GIGAOM RESEARCH

The industry leader in emerging technology research

PENETRATION TESTING AND BUG BOUNTIES

MARKET LANDSCAPE REPORT

AUTHOR: Simon Gibson - GigaOm Analyst

PENETRATION TESTING AND BUG BOUNTIES

MARKET LANDSCAPE REPORT

AUTHORED BY GIGAOM ANALYST, SIMON GIBSON

INTRODUCTION

In a perfect world, networks, computers, and applications would be impenetrable. Data entered, stored, and shared would only be used as designed and, if something were to go wrong, the system would heal itself, not only remediating the issue but learning from and preventing it from ever happening again. Until that perfect state is reached, system operators can use penetration tests (pen test) and bug bounties to help them discover vulnerabilities. These two methods for authorized, simulated cyber attacks are performed to evaluate the security of a system, application, or network.

The process of probing systems to discover, understand, and fix vulnerabilities before they can be exploited may sound straightforward, but is instead complex, nuanced, and requires the right balance between hacking for good and hacking for bad. Motivated to disrupt and break into systems, the pen testers uncover weaknesses and vulnerabilities that can then be fixed to make systems more secure.

Before engaging in simulated (aka ethical) hacking, it is important to clearly define the scope of the operation and evaluate platform features. These so-called rules of the road are critical to defining what is in scope and what is out of scope. They set the expectations and define what security researchers can expect to test and what elements of the application are out of scope. They define the kinds of bounties offered which span the gamut from a credit in the release notes, to a tee shirt, to cash payments.

These rules importantly provide legal indemnification keeping the hackers on the right side of the computer fraud and abuse and DMCA laws provided they're staying within the rules of the road set forth as part of the bounty.

REPORT TOPICS

- Penetration testing and why scope matters
- Binary analysis, application testing, static code analysis, and when to use each
- Bug bounties: nuances between vulnerability disclosure and handling procedures
- Implementing one or multiple strategies in a busy enterprise
- Techniques to measure success

CONSIDERATIONS

- What are the criteria to consider when hiring pen-test and bounty services?
- What are the differences between open and closed bounty programs?
- What legal ramifications must be understood before engaging in a pen test or bounty program?
- How do the two different programs relate to compliance versus engineering requirements?
- What are the milestones to track after implementing one or both programs and how is success measured?

ABOUT

ANALYST SIMON GIBSON

Simon Gibson is a **CISO and subject matter expert on security.** He has been responsible for driving security capability into products, enterprises and supporting complex engagements.

Simon led the Information Security Group at Bloomberg and served as their CISO. He has managed attack teams, incident response teams and been responsible for the defensive security posture in the financial, government, manufacturing and PCI industries.

Simon is a **renowned speaker and panel moderator.** He has counseled fortune 100's on building their programs and worked with US Government public private information sharing initiatives.

@simonhg

https://www.linkedin.com/in/simonhg/

INTERESTED IN GIGAOM REPORTS?

To purchase this report, or to explore opportunities to participate in future GigaOm reports, Email a GigaOm Business Development Representative.

GIGAOM

Find us:
gigaom.com

GigaOm provides technical, operational, and business advice for IT's strategic digital enterprise and business initiatives. Enterprise business leaders, CIOs, and technology organizations partner with GigaOm for practical, actionable, strategic, and visionary advice for modernizing and transforming their business. GigaOm's advice empowers enterprises to successfully compete in an increasingly complicated business atmosphere that requires a solid understanding of constantly changing customer demands.

GigaOm works directly with enterprises both inside and outside of the IT organization. To apply proven research and methodologies designed to avoid pitfalls and roadblocks while balancing risk and innovation. Research methodologies include but are not limited to adoption and benchmarking surveys, use cases, interviews, ROI/TCO, market landscapes, strategic trends, and technical benchmarks. Our analysts possess 20+ years of experience advising a spectrum of clients from early adopters to mainstream enterprises.

GigaOm's perspective is that of the unbiased enterprise practitioner. Through this perspective, GigaOm connects with engaged and loyal subscribers on a deep and meaningful level.