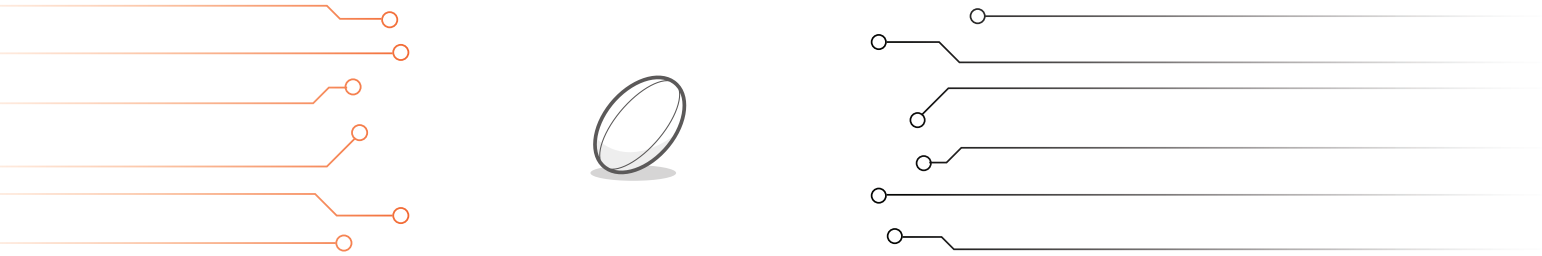
HOW RUGBY HELPS BUILD WINS IN CYBERSECURITY: RED TEAM APPROACHES



RUGBY: KEYS TO A SUCCESSFUL TEAM

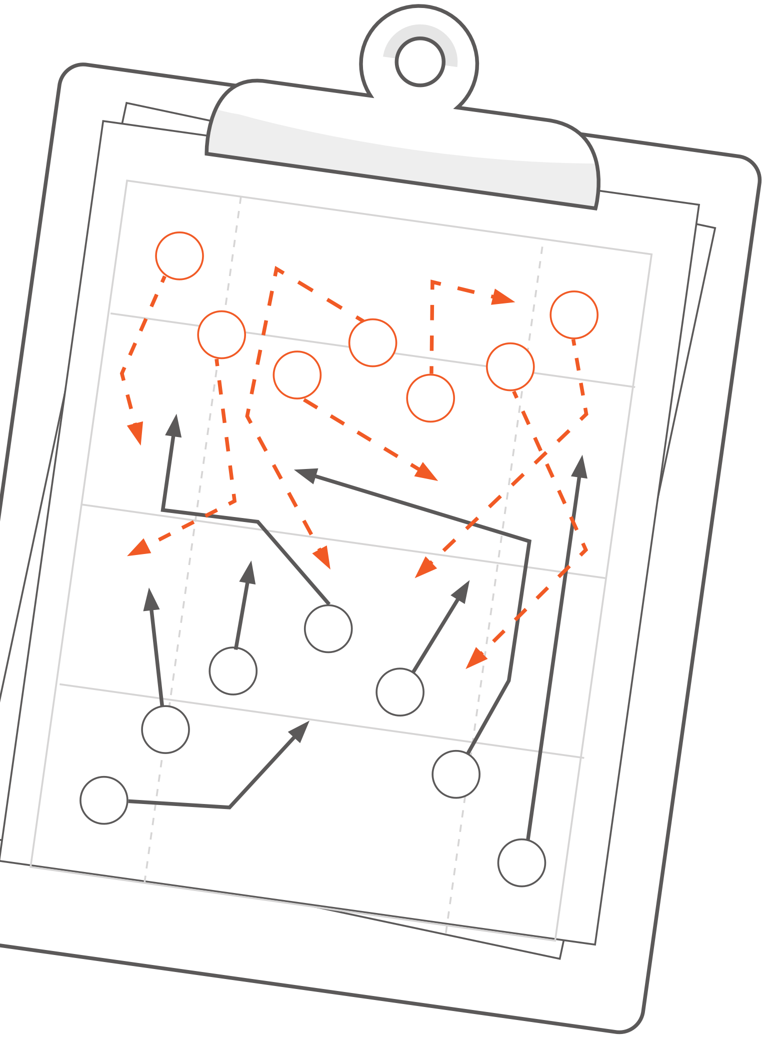
Rugby is one of the world's most popular, fast-paced, and aggressive games on the planet. Played at its highest level, it's a joy to behold and engages the fan to delirium, or despair, depending on which team wins and which one loses. Its success as a spectator sport is undoubted, and the Rugby World Cup is the world's third most watched sporting event, behind only the Olympics and FIFA Soccer World Cup.

There are several keys to rugby success. It starts with creating a program that has a culture of success, accountability, and selflessness. The ability to bring in top-notch coaches and other staff that reinforces the culture and live the team's values in all they do is another foundation of that success. And it is about the players tasked with implementing a game plan from the coach and adapting to the flow of the game and the myriad of approaches they face from the opposition. That adaptability, thinking on your feet, can be the difference between winning and losing, and it has very fine margins.

A few proven, winning formulas are the basis of rugby, and all successful international teams have these formulas at the core of what they can replicate, game in and game out, week in and week out. It varies but not by much.

Fast-paced, creative attack; physical, mobile, aggressive defense; playing for territory; solid to dominant set-piece.

HOW IS CYBERSECURITY LIKE RUGBY?



Ok. Now you've lost me, I hear many say (Bill Russell among them) but hear me out.

Think about Cyber Security and its critical elements. It starts with an attack, an attack that is targeted to overwhelm your defense. It's often based on a territory game where your territory is their threat environment. Bad intentions and a well-executed attack often overwhelm poor defensive shape. If your set-piece defense is weak or ill-prepared, the chances of a successful intrusion are significantly enhanced.

Let's break it down further. Think about the role of a "red-team" in the cybersecurity world. What's their goal? It's simply to create an attack strategy to overcome gaps in your defense. Your defense is based on people, tools, and systems and how they perform in a real-world environment, and the red-team wants to ethically threaten that. A successful red-team exercise is the best predictor of success for an organization as it allows them to build prevention, detection, and remediation capabilities under far less duress than a real-world threat. It doesn't lessen the need to be expeditious; it merely reduces the consequences.

HOW TO OVERCOME AND GROW FROM CYBER ATTACKS

So how do you overcome a fast-paced, creative, carefully crafted red-team attack? It's hard, and there will be many failures, or I prefer breakdowns before you stave off wave after wave of attacks and allow your defense to win out. The best way to build a defense in rugby is by watching video; red-team findings are the cybersecurity equivalent of video review. It's about capturing all the lessons learned from watching the attack and its methods and building a defensive game plan that is robust and agile to defend it.

The "blue-team" is the defense; their ability includes more than only defending against an attack. Some attacks are almost impossible to defend against with increasingly sophisticated and numerous attackers. But their ability to recognize the attack (Detection), adjust to the type of attack (Recognition), and then thwart the attack (Overcome) is critical in any organizations Cyber defense approach.

The territory aspect of Cyber comes down to where you want the battle to occur because it's going to happen. In rugby, we choose to play in the oppontents' half, so that even if they attack, they have a long way to go, and we have time and opportunity to disrupt their attack with the intensity and alignment of our defense. How many brick walls can they run into before they make a mistake? In Cyber, the territory is your perimeter and your ability to secure it. Hyperconnected networks mean that there is an increasing demand for Zero Trust Security, in essence, a network without a perimeter. Don't let them in. Regardless of their appearance, authenticate them constantly on the outside before they ever get inside. And if they do, challenge them again and again until they fail the challenge and make a mistake. The turnover ball is the best ball to turn defense into attack.

SET PIECE SUCCESS

It's your environment, and you must do anything to protect it. In rugby, it's all about the ball. You worked hard to get the ball, now use it effectively and don't be loose with it. As I said, a turnover ball is a really good ball. Don't allow for turnover opportunities. Your enterprise security is your set-piece. Build it right, and you can dominate, build it poorly, and you're subject to financial penalties and much more. The tools you select, the governance you implement, the people you hire, and the teams you build are all critical components of a solid set-piece. Get this right, make it adaptable, but don't deviate from your non-negotiables and your security posture is as safe as it can be in such a threatening landscape. Cut corners, and you will pay the price.

If you want more evidence, look no further than the Rugby World Cup final 2019, where South Africa's set piece laid the platform for a dominant performance from which England couldn't recover. Set-piece to the territory to attack overwhelmed a worn-out defense. Don't be England... well, at least on this occasion.