

**Sujet d'épreuves de la 48<sup>e</sup> Compétition Nationale  
des Métiers**

# **MÉTIER N°54 CYBERSÉCURITÉ**

**BLUE TEAM  
MODULE B ET C**

# EXPLICATION DU SUJET

DUREE TOTALE DE L'ÉPREUVE	4 heures
DIFFUSION DU SUJET	Découvert le jour de la compétition

## INTRODUCTION

Durant cette épreuve, vous serez plongé dans la vie d'un analyse SOC en période de crise.

## CONSEILS

Le sujet est rédigé de sorte que les réponses attendues aux questions soient pour la majorité des réponses uniques et simples, c'est-à-dire que les réponses seront les mêmes pour tout le monde et aucune variation ne sera possible. Ainsi, soyez très attentifs aux éléments de réponse. Si le résultat attendu est « **explorer.exe** », ne donnez pas « **Explorer.exe** » comme réponse, cela sera considéré comme faux par la plateforme. Soyez donc attentifs aux majuscules/minuscules et aux accents.

Votre objectif pour la compétition est de capitaliser un maximum de points. Concentrez-vous sur votre réalisation et non celle des autres. Enfin, n'oubliez pas que vous formez une équipe, alors ne vous précipitez pas. Prenez le temps de lire le sujet une première fois dans son intégralité, communiquez avec votre co-équipier et partagez-vous les tâches, optimisez votre temps.

## DESCRIPTION

L'objectif est de mettre à l'épreuve vos compétences en cybersécurité du point de vue défensif. Pour cela, vous serez placés dans un contexte réaliste d'entreprise ayant subi une attaque.

Au début de l'épreuve, vous aurez à disposition une description suffisante de l'infrastructure de l'entreprise pour naviguer intelligemment dans les journaux. L'épreuve se déroulera sur une après-midi de 4 heures durant laquelle vous travaillerez sur un SIEM open source avec des logs produits en amont par les équipes de Root-Me PRO.

Durant l'épreuve, vous serez évalués selon les critères suivants :

- votre compréhension des journaux et de leur format ;
- votre maîtrise des règles de filtrage afin d'extraire les informations les plus importantes ;
- votre esprit d'analyse afin de corréler les informations récupérées ;
- vos connaissances sur les techniques utilisées par les attaquants pour compromettre le service informatique complet d'une entreprise.

Une plateforme sera mise à votre disposition pour gérer le système de points et vous fournir l'accès au SIEM. Sur celle-ci, vous devrez répondre aux questions posées au fur et à mesure que votre compréhension de l'attaque s'affine. Chaque question rapportera un montant plus ou moins élevé de points en fonction de sa difficulté.

À la fin de l'épreuve, l'accès à la plateforme sera bloqué. Afin de déterminer votre note finale, les évaluateurs se baseront sur les bonnes et mauvaises réponses fournies. Aucune étape liée à la rédaction d'un rapport ne sera proposée.