BLS RA Retrospective: Notes

26 JUN 2019

Action Items		
Action	***Resource***	***Timeline***
RA Recipe – Include estimate time range and resources for each step	Phil H.	15-30 days
Document Prep Tasks – Including time, resources, and personnel assignments	Joel M.	
Document and Investigate Lessons Learned from RAs	Carson S.	
Web Scanning Tools: Research capabilities and pricing	Paul M.	
Web Security Surveys: • Make a wiki entry that goes through the process • Formalize checklist	Paul M.	
SOWs: Update to include a third category for "Prep" (in addition to existing Execution and Reporting)	Adrian S.	
SOWs: Need to explicitly call out • Need for admin credentials for OS-level in critical apps • Need for creds for external apps to support surveys • SLAs/contracts with host/service providers	Adrian S.	
SOWs – Pricing: • Assume 65% billable • Downtime paid for by customer	Adrian S./Larry C.	
Critical App Interview + Data Gathering – Needs to be front-loaded; the most-critical apps get interviews first	Recipe	
Move Interviews w/Network + Security Team early on: • Common Security Controls • Common AV/EDR • Common logging • Email/DNS/IDS IPS/WAF	Recipe	

BLS RA Retrospective: Notes

26 JUN 2019

Customer Questionnaire: Update to incorporate lessons learned	Mike R./Adrian S.	

BLS RA Retrospective: Notes

26 JUN 2019

Process Changes
1. Define Personnel Roles & Responsibilities
2. Add Explicit Hotwash Between Business Lead + Operators
3. Front-load critical app. Interviews
4. Front-load interviews with security personnel
5. Nessus scans for at least 1-2 critical systems MUST be executed Monday/Day 1
6. Uncredentialed Scans should be executed for all critical apps regardless
7. How can we label/categorize findings? Call out the most critical issues for each category of finding.
8. Add revenue/loss section to report for apps with known vulnerabilities

BLS RA Retrospective: Notes

26 JUN 2019

Staffing
1. Minimum of 3 people per trip
2. RA Orchestrator (Lead) • No explicit tasking • Should not be bogged down by technical tasks
3. Technical Person
4. Business Lead

BLS RA Retrospective: Notes

26 JUN 2019

Tooling Candidates		
Tool	***Resource***	***Purpose***
1. Cacher	Paul M.	Click scripts
2. Cherrynote		Notes
3. Keepnote	Phil H.	Notes
4. Kanboard		Risk Management