L’Analyse Inforensique Avancée et Réponse aux Incidents Complexes

Lien : https://innov-systems.com/formation/lanalyse-inforensique-avancee-et-reponse-aux-incidents-complexes

DURÉE
5 jours (35h)

RÉFÉRENCE
SEC292

CATÉGORIE
Analyse Apres Incident : Analyse Forensique, Investigation Numérique et Plan de Continuité

OBJECTIFS DE LA FORMATION

À l'issue de cette formation, vous serez capable de :

- Approfondir la compréhension des mécanismes d’attaque et des artefacts systèmes pour en extraire des preuves fiables
- Maîtriser les techniques d’investigation sur mémoire, réseau et systèmes de fichiers dans des contextes complexes
- Savoir reconstituer des chronologies d’incidents et identifier les vecteurs de compromission
- Exploiter les outils et frameworks d’automatisation de l’analyse (Volatility, Timesketch, OSQuery, MISP, etc.)
- Développer une approche globale de la réponse à incident et de la remédiation post-compromission

POUR QUI ?

- Investigateurs numériques confirmés souhaitant se spécialiser dans les environnements complexes
- Analystes SOC, membres de CSIRT/CERT
- Administrateurs systèmes, réseaux et sécurité expérimentés
- Experts techniques en réponse à incident et sécurité opérationnelle

Programme détaillé

1 / CONTEXTE ET MÉTHODOLOGIE D'INVESTIGATION

- Phases d'une investigation numérique avancée
- Chaîne de conservation et intégrité des preuves
- Outils de collecte et d'analyse : panorama et critères de choix

2 / INDICATEURS DE COMPROMISSION ET THREAT INTELLIGENCE

- Typologie et cycle de vie des IOC
- Corrélation via plateformes MISP et Yeti
- Génération et automatisation d'IOC
- Exploitation du renseignement de menace pour orienter l'investigation

3 / OUTILS DE HUNTING ET AUTOMATISATION

- Introduction à OSQuery, Kansa et GRR
- Création de scénarios de détection avancés
- Automatisation du triage et du hunting via scripts et frameworks open source

4 / INVESTIGATION SUR LES CAPTURES ET JOURNAUX RÉSEAUX

- Analyse des logs de services critiques : DNS, Proxy, HTTP, Syslog, Firewall
- Étude des flux suspects et anomalies comportementales
- Reconstitution de sessions et corrélation multi-sources

5 / DÉTECTION DES CANAUX DE COMMANDE ET DE COMMUNICATIONS CACHÉES

- Analyse de trafic PCAP et Netflow
- Identification des canaux de Command & Control (C2)
- Détection de tunnels ICMP, DNS et HTTP déguisés

- Rétro-conception de protocoles de communication

6 / CRÉATION DE SIGNATURES ET RÈGLES DE DÉTECTION

- Règles YARA et Suricata
- Méthodologie de validation et tests de détection
- Intégration dans des SIEM et outils de corrélation

7 / STRUCTURES MÉMOIRES ET MÉTHODES D'EXTRACTION

- Architecture mémoire Windows et Linux
- Méthodes de capture (DumpIt, WinPMem, LiME)
- Extraction et vérification d'intégrité

8 / INVESTIGATION DES PROCESSUS ET DES INJECTIONS DE CODE

- Détection de processus cachés et d'injections (Process Hollowing, DLL Injection)
- Analyse des shellcodes et de leur comportement
- Suivi des handles, modules et communications inter-process

9 / INVESTIGATION KERNEL ET DEBUGGING AVANCÉ

- Analyse des structures SSDT, IDT et Memory Pool
- Utilisation de Windbg et Volatility pour la mémoire noyau
- Cas pratiques : analyse live et mini-dumps

10 / ARTEFACTS DU FILESYSTEM NTFS

- MFT, USN Journal, LogFile et $Secure
- Corrélation temporelle et anomalies d'accès
- Analyse des altérations de métadonnées (timestomping, antiforensics)

11 / TIMELINE FORENSIQUE ET SUPER-TIMELINE

- Fusion des sources temporelles (FS, mémoire, logs, réseau)
- Création de super-timelines avec Plaso et Timesketch
- Étude de cas : reconstruction d’une compromission complète

12 / MÉCANISMES DE PERSISTANCE ET MOUVEMENTS LATÉRAUX

- Détection de services, tâches planifiées, WMI et clés de registre suspectes
- Analyse des comptes et rôles Active Directory
- Investigation des EventID critiques et corrélation avec attaques connues (Pass-the-Hash, Golden Ticket)

13 / RECONSTITUTION D’UNE CHAINE D’ATTAQUE

- Étude de cas complète : de la compromission initiale à la persistance
- Corrélation mémoire / réseau / système
- Élaboration d’un rapport d’investigation et de recommandations

14 / DÉFENSE ET REMÉDIATION POST-INCIDENT

- Validation de la remédiation et contrôle de réinfection
- Amélioration continue du plan de réponse à incident
- Mise en œuvre d’alertes et scénarios automatisés

15 / ÉVALUATION ET SYNTHESE

- Quiz technique de validation des acquis
- Échanges et retours d’expérience
- Ressources et outils complémentaires pour aller plus loin

Approche pédagogique

- Support Ecrit et Projection
- Exposés Interactifs, Podcasts et Vidéos
- Brainstorming et Jeux de Rôle
- Cas Pratiques et Labs inclus pour leur impact opérationnel
- Test de Validation des Acquis des Connaissances

Prochaines dates programmées

06 au 10 Juil. 2026	Présentiel - Casablanca
31 Août au 04 Sep. 2026	Distanciel
26 au 30 Oct. 2026	Distanciel

Autres dates possibles sur demande. Contactez-nous pour organiser une session intra-entreprise.

Réservation & Renseignements

Téléphone : +212 522 247 210
Email : contact@innov-systems.com
Web : https//www.innov-systems.com