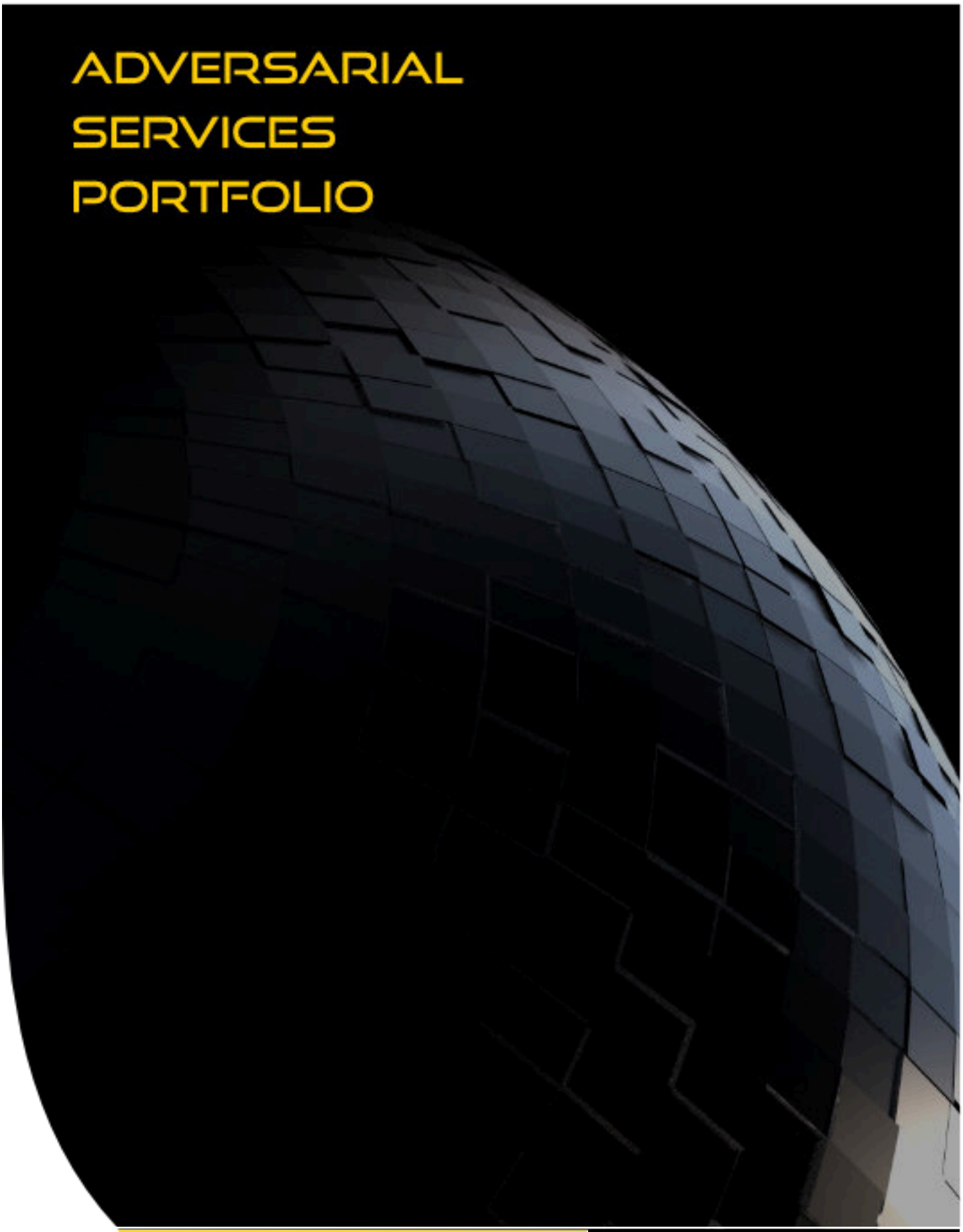
ADVERSARIAL SERVICES PORTFOLIO



COME SAY HELLO. WE ARE TURING COMPLETE!

3606 NORTH 156TH ST.,
SUITE 101 - 294
OMAHA, NE, 68116
SALES@STACKTITAN.COM

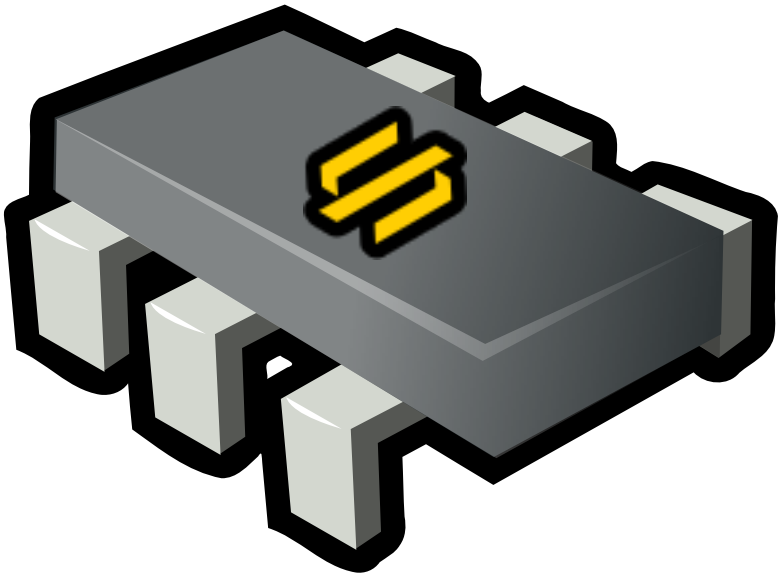
STACKTITAN
WWW.STACKTITAN.COM

AGGRESSIVELY SERIOUS ABOUT INFORMATION SECURITY

Welcome and thank you for reviewing our portfolio!

Thank you for starting your journey with a different kind of professional security provider. Our team of highly skilled practitioners is one of the best in the industry. Each of our customer's needs are unique, we listen and create solutions that solve the challenge. What's our goal? Simple. We want your experience with our team to exceed all expectations from the first conversation, throughout technical execution while forging a long-term professional relationship.

TABLE OF CONTENTS



Our Start and Values

STACKTITAN was founded in 2017 with the premise that the industry deserves better. Whether that be better security solutions, better consulting, or better partners, we knew given our proven Industry experience that we could help our customers achieve their goals.

STACKTITAN is a consulting firm with its roots in executing extremely customized adversarial simulations and penetration testing services. We are also developers with a focus on delivering better methods to track vulnerabilities, malware research, command and control, and kill-chain theory. Most importantly, our team consists of operators that thrive in challenging environments with one unified mission, to succeed no matter the task.

600+

ASSESSMENTS

Our customers mean everything to us. The ability to easily conduct business and provide the necessary risk assurance is paramount to the organizations we service. We have performed security assessments in multiple industry verticals keeping assets safe and secure.

40

YEARS OF EXPERIENCE

Our team of highly experienced technologists and security practitioners come from a diverse industry background. This experience, along with continual professional education, allows the team to stay adept to the emerging threats and techniques.

100%

QUALITY DRIVEN

We want everyone we have the pleasure to work with to receive the quality they deserve. The experience should produce actionable results, provide clear direction, and establish a trusted relationship; one that doesn't end when the project concludes.

“They [STACKTITAN] have been a partner with our organization and that is what we hoped for in our engagements. They have extended our relationship beyond their contractual obligations when necessary and that is part of the true definition of partnership.”

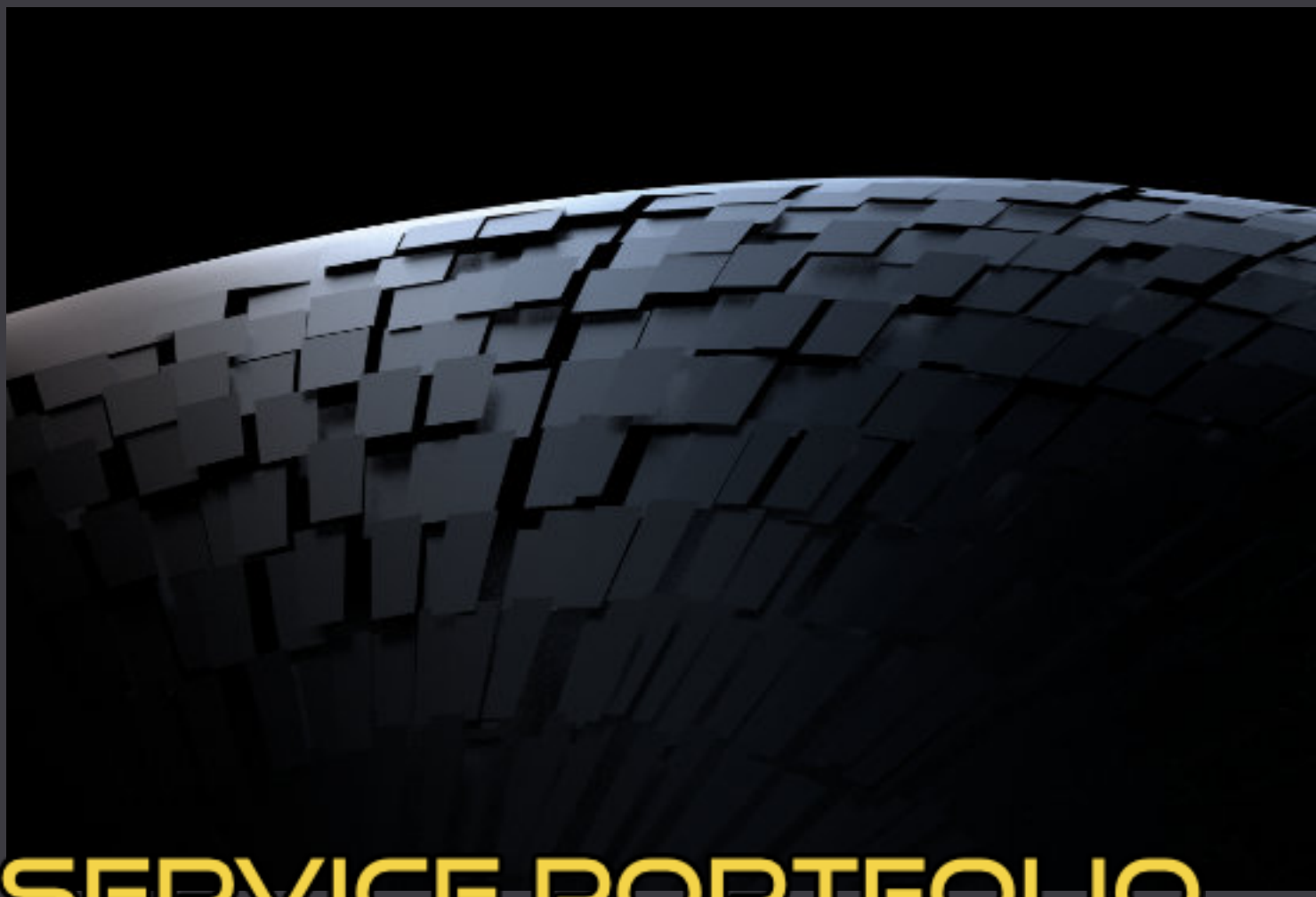
~ Fortune 500 Media Firm

“This is hands down the best red team assessment I've seen a vendor perform.”

~ CISO at Financial Services

“Wow..... you guys are really, really good at your job.”

~ Board of Directors at Insurance Company

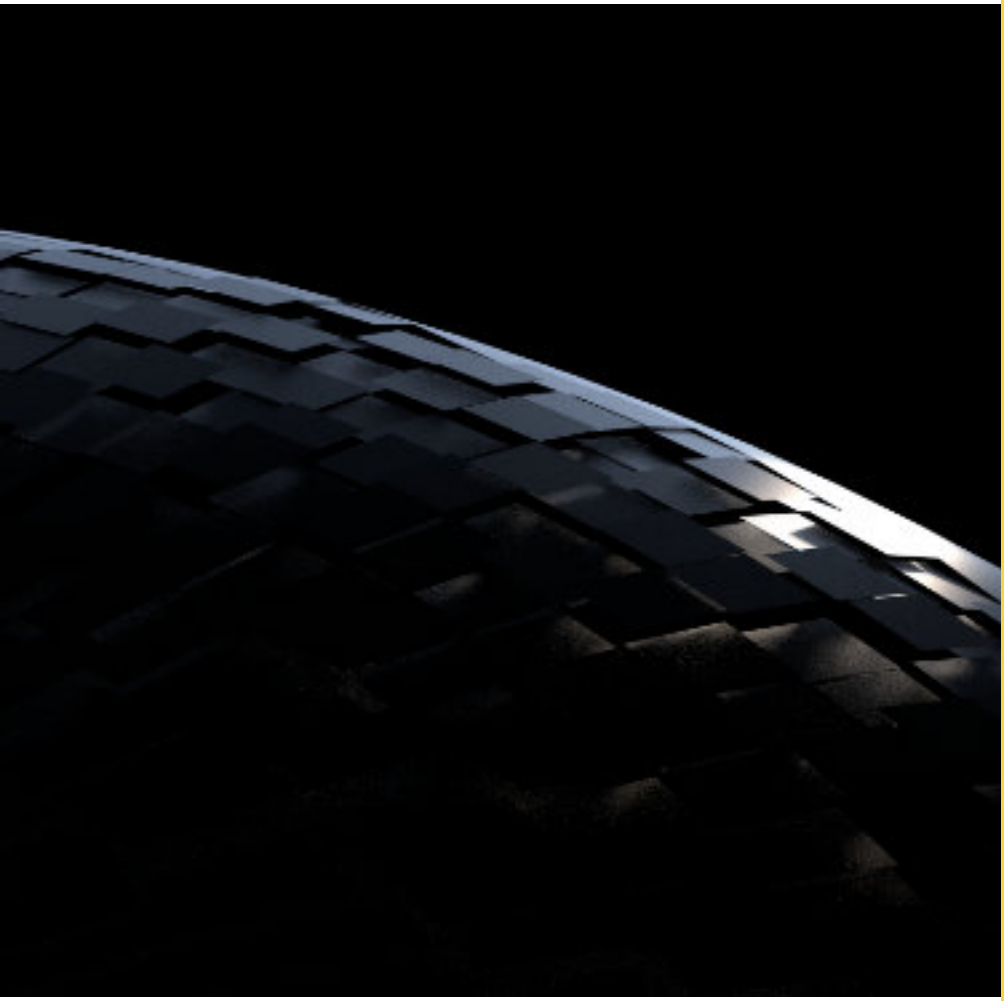


SERVICE PORTFOLIO

So you are tasked with ensuring that your organization can continue business operations as securely as possible while managing risk, reducing vulnerabilities and acknowledging threats...

You need a service provider that can think like an adversary with motive and capacity, and provide the assurance that technology, people and processes are effective at preventing a compromise.

STACKTITAN has years of experience doing just that, securing organizations from attack. We hope you enjoy this portfolio, and when you are ready, we are here for you!



NETWORK

APPLICATION

AWARENESS

CLOUD

HARDWARE

INDUSTRIAL

EDUCATION

READINESS

WIRELESS

OFFENSIVE AND DEFENSIVE TESTING

A skilled penetration test is both parts science and art. Whether it is testing the security controls of an application, hardware device or the entire enterprise network, the assessment must use the relevant tools and techniques. This category of services embodies the hacker mentality of creativity, resourcefulness and mastery of tradecraft to best identify weakness and defend against the adversary.

SECURITY AWARENESS

Your employees are entrusted with safeguarding information, physical assets and human-life. Ensuring that they are well-equipped to enforce company policy, detect social-engineering threats and enact the appropriate response protocols is imperative. STACKTITAN can engage in a full physical and social breach of an organization or perform targeted phishing exercises.

ATTACK READINESS

Concerned on whether or not your organization has the appropriate response protocols in place if targeted by an adversary? Is your organization resilient to a breach or a ransomware attack? STACKTITAN can craft curriculum that is both part tabletop and live-fire exercise to help identify deficiencies in play/run-book protocol. STACKTITAN even has benign ransomware that emulates real-world variants. Great for testing detections.

TRAINING AND EDUCATION

STACKTITAN enjoys teaching their tradecraft. We are only better by sharing our knowledge. Organizations often seek out STACKTITAN's secure software development training to increase code attack resiliency. Internal corporate security teams may want to increase their knowledge of offensive (i.e.,hacking) tradecraft. In any case, our instructors are practitioners with real-world experience. We'll even buy lunch.

CONTRIBUTING TRADECRAFT

How many times have you thought you were getting, promised you were getting, a high-quality penetration test only to be handed commodity vulnerability scan results?! It's frustrating, we know. We are THE exception to the run-of-the-mill fly-by-night security "practitioners". With STACKTITAN, you WILL receive real results, expert consulting to explain the risk, and actionable remediation advice.

STACKTITAN understands that the world runs in code, and having the skillset to solve challenging problems ensures our clients receive the much-deserved attention to detail that they deserve.

Meet our book, Black Hat Go! We authored it so that the industry could create the same tools that we build, have the skills to solve challenges, and learn. We want you to feel comfortable that not only do we know the latest emerging threats, but we also build the utilities that allow us to be effective in our assessments.

TECHNICAL WIZARDRY

HACKERS

Our inquisitiveness drives our passion to learn. That is at our very core.

DEVELOPERS

The world runs on code. Our team is comprised of experienced software developers

RESEARCHERS

Adversaries research the latest emerging attack techniques, and so does our team of researchers.

CREATIVES

Security requires a creative mindset. Our team merges both ART and SCIENCE to solve complex problems.

ARCHITECTS

Out team is comprised of network and software architects that have secured numerous technologies.

EDUCATORS

We want to make our tradecraft knowledge accessible, so we are constantly teaching all things security.

STACKTITAN is a North American based security firm staffed with United States based employees.

PENETRATION TESTING

WHAT IS IT?

Penetration Testing is a methodical approach used by skilled security practitioners to identify vulnerabilities and material weaknesses in devices. These devices often range from commodity IT servers to very specific technology, such as industrial environments (e.g., OT). Every result from a penetration test will demonstrate risk through actual controlled exploitation.

WHY DO IT?

As breaches become pervasively common, insurance providers are requiring penetration testing prior to writing policies. Additionally, many organizations want to prove that their resources are secure, and that the investment in people, process and technology is operating as expected and efficiently. Such engagements are perfect opportunities to discover potential areas in need of improvement.

JUST STARTING OUT OR MAYBE COMPLIANCE?

Vulnerability detection, but no exploitation with this service. This is a good place to understand technical risk, baselining your network vulnerabilities, and meeting quarterly compliance initiatives (e.g., PCI).

THINK YOU HAVE EXPLOITABLE RISK?

Introduce safe exploitation into the vulnerability detection to help demonstrate the real technical impact of a vulnerability. This approach often helps to demonstrate the need for additional security controls, instrumentation, staff, etc.

IS IT TIME TO BE SNEAKY?

So you have been training, spending on defenses, and people are ready for the inevitable attack. Good, we're up for the challenge. This is when the custom tooling and techniques come out to play and we really test both the human and technical element.

WE ATTACK, YOU DEFEND. WE ALL GET BETTER.

"In the midst of chaos, there is also opportunity"
~ Sun Tzu.

Knowledge is very powerful, so let's collaboratively spar together and learn how we improve along the way.

A CERTAIN THREAT ACTOR GOT YOU DOWN?

Your security operations teams have been creating detection rules, fine-tuning and really studying all of those indicators. What better means to test effectiveness than by really emulating the actual tactics employed by a capable threat actor.

I DON'T TAKE THINGS FROM STRANGERS, UNTIL. . .

Part of a merger or acquisition, and need to understand the technical risk either organization may introduce upon one another? We can perform an assessment that will provide you with the details, while emphasizing the priority concerns.

APPLICATION SECURITY

WHAT IS IT?

Applications are the heart of technology. They are present on mobile, desktop, cloud, industrial and anywhere in-between. Our skilled developers leverage their experience to review source-code and run-time applications. The results of an application assessment will present actual vulnerabilities that are accurate, concise, and actionable for technical and non-technical audiences to consume.

WHY DO IT?

Imagine introducing your prized business-critical application or product for public consumer access without any formal skilled security review. Bad things can happen. Application security assessments provide the necessary level of assurance that your consumers demand. Such assessments exemplify that your organization is serious about security and engages in a mature secure development process.

CONCERNS ABOUT APPLICATION CODE?

Applications are only as good as the code that instructs them to operate. A thorough review of the source code can surface both design and security issues that could lead to a wide variety of issues (e.g., memory leaks, hardcoded secrets, weak crypto, etc.)

IS MY RUNNING APPLICATION VULNERABLE?

This is a deep analysis of the application within its intended running state. Applications can be manipulated by consumers, and it is imperative that the application is resilient to attack. This could pertain to a web, thick, kiosk, or similar application as they all have some level of attack surface while operational.

APPLICATIONS THAT MOVE WITH US. . .

Mobile applications require numerous assessment disciplines and present a unique challenge in that security controls are both client- and server-side. Applications demand a varying degree of security, ranging from non-existent, trivial implementations to those that employ complex, anti-tampering features.

LIGHTER APPLICATIONS WITH INSTALLERS. . .

Applications have converged within frameworks to present a hybrid user experience, part web but often installed locally on the desktop. As such, there are aspects of these applications that employ thick and web API based technologies. All of which can be subject to user manipulation.

SOMETIMES THE SOURCE CAN'T BE FOUND

Sometimes it is necessary to gain a level of assurance that the commercial library being integrated into your product code is secure. Other times, you may suspect the code to be performing something nefarious. Reversing is the discipline of inspecting and/or tampering with an application's base assembly code.

LEARN TO IDENTIFY BAD CODE DRAGONS!

Alas, developers want to create code, but sometimes they don't always consider the potential impact their code might have on the secure state of the application. That is what our secure coding workshop aims to achieve, helping developers write secure code.

HARDWARE | IOT SECURITY

WHAT IS IT?

Hardware allows operating systems to interface with the physical world. For example, this is ever present in Industrial control systems, which leverage hardware for controllers, actuators, and sensors. All of which play an important role and must be secure. Hardware assessments require skilled engineers and the right tools. STACKTITAN has everything necessary to perform these skilled assessments.

WHY DO IT?

Most manufacturing organizations want to ensure their product, either net-new or refresh, is secure prior to a go-to-market. The companies range from industrial (e.g., satellite components) to residential (e.g., wireless routers), but many share similar concerns. Industrial manufacturing will often also require assurance that their processes (e.g., discrete, continual, etc.) are as secure as possible.

WHEELS ON THE BUS GO ROUND N ROUND. . .

Well it is more like CAN-BUS or Class-2 BUS or any other BUS on a vehicle, which permits connected communications. As both consumer and commercial vehicles evolve so does the potential to evaluate the security of such technologies.

STAYING ALIVE, STAYING ALIVE. . .

Unlike the greatest hits, the life-sciences and medical manufacturing industry has so much possible risk that the FDA has released guidance on performing security assessments. Rightfully so, with the pervasiveness of medical technology and its criticality, it must be held to the highest secure standards.

HOUSTON, WE HAVE A PROBLEM. . .

Assessing the security of communications as they apply to vehicular connected protocols, satellite ground stations are still of relevant concern in modern day . A thorough review of items such as telematics and RF implementations can help to identify material weaknesses and vulnerabilities.

RISE OF THE MACHINES. . .

Whether a textile mill or an oil refinery rig, industrial processes are in motion doing everything to make our lives come together. Securing their ability to be available and operable when required is the fundamental tenet of operational security controls.

NOT AS MUCH RISING OF THE MACHINES. . .

What about the consumer products, like wireless routers or smart devices? The security of these devices are increasingly important as they interface with personal lives and carry our personal information. Ensuring secure interaction with such devices is critical to safeguard the everyday consumer.

HACK, BUT ALSO SAVE, THE PLANET. . .

Green manufacturers often have unique processes that depart from traditional industrial technology. Organizations that create green products, such as water and air filtration have a responsibility to ensure the consumables and process are secure.

CLOUD SECURITY

WHAT IS IT?

Whether an organization has implemented a cloud native or hybrid (i.e., partial on-premises and cloud) infrastructure, many unique security concerns will arise. STACKTITAN's cloud security services range from cloud penetration testing, secure configuration and architectural reviews, to risk assessments. Additional emphasis is also on the third-party services and integrations within the cloud deployment.

WHY DO IT?

Cloud technology introduces a new paradigm of security, architecture, and operations. Organizations with a considerable cloud presence, software-as-a service vendors that provide cloud applications to consumers, and other diverse software-defined solutions will gain visibility into their vulnerabilities and general risk exposure. This will help provide assurance at the build, deployment and operational phases.

MORE THAN JUST EMAIL. . .

The Microsoft M365 environment can be so much more than just o365. With endless third-party integrations and Software-as-a-Service solutions, the functionality and complexity increases. Understanding the security implications is crucial at this level.

HEAD IN THE CLOUD INFRASTRUCTURE. . .

Azure and AWS provide their respective cloud environments to host numerous as-a-service technologies. These range from infrastructure to applications, and beyond. These implementations will influence risk of cloud-native and on-premises hybrid solutions without adequate security controls.

HACKERS GONNA HACK CLOUD THINGS. . .

Ever wonder how the criminals compromise cloud networks and resources? We can show you through demonstration while seeking out the most relevant and available vulnerabilities. Such a perspective can not only help secure the environment, but may also present a relevant narrative for leadership.

SO YOU HAVE A SAASY APPLICATION. . .

Service providers often create cloud native Software-as-a-Service solutions, while many have powerful features and depth of reach, such as those intended for multi-tenants. A thorough application and cloud infrastructure security assessment is ideal for detecting impactful vulnerabilities.

GETTING STARTED

What to expect.

Q: How much involvement will be required of my team?
A: First, we want you to be comfortable throughout the engagement. We are all self-sufficient with years of experience, but this is truly your preference.

Q: Will your testing have a negative impact on my business?
A: The potential of impacting information systems and business processes is minimal. We are very careful in our approach to ensure the survivability and sustainability around your business operations.

Q: How long does the assessment take?
A: This truly depends on the number of assets and resources within the environment. This is also contingent on the complexities associated with a particular technology we may be assessing. However, we will be transparent and remain on-task throughout the project plan.

Q: Do you need to be onsite to perform the assessment work?
A: Most of the time it is not necessary, but we will if you prefer. We have low-interaction solutions that we can deploy within your environment, such as our secure virtual machine (VM) or hardware testing device. We do all the heavy lifting so all you have to do is install the VM guest image or plug the hardware device into network port.

Q: What sets you apart from other providers out there?
A: This is a fun question and something that is often realized once we work together. A vast majority of our customers are repeats ranging from mid to enterprise Fortune 500 companies. We will always aim to ensure the highest level of professionalism with communication being the key along the way. Our customers state that we are consistent and always provide valuable insight and value. We are serious about the security of your assets.

Q: You are more expensive than some other providers?
A: Here is the ugly fact about this industry. Many service providers are selling vulnerability scans and trying to pass them as skilled penetration or adversarial assessments. We aren't the provider to seek if you need a scan; however, we are the team to engage if you want to really understand attack resiliency. Think about ransomware, what if you could live-fire a benign variant with a skilled provider and analyze your team's response along the way. You would be better prepared, right? To be able to offer a service like that takes understanding, research and dedication to our tradecraft so you are best equipped to defend the enterprise.

Q: We have a custom requirement but it isn't listed on this portfolio?
A: This is really where we thrive. The portfolio describes our core services. However, we perform custom engagements all the time. Additionally, we partner with some great organizations to better serve and present a comprehensive solution-set, overall.

ASSESSMENT STRUCTURE

1

Project Scoping

Starting with the pre-sales process, STACKTITAN ensures the solutions accurately align with the requirements.

2

Establish Project Plan

STACKTITAN will present a project plan with mutually agreed timelines, points of contact, status reporting, and milestone tracking.

3

Introductions

STACKTITAN will introduce the skilled technical delivery team during the commencement meeting, if not sooner.

4

Technical Execution

This is the time when the delivery team will execute the various technical components of the overall security engagement.

5

Participation & Engagement

It is not uncommon for client's to want to get involved. Clients often ride-along and participate in knowledge transfer sessions.

6

Training & Workshops

Maybe the ride along wasn't enough and the client wants a formal training or workshop. No problem, as this is also something the team can deliver.

7

Project Readout

The STACKTITAN team will present the project results via a formal readout. The audience may be either technical and/or executive level members.

8

Remediation Retesting

The delivery team will perform follow-on validation testing to ensure that the original risk has been adequately mitigated.