Ce travail a bénéficié d'une aide de l'État gérée par l'Agence Nationale de la Recherche au titre de France 2030 portant la référence «ANR-23-CMAS-0026».



ANALYSE FORENSIQUE ET RÉPONSE AUX INCIDENTS EN ENVIRONNEMENT WINDOWS

« Devenez un expert de la réponse à incident et de l'analyse forensique en environnement Windows ! »

SYLLABUS

Bienvenue dans la formation " Analyse forensique et Réponse aux incidents en environnement Windows".

Ce syllabus a pour fonction de vous fournir un aperçu clair des étapes du parcours et des ressources mises à votre disposition en précisant notamment ses objectifs, son programme et ses méthodes pédagogiques. Il est pensé comme un guide pratique dans

lequel vous trouverez toutes les informations nécessaires pour suivre le fil conducteur de la formation et anticiper les prochaines étapes.

Nous vous invitons à le consulter régulièrement pour tirer pleinement parti de cette formation.

INFORMATIONS GÉNÉRALES

Titre du cours : Analyse forensique et Réponse aux incidents en environnement Windows

Prix : 3 075 €

Dates : du 30 novembre 2026 au 6 février 2027

Durée en semaine : 8

Effort (h) : 30 heures *(15h théorie et connaissance, 15h TP et lab + examen)*

Rythme recommandé par semaine : 4 heures / semaine

Permanences virtuelles : 4 heures - 1 heure toutes les 2 semaines

Langue : Français

PRÉREQUIS

Cette formation s'adresse aux analystes SOC, aux équipes d'IR, aux administrateurs sécurité et à toute personne qui souhaite renforcer sa capacité d'analyse post-incident.

Prérequis de connaissances / compétences :

- Bases Windows ;
- Notions réseau TCP/IP ;
- Compréhension générale des attaques informatiques ;
- Utilisation basique de la ligne de commande.

Avant toute inscription nous vous conseillons de réaliser le test de positionnement.

ÉQUIPEMENT REQUIS

- Ordinateur avec accès à Internet (cours depuis Moodle FUN MOOC, TPs sur VM CyberRange M&NTIS en ligne.

INSCRIPTION AUPRÈS DE L'UNIVERSITÉ DE RENNES

En vous inscrivant, vous accéderez à la formation portée par l'Université de Rennes, qui va certifier la formation.

TEST DE POSITIONNEMENT POUR RÉUSSIR VOTRE MICRO-CERTIFICATION

Avant de vous inscrire, si vous souhaitez évaluer vos connaissances, vous pouvez accéder à un test de positionnement. Le lien est disponible sur le catalogue.

RESPONSABLE PÉDAGOGIQUE

Tristan Pinceaux, Head of CERT Almond, Administrateur InterCERT-France



Passionné de la première heure et fort de plus de 15 ans d'expérience en réponse à incidents (Orange, CNRS, Airbus, IBM), Tristan est le fondateur du CERT Almond. Habitué des situations d'urgence, il a piloté avec son équipe des centaines de crises et réponses à incidents, dont plus de 50 attaques par ransomwares.

Très impliqué dans la communauté (CTF, veille, partage de connaissances), il consacre également son temps à la transmission, notamment comme enseignant dans plusieurs écoles d'ingénieurs (UTT, ESILV).

Auteur d'articles et conférencier régulier (InterCERT, CESIN, CLUSIF, Campus Cyber, FIC, ...), vous le croiserez souvent lors d'événements Blue Team / DFIR ou au détour d'une rump.

ÉTABLISSEMENT

almond

DESCRIPTION

Cette formation couvre l'ensemble de la chaîne de traitement d'un incident de cybersécurité Windows, depuis la qualification initiale et l'investigation forensique avancée, l'analyse mémoire, le reverse engineering de malwares, jusqu'au reporting et aux recommandations à appliquer.

Le parcours est structuré autour de cas réels, de méthodologies opérationnelles et d'artefacts techniques issus d'environnements Windows modernes.
L'objectif est de former des analystes capables de :

- ✓ Comprendre le cycle complet d'une réponse à incident ;
- ✓ Collecter et préserver la preuve numérique ;
- ✓ Analyser des traces systèmes, réseau et mémoire ;
- ✓ Identifier des mécanismes de persistance et d'exécution ;
- ✓ Reconstruire une timeline d'attaque ;
- ✓ Produire des livrables exploitables en contexte SOC/CERT/CSIRT ;
- ✓ Conduire une investigation DFIR de bout en bout.

OBJECTIFS

Cette formation a été conçue pour vous donner une méthodologie concrète pour **répondre à un incident de sécurité**, de la détection des premiers symptômes à la sortie de crise. Elle vous apportera des **clés de compréhension** opérationnelles et concrètes pour :

- ✓ Dimensionner le périmètre,
- ✓ Définir les éléments à collecter
- ✓ Parser ces artefacts systèmes
- ✓ Effectuer les investigations : corréler et les analyser les éléments pour transformer la donnée en information
- ✓ Et ainsi exploiter ces traces pour reconstruire la chronologie de l'attaque de manière détaillée

L'objectif n'est pas seulement de connaître les outils, mais de comprendre : où chercher, quoi corréler, et surtout de répondre à la question « **que s'est-il passé ?** »
Enfin, apporter des solutions sur le « **que faire maintenant ?** » pour guider la victime vers la sortie de crise, la reprise de contrôle du SI ; tout en réduisant l'effort de reconstruction et en garantissant un niveau de sécurité élevé.

Lors de ces 16 modules qui représentent environ 15h de formation et 15h de pratique, nous allons travailler sur des cas réalistes, avec un fil conducteur clair : la logique du **framework MITRE ATT&CK**, appliquée à une démarche d'enquête, illustrant les principales tactiques observées lors d'une compromission.
À travers des exemples réels, nous verrons quelles traces permettent d'en reconstruire la logique et la chronologie.

Nous commencerons par le cadre d'intervention : contexte, périmètre, collecte et conservation des preuves pour sécuriser le périmètre et préserver l'intégrité des données.
Nous étudierons les bonnes pratiques de gestion de crise.

Nous reconstruirons ensuite les premières phases d'activité suspecte à travers l'analyse des **Event Logs Windows**, des artefacts réseau et la corrélation via un SIEM afin d'identifier les premiers indicateurs d'actions malveillantes ou suspectes.

Nous approfondirons les preuves d'activité locale avec les artefacts liés au système de fichiers et les artefacts d'exécution pour comprendre ce qui a été lancé, quand, et dans quel contexte.
Nous analyserons ensuite les mécanismes de persistance, les artefacts utilisateurs, ainsi que les détournements de binaires natifs dits "living off the land" souvent associées à des tactiques d'évasion de défense.

Nous aborderons ensuite la **mémoire vive** avec Volatility et MemProcFS selon une méthodologie structurée pour identifier ce qui n'apparaît pas sur disque.

Nous verrons également comment procéder à l'**analyse de code malveillant**, à travers des techniques d'analyse statique et dynamique, afin de comprendre le comportement réel d'un binaire identifié durant l'investigation.
Enfin, nous verrons comment travailler de manière collaborative et comment **structurer un rapport** d'investigation clair et exploitable.
Pour terminer vous serez invité à travailler sur une **étude de cas** permettant de consolider l'ensemble des 16 modules.

Chaque module s'inscrit dans une vision globale : celle d'un attaquant qui progresse par étapes, et d'un analyste capable de reconstruire ces étapes à partir d'artefacts et de corrélations. Cette formation vous apportera une méthodologie concrète pour réaliser une réponse à incident de la détection des premiers symptômes jusqu'à la sortie de crise.

1. Bloc 1 - Cadre & Méthodologie

> Cadre d'intervention, contexte, périmètre, sécuriser la zone de crime et sauver ce qui peut encore l'être. Collecte et conservation des preuves notamment pour préserver l'intégrité des éléments qui pourront être utilisés plus tard. Bonnes pratiques de la gestion de crise.

2. Bloc 2 - Détection & Corrélation

> Premières phases d'investigation à travers de l'activité suspecte via les journaux d'événement Windows et les artefacts réseau. Comment corréler dans un SIEM ces premiers indicateurs afin d'identifier les premières traces d'action malveillante et de compromission.

3. Bloc 3 - Artefacts système & investigation ciblée

> Preuves d'activité locale, éléments liés au système de fichiers et artefacts d'exécution. Persistances, artefacts utilisateurs et détournement des lolbin, (living of the land binaries).

4. Bloc 4 - Mémoire vive & Malware

> Analyse via deux outils volatility et même procfs. Méthodologie PONIRD qui vous permettra d'identifier ce qui n'apparaît pas sur un disque. Analyse de code malveillant, analyse statique et analyse dynamique.

5. Bloc 5 - Restitution & Synthèse

> Travail collaboratif. Comment structurer un rapport d'investigation clair et actionnable ? Etude de cas.

PROGRAMME / DEROULÉ

1. **Introduction, Gestion de crise et Logs (Modules 1 à 4 ; 3h30 théorie)**
   - **Module 1** : Introduction et histoire, cycle de vie d'un incident, présentation du CERT, description d'une attaque et déroulé d'une Réponse à Incident (RI).
   - **Module 2** : Comprendre la preuve numérique, priorisation, préparation opérationnelle et méthodologie de collecte.
   - **Module 3** : Gestion de crise, appel de qualification, stratégie de pilotage, investigation (timeline), séquence E3R, sortie de crise et bilan.
   - **Module 4** : Introduction aux events logs (ex: EVTX), événements clés pour la détection, journalisation et mise en pratique DFIR.
2. **Réseau, SIEM, Filesystem et Artefacts d'exécution (Modules 5 à 8, 4h15 de théorie)**
   - **Module 5** : Artefacts réseaux, méthodes d'analyse et RETEX, détection/alerting avec Suricata et inspection de paquets.
   - **Module 6** : Comprendre le SIEM et Panorama, analyse et corrélation des événements, découverte de Splunk et automatisation de l'analyse.
   - **Module 7** : Introduction au filesystem, analyse de la MFT, journal MFT UsnJrnl et ADS.
   - **Module 8** : Artefacts d'exécution et registre Windows : fondamentaux forensiques, Prefetch, AmCache, ShimCache, SRUM et MUICache.

3. **Persistance, Navigation et Traces d'utilisation (Modules 9 à 12, 3h35 de théorie)**

   - **Module 9** : Introduction à la persistance, ASEP (Auto-Start Extensibility Points), Autoruns et exemples/cas de persistances.
   - **Module 10** : Historique de navigation et PowerShell forensic.
   - **Module 11** : Traces d'accès utilisateur : Jump Lists, LNK, UserAssist, Shell Bags, Cache RDP et autres artefacts d'usage.
   - **Module 12** : Composants Windows à capacité réseau : LOLBIN, LOLBAS, BITS, CertUtil, SUM UAL et RETEX Lolbin.

4. **Mémoire, Reverse Engineering et Finalisation (Modules 13 à 16, 4h45 de théorie)**

   - **Module 13 :** Forensique mémoire : architecture, collecte, recherche en clair, outils d'analyse et méthodes PONIRD (process, object & network, injection & rootkit, extraction dump).
   - **Module 14 :** Introduction au Reverse Engineering (RE), méthodologie d'analyse d'un exécutable, analyse statique, Yara et CAPA.
   - **Module 15 :** Analyse dynamique et sandboxing, sections mémoires, instructions/compilation et techniques d'obfuscation.
   - **Module 16 :** Méthode de travail, consolidation de la timeline et préparation des livrables finaux.

COMPÉTENCES VISÉES

Le parti pris est volontairement pragmatique : nous ne cherchons pas la théorie académique, mais la capacité à reconstruire une attaque avec des preuves exploitables.

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

- ✓ D'identifier des artefacts clés sur un système Windows compromis,
- ✓ De comprendre la logique d'un attaquant
- ✓ De corréler des sources multiples et prendre du recul,
- ✓ Et de structurer une analyse forensic cohérente.

Prenez le temps d'assimiler chaque module. Le forensic n'est pas une course : c'est un travail de méthode et de rigueur.

RESSOURCES PÉDAGOGIQUES ET ATTENDUS

La formation est réalisée en autonomie avec des temps d'accompagnement destinés à favoriser la progression des apprenants tout au long du parcours. Vous y trouverez des ressources variées telles que des vidéos, des documents de référence, des fiches pratiques et des Travaux Pratiques pour mettre en application les contenus théoriques. Ces ressources sont complétées par des quiz permettant de vérifier progressivement votre progression.
Vous serez également invités à participer aux échanges au travers des forums, afin de partager votre expérience, vos représentations, et enrichir votre réflexion.
Vous bénéficiez de **4 heures de permanence virtuelle**, à raison d'1 heure toutes les 2 semaines.
Nous vous recommandons de consulter régulièrement les ressources pédagogiques, de réaliser les activités et les évaluations proposées, et de participer aux échanges dans les forums afin de tirer pleinement profit de la formation.

ASSIDUITÉ ET VALIDATION DE LA FORMATION

Certaines activités sont obligatoires pour témoigner de votre assiduité et pour l'obtention de votre micro-certifications. Elles vous seront précisées dans l'espace de formation.

ÉVALUATION ET CERTIFICATION

La validation de la formation est conditionnée par l'achèvement d'activités qui jalonnent le parcours et attesteront de son suivi.

Ces activités sont :

- Les tests et quiz ;
- Les TP réalisés sur la plateforme de TP CYBERRANGE M&NTIS ;
- Le quiz final.

De manière générale, l'esprit des évaluations est formatif et vise à accompagner le développement des participants, quels que soient leurs connaissances et expériences antérieures.

Les apprenants en situation de handicap sont invités à se rapprocher de leur gestionnaire administratif (coordonnées dans le contrat de formation) pour une adaptation des modalités d'évaluation.

ACCESSIBILITÉ

Nos formations sont ouvertes à toutes et à tous. Si vous présentez un handicap (moteur, visuel, auditif, cognitif, trouble dys ou maladie invalidante), un aménagement spécifique est peut-être possible.

Avant de vous inscrire ou dès votre convocation, contactez notre référent handicap pour étudier ensemble vos besoins et adapter l'accueil, les supports pédagogiques ou les rythmes de la session, contact : pve@univ-rennes.fr.

Cette formation a été conçue pour être accessible au plus grand nombre. Les équipes de conception ont veillé à respecter autant que possible les recommandations du Référentiel Général d'Amélioration de l'Accessibilité (RGAA), publié par la Direction Interministérielle du Numérique. En particulier, toutes les vidéos incluent un sous-titrage et une transcription téléchargeable.

Vous pouvez également signaler à tout moment un problème d'accessibilité au responsable pédagogique ou à un tuteur afin que des solutions adaptées soient rapidement mises en place.

AIDE ET CONTACTS

Pour toute question sur le fonctionnement de la plateforme ou de votre compte FUN : formapro@fun-mooc.fr

Pour tout renseignement sur le contenu de la formation ou toute question d'ordre pédagogique, écrivez à cette adresse.

COMMUNICATION

En amont de la formation

Pour toute question sur le fonctionnement de la plateforme ou de votre compte FUN vous pouvez nous contacter via l'espace suivant : https://www.fun-mooc.help/hc/fr

Pendant la formation

Pour communiquer avec le responsable pédagogique, un forum dédié est à votre disposition. Vous pouvez y poser des questions générales sur la formation, des questions spécifiques sur le contenu des ressources proposées, ou préparer vos interventions pour les deux sessions synchrones. Les messages sont consultés quotidiennement, avec un délai de réponse maximal de trois jours.

Un espace dédié est prévu pour les questions techniques liées à la plateforme. Cet espace vous permet de signaler des problèmes et de contacter directement l'assistance techno-pédagogique.

Nous vous encourageons à maintenir un climat respectueux et collaboratif dans tous vos échanges – qu'ils soient avec l'enseignant, l'ingénieur pédagogique, les tuteurs ou vos pairs.

COLLECTE DE DONNEES PERSONNELLES SUR LA PLATEFORME DE TP

Dans le cadre de cette formation les TP sont réalisés sur la plateforme de TP CYBERRANGE M&NTIS.

Pour y accéder, les données suivantes vous concernant sont collectées et transmises à la plateforme : nom, prénom, log de connexion, login, date début, date de fin, cours inscrit.

Pour consulter la politique de confidentialité de la plateforme cliquez ici.