LeMagIT
L'informatique pour et par les pros
TechTarget

E-guide #cyberrange

Contenu PRO+

Tout pour entraîner ses équipes à la défense de son Système d'Information

Dans ce guide

- Comment le cyber-range s'impose peu à peu dans l'entreprise
- Le cyber-range, une plateforme de simulation pour entraîner ses équipes
- Formation : immersion dans les méthodes des cyber-attaquants avec BlueCyForce
- Airbus CyberSecurity trouve des usages multiples à son cyber-range
- Accéder à plus de contenu Pro+

Introduction

La sécurité informatique doit aujourd'hui se réinventer sous l'impulsion de deux grands moteurs : d'une part l'évolution des marchés et des entreprises, d'autre part la course aux armements technologiques qui opposent les cybercriminels aux acteurs de la cybersécurité.

Dans ce guide, LeMagIT propose d'étudier les méthodes les plus efficaces de défense du SI et plus particulièrement les solutions de simulations d'incidents (cyber-range). Vous y trouverez également des cas d'usages clés pour vous inspirer dans votre stratégie de sécurité.

Dans ce guide

- Comment le cyber-range s'impose peu à peu dans l'entreprise
- Le cyber-range, une plateforme de simulation pour entraîner ses équipes
- Formation : immersion dans les méthodes des cyber-attaquants avec BlueCyForce
- Airbus CyberSecurity trouve des usages multiples à son cyber-range
- Accéder à plus de contenu Pro+

Comment le cyber-range s'impose peu à peu dans l'entreprise

Valéry Marchive, Rédacteur en chef adjoint

Les premiers environnements de simulation d'incidents de sécurité informatique, ou cyber-ranges, sont véritablement apparus autour de 2007 avec en particulier, aux Etats-Unis, le National Cyber Range (NCR) de la Darpa. Grégory Fresnais a participé au déploiement de plusieurs de ces environnements à travers le monde. Alors il se souvient : « à l'époque, il s'agissait d'environnements totalement physiques, des installations immenses ». Les militaires s'y intéressaient principalement. Mais depuis, les choses ont bien changé.

Fort de son expérience, Grégory Fresnais a co-fondé Cyber Test Systems en 2014. La jeune pousse a reçu le prix de la PME innovante lors de l'édition 2016 du Forum International de la Cybersécurité (FIC). Sa plateforme a été utilisée pour l'exercice de cyberdéfense interarmes Defnet, en mars dernier, avec celle de Diateam, ou encore Locked Shields organisé par l'Otan.

Dans ce guide

- Comment le cyber-range s'impose peu à peu dans l'entreprise
- Le cyber-range, une plateforme de simulation pour entraîner ses équipes
- Formation : immersion dans les méthodes des cyber-attaquants avec BlueCyForce
- Airbus CyberSecurity trouve des usages multiples à son cyber-range
- Accéder à plus de contenu Pro+

Une grosse décennie d'évolutions

Au tournant des années 2010, les cyber-ranges ont commencé à se démocratiser et à se multiplier, profitant des apports de la virtualisation, tant en termes d'espace physique occupé que d'administration et d'exploitation. Elbit Systems s'est fait un nom dans le domaine. Sa plateforme Cyberbit est largement utilisée à travers le monde, par RUAG en Suisse, notamment. C'est aussi en 2010 que Boeing présente son Cyber-Range-In-a-Box (Criab).

L'engouement progresse largement à partir de 2013 et là, se souvient Grégory Fresnais, beaucoup d'acteurs liés au monde de la défense se lancent : BAE, Thales, Airbus, ou encore Raytheon. L'offre se diversifie, avec SimSpace, Daedalus de Root9B, Quali Systems...

Des évolutions techniques...

Du virtuel, l'offre s'étend au Cloud pour gagner encore en flexibilité. Mais ce n'est pas sans limites : « cela ne permet pas de couvrir tous les vecteurs d'attaque ». Par exemple, pour s'entraîner avec d'authentiques maliciels, il faut utiliser un cyber-range virtualisé, qu'il soit déployé et exploité en interne, ou par un prestataire. Mais ce n'est pas la seule limite des environnements virtualisés ou en mode cloud.

Dans ce guide

- Comment le cyber-range s'impose peu à peu dans l'entreprise
- Le cyber-range, une plateforme de simulation pour entraîner ses équipes
- Formation : immersion dans les méthodes des cyber-attaquants avec BlueCyForce
- Airbus CyberSecurity trouve des usages multiples à son cyber-range
- Accéder à plus de contenu Pro+

Pour son cyber-range, Airbus CyberSecurity reconnaît ainsi qu'il convient d'utiliser un générateur de trafic matériel pour simuler efficacement des attaques en déni de service. Grégory Fresnais juge que cela vaut aussi pour des exercices impliquant des objets connectés ou des systèmes de contrôle industriel (ICS/Scada) : « le niveau de réalisme n'est pas le même sans composants physiques ». L'actuelle et troisième génération de plateformes de cyber-range est donc hybride. Mais les évolutions n'ont pas été que techniques.

...et organisationnelles

Les premiers cyber-range se contentaient, pour l'essentiel, de permettre de confronter attaquants – la *red team*– et défenseurs – la *blue team*. A l'instar de ce que font encore de nombreux outils, comme ceux de Verodin et d'AttackIQ, relève Grégory Fresnais.

Pour autant, ce n'est pas suffisant pour entraîner ses équipes avec un minimum de réalisme : d'où l'ajout de la notion de *green team*, pour l'intégration de trafic réseau tout ce qu'il y a de banal et de légitime. Puis est venue celle de *yellow team* : « des utilisateurs qui se font piéger par des opérations de *phishing*, par exemple ».

Mais là encore, « ce n'était pas suffisant et l'Otan a développé la notion de *purple team* », celle qui s'occupe notamment des dimensions communication

Dans ce guide

- Comment le cyber-range s'impose peu à peu dans l'entreprise
- Le cyber-range, une plateforme de simulation pour entraîner ses équipes
- Formation : immersion dans les méthodes des cyber-attaquants avec BlueCyForce
- Airbus CyberSecurity trouve des usages multiples à son cyber-range
- Accéder à plus de contenu Pro+

et juridique de la gestion des incidents, intégrant donc la gouvernance d'entreprise. A cela est venue s'ajouter une dernière notion, celle de *white team* : « les instructeurs qui vont gérer le dynamisme de l'exercice, en superviser le déroulement ».

Une demande croissante

L'évolution du cadre d'entraînement a conduit les plateformes à évoluer au-delà de la génération de trafic ou de l'orchestration de l'infrastructure virtuelle, pour intégrer la notation des participants à plusieurs dimensions : délais, collaboration, etc. Car au final, c'est la capacité d'équipes à intervenir ensemble pour réagir à une attaque qu'il s'agit d'évaluer.

Grégory Fresnais relève en outre que l'intérêt pour ces plateformes de simulation va aujourd'hui bien au-delà du seul monde de la défense : « de plus en plus d'entreprises s'y intéressent, ne serait-ce que pour des besoins réglementaires » - qui touchent notamment les opérateurs d'importance vitale et de services essentiels, mais sans exclusivité. Pour éprouver son infrastructure, ses processus, et se donner une chance de réussir un premier audit un peu strict, « il faut répliquer à minima une infrastructure de production, pour voir comment l'on sait réagir à des attaques sans affecter ses systèmes de production. D'où la demande croissante ».

Dans ce guide

- Comment le cyber-range s'impose peu à peu dans l'entreprise
- Le cyber-range, une plateforme de simulation pour entraîner ses équipes
- Formation : immersion dans les méthodes des cyber-attaquants avec BlueCyForce
- Airbus CyberSecurity trouve des usages multiples à son cyber-range
- Accéder à plus de contenu Pro+

Pour des publics plus variés

Les établissements scolaires s'intéressent également au cyber-range : « toutes les écoles polytechniques sont équipées à Singapour, pour la formation des étudiants. Et aux Etats-Unis, beaucoup d'universités le font aussi ». C'est moins le cas en France, mais comme l'a montré Airbus CyberSecurity l'an passé, au travers de quatre partenariats, cela commence.

Et bien sûr, il faut compter avec tous les exercices de type *Capture the flag*, visant à éprouver les compétences des participants. De plus en plus populaires depuis quelques années, « ils permettent notamment à des entreprises d'identifier de futurs employés potentiels ».

Dans ce guide

- Comment le cyber-range s'impose peu à peu dans l'entreprise
- Le cyber-range, une plateforme de simulation pour entraîner ses équipes
- Formation : immersion dans les méthodes des cyber-attaquants avec BlueCyForce
- Airbus CyberSecurity trouve des usages multiples à son cyber-range
- Accéder à plus de contenu Pro+

Le cyber-range, une plateforme de simulation pour entraîner ses équipes

Valéry Marchive, Rédacteur en chef adjoint

Les premières plateformes de simulation d'incidents de sécurité sont apparues il y a plus de quinze ans. Pour autant, selon Gartner, moins de 1 % des grandes entreprises y ont aujourd'hui recours. Cette part devrait passer à 15 % à l'horizon 2022.

Dans une note d'information à l'intention de ses clients, le cabinet décrit ce que l'on appelle aussi "cyber-range", comme « des plateformes de simulation permettant aux équipes de sécurité de s'entraîner, de développer leur expertise, et de gérer la planification de leurs ressources humaines ». Il s'agit donc de répliquer un environnement réel pour y éprouver et développer des compétences « telles que test d'intrusion, protection du réseau, durcissement de systèmes, modélisation de menaces et réponse à incident », mais également pour développer l'implication d'autres populations de l'entreprise susceptibles d'être concernées par la gestion d'incidents.

Dans ce guide

- Comment le cyber-range s'impose peu à peu dans l'entreprise
- Le cyber-range, une plateforme de simulation pour entraîner ses équipes
- Formation : immersion dans les méthodes des cyber-attaquants avec BlueCyForce
- Airbus CyberSecurity trouve des usages multiples à son cyber-range
- Accéder à plus de contenu Pro+

Un environnement aux usages multiples

En outre, un cyber-range peut aider à tester de nouveaux produits et contrôles de sécurité face à des attaques simulées dans un environnement maîtrisé, confiné, voire mettre à l'épreuve des candidats à l'embauche.

Dans ce contexte, Gartner recommande aux entreprises d'évaluer la pertinence du recours à un cyber-range à l'aune de leurs pratiques internes, des approches possibles pour combler les manques de compétences, pour enfin déterminer les éventuels cas d'usage susceptibles de justifier les coûts induits et les gains de résiliences.

Car selon le cabinet, à ce jour, « les cyber-ranges impliquent des coûts et un investissement opérationnel importants ». C'est d'ailleurs sans surprise que « beaucoup d'organisations utilisent des prestataires de services tiers pour accéder à un cyber-range en mode service ». Les offres en la matière ne manquent d'ailleurs pas de se développer. En France, on peut ainsi penser à Airbus Cybersecurity, BlueCyForce, ou encore Cyber Test Systems.

Gagner en « dextérité numérique »

Mais les bénéfices à l'utilisation d'un cyber-range ne sont pas négligeables. Pour Gartner, il s'agit avant tout de gagner en « dextérité numérique ». Le

Dans ce guide

- Comment le cyber-range s'impose peu à peu dans l'entreprise
- Le cyber-range, une plateforme de simulation pour entraîner ses équipes
- Formation : immersion dans les méthodes des cyber-attaquants avec BlueCyForce
- Airbus CyberSecurity trouve des usages multiples à son cyber-range
- Accéder à plus de contenu Pro+

cabinet définit ce concept comme « la capacité et la volonté d'exploiter des technologies existantes et émergentes pour obtenir de meilleurs résultats métiers ».

Et justement, selon Sam Olyaei et Matthew Stamper, les analystes à l'origine de la note d'information du cabinet, un cyber-range peut servir de socle à « une practice de cybersécurité proactive, agile et digne de confiance » en répondant aux besoins de sécurité induits par « de nouveaux modèles technologiques ». Car il « aide à développer des équipes dotées des compétences nécessaires à la sécurisation et à l'exploitation de plateformes requises pour constituer une organisation résiliente ».

Au passage, les exercices conduits sur un cyber-range peuvent aider à renforcer la sensibilisation en interne, là où d'autres méthodes auraient échoué. Le tout grâce à des sessions interactives reproduisant des scénarios bien réels : « cela peut influencer la culture de l'organisation pour la rendre plus consciente du risque ».

Définir ses attentes

Sam Olyaei et Matthew Stamper soulignent que l'une des valeurs clés d'un cyber-range est sa capacité à répliquer un environnement de production et/ou à valider l'impact de nouvelles technologies. Et cela ne veut pas

Dans ce guide

- Comment le cyber-range s'impose peu à peu dans l'entreprise
- Le cyber-range, une plateforme de simulation pour entraîner ses équipes
- Formation : immersion dans les méthodes des cyber-attaquants avec BlueCyForce
- Airbus CyberSecurity trouve des usages multiples à son cyber-range
- Accéder à plus de contenu Pro+

simplement dire environnement IT, mais également environnement mixte IT/OT pour tenir compte des systèmes industriels.

Surtout, « pour assurer l'usage réussi d'un cyber-range, il convient d'établir ses attentes et ses besoins ». Le sujet apparaît d'autant plus important que, selon les analystes, pour les cyber-range en mode service, la facture s'établit généralement « par utilisateur et par module, et peut aller de 50 000 $ à 200 000 $ ». Pour un déploiement interne, dans une grande organisation – « dotée typiquement d'au moins 30 professionnels de la sécurité à temps plein » –, il faut compter « entre 500 000 $ et 1,5 M$ ». A ce prix-là, pas question de rater son projet.

Dans ce guide

- Comment le cyber-range s'impose peu à peu dans l'entreprise
- Le cyber-range, une plateforme de simulation pour entraîner ses équipes
- Formation : immersion dans les méthodes des cyber-attaquants avec BlueCyForce
- Airbus CyberSecurity trouve des usages multiples à son cyber-range
- Accéder à plus de contenu Pro+

Formation : immersion dans les méthodes des cyber-attaquants avec BlueCyForce

Valéry Marchive, Rédacteur en chef adjoint

BlueCyForce n'est pas inconnu des participants du Forum International de la Cybersécurité. La société s'y était fait largement remarquer par ses démonstrations pour le moins frappantes. Mais l'entreprise, issue d'un partenariat entre CEIS – organisateur du FIC – et Diateam, est connue au-delà. Sa spécialité ? Former à la lutte contre les attaques informatiques, à tous les niveaux, depuis les dirigeants jusqu'aux ingénieurs en cybersécurité appelés à travailler à l'exploitation d'équipements de sécurité, dans les SOC, ou encore dans les équipes de réponse à incidents.

Début octobre, BlueCyForce organisait l'une de ces sessions de formation, pour une dizaine de personnes aux profils variés. On trouvait là des ingénieurs sécurité, des développeurs de logiciels de gestion de la sécurité, et plus encore. Pour beaucoup, cette session était une recommandation de leur hiérarchie. Avec des objectifs aussi divers que les profils : rafraîchir leurs compétences opérationnelles, découvrir des points d'amélioration de leurs outils et de leurs configurations, valider la session pour la suggérer ensuite à des clients Pour certains, la session, dite Opsec 1, est apparue très vite comme particulièrement motivante.

Dans ce guide

- Comment le cyber-range s'impose peu à peu dans l'entreprise
- Le cyber-range, une plateforme de simulation pour entraîner ses équipes
- Formation : immersion dans les méthodes des cyber-attaquants avec BlueCyForce
- Airbus CyberSecurity trouve des usages multiples à son cyber-range
- Accéder à plus de contenu Pro+

Le point de vue de l'attaquant, par la pratique

D'abord, il y a le style particulier de Guillaume Prigent, jamais avare d'une explication ou d'une illustration tirée de l'actualité. Il offre généreusement aux participants son expérience, ses compétences et ses connaissances. Et pas question de prendre qui que ce soit de haut : il n'est pas question de courir le risque de perdre qui que ce soit en route.

Certes, cette session n'est qu'un tronc commun préalable à la suite, Opsec 2. Une sorte de mise en condition des participants et de sensibilisation, tant aux outils fréquemment utilisés par les attaquants, que ceux des défenseurs. Mais elle n'en est pas moins riche en apprentissages, par la pratique. Pour certains participants, c'est d'ailleurs une spécificité plus que rafraîchissante, par rapport à d'autres formations, dont certaines certifiantes, en comparaison jugées « trop théoriques ».

Il faut dire que beaucoup de thèmes sont couverts : depuis la collecte de renseignements en sources ouvertes, à l'implantation de reverse-shell sur une machine cible compromise, en passant par l'exploitation de vulnérabilités sur un site Web, sous Wordpress, jusqu'à la détonation de maliciels dans le célèbre bac à sable Cuckoo. Et tout cela, toujours, par la pratique.

Dans ce guide

- Comment le cyber-range s'impose peu à peu dans l'entreprise
- Le cyber-range, une plateforme de simulation pour entraîner ses équipes
- Formation : immersion dans les méthodes des cyber-attaquants avec BlueCyForce
- Airbus CyberSecurity trouve des usages multiples à son cyber-range
- Accéder à plus de contenu Pro+

Et les bonnes raisons à une telle approche sont faciles à trouver. La mise en pratique de metasploit permet par exemple de mesurer à quel point les outils de piratage – efficaces – sont accessibles à tous, et de comprendre pourquoi ceux que l'on appelle les *scripts kiddies* sont appelés à se multiplier. Certes, lancer une attaque ciblée à grand renfort de vulnérabilités inédites, les fameux *0 days*, n'est toujours pas à la portée de tout le monde. Mais détourner une instance Wordpress non tenue à jour par ses propriétaires s'avère d'une facilité déconcertante. Et cela peut s'avérer suffisant dans bien des cas. Sur Internet, cela ne fait aucun doute, il n'est pas si difficile de disposer d'un réel pouvoir de nuisance.

Comprendre la menace, pour mieux la contrer

Mais alors pourquoi se mettre à la place des cyber-délinquants et de leurs méthodes de collecte de l'information ?

Parce qu'à bien y réfléchir, ce pourrait bien être la première chose à faire pour défendre son infrastructure : assurer un suivi régulier de l'exposition de son entreprise – personnes et systèmes – sur Internet. De fait, gérer ses vulnérabilités, c'est d'abord les connaître. Equifax a, à ce titre, reçu un douloureux rappel à l'ordre

Dans ce guide

- Comment le cyber-range s'impose peu à peu dans l'entreprise
- Le cyber-range, une plateforme de simulation pour entraîner ses équipes
- Formation : immersion dans les méthodes des cyber-attaquants avec BlueCyForce
- Airbus CyberSecurity trouve des usages multiples à son cyber-range
- Accéder à plus de contenu Pro+

Mais ce n'est pas tout. Les équipements capables de bloquer les attaques DDoS existent. Ceux susceptibles d'identifier des tentatives d'injection SQL aussi. Mais encore faut-il les avoir déployés, qu'ils soient bien configurés, et leur accorder tout le suivi qu'ils méritent. Et là encore, la démonstration est édifiante. La compromission du serveur Web par le biais d'une injection SQL ? Le pare-feu de nouvelle génération déployé dans l'environnement d'entraînement l'a détectée. Même chose pour la recherche de vulnérabilités. De même que les sondes Suricata. Mais encore fallait-il suivre et prendre au sérieux leurs alertes...

Au sortir de cette journée d'entraînement, les participants sont assurément ressortis avec un regard aiguisé sur les cartes que les attaquants ont dans leurs manches... mais aussi sur celles qu'ils tiennent dans leurs mains. Un regard en forme d'éveil, peut-être même de prise de conscience, sur ce qu'il est possible, voire indispensable, d'améliorer, sinon tout simplement de mettre en place, pour mieux se protéger contre des attaques qui ne sont certainement pas appelées à disparaître.

Dans ce guide

- Comment le cyber-range s'impose peu à peu dans l'entreprise
- Le cyber-range, une plateforme de simulation pour entraîner ses équipes
- Formation : immersion dans les méthodes des cyber-attaquants avec BlueCyForce
- Airbus CyberSecurity trouve des usages multiples à son cyber-range
- Accéder à plus de contenu Pro+

Airbus CyberSecurity trouve des usages multiples à son cyber-range

Valéry Marchive, Rédacteur en chef adjoint

Cela fait plusieurs années qu'Airbus CyberSecurity développe sa plateforme de simulation d'incidents de sécurité informatique, son cyber-range, initialement pour répondre à ses besoins de sensibilisation et formation internes, ou encore organiser des « challenges » de sécurité des systèmes d'information. Mais la plateforme est depuis arrivée à maturité et Airbus CyberSecurity a commencé à en étendre les cas d'usage.

En septembre dernier, le groupe a ainsi annoncé des partenariats avec l'IMT Atlantique, l'ESIEA Paris-Laval, l'Efrei, et l'Insa Centre-Val de Loire. Là, explique Frédéric Julhes, directeur France d'Airbus CyberSecurity, la plateforme est mise à disposition pour permettre, notamment, la mise en place de travaux pratiques avec les étudiants. Le groupe peut aider à l'exploitation, apporter son expertise sur certains cursus, mais également profiter des retours de ses partenaires pour faire ses propres scénarios d'exercices. L'objectif principal est bien d'aider à la formation de recrues talentueuses, en pleine pénurie de ressources qualifiées. Qu'elles soient embauchées ensuite par Airbus ou par d'autres importe finalement moins que d'augmenter la disponibilité de profils toujours très recherchés.

Dans ce guide

- Comment le cyber-range s'impose peu à peu dans l'entreprise
- Le cyber-range, une plateforme de simulation pour entraîner ses équipes
- Formation : immersion dans les méthodes des cyber-attaquants avec BlueCyForce
- Airbus CyberSecurity trouve des usages multiples à son cyber-range
- Accéder à plus de contenu Pro+

Et l'intérêt n'est pas limité là à la formation initiale. Alors que les entreprises sont appelées à convertir d'autres profils à la cybersécurité, les besoins de sensibilisation et de formation, voire d'entraînement, ne font que se développer. Et même les spécialistes, les RSSI, peuvent profiter d'exercices pour rester à niveau dans un environnement où « tout bouge très vite ».

Construire des modèles au plus près du réel

Comme le souligne Eric Chambareau, directeur intégration et entraînement d'Airbus CyberSecurity, avec un cyber-range, pas question de verser dans la formation traditionnelle, théorique, voire parfois quelque peu hors-sol. L'objectif, « c'est de modéliser un système d'information qui correspond au métier du client, pour y créer des exercices sur-mesure ». Le tout pour aboutir à des scénarios aussi plausibles que possible. C'est ce que ses équipes font notamment avec Alstom.

Bien sûr, « il ne faut pas croire que cela se fait en deux jours ». Mais c'est toute la force d'une plateforme de cyber-range : à chaque fois que quelque chose de nouveau est créé pour un scénario, cela vient alimenter une bibliothèque de composants qui pourront être déclinés, personnalisés. Les composants sont donc réutilisables ; ce sont les cas d'usage qui sont personnalisés. Et avec le temps, plus la plateforme est utilisée, « plus il est aisé de créer des scénarios ».

Dans ce guide

- Comment le cyber-range s'impose peu à peu dans l'entreprise
- Le cyber-range, une plateforme de simulation pour entraîner ses équipes
- Formation : immersion dans les méthodes des cyber-attaquants avec BlueCyForce
- Airbus CyberSecurity trouve des usages multiples à son cyber-range
- Accéder à plus de contenu Pro+

Ce n'est pas tout. Pour coller aux métiers des clients, encore faut-il les comprendre. Afin de répondre aux besoins spécifiques dans le domaine des systèmes de contrôle industriel (ICS/Scada), Airbus CyberSecurity a donc embauché l'an passé trois automaticiens.

Frédéric Julhes relève en outre que le cyber-range permet d'aller au-delà de la seule formation et de l'entraînement, sur le terrain du test. Ainsi, en réponse à des demandes de clients, Airbus CyberSecurity a utilisé sa plateforme de simulation pour étudier au plus près les offres d'une dizaine de spécialistes de la sécurisation des environnements industriels : « cela permet de vérifier les forces de chacun et les complémentarités ».

Une plateforme développée en interne

Pour son cyber-range, Airbus CyberSecurity s'appuie sur Lade, une plateforme développée en interne sur une couche de virtualisation VMware, avec ouverture prévue sur les environnements de production cloud. Eric Chambareau explique que le groupe avait commencé par utiliser KVM, mais ce dernier a vite montré ses limites « pour la montée en charge. Et aujourd'hui, nous voulons intégrer les objets connectés, ce qui induit des scénarios avec un grand nombre de composants ». Tous ne sont d'ailleurs pas intégrés sous la forme de machines virtuelles, mais également sous celle de micro-services Docker.

Dans ce guide

- Comment le cyber-range s'impose peu à peu dans l'entreprise
- Le cyber-range, une plateforme de simulation pour entraîner ses équipes
- Formation : immersion dans les méthodes des cyber-attaquants avec BlueCyForce
- Airbus CyberSecurity trouve des usages multiples à son cyber-range
- Accéder à plus de contenu Pro+

Le choix de VMware répond également à un besoin d'industrialisation : « nombre des partenaires avec lesquels nous travaillons, comme Cisco, Palo Alto Networks ou encore Stormshield, proposent leurs produits directement sous la forme d'appliances virtuelles avec images pouvant être instanciées directement, sans conversion », explique Eric Chambareau.

Le cyber-range d'Airbus CyberSecurity est proposé en trois capacités nominales, supportant de 4 à 48 utilisateurs, de 75 à 300 machines virtuelles, et de 2 500 à 10 000 conteneurs Docker. La version la plus modeste ne supporte que 4 environnements de jeux indépendants, auxquels sont rattachés individuellement les participants, contre 16 pour la version la plus musclée. Le catalogue d'attaques s'étend de 30 à 100 modèles selon les versions. Les deux versions à la capacité la plus élevée embarquent en outre un centre opérationnel de sécurité (SOC) virtualisé.

Le cyber-range embarque donc un générateur de trafic malicieux logiciel. Mais un générateur matériel, optionnel, est nécessaire pour les exercices impliquant domaines et sites Web malicieux ou encore menaces et maliciels émergents. Le générateur de trafic matériel est en outre plus efficace pour les simulations d'attaques en déni de service.

Comment le cyber-range s'impose peu à peu dans l'entreprise

Le cyber-range, une plateforme de simulation pour entraîner ses équipes

Dans ce guide

- Comment le cyber-range s'impose peu à peu dans l'entreprise
- Le cyber-range, une plateforme de simulation pour entraîner ses équipes
- Formation : immersion dans les méthodes des cyber-attaquants avec BlueCyForce
- Airbus CyberSecurity trouve des usages multiples à son cyber-range
- Accéder à plus de contenu Pro+

Formation : immersion dans les méthodes des cyber-attaquants avec BlueCyForce

Airbus CyberSecurity trouve des usages multiples à son cyber-range

Accéder à plus de contenu exclusif PRO+

Vous avez accès à cet e-guide en tant que membre via notre offre PRO+ : une collection de publications gratuites et offres spéciales rassemblées pour vous par nos partenaires et sur tout notre réseau de sites internet.

L'offre PRO+ est gratuite et réservée aux membres du réseau de sites internet TechTarget.

Profitez de tous les avantages liés à votre abonnement sur: http://www.lemagit.fr/eproducts

Images; stock.adobe.com