati temi utili ad inquadrare l'intero percorso in Information Security Management, fornendo un'introduzione completa al moderno ruolo del manager dell'Information Security, inclusiva di aspetti tecnologici, di governance e legali, senza trascurare la "vision" e le nuove attitudini sempre più richieste a tale figura professionale.

1.1

La gestione della sicurezza oggi

Raoul Brenna

- Apertura del percorso ISM
- Introduzione sullo scenario attuale della sicurezza informatica: trend e casi pratici
- Introduzione sul ruolo e le responsabilità in continuo mutamento del Information Security Manager
- La vision futura e le possibili evoluzioni
- Testimonianza aziendale sulle moderne sfide poste dalla sicurezza informatica nelle enterprise

1.2

Sicurezza nelle enterprise

Stefano Testoni

- La sicurezza informatica nelle imprese
- La centralità del dato. La protezione a 360°
- Una panoramica sulle contromisure tecnologiche, di contrasto e di monitoraggio
- Gli elementi tipicamente trascurati (mobile, SCADA, ecc.)

1.3

Security governance

AIEA

- Governo della sicurezza informatica. Processi di gestione e implicazioni organizzative
- Gestione del rischio e conformità
- Realizzazione e gestione di un programma coerente per la sicurezza informatica. Pianificazione e realizzazione del sistema dei controlli
- Gestione degli incidenti di sicurezza informatica e della continuità operativa

1.4

Il quadro normativo

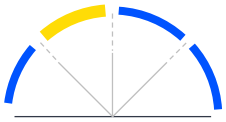
Gabriele Faggioli

- Sicurezza informatica e elementi legali: introduzione, elementi rilevanti, casistica
- L'attuale panorama normativo in materia di sicurezza informatica ("GDPR ma non solo")
- Le scelte del legislatore negli ultimi anni
- I provvedimenti settoriali: banche, società di telecomunicazione, sanità, ecc.

Stream1

2 Mobile e Payment, Cloud e IoT, Scada e Blockchain: le moderne sfide per la sicurezza

21-22 Marzo 2019



Il modulo si propone di esplorare alcune problematiche di sicurezza derivanti dalla massiva diffusione dei paradigmi cloud, smart/mobile e IoT. A questi temi si affiancano aspetti di sicurezza di natura tecnologica e di natura social, fenomeni di consumerization e di abitudine dell'utente a comportamenti intrinsecamente insicuri. A questo si affianca la crescente interconnessione della nuova tecnologia con reti e architetture legacy, ad esempio in ambito SCADA. Ne consegue l'insorgenza di rischi specifici, ma anche di opportunità e fenomeni nuovi (biometria sempre più usabile, blockchain per pagamenti e transazioni, ecc.).

L'obiettivo è quello di fornire una tassonomia delle possibili minacce per le infrastrutture, i dispositivi e le applicazioni, approfondendo approcci metodologici, strumenti e soluzioni organizzative per una corretta gestione della sicurezza in questi ambiti.

2.1

Introduzione al cloud computing, architetture, tecnologie e sicurezza

Stefano Testoni

- Modalità di erogazione del cloud: caratteristiche e rischi. Come il cloud cambia i concetti della sicurezza e trasferisce i rischi fra gli attori
- I rischi legati alla virtualizzazione
- Nuovi strumenti per la sicurezza in ambienti "software defined", la virtualizzazione come opportunità per la sicurezza informatica dei sistemi
- La Security-as-a-Service: stato dell'arte e tendenze
- Mappa dei principali rischi legati alla migrazione su approcci cloud: rischi di sicurezza e rischi tecnologici

2.2

Sicurezza IoT - blockchain – sistemi medicali

Roberto Spigolon, Raoul Brenna

- Le blockchain e l'impiego nella gestione di pagamenti e transazioni
- L'IoT, le relazioni con la filiera tecnologica e gli aspetti di sicurezza
- Seminario a cura di Deloitte - Cybersecurity nei medical devices: standard di riferimento europei e US e framework per la gestione sicura del ciclo di vita dei dispositivi biomedicali

2.3

Sicurezza dei sistemi SCADA/ICS

Enzo Tieghi

- Le caratteristiche dei sistemi SCADA/ICS
- Gli approcci architetturali e la mancanza di sicurezza intrinseca
- Le feature di sicurezza applicabili e i motivi di una mancata applicazione (caratteristiche dei protocolli e sistemi, difese aggiuntive)
- I recenti e moderni attacchi alle infrastrutture SCADA/ICS e il livello di esposizione
- Modalità di rientro e sviluppo sostenibile degli SCADA anche in ottica di integrazione in approcci Industry 4.0

2.4

Mobile malware - sicurezza e-commerce - mobile payment

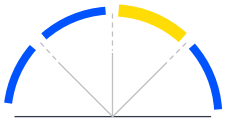
Enrico Frumento

- Le nuove tendenze di attacco ai dispositivi mobili
- Il mobile malware
- Il ruolo dell'utente e dei contenuti fruiti nella sicurezza dei dispositivi mobili
- Sicurezza delle applicazioni mobili, i recenti modelli di autenticazione via mobile, il mobile e la biometria
- La sicurezza dei marketplace e dei modelli di delivery dei contenuti
- Il mobile payment e il mobile commerce, nuovi approcci, tendenze e nuovi rischi

Stream1

3 Applicazioni, accessi e dati. Dalla sicurezza del codice al GDPR, passando per la social engineering

04 - 05 Aprile 2019



Il modulo è dedicato all'esame delle problematiche di sicurezza nelle applicazioni Web e sui dati, intesi sia in termini di credenziali di accesso che di informazioni. Le prime sono spesso trascurate in quanto vi è la tendenza ad attuare verifiche e assessment sul solo IT a livello infrastrutturale e sistemistico, trascurando lo strato applicativo. Quest'ultimo, alla luce anche della progressiva conversione alla fruizione web/mobile oriented, rappresenta in realtà spesso la chiave di accesso ai sistemi da parte degli attaccanti. Dalle vulnerabilità delle applicazioni web nascono spesso seri problemi di disclosure dei dati utente e conseguenti violazioni normative nel loro trattamento (es. GDPR).

Il corso fornisce, gli elementi per valutare il potenziale impatto di eventuali attacchi o databreach e per incorporare la sicurezza by design negli sviluppi.

3.1

Sicurezza delle applicazioni web (elementi fondamentali)

Raoul Brenna

- Le minacce specifiche alle applicazioni web
- Il framework OWASP e le OWASP top 10
- LE evoluzioni delle vulnerabilità nel tempo (aggiornamento a Top 10 2017)
- Casi pratici esemplificativi e panorama delle tipologie di attacco
- Altri attacchi e possibili contromisure generali e puntuali

3.2

Crittografia, autenticazione e comunicazioni sicure

Enrico Frumento

- Il rischio legato ai dati in transito e all'accesso dell'utente ai sistemi
- I concetti e le tecniche di cifratura
- L'autenticazione dell'utente
- L'integrità del dato
- La firma digitale

3.3

L'evoluzione della social engineering, l'esposizione e la protezione dell'identità digitale

(personale e aziendale)

Raoul Brenna

- Il fattore umano come anello debole della sicurezza informatica: la nuova giovinezza della social engineering
- L'esposizione dell'identità sui social media, e gli abusi collegati
- Strumenti per la raccolta di identità e contromisure
- Gli attacchi abilitati dall'ingegneria sociale
- Le nuove tecniche di assessment (integrato sicurezza tecnologica e del fattore umano), la metodologia Cefriel (applicazione e risultati)
- Il ciclo di vita dell'identità digitale, la gestione dell'identità digitale, le tecnologie a supporto
- SPID e "l'identità unica"

3.4

Data privacy e GDPR

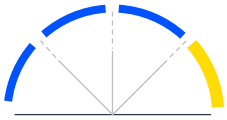
Gabriele Faggioli

- Il concetto di data privacy, l'evoluzione e le interpretazioni nel tempo
- L'attuale panorama normativo in materia di sicurezza dei dati personali alla luce del GDPR
- Il nuovo approccio e l'accountability
- Il Data Privacy Officer: il ruolo, la funzione, l'attribuibilità
- La Data Privacy Impact Analysis
- Le linee guida e gli strumenti a supporto

Stream1

4 Cybercrime e attacchi avanzati: tecniche di attuazione e modalità di contrasto (con live lab)

18 - 19 Aprile 2019



Il modulo si propone di mostrare con approccio estremamente esperienziale e pratico le moderne tecniche di compromissione applicabili ai sistemi informativi e l'(in)efficacia delle varie tipologie di difese attuabili per renderli sicuri.

Il corso illustra, con approccio teorico/pratico, alcune delle moderne tecniche di sfruttamento di vulnerabilità (tipiche o meno note) dei sistemi informativi aziendali e le modalità di realizzazione di attacchi cosiddetti “APT” (Advanced Persistent Threats), oggi comunemente adottati nel panorama degli attacchi legati al Cybercrime.

Il modulo prevede una laboratorio ove i partecipanti possono toccare con mano alcune delle reali modalità di attuazione di attacchi informatici (in modalità red teaming), ed un esercizio finale di blue teaming basato sul format capture the flag.

4.1

Elementi di sicurezza avanzata

Raoul Brenna

- Approfondimento sulle principali tipologie di contrasto alle intrusioni informatiche
- La sicurezza del dato (supporto e contenuto)
- La sicurezza dei sistemi (non solo interni)
- La sicurezza del perimetro (anche esteso)
- Altri fattori a supporto di una sicurezza aziendale distribuita

4.2

Vulnerability assessment e penetration test (con case study)

Stefano Testoni

- Il concetto di vulnerabilità
- Modalità di test e valenza degli strumenti automatizzati
- Modalità di intrusione e attività di penetration test
- Realismo vs. necessità di preservare i sistemi
- Case study

4.3

Hacking Lab (Red Teaming Activity)

Federico Valentini

- Un ambiente simulato in cui i partecipanti dovranno attuare, guidati da esperti Cefriel, attacchi informatici realistici mediante l'adozione delle tecniche comunemente utilizzate in ambito di cybercrime
- L'occasione per un approccio "hands-on" e per valutare in prima persona la complessità (o la relativa semplicità) dietro ai crimini informatici che "fanno notizia"

4.4

Capture the Flag (Blue Teaming Activity)

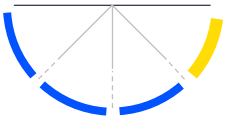
Marco Festa

- L'adattamento al percorso ISM del format "capture the flag", estremamente efficace per la creazione di competenze teorico-pratiche nell'ambito dell'information security
- Mediante la realizzazione di "sfide" e la competizione tra gruppi, si affineranno le competenze e le attitudini utili all'attività di contrasto delle intrusioni informatiche
- Realizzato con la partecipazione di professionisti Cefriel qualificati tra le "7 grandi" dell'hacking mondiale al DEF CON 2018

Stream2

5 Gli economics e la gestione dei progetti di infosecurity

09-10 Maggio 2019



Il modulo si propone di fornire gli elementi fondamentali per una corretta valutazione economico-finanziaria e una corretta implementazione dei progetti di

In particolare, il modulo si propone:

- di illustrare le principali metodologie utilizzate per la una corretta valutazione degli impatti dei progetti di information security sugli economics di un'impresa, e, quindi, della reale attrattività (economico-finanziaria) degli investimenti di natura tecnologica e organizzativa;
- di fornire gli strumenti e le soluzioni organizzative per una corretta gestione dei progetti di implementazione di soluzioni di information security (project management);
- di illustrare le finalità di un sistema di misurazione delle performance delle soluzioni implementate, e, più in generale, del sistema complessivo di gestione dell'information security (e quindi del suo contributo al raggiungimento degli obiettivi aziendali), nonché i principali approcci per l'identificazione dei key performance indicators (KPI)

5.1

La valutazione economico-finanziaria delle alternative progettuali

Paolo Maccarrone

- I criteri e la metrica per la valutazione di un progetto di investimento
- L'applicazione ai progetti di sicurezza informatica

5.2

La misurazione delle prestazioni delle soluzioni di information security

Paolo Maccarrone

- Le finalità di un sistema di misurazione di prestazioni. Il processo di individuazione dei key performane indicators
- Le peculiarità di un Information Security Performance Measurement System

5.3

Project Management

Sara Grilli

- La gestione dei progetti e le specificità delle iniziative di info security (project management)
- L'avvio dei progetti e la complessità del coinvolgimento degli stakeholder
- La dinamicità degli schedule e le problematiche di priorità
- Il controllo dell'avanzamento del progetto. Come valorizzare la sicurezza informatica?

5.4

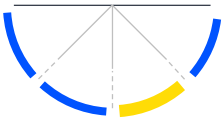
Project Management

Sara Grilli, Giulio Perin

- La gestione dei rischi di progetto nel contesto della sicurezza informatica
- La chiusura dei progetti e il trasferimento del valore generato, come chiave per un ruolo efficace della sicurezza informatica in azienda

6 Incidenti e reati informatici

23 - 24 Maggio 2019



Il manager dell'Information Security deve aiutare il management nella gestione del rischio per l'impresa. Ad un apparato per la prevenzione e il contrasto deve associarsi un'organizzazione in grado di gestire l'eventualità di un incidente di sicurezza informatica, sia da un punto di vista tecnologico e organizzativo, mediante l'attuazione degli opportuni processi (identificazione, riconoscimento e mitigazione) che da quello di un eventuale follow-up di natura legale, secondo i dettami della computer forensics. A tal fine, è essenziale la conoscenza degli aspetti tecnologici delle piattaforme su cui si interviene, ma anche quella dei limiti di intervento al fine di preservare il valore legale della digital evidence. Questo sia in ottica di analisi di singoli elementi probatori, che in un più ampio contesto di realizzazione di una soluzione per la gestione degli eventi di Sicurezza Informatica (SIEM).

6.1

I reati informatici e il regime delle responsabilità

Gabriele Faggioli

- Elementi legali inerenti i principali reati informatici
- I riflessi in materia di responsabilità amministrativa d'impresa (d.lgs 231/01)
- Casistica giurisprudenziale
- La responsabilità dell'azienda e dei lavoratori nell'utilizzo delle strumentazioni informatiche e telematiche
- Diritti, doveri e limiti del datore di lavoro nell'utilizzo di sistemi di controllo
- I provvedimenti del Garante per la protezione dei dati personali
- Casistica giurisprudenziale

6.2

Computer forensic

Andrea Ghirardini

- Profili legali delle attività di computer forensic
- Elementi civilistici e penalistici
- Applicazione pratica delle metodologie e lessons learned

6.3

Le dinamiche della pirateria informatica, l'hacking e la reverse engineering, la malware analysis (preservazione vs. studio)

Enrico Frumento

- Capire il mondo della pirateria informatica
- L'importanza di proteggere le applicazioni
- Tipi comuni di attacco alle applicazioni
- La reverse code engineering
- Il processo di reversing e le tipologie di attacchi
- La malware analysis
- Le analisi live e post-mortem

6.4

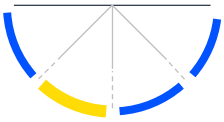
Gestione degli incidenti e SIEM (con esercitazione teorica)

Stefano Testoni

- La gestione degli incidenti, gli obiettivi e i ruoli
- La gestione dell'incidente prima, durante e dopo
- Le policy
- La prevenzione, il monitoraggio e l'analisi (identificazione preventiva vs. proattiva, ricostruzione)
- I log e i SIEM: elementi, architetture, soluzioni
- Esempi e casi
- Seminario a cura di Deloitte - Il ruolo del CERT e i modelli di gestione degli incidenti di sicurezza

7 Elementi tecnici di approfondimento

06 - 07 Giugno 2019



Per una corretta e consapevole gestione del panorama ICT aziendale in ottica di sicurezza informatica, il professionista deve conoscere elementi tecnici avanzati che si riflettono in scelte tecnologiche e/o architetturali da indirizzare.

Il modulo tratta aspetti della sicurezza informatica o della configurazione sicura di sistemi e/o architetture informative. Si tratta di elementi di approfondimento nel campo della sicurezza di applicazioni web e delle comunicazioni in generale (a livello di canale ma anche di API, in ottica di API strategy), ma sono affrontati anche elementi specifici su sicurezza e controllo accessi di altre tipologie di applicativi (da legacy a SAP), nonché le nuove opportunità ed i rischi connessi all'introduzione dei paradigmi di Machine Learning e Artificial Intelligence.

7.1

Artificial intelligence e machine learning - Il futuro dell'information security tra minacce e opportunità

Luca Mastrangelo

- Il machine learning e l'artificial intelligence: definizioni, evoluzione, stato attuale
- Il legame con la futura evoluzione tecnologica
- I rischi connessi con la diffusione dell'artificial intelligence
- La opportunità abilitate
- L'applicazione specifica alle attività di sicurezza informatica
- Il "nuovo ruolo" dell'uomo

7.2

La gestione delle identità in applicativi complessi – Il caso SAP

Massimo Manara

- Security & Identity Access Governance nel sistema SAP (un esempio di gestione per ruoli)
- SAP security concept
- I processi aziendali e la Segregation of Duties
- La relazione con HR
- Introduzione alle logiche di Identity

7.3

Sicurezza del codice nelle applicazioni legacy

Enrico Frumento

- Approccio globale alla protezione
- L'obiettivo della protezione del software
- Modellazione delle minacce e metodologia STRIDE
- Procedure per migliorare la protezione
- Metodologie di programmazione e strumenti a supporto (checklist, CMM)
- Costi da considerare per la protezione

7.4

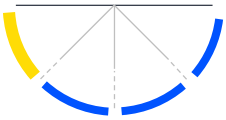
Aspetti avanzati di sicurezza delle applicazioni web e delle API

Raoul Brenna

- L'analisi dei casi di attacco
- Focus sulle reali possibilità di sfruttamento delle vulnerabilità più diffuse
- La composizione di vulnerabilità
- Il web come componente di numerosi attacchi
- Le API, una componente spesso trascurata
- Le tipologie di API e le feature di sicurezza
- Architetture di API sicure
- API strategy, ecosistemi e la sicurezza complessiva

8 Infosecurity «ai morsetti»

20 - 21 Giugno 2019



L'Information Security si interfaccia con il mondo esterno in vari modi. Da un lato gli standard (ISO 27001 in primis) che creano un linguaggio comune per un'efficace analisi dei rischi. Dall'altro la necessità di mostrare e comprendere i risultati delle attività di sicurezza effettuate (con approcci anche innovativi legati alla data visualization e dei nuovi strumenti as a service che la abilitano), e di gestire le problematiche anche normative di un dato sempre più spesso fuori dal controllo diretto dell'azienda.

Il modulo copre un insieme eterogeneo di competenze, tuttavia utili al manager dell'information security giunto alla fine del percorso formativo per relazionarsi a tutto campo con una serie di interlocutori tipici: il mondo della compliance, quello della certificazione, quello del management e del budgeting, quello dei fornitori di servizi in cloud, ecc.

8.1

ISO 27001 e l'IS management system

Giulio Perin

- La famiglia di standard ISO 27000 e il loro ruolo per l'implementazione di un Information Security Management System
- L'implementazione di un ISMS basato sullo standard ISO 27001
  - Clauses 4-10
  - Appendice A – Controlli di Sicurezza
- La relazione con altri standard di rilievo
- Seminario a cura di Deloitte - Framework di security governance: ISO27k, NIST Cyber Security Framework, NIST 800-53 Special Publication Rev4 (in aggiornamento verso la Rev5), Framework Nazionale per la Cyber Security, Direttiva Network & Information Security (NIS)

8.3

Analisi del Rischio dei Sistemi Informativi

Giulio Perin

- Il rischio legato ai sistemi informativi
- Il limite delle metodologie teoriche
- Metodologie pratiche per l'attuazione di analisi del rischio
- Organizzazione di una risk analysis
- Strumenti a supporto

8.2

Il dato distribuito e il cloud: aspetti normativi

Gabriele Faggioli

- Monitoraggio del cloud provider, definizione dei Key Security Indicators e verifica di conformità
- Auditabilità e supporto alla forensics sui sistemi
- Gestione «allargata»: il controllo delle 3d party nelle App
- Case study

8.4

Dashboarding e approcci visuali (basato su case study)

Esther Ferruccio, Raoul Brenna

- La data visualization, principi e regole guida
  - Dashboard vs report
  - Quale informazione
- Tecniche di realizzazione
- I benefici della data visualization per l'information security
  - L'esplorazione dei dati
  - Il vulnerability management
  - La cristallizzazione della conoscenza per la modellazione di fenomeni e processi
  - Le dashboard a supporto dell'operatività
  - L' awareness e la comunicazione verso le funzioni manageriali
- Dal dato alle dashboard direzionali, gli aspetti pratici e le problematiche dall'esperienza

Metodologie e possibili percorsi

Metodologie Didattiche

Il percorso combina:

- momenti di formazione d'aula
- condivisione di esperienza tra i partecipanti
- esercitazioni e sviluppo di casi
- testimonianze aziendali. In passato hanno dato la loro testimonianza ENI, GUCCI, WIND Tre
- dimostrazioni mediante utilizzo di tools (commerciali e open source)
- hacking lab and CTF

All'interno del percorso è previsto un Project Work individuale o di gruppo con la supervisione di un esperto della Faculty.

Il Project Work consente di apprezzare le implicazioni che la sicurezza informatica ha nei progetti ICT e la complessità intrinseca delle iniziative di cybersecurity. Si tratta di un serious game, un modo per mettersi in gioco e mettere in pratica quanto appreso in aula.

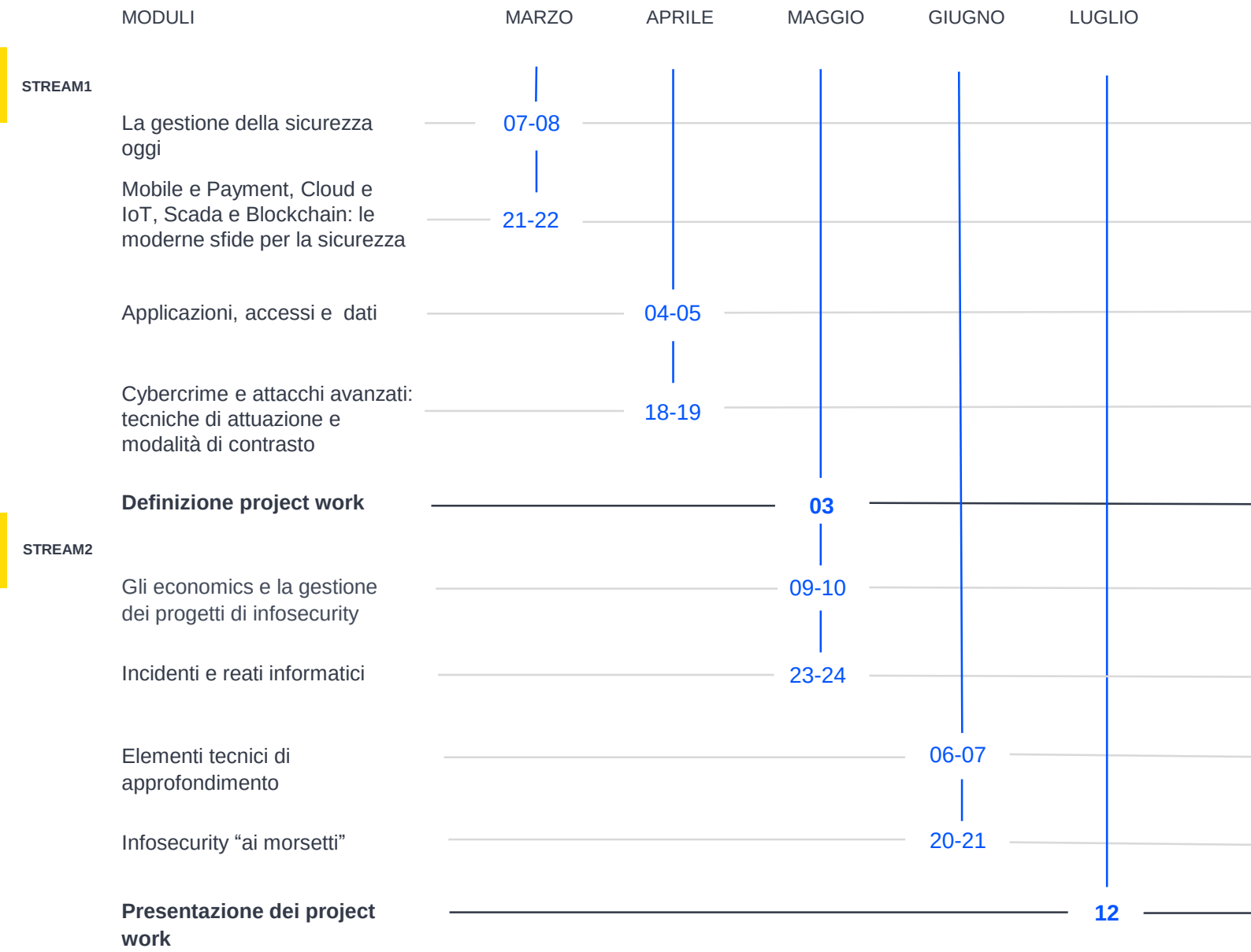
Percorsi

Flessibilità e personalizzazione sono le caratteristiche di questo percorso.

La formulazione è studiata per andare incontro alle diverse esigenze di chi opera nel settore ed ha la necessità di approfondire alcune specificità. Sono possibili diverse modalità di fruizione:

- Percorso completo (Stream1+ Stream2)
- Stream1
- Singolo modulo, 2 giorni consecutivi (giovedì e venerdì)

Calendario



ORARIO

Mattina: 9.00 / 13.00
Pomeriggio: 14.00 / 18.00

Cefriel
Experience Center

Viale Sarca, 226 - 20126 Milano

Ammissione e costi

Ammissione

Il percorso è dedicato a professionisti con consolidata esperienza lavorativa in ambito IT che hanno necessità di acquisire/incrementare conoscenze e competenze in aree chiave dell'IS.

Al fine di assicurare un'adeguata omogeneità delle esperienze in aula è prevista una selezione basata sulla valutazione dei curricula dei candidati e su colloqui individuali.

Per informazioni e iscrizioni contattare mariateresa.bloise@cefriel.com

Percorso Completo
8 moduli, 16gg

6.500 € + IVA (per le iscrizioni a titolo aziendale)

5.500 € + IVA (per le iscrizioni a titolo personale)

- Sconto 10% per iscrizioni con anticipo di 40 giorni sulla data di partenza del corso prescelto
- Sconto 20% sul 3° iscritto della stessa azienda al medesimo corso

Stream1
4 moduli, 8 gg

3.500 € + IVA

E' esclusa la possibilità di acquistare lo Stream2

Singolo Modulo
2 gg

1.200 € + IVA

Sono previste delle agevolazioni per iscrizioni ai singoli corsi brevi

- Sconto 10% per iscrizioni con anticipo di 40 giorni sulla data di partenza del corso prescelto
- Sconto 20% sul 3° iscritto della stessa azienda al medesimo corso

Cefriel
POLITECNICO DI MILANO

cefriel.com

Milano
Viale Sarca 226
20126 Milano – Italy

London
4° floor
57 Rathbone Place
London W1T 1JU – UK

New York
One Liberty Plaza
165 Broadway, 23rd Floor
New York City, New York, 10006 USA