Description de la conférence :Cyber défense active (ThreatHunting)
Par : Michel Cusin

Le portrait des cyberattaques et la sécurité est en constante évolution et a beaucoup changé au cours des dernières années. Plusieurs rapports annuels provenant de joueurs importants et réputés en sécurité tels que le Verizon Data Breach Investigations Report (DBIR)ou encore le M-Trends Report de FireEyele démontrent clairement.

La question n'est pas de savoir si nous serons piratés, mais plutôt quandet pendant combien de temps les pirates auront le contrôle de nos infrastructures et de nos données.

Un des défis majeurs auquel les organisations font face aujourd'hui est de réussir à détecter la présence d'intrus. Les multiples mécanismes de défense « traditionnels » tels que les coupe-feu, les antivirus, les systèmes de détection d'intrusion ou encore les solutions de sécurité de type«Endpoint » ne sont malheureusement plus suffisants pour faire face aux menaces actuelles. En effet, les attaquants sérieux et motivés réussissent à contourner ces mécanismes de défense afin de prendre le contrôle de nos infrastructures et de nos données, peu importe les moyens de défense que nous mettons en place.

Actuellement, selon le M-Trend Report 2018, le temps moyen pour détecter une brèche est de 101 jours. Selon les cas, cette période va de moins d'une semaine à plus de 2000 jours.

Il n'est pas rare de constater que la majorité des équipes de sécurité attendent souvent de recevoir une alerte pour réagir. Cette réalité est d'autant plus problématique si une brèche de sécurité ne génère aucune alerte, comme c'est souvent le cas.

Les attaquants utilisent et déploient plusieurs types de backdoorssur les systèmes qu'ils compromettent. Ils regorgent d'ingéniosité pour contourner les mécanismes de défense afin de pouvoir communiquer avec les serveurs de Command and Control (C2), lesquels sont difficiles à détecter si les données sont cachées, encryptésou si des méthodes d'obfuscation sont utilisées.

C'est pour cette raison que la mise en place d'une stratégie de cyber défense active (ThreatHunting) notamment basée sur la détection comportementale est essentielle.

Contrairement aux solutions "traditionnelles" telles que la détection d'intrusion ou les antivirus, l'analyse comportementale ne dépend pas des signatures et n'a pas nonplus besoin de décrypter le trafic pour l'analyser.

En fait, elle utilise plutôt des éléments tels que les schémas (patterns) de trafic réseau afin d'identifier le trafic malicieux que les solutions "traditionnelles" ne sont pas en mesure de détecter.

Lors de cette présentation, nous explorerons ensemble diverses problématiques liées à des scénarios d'attaques actuels et comment la mise en place d'une stratégie de cyber défense active (ThreatHunting) peut changer la donne afin de ne pas perdre la guerre.