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 JOURNAUX

« Apprenez à analyser les journaux systèmes, applicatifs et de sécurité afin de détecter les anomalies, d'investiguer les incidents et de renforcer vos capacités de réponse face aux cybermenaces. »

Bienvenue dans la formation « Analyser des journaux »

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 journaux

Prix : 2000€

Date : du 30 novembre 2026 au 17 janvier 2027

Durée en semaine : 5

Effort (h) : 20 heures.

Rythme recommandé par semaine : 4h par semaine

Permanences virtuelles : 2 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 journaux systèmes, applicatifs, réseau et de sécurité afin de détecter, qualifier et investiguer les événements susceptibles de révéler une compromission. Elle aborde les principales sources et formats de logs, les mécanismes de collecte, de centralisation et de normalisation, ainsi que les techniques de recherche, de filtrage et de corrélation nécessaires à l'analyse d'incidents.

Résolument orientée vers la pratique, elle alterne des apports théoriques ciblés, des démonstrations outillées, des études de cas et des travaux pratiques progressifs réalisés à partir de jeux de données réalistes ou simulés. Les apprenants manipulent notamment des journaux Linux et Windows, des traces issues d'équipements réseau et de solutions de sécurité, afin d'identifier des activités anormales, des indicateurs de compromission et des séquences d'événements significatives.

Le parcours propose également une initiation à l'exploitation d'outils et de méthodes dédiés à l'analyse des logs, tels que les SIEM, les expressions régulières, les règles Sigma et l'automatisation par scripts. Il s'appuie sur des capsules vidéo, des démonstrations, des fiches pratiques, des ressources de référence, des quiz, des exercices guidés et une paillasse numérique. Cette approche par compétences permet aux participants de développer des réflexes directement mobilisables dans des contextes de supervision de sécurité, d'investigation numérique et de réponse à incident.

OBJECTIFS

Cette formation vise à développer les compétences nécessaires pour collecter, interpréter et exploiter les journaux issus des systèmes, applications, équipements réseau et solutions de sécurité. Elle permet aux participants de transformer des données techniques brutes en éléments d'analyse utiles à la détection des menaces, à l'investigation des incidents et à la réponse opérationnelle. À l'issue du parcours, les apprenants disposent d'une méthode structurée pour rechercher, qualifier, corréler et restituer les événements de sécurité.

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

1. Identifier les sources de journaux pertinentes

> Distinguer les journaux issus des systèmes, applications, équipements réseau et solutions de sécurité, et apprécier leur intérêt pour la supervision et l'investigation.

2. Comprendre la structure et le contenu des logs

> Lire et interpréter les principaux formats de journaux, notamment Syslog, Windows Event Log et les formats produits par les outils de sécurité.

3. Collecter, centraliser et normaliser les journaux

> Mettre en œuvre les principes de collecte, de stockage et de normalisation des logs afin de faciliter leur exploitation et leur corrélation.

4. Rechercher et filtrer des informations dans les logs

> Utiliser des requêtes, des filtres et des expressions régulières pour extraire des événements, des attributs ou des indicateurs pertinents au sein de jeux de données volumineux.

5. Analyser les journaux systèmes et de sécurité

> Identifier et interpréter les événements significatifs issus notamment des environnements Linux et Windows, des équipements réseau et des solutions de protection.

6. Détecter les anomalies et les indicateurs de compromission

> Repérer des comportements suspects, des événements critiques et des schémas d'attaque à partir des traces disponibles.

7. Corréler des événements issus de sources multiples

> Mettre en relation différentes sources de journaux afin de contextualiser une alerte, de confirmer une hypothèse et de reconstituer une séquence d'événements.

8. Exploiter un SIEM dans une démarche d'analyse

> Utiliser les fonctions essentielles d'un SIEM pour interroger des données, construire des recherches ou des règles simples de détection, et analyser des alertes.

9. Automatiser certaines tâches d'analyse

> Mobiliser des scripts ou des mécanismes d'automatisation simples pour faciliter la collecte, le filtrage, l'extraction ou l'analyse initiale des journaux.

10. Réaliser une investigation et restituer les résultats

> Analyser un cas d'incident à partir de journaux multiples, formuler des conclusions étayées et produire un rapport structuré incluant les constats, les indicateurs relevés et les recommandations.

PROGRAMME / DEROULÉ

1. Introduction à l'analyse des journaux (2h)

- Compréhension du rôle des journaux dans un système d'information.
- Identification des différentes sources de logs (systèmes, réseaux, applications, sécurité).
- Capacité à situer l'analyse des journaux dans la détection et la réponse à incident.

2. Format, normalisation et stockage des logs (2h)

- Capacité à reconnaître des formats de logs courants (Syslog, Windows Event, etc.).
- Compréhension des mécanismes de centralisation et de stockage.
- Application des principes de normalisation pour faciliter la corrélation.

3. Analyse des journaux systèmes (Linux, Windows) (3h)

- Capacité à localiser, lire et interpréter les fichiers de logs natifs sous Linux et Windows.
- Identification des événements critiques liés à la sécurité.
- Extraction des données d'intérêt dans les logs bruts.

4. Détection d'anomalies et événements critiques (3h)

- Définition des comportements anormaux à partir des logs.
- Identification des signes de compromission ou d'activité suspecte.
- Utilisation des indicateurs pour générer des alertes.

5. Corrélation multi-source avec un SIEM (4h)

- Compréhension du fonctionnement d'un SIEM (indexation, corrélation, alerting).
- Construction des requêtes de corrélation simples.
- Analyse d'un incident à partir de plusieurs sources de logs via un SIEM (ELK, Splunk, etc.).

6. Automatiser l'analyse des logs (3h)

- Conception ou utilisation des scripts pour extraire et analyser des logs (ex. : Python, bash).
- Découverte de l'apport des SOAR pour le traitement automatisé des événements.
- Mise en œuvre des chaînes d'analyse automatique simples.

7. Étude de cas – Investigation post-incident (3h)

- Mise en œuvre de l'ensemble des compétences acquises.

COMPÉTENCES VISÉES

Compétence 1 : Analyse des journaux.

Compétence 2 : Analyse des données/informations.

Compétence 3 : Détection des intrusions.

Compétence 4 : Analyse des menaces.

Compétence 5 : Corrélation des données de menace.

Compétence 6 : Interprétation des données.

Compétence 7 : Rédaction et présentation de rapports de renseignement.

Compétence 8 : Production de rapports d'analyse.

Compétence 9 : Analyse réseau.

Compétence 10 : Surveillance et identification des événements.

Compétence 11 : Analyse des métadonnées.

Compétence 12 : Recherche et analyse de signatures malveillantes.

Compétence 13 : Utilisation d'outils d'analyse de sécurité.

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 **2 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 ;
- Les devoirs et les TP réalisés
- Une étude cas - Investigations post-incident.

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.