Zeitschrift: Revue Militaire Suisse
Band: - (2015)
Heft: 2

Artikel: Red Teaming : Un point de vue équilibré
Autor: [s.n.]
DOI: https://doi.org/10.5169/seals-781253

MH-53 du 20e escadron expéditionnaire des opérations spéciales survolant l'Irak lors de leurs dernières missions de combat, le 27 septembre 2008.

Cyber

Red Teaming: Un point de vue équilibré

Red Team Journal

Défini vaguement, l'équipe rouge est la pratique de la visualisation d'un problème d'un point de vue contradictoire ou contrariante. Alors que certains red teamers définissent la pratique de façon plus étroite ou plus large, presque tous s'accordent à dire qu'un red team doit jouer ou modeler l'attaquant, l'adversaire, ou simplement jouer à l'avocat du diable.

L'objectif de la plupart des *red teams* est d'améliorer la prise de décision en remettant en cause les hypothèses et explorer de nouvelles idées, généralement depuis la perspective d'un adversaire ou d'un concurrent. Un red team, par exemple, pourrait jouer le rôle d'un attaquant et tester la sécurité d'un système. Il pourrait également examiner et évaluer les hypothèses d'un plan stratégique d'entreprise. Si un *red team* adopte un point de vue spécifique, la méthode ou la boîte à outil dépend de la nature du problème et les circonstances dans lesquelles il se trouve. Un *red team* qui effectue un type de tâche à plusieurs reprises est susceptible de développer un cadre de processus et une boîte à outils associée.

Avantages

Les *red teams* qualifiés offrent à un décideur plusieurs avantages potentiels. Le plus important pouvant être la capacité d'identifier une décision-piège qui autrement aurait été négligée ou sous-estimée. Ce piège peut être dans un système ou un processus vulnérable, une préférence de l'adversaire ou la capacité d'un concurrent qui n'auraient pas été envisagés. Etroitement liée à cet avantage, un *red team* expérimenté a la capacité de mettre en exergue les oeillères, idées préconçues et préjugés d'un décideur. Enfin, un bon *red team* emploiera une vue des systèmes afin d'aider à révéler les aspects et connexions cachées. Ce dernier avantage est particulièrement important lorsque ces aspects et connexions représentent des faiblesses exploitables avec des possibles effets non linéaires.

Dans la pratique, ces avantages ont tendance à être démontré de façon anecdotique. C'est à la fois une force et une faiblesse. C'est une force parce que ces anecdotes et histoires sont une méthode puissante de communiquer des expériences, principes et leçons. Entre autres, elles parlent directement à nos doutes et appréhensions. Les anecdotes des red teams les plus persuasives illustrent le désastre évité (en raison de la diligence du *red team*). Il n'est donc pas surprenant que les organisations ne les partagent pas volontiers. Toutefois, les démonstrations anecdotiques sont aussi une faiblesse. Dans une ère de budgets serrés, les décideurs veulent des chiffres : « Combien est-ce qu'un *red team* va m'économiser ? » demande le client potentiel. C'est une question extrêmement difficile à répondre, en partie parce qu'elle implique une chaîne de « si » qu'un *red team* ne peut évidemment pas résoudre.

Limites et contraintes

Malgré les nombreux avantages d'un *red team*, tout honnête soit-il, la pratique est soumise à diverses limitations et contraintes. Un *red team* ne peut pas prédire avec certitude ce que l'adversaire va faire et il ne peut pas découvrir toutes les faiblesses possibles dans un concept, un plan ou système. Les *red teams* qui prétendent ces capacités surestiment leurs compétences et inévitablement trompent leurs clients. Les décideurs qui tentent d'utiliser un *red team* afin de deviner les événements spécifiques risquent de faire pire que de ne rien faire. En outre, peu de *red teams* travaillent gratuitement ; quelqu'un doit les payer, et ce quelqu'un est habituelle-ment plus intéressé à sa propre organisation, système, plan ou mandat. Cependant les adversaires du monde réel ont tendance à penser aux organisations, systèmes, plans et mandats comme un ensemble. Cela signifie que dans certains cas un client dirigera un *red team* afin d'adopter une vision qui est plus étroite que celle de ses adversaires potentiels. Les *red teams* inférieurs ne parviennent pas àé détecter ces contraintes et travaillent

strictement dans une zone définie (ne sachant rien faire d'autre) ; les *red teams* supérieurs font de leur mieux pour travailler dans et autour de la tension. En fait, un *red team* supérieur saisira l'occasion de divulguer les dépendances problématiques qui émergent des contraintes liées aux clients.

Red teams supérieurs et inférieurs

De toute évidence, différents *red teams* ne sont pas égaux. Par exemple, les *red teams* supérieurs ont tendance à :

- Voir le problème en question d'un point de vue systémique ;
- Mettre en évidence les préjugés culturels des décideurs et, le cas échéant, adopte le point de vue culturel de l'adversaire ou du concurrent ;
- Employer une gamme pluridisciplinaire de compétences, talents et méthodes ;
- Comprendre comment les choses fonctionnent dans le monde réel ;
- Eviter des explications absolues et objectives des comportements, préférences et des événements ;
- Tout questionner (incluant leur client et eux-même) ;
- Casser les « règles ».

On peut dire que les meilleurs *red teamers* sont nés, pas formés. Il semble que certaines personnes ont une capacité instinctive au *red teaming* tandis que d'autres, malgré une formation approfondie, ne peuvent jamais échapper à la sécurité qu'apporte le conventionnel. En fait, ceci est peut-être la caractéristique principale d'un *red team* inférieur: une incapacité ou le refus de dépasser les lignes. Les *red teams* inférieur ont également tendance à :

- Accepter sans remettre en question la description du problème du client ;
- Embrasser les biais inhérents à leurs propres valeurs et culture ;
- Adopter la première ou la réponse la plus facile ;
- S'en remettre à la réputation ou au statut ;
- Tout savoir.

Curieusement, dans les deux cas, un manque de confiance ainsi qu'une arrogance incontrôlée peuvent nuire aux red teams. Les membres d'un *red team* inférieure pourraient inclure des technocrates déférents ainsi que des experts indépendants vaniteux.

Résistance

Pas tous les décideurs souhaitent un *red team* (ou du moins un *red team* honnête). Un *red team* peut miner les stratégies privilégiées d'un décideur ou remettre en cause ses choix, politiques et intentions. Il faut un décideur à l'intégrité solide pour parrainer, habiliter et gérer un red team supérieure. Cela dit, un décideur réfléchi mesure les coûts et avantages de *red teaming* avec les coûts et avantages des plaidoyers, compromis et consensus nécessaires. Il est également important de noter que toute résistance n'est pas nuisible ; elle peut représenter des intérêts valides, des préoccupations et des risques dont le *red team* n'est tout simplement pas au courant.

« To *Red Team* or Not to *Red Team* »

Presque tout le monde peut bénéficier d'une certaine forme ou d'un degré d'un *red team*. Que le *red team* soit une unité formelle et structurée ou un avocat du diable autoproclamé, presque chaque idée, concept, design ou plan bénéficiant d'une opposition ou de tests est gage de bonne santé. Trop de *red teaming* cependant peut être aussi néfaste que trop peu. Personne ne veut d'un implacable contradicteur gommant chaque phase d'un projet. Il ne sera pas long avant que tout le monde se mette à le rejeter comme une nuisance.

Les décideurs doivent veiller à appliquer judicieusement un *red team*. D'autres facteurs comme la synchronisation sont particulièrement importants. L'établissement d'un *red team* trop tôt peut conduire à des tergiversations sans but ; l'établir trop tard peut déclencher une résistance farouche (et justifiable). Ainsi, l'adage « mieux vaut tard que jamais » peut parfois s'appliquer. Si un adage devait toujours s'appliquer au red teaming, il serait « une taille [ne peut pas] convenir à tous. » Tout cela défie le décideur et le red teamer qui vont devoir réexaminer et reconsidérer le contexte des activités du red team tout au long du cycle de vie de l'effort.

Il est également important d'examiner et d'évaluer la perspective de toutes les parties prenantes du client. Pas tous les problèmes ont une frontière distincte délimitée par un seul point de vue impartial. Souvent la caractéristique primordiale d'un problème complexe est l'enchevêtrement imprécis, contradictoire et confus des relations et préoccupations entre les différents acteurs. Plus le problème est grand, plus le défi l'est aussi. En effet, ceci peut expliquer pourquoi les initiatives au niveau national bénéficie rarement d'un red team honnête. Les *red teams* doivent éviter de servir de complices à un parti pris lorsqu'ils travaillent sur des problèmes complexes de ce genre.

En résumé, la décision de quand et comment utiliser un *red team* peut être étonnamment complexe. La suppression d'un *red team* dans une situation politique très chargée peut saper la confiance et éroder un consensus durement gagné. De même, *red teamer* une décision lors de son implémentation peut soulever plus de questions que de réponses, saboter le moral et inciter un décideur à inutilement remettre en question de bonnes décisions. D'autre part, mettre un *red team* expérimenté sur un problème ou système au bon moment, avec le mandat approprié, peut guider un décideur loin d'une catastrophe qui l'attendrait autrement.

R.T. J.

Cet *article initialement publié en anglais dans le* Red Team Journal *datant du 14 février 2013. Traduction: Yves Garcia.*