Ministero dell'Interno

DIPARTIMENTO DELLA PUBBLICA SICUREZZA
SEGRETERIA DEL DIPARTIMENTO
UFFICIO PER LE RELAZIONI SINDACALI

N. 555/RS/01|58|6330 Roma, 30/10/2019

OGGETTO: Nuove qualificazioni operativo-professionali per la Polizia Postale e delle Comunicazioni – Corsi di qualificazione.

ALLA SEGRETERIA NAZIONALE SIULP	= ROMA =
ALLA SEGRETERIA GENERALE SAP	= ROMA =
ALLA SEGRETERIA NAZIONALE FEDERAZIONE COISP	= ROMA =
ALLA SEGRETERIA NAZIONALE SIAP	= ROMA =
ALLA SEGRETERIA GENERALE FSP POLIZIA DI STATO - ES-LS-PNFD-LI.SI.PO.-ADP-U.S.I.P.-CONSAP-M.P.	= ROMA =
ALLA SEGRETERIA NAZIONALE FEDERAZIONE SILP CGIL – UIL POLIZIA	= ROMA =

Per immediata conoscenza, si rappresenta che la Struttura di missione per l'istituzione di un polo centrale della sicurezza cibernetica del Ministero dell'Interno ha qui comunicato di aver avviato le procedure per l'istituzione di nuove figure di qualificazione professionale per gli operatori della Polizia Postale.

L'iniziativa ha il duplice obiettivo di affinare le capacità investigative del personale deputato al mantenimento della sicurezza cyber, e, dall'altro, di fornire una risposta adeguata ai sempre mutevoli scenari della criminalità informatica.

I profili professionali selezionati rispecchiano infatti le attuali esigenze operative della Polizia Postale e delle Comunicazioni, peraltro cristalizzate nella Direttiva Minniti sui "Comparti di Specialità e razionalizzazione dei presidi delle Forze di Polizia" del 15 agosto 2017, e sono enucleabili in tre categorie:

- ANALISTA DI FONTI APERTE: OSINT E SOCMINT
- CHILD SEXUAL EXPLOITATION OPERATOR
- INCIDENT RESPONDER

ANALISTA DI FONTI APERTE: OSINT e SOCMINT

Il corso è volto all'acquisizione di tecniche utili a raccogliere dati dalle fonti aperte, a correlarli ed a trarne, quindi, analisi produttive in modo da validarli alla stregua di "informazioni" utili ai fini investigativi/preventivi.
Tra i principali obiettivi formativi, si segnalano: metodologia e caratteristiche delle fonti aperte; tecniche operative di SOCMINT (Social Media Intelligence); strategie di ricerca; software di ricerca; piano di ricerca; visualizzazione dei dati; ricerche avanzate con Facebook, scansione profili social.

CHILD SEXUAL EXPLOITATION OPERATOR

In relazione agli aspetti fondamentali del contrasto alla pedopornografia on-line, l'operatore dovrà essere in grado di acquisire metodologie per condurre attività di investigazione complessa in ambienti virtuali, sia che essi si collochino nella *clearnet* sia che utilizzino *hidden service* delle *darknet*. Saranno, inoltre, sviluppate le tecniche di analisi immagine finalizzate all'identificazione delle vittime di abusi.
Tra gli obiettivi formativi si segnalano: conoscenze in ambito di sistemi operativi, protocolli di rete, linguaggi e strumenti per lo sviluppo web (HTML, PHP, CSS, Java, MySQL, etc.) nonché dei linguaggi di *scripting* (Pyton, Javascript), strumenti di analisi forense (Encase, FTK, Magnet Axiom, Xways, UFED Cellebrite, Oxigen Forensics) sia "live" sia "post mortem"; attività di indagini informatiche alla luce dell'ordinamento giuridico italiano; tecniche di indagine informatica; computer crimes e i reati eventualmente informatici; ruolo e rapporti con gli *Internet Service Providers*; acquisizione, conservazione, analisi e produzione dei dati; attività nel *dark web*; tecniche di trattamento dei reperti informatici.

INCIDENT RESPONDER

Al verificarsi di attacchi informatici aventi ad oggetto reti e infrastrutture critiche, l'operatore sarà in grado di assicurare un intervento tempestivo volto a ridimensionare le conseguenze negative e ripristinare la continuità dei servizi erogati alla comunità. Partendo dagli aspetti fondamentali del *cyberspace* relativi ai sistemi operativi, Internet, e sistemi *cloud*, l'operatore dovrà essere in grado di acquisire e sviluppare metodologie e strumenti per condurre attività di difesa *cyber*, test di sistemi in rete, analisi e investigazione digitale. Tra gli obiettivi formativi si segnalano: la sicurezza dei sistemi in rete, analisi di *Security Operations Center*, attività di *Penetration Testing* e *Vulnerability Assessment*, analisi di sistemi compromessi, acquisizione di conoscenze di linguaggi e strumenti per lo sviluppo Web (HTML, PHP, CSS, Java, MySQL, etc.), nonché dei linguaggi di *scripting* (Pyton, Javascript), modalità di analisi e recupero dati dai più diffusi supporti di memoria, server e dispositivi mobili (unitamente agli aspetti giuridici della *Digital Forensics* e della *Privacy*), riconoscimento preventivo di

eventuali errori o possibili vulnerabilità nella rete, sviluppo di un sistema di procedure sulla gestione di un'emergenza, analisi del rischio e *audit* di sicurezza; *report* di incidenti per eventuali profili investigativi.

Per garantire una maggiore versatilità d'impiego degli operatori formati, ferma restando la frequenza del corso di specializzazione di primo livello, che resta primo riferimento formativo per il personale che fa ingresso in Specialità, si è optato per la previsione di competenze polivalenti, in modo da formare il personale sotto il profilo del metodo di approccio al crimine informatico, dotandolo di qualificazioni operativo-professionali che efficientano l'attività di polizia, tutelando al contempo chi l'attività svolge.

Per ciò che concerne l'offerta formativa, il primo corso che sarà istituito presso la Direzione Centrale degli Istituti d'Istruzione sarà il corso "ANALISTA OSINT SOCMINT", strutturato (secondo un modello comune alle tre qualificazioni professionali) in tre fasi:

Fase *e-learnig*, mediante la frequenza di moduli didattici secondo le modalità consolidate in materia di aggiornamento professionale (durata: una settimana);

Fase residenziale: consistente nella frequenza di lezioni frontali, ove saranno ulteriormente approfonditi gli argomenti trattati in modalità *e-learning* ed affrontati di nuovi, con la possibilità di confronto diretto tra docente e discenti in merito alle questioni tecnico-operative affrontate (durata: una settimana, con previsione di esame finale);

Fase di tirocinio applicativo presso gli uffici di appartenenza, ove gli operatori formati saranno affiancati da esperti del settore per mettere concretamente in pratica le tecniche acquisite nell'attività di polizia di carattere specialistico (durata: una settimana).

IL DIRETTORE DELL'UFFICIO
(De Bartolomeis)