



MFE-IT
Mes Formations d'Expertise

Référence : en-2ctd

Formation Claroty CTD – Surveillance Active et Détection de Menaces pour Systèmes Industriels

Durée : **5 jours** | Volume horaire : **35 h**

Distanciel · Sessions garanties dès 1 inscrit · 60 % de pratique

DESCRIPTION

La formation Claroty CTD vous apprend à détecter les menaces, analyser les comportements anormaux et intervenir rapidement au sein d'un environnement industriel. Grâce à cette approche pratique, vous maîtrisez la plateforme Claroty pour renforcer la sécurité de vos infrastructures OT et ICS sans compromettre leur disponibilité.

Les environnements OT (Operational Technology) deviennent des cibles privilégiées pour les cyberattaques. Les systèmes industriels, souvent isolés ou mal protégés, nécessitent une surveillance continue, capable d'identifier les anomalies et de limiter les intrusions.

Claroty Continuous Threat Detection (CTD) répond à ces enjeux. La solution permet de cartographier les actifs industriels, de surveiller le trafic réseau en temps réel et de détecter les comportements suspects. Vous bénéficiez ainsi d'une visibilité complète sur votre environnement OT, tout en renforçant la posture de sécurité globale de votre organisation.

OBJECTIFS PÉDAGOGIQUES

À l'issue de la formation, le participant sera capable de :

- Comprendre les enjeux de cybersécurité propres aux environnements industriels OT.
- Prendre en main l'interface Claroty CTD et ses fonctionnalités clés.
- Cartographier et inventorier automatiquement les actifs connectés.
- Détecter les menaces, comportements anormaux ou intrusions réseau.
- Comprendre les alertes générées et affiner les règles de détection.
- Intégrer CTD dans une démarche SOC, SIEM ou stratégie de défense en profondeur.

PRÉREQUIS

- Connaissance de base des architectures industrielles OT (SCADA, PLC, DCS).
- Notions de sécurité réseau : firewalls, VLAN, protocoles industriels.
- Expérience avec un outil de supervision ou SIEM appréciée.

Parce que chaque participant est unique, un entretien personnalisé en amont avec notre expert nous permet de concevoir une formation parfaitement alignée avec ses objectifs, son niveau et ses enjeux professionnels.

PUBLIC VISÉ

- Ingénieurs OT et automaticiens.
- Responsables sécurité et RSSI industriels.
- Équipes SOC en charge de la supervision de périmètres industriels.
- Toute personne impliquée dans la cybersécurité des systèmes SCADA, PLC ou DCS.

PROGRAMME DÉTAILLÉ

La formation alterne apports théoriques et travaux pratiques (environ 60 % du temps). Les modules sont construits autour d'exercices concrets reprenant les cas d'usage du métier visé.

Enjeux de cybersécurité dans les environnements OT

- Spécificités des menaces industrielles.
- Surfaces d'attaque OT et ICS.
- Retour d'expérience sur des incidents critiques.
- Cadre réglementaire : NIS2, LPM, IEC 62443.

Introduction à Claroty CTD

- Architecture de la solution Claroty.
- Positionnement sur le réseau industriel.
- Composants principaux : Sensors, Central, EMC.
- Tableau de bord et premiers indicateurs clés.

Découverte et cartographie des actifs

- Détection passive et non intrusive.
- Inventaire automatique des équipements OT.
- Classification des équipements par type et criticité.
- Protocoles industriels supportés (Modbus, Profinet, DNP3, S7).

Détection des menaces et alertes

- Analyse comportementale des flux réseau.
- Alertes par profil ou par signature.
- Scénarios types : changements non autorisés, scan réseau, trafic anormal.
- Classification des alertes et priorisation.

Réaction, investigation et intégration SIEM

- Traitement des incidents de bout en bout.
- Journalisation et exportation des logs.
- Corrélation avec un SOC et un SIEM existant.
- Construction de dashboards personnalisés.

Bonnes pratiques et retour d'expérience

- Cas d'usage concrets en industrie manufacturière et énergie.
- Indicateurs de performance sécurité OT.
- Préparation à une inspection ou un audit cyber-industriel.
- Intégration dans une démarche de défense en profondeur.

MODALITÉS PÉDAGOGIQUES

Format et déroulement

La formation se déroule en distanciel via une classe virtuelle interactive. Elle peut également être réalisée sur le site du client, avec une personnalisation du contenu en fonction des enjeux du projet professionnel. La répartition théorie / pratique est d'environ 40 % / 60 %. Le programme s'articule autour d'apports théoriques, de démonstrations, de travaux pratiques sur application fil rouge et de phases d'échanges entre participants et formateur.

Format ultra-personnalisé MFE-IT

Chaque session regroupe entre 1 et 3 participants, afin de garantir un suivi individuel très poussé. Un entretien en amont permet d'ajuster le contenu au profil de chacun : niveau, objectifs, contexte professionnel, enjeux.

Les sessions inter-entreprises sont garanties dès 1 seul inscrit (sauf cas de force majeure).

Moyens techniques

La formation est accessible depuis n'importe quel poste disposant d'une connexion Internet haut débit. Avant le démarrage, notre équipe logistique prend contact avec chaque participant pour valider l'environnement technique et présenter la plateforme.

Pendant toute la formation, le stagiaire bénéficie d'une assistance technique et pédagogique par e-mail, avec un délai de traitement qui n'excède pas 24 heures ouvrées.

Évaluation des acquis

Tout au long de la formation, le formateur évalue la progression des participants au travers de QCM, de mises en situation et de travaux pratiques. Le faible effectif par session rend possible une validation individuelle à la fin de chaque atelier.

À l'issue de la formation, une attestation de validation des acquis est remise à chaque participant, mentionnant les objectifs, la nature, la durée de l'action et les résultats de l'évaluation.

Accessibilité et handicap

MFE-IT est attentif à l'accueil des personnes en situation de handicap. Pour toute demande d'aménagement, un échange avec notre référent handicap permet d'identifier les besoins spécifiques et d'adapter le dispositif de formation. Contact : contact@mfe-it.com.

Assistance post-formation

Pendant le mois qui suit la formation, chaque stagiaire peut solliciter l'aide des formateurs MFE-IT sur des questions de mise en œuvre des connaissances acquises. Une réponse est apportée par e-mail ou par téléphone sous 48 heures ouvrées.

INFORMATIONS PRATIQUES

Prise en compte du handicap

MFE-IT accorde une attention particulière à l'inclusion des personnes en situation de handicap. Afin que la formation se déroule dans les meilleures conditions, nous invitons les participants concernés à nous contacter en amont, par e-mail (contact@mfe-it.com) ou via le formulaire de notre site. Un échange avec notre référente handicap permettra d'identifier ensemble les besoins spécifiques et les aménagements utiles à la réussite du parcours.

Modalités pédagogiques et techniques

Le dispositif pédagogique combine apports théoriques, démonstrations guidées, travaux pratiques sur application fil rouge et temps d'échange entre participants et formateur, selon une répartition voisine de 40 % de théorie et 60 % de pratique.

La formation est accessible à distance depuis n'importe quel lieu disposant d'une connexion Internet haut débit. En amont de la session, nos équipes prennent contact avec chaque stagiaire afin de réaliser une vérification technique et de présenter l'environnement de travail.

Durant toute la durée de l'action, le stagiaire bénéficie d'une assistance technique et pédagogique par e-mail, avec un délai de prise en charge inférieur à 24 heures ouvrées. Un rendez-vous pédagogique individuel avec un formateur peut également être programmé pour approfondir un point précis.

La durée indiquée dans le programme constitue une estimation qui peut évoluer en fonction du profil du participant et de ses attentes, notamment lorsqu'un passage de certification est envisagé.

Moyens mis en œuvre par le formateur

- Des démonstrations structurées en modules et séquences pédagogiques fines, alignées sur le programme détaillé
- Des énoncés et corrigés de travaux pratiques, à réaliser tout au long de la formation
- Un environnement technique prêt à l'emploi pour la réalisation des ateliers pratiques
- Une validation par le formateur des connaissances acquises à l'issue de chaque atelier
- Un ou plusieurs supports numériques faisant office de documents de référence

Validation et sanction de la formation

À l'issue de la formation, une attestation est adressée par e-mail au stagiaire. Elle précise les objectifs, la nature, la durée de l'action ainsi que les résultats de l'évaluation des acquis. Un certificat de réalisation peut également être fourni sur demande.

Type de formation

Action de formation professionnalisante, visant le perfectionnement et l'élargissement des compétences des participants.

Suivi de l'exécution de l'action

L'assiduité des participants est vérifiée par la signature d'une feuille de présence par demi-journée, cosignée par le formateur.

Modalités d'évaluation des acquis

Les participants mettent en pratique les éléments du cours au travers de travaux pratiques réalisés sur poste individuel. La validation des acquis est effectuée par le formateur à l'issue de chaque atelier. Le très faible effectif par session rend possible un suivi individualisé (1 à 3 participants).

À l'issue de la formation, le stagiaire a atteint les objectifs pédagogiques fixés par le programme.

Aide à l'orientation

Pour chaque grande thématique de notre catalogue, nos experts proposent un entretien téléphonique ou en visio afin d'aider les personnes qui le souhaitent à choisir le programme ou le parcours de formation le mieux adapté à leur profil et à leurs objectifs.

Aspects pratiques

Dès l'inscription, nos équipes prennent contact avec les participants pour vérifier la qualité du lien Internet disponible sur le lieu où ils souhaitent se former, ainsi que l'adéquation du matériel (PC portable, webcam, micro-casque).

Avant le démarrage, les participants reçoivent un lien d'accès à la classe virtuelle accompagné de leurs identifiants personnels. Une aide à la prise en main de la solution de visioconférence est également mise à disposition.

Le jour de la formation, les participants rejoignent la salle virtuelle depuis leur navigateur. Ils voient et entendent le formateur ainsi que les autres stagiaires, et peuvent échanger à tout moment. Les ateliers se déroulent dans des conditions proches d'une salle physique, avec possibilité pour le formateur de prendre la main à distance pour accompagner ou vérifier un TP.

Bénéfices pour les participants

- Se former depuis son lieu de travail ou son domicile, sans déplacement
- Bénéficier d'un formateur consultant expert du sujet animé
- Profiter d'un format ultra-personnalisé (1 à 3 participants) favorisant les échanges et la pratique
- Continuer à se former même en cas d'imprévus professionnels ou personnels

Bénéfices pour l'entreprise

- Optimiser le budget formation en limitant les frais de déplacement et d'hébergement
- Offrir des formations de qualité à l'ensemble des collaborateurs, quelle que soit leur localisation
- Réduire les temps d'absence liés aux trajets
- Élargir le choix des formations proposées aux collaborateurs peu mobiles
- Soutenir la montée en compétences des équipes dans tous les contextes