eSENTIRE

Technical Testing – External Vulnerability Scan and Penetration Test

This engagement includes eSentire scanning (at such frequency as agreed to by eSentire and Client) the quantity of IP Addresses (including cloud-hosted and on-premise assets) set out on the applicable Order Form and which have been provided to eSentire by Client, identifying services running on each host, and identifying service versions running on each host, as well as:

i. Penetration attempts on hosts and/or services identified by Client and which have known vulnerabilities;
ii. Attempt external infrastructure attacks (excluding denial of service attacks);
iii. Attempt external data access attacks (including brute force attacks);
iv. Attempt basic technical security violations of external facing applications (including cross site scripting attacks, cross site referencing, and SQL injection attacks); and
v. Attempt deep dive exploitation of identified weaknesses in external systems into internal systems.

External Vulnerability Rescan. eSentire will perform an External Vulnerability Rescan if Client received a one-time or annual recurring External Vulnerability Scan. After remediation activities undertaken by Client have been completed following an External Vulnerability Scan, eSentire will, no later than three (3) months following eSentire delivering to Client its draft report, rescan only those servers identified by eSentire to have high or critical security issuers to validate such remediation.

Open Source Intelligence Gathering. eSentire will use custom tools and a variety of other services to collect data related to Client employees and their external network (OSINT) to generate lists of potential usernames and passwords, discover publicly available email addresses, and generate a snapshot of open ports and services for use in penetration testing.

Detailed Technical Report

If applicable, eSentire will provide a document which identifies the findings discovered through the assessment. This will include:

- Methodology employed
- Positive security aspects identified
- Detailed technical findings
- An assignment of a risk rating for each vulnerability when appropriate
- Supporting detailed exhibits for vulnerabilities when appropriate
- Technical remediation steps