# L’automatisation permet d’unifier les opérations de sécurité

Une attaque massive, opérée au moment opportun contre une entreprise, peut avoir des conséquences dévastatrices. Certaines des plus récentes et médiatisées visant des industriels, des compagnies aériennes et encore des chaînes hôtelières, ont entraîné des baisses de la productivité, des atteintes à la réputation ainsi que des amendes conséquentes.

Dans ce contexte, la sécurité des entreprises a fait l’objet d’un examen approfondi. Les équipes de sécurité font généralement un travail admirable. Néanmoins, elles sont désormais chargées de sécuriser de vastes infrastructures multi-fournisseurs. Or, leur capacité à faire face à cette nouvelle complexité et à gérer des opérations à grande échelle peut être considérablement renforcée par l’automatisation des opérations de sécurité.

Les équipes en charge de la sécurité disposent rarement d’un framework commun pour partager leurs concepts, leurs processus et leurs idées. Pour pallier ce manque, elles peuvent rassembler leurs opérations (parfois hétérogènes dans une grande entreprise) au sein d’un ensemble spécifique de workflows et de processus automatisés.

L’automatisation, déjà bien installée dans de nombreux domaines de la technologie et de la mise en réseau, insuffle une véritable culture de la collaboration entre les différents acteurs de l’informatique. La sécurité étant de plus en plus étroitement intégrée aux départements informatiques, les équipes qui en ont la charge peuvent elles aussi adopter l’automatisation. Toutefois, il faut reconnaître qu’il ne s’agit pas d’une entité unique mais de la composition de différents éléments tels que la sécurité des terminaux, des réseaux et des données.

Les entreprises sont capables de mieux intégrer leurs équipes, leurs fonctions, leurs processus et leurs applications en adoptant un modèle automatisé de la sécurité. Néanmoins, la capacité de l’automatisation à favoriser un esprit d’ouverture et de collaboration dépend de certains facteurs clés.
Le plus important d’entre eux est la nécessité de mettre en place un langage universel programmable, accessible à tous. Celui-ci doit être facile à appréhender afin que les informations puissent être documentées et partagées entre les professionnels de la sécurité ayant des compétences spécialisées dans leur domaine respectif.

De surcroît, l’automatisation doit s’appuyer sur une approche sans parti pris. A défaut, elle ne sera rien d’autre qu’un système fermé bouleversant l’équilibre délicat des écosystèmes de sécurité complexes. Enfin, l’automatisation se doit d’être modulaire pour s’adapter aux solutions des nombreux fournisseurs qui composent la vaste infrastructure de sécurité des entreprises.

Une fois tous ces prérequis implémentés, les professionnels de la sécurité seront en mesure de fournir à leurs collègues un accès aux systèmes et aux applications. Ils peuvent communiquer entre eux par le biais de workflows automatisés qui contiennent des instructions explicites sur la manière d’effectuer chaque tâche. L’administrateur peut fournir autant d’accès que nécessaire, et avec la certitude qu’ils ne seront pas compromis, de même que son autorité.

Malgré cela, des équipes aux domaines de compétence hétérogènes peuvent rencontrer des difficultés à communiquer, ce qui étouffe la collaboration. Le dénominateur commun est donc la mise en place d'un système impartial articulé autour d'un langage universel.

Bien qu'il existe beaucoup d'approches de la sécurité parmi lesquelles choisir, il y a des avantages évidents à adopter des normes ouvertes. Cela permet la mise en place de workflows structurés dédiés à la conduite des opérations de sécurité pouvant être intégrés dans les plateformes SOAR (Security Orchestration, Automation and Response) et les applications SIEM (Security Information and Event Management) existantes. In fine, ce modèle contribue à renforcer les barrières aux attaques de l'entreprise.

L'utilisation de cette approche globale présente de multiples avantages. Les responsables de la sécurité bénéficient d'une plus grande visibilité sur l'ensemble de leur fonction, tandis que les équipes peuvent s'engager dans l'échange, nourrir leurs relations et partager la responsabilité ; ce dernier point résultant bien souvent d'une organisation en silos plus que d'un manque de confiance.

L'automatisation fournit ainsi aux équipes de sécurité un terrain pour se coordonner et résoudre des problèmes. Une approche de l'automatisation de la sécurité optimale relie des systèmes disparates de l'entreprise via des workflows automatisés.
Les professionnels de la sécurité peuvent ainsi concevoir un code exécutable afin de piloter de nouveaux processus et réduire la quantité d'erreurs humaines. Les équipes en charge des opérations de sécurité ont, quant à elles, la possibilité d'opérer une série d'actions sur les différentes solutions de l'entreprise plus rapidement et ainsi de contrer les menaces plus efficacement.

Le véritable changement dépend également du facteur humain et de la capacité d'équipes autrefois diversifiées et travaillant en silos à se réunir autour d'une table pour évoquer la manière dont elles peuvent collaborer pour servir leurs objectifs communs.

Les équipes utilisant un framework de sécurité ouvert peuvent développer un ensemble de processus unifiés dont les bénéfices sont visibles à l'échelle de toute l'entreprise. Cela signifie que des équipes diversifiées ayant des compétences dans des domaines variés peuvent collaborer avec davantage de fluidité et mutualiser la responsabilité