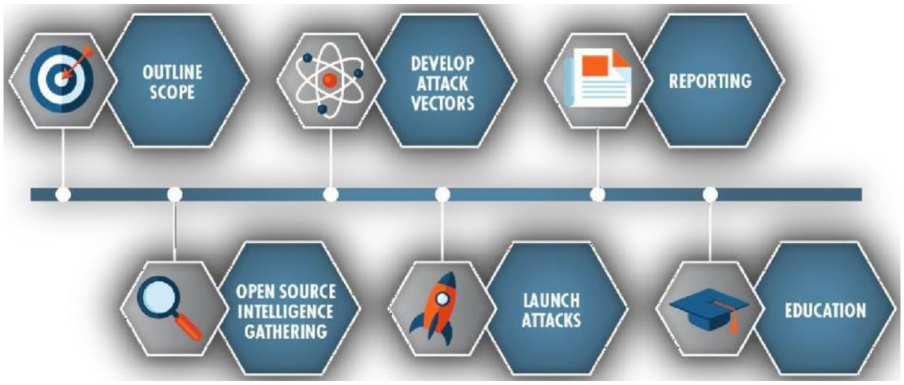
Test. Educate. Protect.
SOCIAL-ENGINEER

800.956.6065
www.social-engineer.com

Benefits of a Social Engineering Risk Assessment Engagement

Your company is important. Indeed, the data you hold for your clients or employees is very valuable and attackers seek to capitalize on that data any way they can. This is where a Social Engineering Risk Assessment (SERA) engagement can help uncover possible vulnerability to attackers.



Path of Least Resistance

When an attacker targets your company, they are looking for the easiest way to achieve their set goal. Typically, they will avoid the most complex paths if they can. Hopefully, your security awareness training is informing your users that the data they have access to is valuable and that they are in charge of protecting it. As defenders, we need to protect so many different paths to compromise but, as adversary simulators, we only need one, one good one, to get what we are after.

Finding that easiest path is the first goal of any attacker. Is it a vulnerability scan of your network? Will the attacker find misconfigured or unpatched services they can exploit? Maybe. If they identify one, that could be the entry point into your company network they are looking for. However, what if your network is fully patched, and locked down? Maybe many of the blinky lights in the data center are on devices that use machine learning to stop those network attacks. Well, then that is not the easiest path to compromise any more. What is the next path?

Focusing on the Human Element

The current digital landscape offers many opportunities for attackers. Without ever contacting you they can learn about you, your company, and your co-workers. How is this possible? Enter the world of Open-Source Intelligence (OSINT) gathering. This is a technique where anyone, not just attackers, can research an individual or organization and build up a dossier or profile. Based on the discovered information, the attacker can now customize and personalize meaningful attack scenarios. In fact, multiple researchers point out that phishing and vishing are close to, or are, the top methods for gaining an initial foothold in a coordinated attack against an organization or individual that result in security and data breaches

Knowing as much about a potential target as possible increases the success rate of the proposed attacks. Human vulnerabilities cannot be enumerated via a scan or a software appliance. That is where a SERA can provide the needed information that enables stakeholders of a security awareness program to make informed decisions. A SERA consists of a focused OSINT investigation on high-level or high-value targets within your organization. This is done to expose their possible vulnerabilities that could be used to facilitate a targeted attack. We combine this with a phishing and/or vishing component to make the point that this information could be a vulnerability that they may or may not be aware of. We perform this in a manner that will not leave the targets feeling embarrassed or victimized. Rather, we provide the targets with teachable moments. They learn an attacker's perspective about information and how it could possibly be used against them in a real-world attack.

Repeatable Deliverables and Verifiable Data

At the conclusion of a SERA, you receive a detailed report with easy-to-follow steps to re-create the OSINT investigation, to see the data for yourself, rather than just taking us at our word, that the data is freely available. In addition, if you elected for a simulated attack based on that data, you receive details about the actions taken by the chosen targets in order to better educate them on the events that occurred and the data that was used to facilitate the attacks. This is, in effect, the human vulnerability scan. Help protect your organization by talking to us about the benefits of a Social Engineering Risk Assessment engagement of your employees, so you have a clear, actionable picture of their exposure and possible vulnerabilities.

www.social-engineer.com