SECURITY TESTING
Cheat Sheet

LMG SECURITY

What security tests should your organization run and how often should these tests be performed? Find out in this handy cheat sheet of today's best practices!

SERVICE	OVERVIEW	RECOMMENDED FREQUENCY
Penetration Testing	The goal of a penetration test is to identify vulnerabilities in your systems' security, validate they are exploitable, and exemplify the risk these vulnerabilities create for your organization. During a penetration test, ethical hackers simulate a cyberattack to uncover security gaps such as unpatched vulnerabilities, system misconfigurations, authentication and session issues and more.	Annually or upon major changes
Vulnerability Scanning	In today's threat landscape, monitoring your external attack surface is critical. LMG's team can implement a continuous monitoring solution that scans your Internet-facing systems to help you quickly identify if assets are exposed or vulnerable. Protect your organization from vulnerabilities such as Log4j and more. Our solution continuously monitors your attack surface, discovers unpatched vulnerabilities, verifies patch status and more.	Continuously!
Web App Pentesting	The security of web applications degrades over time, as new vulnerabilities such as Log4j are uncovered, so web app pentesting is now a foundational security practice for organizations to identify and mitigate vulnerabilities in SaaS platforms and web applications before the hackers find them.	Annually or upon major changes
Attack Detection & Response Testing	How do you know your monitoring is effective? Find out! LMG's experts will launch a simulated attack and test your detection and response capabilities. Our methodical, timed, testing can include reconnaissance, vulnerability scanning activities and exploitation attempts. Throughout the testing process, we will keep meticulous, time-based records of the simulated "attacker" activities for post-test analysis.	Annually
Cloud Configuration Review	Cloud breaches are all too common. LMG will review a variety of technical controls, including: access and sharing, authentication, encryption, monitoring, logs, automatic back-up schedules and much more. Our team provides a detailed report that helps you close security gaps, refine internal policies and reduce your cloud security risks. Platforms include AWS, Azure, Microsoft Office 365, Google Cloud, Oracle Cloud, Citrix, and more.	Annually or upon major changes
Threat Hunting	Is malware lurking in your network without your knowledge? Modern threats such as fileless attacks bypass traditional antivirus and perimeter defenses by entering through vulnerabilities in your operating system or other trusted software. Our proactive threat hunting service looks for abnormal activity and evidence of intrusion to detect these sophisticated threats so that you can eradicate them.	Monthly or upon signs of an incident
Red Team Testing	Can hackers penetrate your network and gain access to your sensitive data or impact operations? Find out with a red team test. A highly skilled team of experienced penetration testers are given creative freedom to "think like hackers" and see how far they can go in your network. The red team will have customized goals, and use a combination of attack techniques to not only penetrate your network, but also identify and exploit vulnerabilities in your people, processes, facilities and technology to capture their target data.	Annually

Contact us for a customized testing plan for your organization!

1-855-LMG-8855 | info@LMGsecurity.com | **www.LMGsecurity.com**