

SCHEDA CORSO SOC SPECIALIST

Dati del corso

Voce	Dettaglio
Titolo	SOC Specialist
Erogato da	Fata Informatica S.r.l. – CybersecurityUP
Modalità	E-learning
Struttura	6 moduli indipendenti, acquistabili singolarmente, in 2 pacchetti o come percorso completo
Durata video	28 ore 50 min complessive (10 h 52 min SOC Specialist Base · 17 h 58 min SOC Specialist Avanzato)
Lingua	Italiano
Accesso	h24, per 12 mesi
Piattaforma pratica	HackMeUP: 1 anno di accesso incluso nel percorso completo
Docenti	Docenti universitari ed esperti del settore
Attestati	Attestato di partecipazione al termine di ogni modulo
Certificazioni	CPSS o CTSS, solo con il percorso completo, in base ai requisiti richiesti per l'accesso all'esame
Prezzo	Pagamento unico o rateale: vedi sezione «Prezzi e modalità di pagamento»

Presentazione e finalità

Il percorso SOC Specialist forma la figura professionale del Security Operation Center Specialist, dedicata alla difesa della sicurezza IT, con competenze specifiche nelle tecniche di Incident Response.

I corsi sono tenuti da docenti universitari ed esperti del settore, per garantire un apprendimento pratico e altamente qualificato. Il percorso parte dalle nozioni fondamentali (reti, protocolli, minacce) e arriva a competenze avanzate: gestione degli incidenti, firewall e intrusion detection, SIEM e Threat Hunting.

Il percorso garantisce non solo la conoscenza teorica, ma lo sviluppo di competenze operative concrete, in linea con le attività svolte in un Security Operation Center e con i requisiti richiesti per la certificazione. A supporto sono integrati strumenti avanzati e ambienti pratici per le attività di monitoraggio, analisi degli eventi di sicurezza e gestione degli incidenti.

Completando il percorso completo è possibile accedere all'esame per la certificazione CPSS (Certified Professional SOC Specialist) o, in assenza dei requisiti, CTSS (Certified Technician SOC Specialist). Il percorso completo include 1 anno di accesso a HackMeUP, l'ambiente operativo dove simulare scenari reali di SOC.

A chi è rivolto e requisiti per iscriversi

Il percorso è finalizzato alla formazione del Security Operation Center Specialist. Questa figura deve saper applicare le conoscenze in ambito networking e sulle TTP (tattiche, tecniche e procedure) degli attori di minaccia, per mettere in atto processi e procedure adeguate nelle fasi di identificazione, contenimento e risposta agli incidenti, fino a prevenire gli attacchi prima che causino danni all'azienda.

Moduli	Competenze richieste
Foundation, Threats, Response, Defense, Monitoring	Nessuna competenza specifica, solo dimestichezza con PC e navigazione Internet. I moduli forniscono le conoscenze di base per costruire le competenze richieste.
Threat Hunting	Conoscenza dei fondamenti di networking TCP/IP, della Cyber Kill Chain e delle nozioni sulle minacce informatiche (APT, malware, ecc.), oltre agli argomenti dei moduli precedenti.

I prerequisiti specifici di ciascun modulo sono indicati nel programma dettagliato. Fata Informatica non fornisce consulenza sulle esigenze formative del Cliente: la scelta dei moduli è responsabilità dell'acquirente.

Obiettivi formativi

Al termine del percorso completo il discente sarà in grado di:

- Comprendere cos'è un attacco informatico, le fasi della Kill Chain e i principali attori, tecniche e vettori d'attacco.
- Acquisire solide basi di reti e protocolli (ISO/OSI, TCP/IP, routing, DNS, DHCP, protocolli applicativi e web) e conoscere i sistemi di protezione della rete.
- Riconoscere le minacce che un SOC affronta ogni giorno: vulnerabilità web (OWASP Top 10), attacchi, social engineering e malware.
- Padroneggiare il ciclo dell'Incident Response (preparazione, detection & analysis, contenimento, eradicazione, recovery, attività post-incident).
- Usare strumenti di diagnostica di rete e di packet inspection (Nmap, Tcpdump, Tshark, Wireshark).
- Configurare e amministrare firewall open source (Netfilter/Iptables, BSD pf) e commerciali (Check Point) e sistemi IDS/IPS con Snort.
- Lavorare con i SIEM IBM QRadar e Splunk: raccolta eventi, regole, allarmi, ricerche in SPL, report e dashboard.
- Condurre attività di Threat Hunting: ipotesi, modelli di riferimento, caccia in rete lungo la pila ISO/OSI, analisi di flussi sospetti.
- Prepararsi all'esame per la certificazione professionale CPSS o CTSS.

Gli obiettivi specifici di ogni modulo sono riportati nel programma dettagliato.

Struttura del percorso: moduli e pacchetti

Il percorso è articolato in 6 moduli indipendenti, acquistabili singolarmente, in pacchetti consigliati o come percorso completo.

Cod.	Modulo	Pacchetto	Durata video
SOC-BAS	Foundation: reti e sicurezza	SOC Specialist Base	02:22:39
SOC-THR	Threats: attacchi, social engineering e malware	SOC Specialist Base	04:36:51

Cod.	Modulo	Pacchetto	Durata video
SOC-RSP	Response: incident response e network analysis	SOC Specialist Base	03:52:32
SOC-DEF	Defense: firewall e intrusion detection	SOC Specialist Avanzato	06:00:16
SOC-MON	Monitoring: SIEM e SOC Operations	SOC Specialist Avanzato	04:34:52
SOC-HNT	Threat Hunting	SOC Specialist Avanzato	07:22:59
	Totale		28:50:09

Pacchetti

Pacchetto	Codice	Moduli inclusi	Durata video
SOC Specialist Base	SOC-PKG-JR	Foundation, Threats, Response	10:52:02
SOC Specialist Avanzato	SOC-PKG-SR	Defense, Monitoring, Threat Hunting	17:58:07
Percorso completo	SOC-PKG-FULL	Tutti i 6 moduli + HackMeUP (1 anno) + voucher esame nominale	28:50:09

SOC Specialist Base è il punto di partenza per chi vuole entrare in un Security Operation Center: dai fondamenti di reti e sicurezza alla conoscenza di minacce, attacchi e malware, fino a incident response e analisi di rete. **SOC Specialist Avanzato** è il livello avanzato: difesa attiva e presidio della sicurezza, dalla configurazione di firewall e IDS/IPS al monitoraggio con SIEM, fino alla caccia proattiva alle minacce. Il **Percorso completo** è l'unica opzione che dà accesso alla certificazione professionale.

Modalità di erogazione e metodologia didattica

E-learning

Il corso è fruibile 24 ore su 24 dalla piattaforma di formazione di Fata Informatica, con credenziali personali (username e password). Ogni modulo comprende:

- video lezioni registrate;
- test ed esercizi di valutazione;
- laboratori didattici (dove previsti, vedi tabella dei moduli);
- materiale scaricabile;
- e-mail di supporto per interagire con i docenti;
- Uppy, l'AI Tutor addestrato sui materiali ufficiali del corso, disponibile 24/7;
- attestato di partecipazione al termine del modulo.

Il percorso completo include inoltre 1 anno di accesso a HackMeUP e il voucher per l'esame nominale.

Uppy – il tutor AI

Uppy è incluso nel percorso formativo e risponde in modo istantaneo sui temi complessi, assiste durante le esercitazioni pratiche e aiuta nel ripasso mirato prima degli esami, 24 ore su 24.

HackMeUP – la cyber arena per le competenze operative SOC

Nel contesto di un Security Operation Center la capacità di analizzare eventi, correlare informazioni e rispondere agli incidenti è fondamentale. HackMeUP è la piattaforma pratica integrata nel percorso (1 anno di accesso nel percorso completo, acquistabile anche singolarmente) per sviluppare competenze operative in ambienti simulati realistici:

- simulazione di scenari SOC: attività pratiche su log, eventi di sicurezza e flussi di rete per l'identificazione e la gestione delle minacce;
- approccio analitico strutturato: esercitazioni su triage degli incidenti, correlazione degli eventi e definizione delle priorità di intervento;
- sviluppo del "SOC mindset": allenamento progressivo alla lettura degli indicatori di compromissione e alla comprensione del contesto degli attacchi;
- esercitazioni progressive, dalla detection alla risposta;
- laboratori aggiornati per riflettere nuove tecniche di attacco e nuove modalità di rilevazione.

Verifiche, attestati e certificazioni

Ogni modulo prevede test di valutazione dell'apprendimento, composti da domande a risposta multipla e/o prove pratiche. Il superamento dei test è requisito necessario per completare il percorso.

Titolo	Chi lo ottiene	Come
Attestato di partecipazione	Chi acquista singoli moduli o pacchetti parziali (Base, Avanzato)	Al termine di ogni modulo, dopo aver completato i materiali e superato i test; rilasciato su richiesta
CPSS – Certified Professional SOC Specialist	Chi completa il percorso completo e possiede i requisiti previsti	Esame finale, le cui modalità sono illustrate durante le lezioni
CTSS – Certified Technician SOC Specialist	Chi completa il percorso completo ma non possiede ancora i requisiti per la CPSS	Esame finale, come sopra

L'accesso all'esame e alle certificazioni è riservato a chi acquista il percorso completo, che include il voucher per l'esame nominale. Il mancato superamento dell'esame non consente di conseguire la certificazione.

Certificazione CPSS

La CPSS è rilasciata da Fata Informatica, ente accreditato secondo ISO/IEC 17024:2012 e conforme alle norme UNI 11506:2021 e UNI 11621-4:2024. È rivolta agli specialisti della sicurezza delle informazioni che si concentrano sulla protezione dei dati e sulla gestione delle minacce all'interno di un'organizzazione, e attesta competenze avanzate nella progettazione, implementazione e gestione di sistemi di sicurezza delle informazioni, inclusi i controlli di sicurezza e la risposta agli incidenti. In linea con la Legge 4/2013, i professionisti certificati saranno inseriti nel registro Accredia dei Certified Professional SOC Specialist.

Requisiti per la CPSS

- Istruzione: almeno il diploma di scuola secondaria di primo grado.
- Formazione: almeno 24 ore di aggiornamento nell'ultimo anno.

- Esercizio dell'attività di SOC Specialist: 3 mesi per chi ha una laurea o corsi post-diploma, 5 mesi per chi ha completato la scuola superiore, 6 mesi per chi possiede il diploma di scuola media.

Mantenimento. Ogni anno il professionista trasmette a Fata Informatica l'evidenza di formazione continua specifica nell'ambito SOC (corsi, convegni o sfide su piattaforme), l'evidenza di continuità professionale (o di incremento della formazione, in caso di perdita di lavoro) e l'evidenza della registrazione e del trattamento di eventuali reclami ricevuti.

Rinnovo. Al quinto anno il professionista presenta l'assenza o la corretta gestione dei reclami, il continuo esercizio della professione, i crediti formativi acquisiti negli anni di mantenimento, supera l'esame di rinnovo e paga la relativa quota, come indicato nel tariffario ufficiale. In funzione degli esiti il certificato può essere rinnovato, sospeso o revocato.

Le certificazioni sono progettate per formare esperti nella gestione delle operazioni di sicurezza SOC e differiscono per contenuti, metodologia d'esame, conformità normativa e valore nel mercato europeo.

Programma dettagliato

Ogni modulo include: e-learning, video lezioni registrate, accesso h24, test ed esercizi di valutazione, laboratori didattici, materiale scaricabile, attestato di partecipazione, e-mail di supporto per interagire con i docenti e Uppy, l'AI Tutor disponibile 24/7. Di seguito, per ciascun modulo, sono indicati i numeri specifici.

SOC-BAS – Foundation: reti e sicurezza

Introduzione. Costruisce le fondamenta indispensabili per lavorare in un Security Operation Center: capire cos'è un attacco informatico e come si sviluppa lungo la Kill Chain, e padroneggiare il funzionamento di reti e protocolli. Sono le basi tecniche e concettuali su cui poggia tutto il percorso: senza una solida comprensione di come viaggiano i dati e di come agisce un attaccante, non è possibile monitorarli, analizzarli e difenderli in modo efficace.

Obiettivi

- Comprendere cos'è un attacco informatico, chi sono gli attori in gioco e quali tecniche e vettori privilegiano.
- Conoscere il processo di Incident Response e i principi della Triade CIA.
- Padroneggiare le fasi della Kill Chain e riconoscerle in scenari reali.
- Acquisire solide basi di reti e protocolli: dai modelli ISO/OSI e TCP/IP a routing, DNS, DHCP e protocolli applicativi.
- Conoscere il funzionamento delle applicazioni web e i principali sistemi di protezione della rete (firewall, proxy, IDS/IPS, VPN, DLP, Honeypot).

A chi è rivolto. A chi si affaccia per la prima volta al mondo dei Security Operation Center.

Competenze richieste. Nessuna competenza specifica, solo dimestichezza di base con PC e navigazione Internet.

Programma del corso

- 1. Introduzione alla Cybersecurity.** La Cyber Security: cos'è un attacco informatico, il processo di Incident Response, la Triade CIA, le tipologie di Hacker, Cyber Theft Ring, quanto valgono i nostri dati sul Dark Web, i principali attori, attacchi, tecniche e vettori preferiti · La Kill Chain: le fasi (Targeting, Reconnaissance, Weaponization, Delivery, Exploitation, Installation, Command & Control, Action), l'attacco a Target.
- 2. Le reti.** Il protocollo TCP/IP: i pacchetti (modello ISO/OSI, modello TCP/IP, livelli, incapsulamento), gli Header (TCP, IP, Ethernet), il protocollo IP (indirizzi, classi, netmask, IPv6), il routing IP (tabelle di routing, Autonomous System, protocolli IGP/EGP, Distance Vector, RIP, Link State, Path Vector), il livello Data Link (indirizzi MAC, MAC Table, switch, protocollo ARP), TCP e UDP (porte, header, Netstat, three way handshake), DNS (struttura, risoluzione), il protocollo DHCP (fasi, discover, offer, request, hack, rinnovo), altri protocolli: SNMP, ICMP, FTP, SMTP, IMAP, POP3 · Le applicazioni WEB (HTTP, request, response, HTTPS, cookies, sessioni) · I sistemi per proteggere la rete: proxy, firewall, honeypot, VPN, IDS/IPS, sistemi DLP.

SOC-THR – Threats: attacchi, social engineering e malware

Introduzione. Porta nel mondo delle minacce che ogni giorno un Security Operation Center deve riconoscere e affrontare. Dalle vulnerabilità delle applicazioni web catalogate dall'OWASP alle principali categorie di attacchi, dal social engineering alle molte forme di malware: si impara a conoscere il nemico nei suoi metodi e nelle sue tecniche. È una conoscenza indispensabile per chi difende, perché non si può rilevare e contrastare ciò che non si sa riconoscere.

Obiettivi

- Conoscere il framework OWASP e la Top Ten delle vulnerabilità delle applicazioni web.
- Riconoscere le principali categorie di attacchi: DoS/DDoS, MITM, poisoning, hijacking, spoofing, attacchi a WiFi e Bluetooth.
- Comprendere gli attacchi crittografici e le tecniche di attacco alle password.
- Riconoscere le tecniche di social engineering: phishing, vishing, smishing, BEC e altre.
- Conoscere le diverse tipologie di malware, i meccanismi di infezione, persistenza ed evasione, fino a ransomware ed exploit kit.

A chi è rivolto. A chi vuole imparare a riconoscere le minacce che un SOC deve affrontare quotidianamente.

Competenze richieste. Conoscenze di reti e protocolli equivalenti a quelle fornite dal modulo Foundation.

Programma del corso

- 1. Le vulnerabilità delle applicazioni web.** Chi è OWASP · Come si compone un'applicazione web · La Top Ten OWASP (Injection, Broken Authentication, Sensitive Data Exposure, XML External Entities, Broken Access Control, Security Misconfiguration, Cross Site Scripting, Insecure Deserialization, Using Components with Known Vulnerabilities, Insufficient Logging and Monitoring).
- 2. Gli attacchi.** Cos'è uno Zero Day · DoS, DDoS e DRDoS (Smurf, Xmas Scan Attack), Man in the Middle, Man in the Browser, Buffer Overflow, Privilege Escalation, ARP Poisoning, DNS Poisoning, Domain Hijacking, ClickJacking, Session Hijacking, Spoofing (MAC, Email, Phone) · Downgrade Attack · Attacchi a WiFi (protocolli Wi-Fi, Reply Attack, Rogue AP, Evil Twin, attacchi a WPS) · Attacchi a Bluetooth (Bluejacking, Bluesnarfing, Bluebugging) · Attacchi Crittografici, funzioni Hash, Pass the Hash · Attacco alle password (tabelle arcobaleno, sale, attacchi a dizionario, ibridi, online, Brute Force, attacco al compleanno).
- 3. Il Social Engineering.** Cos'è il social engineering, scenari · Phishing, spear phishing, lateral phishing, truffe BEC, smishing, vishing · Tailgating, impersonation, dumpster diving, shoulder surfing, watering hole · I principi base del social engineering, un esempio di attacco, Social Engineering Attack Framework.
- 4. Il Malware.** Il formato PE, le DLL, Kernel Mode vs User Mode, i Protection Ring, le API · Come si viene infettati, le firme, obfuscation & mutation, malware polimorfico e metamorfico, mutation engines · La persistenza (registri di sistema, DLL Hijacking, DLL Load Order Hijacking, Trojanized System Binaries) · Le tipologie di malware (virus, backdoor, adware, spyware, keylogger, trojan, RAT, cryptojacking) · I rootkit (user mode, kernel mode, IAT Hooking, bootkit) · I malware ibridi (Conficker) · I Ransomware (fasi di un attacco, WannaCry, come comportarsi) · Macrovirus, Scareware, Fileless Malware · Gli Exploit Kit (Angler, Zeus Builder), Crime as a Service (GrandCrab).

SOC-RSP – Response: incident response e network analysis

Introduzione. Porta nel cuore operativo del mestiere: la risposta agli incidenti e l'analisi di rete. Partendo dal ruolo e dalle mansioni del SOC Specialist, si impara a gestire l'intero ciclo dell'Incident Response, dalla preparazione alla recovery, e a usare gli strumenti di diagnostica e packet inspection per leggere ciò che accade sulla rete. È il modulo che trasforma la conoscenza delle minacce in capacità concreta di individuarle, contenerle e neutralizzarle.

Obiettivi

- Comprendere il ruolo, le mansioni e la preparazione richiesta al SOC Specialist.

- Padroneggiare l'intero processo di Incident Response: preparazione, detection & analysis, contenimento, eradicazione, recovery e attività post-incident.
- Utilizzare gli strumenti di diagnostica di rete ai diversi livelli ISO/OSI (ARP scanning, ICMP scanning, traceroute, port probing, netcat, nslookup/dig, curl/wget).
- Eseguire il rilevamento automatico di oggetti e servizi di rete con Nmap e tecniche di sweeping.
- Condurre la packet inspection con Tcpdump, Tshark e Wireshark, applicando i filtri.

A chi è rivolto. A chi vuole imparare a gestire concretamente un incidente di sicurezza, dalla diagnosi alla risposta.

Competenze richieste. Contenuti dei moduli Foundation e Threats (reti, protocolli, conoscenza delle minacce).

Programma del corso

1. **Il ruolo del SOC Specialist.** Il ruolo e le mansioni · La preparazione e l'esperienza.
2. **Il processo di Incident Response.** La preparazione · Detection & Analysis · Contenimento · Eradicazione · Recovery · Attività post-incident.
3. **La diagnostica di rete.** Strumenti per i diversi livelli ISO/OSI: ARP scanning, ICMP scanning, traceroute/tracepath, port probing, netcat, nslookup/dig, curl/wget · Rilevazione automatica degli oggetti e servizi di rete: Nmap, Sweeping.
4. **La Packet Inspection.** Introduzione, contesto di utilizzo · Tcpdump, Tshark · Introduzione a Wireshark (utilizzo dei filtri).

SOC-DEF – Defense: firewall e intrusion detection

Introduzione. Porta sul fronte della difesa attiva. Si impara a configurare e amministrare i firewall, sia open source (Netfilter/Iptables, BSD pf) sia commerciali (Check Point), e a padroneggiare i sistemi di intrusion detection e prevention con Snort. È il modulo in cui si passa dalla comprensione delle minacce alla costruzione concreta delle barriere che le fermano, imparando a scrivere regole, gestire allarmi e analizzare il traffico.

Obiettivi

- Configurare e amministrare firewall open source: Linux Netfilter/Iptables (regole, firewallld, ufw) e BSD pf.
- Gestire firewall ed endpoint protection commerciali con Check Point (WebUI, Clish, Smart Console, politiche di sicurezza).
- Comprendere architettura e modello di difesa dei diversi firewall.
- Configurare e gestire IDS/IPS con Snort: detection engine, regole, integrazione in PfSense.
- Gestire allarmi e log e analizzare il traffico con Tcpdump in PfSense.

A chi è rivolto. A chi vuole imparare a configurare attivamente le barriere difensive di un'infrastruttura.

Competenze richieste. Contenuti del modulo Foundation; utile familiarità con Response per il contesto operativo.

Programma del corso

1. **I firewall open source.** Linux Netfilter/Iptables: architettura, modello di difesa, le regole, amministrazione, old school, firewallld, ufw e altre interfacce · BSD pf: architettura, modello di difesa, le regole, amministrazione.
2. **Firewall ed endpoint-protection commerciali.** Check Point Firewall: architettura, modello di difesa, WebUI e Clish, Smart Console, gestione politiche di sicurezza.
3. **Gli IDS/IPS.** Snort: introduzione, primi passi, la detection engine e le regole, Snort in PfSense, gestione delle regole, gestione allarmi e log, Tcpdump in PfSense.

SOC-MON – Monitoring: SIEM e SOC Operations

Introduzione. Porta nel cuore tecnologico del Security Operation Center: i SIEM, i sistemi che raccolgono, correlano e analizzano gli eventi di sicurezza dell'intera infrastruttura. Si lavora con due tra le piattaforme più diffuse sul mercato, IBM QRadar e Splunk, imparando a raccogliere eventi e flussi, costruire regole, gestire allarmi e trasformare grandi quantità di dati in dashboard e informazioni operative. È il modulo che mette nella postazione di chi monitora e presidia la sicurezza in tempo reale.

Obiettivi

- Comprendere il ruolo e l'architettura di un SIEM nelle operazioni di un SOC.
- Utilizzare IBM QRadar: raccolta eventi e flussi, gestione degli allarmi, costruzione delle regole.
- Padroneggiare Splunk nel contesto Big Data: piattaforma, ecosistema e soluzioni per la sicurezza (Enterprise Security, SOAR, UBA).
- Comprendere indici, indicizzazione, eventi, dataset e architetture Splunk (forwarder, indexer, search head, cluster).
- Utilizzare il Search Processing Language (SPL), lookup e macro per ricerche, report e dashboard.
- Applicare le competenze in un laboratorio pratico: dall'analisi di log firewall alla creazione di dashboard e visualizzazioni.

A chi è rivolto. A chi vuole lavorare con le piattaforme SIEM per monitorare la sicurezza in tempo reale.

Competenze richieste. Contenuti dei moduli Foundation e Response; utile familiarità con Defense.

Programma del corso

1. **I SIEM – IBM QRadar.** Introduzione, architettura, raccolta eventi e flussi, gestione degli allarmi, costruzione delle regole, caso d'uso.
2. **I SIEM – Splunk.** Introduzione a Splunk e al contesto Big Data: gestione e analisi di grandi quantità di dati strutturati, semi-strutturati e non strutturati; limiti organizzativi e tecnologici; approccio data-driven · Piattaforma ed ecosistema Splunk: raccolta, aggregazione, normalizzazione, ricerca e visualizzazione dei dati; ambiti applicativi (IT Operations, cybersecurity, DevOps, business analysis); azienda, acquisizione da parte di Cisco, community Splunkbase; portafoglio prodotti e licenze · Soluzioni Splunk per la sicurezza: Splunk Enterprise Security (SIEM), Splunk SOAR (orchestrazione e automazione tramite playbook), Splunk User Behavior Analytics (rilevamento anomalie tramite machine learning), integrazione tra ES, SOAR e UBA · Caratteristiche generali di Splunk Enterprise: funzionamento multiplatforma, acquisizione dati da sistemi/applicazioni/database/dispositivi di rete/ambienti virtuali e cloud, processo di ingestione/indicizzazione/ricerca, Splunk Web, CLI e applicazioni installabili · Indici, indicizzazione ed eventi: struttura degli indici, organizzazione in bucket, ruolo dell'indicizzatore, trasformazione dei flussi in eventi, timestamp ed estrazione campi, concetti di host/source/sourcetype · Eventi, metriche e set di dati: differenze tra eventi e metriche, indici dedicati, organizzazione in dataset, modelli di dati e Pivot Editor · Architetture Splunk: istanza singola vs distribuita, livelli di acquisizione/indicizzazione/ricerca, forwarder/indexer/search head, Heavy e Universal Forwarder, scalabilità orizzontale e cluster di indicizzazione · Interfaccia operativa e flusso dei dati: organizzazione di Splunk Web, acquisizione da file/directory/protocolli di rete/HTTP/HTTPS/script/servizi di sistema, percorso dei dati dalle sorgenti agli indici · Fondamenti della ricerca: applicazione Search & Reporting, selezione dati per indice/host/source/sourcetype/campi estratti, operatori logici e caratteri jolly, intervalli temporali relativi/assoluti/personalizzati · Oggetti di conoscenza, report e dashboard: knowledge base, salvataggio ricerche e pivot come report, pianificazione e condivisione, creazione di avvisi, dashboard con Splunk Dashboard Studio · Search Processing Language (SPL): struttura del linguaggio, pipeline di elaborazione, categorie di comandi (streaming, trasformazione, generazione, elaborazione dataset), riepiloghi statistici e visualizzazioni, comandi personalizzati in Python · Lookup e macro di ricerca: arricchimento dati con lookup (file, KV Store, script), creazione e applicazione automatica di lookup, macro SPL riutilizzabili e parametrizzate · Laboratorio

pratico: dalla ricerca alla dashboard – analisi di log firewall, individuazione di attività di discovery, identificazione sorgenti oltre soglia, creazione di visualizzazioni e pannelli con indicatori di tendenza.

SOC-HNT – Threat Hunting

Introduzione. Porta al livello più avanzato della difesa: la caccia proattiva alle minacce. Invece di aspettare l'allarme, si impara a cercare attivamente le tracce di un attacco già presente nella rete, formulando ipotesi, esplorando il traffico e analizzando i flussi lungo tutta la pila ISO/OSI. Attraverso modelli di riferimento, threat intelligence e casi reali di infezione da malware noti, si sviluppa il "mindset del cacciatore": l'atteggiamento che distingue un SOC Specialist maturo, capace di anticipare le minacce prima che causino danni.

Obiettivi

- Comprendere cos'è il Threat Hunting, i suoi obiettivi, le strategie e gli strumenti.
- Collocare il Threat Hunting all'interno dei processi di Incident Response e Risk Management.
- Applicare i modelli di riferimento: piramide della paura, Kill Chain, modello a diamante.
- Condurre la caccia in rete analizzando il traffico anomalo con packet inspection (Tcpdump, TShark, Wireshark).
- Ricercare le minacce lungo la pila ISO/OSI, dal livello fisico a quello applicativo.
- Analizzare flussi sospetti e riconoscere infezioni da malware noti (Ursnif, Qakbot).

A chi è rivolto. A chi vuole affrontare il livello più avanzato della difesa: la ricerca proattiva delle minacce.

Competenze richieste. Conoscenza dei fondamenti di networking TCP/IP, della Cyber Kill Chain e delle nozioni sulle minacce informatiche (APT, malware, ecc.), oltre ai contenuti dei moduli precedenti.

Programma del corso

- 1. La ricerca della minaccia.** Introduzione, cos'è il Threat Hunting, tipo di strategia, strumenti, obiettivi · Il Threat Hunting all'interno del processo di Incident Response · Il Threat Hunting e il processo di Risk Management · Le fasi della caccia, i confini della caccia · La threat intelligence e l'analisi forense · Le informazioni di intelligence: IoC.
- 2. Modelli e metodi.** I modelli di riferimento, piramide della paura · La Kill Chain e le contromisure, il modello a diamante · Come si esplora il terreno di caccia · Dalle ipotesi al report: il processo di caccia, la struttura di un report.
- 3. La caccia in rete.** Dalla intelligence all'infrastruttura, il ruolo del cacciatore · L'origine della caccia: il traffico anomalo · La Packet Inspection (live o registrata, strategie e piani per la difesa, strumenti, punti di indagine e inserzione) · Libpcap e gli strumenti derivati: Tcpdump, TShark · Uno strumento agile: Wireshark (filtri, identificazione User ed Hosts, esportazione flussi Pcap).
- 4. Ricerca delle minacce attraverso la pila ISO/OSI.** Livello fisico: anatomia e sfruttamento del protocollo ARP, ARP ping, criteri di sicurezza · Livello IP: anatomia e sfruttamento del protocollo ICMP, ping sweep, esfiltrazione dati · Livello trasporto (TCP): 3-way handshake, contatori Wireshark · Scanning: nmap (host discovery, port sweep), TCP SYN/stealth, TCP connect, FIN, NULL, XMAS scan · Livello trasporto (UDP): protocollo, traffico normale e non, attività di scansione · Livello applicazione: DHCP, DNS, HTTP (anatomia, traffico, strumenti Wireshark dedicati, HTTPS, analisi e decifratura).
- 5. Analisi di flussi sospetti.** Il rilevamento di attacchi mediante analisi dei flussi, un traffico sconosciuto · Esame di flussi collegati a malware noti: infezione da Ursnif, infezione da Qakbot.

Requisiti hardware e software

Componente	Requisito
Personal computer	Per le sessioni di teoria e pratica sono necessari PC desktop o notebook, mentre per la fruizione dei contenuti teorici è possibile utilizzare dispositivi mobile. In particolare, nelle sessioni pratiche è suggerito l'uso di PC con processori 64 bit, almeno quad-core, con supporto Intel VT-x / AMD-V o tecnologia equivalente per compatibilità con ambienti di virtualizzazione locali, con minimo 8 GB di RAM (consigliati almeno 16 GB) e almeno 80 GB di spazio libero su disco per l'installazione e l'esecuzione delle macchine virtuali. Monitor con risoluzione minima consigliata di 1280 × 720 pixel. Scheda audio e cuffie o altoparlanti. Webcam e microfono qualora siano previste attività formative in modalità blended.
Software di virtualizzazione	La postazione dedicata alle sessioni pratiche dovrà consentire l'installazione e l'utilizzo di un software di virtualizzazione compatibile con le macchine virtuali messe a disposizione per le esercitazioni, o comunque suggerite nell'ambito dei laboratori quale strumento per la costruzione di un proprio insieme di strumenti. Le VM saranno distribuite in formato OVA. Per la realizzazione di VM al fine della costruzione di un proprio laboratorio è consigliato seguire l'esempio d'uso di ciascun corso al fine di rendere speculare l'esperienza nelle videolezioni con la pratica. In ambito aziendale/corporate è del tutto evidente che l'utente dovrà disporre dei permessi necessari per installare, configurare ed eseguire software e macchine virtuali sulla propria postazione o avere soddisfatti in modo alternativo i requisiti. Per garantire la piena fruibilità delle attività formative e dei laboratori, <u>è pertanto raccomandato l'utilizzo di un PC personale</u> sul quale l'utente disponga di privilegi amministrativi.
Browser	È necessario utilizzare una versione aggiornata e supportata di uno dei principali browser web, quali: • Google Chrome • Mozilla Firefox • Microsoft Edge • Apple Safari Il browser dovrà consentire l'esecuzione di JavaScript, l'utilizzo dei cookie, il download di file e la riproduzione di contenuti multimediali.
Connettività	Connessione Internet ad alta velocità e stabile, necessaria per lo streaming dei video e per accesso ai laboratori

Componente	Requisito
Requisiti di rete e sicurezza	La postazione e la connessione utilizzate devono consentire l'accesso ai servizi Internet necessari alla fruizione della piattaforma e allo svolgimento delle esercitazioni. Eventuali firewall, proxy, VPN, sistemi di filtraggio, DNS filtering, endpoint security o altre policy di sicurezza applicate da reti aziendali/corporate non devono impedire o limitare: • L'accesso alla piattaforma di erogazione e agli eventuali servizi esterni integrati; • Il download dei materiali didattici e delle immagini delle macchine virtuali • La riproduzione di contenuti audio/video • L'utilizzo di cookie, JavaScript e degli altri servizi web richiesti • Eventuali connessioni necessarie allo svolgimento dei laboratori pratici (VPN via UDP in porta non standard) Qualora venga utilizzata una postazione o una rete aziendale soggetta a restrizioni, l'utente dovrà verificare preventivamente la disponibilità dei permessi di installazione, virtualizzazione e accesso alla rete necessari. Per garantire la piena fruibilità delle attività formative e dei laboratori, <u>è pertanto raccomandato l'utilizzo di un PC personale</u> sul quale l'utente disponga di una connessione Internet non soggetta a restrizioni corporate incompatibili con le attività previste.
Lettura documenti	Software di lettura di file in formato .pdf
Audio e video	Software e dispositivi per la riproduzione di file audio e video (casse o cuffie)
Laboratori	I laboratori potranno essere fruibili attraverso: • Materiale scaricabile da sottoporre a strumenti locali (la cui installazione è a carico dell'utente), quali simulatori, analizzatori, ecc. Questi strumenti potranno essere collocati su proprio PC o in apposita VM sperimentale • Connessione Web diretta a piattaforma di simulazione/esercitazione • Connessione VPN (tramite differenti porte) ad infrastrutture virtuali remote. Gli strumenti di indagine devono essere predisposti dall'utente nel proprio PC o all'interno di VM predisposte all'esercitazione. In alcun caso viene fornito un ambiente di analisi o strumentazione di attacco attraverso le piattaforme. ATTENZIONE! In alcuni casi è possibile che il laboratorio trattino materiale pericoloso quale exploit o malware. È fondamentale trattare questi casi in VM isolate e protette in modo da evitare contaminazioni o incidenti alle infrastrutture estranee ai laboratori.

Il Cliente si impegna ad adeguare i propri sistemi hardware e software in caso di aggiornamenti o mutamenti della piattaforma. Fata Informatica non risponde dei difetti di fruizione dovuti al mancato possesso dei requisiti minimi di sistema.

Durata dell'iscrizione, accesso e assistenza

Voce	Dettaglio
Validità dell'iscrizione – singolo modulo	12 mesi dalla data di iscrizione
Validità dell'iscrizione – path o Path completo	12 mesi dalla data di iscrizione
Scadenza	Terminato il periodo, l'iscrizione viene disattivata automaticamente: lezioni e test vanno completati entro la scadenza
Accesso ai materiali	h24, con username e password personali, non cedibili
Area personale	Elenco dei corsi frequentati e dei materiali correlati
Credenziali	Generate automaticamente e inviate dal tutor didattico dopo l'iscrizione e il pagamento
Assistenza didattica	Sistema di ticket per domande ai docenti e allo staff, attivo per tutta la durata dell'iscrizione; e-mail di supporto supportodidattico@fatainformatica.it ; tutor AI Uppy 24/7
Reclami	Per iscritto a Fata Informatica, Via Tiburtina 912, 00156 Roma; esito comunicato entro 20 giorni lavorativi
Accesso HackMeUP	1 anno, incluso nel percorso completo dalla data di iscrizione

Prezzi e modalità di pagamento

I prezzi sono espressi in euro, IVA inclusa. Ogni opzione è acquistabile in un'unica soluzione oppure, dove indicato, a rate.

Il pagamento avviene online tramite il servizio Stripe. Fata Informatica non gestisce né memorizza i dati degli strumenti di pagamento. Eseguito il pagamento, viene emessa la fattura. Il pagamento a rate è disponibile solo ove espressamente indicato. Completata l'iscrizione e saldato il prezzo, il Cliente riceve le credenziali di accesso. Il pagamento a rate comporta una maggiorazione del 5%.

Recesso e condizioni di vendita

L'acquisto è regolato dalle Condizioni di Vendita dell'e-commerce di Fata Informatica S.r.l. (Rev. 03 del 07.10.2026) che il Cliente accetta con modalità point and click prima dell'acquisto. Il Cliente dichiara di aver letto questa Scheda del Corso prima di acquistare.

- **Recesso (consumatori).** 14 giorni dalla data di acquisto, senza motivazione e senza costi (art. 52 Codice del Consumo).
- **Perdita del recesso.** Il diritto non è più esercitabile dopo l'invio delle credenziali che danno accesso immediato alla piattaforma. Chi vuole recedere deve attendere i 14 giorni prima di ricevere le credenziali.
- **Fruizione immediata.** Il Cliente può chiedere, durante l'ordine, di accedere subito al corso, accettando di perdere il diritto di recesso (art. 59, comma 1, lett. o). Riceve conferma del contratto e ricevuta via e-mail.
- **Rimborso.** In caso di recesso valido, entro 60 giorni dall'esercizio, con riaccredito sullo stesso strumento di pagamento.

- **Diritto d'autore.** Videolezioni, slide e materiali sono di proprietà di Fata Informatica: è vietato copiarli, distribuirli o cederli. Le credenziali sono personali e non cedibili.
- Il testo completo delle Condizioni di Vendita prevale su quanto qui sintetizzato.