NuTech CYBER

Assessments & Solution Services Portfolio

ASSESMENTS

Fixed price services consist of a documented report, of recommendations, and knowledge transfer

		SKU #	Service Brief/Custom
Initial Assessment w/ Road Map Penetration Test	When you don't know where to start, the initial assessment is the way to go! This Assessment applies the first several stages of a penetration test (passive information gathering, active information gathering, and vulnerability identification) where we identify the opportunities where your IT Infrastructure is exposed to hackers. This information will enable us to provide you with a preliminary road map to help mitigate risks with what is needed in order to secure your gaps along with building a layered defense that will stop most hackers in their tracks.	PS-BAS-PEN-IN-RM	Service Brief Available
Enterprise Application Penetration Test	Adversary emulation focuses on simulating the tactics, techniques, and procedures (TTPs) employed by known threat actors. The goal is to determine whether or not you would be able to detect that adversary if it was present in your environment.	PS-BAS-ADV-EM	Service Brief Available
Adversary Emulation	Enterprise application penetration testing identifies the vulnerabilities found withinapplications found your desktop or laptop Using a provided end-user device, the testing team goes through the executable and application memory looking for flaws in authentication management, session management, configuration management, data validation, and more. They identify the ways that your application can be manipulated to leak data, to perform unauthorized actions, or even how it might grant access to backend systems. We prepare it and you for life in the hostile world of the corporate network.	PS-BAS-PEN-E-AP	Service Brief Available
Internal Network Penetration Test	Internal penetration testing is a type of ethical hacking in which testers with initial access to a network attempt to compromise it from the inside to intrude and gain further access. The insider or tester with network access simulates the actions of a real attack.	PS-BAS-PEN-INRL	Service Brief Available
Mobile Application Penetration Test	Mobile application penetration testing identifies the vulnerabilities found within your iOS or Android application. After unpacking the application, the testing team goes through all layers of your application logic including authentication management, session management, configuration management, data validation, and more. They identify the ways that your application can be manipulated to leak data, to perform unauthorized actions, or even how it might grant access to backend systems. This type of test helps secure Mobile Application for life in the hostile world of the Internet.	PS-PEN-M-AP	Service Brief Available
Perimeter Network Penetration Test	Perimeter network penetration testing begins by identifying your attack surface. Within that attack surface, the testing team identifies not only common vulnerabilities, but also those unique to you and your environment. Reading between the lines, the testing team finds what scanners miss. It determines how effective your perimeter security deters external threats and how well it spots flaws in internet-facing assets like Web servers, FTP servers, Etc.	PS-BAS-PEN-P-NTK	Service Brief Availbale

NuTech CYBER

Fixed price services consist of a documented report, of recommendations, and knowledge transfer

ASSESMENTS		SKU #	Service Brief/Custom
Red Team Penetration Test	Red team penetration testing is a full-scope, multi-layered test used by a firm to assess how tough the security of the organization really is. Involving not just your perimeter security, network security, and the security of your people and processes, it also involves physical security as well. It directly pits your blue team against our red team to see who comes out on top.	PS-BAS-PEN-RED	Service Brief Available
Web3 Application Penetration Test	Web3 application penetration testing identifies the vulnerabilities found within your blockchain-integrated web applications (decentralized finance). After connecting to your application with our wallet, the testing team goes through all layers of your application logic including authentication management, session management, configuration management, data validation, and more. They identify the ways that your application can be manipulated to leak data, to perform unauthorized actions, or even how it might grant access to backend systems. This service allows a Customer to identify the application's vulnerabilities and to secure it against real world threats.	PS-BAS-PEN-WEB3	Service Brief Available
Web Application Penetration Test	Web application penetration testing identifies the vulnerabilities found within your traditional web applications. After connecting to the application(s) via a web browser, the testing team goes through all layers of your application's logic including authentication management, session management, configuration management, data validation, and more. They identify the ways that your application can be manipulated to leak data, to perform unauthorized actions, or even how it might grant access to backend systems.	PS-BAS-PEN-WEB	Service Brief Available
Threat Hunting	Threat hunting is when computer security experts proactively look for and root out cyber threats that have secretly penetrated their computer network. Threat hunting involves looking beyond the known alerts or malicious threats to discover new potential threats and vulnerabilities.	PS-BAS-THREAT	Service Brief Available
Single Scan Vulnerability Scan	A vulnerability scann is an automated vulnerability testing tool that monitors for misconfigurations or coding flaws that pose cybersecurity threats. Vulnerability scans either rely on a database of known vulnerabilities or probe for common flaw types to discover unknown vulnerabilities	PS-BAS-V-SCAN	Service Brief Available
CUSTOM			
Continuous Vulnerability Scan	Monthly Vulnerability Scanning	PS-BAS-VS-C	Custom

NuTech CYBER

Custom services requires a scoping call, and will be defined in a SOW (Statement of Work)

		SKU #	Service Brief/Custom
CUSTOM			
Zero Trust Strategy	Zero trust is a security posture of hosts within an organization that is based on various signals, such as user identity, device compliance, requester location, data sensitivity, and application type. It is based on the principle of verifying every request explicitly and enforcing granular access policies (Never Trust, Always Verify). The zero trust assessment can help organizations improve their risk management and protect their private applications from unauthorized access by identifying the pieces that they need to put into place that are necessary to achieve that elusive but often sought after goal of, Zero Trust.	PS-ADV-ZT	Custom
SASE Advisory	SASE is the convergence of WAN (Wide-Area-Networking) and network security services such as CASB or FWaaS into a single, cloud-delivered service model. It is often a key component of implementing Zero Trust for many organizations. SASE advisory lets us help you architect the perfect solution for your cloud-based enterprise so that you can keep it secure. Even more, we can help you build on your SASE to produce the interlocking solutions necessary to achieve Zero Trust.	PS-ADV-SASE	Custom
Expert on Demand (EOD)	NuTech Cyber Expert On-Demand (EOD) services provides cyber security consulting by a subject matter expert for ongoing engagements, assessments, strategy, planning and staff augmentation in order to help mitigate the risks associated with your security posture. All EOD hours and terms are defined by a SOW (Statement of Work)	PS-ADV-EOD	Custom
Strategy, Consulting w/Road Map	The role of a security strategy is to align company security and business goal, provide a common security program framework to focus efforts and optimize compliance efforts, and ultimately use securtiy as a business facilitator. This is a more comprehensive engagement beyond the Inital Pen Test with Road Map..	PS-ADV-SCRM	Custom
SUBSCRIPTION			
Vulnerability Management	Going beyond just the scan, we process those scan resutls and compile task lists for you engineering team. There is no more looking at the scan results wondering what to do next. You have your marching orders in hand and can begin remediating on day one. We also turn those scan results into metrics. We track those metrics from month to month. We let you know what your progress is and how to make more of it. Your vulnerabilities go from being chased down to being managed and under control.	PS-SUB-VMT	Custom
Assessment Subscription	An annual subscription comprised of 3 or more service briefs at a discount.	PS-SUB-ASTS	Custom