Penetration Testing as a Service

Xcape, Inc. offers a catalog of attack surface enumeration, and offensive security assessment service offerings specifically designed to scale as your organization grows. Locking in scheduled assessment services before a critical situation arises allows organizations to ensure that their IT and security programs have the support they need to address operational requirements without the looming threats of ballooning costs.

Unlike other service providers, Xcape fully partners with your organization, providing not just best effort assessment services, but an established IT MSP capability that offers the support your organization requires to address all findings and concerns.

Xcape will never leave you with a “bag a bugs” to triage and remediate on your own.

Blue Team Services	Red Team Services
Incident Response / Ransomware Recovery	Blended Threat Assessments (Red Team)
Threat Hunting	Vulnerability Assessments
Program Development Consulting	Penetration Testing
Customized Solution Development	Continuous Attack Surface Enumeration
Adversary Engagement	Automated Adversary Emulation

info@xcapeinc.com | +1 (888) 732-4697 | xcapeinc.com | Schedule Consultation

Continuous Attack Surface Enumeration

With our automated scanning infrastructure we'll continue to monitor and report on exposed endpoints of your infrastructure providing you visibility into what's exposed publicly. The internal version of this type of scan gives you the perspective of what an attacker might be capable of if they were to breach your perimeter.

Integrated Post Exploitation

With vulnerabilities found in exposed end points we'll launch automated attacks against those endpoints and provide associated reports detailing the attack kill chain used to gain access to systems.

Continuous Penetration Testing

Our automated scanning infrastructure is the basis for our automated penetration testing platform to build an attack profile on your infrastructure, once we've identified targets the system will begin executing automated attacks on the exposed endpoints, constantly updating the attack profile based on new vulnerabilities as they are identified in the wild and our tools are updated.

Findings Manual Review

Our team can work with your internal team to identify a remediation plan in an effort to assist resolving issues with found vulnerabilities.

Scheduled Manual Post Exploitation

Schedule a deep dive on exploitable exposed endpoints and have a tester work on post exploitation attack methodologies.

Scheduled Threat Hunting and Response

Our team will review logs periodically to look for indicators of compromise to determine if there's been a breach. Building detections based on log data and samples collected from our EDR platform.

Incident Response / Ransomware Recovery Retainer

Our incident response team can act quickly in response to a breach, providing valuable information and resources to lock out the attacker and your infrastructure.

Appliance

Our appliance is available for both physical and virtual infrastructures, the physical appliance gives us the ability to independently scan and audit your internal network. It's our foothold for remote auditing activities as well as our utility for wireless audits should that be required. (*Adding the appliance to the basic package provides internal enumeration)

Managed Detection and Response / Endpoint Detection and Response

We continuously monitor endpoint activities looking for nefarious activity to offer early visibility into potential attacks, providing valuable information during incidents. Our MDR team will affect real-time changes in your environment when security incidents are identified. Additionally we provide a full service EDR solution that is also managed by our team suitable for Desktop, Server, and Cloud infrastructure.

Remote Monitoring & Management

Our remote monitoring & management solution provides patch management for OS and third party applications, compliance monitoring, scheduled maintenance, and performance monitoring.

Choose the service level right for your organization.

Services	Basic	Standard	Professional	Ent..
Continuous Attack Surface Enumeration	*✓	☑	☑	☑
Integrated Post Exploitation	$299/hr	✓	☑	☑
Continuous Penetration Testing	✓	☑	☑	☑
Findings Manual Review	$299/hr	$299/hr	✓	☑
Scheduled Manual Post Exploitation	$399/hr	$399/hr	$399/hr	☑
Scheduled Threat Hunting and Response	$299/hr	$299/hr	☑	☑
Incident Response / Ransomware Recovery	$399/hr	$399/hr	$399/hr	☑
Pricing	**$2,500/mo**	**$5,000/mo**	**$10,000/mo**	**Call**
Add - Ons				
Appliance ($800 Per Site)	*$800	1 Site Incl.	2 Sites Incl.	Call
MDR & EDR (Workstations / Servers)	$15/$20	$15/$20	$15/$20	Call
Remote Monitoring & Management (per host)	$10	$10	$10	Call

External ✓ | External and Internal ☑
***Appliance add-on provides internal Attack Surface Enumeration**

Get In touch!

Contact us to start on your security service journey today.

info@xcapeinc.com | +1 (888) 732-4697 | xcapeinc.com | Schedule Consultation