Le leurrage numérique comme complément de l'approche de cyber défense

Laurent Cordival, Fabien Thurot, Matthieu Riche, Antoine Ladune, Guillaume Mey-net

Beijaflore
lcordival073@beijaflore.com

Résumé

Les entreprises développent de plus en plus leurs capacités de cyber défense pour répondre à l'accroissement des risques et menaces cyber.
Ces stratégies souvent basées sur le log management en vue de répondre aux besoins de détection et d'investigation bénéficient d'ajouts ponctuels de solutions spécialisées dites « best of breed » pour des périmètres spécifiques et potentiellement complexes. Cela tend à combler leurs faiblesses voire à adresser de nouvelles problématiques. Un premier exemple serait l'intégration du SIEM au SOAR pour industrialiser voire automatiser les processus d'investigation ou de réponse à incident ou encore l'usage de l'EDR pour adresser les use-cases de détection techniques systèmes et faciliter la réponse au niveau endpoint.
Le log management n'en reste pas moins la pierre angulaire de la cyber défense de nombreuses entreprises. Cette approche présente des faiblesses dont notamment la quantité/qualité des logs, la scalabilité, la qualité de la stratégie de détection impactant notamment le pourcentage de faux positifs.
Toujours dans l'optique de renforcer voire de combler les lacunes de l'approche log management, le leurrage numérique appelés « deception tools » en anglais, peut être employé. Cette technologie qui consiste à placer des pièges ou leurres dans un Système d'Information permettrait notamment de renforcer la détection sur des cas de cyber attaques spécifiques, de faciliter la levée de doute voire même pour les entreprises les plus matures, d'initier des processus de réponse à incident industrialisés.
Bien qu'apparu il y a plusieurs dizaines sur les réseaux internet, le concept de leurrage numérique profite d'une offre en plein essor et fait l'objet ici d'une étude sur les bénéfices et les limites des différentes solutions du marché pour renforcer les capacités de détection et de réponse des entreprises actuelles.

Mots clés:
Leurre, Deception tools, Cyber sécurité, Big data, Right data, SOC, SIEM, Détection, Réponse, Threat Intelligence, Use cases, Vraisemblance, Interactivité.