Security Control Cyber Range

I have been reading up on the concept of "Cyber Ranges". I've seen articles about how organizations are trying to set these concepts up with testing environments. These Cyber Ranges are promising to help train Cyber Warriors and Cyber Defenders, provide a technology testing environment for new Cyber technologies and even to help baseline normal processes, traffic and logging. But, I must wonder, is it really using the power of a Cyber Range to its full potential or not?

One of the things that is plaguing the Cybersecurity world is a true understanding of Cybersecurity as it pertains to an environment down to a Security Control level. Therefore, we continue to get taken as a Cybersecurity community from our adversaries. We are beholden to baselines and auditing, best practices and the limited knowledge of SMEs rather than the scientific process and evidence to help us create true Cybersecurity.

Now that last statement may seem accusatory or even arrogant. I don't mean it that way. What I mean is, we as Cybersecurity practitioners can NOT be experts in all technology, all the time. BUT, we CAN be an expert on the approach to Cybersecurity to ensure the process, evidence collection and the ability to "put it all together" for a purpose is met. This is true Cybersecurity Awareness and Resiliency (CAR).

So, how can a Cyber Range be used to develop Cybersecurity practitioners and their pursuit of expertise in process, evidence collection and the ability to "put it all together"?

We know Cyber Ranges are expected to be built like production environments. When an attacker "looks" at the environment he/she is trying to figure out weaknesses and vulnerabilities. They try different things. If they are successful with something, then they begin their exploitation. We can monitor them to look for patterns. After all, that is how we get threat intelligence. Identification of patterns. That is also how we fingerprint attribution. BUT, attackers are mostly opportunistic as well. I argue that can lead to false identification.

For instance, just like in a chess game, the black side reacts to the white side's first move. If White uses move A to open, the Black will use defense H not defense Z. Once Black uses defense H, White will not go to next move B but change to move M because he/she recognizes the defense H chosen by Black. That forces Black to use defense U instead of defense I. As you can see, if we were looking for pattern A, B, C to identify bad actor #1, we would not find it. Yet, bad actor #1 could be the attacker only reacting to what he or she finds. The attacker is opportunistic not fixed to their pattern. Similarly, defenders can be pattern matched or not as well.

In Cyber Ranges, we could change our approach. Instrument the entire environment so that we can see and log everything verbosely. Begin a cyber exercise. Monitor down to the security control level. That is, after all, the foundational building block to Cybersecurity. We can then analyze the effectiveness of the Security Control. The log analysis will help us to increase the effectiveness of

Security Control Cyber Range

security control implementation. Today we only assess (via baselines and audits) DID we implement the controls. We use Risk Management Framework to argue the elimination of Security Controls for convenience. BUT, we should really be implementing controls and the risk we are debating is the EFFECTIVENESS of the Security Controls.

By approaching Cyber Ranges this way, we can do some other intriguing things as secondary benefits. We could evaluate effectiveness of Security Controls as it pertains to Resiliency. We could evaluate effectiveness of Security Controls as it pertains to the design of a solution (think engineering practices). We could evaluate the effectiveness of Security Controls as it pertains to architecture. We could evaluate the approaches to monitoring Security Controls (think SOC processes). We could evaluate the performance of the defenders. This one is interesting because now we could map Security Personnel and their role in Cybersecurity to the NIST CWF down to the Security Control. This monitoring of Security Controls aligned to the defender allows us to evaluate the performance of the defender. We can analyze the true understanding of the defender to the Security Control. We can analyze their actions to see if they truly understand the intent and mechanisms of the Security Control and improve their ability to monitor it. This, of course, allows us to develop a training profile for the defender so that we can ensure they are growing and improving in their Cybersecurity role with a purpose, rather than an arbitrary training schedule. Additionally, we can use Security Control monitoring in a Cyber Range to validate security boundaries, nest Security Controls to increase effectiveness, or validate Security Controls in Supply Chain artifacts.

There is no end to the science of Security Control Cyber Ranges rather than the early incarnations of today's Cyber Ranges.

For Additional Information Contact:

Eigenspace
312 Main Street, Suite 300
Gaithersburg, MD 20878
240-654-4097
www.eigenspace.us