# Impact

Réputation

Faire la com

Sincère et responsable

Fiche réflexe

# Crise cyber

Salle de gestion de crise

# Equipe blue team

Un SOC (Security Operations Center), un CERT (Computer Emergency Response Team) et un CSIRT (Computer Security Incident Response Team) sont des équipes spécialisées en cybersécurité qui ont des rôles différents mais complémentaires.

## Un SOC

est une équipe qui surveille en temps réel les systèmes informatiques et les réseaux pour détecter et prévenir les incidents de sécurité. Il est généralement responsable de la surveillance, de l'analyse et de la réponse aux événements de sécurité.

## Un CERT

est une équipe qui répond aux incidents de sécurité informatique. Il est généralement responsable de la coordination des efforts de réponse aux incidents, de l'analyse des incidents, de la gestion des vulnérabilités et de la diffusion d'informations sur les menaces de sécurité.

## Un CSIRT

est une équipe de réponse aux incidents de sécurité informatique qui est généralement créée pour des organisations gouvernementales ou des entreprises de grande envergure. Il est souvent responsable de la coordination des efforts de réponse aux incidents à grande échelle, de la gestion des vulnérabilités et de la coordination avec les autorités gouvernementales en cas d'incident de sécurité nationale.

# SIEM

Un SIEM (Security Information and Event Management) est un système de sécurité informatique conçu pour fournir une vue d'ensemble des événements de sécurité dans un environnement informatique. Il s'agit d'un outil de gestion centralisée des informations de sécurité, qui collecte, agrège et analyse les données de diverses sources, notamment les journaux d'événements, les alertes de sécurité, les flux de données et les informations de configuration.

Le SIEM permet de détecter les menaces de sécurité, de surveiller les activités suspectes et de répondre rapidement aux incidents de sécurité. Il utilise des techniques de corrélation et d'analyse de données pour identifier les tendances et les modèles qui indiquent des activités potentiellement malveillantes. Les résultats de cette analyse sont présentés sous forme de tableaux de bord, de rapports et d'alertes pour aider les analystes de sécurité à prendre des décisions éclairées sur la gestion des incidents de sécurité.

Le SIEM est une technologie importante pour la sécurité des systèmes d'information et est utilisé dans de nombreux secteurs, notamment la finance, la santé et les gouvernements. Les principales fonctions du SIEM incluent la collecte de données, la corrélation d'événements, l'analyse comportementale, la surveillance en temps réel, la gestion des incidents et la génération de rapports.