Répondre aux incidents et aux demandes d’assistance et d’évolution (Première année)

WatchGuard EPDR :

Lors de mon premier stage, j’ai eu l’opportunité de travailler sur la gestion des incidents et des demandes d’assistance ou d’évolution liées à la sécurité informatique, en utilisant la solution WatchGuard EPDR. Mon rôle consistait à traiter les tickets reçus par mail, à analyser les problèmes rencontrés par les utilisateurs, puis à les contacter par téléphone pour leur apporter une solution rapide et efficace. Cela m’a permis de développer mes compétences en support technique, en communication client et en gestion de la sécurité des postes de travail.

Bonjour,

Les menaces suivantes ont été détectées entre le 02/07/2024 07:55 et le 02/07/ 07:55 (UTC)

64 TENTATIVE(S) D'INTRUSION BLOQUÉE(S) SUR 1 ORDINATEUR

INFORMATIONS SUR LE ORDINATEUR AFFECTÉ :

Nom : **PC-AVA6-207**

Adresse IP : **10.10.0.113**

Groupe : **Tous\Postes de travail Equipe Technique - No Encrypt**

Sincèrement,

L'équipe WatchGuard.

Cher administrateur,

WatchGuard EPDR a détecté une activité par une menace de type **"Programme potentiellement indésirable"** nommée **'PUP/RemoteAdmin"** sur l'ordinateur **"EBPC-16PY623"**, le 02/07/2024 01:10:30 UTC.

Contactez notre équipe d'assistance technique pour toute question éventuelle.

Détails de la menace

Ordinateur :	EBPC-16PY623
Groupe:	Tous\ERIC BOMPARD\Postes de travails\Windows
Nom :	PUP/RemoteAdmin
Chemin :	PROGRAM_FILESX86|\AnyDesk-ad_31470325_msi\AnyDesk-ad_31470325_msi.ex
Hachage :	356A8A3B686D056556EA6D3832F4C0D7
Ordinateur source de l'infection :	
Adresse IP source de l'infection :	
Utilisateur source de l'infection :	

WithSecure :

High risk alert

Suspicious activity detected (ID 243833788-43862)

WithSecure Elements Endpoint Detection and Response detected the following activity:

Category:	Privilege Escalation
Risk level:	High risk 82
Confidence:	Info
Criticality:	Info
Affected devices:	hp-5cd106fk1z.ariane.intra
Company:	Mairie d'ALBERTVILLE


HP-5CD106FK1Z
WININIT.EXE
SERVICES.EXE
LC7AGENT.EXE
LSASS.EXE