Cyberdefense: The human factor at the center of operational efficiency — testing defenses is indispensable for making progress

Vincent Riou,
Associate director Cybersecurity, CEIS

Abstract:
To improve our defenses and cope with cybermenaces, is it worthwhile to continually lay out more funds while piling up solutions sold as "miracles" for the computerized infrastructure? Of course not. In a context of totally asymmetrical cyberwarfare, the human factor should be placed back at the center of cybersecurity arrangements: testing operations by red teams, training operational and managerial teams, adopting misleading strategies to deceive the enemy, raising the personnel's awareness of cyberthreats…. Know your enemy and know yourself — the very basis of the art of warfare.

How does it happen that a combination of the best technology for detecting and preventing attacks along with the best sources of cyberthreat intelligence (CTI), all of this used by a team devoted to defending an information system, fails, again and again, to halt advanced attacks? How can it be that the number of massive data thefts is exploding even though cybersecurity budgets have continuously risen? The answer is simple. In a context of totally asymmetric cyberwarfare, the defender fails even if, after having stopped thousands of attacks, he leaves just one take place. In contrast, the attacker, after having been blocked hundreds of times, wins if a single attack is successful. The game is skewed.[1]

So, is it worthwhile raising, again and again, the budget for cybersecurity and accumulating on a network the "magic toolkits" hyped by software editors? As shown by the number of companies that have experienced a major attack despite the millions of euros spent on security tools, spending more does not limit risks. It is necessary to spend better. To be convinced, hire a red team and watch where it penetrates your network (for sure, not through an armored gateway!), how its members move laterally while erasing their tracks and tricking the magic toolkit acquired at great expense… all this without being detected even once by your security operation center (SOC). During these tests by the red team, SOC receives dozens, even hundreds, of alerts; but most of them are false positives, decoys wittingly orchestrated by the attacking forces to "ring" the SOC and draw its attention away from the zones that will bear the brunt of the attack. These false positives wear down work teams, causing fatigue and a loss of attention and motivation, which inevitably makes ineffective a setup that is supposed to handle advanced attacks.

Here is the question we need to ask: before reinvesting in new wonder-working tools might it not be high time to learn to use to their full capacity the means already in our hands? The importance of drilling the troops, of training, of knowing one's strengths and weaknesses, of

[1] This article has been translated from French by Noal Mellott (Omaha Beach, France).

anticipating the enemy's strategies, dissimulating, using decoys, baiting… it's all in *The Art of War*, a book oft mentioned but seldom applied.

Testing yourself

Rather than following general normative principles, cybersecurity has to be envisioned from the attacker's viewpoint (the red team, operational training, emergency drills). This requires that the organization has the courage to put itself to the test — this is the key to success.

A successful cyberattack has serious consequences: a tarnished image, financial loses, ransom, data theft, business at a standstill, and even major dangers for the population when the attack has targeted a sensitive infrastructure. No statistics are needed at this point (they are available elsewhere). This article seeks to explore a fundamental approach — testing and training — for circumscribing the phenomenon.

At a first level, awareness campaigns in firms enable employees, regardless of their technical competence, to learn the basic behavior patterns to be adopted. ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information) has called this "information system hygiene". As with health and safety rules, regular training is required to create automatic reflexes. Recurrently scheduling cybersecurity exercises for a large proportion of the work force will help raise employee awareness. The worth of an employee forewarned is doubled; and most of the costs of staging such exercises are amortized due to lower risks, since the right reflexes will have been ingrained throughout the firm.

The training of cybersecurity professionals in firms or service-providers must, of course, go much farther. To acquire and retain the reflexes indispensable for their profession, these employees must undergo permanent training. To draw a parallel with physical security, we cannot imagine specialized forces of intervention leaving on a mission without intensive training so that their reflexes are extremely effective in the field. They will evaluate all possible behaviors an attacker might adopt and prepare a counteroffensive. When faced with a large-scale attack, the teams that respond to incidents in information systems must, in like manner, be prepared. More than emergency instructions, they have to have emergency reflexes.

Education vs. training

What distinguishes training from education is its immersive nature. Whereas education enhances the person's theoretical credentials, training consists of placing people in a situation where the level of difficulty is correlated with the professional's level of skills. Whereas education teaches basic techniques in the cyberdefense toolkit, training enables defenders to master these techniques through practice in order to increase the quality and speed of execution and lessen stress in real-life situations. Training is what makes it possible to acquire vital reflexes in case of aggression and improve the effectiveness of reactions: "The more I practice, the luckier I get" in Arnold Palmer's words.[2]

[2] https://www.inc.com/kevin-daum/17-arnold-palmer-quotes-that-inspire-success.html.

Operational effectiveness does not depend just on the mass of knowledge that, often too theoretical, has been acquired. On the contrary, it comes out of reflexes that are learned only through intensive practice. The vocabulary and forms of action of cyberdefense are similar to those in the marshal arts: attack, defense, feints, anticipation, reflexes, endurance, stamina, etc. The parallel with the armed forces is evident: our soldiers must know weapons, tactics and operations like the back of their hands before leaving on assignment. This holds even more since the means used for cyberdefense — evolving in line with new attack techniques and technological progress — are becoming more complex and thus harder to master, whence a greater need for regular training.

We can draw a parallel to the qualities necessary for competitive sports, qualities that have to be acquired through regular training:

- Remain cool, calm and collected when an attack occurs. Tense contractions mean a loss of effectiveness. “Letting go” reduces pressure and stress, and fosters a state of mind that decreases reaction time and increases the quality of responses.
- Use adapted techniques: be supple and agile, and adapt to the situation. Responding to an incident calls for a broad range of techniques, as exhaustive as possible, that have to have been learned beforehand, prior to a major incident. Defense capacities have to be regularly updated through training and drills in a simulated environment.
- Lessen reaction time. Apart from experience in the field, only realistic training can help reduce reaction time. This reduction is crucial for improving the quality of responsiveness and limiting damages during an attack. Beyond theoretical knowledge, drills — the repetition of practices — automate reactions and turn them into “reflexes”.
- Encounter a variety of opponents. A boxer will not make any progress if he constantly trains with the same partner. If, on the contrary, he varies the training (punching balls, bodybuilding, mobile targets, different sparring partners, speed work, etc.), his learning curve will peak. The same holds for cyberdefense. Defenders must encounter a wide variety of attacks in different operational contexts, with different tools, in order to hone their senses and optimize their reactions (which should be, above all, human — though heavily dependent on technology).
- Focus attention. When an attack occurs, it is essential to look past the stimuli that parasite one’s attention, to manage efforts and react appropriately to commands passed along the decision-making chain. This is not learned in theory but in practice.

Besides these personal qualities, let us add the qualities related to team work, as occurs in cyberdefense. Each actor on the chain of defense has an assignment, specific to the person but complementary to the team. Let us draw a parallel to a rugby or football team. The qualities of individuals are summed by implementing team strategies, through solidarity and mutual support, the optimization of the decision-making chain, the placing of initiatives at the service of the group, the reporting, respect for roles and rules, etc.

To be effective, there must be regular — individual and group — training. Since cyberthreats are constantly evolving, specialists in this domain never remain experts for long if they rely on what they have already learned. Since cybercriminals are constantly developing new techniques of attack; it is necessary to be prepared to limit both the impact of surprise attacks and the damage wrought by attacks. Cyberthreat intelligence is essential, rightly so. However we must not be satisfied with taking into account the tactics and procedures used in past attacks. It is necessary to anticipate how the enemy will adapt them.

Education and training should be adjusted to the requisite level and needs, ranging from awareness campaigns to intensive training, from life-saving “first aid” in the case of aggression to the training of professional “cyberdefenders”. For education and training in cyberdefense, a firm might decide to set up in-house programs based on skills available within the company; or it might choose to rely on a professional training center (like Bluecyforce in France), which has adapted teaching methods as well as the means and equipment for immersing trainees in a realistic crisis situation. Adequate training implies having important means for augmenting the realism of an immersion. Effective progress is made only through action.

Let us return to the parallel with sports. To improve his performance, the amateur boxer enrolls at a gym that has all the equipment needed for him to practice: rings, sandbags, speedballs, punching bags, sparring partners, coaches and so forth. The courses will be adjusted to his level so that he advances from one stage to the next by encountering ever stronger opponents. All this will take place in a pleasant, recreational setting with physical challenges that put him under pressure and are followed with periods of relaxation, the goal being to improve his performance both mentally and physically. As much can be said for education and training in cyberdefense.

The ring and all the accessories for training? A closed, controlled environment with large network topologies, realistic streams of data and simulated information systems so that attacks of any level of intensity can be launched, in full security, without the risk of them going out of control.

The sparring partners? A red team of professional, ethical, experienced hackers whose attacks will be adjusted to the level of trainees. The goal is not to “knock them out” but, on the contrary, to help them progress.

The boxer’s fists, gloves, eyes and muscles? The set of technical means in an information system’s chain of defense: firewalls, WAF, SIEM, EDR, detection probes, forensic tools, etc. These means should not simply be implemented in the information system’s environment: they have to be mastered in a context as part of a coherent set.

To all this, let us add an essential training parameter: gaming. The goal of basing training on games is total immersion, to increase stress (which trainees have to learn to control), an immersion with stakes high enough to be worth defending. The quality of the proposed scenarios is essential to training, along with the complementarity of the profiles of the trainers of the future champions of cyberdefense.

Baiting the enemy

Testing defense teams against an experienced red team naturally leads to defining new strategies for responses. How to combat a furtive, agile enemy whose continual adaptations are not restricted by any legal or regulatory straitjacket? Since the law forbids counteroffensives, it is necessary to entrap the enemy. This concept underlies what has been called “deceptive cybersecurity”. Decoys, dissimulation, deception… are part of the array of countermeasures that are familiar in the circles of electronic warfare. We have to adapt them to cyberspace so that a passively defensive position based on actions of detection and remediation not allow attackers to move about untroubled. For the time being, “mature” firms believe they are sheltered behind high walls, but the enemy is learning to fly!

Training operational teams, exercises in emergency situations, and encounters with a red team are trials by fire, the only way to determine a cybersecurity strategy’s actual effectiveness, while making progress all along the line of defense.

Encounters, readaptations, not being satisfied with following norms, not trusting cybersecurity tools alone for one’s defense… humans are the core of operational effectiveness.