Vulnerability Management

Assigned Vendor:_____ Tel : ____-____- _____ Tester's Name:_____

Scan Test Date: ____/____/_____

Scan Software used: _____ Version: _____

On a scale of 1—5, where is this Scan Software: ranked among the top 5: ___

Can the results of this test be trusted: (YES/NO) _____

Is the Vendor using the most up to date version of the software: (YES/NO) _____

Results

Has the Vendor communicated the test results to the Client: (YES/NO) _____

Were any critical vulnerabilities detected: (YES/NO) _____

Has the Vendor made remediation recommendations: (YES/NO) _____

What are the remediation recommendations: _____

Will the Vendor remediate : (YES/NO) _____

OR– is the remediation effort associated with another Vendor: (YES/NO) _____

Was the associated Vendor (Name)_____ contacted for remediation: (YES/NO) _____

Resolution/ Remediation

1. Was the remediation done: (YES/NO) _____
2. What kind of remediation/Patch was needed:: _____

_____

3. Was a **subsequent** Scan test done after the patch to confirm the vulnerability was removed: (YES/NO) _____

4. Was the vulnerability a User/human created one: (YES/NO) _____

5. If "YES". Are the proper protocols now in plate to avert another similar vulnerability: (YES/NO) _____

Management Notification

Was management notified of the business risk due to the vulnerability : (YES/NO) _____

Did Management agree to the resolution method: (YES/NO) _____

Is management aware that the risk has been remediated: (YES/NO) _____

Follow-up Action Plan

1. Is additional User training necessary: (YES/NO) _____ 2. Any software updates needed: (YES/NO) _____
3. Are server O/S updates necessary: (YES/NO) _____ 4. Are SENGRID/ DEMARC Upgrade necessary: (YES/NO) _____
1. Are Firewall Upgrades needed: (YES/NO) _____ Any recommendations from the Scan testing : (YES/NO) _____

Recommendations:_____

_____

Completed by :_____ Date: ____/____/ _____

Countersigned by ASIC-IT: _____ Date: ____/____/ _____

Vulnerability Management

VULSCAN (EDR & SEIM)

Assigned Vendor:_____ Tel : ____-____- _____ Tester's Name:_____

Last Scan Date: ____/____/_____

Scan Software used: _____ Version: _____

On a scale of 1—5, where is this Scan Software: ranked among the top 5: ___

Can the results of this test be trusted: (YES/NO) _____

Is the Vendor using the most up to date version of the software: (YES/NO) _____

Results

Has the Vendor communicated the test results to the Client: (YES/NO) _____

Were any critical vulnerabilities detected: (YES/NO) _____

Has the Vendor made remediation recommendations: (YES/NO) _____

What are the remediation recommendations: _____

Will the Vendor remediate : (YES/NO) _____

OR– is the remediation effort associated with another Vendor: (YES/NO) _____

Was the associated Vendor (Name)_____ contacted for remediation: (YES/NO) _____

Resolution/ Remediation

1. Was the remediation done: (YES/NO) _____
2. What kind of remediation/Patch was needed:: _____

_____

3. Was a **subsequent** Scan test done after the patch to confirm the vulnerability was removed: (YES/NO) _____

4. Was the vulnerability a User/human created one: (YES/NO) _____

5. If "YES". Are the proper protocols now in plate to avert another similar vulnerability: (YES/NO) _____

Management Notification

Was management notified of the business risk due to the vulnerability : (YES/NO) _____

Did Management agree to the resolution method: (YES/NO) _____

Is management aware that the risk has been remediated: (YES/NO) _____

Follow-up Action Plan

1. Is additional User training necessary: (YES/NO) _____ 2. Any software updates needed: (YES/NO) _____
3. Are server O/S updates necessary: (YES/NO) _____ 4. Are SENGRID/ DEMARC Upgrade necessary: (YES/NO) _____
1. Are Firewall Upgrades needed: (YES/NO) _____ Any recommendations from the Scan testing : (YES/NO) _____

Recommendations:_____

_____

Completed by :_____ Date: ____/____/ _____