Design Document

Executive Summary

CyberCompany is a startup cybersecurity company that has recently obtained a new revenue stream. The revenue stream will require entry-level IT personnel, within the Core Lab, to analyze and investigate various artifacts and cases to support a senior team within the company.

Due to IT personnel having less than 1 year experience in cybersecurity, *CyberCompany* is ready to create an onboarding experience for all new hires in the Core Lab to begin forensic investigation by the end of their first month with the company.

Client has requested a definite 3-month deadline for the onboarding project. Onboarding will cover one process of basic forensic investigation skill set, a system access process, and recordings of tasks that require specific context for completion. Client and Whitney Salas have agreed this is phase one of a larger organization goal for an in-house academy. This consulting capsule only includes Phase 1 training goals.

Project Success Statement

Whitney Salas will develop a blended learning onboarding program with a SharePoint knowledge base and support material that can be implemented within 3 months.

At the end of 1 month of hiring, *CyberCompany* will see a 67% increase in new hires confidently accepting and investigating engagements autonomously. We will meet this goal by shortening current training from 3-5 months before a new hire can confidently take a case to 1 month.

Findings & Recommendations

After analysis we have found the complexity of cybersecurity and getting new hires from having no experience in cybersecurity to becoming an expert requires a 3-phase approach to learning development. Phases 2 and 3 require simulation creation and real-time problem resolution with two cases that compromise 90% of Core Lab case work: Business Email Compromise and Ransomware. However, before we can implement Phases 2 and 3 of learning creation, we must create a platform to meet the workload demand coming in 4 months. The table below is Phase 1 training implementation that includes the problems we are solving, their root causes, solutions to these problems, and actions we must take to complete the project.

Problem	Root Cause	Solutions	Actions
No process for obtaining system accesses once onboarded	-Director of Security Engineering resolves issues for the company and individuals within multiple departments (e.g., granting accesses) -Lack of procedures or documentation for new hires	-With core lab manager and Director of Security Engineering, document and create a checklist for each item a new hire requires access for. -Create an 'in-house' onboarding team on Microsoft Teams and delegate which items can be automated, completed by an assistant, or requires management -Create task cards on Teams and assign them to each in-house onboarding personnel -Once a new hire has accepted job offer, have core lab manger notify team on Teams to begin the process, then grant new hire viewing rights to team and require new hire to maintain and contact individuals if access is delayed (names will be on task cards within Teams)	-Schedule a meeting to align tasks required for access and information needed before granted access -ID will utilize and update parent company's (*Agents*) onboarding packet to current requirements of access per the Security of Engineering -Build a homepage and additional page on SharePoint to host new hire content -Develop an Onboarding Team and task cards within Microsoft Teams to assign individuals and tasks

Problem	Root Cause	Solutions	Actions
No training on investigating digital forensics	-A SANS course costs between $6-8K per person -Each digital artifact is different and requires multiple avenues to investigate depending on the context -Focus of priority on management for development -Core Lab Services Manager is the trainer and leader (no dedicated personnel)	-Insert a 1-year requirement for new hires in Core Lab Services to stay at company -Develop a one-month roadmap for technical training: -First two weeks – SANS GCFE class -Third week - new hires take what they learned in SANS and shadow senior consultants. Conduct a 1-hour meeting with management, new hires, and senior consultants to have a 'meet and greet' meeting and the purpose of the next two weeks shadowing and mentoring (1 new hire to 1 mentor). Ask senior consultants to record their screens with Teams during this week -Fourth week - new hires complete a BEC or Ransomware case with a senior mentor 'on call' (an as need basis) -Develop a job aid 'playbook' for basic actions: -pulling data -assessing what the data can tell the investigator -applying the data for solutions -identify baseline of clean evidence versus infected -keyboard shortcuts for software tools	-Give current contract to legal team of parent company to develop a 1-year sign-on agreement for new hires -Contact SANS about group packages, class schedules, requirements to take courses, and obtain any information they have prior to course offering -Work with senior consulting team to develop a rubric for items to discuss when mentoring and time availability schedules -Schedule 3-weekly meetings with the Managing Principle of DFIR to develop playbook -Add transcript and trim screen recordings

Project Management Documentation

Project Overview

Phase 1 training implementation requires collaboration with *CyberCompany*'s Core Lab Manager, the Director of Security Engineering, Technical Writer, and the Managing Principle of DFIR. We will communicate via email and meet via Microsoft Teams. Whitney Salas will present a weekly status update of project deliverables. The following personnel will work with Whitney to complete the assigned tasks:

- Technical Writer – Branding, colors, tone/voice, keywords & marketing emails
- Director of Security Engineering – System access content
- Senior Consultants – Screen recordings
- Managing Principle of DFIR – Playbook reviews

Scope of Work

Sub-Phase	Title	Description of Services	Estimated Time in Hours
1	Needs Analysis	• Content and external company research, with meetings • Kickoff meeting with key stakeholders to set project goals • Interviews with SMEs • Interviews with learners (up to 2 learners and 2 personnel in management) • Observe tenured SME completing job task • Gather current documents and resources and data analysis • Develop Internal Content Playbook (branding, colors, tone/voice, key words) in collaboration with the Technical Writer of *CyberCompany*.	70
2	Curriculum Content Development	• Determine onboarding committee and content • Determine FAQs • Write an onboarding checklist with links (1 round review) • Write a workbook content for up to 6 key concepts with examples per concept • Revise (2 rounds review) in accordance with author input • Up to 1 onboarding checklist, 1 job aid, 1 FAQ page	40
3	SharePoint Webpage and Microsoft Teams Development	• Create a wireframe for 2 SharePoint pages (home page and new hire page) (2 rounds review) • Outline content for onboarding webpage • Outline and develop Microsoft Team and task cards • Match key resources to committee members	40

		• Revise webpages and task cards per feedback (1 round review)	
Phase	Title	Description of Services	Estimated Time in Hours
4	Recording Content Needs	• Write guideline of screen recording • Walk-through screen recordings with senior member • Trim recordings to sizable content • Write transcripts • Revise (1 round review) in collaboration with senior member • Up to 10 video screen recordings	200
5	Marketing	• Develop wording for marketing emails about the new SharePoint page and its new hire content • Write emails with Technical Writer (1 round review with Executive team)	5
6	Upload/ Implementation	• Upload content into SharePoint and Teams • Schedule emails on a daily schedule for 1 week	5
	Misc	• Miscellaneous meetings and project management	40
TOTAL			400
ESTIMATED COMPLETION TIME			12-15 weeks

Review Schedules

Four (4) reviews will be provided within the scope of work for each sub-phase.

- Review 1 – Curriculum Content Review
  - Review 1.5 – Accuracy and Pass
- Review 2 – Web Tools Review
- Review 3 – Recordings Review
  - Review 3.5 – Accuracy and Pass
- Review 4 – Marketing Review

If excessive reviews and/or change requests are requested in Review 1 and Review 4, cost may go up. These include large style changes.