S'ADAPTER À UNE CYBERCRIMINALITÉ en mutation

ESET est une société de cybersécurité fondée en 1992. Pionnière dans la lutte contre les logiciels malveillants, elle a dû sans cesse trouver de nouvelles réponses aux attaques de plus en plus complexes et variées, tout en se développant fortement à l'international. ***Expert en cybersécurité et associé de la société, Benoît Grunemwald*** nous explique les enjeux d'un monde sans cesse en mouvement.

Benoît Grunemwald

"Nos challenges sont plus complexes qu'avant – et cela se répercute sur les compétences que l'on doit réunir."

Pouvez-vous nous présenter vos activités ?
Nous sommes une entreprise qui édite des logiciels de cybersécurité. ESET existe depuis trente ans et elle a été créée au cœur de l'Europe, en Slovaquie, à Bratislava. Notre activité a beaucoup évolué dans cette période. Au début, notre travail consistait essentiellement à stopper des logiciels malveillants. Aujourd'hui, les cybercriminels se sont professionnalisés : ils ont évolué dans leurs méthodes et nous devons détecter bien au-delà des phénomènes malveillants et sur des périmètres beaucoup plus larges qu'ils ne l'étaient auparavant.
Globalement, ESET est une société tournée vers la technique. Nous traitons environ 500 000 menaces par jour : les êtres humains seuls ne peuvent pas gérer autant de menaces. Nous avons donc de nombreux métiers liés à l'intelligence artificielle. Nos ingénieurs vont également se charger de la rétro-ingénierie logicielle pour pouvoir décompiler, analyser du code malveillant. Enfin, nous avons des ingénieurs qui vont s'occuper de l'analyse des groupes d'attaquants, sur un aspect technique mais aussi un peu plus général, touchant à la victimologie : qui a été attaqué, pourquoi ? C'est notamment le cas en ce moment, où ont lieu beaucoup d'opérations de cyber espionnage.

La connaissance de la menace est importante pour vous dans ce cadre ?
La connaissance de la menace est fondamentale, notamment quand nous participons à des opérations avec des forces de l'ordre. La télémétrie, la connaissance des informations qui nous arrivent depuis différents points, représente 110 millions de points à travers le monde, ainsi que de nombreuses autres sources que l'on agrège : il faut donc des moyens importants pour traiter l'ensemble. Dans notre mode de fonctionnement avec les forces de l'ordre, l'un des objectifs est de cartographier et de comprendre la menace, au sens large, c'est-à-dire celui qui l'opère et les outils qui servent à opérer cette menace. Nous dressons donc une cartographie qui servira aux forces de l'ordre de plusieurs pays, les attaques émanent souvent de différents pays et ciblent différents pays. Cette cartographie leur permettra de remonter jusqu'aux victimes, jusqu'aux attaquants. Les données que nous leur fournissons sont uniques car nous avons une vision mondiale : notre logiciel est installé sur un grand nombre de machines.
Nous avons également un double partenariat avec Google : sur Google play store, et sur un outil qui s'appelle Google tool clean up, permettant d'analyser chaque fichier téléchargé avant qu'il ne soit exécuté. Nos technologies sont embarquées dans les produits Google sans que les utilisateurs le sachent, on peut donc dire que l'on protège plus d'un milliard d'internautes à travers le monde.

Quel regard portez-vous sur la place de votre entreprise dans son environnement concurrentiel ?
Nous avons des concurrents plus connus que nous ; pourtant, nous sommes le premier éditeur européen, selon l'analyste Gartner. Devant nous, les éditeurs sont américains ou d'autres nationalités extra-européennes. C'est un paramètre important dans un monde où

le RGPD, où la protection des données de manière générale, importe de plus en plus. Partager ces valeurs est une grande force pour nous. Par ailleurs, nous travaillons depuis trente ans aux bases de données, aux algorithmes et au machine learning : c'est un temps d'avance, une expérience difficile à rattraper.
Notre empreinte de consommation au poste de travail est très légère, calculée au plus juste. Nous sommes connus dans les milieux industriels, ou dans les milieux où les machines n'ont pas beaucoup de ressources (l'administration, les écoles), mais également chez les gamers, qui ont besoin de beaucoup de ressources et qui ont conscience des enjeux de sécurité.
Enfin, un point important : toutes nos solutions sont développées en interne. Nous en sommes propriétaires. Par ailleurs, la société est détenue par ceux qui l'ont créée. C'est ce qui nous permet de nous concentrer sur deux objectifs seulement : être rentables et protéger les utilisateurs.

Pouvez-vous nous présenter une problématique concrète à laquelle vous êtes confrontés ?
Nous protégeons la Gendarmerie nationale : chaque poste est équipé avec nos solutions. Le déploiement a été très bien géré par la gendarmerie, avec des périodes de test enrichissantes pour nous aussi. Avant de nous choisir, ils devaient s'assurer de la bonne compatibilité de leurs systèmes d'informations, mais aussi de la probité de l'entreprise. Il a fallu ensuite les accompagner pour superviser et mettre en place des rapports pour savoir s'il y a une tentative d'intrusion sur leur parc. Nous travaillons autant sur la plateforme linux que sur windows, avec une très grande souplesse dans le paramétrage pour s'adapter aux contraintes opérationnelles qui sont les leurs. Cette expérience a été une preuve de notre capacité d'adaptation.

Quels sont pour vous les grands défis actuels dans votre secteur d'activité ?
Il y a une mutation de la cybercriminalité, et elle conduit à des changements structurels : c'est-à-dire sur la façon dont les criminels s'organisent, se rassemblent en mafias, et donc sont de plus en plus outillés, puissants, financés ; mais aussi sur la manière dont ils agissent : auparavant, l'outillage des cybercriminels consistait en des virus ; aujourd'hui, ils exploitent les failles zero day, les failles qu'eux seuls connaissent, les vulnérabilités que personne ne protège ou ne cherche à protéger. On voit bien que l'utilisation de ces failles va permettre d'écouter, d'espionner, de se renseigner sur des cibles étatiques ou proches des États et ce à travers tous les continents. Nous constatons aussi une modification des cibles : on voit que certains groupes d'attaquants étendent leur zone d'action en Afrique par exemple - où nous sommes d'ailleurs très présents.
En conséquence, notre entreprise est en évolution depuis trente ans : nous nous adaptons et nous essayons d'anticiper, grâce à la cyber threat intelligence. Nos défis sont multiples, notamment dans la poursuite d'éléments d'intelligence artificielle pour être efficaces dans la classification des menaces, mais aussi dans la poursuite des signaux faibles, ceux qui ne relèvent pas de campagnes de masse, et qui sont des marqueurs faibles.
Le défi est de pouvoir apporter les services d'intelligence sur la menace, et d'apporter un accompagnement préalable. Nous utilisons quatre termes pour définir nos objectifs : prédire, prévenir, détecter, répondre. Dans le passé, l'antivirus suffisait à ces impératifs ; mais maintenant il faut y ajouter des services et de l'intelligence humaine, au-delà du logiciel.

Cette évolution correspond-elle donc à de nouveaux besoins en terme de recrutement ?
Nos challenges sont plus complexes qu'avant – et cela se répercute sur les compétences que l'on doit réunir : des ingénieurs sur l'intelligence artificielle, des ingénieurs sur la menace, sur les logiciels. Nos logiciels se sont complexifiés pour pouvoir couvrir plus de périmètres, je pense notamment à la messagerie Microsoft 365. Il y a clairement une pénurie de talents dans le monde, et c'est pourquoi nos postes sont ouverts à des personnes qui viennent de secteurs différents : nous préférons former des personnes motivées plutôt que de se priver de talents. Le secteur a un bel avenir en terme de recrutement. D'autant plus que la cybersécurité est un domaine où l'on ne s'ennuie pas : chaque jour est différent. Les cybercriminels nous amènent vers de la nouveauté en permanence, et nous sommes poussés à innover : il faut anticiper constamment les nouvelles menaces !

EN BREF

ESET emploie 3000 personnes dans le monde, et dispose de 13 laboratoires de recherche. Elle apporte des solutions à des entreprises et des particuliers dans 200 pays différents.