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».



ANALYSER ET PERTURBER LES CYBERMENACES SOPHISTIQUÉES

« Passer d'une lecture technique des attaques à une analyse qui anticipe les mouvements adverses, prépare des actions de défense active et éclaire des décisions prises sous incertitude. »

Bienvenue dans la formation « Analyser et perturber les cybermenaces sophistiquées ».
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 : Analyser et perturber les cybermenaces sophistiquées

Prix : 3 000 €

Dates : du 30 novembre au 6 février 2027

Durée en semaine : 8

Effort (h) : 30 heures.

Rythme recommandé par semaine : 4 heures

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

Langues : Français. Une partie des documents de travail analysés est en anglais, conformément à la réalité du métier.

PRÉREQUIS

Prérequis de connaissances / compétences : cette micro-certification s'adresse à des professionnels déjà formés ou expérimentés au renseignement sur les menaces. Sont attendus une pratique de l'analyse de la menace ou de la réponse à incident, la connaissance des cadres usuels de description d'une intrusion (Kill Chain, ATT&CK, modèle en diamant), et la capacité à lire des rapports techniques en anglais. Aucun prérequis de programmation, d'administration système ou de manipulation d'outil n'est demandé. Les publics visés sont les analystes CTI et SOC expérimentés, les répondants à incident, les traqueurs de menaces (« threat hunter »), les praticiens de la Red Team, les RSSI techniques et les responsables de cellule renseignement d'intérêt cyber.

ÉQUIPEMENT REQUIS

Aucune machine virtuelle ni plateforme de travaux pratiques n'est requise. La paillasse de cette formation est documentaire : l'apprenant lit et sur-analyse des rapports produits par d'autres, il ne manipule pas d'outil technique. Un poste bureautique suffit, avec un navigateur à jour, un lecteur de PDF, une connexion internet permettant la lecture de vidéo, et un casque ou des écouteurs pour les capsules. Les dossiers documentaires sont téléchargeables aux formats PDF et DOCX.

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



Ronan Mouchoux, responsable pédagogique et intervenant principal. Cofondateur et directeur technique de XRATOR, entreprise française spécialisée dans la gestion de l'exposition aux menaces. Il travaille depuis plusieurs années dans le renseignement sur les menaces et sur la manière de transformer des données et des rapports sur les organisations adverses en décisions opérationnelles. Il intervient dans l'enseignement supérieur sur des sujets liés à la cyberdéfense et à la sécurité des organisations. Il est l'auteur des contenus de cette formation.

François Moerman, support métier. Cofondateur et dirigeant de XRATOR, spécialiste en sécurité offensive, avec une pratique centrée sur les tests d'intrusion et les exercices de Red Team. Il apporte à la formation une lecture terrain de l'adversaire : comment un attaquant prépare ses actions, gère ses contraintes, et réagit quand l'environnement change.

ÉTABLISSEMENT

XRATOR
CONQUER YOUR RISK

DESCRIPTION

Cette micro-certification vise un changement de posture : passer d'un renseignement sur les menaces surtout descriptif à une analyse structurée qui aide à anticiper et à soutenir des décisions prises en contexte d'incertitude. Les trois premières séquences installent la grammaire commune : ce qu'est un renseignement utile, comment on raisonne sous incertitude, comment on évite le scénario unique. Vient ensuite l'idée que l'adversaire n'est pas seulement une source de traces, mais un acteur qui peut chercher à orienter les conclusions du défenseur, en jouant sur la chaîne de preuve, l'imperfection des sources et les limites des capteurs. Le dernier arc installe la maîtrise du méta-jeu entre attaquant et défenseur, avec des tactiques de perturbation employées à des fins de capitalisation d'informations.

L'approche pédagogique repose sur une paillasse documentaire. L'apprenant ne manipule pas d'outil informatique, il lit et (ré)analyse des rapports produits par d'autres : SOC, forensique, rétro-ingénierie, cellules de renseignement. Un cas fil rouge unique traverse les dix séquences et les deux situations d'évaluation, ce qui permet de retrouver chaque semaine un terrain déjà connu et d'y appliquer un outil nouveau.

Chaque séquence repose sur la même mécanique, pour créer une habitude professionnelle : une ou plusieurs capsules vidéo de cadrage, une lecture guidée courte, une activité sur dossier documentaire, puis un questionnaire ciblé. Les médias mobilisés sont des capsules vidéo sous-titrées et accompagnées d'une transcription téléchargeable, des ressources académiques rédigées pour la formation, des dossiers documentaires reproduisant des livrables réels, des fiches d'activité, des questionnaires et deux rendez-vous synchrones à distance. Les consignes précisent le niveau cognitif attendu : comprendre, analyser, évaluer, concevoir. Les pauses et les temps de bilan sont annoncés explicitement pour aider l'apprenant à se situer dans le parcours.

OBJECTIFS

Les objectifs décrivent les savoir-agir attendus en fin de parcours. Ils sont adossés aux cinq compétences visées listées plus bas.
À la fin de cette formation, les participants seront en mesure de :

1. Produire un jugement analytique orienté décision

> Le fait, l'interprétation et le jugement sont séparés explicitement. L'apprenant sait dire ce qui est établi, ce qui est plausible, ce qui manque et ce que la décision doit trancher.

2. Modéliser un adversaire comme une organisation contrainte

> Ressources, chaîne logistique, tolérance au risque et frictions deviennent des variables d'analyse, ce qui évite de le surestimer le potentiel réel de l'attaquant.

3. Construire et départager des scénarios concurrents

> Plusieurs hypothèses plausibles sont formulées, les lacunes de connaissance sont explicitées, et des indicateurs discriminants orientent une collecte ciblée.

4. Évaluer la robustesse d'une analyse sous tromperie

> Manipulabilité des sources, chaîne de transformation des indices et indépendance des corroborations sont qualifiées explicitement.

5. Concevoir, piloter et capitaliser une opération de défense active

> Objectif, signaux, instrumentation, critères d'arrêt et retour d'expérience sont alignés avant toute action d'engagement.

PROGRAMME / DEROULÉ

Le parcours se déroule sur dix semaines, à raison de trois heures par semaine. Chaque semaine, les trois heures sont découpées en micro-séquences de dix à vingt minutes de contenus vidéos, avec environ quarante-cinq à soixante minutes de contenus guidés et une heure trente à deux heures d'activités appliquées et d'auto-évaluation. Les deux situations authentiques d'évaluation et les deux rendez-vous synchrones sont pris dans ce budget hebdomadaire.

1. **Posture proactive et spectre analytique (3h)**
   - Distinguer faits, interprétations et jugements, et repérer la question de décision qui se cache derrière un produit d'analyse.
   - Reformuler une demande floue en besoin en renseignement exploitable, puis rédiger un jugement court qui dit ce qui est établi, ce qui est plausible, ce qui manque et ce que la décision doit trancher.
2. **Cybercriminologie opérationnelle (3h)**
   - Lire l'adversaire comme une organisation contrainte : chaîne logistique, ressources, tolérance au risque, frictions, dépendances.
   - Lire une intrusion comme une trajectoire d'objectifs et de contraintes, et non comme une simple chronologie de techniques et d'indicateurs.
3. **Scénarios d'intrusion et collecte ciblée (3h)**
   - Construire des scénarios concurrents d'évolution d'une situation et expliciter les lacunes de connaissance situationnelle.

- Concevoir des indicateurs discriminants qui départagent ces scénarios afin d'orienter la collecte et la supervision.

4. Analyser sous désinformation (3h)

- Traiter la tromperie comme une hypothèse concurrente, et évaluer la manipulabilité des sources et des capteurs.
- Documenter les pratiques de tromperies de l'adversaire, ses opportunités et ses moyens de tromperie, puis produire une sortie opérationnelle fiable malgré cette possibilité.

5. Prouver sous désinformation, puis situation authentique d'évaluation n°1 (3h)

- Qualifier chaque élément (fait, indice, jugement), tracer sa source, sa chaîne de transformation, son indépendance et la confiance qu'on lui accorde.
- Sortir d'une culture de convergence des sources pour une validation indépendante et traçable de la chaîne de jugement.
- Situation authentique d'évaluation n°1, qui clôt le premier arc du parcours et intègre les séquences 1 à 5.

6. Penser la planification adverse (3h)

- Appliquer à l'adversaire les notions de sujet, question et besoin prioritaire en renseignement, dans une approche du dehors vers le dedans (« outside-in »).
- Dériver les priorités d'information adverses de ses objectifs et de ses contraintes, pour identifier ses comportements de collecte probables et les moments où il est obligé de prendre des informations.

7. Préparer une opération de défense active (3h)

- Structurer l'environnement de confrontation, définir l'objectif et les effets visés, choisir les signaux à observer et encadrer le risque.
- Formuler une hypothèse d'effet, instrumenter l'environnement pour la mesurer, et fixer des critères d'arrêt et de contrôle.

8. S'informer pour dégrader l'adversaire (3h)

- Concevoir une collecte proactive qui vise la révélation d'une activité adverse, non pour la bloquer techniquement mais pour la dégrader opérationnellement.
- Concevoir des actions à faible coût, proportionnées aux contraintes organisationnelles et juridiques, et pilotées par des indicateurs.

9. Éliciter pour renseigner (3h)

- Provoquer de manière délibérée et mesurable une action révélatrice de l'adversaire, pour exposer une capacité, une méthode, une contrainte ou un objectif.
- Concevoir une opération cohérente : objectif d'élicitation, mise en scène, actions, signaux, critères d'arrêt et gestion des risques, en gardant la maîtrise du tempo de la confrontation.

10. Comprendre et capitaliser, puis situation authentique d'évaluation n°2 (3h)

- Formaliser un retour d'expérience structuré : ce qui a été tenté, observé, confirmé ou infirmé, et ce qui doit changer dans les manuels analytiques et opérationnels.
- Transformer l'opération en doctrine réutilisable, gouvernable et mesurable, ce qui prépare un nouveau cycle d'engagement de l'adversaire.
- Situation authentique d'évaluation n°2, qui clôt l'arc final et valide la promesse du parcours : passer de l'analyse à l'action, puis de l'action à l'amélioration continue.

COMPÉTENCES VISÉES

Compétence 1 : maîtriser le spectre analytique, en transformant des descriptions de traces techniques et de rapports en éléments orientés vers l'estimation, l'anticipation et le soutien à la décision.

Compétence 2 : modéliser un écosystème adverse contraint, en représentant l'adversaire comme une organisation humaine dotée de ressources limitées, de contraintes, d'une tolérance au risque et de faiblesses exploitables.

Compétence 3 : orienter et qualifier le renseignement, en formulant des besoins alignés sur des décisions à prendre, en choisissant des sources adaptées et en évaluant leur qualité.

Compétence 4 : anticiper de manière structurée, en identifiant, comparant et réfutant des hypothèses, en explicitant les lacunes de connaissance et en produisant des indicateurs et des scénarios.

Compétence 5 : concevoir et capitaliser une reprise d'initiative, en pilotant des opérations de défense active et en transformant l'action en doctrine réutilisable

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-certification. Il s'agit des dix questionnaires de fin de séquence, des deux situations authentiques d'évaluation, et des deux rendez-vous synchrones ou de leur rediffusion. Le détail est rappelé 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 dix questionnaires à choix multiples de fin de séquence ;
- La situation authentique d'évaluation n°1, à l'issue de la séquence 5 ;
- La situation authentique d'évaluation n°2, à l'issue de la séquence 10.

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.

La note finale est calculée ainsi : les dix questionnaires comptent pour 20 %, soit 2 % par séquence ; la situation authentique d'évaluation n°1 compte pour 30 % ; la situation authentique

d'évaluation n°2 compte pour 50 %. Pour passer à la séquence suivante, il faut atteindre 80 % au questionnaire de la séquence en cours. La micro-certification est délivrée si les dix questionnaires sont validés, si chacune des deux situations authentiques d'évaluation atteint au moins 75 %, et si la note finale atteint 80 %.

La situation authentique d'évaluation n°1 clôt le premier arc du parcours. À partir d'un dossier documentaire comportant un état de l'art d'une investigation, des faits nouveaux et des éléments de contexte, l'apprenant produit une analyse de situation, formule des hypothèses concurrentes, évalue les preuves avec une démarche structurée et recommande une posture opérationnelle qui intègre l'incertitude résiduelle.

La situation authentique d'évaluation n°2 clôt l'arc final. À partir d'un contexte de menace et d'un dossier de situation incluant contraintes organisationnelles et juridiques, capacités de capteurs et objectifs de renseignement, l'apprenant conçoit une opération de défense active en plusieurs temps, définit son pilotage par signaux et ses critères d'arrêt, puis produit un retour d'expérience et une doctrine de capitalisation réutilisable.

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 DONNÉES PERSONNELLES

Cette formation ne mobilise aucune plateforme de travaux pratiques. Aucune donnée personnelle n'est donc collectée à ce titre. Les seules données traitées sont celles de la plateforme FUN, qui héberge l'espace de formation, et celles nécessaires à l'inscription auprès de l'Université de Rennes : nom, prénom, adresse électronique, identifiant et journaux de connexion, dates de début et de fin, et cours suivis.