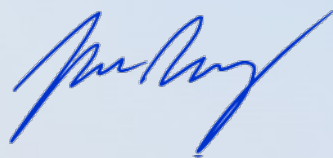February 11, 2017

On September 26, 2016, Pivot Point Security conducted a vulnerability assessment and penetration test of The Secure Bucket's public external infrastructure as defined by the client at the time of testing. The purpose of the assessment was to provide assurance that the information technology resources integral to delivering services to their clients is secured in a manner consistent with prevailing good practice.

Our Penetration Testing Methodology follows the testing approach recommended by the National Institutes of Standards & Technology (NIST) and has been vetted across thousands of engagements since 2001. Our testing included a full discovery scan, port scan, vulnerability assessment, and manual penetration testing covering tens of thousands of potential vulnerabilities (e.g., backdoors, CGI abuses, local security flaws, DoS, remote shells, malware), across all systems and services that were accessible during the test.

We determined that The Secure Bucket's systems were secured in a manner consistent with industry best practice and moderately better than that of peer organizations that we have tested.

Pivot Point Security has been architected to provide maximum levels of independent and objective information security expertise to our varied client base. The team responsible for conducting security assessments of this nature is led by a Certified Information Security Auditor/IRCA ISO 27001 Auditor and includes personnel appropriately qualified to render this opinion (e.g., Certified Information System Security Professionals, Microsoft Certified System Engineers, Certified Ethical Hackers, etc.)

If there are any questions regarding this attestation, please feel free to contact me at 609.581.4600 x300.

John Verry, 27001-CLA/CISA/CRISC/CTPRP
Principal Enterprise Security Consultant

PivotPoint
SECURITY