EITS
Enterprise IT Security

Penetration Testing as a Service

Penetration Testing
as a Service
focused on helping customers **prioritize** and **remediate findings,** not just testing and reporting the gaps

New Approach in 2021

In response to our customers feedback, we have expanded our service offerings to now include "Penetration Testing as a Service." Many customers desire to offload the responsibility of certain tasks to an external entity which will provide a higher level of expertise than the job market can afford them. This shift to "everything as a service" has resulted in significant cost savings in many IT areas, and remedies the following:

- Difficulties around procurement speed
- Remediation efforts
- Validation
- Training
- Risk guidance

Customers benefit from the skillsets and contactable resources without the expense of hiring and training new staff.

How Does this Service Differ from Typical Penetration Testing?

Legacy Penetration Tests were a point in time assessment of your environment where the limiting factor was always time. You receive a report with findings and hopefully remediation recommendations that guide you in the right direction to fix the issues yourself. Those remediation efforts would occur sometime throughout the coming year in preparation for the next test. The next year you receive another report with findings that you spend another year remediating and continue to repeat this process ad infinitum.

Some large organizations with the luxury of equally large budgets employ internal penetration testing teams that work year round to test new attack types that are released daily. These internal teams collaborate with defensive counterparts to perform training exercises and determine risk exposure when new headline snatching exploits are discovered. This "Continuous Monitoring", a buzzterm in recent years, represents a dedicated team reviewing telemetry to discover attackers as quickly as possible within environment. EITS is offering "Continuous Testing", the same concept but from the offensive perspective.

Are You Comfortable with Your Current Security Posture?

Does your security team have questions?

Though it may not take an entire year to remediate your penetration test findings, the security team probably has questions about the latest exploits and could use help determining the organizations risk exposure. Maybe your security team would like to understand how the exploit takes advantage of a vulnerability that the organization cannot patch so that it can be properly mitigated. It would probably be beneficial to validate that mitigation is working as intended by attempting the exploit in production.

Do you perform Incident Response Tabletop exercises?

If not, you should be. But even if you already are, how applicable are the scenarios to your business? Most times these exercises are purely on paper and give the benefit of doubt to your staff that they will follow the procedures that were meticulously labored over before adoption. A more beneficial approach to these exercises would be to use real compromise scenarios performed during a penetration test to see where the processes broke down in a non-hypothetical way. The lessons learned from that type of effort will be exponentially more helpful than an "on rails" scenario where everything is assumed to have gone perfectly.

What size organization will benefit from this service?

It is EITS' goal to provide the benefits of internal penetration testing teams of larger organizations, to businesses of any size. Customers will be able to reach out to a penetration tester at any time throughout the year – a phone call away. Instead of waiting a full year to identify remaining items to remediate, old findings can be validated immediately upon being addressed. Additionally, testers can learn more about your environment over longer periods of time, which will result in identifying deeper issues and assist in developing a long-term plan to protect your most sensitive information, ensuring that no matter that attack vector, the organizations risk is as low as possible. When new vulnerabilities are discovered, an exploitation expert is at your disposal to explain the difficulty to execute that attack and even more importantly, how that new vulnerability can be leveraged with older ones to achieve compromise in a way not being reported in the media. This will also remove guesswork in determining impact, as your testing team will perform the exploitation to prove effectiveness.

What kind of budget will this service consume?

For less than the cost of employing a qualified security professional, our customers receive the benefits of an internal testing team. We are offering the capability to perform "Continuous Testing", thereby reducing time to detection of exploitable vulnerabilities, and hopefully beating the attacker to the hole.

What types of tasks can customers leverage with this service?

As customer needs evolve, our service offerings will continue to grow each year. Currently, customers will be able to request the below tasks as a part of this service offering:

- Table Top IR with scenarios customized for the specific customers environment
- Remediation guidance and validation
- Purple Team Exercises
- Consulting for new technology deployment or network design as it relates to security
- Additional highly scoped testing
- Training
- Prioritization of remediation activities
- Applicability assessment for headline snatching vulnerabilities

Why Use EITS? What Qualifies Us?

GIAC Defensible Security Architecture GDSA
GIAC Certified Enterprise Defender GCED
Global Industrial Cyber Security Professional GICSP
GIAC Certified UNIX Security Administrator GCUX
GIAC Certified Forensic Examiner GCFE
GIAC Certified Incident Handler GCIH
GIAC Certified Penetration Tester GPEN
GIAC Web Application Penetration Tester GWAPT
GIAC Security Essentials Certification GSEC
GIAC Certified Windows Security Administrator GCWN
Magnet Certified Forensics Examiner M·C·F·E
C|NDA™ Certified Network Defense Architect
C|EH™ Certified Ethical Hacker

www.eits.com • 704-900-8042