Détection d'incidents : Thales dévoile sa sonde prête pour les OIV

Comme les autres industriels français de la cybersécurité, Thales marque à la culotte les avancées de l'Anssi (Agence nationale pour la sécurité des systèmes d'information) sur la mise en place de la Loi de programmation militaire, législation qui se traduit par un renforcement des exigences de sécurité imposées aux grandes organisations françaises. Après s'être engagé dans les qualifications PASSI (audit), PRIS (réponse à incident) et PDIS (détection d'incidents) ou dans celle de ses boîtiers de chiffrement, le Français dévoile aujourd'hui une sonde de sécurité en cours de qualification par l'Anssi.

L'agence étatique devrait en effet prochainement dévoiler une liste de sondes habilitées que les Opérateurs d'importance vitale (OIV), environ 250 organisations dont la sécurité se voit peu à peu encadrée par l'Etat, devront déployer d'ici à 2019 pour protéger leurs systèmes d'information critiques. Le modèle que propose Thales, conçu et développé en France, serait, selon son concepteur, le premier à être en passe d'être adoubé par l'Anssi.

« *La sonde embarque des algorithmes comportementaux capables de détecter des événements anormaux sur le réseau. Elle intègre également des signatures ou empreintes d'attaques, et pourra être alimentée par du renseignement spécifique sur les menaces ciblées afin d'identifier et de contrer plus rapidement les attaques connues* », explique Thales dans un communiqué. Si on se fie à une déclaration de Guillaume Poupard, le directeur général de l'Anssi, les sondes qualifiées devront notamment être en mesure d'intégrer des signatures de menaces fournies par l'agence. L'Anssi ne fait pas mystère de sa volonté de jouer le rôle du tiers neutre permettant un partage de l'information sur les menaces entre OIV.

OIV : la revanche des technos françaises ?

Disponible pour différents débits de réseau, la sonde peut être exploitée par la DSI ou par Thales, dans le cadre d'un service global de supervision de la sécurité. Le SOC (Security Operation Center) du Français, basé à Elancourt (Yvelines), gère la supervision d'une quarantaine de grands comptes. Rappelons que le groupe de Patrick Caine a récemment remporté un contrat de 5 ans auprès d'Engie, contrat portant sur la supervision des infrastructures mondiales de ce groupe de 155 000 personnes.

La qualification par l'Anssi, qui passe par un examen en profondeur des solutions, pourrait gêner aux entournures un certain nombre d'industriels, surtout américains : « *Certains ne peuvent pas répondre à nos critères* », reconnaissait d'ailleurs voici quelques mois Guillaume Poupard dans nos colonnes. Pour les industriels français, comme Thales, l'opportunité est belle de reprendre quelques parts de marché à la technologie américaine, ultra-dominante dans la cybersécurité.

Thales précise que cette sonde n'est pas issue du partenariat qu'il a signé en juin dernier avec Cisco et visant à co-développer une solution de détection des menaces et de réponse aux attaques. Le fruit de ces travaux communs entre le géant des réseaux et le groupe de défense, qui doivent aussi

impliquer des start-ups, doit toutefois être dévoilé lors des Assises de la sécurité, un événement qui a ouvert ses portes aujourd'hui à Monaco.

A lire aussi :

Orange Cyberdéfense entend surfer sur la législation des OIV

OIV : la détection des attaques passe sous le contrôle de l'Etat

L'Etat français va certifier les Cloud de confiance