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 DES FLUX RÉSEAUX

« Apprenez à analyser le trafic réseau pour détecter les anomalies et les menaces : une formation opérationnelle pour renforcer vos compétences en supervision et en réponse à incident. »

*Bienvenue dans la formation "Analyser des flux réseaux".*

*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 des flux réseaux

**Prix : 1 210 €**

**Dates :** du 30 novembre 2026 au 24 janvier 2027

**Durée en semaine :** 6

**Effort (h) :** 22 heures

**Rythme recommandé par semaine :** 4 heures

**Permanences virtuelles :** 3 heures - 1 heure toutes les 2 semaines

**Langues :** Français

## PRÉREQUIS

**Prérequis de connaissances / compétences :**

- Connaissances fondamentales en systèmes d'exploitation (Windows/Linux) ;
- Connaissances de base en architecture réseau (protocoles, topologies) ;
- Familiarité avec les principes de sécurité des systèmes d'information ;
- Être familiarisé avec les environnements de virtualisation (VMware, VirtualBox).

## ÉQUIPEMENT REQUIS

Un ordinateur munis d'une connexion internet.
Idéalement, l'apprenant disposera des droits admins sur sa machine, des outils devront en effet être téléchargés et manipulés.

## 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

Jonathan GARRY

Jonathan est ingénieur consultant, ancien élève de Télécom Sud Paris.

## ÉTABLISSEMENT

## DESCRIPTION

Cette formation permet d'acquérir une méthode structurée d'analyse des flux réseaux afin d'identifier des comportements anormaux, des indicateurs de compromission et des scénarios d'attaque. Elle aborde les principaux protocoles réseaux, les techniques de capture et d'inspection du trafic, ainsi que l'exploitation d'outils tels que tcpdump, Wireshark, Zeek et Suricata.

Résolument orientée vers la pratique, elle alterne des apports théoriques ciblés, des démonstrations outillées, des études de cas et des travaux pratiques progressifs à partir de captures réseaux réelles ou simulées. Les apprenants sont ainsi amenés à analyser des traces de trafic, détecter des activités suspectes — scan, beaconing, commande et contrôle ou exfiltration de données — puis à reconstituer une chronologie d'incident et à produire un rapport d'analyse exploitable.

Le parcours est proposé à distance, en autonomie, et s'appuie sur des capsules vidéo, des supports de cours, des fiches pratiques, des ressources interactives, des quiz d'auto-évaluation et des travaux pratiques. Cette approche par compétences favorise une mise en application directe dans des contextes de supervision de sécurité, de SOC, de CERT ou de réponse à incident.

## OBJECTIFS

**L'objectif pédagogique est clair : permettre aux participants de lire, interpréter et corréler les flux réseaux pour identifier rapidement les signaux faibles, les anomalies et les indicateurs de compromission.** L'approche par cas concrets issus de contextes variés (exfiltration de données, commande & contrôle, lateral movement, etc.) offre une immersion progressive dans des scénarios réalistes, tout en renforçant les réflexes d'analyse critique.

À la fin de cette formation, les participants seront en mesure de :

### 1. Comprendre et interpréter les flux réseaux

> Identifier les principaux protocoles, leurs rôles et leurs interactions afin de caractériser le fonctionnement normal d'un environnement réseau.

### 2. Réaliser des captures de trafic réseau

> Mettre en œuvre les techniques de collecte et d'inspection du trafic, notamment au moyen de mécanismes de capture adaptés et de fichiers de traces réseaux.

### 3. Utiliser les principaux outils d'analyse réseau

> Prendre en main tcpdump, Wireshark et Zeek pour capturer, filtrer, visualiser et exploiter les données issues des flux réseaux.

### 4. Identifier les anomalies et comportements suspects

> Repérer les schémas de communication anormaux ou malveillants, tels que les scans, le beaconing, les communications de commande et contrôle ou les tentatives d'exfiltration de données.

### 5. Identifier et exploiter des indicateurs de compromission

> Extraire, qualifier et enrichir les indicateurs techniques présents dans les flux et les journaux réseaux afin d'étayer une analyse de sécurité.

### 6. Mener une investigation à partir de traces réseaux

> Reconstituer la chronologie d'un incident, identifier les systèmes concernés et formuler des hypothèses fondées sur les éléments de preuve collectés.

### 7. Corréler les données réseaux avec d'autres sources

> Mettre en relation les flux et journaux réseaux avec des alertes issues d'outils de détection, d'un SIEM, de sources de renseignement sur les menaces ou de données issues des postes de travail.

### 8. Restituer une analyse exploitable

> Produire un rapport d'analyse réseau structuré, présentant le contexte, les constats, les indicateurs identifiés, la chronologie de l'incident et les recommandations associées.

## PROGRAMME / DEROULÉ

1. **Introduction aux flux réseaux (2h)**
   - Revue des fondamentaux du réseau et de ses composants pour la surveillance.
2. **Outils d'analyse réseau (4h)**
   - Prise en main de tcpdump, Wireshark, Zeek, et compréhension de leur usage dans l'analyse.
3. **Détection d'anomalies réseaux (4h)**
   - Identification et interprétation des comportements anormaux (scan, C2, beaconing…).
4. **Investigation post-incident (5h)**
   - Reconstitution des scénarios d'attaque à partir des flux réseaux capturés.

5. **Forensique réseau et corrélation (4h)**
    - Intégration de l'analyse réseau dans un processus forensique global, en lien avec les logs et systèmes.
6. **Évaluation et synthèse (3h)**
    - Mise en œuvre de l'ensemble des compétences acquises.

## COMPÉTENCES VISÉES

**Compétence 1 :** Définir et caractériser les aspects d'un environnement opérationnel.

**Compétence 2 :** Reconnaître les changements significatifs dans les schémas de communication.

**Compétence 3 :** Réaliser une analyse du système cible.

**Compétence 4 :** Déterminer l'effet des configurations routeur/pare-feu sur le trafic.

## 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 **3 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 quiz intermédiaires ;
- Le quiz final de chaque module.

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

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.