



BRIGHT MINDS

Q & A SERIES



DECEMBER 2021

Adversarial Simulation Is Proactive in a Reactive World

Itzik Kotler, ICIT Fellow
Co-Founder & CTO, SafeBreach

ICIT's Bright Minds Q&A Series

Adversarial Simulation is Proactive in a Reactive World

With Itzik Kotler, ICIT Fellow and Co-Founder and CTO, SafeBreach

December 2021

Copyright 2021 Institute for Critical Infrastructure Technology. Except for (1) brief quotations used in media coverage of this publication, (2) links to the www.icitech.org website, and (3) certain other noncommercial uses permitted as fair use under United States copyright law, no part of this publication may be reproduced, distributed, or transmitted in any form or by any means, including photocopying, recording, or other electronic or mechanical methods, without the prior written permission of the publisher. For permission requests, contact the Institute for Critical Infrastructure Technology.

About This ICIT Bright Mind Q&A:

In continued support of our mission to cultivate a cybersecurity renaissance that will improve the resiliency of our nation's 16 critical infrastructure sectors, defend our democratic institutions, and empower generations of cybersecurity leaders, ICIT has embarked on a journey to hold candid interviews with some of the brightest minds in national security, cybersecurity, and technology. Our goal is to share their knowledge and insights with our community to shed light on solutions to the technology, policy, and human challenges facing our community. Our hope is that their words will motivate, educate, and inspire you to take on the challenges facing your organizations.

About ICIT:

The Institute for Critical Infrastructure Technology (ICIT) is a 501c(3) cybersecurity Think Tank with a mission to cultivate a cybersecurity renaissance that will improve the resiliency of our Nation's 16 critical infrastructure sectors, defend our democratic institutions, and empower generations of cybersecurity leaders.

About this Bright Mind:

Itzik Kotler is CTO and Co-Founder of SafeBreach. Itzik has more than a decade of experience researching and working in the computer security space. He is a recognized industry speaker, having spoken at DEFCON, Black Hat USA, Hack In The Box, RSA, CCC and H2HC. Prior to founding SafeBreach, Itzik served as CTO at Security-Art, an information security consulting firm, and before that he was SOC Team Leader at Radware. (NASDAQ: RDWR).

About Adversarial Simulation

Organizations that only invest in reactive cybersecurity solutions are doomed to suffer the increasingly costly impacts of cybersecurity incidents. According to the [IBM Cost of a Data Breach Report 2021](#), this year the average data breach costs rose from USD 3.86 million to USD 4.24 million. In addition to the financial cost of remediation, breached organizations may face reputational harm, significant downtime, or the loss of sensitive data and intellectual property. Worse, their consumers and partners may be exploited or compromised. It behooves organizations to adopt a more proactive approach to cybersecurity such as "red-teaming" or adversarial simulation.

Adversarial simulations mimic the tools, tactics, techniques, and procedures of known and emerging attackers to find exploitable vulnerabilities in networks and mission-critical systems. In this Bright Minds Q&A, ICIT Fellow Itzik Kotler, Co-Founder and CTO, [SafeBreach](#), explains the basics and benefits of adversarial simulation and he expounds on why the proactive approach is essential for securing critical infrastructure.

ICIT:

How would you define adversarial simulation?

Kotler:

Adversarial simulation is taking the hacker's view and simulating attacks against your own infrastructure to discover security gaps and fix them before an adversary can breach your environment.

For best coverage, the attack simulations must cover the entire ecosystem, including cloud, web, endpoint, network, application, and email vectors. Critical to effective attack simulation is using a comprehensive attack playbook. Attack playbooks should be continually updated with newly discovered attacks including attacks and vulnerabilities published in US-CERT alerts, to test defenses against emerging and known threats.

The simulations must be built and executed such that no components in a production environment are ever at risk while attack simulations are run, and simulators must be lightweight to ensure that an environment's performance will not be affected.

ICIT:

What would you characterize as its key benefits?

Kotler:

Adversarial simulation helps security teams proactively identify security risk and make informed decisions to best protect their organization. It empowers teams to:

- Continuously validate & optimize the efficacy of cloud and on-prem security controls across the ecosystem
- Test security posture against emerging and known threats and discover and mitigate gaps before adversaries can exploit them.

Advanced simulation tool features can help:

- Prioritize and automate remediation of security gaps to efficiently mitigate risk
 - Measure and report security risk data to facilitate prioritizing and justifying security programs and projects
-

ICIT:

What kinds of data sources and inputs generate realistic adversarial simulations?

Kotler:

A comprehensive attack playbook is critical to effective simulations. Attack playbooks should be continually updated with newly discovered attacks including attacks and vulnerabilities published in US-CERT alerts. To achieve this, attack simulation research teams must externally monitor the hacker underground, source intelligence feeds, and collaborate with other external security research teams, including teams working on frameworks such as MITRE, to harvest the latest attack methods for simulations. These teams must also work to develop new attack methods -- before hackers craft them - to anticipate and simulate the hacker's next move.

ICIT:

How closely do adversarial simulations mirror real-world attack campaigns?

Kotler:

Attack simulations are based on real attacker techniques that span the range of the cyber kill chain, including infiltration, lateral movement, and exfiltration methods. Attacks in the wild are researched and broken into individual breach methods for simulation. For efficiency, this process is automated to allow for rapid development of new simulations in response to new attacks that appear in the headlines.

As an example, for a malware transfer simulation, an artificial malware transfer model is created using reverse engineering to mimic the behaviors of a malware attack sample, such as writing files, accessing registry keys, opening a socket, and attempting to communicate externally. On its own, this reverse engineered "malware transfer model" will not do any damage. To simulate a malware, download and drop attack, a real malware payload sample is added to the model and then executed from a "server" simulator to a "client" simulator to see if the malware is saved to disk or if security controls effectively defend against the attack and block the malware before it's saved to disk. After confirmation that the action is blocked or allowed, the sample is then removed.

Attacker remote attacks can also be simulated, such as Zerologon (CVE-2020-1472), RDP Bruteforce, and remote exploitation of Apache Struts server vulnerabilities. These remote attacks are kept safe by sending the malicious packets that the real exploit would have sent, but containing the impact to simulators, not actual in-production devices, or applications that the attack was meant to exploit. A security device such as an NIPS, IDS, or NBAD will still recognize the exploitation packets as malicious, but no harm will come to the production environment.

ICIT:

Are the simulations predominantly red-team, blue-team, or both?

Kotler:

Adversarial simulations are useful for both red teams and blue teams. Red teams benefit from a comprehensive suite of attacks that can be automated and customized to assess security posture more efficiently. Blue teams benefit because not only do attack simulations identify gaps in security, but advanced attack simulation tools also analyze the risk associated with an identified security issue and provide guidance to prioritize and remediate the gaps. Attack results can also be mapped to frameworks such as MITRE ATT&CK for reporting and tracking purposes. In addition, after remediation, rerunning an attack simulation can verify that the remediation was effective.

ICIT:

Do you experience resistance from cybersecurity stakeholders in undergoing or heeding the simulations? If so, why do you think stakeholders might be resistant and what steps can be taken to increase participation?

Kotler:

A big challenge for cybersecurity stakeholders is competing priorities. Stakeholders are challenged to secure digital business transformation initiatives, defend against emerging threats and demonstrate effectiveness of their security program all while staying within budget. Attack simulation is uniquely able to help stakeholders better prioritize and meet these challenges. Adversarial simulations can help evaluate the effectiveness of new and existing security technologies to defend against attack. They can also quickly test security posture against emerging threats, identify security gaps and prioritize and automate remediation. Stakeholders that understand the value that adversarial simulation provides recognize that adopting an adversarial simulation solution can help them better prioritize security projects and efficiently reduce cyber risk. Adversarial simulation tools are an emerging market, educating security professionals on the benefits of simulations will be key to increase participation.

ICIT:

Do you expect adversaries might evolve their tools, tactics, and procedures based on monitoring and simulation efforts?

Kotler:

Adversaries are persistent. There are many adversaries, many attack techniques and new attacks are continuously created. Adversaries' goal is to find gaps in security infrastructure. Attack methods that are successful are often repurposed against additional target organizations.

Attack methods that are not successful, may be less used or abandoned for a period of time. Organizations that practice attack simulation to proactively detect security gaps and optimize defenses will be able to better defend against attack.

ICIT:

How do you model against and adapt to emerging threats and malware whose behavioral patterns are not yet widely known?

Kotler:

Attack simulation methods are developed by dedicated teams of white hat hackers. New methods are created via external monitoring of the hacker underground, sourcing of intelligence feeds and collaboration with security research teams. Attacks in the wild are researched and broken down into individual breach methods. This process is automated for efficiency, allowing very quick creation of new attack simulations in reaction to attacks in the headlines.

ICIT:

Based on the lessons you have learned from countless simulations, from a blue-team perspective, what behaviors or solutions can best combat cyber-attack campaigns?

Kotler:

The IT environment and threat landscape are constantly evolving. Security strategies and technology also evolve to defend against new threats. The best way for blue-teams to combat cyber-attack campaigns is by adopting adversarial simulation tools to continuously test their security posture and proactively identify and remediate security gaps before their adversaries.
