l'Incubateur de
l'InterCERT France

Accélérateur de Maturité des CERTs émergents

InterCERT
FRANCE

Promotion

# Cédric Blancher

Octobre 2024

# Hommage à Cédric Blancher

Le monde de la cybersécurité est encore jeune et avant même qu'il ne s'appelle ainsi – quand il n'était encore question que de sécurité des systèmes d'information – certaines personnalités ont su l'animer et promouvoir à leur façon leur souhait de partager des informations, d'animer les échanges, de coopérer et finalement de contribuer à bâtir un monde plus sûr.

Cédric 'Sid' Blancher était sans aucun doute de ceux-là. Avec son blog « Ma petite parcelle d'Internet » il a publié sans relâche ses avis – souvent tranchés, mais toujours étayés – où son œil d'expert nourrissait la réflexion de ses lecteurs dont j'avais la chance de faire partie. Ses interventions dans de nombreuses conférences de renom étaient toujours un moment attendu : on était sûr d'y apprendre quelque chose d'utile, son appétit de transmettre était perceptible, autant que la malice qui trahissait sa passion pour les sujets de sécurité.

Il a montré l'importance de mettre son savoir au service d'une cause et la nécessité de le partager pour la faire avancer. Sa disparation brutale en novembre 2013 a laissé une communauté orpheline de l'un de ses leaders naturels.

J'ai proposé que cette communauté qui a grandit rende hommage à l'un de ses précurseurs et, avec l'accord ses proches, que ce premier incubateur de l'InterCERT France porte son nom. Nous perpétuerons la mémoire de Cédric et les valeurs qu'il incarnait.

**Frédéric Le Bastard**
Président

# L'Incubateur de l'InterCERT France : Accélérateur de Maturité pour les CERTs Émergents

**L'Incubateur de l'InterCERT France, un programme exclusif conçu pour les CERTs émergents cherchant à renforcer leur maturité opérationnelle et leur expertise en cybersécurité.**

Cette initiative, ouverte à dix membres de CERTs qui seront sélectionnés après analyse de leur dossier de candidature, offre une opportunité unique d'acquérir des compétences spécialisées tout en favorisant le partage de connaissances au sein d'une communauté dynamique.

## PARTICIPATION FINANCIÈRE :

Pour garantir le sérieux des engagements et assurer la qualité des ressources mises à disposition, une participation financière de 500 euros sera demandée à chaque participant d'une équipe de CERT souhaitant rejoindre l'incubateur.

Ces fonds contribueront à couvrir les coûts logistiques et pédagogiques du programme, garantissant ainsi une expérience enrichissante et personnalisée pour chaque participant.

## OBJECTIF DU PROGRAMME :

L'incubateur se donne pour mission d'offrir un accompagnement structuré, comprenant une quarantaine de modules spécialisés couvrant des sujets tels que :

- la gestion de crise, la communication de crise,
- les opérations de cyberdéfense,
- la production de connaissance de la menace, et bien d'autres.

Chaque module est soigneusement élaboré pour répondre aux besoins spécifiques des CERTs et favoriser leur développement continu.

## FORMATION DISPENSÉE PAR DES EXPERTS DE L'INTERCERT FRANCE :

L'une des spécificités de notre incubateur réside dans le fait que l'ensemble des modules de formation sont dispensés par les membres expérimentés de l'InterCERT France. Ces experts partageront leur savoir-faire, leurs retours d'expérience et leur expertise directement avec les participants, offrant ainsi une formation à la fois pragmatique et orientée vers les réalités opérationnelles.

CERTs participants à ce programme. :

- Olivier Caleff Membre Liaison de l'InterCERT-France
- CERT - Stoïk
- CERT - La Poste
- CERT - FR
- CSIRT - SUEZ
- CERT - IST
- CSIRT - PJ
- CERT - Societe Générale
- CERT - Thales
- CERT - OCD
- CERT - Sekoia
- CERT - Michelin
- CERT - Engie
- OWN - CERT
- CSIRT - OVH
- CERT - Santé

## POUR QUI :

Cet incubateur est exclusivement réservé aux CERTs déjà établis ou en cours de constitution, en quête d'amélioration continue. Les dix équipes sélectionnées auront l'opportunité d'approfondir leurs compétences, de partager des bonnes pratiques, et de bénéficier d'une collaboration unique au sein de la communauté de l'InterCERT France.

## MODALITÉS DE PARTICIPATION :

Inscription : Les équipes intéressées sont invitées à postuler en fournissant les informations nécessaires sur leur CERT et en exposant leurs motivations à rejoindre l'incubateur.

Sélection : Une commission évaluera les candidatures et sélectionnera les dix membres d'équipe CERTs les plus adaptés au programme.

Participation Financière : Les équipes retenues devront s'acquitter d'une participation financière de 500 euros, symbolisant leur engagement envers le programme.

Démarrage du Programme : Une fois les équipes sélectionnées et les participations reçues, le programme débutera avec une réunion de lancement.

**Si votre CERT est prêt à investir dans son excellence opérationnelle, à partager son savoir-faire, et à bénéficier d'une expérience d'incubation unique, rejoignez l'Incubateur de l'InterCERT France. Ensemble, façonnons l'avenir de la cybersécurité.**

# TABLE DES MATIÈRES

# Les Modules

MODULE 01

# Le CERT dans son organisation

Au cœur de notre incubateur, le module «Le CERT dans son organisation» offre une plongée approfondie dans la structure et le fonctionnement des CERTs. Dispensé par Oliver Caleff Membre Liaison de l'InterCERT France, ce module vise à doter les équipes participantes des connaissances essentielles pour optimiser leur organisation interne.

*Olivier Caleff, Membre de Liaison InterCERT France*

## CONTENU DU MODULE :

**Structure et rôles**

Comprendre les composantes clés d'un CERT, depuis la définition des rôles spécifiques jusqu'à la création de structures efficaces favorisant la collaboration et la réactivité.

**Processus opérationnels**

Explorer les processus opérationnels essentiels, de la détection initiale des incidents à la gestion de crise, en passant par la collecte de données forensiques et la communication stratégique.

**Gestion des ressources**

Acquérir des compétences pratiques dans la gestion des ressources humaines, techniques et financières nécessaires au bon fonctionnement d'un CERT.

**Intégration dans l'écosystème**

Intégration dans l'écosystème : Comprendre comment positionner le CERT au sein de l'écosystème de sécurité, en collaboration avec d'autres entités internes et externes.

## OBJECTIF FINAL :

À la fin de ce module, les équipes auront acquis une compréhension approfondie de l'organisation interne d'un CERT, renforçant ainsi leur capacité à anticiper, détecter et répondre de manière efficiente aux incidents de sécurité numérique. Cette formation constitue un jalon crucial dans le parcours vers l'excellence opérationnelle de chaque CERT participant.

MODULE 02

# RFC 2350 - Comprendre les principes fondamentaux du CERT

Le module sur la RFC 2350 est une pierre angulaire de notre programme d'incubation, conçu pour offrir une vision approfondie des principes fondamentaux régissant les CERTs. Ce module, dispensé en deux temps par des experts de l'InterCERT France, vise à équiper les équipes participantes des connaissances clés nécessaires à la mise en œuvre de meilleures pratiques de gestion des incidents.

*Olivier Caleff, Membre de Liaison InterCERT France*

## PARTIE I : INTRODUCTION À LA RFC 2350

### Contexte et fondements

Explorer le contexte historique et les principes fondamentaux de la RFC 2350, fournissant ainsi un cadre de référence essentiel pour comprendre les normes de fonctionnement des CERTs.

### Éléments clés de la RFC 2350

Examiner en détail les éléments clés de la RFC 2350, notamment la mission du CERT, sa portée, ses activités opérationnelles, et les mécanismes de communication.

### Application pratique

Mettre en lumière des exemples concrets d'application de la RFC 2350 dans des scénarios réels, illustrant ainsi son importance dans la gestion proactive des incidents.

## PARTIE II : MISE EN PRATIQUE ET INTÉGRATION

### Implémentation des Principes

Approfondir la compréhension en explorant la manière dont les principes de la RFC 2350 peuvent être intégrés dans la structure opérationnelle quotidienne d'un CERT.

### Études de cas

Analyser des études de cas spécifiques, permettant aux équipes de tirer des enseignements pratiques pour renforcer leur propre préparation et réponse aux incidents.

### Discussion collaborative

Faciliter une discussion interactive entre les équipes participantes pour échanger des idées et des perspectives sur l'application concrète de la RFC 2350 dans leurs environnements respectifs.

## OBJECTIF FINAL :

À la fin de ce module en deux parties, les équipes auront acquis une compréhension approfondie des normes énoncées dans la RFC 2350 et seront mieux préparées à aligner leurs pratiques opérationnelles sur ces standards reconnus au niveau international

MODULE 03

# Coopération et réseaux de CSIRT

Au cœur de notre incubateur, le module «Coopération et Réseaux de CSIRT» offre une plongée approfondie dans l'importance de la coopération entre CSIRT (Computer Security Incident Response Team). Dispensé par des experts de l'InterCERT France, ce module vise à équiper les équipes participantes des compétences clés nécessaires pour collaborer de manière efficace au sein de réseaux de CSIRT.

*Martine Giralt, Vice-présidente de l'InterCERT France*

CERT-IST
INDUSTRIE | SERVICES | TERTIAIRE

## CONTENU DU MODULE :

### Notions fondamentales

Comprendre les principes fondamentaux de la coopération entre CSIRT, en mettant l'accent sur les avantages, les défis et les meilleures pratiques.

### Modèles de coopération

Explorer différents modèles de coopération, des partenariats bilatéraux aux collaborations sectorielles, afin de mieux s'adapter aux besoins spécifiques de chaque CERT.

### Outils de communication

Identifier et mettre en œuvre des outils de communication efficaces pour faciliter l'échange rapide et sécurisé d'informations sensibles entre les CSIRT.

## OBJECTIF FINAL :

À la fin de ce module, les équipes auront développé une compréhension approfondie des mécanismes de coopération au sein des réseaux de CSIRT. Ce module vise à habiliter les CERTs à établir des relations fructueuses, à partager efficacement des informations cruciales et à collaborer de manière proactive dans la protection de l'écosystème numérique.

MODULE 04

# Veille et publication d'alertes

Emerge comme une clé de voûte pour anticiper et réagir efficacement aux menaces émergentes. Guidé par un Coordinateur en Analyse et Renseignement sur les Menaces, THALES, ce module offre une plongée stratégique dans les pratiques avancées de veille et de diffusion proactive d'alertes, essentielles pour maintenir la résilience face aux évolutions constantes de la menace cybernétique.

*Coordinateur en Analyse et Renseignement sur les Menaces* THALES

## CONTENU DU MODULE :

### Stratégies de veille

Comprendre les méthodes avancées de collecte d'informations, allant des sources ouvertes aux darknets, pour anticiper les tendances et les éventuelles attaques.

### Analyse proactive

Développer des compétences d'analyse prédictive afin d'identifier les signaux faibles et de déclencher des alertes avant que les incidents ne prennent de l'ampleur.

### Coordination et communication

Explorer les meilleures pratiques en matière de coordination avec d'autres CERTs, organismes de sécurité et partenaires, et perfectionner les techniques de communication rapide et ciblée.

### Publication d'alertes

Apprendre à structurer et à diffuser des alertes de sécurité de manière claire et efficace, en tenant compte des besoins spécifiques des parties prenantes internes et externes.

## OBJECTIF FINAL :

À la fin de ce module, les participants auront développé une expertise avancée en veille et en publication d'alertes, renforçant ainsi leur capacité à anticiper les menaces et à coordonner des réponses préventives. Ce module vise à outiller les équipes pour jouer un rôle proactif dans la préservation de l'intégrité des systèmes d'information et à contribuer activement à la sécurité numérique globale.

MODULE 05

# Activité de Réponse au sein du CERT-FR

Le CERT-FR est un acteur clef de la sécurité opérationnelle en France. Il s'est construit et organisé au fil des années pour traiter des incidents toujours plus intenses en volume et en criticité. En présentant son activité, Rémi BOUJU, chef de la Division Réponse au sein du CERT-FR, reviendra sur les réflexions qui ont amené à l'organisation actuelle de l'activité de réponse à incident.

*Rémi BOUJU, chef de la Division Réponse, CERT-FR, ANSSI*

## CONTENU DU MODULE :

- Missions et positionnement du CERT-FR : partir du besoin opérationnel pour définir une organisation adaptée
- Chaîne de traitement des incidents : gérer le volume en concentrant la valeur ajoutée sur les sujets prioritaires
- Opérations de cyberdéfense : s'organiser pour traiter les sujets d'ampleur
- Posture opérationnelle : s'adapter à l'intensité opérationnelle du moment

## OBJECTIF FINAL :

À la fin de ce module, vous aurez une bonne compréhension de l'organisation du CERT-FR et des interactions que vous pourriez avoir avec lui lors du traitement d'un incident. Les échanges et réflexions sur les choix organisationnels adoptés par le CERT-FR vous permettront de bénéficier d'un retour d'expérience pour que vous puissiez optimiser votre propre organisation.

MODULE 06

# Mener une évaluation de maturité avec le Référentiel SIM3

Au cœur de notre incubateur, le module «Mener une évaluation de maturité avec le Référentiel SIM3» offre une approche stratégique pour évaluer et améliorer la maturité opérationnelle des CERTs. Guidé par l'expertise d'Olivier Caleff Membre de Liaison de l'InterCERT France, ce module plonge les participants dans l'utilisation du référentiel SIM3, fournissant un cadre structuré pour évaluer les compétences et les capacités des équipes de réponse à incident.

*Olivier Caleff, membre de Liaison InterCERT France*

## CONTENU DU MODULE :

### Compréhension du référentiel SIM3

Examiner les principes fondamentaux du référentiel SIM3, mettant l'accent sur ses catégories et ses critères d'évaluation spécifiques.

### Étapes de l'évaluation de maturité

Décomposer le processus d'évaluation en étapes clés, de la planification à la mise en œuvre, en passant par l'analyse des résultats et la définition d'un plan d'amélioration.

### Identification des facteurs de maturité

Apprendre à identifier les facteurs clés de maturité au sein d'un CERT en se basant sur le référentiel SIM3, couvrant les aspects organisationnels, techniques et opérationnels.

### Élaboration d'un plan d'amélioration

Guider les équipes dans l'élaboration d'un plan d'amélioration basé sur les résultats de l'évaluation, avec des objectifs spécifiques pour renforcer la maturité opérationnelle.

## OBJECTIF FINAL :

À la fin de ce module, les participants auront acquis les compétences nécessaires pour mener une évaluation de maturité avec le référentiel SIM3, permettant une compréhension approfondie des forces et des faiblesses de leur CSIRT. Ce module vise à positionner les équipes sur la voie de l'amélioration continue, en alignant leurs pratiques sur les normes de l'industrie et en renforçant leur efficacité opérationnelle.

MODULE 07

# CERT et Écosystème Interne (DSI/DAF/DPO/COMEX/Constituents/...)

Le module «CERT et Écosystème Interne» se distingue comme un levier essentiel pour la collaboration harmonieuse entre le CERT (Computer Emergency Response Team) et les différents acteurs internes au sein d'une organisation. Sous la conduite Pierre Raufast, Responsable Adjoint du CERT-Michelin & Fellow Cyber du Groupe Michelin, ce module offre aux participants une plongée stratégique dans les dynamiques de coopération entre le CERT et l'écosystème interne, englobant la DSI, la DAF, le DPO, le COMEX, ainsi que les divers constituants de l'organisation.

*Pierre Raufast, Responsable Adjoint du CERT-Michelin & Fellow Cyber du Groupe Michelin*

## CONTENU DU MODULE :

**Alignement stratégique**

Comprendre l'importance de l'alignement stratégique entre le CERT et les différentes entités internes, assurant une cohérence avec les objectifs globaux de l'organisation.

**Collaboration opérationnelle**

Explorer les mécanismes de collaboration opérationnelle entre le CERT et la DSI, la DAF, le DPO, le COMEX, et les autres constituants, en identifiant les synergies pour une réponse aux incidents efficace.

**Communication et sensibilisation**

Développer des compétences en communication et en sensibilisation, permettant au CSIRT de transmettre efficacement des informations cruciales sur la sécurité à l'ensemble de l'écosystème interne.

**Scénarios pratiques**

Mettre en pratique les concepts enseignés à travers des scénarios de simulation, favorisant ainsi une collaboration proactive et une compréhension mutuelle entre le CERT et les différentes entités.

## OBJECTIF FINAL :

À la fin de ce module, les participants auront acquis une vision approfondie de la collaboration entre le CERT et l'écosystème interne. Ce module vise à renforcer la capacité du CERT à s'intégrer harmonieusement dans l'organisation, à collaborer efficacement avec les diverses parties prenantes, et à jouer un rôle clé dans la préservation de la sécurité globale des systèmes d'information.

MODULE 08

# Exercice de crise

Au cœur de notre incubateur, le module «Exercice de crise» se profile comme une étape essentielle, préparant les équipes de CERT à affronter des situations d'urgence à travers des simulations pratiques. Guidés par ce module offre aux participants l'opportunité de mettre en œuvre leurs compétences et stratégies dans un environnement contrôlé, favorisant ainsi l'amélioration continue et la préparation effective face aux incidents de cybersécurité.

*Pierre Raufast, Responsable Adjoint du CERT-Michelin & Fellow Cyber du Groupe Michelin*

## CONTENU DU MODULE :

### Planification d'exercices

Acquérir des compétences pour planifier, concevoir, et exécuter des exercices de crise, adaptés aux scénarios réalistes et aux objectifs spécifiques.

### Simulation d'incidents

Mettre en place des simulations d'incidents variées pour tester la réactivité des équipes, la coordination des opérations, et les procédures de communication.

### Évaluation des performances

Développer des mécanismes d'évaluation des performances lors des exercices, permettant une analyse constructive des points forts et des axes d'amélioration.

### Rapports d'après-exercice

Explorer la création de rapports d'après-exercice détaillés, fournissant des insights cruciaux pour ajuster les processus et les plans de réponse.

## OBJECTIF FINAL :

À la fin de ce module, les participants auront développé une expérience pratique de la gestion de crise à travers des exercices simulés, renforçant ainsi leur aptitude à réagir efficacement lors d'incidents réels. Ce module vise à inculquer une culture de l'amélioration continue et de la préparation proactive au sein des équipes de CERT, contribuant ainsi à la robustesse et à l'efficacité de la réponse aux cybermenaces.

MODULE 09

# Enjeux RH dans un CERT

Dans le cadre de notre incubateur, le module «Enjeux RH dans un CERT» se focalise sur les aspects cruciaux de la gestion des ressources humaines au sein d'un CERT (Computer Security Incident Response Team). Animé par des experts de l'InterCERT France, ce module offre aux participants un éclairage approfondi sur les défis et les meilleures pratiques liés aux ressources humaines au sein d'une équipe dédiée à la réponse aux incidents de sécurité.

*Frédéric Le Bastard, Responsable du Service de Lutte contre la Cybercriminalité, Groupe La Poste*

LA POSTE GROUPE

## CONTENU DU MODULE :

**Recrutement et profil des collaborateurs**

Explorer les compétences essentielles recherchées chez les membres d'un CERT, ainsi que les stratégies de recrutement adaptées pour constituer une équipe performante.

**Développement des compétences**

Comprendre les mécanismes de formation continue et de perfectionnement des compétences au sein d'un CERT, en tenant compte de l'évolution rapide du paysage de la cybersécurité.

**Motivation et rétention**

Analyser les facteurs de motivation et de rétention spécifiques aux équipes de sécurité informatique, et élaborer des stratégies visant à fidéliser les talents clés.

**Gestion de crise RH**

Se pencher sur les enjeux spécifiques liés à la gestion des ressources humaines lors de situations de crise, en mettant l'accent sur la résilience et la solidarité au sein de l'équipe.

## OBJECTIF FINAL :

À l'issue de ce module, les participants auront acquis une compréhension approfondie des enjeux liés aux ressources humaines dans un CERT. Ils seront mieux préparés à relever les défis de recrutement, de formation et de gestion des équipes, contribuant ainsi à renforcer la capacité du CERT à faire face aux incidents de sécurité de manière efficace et efficiente.

MODULE 10

# La notion de RPS - Définir ce que sont les risques psychosociaux, les formes et les impacts.

*Sébastien Mériot - Head of CSIRT, OVH*

*Olivier Cros - Analyste inforensique - Réponse sur incidents, CERT-Santé*

## CONTENU DU MODULE :

**Panorama des risques inhérents aux CERT**

Explorer les RPS pouvant survenir dans les missions quotidiennes des membres d'un CERT, des missions les plus habituelles aux missions parfois inattendues au travers d'une analyse de risques.

**Détecter et prévenir**

Que ce soit la formation, la sensibilisation, mais également l'observation et le dialogue, de nombreux moyens permettent d'identifier des membres en difficulté. Mais une fois l'identification opérée, la question qui se pose souvent est de savoir quoi faire.

**Gestion des situations de crise et Accompagnement**

Quand la prévention n'a pas fonctionné, comment accompagner un membre en difficulté et sur quels acteurs s'appuyer.

## OBJECTIF FINAL :

A la fin de ce module, les participants prendront conscience des RPS inhérents aux activités d'un CSIRT, que ce soit pour se prémunir soi, mettre en place le bon niveau d'écoute au sein de l'équipe, ou encore savoir accompagner les victimes d'un incident vers les bons moyens de prise en charge.

MODULE 11

# Judiciarisation des incidents et enjeux juridiques d'un CSIRT

Au sein de notre incubateur, le module «Judiciarisation des incidents et enjeux juridiques d'un CSIRT» s'impose comme une composante critique pour les CERTs, soulignant les aspects légaux et judiciaires entourant les activités de réponse à incident. Sous la tutelle des experts de l'InterCERT France, ce module offre aux participants une plongée approfondie dans les implications juridiques des opérations d'un CSIRT, abordant les enjeux liés à la judiciarisation des incidents.

*Commandant Stéphane Deldicque - Chef de la section des cyberattaques à l'OFAC, DNPJ*

*Nha-Khanh Nguyen - Analyste forensic et malware au CSIRT-PJ, DNPJ*

## CONTENU DU MODULE :

Judiciarisation des incidents et enjeux juridiques d'un CERT

**Cadre juridique de la cybercriminalité**

explorer le paysage juridique en constante évolution lié à la cybercriminalité et décrire l'organisation de la lutte contre la cybercriminalité en France.

**Collaboration avec les autorités policières judiciaires**

développer des compétences pour collaborer efficacement avec les autorités judiciaires, en comprenant les procédures de signalement, de dépôt de plainte et de transmission d'informations cruciales.

**Protocoles de collecte de preuves**

familiariser les équipes avec les protocoles et à l'intérêt de la collecte de preuves numériques, assurant la conformité légale tout en préservant l'intégrité des éléments probants.

## OBJECTIF FINAL :

À la fin de ce module, les participants auront acquis une compréhension approfondie des dimensions juridiques entourant les activités d'un CSIRT. Ce module vise à doter les équipes des connaissances nécessaires pour naviguer dans le paysage juridique complexe, assurant ainsi la légalité et la transparence dans les opérations de réponse à incident, tout en préservant les droits et la confidentialité des parties impliquées.

MODULE 12

# Standards de réponse aux incidents

Au sein de notre incubateur, le module «Standards de réponse à incident» se concentre sur l'adoption de normes et de bonnes pratiques pour optimiser la réaction aux incidents de sécurité. Animé par des experts de l'InterCERT France, ce module offre aux participants une immersion dans les standards reconnus, visant à renforcer la capacité des équipes de réponse à anticiper, détecter, et atténuer les incidents de manière cohérente.

*Vincent Nguyen, Directeur Cybersécurité, CERT- STOÏK*

stoïk

## CONTENU DU MODULE :

**Étude des standards reconnus**

Examiner en détail les normes internationales telles que ISO/IEC 27035, NIST SP 800-61, et d'autres référentiels qui définissent les bonnes pratiques en matière de réponse à incident.

**Adaptation aux besoins spécifiques**

Comprendre comment adapter ces standards en fonction des caractéristiques et des contraintes propres à chaque organisation et CSIRT.

**Création de plans de réponse**

Guider les équipes dans l'élaboration de plans de réponse à incident basés sur les standards, en mettant l'accent sur la coordination, la documentation, et l'amélioration continue.

**Exercices pratiques**

Mettre en pratique les concepts enseignés à travers des simulations d'incidents, permettant aux équipes de tester et d'affiner leurs processus de réponse.

## OBJECTIF FINAL :

À la fin de ce module, les participants auront acquis une compréhension approfondie des standards de réponse à incident, renforçant ainsi leur capacité à structurer et à exécuter des réponses cohérentes et efficaces. Ce module vise à équiper les équipes pour faire face aux défis de la cybersécurité tout en maintenant une approche alignée sur les meilleures pratiques internationales.

MODULE 13

# Atelier pratique - Collecte et analyse “forensic”

Au sein de l’incubateur, cet atelier pratique est en parfaite complémentarité avec les modules précédemment dispensé, notamment le module 07. De la manipulation d’un copieur de disque à la réalisation de timeline (chaîne chronologique de l’incident), ce module contribue à renforcer la capacité du CERT à réaliser l’analyse forensique par la pratique. Parce qu’il aborde tant la dimension technique que la restitution, cet atelier pratique s’adresse à tout type de profil.

*Grégory GUILLERMIN, Incident Detection & Response Team leader*

*Arnaud L’HUTEREAU, Analyste DFIR*

## CONTENU DU MODULE :

### Collecte de données

Démonstration et mise en pratique de la collecte de données sur machine potentiellement compromise.

Que faire face à une machine potentiellement compromise ? Quoi récupérer, et comment ? Quels outils utiliser ? Comment assurer l’intégrité de la donnée ? Où la stocker ?

### Construction de timeline

Exploitation d’un jeu de données mis à disposition pour l’exercice, afin de reconstituer la chaîne chronologique d’évènements de sécurité caractérisant un incident.

Comment faire parler la donnée ? Quels outils utiliser ? Quels écueils éviter ? Quelles bonnes pratiques appliquer ?

### Livrable et restitution

Présentation des résultats obtenus, avec mise en pratique de la rédaction du rapport à la restitution.

Comment restituer de façon claire à n’importe quel public ?
Quels sont les éléments essentiels à inclure ? Quid des éléments juridiques ?

## OBJECTIF FINAL :

Ce module a pour objectif de faire expérimenter aux participants la réalité de la réponse à incident sur le terrain, de la collecte de données à la reconstitution de la chaine chronologique des évènements constituant l’incident. A la fin de ce module, les participants auront pu mettre en œuvre dans des conditions réalistes d’entrainement, sur des machines dédiées, les actions essentielles de l’analyse forensique. Ils auront utilisé différents outils de collectes de données et des outils de reconstitution de chaîne chronologique d’évènements à l’état de l’art. Ils auront ensuite réalisé l’exercice de restituer les éléments observés dans un rapport. La mise en pratique sera l’occasion de bénéficier des retours d’expérience et bonnes pratiques de chacun.

MODULE 14

# Outillage d'un CERT

Se positionne comme un socle fondamental, mettant en lumière l'importance stratégique des outils et technologies dans le fonctionnement optimal d'un (CERT). Sous la houlette de Thibaud Binetruy, Responsable du Csirt-Suez et administrateur de l'InterCERT France, ce module offre aux participants une exploration approfondie des solutions technologiques, des plateformes, et des bonnes pratiques nécessaires pour optimiser les opérations d'un CERT.

*Thibaud Binetruy*

## CONTENU DU MODULE :

Les équipes de réponse aux incidents de cybersécurité ont des besoins très spécifiques d'outillage afin de mener leurs missions à bien.  Ce module passera en revue différentes catégories d'outils qui peuvent être indispensables ou simplement fortement utiles lors des différentes phases de réponses aux incidents.

L'objectif n'est pas tant de fournir une liste d'outils à utiliser absolument, mais plutôt d'initier une réflexion pour aider les participants à sélectionner les outils les plus adaptés à leurs contextes.

Les sujets évoqués sont les suivants :

- pourquoi une équipe CSIRT est à part ?,
- processus d'achats exceptionnels pour les urgences,
- du hardware spécifique ?,
- une infrastructure à part ?,
- quels outils pour tracker ses incidents ?,
- matériel spécialisé pour le forensic et les cas judiciarisés,
- outils et environnements d'analyse de malware,
- virustotal,
- outils d'analyse CTI,
- EASM,
- dataleak monitoring

## OBJECTIF FINAL:

À la fin de ce module, les participants auront une meilleure connaissance des différents outils auxquels ils pourraient avoir recours pour faciliter la réponse aux incidents. Ce module est aussi l'occasion d'identifier les processus d'exception potentiels à mettre en oeuvre au sein de leur structure pour répondre à des besoins d'outillage spécifique en urgence.

MODULE 15

# Fondements de la collecte « forensic »

Comprendre les principes de base de la collecte d'indices numériques, depuis la préservation de l'intégrité des données jusqu'à l'utilisation d'outils spécialisés.

*Nha-Khanh Nguyen - Analyste forensic et malware au CSIRT-PJ, DNPJ*

CSIRT-PJ

## CONTENU DU MODULE :

### Techniques de collecte avancées

Approfondir les compétences en matière de collecte en explorant des techniques avancées telles que la mémoire volatile, la recherche de signatures, et l'analyse du réseau.

### Analyse de la chaîne d'incident

Examiner les méthodes systématiques pour analyser la chaîne chronologique des incidents, permettant une reconstitution précise des événements.

### Intégration dans le processus de réponse

Identifier comment intégrer la collecte et l'analyse « forensic » de manière efficace dans le processus global de réponse à incident.

## OBJECTIF FINAL :

À la fin de ce module, les participants auront développé une expertise solide en matière de collecte et d'analyse « forensic », renforçant ainsi leur aptitude à investiguer et à résoudre les incidents de sécurité de manière approfondie. Ce module vise à doter les équipes des compétences nécessaires pour conduire des enquêtes numériques robustes, contribuant ainsi à la sécurité et à la résilience de leurs systèmes d'information.

MODULE 16

# Gestion de crise d'origine cyber - Bonnes pratiques et organisation

Au sein de notre incubateur, le module «Gestion de crise d'origine cyber - Bonnes pratiques et organisation» prend une place centrale en préparant les CSIRT à faire face aux situations d'urgence avec efficacité et coordination. Guidé par Vincent Nguyen, Directeur de la Cybersécurité, Stoïk et Responsable du projet Incubateur l'InterCERT France, ce module offre aux participants un cadre solide pour comprendre et mettre en œuvre des pratiques de gestion de crise, cruciales pour atténuer les impacts d'une cyberattaque.

*Vincent Nguyen, Directeur Cybersécurité, Stoïk*

stoïk

## CONTENU DU MODULE :

**Préparation à la crise**

Acquérir des compétences essentielles pour anticiper et planifier en amont les scénarios de crise potentiels, établissant ainsi une base solide pour la réactivité en temps réel.

**Organisation des équipes**

Explorer les meilleures pratiques d'organisation des équipes de réponse, définissant les rôles, les responsabilités, et les canaux de communication pour une coordination optimale.

**Processus de gestion de crise**

Identifier les différentes étapes d'une gestion de crise et les plans d'actions à définir : investigation, remédiation, reconstruction, communication, juridique, etc.

**Rétablissement post-incident**

Comprendre les phases critiques du rétablissement post-incident, en mettant l'accent sur l'apprentissage continu, la révision des procédures, et l'amélioration de la préparation future.

## OBJECTIF FINAL :

À la fin de ce module, les participants auront développé une expertise solide en gestion de crise cyber, renforçant ainsi leur capacité à réagir efficacement face aux incidents majeurs. Ce module vise à doter les équipes des outils nécessaires pour gérer les situations de crise avec sang-froid, coordination, et efficacité, minimisant ainsi les impacts sur la sécurité des systèmes d'information.

MODULE 17

# Communication de crise

Au cœur de notre incubateur, le module «Communication de Crise» se dévoile comme un volet essentiel, formant les équipes de CERTs à maîtriser l'art délicat de la communication en situation d'urgence. Sous la conduite de Vincent Nguyen, Directeur Cybersécurité, Stoïk, ce module offre aux participants une plongée approfondie dans les meilleures pratiques de communication de crise, élément clé pour maintenir la confiance, assurer la transparence, et coordonner efficacement les actions lors d'une gestion de crise d'origine cyber.

*Vincent Nguyen, Directeur Cybersécurité, Stoïk*

stoïk

## CONTENU DU MODULE :

Planification de la communication : Acquérir des compétences pour élaborer des plans de communication dédiés à la gestion de crise, identifiant les publics cibles, les messages clés, et les canaux appropriés.

Gestion des médias : Explorer les stratégies de gestion des médias en période de crise, minimisant les risques de désinformation tout en fournissant des informations précises et rassurantes.

Communication interne : Développer des compétences en communication interne, assurant une transmission efficace des directives, des mises à jour, et des consignes au sein de l'équipe de réponse.

Rétablissement de la réputation : Comprendre les mécanismes de rétablissement de la réputation après un incident, en mettant en place des stratégies pour restaurer la confiance des parties prenantes.

## OBJECTIF FINAL :

À la fin de ce module, les participants auront développé une maîtrise avancée en communication de crise, renforçant ainsi leur capacité à gérer les aspects médiatiques et internes lors de crises d'origine cyber. Ce module vise à positionner les équipes pour une communication transparente, cohérente, et rassurante.

MODULE 18

# Atelier pratique - Enrichissement et pivots techniques : la CTI appliquée à la réponse à incident

Au sein de l'incubateur, cet atelier pratique sera l'occasion pour les participants de réaliser par eux même une investigation technique en sources ouvertes sur des infrastructures d'attaque à partir d'outils à l'état de l'art. Complémentaire des différents modules sur la CTI, les indicateurs et la veille, cet atelier offre une vision concrète et opérationnelle de la CTI appliquée aux réalités quotidiennes d'un CERT : la levée de doute suite à une détection (phishing, navigation ou connexion suspecte...), la réponse à incident, la connaissance de la menace.

*Jean-Michel DOAN, MOA Tracking Tech lead, OWN-CERT*

*Erwan LE BLAVEC, Analyste CTI, OWN-CERT*

## CONTENU DU MODULE :

### Présentation des concepts d'investigation fondamentaux

- Orienter son renseignement
- Préparer un plan de recherche
- Notions essentielles pour pivoter sur des infrastructures malveillantes : IP, domaines, fichiers, etc.
- Outils et posture initiale

### Réalisation d'investigations

A partir d'éléments d'infrastructure suspects, nous investiguerons afin de lever le doute, comprendre le rôle de ces éléments, et étendre et enrichir la connaissance sur l'infrastructure d'attaque.

### Mise en action et capitalisation de la connaissance obtenue

- Trouver les «key findings» issus de l'investigation
- Produire des recommandations opérationnelles à engager suite à l'investigation

## OBJECTIF FINAL :

A la fin de ce module, les participants disposeront d'une boîte à outil comprenant les sources, pratiques et outils incontournables de l'enrichissement technique, leur permettant de réaliser des pivots simples et efficaces à partir d'indicateurs collectés dans le cadre de leur activité quotidienne, afin de contextualiser au mieux les incidents. Les participants gagneront ainsi en autonomie sur la production de renseignement technique.

MODULE 19

# Production de connaissance de la menace

Au cœur de notre incubateur, le module «Production de connaissance de la menace» émerge comme une étape cruciale, soulignant l'importance stratégique de générer une compréhension approfondie des menaces cybernétiques. Guidés par les participants exploreront les méthodologies avancées de production de connaissances, contribuant ainsi à renforcer la capacité d'un CSIRT à anticiper et à contrer les menaces émergentes.

*Maxime Arquiliiere, Analyste en renseignement sur la cybermenace*

## CONTENU DU MODULE :

### Veille Avancée

Acquérir des compétences approfondies en matière de veille stratégique, allant au-delà des simples indicateurs d'incidents pour comprendre les motivations, les tactiques, et les techniques des acteurs malveillants.

### Analyse de menaces complexes

Explorer les méthodes d'analyse avancée pour décomposer les menaces complexes, permettant une compréhension approfondie des vecteurs d'attaque et des motivations sous-jacentes.

### Production de rapports stratégiques

Développer des compétences dans la création de rapports de menace clairs et stratégiques, fournissant une intelligence opérationnelle pertinente pour les prises de décision et les actions préventives.

### Collaboration avec la communauté de CERTs

Favoriser la collaboration avec d'autres CSIRTs, organismes de sécurité, et partenaires du secteur pour enrichir la production de connaissances par l'échange d'analyses et d'informations.

## OBJECTIF FINAL :

À la fin de ce module, les participants auront acquis une expertise avancée dans la production de connaissance de la menace, renforçant ainsi leur capacité à anticiper les évolutions du paysage cybernétique. Ce module vise à outiller les équipes pour devenir des contributeurs actifs à la communauté de sécurité, favorisant ainsi une défense collective contre les menaces numériques en constante évolution.

MODULE 20

# Audition InterCERT France - Feuille de route

Le module «Audition InterCERT France - Feuille de Route» émerge comme une étape stratégique, offrant aux participants une opportunité exclusive d'interagir avec l'InterCERT-France, une référence nationale en matière de cybersécurité. Sous la tutelle d'experts chevronnés, ce module permettra aux équipes de CERT d'explorer la feuille de route d'InterCERT France, en se penchant sur les meilleures pratiques, les orientations stratégiques, et les défis du paysage cybernétique actuel.

*Haude COSTA – Directrice de l'InterCERT France*

## CONTENU DU MODULE :

**Présentation de l'InterCERT France**

Comprendre le rôle, la mission, et l'impact de l'InterCERT-France dans le panorama de la cybersécurité nationale.

**Feuille de route**

Explorer la feuille de route d'InterCERT-France, mettant en lumière les initiatives clés, les projets à venir, et les projets de l'association.

**Participation active**

Favoriser les échanges interactifs, permettant aux équipes de CERT de poser des questions, de partager des expériences, et de bénéficier de conseils pratiques pour améliorer leurs propres pratiques.

**Alignement avec les initiatives nationales**

Identifier les synergies entre les activités du CERT local et les initiatives nationales, contribuant ainsi à une coopération harmonieuse pour renforcer la résilience nationale face aux menaces cybernétiques.

## OBJECTIF FINAL :

À la fin de ce module, les participants auront acquis une compréhension approfondie de la vision stratégique d'InterCERT France et auront établi des liens concrets avec les efforts nationaux de cybersécurité. Ce module vise à inspirer les équipes de CERT à aligner leurs propres pratiques sur les meilleures normes, contribuant ainsi activement à la sécurité globale du paysage numérique.

MODULE 21

# Mini examen de clôture et diplôme

En conclusion de notre incubateur, le module offre une évaluation finale permettant de consolider les connaissances acquises et de reconnaître les compétences développées au cours du programme. Sous la supervision des experts de l'InterCERT France, ce module vise à évaluer de manière succincte la maîtrise des concepts clés et à conférer un diplôme attestant de la participation et de la réussite dans l'incubateur.

*Vincent Nguyen, Directeur Cybersécurité, Stoïk*

stoïk

*Olivier Caleff, Membre de liaison, InterCERT France*

CSIRT FRANCE

## CONTENU DU MODULE :

### Examen de synthèse

Mettre en place un mini examen couvrant les principaux domaines abordés au cours de l'incubateur, évaluant la compréhension et l'application des connaissances.

### Réflexion sur les cas pratiques

Intégrer des cas pratiques permettant aux participants de démontrer leur capacité à appliquer les compétences acquises dans des scénarios concrets.

### Évaluation des compétences transversales

Évaluer les compétences transversales telles que la collaboration, la communication, et la résolution de problèmes, cruciales pour le succès opérationnel d'un CERT.

### Remise des diplômes

Conférer un diplôme officiel aux participants ayant satisfait aux critères d'évaluation, reconnaissant ainsi leur engagement et leur réussite dans le programme d'incubateur.

## OBJECTIF FINAL :

À la fin de ce module, les participants auront passé avec succès le mini examen de clôture et recevront un diplôme officiel de l'incubateur. Ce module vise à célébrer les accomplissements individuels et collectifs, tout en fournissant une reconnaissance formelle des compétences acquises au cours du programme.

MODULE 22

# Visite de CERTs Opérationnels

Au sein de notre incubateur, la Visite de CERTs Opérationnels offre aux participants une opportunité unique de tirer des enseignements pratiques en se plongeant dans l'environnement opérationnel de CERT en activité. Sous la direction des Responsables de l'Incubateur de l'InterCERT France : Olivier Caleff et Vincent Nguyen, ces visites proposent une exploration concrète des bonnes pratiques et des retours d'expérience.

*Omar ABDELMOUMEN, Head of Cyber Defense CERT-Engie*

*Rodrigue Le Bayon, Head of Global CERT chez Orange Cyberdefense*

## CONTENU DU MODULE :

### Planification de visites

Acquérir des compétences pour planifier et organiser des visites de CERTs opérationnels, identifiant les objectifs d'apprentissage spécifiques à chaque équipe.

### Observation pratique

Explorer les opérations en direct au sein de CERTs, permettant aux participants d'observer les processus, les technologies, et les interactions.

### Échanges avec les équipes

Faciliter des échanges directs avec les membres opérationnels des CERTs visités, permettant aux participants de poser des questions, de partager des expériences, et de bénéficier d'enseignements concrets.

## OBJECTIF FINAL :

À la fin de ce module, les participants auront acquis des perspectives pratiques en visitant des CERTs opérationnels. Ce module vise à favoriser l'échange de connaissances, le partage d'expériences, et à inspirer les nouveaux CERTs à appliquer les meilleures pratiques observées pour renforcer leurs propres opérations de cybersécurité.

# Responsables du projet Incubateur

## Vincent Nguyen – Directeur Cybersécurité Stoïk

Fort de plus de 15 ans d'expérience dans le domaine de la cybersécurité, Vincent a dirigé et géré la résolution de nombreuses crises d'origine cyber tant au sein de Stoïk où il office depuis début 2023 en tant que Directeur Cybersécurité, qu'au sein de Wavestone de 2010 à 2021 où Vincent y a créé et dirigé le CERT-Wavestone.

Aujourd'hui, outre ses responsabilités chez Stoïk, Vincent est également évaluateur PRIS et formateur en cybersécurité sur différents sujets tels que la gestion de crise d'origine cyber et les normes internationales de réponse aux incidents de sécurité.

## Olivier Caleff – Membre de Liaison InterCERT France

Il travaille dans le domaine de la sécurité informatique depuis le début des années 90, et traite plus spécifiquement des problématiques de veille, de gestion d'incidents de sécurité et de cyber résilience. Il a participé à la création d'une douzaine de CSIRTs et est aussi membre de la TF-CSIRT et du FIRST, dont il est l'un des membres du Conseil d'Administration.

Il anime des formations TRANSITS spécialisée pour les membres de CSIRTs depuis une douzaine d'années en français et en anglais, et est l'un des 6 formateurs certifiés pour délivrer des formations sur SIM3, le modèle de maturité des CSIRTs.

Il est Auditeur Certifié SIM3, et a participé à la rédaction de documents liés à l'activités de CSIRTs ou d'ISAC au FIRST et à l'ENISA.

Profil LinkedIN : https://www.linkedin.com/in/caleff/

Incubateur de l'InterCERT France
Campus Cyber, Tour Eria
5-7 rue Bellini
92800 PUTEAUX
contact@intercert-france.fr
07 52 08 04 21