San Jacinto College Pipeline for Cybersecurity Careers Aligned to National Standards: Program Year 1 Evaluation Report

May 30, 2025

HELIX SOLUTIONS

HELIX SOLUTIONS

THIS DOCUMENT IS:

CONTROLLED BY:	Helix Solutions 1107 E. Robinson Ave El Paso, Texas 79902
PREPARED UNDER:	Contract with San Jacinto College
PREPARED ON:	Adobe InDesign (Version 20.3.1)
DOCUMENT NO:	2023-41-DOC-1
TITLE:	**San Jacinto College Pipeline for Cybersecurity Careers Aligned to National Standards: Program Year 1 Evaluation Report**
ORIGINAL RELEASE DATE:	May 30, 2025

PREPARED BY:

Randy Taylor
rstaylor@helixeval.com
(915) 478-1918

Jane Choi
hschoi@helixeval.com

Christopher Villa
cvilla@helixeval.com
(915) 526-2042

REVISIONS

LTR	DESCRIPTION	DATE	APPROVAL
NEW	Initial Release.	05/30/25	C. Villa

Table of Contents

List of Tables

List of Figures

Section 1: Introduction

San Jacinto College (SJC, https://sanjac.edu), located at 4620 Fairmont Parkway, Pasadena, Texas 77504, contracted with Helix Solutions, LLC (https://www.helixeval.com), located at 1107 E Robinson Ave, El Paso, Texas 79902, to evaluate its *Pipeline for Cybersecurity Careers Aligned to National Standards* (PCCANS) program. The project is supported by the National Science Foundation's (NSF) *Advanced Technological Education opportunity* (ATE): *Hispanic-Serving Institutions* (HSI Program) (Award Number 2350310). The current report provides the evaluation findings from the inaugural year (June 15, 2024, to May 31, 2025). The grant period is estimated to end in May 2027.

The project's Principal Investigator (PI) and co-PIs are as follows:

- Alyssa Phillips (Principal Investigator)
- David Carpenter (Co-Principal Investigator)
- Eric Servin (Co-Principal Investigator)

Section 1-1: Brief Description of the Program

The SJC PCCANS program broadly addresses shortages in the cybersecurity workforce within the Gulf Coast region of Texas. The program's goal is to prepare SJC students for immediate entry into the cybersecurity workforce or continued education in a bachelor's degree program or beyond. To achieve these aims, the program is focused on:

- Identifying national education standards and industry needs
- Aligning program curriculum and activities to standards and needs
- Providing real-world, hands-on cybersecurity experience

To identify national education standards and industry needs, the program design included obtaining the National Security Agency Center of Academic Excellence (CAE) designation, which recognizes rigorous, high-quality programs. Completing the process takes several months and requires the collection and review of information from various institutional data sources. To identify the market needs of the cybersecurity industry, the program included a Cybersecurity Advisory Committee through which industry partners provided their input on the needs of the field.

The program plans included obtaining CAE designation by developing an internal report summarizing national and local cybersecurity education standards, which will serve as the basis from which the existing curriculum can be supplemented and modified to be in alignment. Alignment activities will focus on updating semester courses as well as supplemental labs. Alignment activities will be documented through new syllabi being created and disseminated, as well as course instructors (faculty and adjunct) being provided guidance to ensure that students receive relevant, high-quality cybersecurity instruction.

In addition to enhanced instruction, the program will provide students with real-world and hands-on cybersecurity experience to give them a better understanding of what working in the cybersecurity

field is like and make students more competitive in the job market and for continued educational opportunities (such as transferring to a four-year college). These experiences will include students working in SJC's Security Operations Center (SOC), a centralized team within an organization that monitors and responds to cybersecurity threats.

Section 2: Evaluation Methods

As discussed in the initial grant proposal, the evaluation team focused on conducting a formative project assessment. Also called "process evaluations," formative evaluation studies assess a project's implementation, satisfaction, and fidelity. Rossi, Lipsey, and Freeman (2004) explain that "audiences for formation evaluations typically are program planners, administrators, oversight boards, or funders with an interest in optimizing the program's effectiveness" (p. 34). The primary goal of the formative evaluation is to identify key successes, challenges, and lessons learned from the first program year (PY1) of implementation, as well as develop strategies to improve overall implementation. The current report will describe the steps to understand the extent to which SJC PCCANS program activities have been implemented as intended. The evaluation team used several approaches to determine the assessment, including:

- Conducting a site visit
- Developed a logic model
- Conduct a focus group with the project team
- Developed a fidelity matrix

The following sections provide additional details on the methods of the approaches mentioned above.

Section 2-1: Site Visit

Helix Solutions consultants Christopher Villa and Randy Taylor conducted a two-day site visit on Monday, March 24, and Tuesday, March 25, 2025. The purpose of the visit was to obtain a comprehensive understanding of PY1 progress and accomplishments. The visit included the following activities:

1. Guided tour of the newly built SOC
2. Collaborative refinement of the project's logic model
3. Focus group with project leaders to uncover implementation successes and challenges
4. Review and update the project's fidelity matrix
5. Continuous Quality Improvement meeting to discuss the feedback and next steps

Appendix A contains the full agenda for the site visit. The evaluation team shared a draft agenda with the project team in advance and incorporated their feedback and input. Although the agenda included two focus group sessions—one with the project team and PIs and another with instructors—the second was deemed unnecessary on-site since the same individuals (i.e., the PIs) filled both roles. Therefore, only the first focus group was held, and the evaluation team incorporated the planned questions from both focus group scripts into the one session.

Section 2-2: Logic Model Development

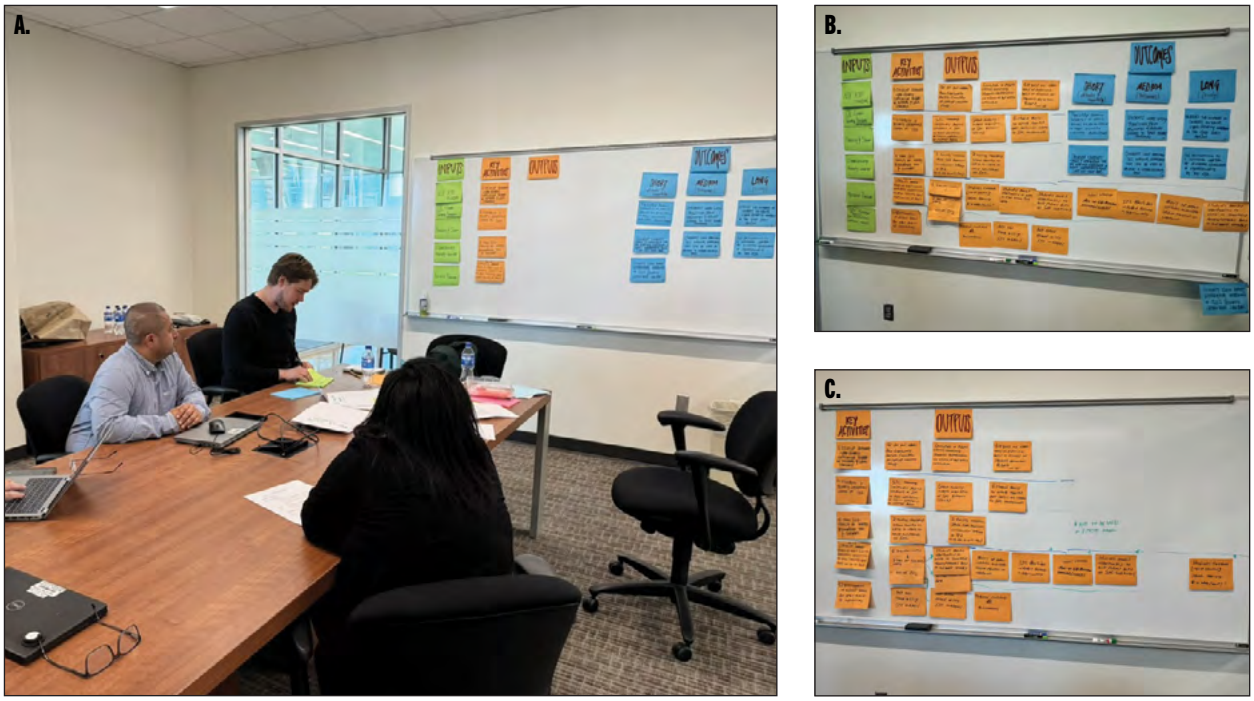
A logic model is a visual roadmap that defines the relationships and sequence between the program components and outcomes. Knowlton and Phillips (2013) describe logic models as a "way to describe and share an understanding of relationships (or connections) among elements necessary to operate the program or change effort" (p. 4). Once developed, a logic model:

- Established a common language between stakeholders
- Documents inputs, outputs, and intended outcomes (i.e., results)
- Provides a reporting framework
- Guides refinements in program delivery (Knowlton and Phillips, 2013)

For the SJC PCCANS project, the logic model will help project and evaluation teams and NSF officers to plan and coordinate implementation, monitor progress, and align expectations. Moreover, because teams must specify the program components and intended outcomes, logic models help track program successes and opportunities for refinement, supporting strong implementation and continuous improvement (Stewart et al., 2022).

To take advantage of the varied perspectives offered by the principal investigators who planned and implemented SJC PCCANS and the evaluation team (Patton, 2015), they collaboratively created the logic model. During the two-day site visit, the evaluation and project teams filled a whiteboard with

Figure 2-1: Logic Model Refinement Sessions with SJC PCCANS Project Team and the Evaluators (March 2025)



A. Evaluators and project staff refine the PCCANS logic model together during the site visit (March 24-25, 2025). **B.** End of Day 1: Preliminary arrangement of logic-model components. **C.** End of Day 2: Finalized "Key Activities" and "Outputs" sections after further discussion.

color-coded sticky notes, through in-depth discussion, to add, rearrange, and remove notes until every component was placed under the appropriate logic model inputs, key activities, outputs, and outcomes sections, as shown in Figure 2-1 on the previous page.

Creating the logic model in person, rather than virtually, offered several advantages. Meeting face-to-face allowed the teams to leverage their physical presence to foster interpersonal connections and trust, leverage nonverbal communication that is less available remotely, and promote dynamic brainstorming and efficient iterative thinking. Moreover, being in-person provided the evaluation team with contextual awareness and the local context of the SJC PCCANS project.

Section 2-3: Program Staff Focus Group

The evaluation team endeavored to gain insight into the program's first year of implementation from the perspective of the project's PI, two co-PIs, and one SJC staff member. All focus group members consented to the session before any data collection. An interview script (Appendix B) was developed to gauge the focus group participants' perspectives on the successes and challenges observed throughout the first year of implementation. The interview script included six primary questions, with the evaluators and the focus group participants engaging in open discussion within the general parameters of each question. These questions included:

1. What do you see as the major activities that have been conducted during PY1 implementation?
2. What challenges has the program faced in the work conducted during PY1? And how were challenges managed or overcome?
3. What successes are you most proud of?
4. How do you envision the lessons learned from PY1 being carried forward into the upcoming years of implementation?
5. Is there anything else you would like to tell us about the PY1 implementation of the Cyber Security program?

As mentioned earlier, the evaluation team had also planned to interview SJC faculty (i.e., those responsible for implementing the new curriculum). However, during the site visit, the evaluation team learned that the project PIs were the leading SJC faculty, apart from a few adjunct professors. It was determined that the additional focus group with SJC faculty was not needed. See Appendix C for a copy of the initial faculty script.

The focus group meeting lasted approximately 80 minutes on March 24, 2025, on the first day of the evaluators' site visit. Audio recordings of the interviews were uploaded to an online transcription service, Rev (https://www.rev.com). The evaluators reviewed the transcripts and conducted an open coding analysis to identify the emergent themes in the responses.

Section 2-4: Fidelity Matrix Development

During the site visit, the evaluation and project team developed a fidelity matrix to assess how the project implemented its proposed program activities. Appendix D provides a copy of the project's fidelity matrix. In other words, the fidelity matrix provides a framework to determine whether the program activities occur as initially proposed. This matrix is a scoring system for measuring the fidelity of each of the project's five key activities (or components) as noted below:

1. Develop an Enhanced Cybersecurity Curriculum Aligned with National and Local Standards
2. Establish a SOC at SJC
3. Train SJC Faculty on Industry-Recommended Tools and Software
4. Provide SJC Students with Hands-On Cybersecurity Workforce Experience to Build Industry-Based and Knowledge
5. Disseminate Lessons Learned and Evidence-based Practices with Other Higher Institutions

The project's logic model served as the base for the fidelity matrix. The evaluators rely on the fidelity matrix to determine how the project implemented its planned components (e.g., whether it built a SOC or whether faculty completed their Splunk certifications). The evaluation and the project teams established levels for adequate (i.e., "adequate fidelity") and inadequate (i.e., "low fidelity") implementation fidelity by setting threshold scores. Lammert, Heinemeir, Schaaf, Fiore, and Howell (2016) define threshold scores as "numeric scores that are used to define different levels of fidelity of a specific indicator" (124).

Said differently, the fidelity matrix assigns scores for possible levels of implementation: inadequate, adequate, or high. For example, four points will be awarded if two faculty complete their Splunk Core Power User certification (i.e., "Adequate Fidelity"), suggesting that the PIs had met plan implementation targets. However, two additional points can be awarded if more than two faculty members complete the course, indicating that the project exceeded its implementation expectations (i.e., "high fidelity"). On the other hand, no points would be given if fewer than two faculty members complete the course (i.e., "low fidelity"). Low fidelity indicates that the project fell short of its implementation objective. **Lower-than-expected scores highlight possible areas for programmatic improvement for the following program years.**

Table 2-1 provides the project's threshold scores for the project's first year of implementation (PY1). The threshold scores indicate the minimum for adequate implementation established by the evaluation team and PIs.

Table 2-1: PCCANS PY1 Score Range and Threshold Score by Key Component

Key Component No.	Key Component	Score Range	Threshold Score
1	Develop an Enhanced Cybersecurity Curriculum Aligned with National and Local Standards	0–5	5
2	Establish a SOC at SJC	0–16	14
3	Train SJC Faculty on Industry-Recommended Tools and Software*	N/A	N/A
4	Project SJC Student with Hands-On Workforce Experience to Build Industry-Based Skills and Knowledge*	N/A	N/A
5	Disseminate Lessons Learned and Evidence-based Practices with Other Higher Institutions*	N/A	N/A
	Total	0–21	19

*The activities will occur starting in PY2.

Not all implementation components (and sub-activities) occur each year. As a result, some implementation activities will be assessed at different program years. For example, Key Components 2 and 3 are scheduled to start in PY2, while some of the activities in Key Component (e.g., build a SOC) will occur only once.

Section 3: Evaluation Findings

The following sections provide the evaluation findings for PY1.

Section 3-1: Security Operations Center Tour

The site visit opened with a 30-minute guided tour of the newly built SOC in Building 2 on the college's South Campus. Senior Director of Cybersecurity Programs Rizwan Virani welcomed the evaluation team and provided an overview of the center's purpose and operations, including explaining its systems. Further, it was noted that SJC's Information Technology Services (ITS) built and financed the facility. Joshua Dray, SJC Chief Information Security Officer, Eric Servin, co-PI, and Kevin Morris, Dean of Business and Technology, joined the tour later.

The SOC, the dedicated space built in a classroom, was designed to mimic an industry-standard SOC. See Figure 3-1 for photos taken during the site visit. The classroom included four large wall-mounted displays. While a live demonstration did not occur during the site visit, it was explained that the display information included the college's network health and other monitoring metrics. The space was also outfitted with 15 student workstations, two technician workstations, and an instructor podium. The SOC's layout matched what was described in the initial proposal under Objective 2 (Creation of an SOC), Activity 2.1 (Setting Up a Physical SOC). The proposal states that the SOC will

include “multiple large-screen displays… as well as workstations from which students can work their investigations and remediation labs” (SJC, 2023, p. 10). The space observed by the evaluation team matched this description.

Figure 3-1: San Jacinto College Security Operations Center (March 2025)

Chief Information Security Officer Josh Dray explained that the center offers SJC students the same tools and experiences as cybersecurity professionals. For example, the SOC relies on Splunk, an industry-standard security information and event management platform. The evaluation team had the following impressions at the end of the tour: 1) the grant supported and facilitated the construction of the SOC, 2) the SOC appears to replicate industry practice needed to provide SJC students with hands-on experience, and 3) the dedicated space demonstrates the college’s commitment to cybersecurity.

Section 3-2: Logic Model

As described in the Evaluation Methods section, the purpose of the logic model is to visually show the program components, the relationship and sequence between the components, and the outcomes. The SJC PCCANS logic model has four sections: 1) inputs, 2) key activities, 3) outputs, and 4) outcomes. The sequence of programs is visualized in logic models by the inputs and activities that drive the outputs, which drive the outcomes. Developed in coordination with the project team, the logic model (see Appendix E) demonstrates the anticipated flow for specific activities and their related outputs and outcomes.

The following sections describe the inputs, activities, outputs, and outcomes.

Section 3-2-1: Inputs

The inputs are the resources required to implement the program, including the NSF ATE funding, the SJC Cybersecurity Program infrastructure, the SJC faculty and staff who will implement SJC PCCANS,

the program partners (the Cybersecurity Advisory Committee), and SJC's funding and resources, including the SOC Construction, software funds, and existing cybersecurity curricula.

Section 3-2-2: Key Activities and Outputs

The activities are the actions necessary for SJC PCCANS implementation, and the outputs are the tasks that show that SJC PCCANS is being implemented well. SJC PCCANS has five key activities.

KEY ACTIVITY 1: Develop an Enhanced Cybersecurity Curriculum Aligned with National and Local Standards

The first key activity is to develop an enhanced cybersecurity curriculum that is aligned with national standards and local business standards. Successful implementation of this key activity will be demonstrated by the following **outputs**:

- The SJC Cybersecurity program earns the Center of Academic Excellence (CAE) designation
- The cybersecurity committee provides two updates a year on current cybersecurity industry trends
- The principal investigators provide an internal report summarizing national and local curriculum standards and the alignment of existing cybersecurity curriculum against those standards
- SJC will update its curriculum, including syllabi, to align with the national and local standards

KEY ACTIVITY 2: Establish a Security Operations Center at SJC

The second key activity is to establish an SOC at SJC, and the **outputs** that indicate the successful establishment of an SOC are:

- SJC constructs the physical components to have a working SOC by installing 15 student workstations, two technician workstations, and one instructor podium.
- SJC maintains Splunk, a cybersecurity defense license.
- SJC establishes a process to connect the data sources needed to support the SOC environment.

KEY ACTIVITY 3: Train SJC Faculty on Industry-Recommended Tools and Software

The third key activity is to train SJC faculty on the tools and software recommended by the cybersecurity industry. The necessary **outputs** are:

- To conduct two meetings per year in the fall and spring between faculty and CISO to update the SOC based on the latest needs and trends.
- To have two faculty members complete the Splunk Core Power User certification by program year 2.

KEY ACTIVITY 4: Provide SJC Students with Hands-on Cybersecurity Workforce Experience to Build Industry-based Skills and Knowledge

The fourth key activity is to provide hands-on cybersecurity workforce experience to students so they can use and further develop their skills and knowledge. The **outputs** for this activity are:

- To have six courses and two labs each semester by the end of PY2.
- For SJC to facilitate student internships.
- For SJC to sign a Memorandum of Understanding with a partner institution to facilitate student transfer and enrollment to the partner institution.
- For students to build resumes based on their SOC experiences.
- For SJC to offer a Bachelor of Applied Technology in IT-Cybersecurity
- For students to complete the Splunk training modules.

KEY ACTIVITY 5: Disseminate Lessons Learned and Evidence-based Practices with Other Higher-Education Institutions

The fifth activity is to share the lessons that the project team learned to benefit other higher education institutions. The **outputs** for this activity are:

- SJC will post lab modules on existing SJC websites.
- SJC will post course syllabi on existing SJC websites.
- SJC will present at one or more ATE conferences

Section 3-2-3: Outcomes

The final section of the logic model details the project's intended outcomes, which should be achieved with the necessary inputs, key activities, and outputs. The outcomes are organized into the short-term, medium-term, and long-term outcomes. The **short-term outcomes** are that faculty are updated on the latest trends and developments in cybersecurity skills and tools, and that students develop the skills and knowledge they need to gain employment in a direct cybersecurity role. The **medium-term outcomes** are that students will transition easily from an Associate's degree program to a Bachelor's degree program and gain work experience from the SOC that they can use to obtain a future job in cybersecurity. The **long-term outcomes** are that SJC increases the number of students entering the cybersecurity workforce in the Gulf Coast region and that SJC is designated as a National Center of Academic Excellence in Cybersecurity by the National Security Agency (CAE).

Section 3-3: Program Staff Interview(s)/Focus Group

In a focus group with four SJC PCCANS team members, they described their perceptions and experiences with the first year of SJC PCCANS, including the project's implementation successes and challenges.

Section 3-3-1: Successes

Overall, the focus group participants characterized PY1 as one of many successes and accomplishments. They described coming together as a cohesive team to plan for the program,

establish needed infrastructure, secure grant funding, align the curriculum to national and local standards, and launch the SOC. The participants emphasized that these achievements were made possible by SJC leadership buy-in and support, coupled with strong inter-departmental collaborations. They also attributed their success to their concrete planning during the NSF grant writing phase, helping them to prioritize and implement key activities efficiently in the first program year. Additionally, participants noted that the SJC PCCANS project is aligned with existing departmental goals and that strong instructors are leading the coursework.

KEY SUCCESS 1:

The first key success was that the project team had full support from SJC leadership across levels to build out the SJC Cybersecurity program. SJC's strategic leadership team (including the provost, chancellor, and vice chancellor), SJC's president, and dean were all invested in this program. Participants described how SJC had plans to enhance the Cybersecurity program and hired full-time faculty with industry experience to lead this initiative prior to the NSF ATE grant. Moreover, SJC leader buy-in helped them easily obtain necessary approvals to initiate SJC PCCANS with one participant who revealed, "Yeah, the paperwork may require 12 signatures, but we had no trouble getting all 12." In addition, participants said that because SJC leaders shared their commitment publicly, other SJC departments were more motivated to support the project teams' efforts. As one participant put it, "I mean, when the president gets up there and announces you're starting a Bachelor's in Cybersecurity, it makes it easier to get support for cybersecurity programs from other people [in SJC]." Another participant said they experienced "no pushback" from SJC throughout PY1.

KEY SUCCESS 2:

The second key success is that strong collaboration across different SJC departments and their advisory committee enabled them to accomplish their goals quicker than anticipated. As described earlier, this was largely because of SJC leadership buy-in, but participants also expressed the commitment they observed throughout various partnerships, especially with the college's IT Department, which took financial and logistical responsibility for building the SOC. Participants shared how IT staff were "on board with the concept and seeing the students involved [with gaining hands-on experience providing Cybersecurity support to SJC]. That's something that he's a fan of." Participants repeatedly described being in awe at how efficiently and successfully the IT Department accomplished the major endeavor of establishing the SOC, despite not having direct oversight of the department. The following exchange demonstrates this efficiency:

Participant 1: I was slightly doubtful [we would get everything done in a year] simply just because of how much of it was out of our hands. The three of us [the PI and co-PIs] did very little to make that room an actual thing. We had to rely on the goodness of [the IT Department's] heart and their time, and funding streams. And yeah, so I wasn't ever doubtful it would get done, I was pleasantly surprised-

Participant 1: How quickly.

Participant 2: How quickly and how well.

KEY SUCCESS 3:

The third key success was that before the start of the grant and as part of drafting the NSF ATE proposal, the project team created detailed plans in collaboration with other SJC departments, such as the IT Department. As one participant put it, this meant that once "[the grant] was awarded, we started rolling" without needing a long, drawn-out start-up phase. As part of the initial planning, the participants described how they had in-depth and iterative discussions with the Grants Office and the IT department to ascertain what was feasible and the timeline, as well as what resources were required. One participant described this in detail:

> So, I think we did a really good job setting everything up while we were writing the grant. So, once we got the grant, everything just kind of got pushed in motion. 'Cause we already had articulated with IT what our next steps would be once we get the grant. Like, this is what's going to happen. Take this, we need to do... We need Splunk, we need this. They knew what it was. So, once we got the okay that the grant came in, it was just like, implement. So, that's why a lot of this was easy for us to navigate through once we got the grant, 'cause the footwork was already done as if we were going to get it.

KEY SUCCESS 4:

The fourth key success was obtaining the NSF ATE funding, which gave the Cybersecurity Department the needed resources to realize its long-standing goals: launching a Bachelor's degree program and attaining CAE designation. Without the grant support, the department did not have the staffing, material, or financial resources to move these initiatives forward. As part of the SJC PCCANS project, the team reviewed and revised the existing curriculum, aligning it with CAE standards. Participants shared that the existing Cybersecurity curriculum was mainly aligned with CAE standards. They only needed to make three main changes to align their existing curriculum with CAE standards: update the scope and sequence, remove two classes (Introduction to Operating Systems and Databases), and add two classes (Computer Programming and Networking). They obtained CAE designation during the grant period, which they see as a success because it "opened the doors for other grants for us as well" and will "pull more students in who are looking for an accredited college."

KEY SUCCESS 5:

The fifth key success was having self-motivated and passionate instructors teach courses. Participants said that both the full-time and part-time instructors had industry backgrounds, which is helpful for students to have practical examples. Participants also showcased how their part-time instructors had full-time jobs in cybersecurity but were still instructors of "the best caliber" because the Cybersecurity Department "[pushes] students to have more hands-on experience, have certifications, things like that, we expect that same from our part-time faculty." In addition, they stated that the part-time instructors are teaching because:

> They want to pass on the knowledge [they have]. So, they have that passion. They're not doing this to get rich, let's just say that, right? But they're doing this out of a sense of kind of duty. This is what they want to do with the spare time that they have after they're working their 9:00 to 5:00.

Section 3-3-2: Challenges

The two major challenges participants shared were getting students to come in-person to the SOC to take advantage of its benefits and boosting the SJC Cybersecurity program's reputation among the local industry to make hiring the Cybersecurity Department graduates more appealing.

KEY CHALLENGE 1:

Participants shared that while students were excited about the SOC, getting students in the door of the SOC was a challenge. Like other two-year colleges, SJC offered all its courses entirely online or through a hybrid model, so most students took them online. Moreover, the SJC campus is divided into north, central, and south campuses, and the commute between the campuses can be challenging, sometimes taking over an hour due to Houston's heavy traffic. Consequently, students enrolled in classes at the North Campus were often reluctant to travel to the SOC on the South Campus because of the inconvenience and added burden that such a commute presents. Participants said they were working on ways to get students into the SOC or make changes so that students can take advantage of the SOC remotely:

> [SOC] participation is something we have to figure [out] as we develop this. Okay, is it going to be a different experience for the in-person kid from the online kid? [...] I mean, end of the day, the SOC really is virtual anyhow, but it's still not quite the same experience [if you are not in-person]. So that'll be an obstacle we have to sort out.

KEY CHALLENGE 2:

The second challenge participants shared was increasing the SJC Cybersecurity program's reputation among the local industry. Participants shared the desire to market the program and students to show the rigor of the program, how capable the students are, and to facilitate students' career prospects:

> We have some very highly qualified, excellent... But they're not hiring our kids. The folks that are hiring our kids aren't the ones that are sitting on our advisory committee [so they don't know about our program]. So, it's kind of a two different effort thing that we need to do. There's a marketing piece to market our program and our students locally.

Relatedly, participants shared the continual need to make sure that the Cybersecurity program was in alignment with what hiring managers and human resources departments want in potential employees. They shared that where students previously struggled was in showing they have hands-on experience, but that the SOC fills this gap:

> If you look at the three components that you need to have a successful start-up in your career, you need education. [...] You need certifications. [...] And then number three is experience, and that's the part that has always been a struggle. So that's where, if we can get more hands-on with the SOC, we can give them that third component that will set themselves apart from other candidates going after the same position. And those three, if you have all of those three boxes checked, you're much more of an attractive candidate on paper.

In sum, the first project year was largely a success for SJC PCCANS, and the project team accomplished more than they had anticipated, such as building the SOC and attaining CAE designation. Participants noted that they still faced challenges drawing their students in person to experience the full benefits of the program and market SJC's Cybersecurity program to local organizations to promote the hiring of their students. However, participants' reports indicate that SJC PCCANS's many accomplishments, particularly the development of the SOC, were meaningful to students. Students expressed excitement to the participants about the opening of the SOC and that it was a major draw for them to continue through SJC's Cybersecurity program rather than transfer to a larger school:

> Some kids come in here thinking that they might just take a few classes [at SJC] and transfer to [the University of Houston], and I've had students think that, and then once we told them about the SOC, they're like, "Oh, I'm staying. Never mind."

Section 3-4: Fidelity Matrix

Table 3-1 below provides each key component's threshold and implementation scores. **Overall, the fidelity matrix findings suggest that the project implemented activities as planned.** Specifically, the project accomplished its two planned tasks defined under key component numbers 1 and 2.

Table 3-1: PY1 Threshold and Implementation Scores by Key Component

Key Component No.	Key Component	Threshold Score	Implementation Score
1	Develop an Enhanced Cybersecurity Curriculum Aligned with National and Local Standards	5	5
2	Establish a SOC at SJC	14	14
3	Train SJC Faculty on Industry-Recommended Tools and Software*	N/A	N/A
4	Project SJC Student with Hands-On Workforce Experience to Build Industry-Based Skills and Knowledge*	N/A	N/A
5	Disseminate Lessons Learned and Evidence-based Practices with Other Higher Institutions*	N/A	N/A
	Total	19	19

*The activities will occur starting in PY2.

Section 3-4-1: Develop an Enhanced Cybersecurity Curriculum

In 2025, SJC earned the CAE designation through the National Security Agency (NSA), which continues through 2030. The designation indicates that the program satisfied the cybersecurity standards established by the NSA. Focus group findings revealed that Senior Director of Cybersecurity Programs Rizwan Virani led the successful application effort. The college announced the honor on April 8, 2025, in a new release titled, "San Jacinto College Designated as a National Center of Academic Excellence in Cyber Defense" (Conger, 2025). Table 3-2 noted that the project met the threshold score for this activity, earning four points.

SJC records show that the project convened a Cybersecurity Advisory Committee made up of college faculty and staff, together with industry partners. Partners included representatives from Cisco, W&T Offshore, Splunk, Alliantgroup, JP Morgan Chase, and Cyber Defense Advisors, to name a few. The committee met twice: once on October 17, 2024, and then again on February 20, 2025. These meetings satisfied the component activity number 1-2, earning one point.

Table 3-2: PY1 Threshold and Implementation Scores for Key Component 1: Develop an Enhanced Cybersecurity Curriculum

Component Activity No.	Description	Threshold Score	Implementation Score
1-1	SJC Cybersecurity Programs earns the CAE designation	4	4
1-2	Meeting conducted with industry professionals and SJC faculty and staff	1	1
1-3	A report documenting the Cybersecurity standards against the SJC curriculum*	N/A	N/A
1-4	After review, SJC updates the curriculum syllabi*	N/A	N/A
	Total	5	5

*The activities will occur starting in PY2.

Section 3-4-2: Establish a Security Operations Center

The SOC in Building 2 on the South Campus is now fully operational, earning an implementation score of eight points, as noted in Table 3-3. The classroom features four large flat-screen displays on the front wall, 15 student workstations, two technician stations, and an instructor podium. Focus group participants noted that the build-out, led by San Jacinto College's Information Technology Services (ITS), was regarded as a top-priority project and completed in one to two months, much faster than originally planned.

The program documentation also reveals that the project supports the SOC software license, specifically Splunk, an analytics platform for monitoring IT security and events. As shown in Table 3-3, two points were awarded for the activity.

The project achieved the threshold key-component implementation score of 14, demonstrating that every planned activity was executed as intended.

Table 3-3: PY1 Threshold and Implementation Scores for Key Component 2: Establish a SOC

Component Activity No.	Description	Threshold Score	Implementation Score
2-1	SJC outfits a physical environment with equipment sufficient to serve as a SOC	8	8
2-2	The project maintains the SOC software (Splunk) license	4	2
2-3	The process by which required data sources are connected to the SOC environment	2	2
	Total	14	14

Section 3-4-3: Train SJC Faculty

For PY1, the project did not plan to implement any Key Component 3 activities. As noted in Table 3-4, none of these activities were scored. The project plans to conduct these activities starting in PY2.

Table 3-4: PY1 Threshold and Implementation Scores for Key Component 3: Train SJC Faculty

Component Activity No.	Description	Threshold Score	Implementation Score
3-1	Meetings between faculty and CISO to update on the latest needs and trends of SOC*	N/A	N/A
3-2	Faculty complete Splunk Core Power User Certification course*	N/A	N/A
	Total	N/A	N/A

*The activities will occur starting in PY2.

Section 3-4-4: Provide SJC Students with Cybersecurity Experience

The project did not schedule any Key Component 4 activities, so Table 3-5 appropriately lists no scores for this component. Like the previous key component, the project plans to implement these activities starting in PY2.

Table 3-5: PY1 Threshold and Implementation Scores for Key Component 4: Provide SJC Students with Hands-on Cybersecurity Workforce Experience

Component Activity No.	Description	Threshold Score	Implementation Score
4-1	Lab activities integrated into six courses, creating opportunities for students to work on simulated threats/attacks based on real-world examples*	N/A	N/A
4-2	MOUs with the University of Houston to facilitate student transfer or enrollment*	N/A	N/A
	Total	N/A	N/A

*The activities will occur starting in PY2.

Section 3-4-5: Disseminate Lessons Learned and Evidence-based Practices

Finally, Key Component 5 activities were not planned for PY1. As a result, Table 3-6 contains no ratings for this component. Some activities are scheduled for the coming program year, which the evaluation team will assess at that time.

Table 3-6: PY1 Threshold and Implementation Scores for Key Component 5: Provide SJC Students with Hands-on Cybersecurity Workforce Experience

Component Activity No.	Description	Threshold Score	Implementation Score
5-1	Post labs modules and materials on existing SJC webpages*	N/A	N/A
5-2	Post course syllabi on existing SJC web pages*	N/A	N/A
5-3	Present at ATE conferences*	N/A	N/A
	Total	N/A	N/A

*The activities will occur starting in PY2.

Section 4: Conclusions and Recommendations

The evaluation team submits the following key findings and recommendations:

KEY FINDING #1:

During the site visit, the evaluation and project teams updated the logic model and, from it, built the fidelity matrix. Together, these tools link the program activities to intended outcomes and give the evaluators (and other stakeholders) a roadmap that spells out data-collection priorities, success indicators, and timelines for monitoring implementation and program effect.

The principal investigators and evaluation team met in person to co-create the logic model detailing the project's inputs, activities, outputs, and outcomes. This collaborative process was a critical step in evaluation planning, as it provided a shared foundation for developing the fidelity matrix, an instrument designed to monitor the consistency and quality of program implementation. The key activities and outcomes fed directly into the fidelity matrix, turning each activity box into a checklist item with success criteria. Both tools will guide ongoing data collection, support evidence-based decision-making, and ensure alignment between the project's goals and its implementation. Additionally, they will serve as dynamic references for continuous quality improvement and communication with project stakeholders, allowing the team to track progress, identify areas for refinement, and demonstrate accountability across the life of the grant.

The logic model and fidelity matrix are living documents, meaning that they should be reviewed and revised as the program undergoes refinement to achieve maximum impact. Thus, the evaluation team recommends that the project PIs revisit the logic model and fidelity matrix to ensure they align with current offerings and structure. Such a review should be conducted at least twice a year: once at the mid-point of the program year and again at the end of the year to maintain accuracy and to identify those programmatic components that are working and what is not working, allowing opportunities to make mid-course adjustments.

KEY FINDING #2:

Focus group discussions and fidelity matrix data confirmed that the program successfully carried out its planned key activities, most notably, constructing the SOC and achieving CAE designation. Moreover, these milestones were achieved faster than anticipated.

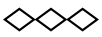
Several key drivers helped accelerate progress in program implementation. Focus group discussions highlighted strong institutional leadership support and effective collaboration with the college's IT department as critical drivers of early success, including the launching of the SOC. The project's goals were also well aligned with existing institutional priorities for expanding cybersecurity education, most notably, the pursuit of the CAE designation and the development of a bachelor's degree pathway. Because of the strong SJC leadership buy-in and the close collaboration between the project team and the college's IT department, the SOC was built, and the CAE designation was obtained ahead of schedule.

KEY FINDING #3:

The SOC is an industry-standard facility, standing out as a centerpiece of SJC's Cybersecurity program. However, the focus group findings indicate that there is work to be done to encourage students to utilize the SOC offerings.

The SOC offers SJC students hands-on and real-world experience. However, the project team noted that many students take courses remotely or, because of an onerous commute, may not go to the SOC on the South Campus if they are part of SJC's North Campus. A recommendation is for the

project team to widely promote the benefits of using the SOC in person to students using a variety of methods through short and engaging videos across its social media channels and email blasts, for example. Postings might address topics such as how the SOC enables students to gain real-life experiences, leading to faster and higher pay rates. However, there might be other outreach strategies that the college could use, including distributing flyers, brochures, and on-campus video screens. Nonetheless, by broadcasting the distinctive benefits and hands-on learning opportunities offered by the SOC, it may be compelling enough to overcome students' concerns about the inconvenience of commuting between campuses.



The SJC PCCANS project has had a strong inaugural year, with marked successes and early achievements. The evaluation will expand to assess feedback from the students enrolled in the SJC's Cybersecurity Program. It is essential that the PIs and the evaluation team maintain the regular communication and collaboration they established in PY1 as the program enters its second year. Together, the teams can ensure that the appropriate evaluation tools are in place, especially since the project intends to gather student feedback. This feedback will be important as it will provide additional insights into how the project affects students, especially how SJC contributes to fulfilling the cybersecurity talent pipeline.

References

Conger, J. (2025, April 8). *San Jacinto College Designated as a National Center of Academic Excellence in Cyber Defense. San Jacinto College*. https://www.sanjac.edu/about/news/2025/san-jac-designated-as-national-center-of-academic-excellence-in-cyber-defense.php

Knowlton, L.W. & Philips, C.C. 2013. *The Logic Model Guidebook: Better Strategies for Great Results.* Thousand Oaks: SAGE Publications, Inc.

Lammert, J. D., Heinemeier, S., Schaaf, J. M., Fiore, T.A., & Howell, B. (2016). *Evaluating special education programs: Resource Toolkit.* Rockville, MD: Westat.

Patton, M. Q. (2015). *Qualitative research & evaluation methods: Integrating theory and practice (4th ed.)*. SAGE Publications, Inc.

Rossi, P.H., Lipsey, M.W., & Freeman, H.E. (2004). *Evaluation: A Systematic Approach, Seventh Edition*. Thousand Oaks: SAGE Publications.

San Jacinto Community College District (SJC). (2023). *Pipeline for Cybersecurity Careers Aligned to National Standards (PCCANS): NSF ATE Small Projects proposal (NSF 15PG)*. National Science Foundation, Advanced Technological Education Program.

Stewart, J., Joyce, J., Haines, M., Yanoski, D., Gagnon, D., Luke, K., Rhoads, C., & Germeroth, C. (2022). *Program evaluation toolkit: Quick start guide (REL 2022–112)*. Washington, DC: U.S. Department of Education, Institute of Education Sciences, National Center for Education Evaluation and Regional Assistance, Regional Educational Laboratory Central. Retrieved December 25, 2024, from https://ies.ed.gov/ncee/edlabs/regions/central/resources/pemtoolkit/resources.asp.

List of Appendices

Appendix A: Site Visit Agenda

Evaluation Site Visit Agenda

Pipeline for Cybersecurity Careers Aligned to National Standards Project
San Jacinto College-Houston

Day 1: Sunday, March 23, 2025

Afternoon	Evaluation team arrives in Houston

Day 2: Monday, March 24, 2025

Meeting Location:	South Campus Building 2 - S2.206 13735 Beamer Rd, Houston, TX 77089
Morning	**9:30–10:00 AM**: **Tour Security Operations Center (SOC)** with *Rizwan Virani* and discuss activities related to its development and operation as well as work towards the Center of Academic Excellence (CAE) **10:30–11:00 AM:** Meet *Joshua Dray* to discuss **SOC implementation activities** **11:15–12:45 PM: Project update** as well as a review/revise of the project's **logic model** with as many members of the project team and PIs (recommended)
Lunch Break	**12:45 PM**
Afternoon	**1:30–3:00 PM**: **Program team focus group** with many members of project team and PIs (recommended). *Alyssa Phillips* and *Eric Servin* are recommended to attend to discuss their work to integrate curriculum and SOC **3:30–4:30 PM**: Discuss and begin drafting **fidelity matrix** instrument and scoring criteria with as many members of the project team and PIs (recommended)

Day 3: Tuesday, March 25, 2025

Meeting Location:	South Campus Building 2 - S2.206 13735 Beamer Rd, Houston, TX 77089
Morning	**9:30–10:30 AM**: Review/collect relevant **program records/documentation** of activities. ▪ PIs can collect relevant records and documents ahead of time, and share copies with the evaluation team to review during this time. If originals are shared, the evaluation team can make copies/take pictures ▪ Materials could include the following items: curriculum development, faculty recruitment/training, capacity building, partnership/advisory council development, etc. ~~**11:00–12:30 PM**: **Interview/focus group with faculty** who have engaged in training and/or started implementation~~

Revised: March 6, 2025

Appendix A: Site Visit Agenda

Lunch Break	**12:45 PM**
Afternoon	**1:30-2:45 PM**: Meet with program staff to **review edits made to fidelity matrix** with as many members of the project team and PIs (Recommended) **3:30–4:30 PM**: Conduct a Continuous Quality Improvement (CQI) meeting with as many members of the project team and PIs (recommended) to discuss the following: a. Review plan for evaluation report submission b. Discuss plan to obtain IRB approval for future evaluation activities, including student data c. Vision for next steps of program implementation d. Future evaluation needs/activities (estimated 1 hour) **4:30–5:00 PM:** Meet with Jason Fontaine **SJC Office of Grants Management**
Evening	Evaluation team departs Houston

Revised: March 6, 2025

Appendix B: PI Focus Group Script

San Jacinto PI Focus Group Script

Date: XXXXX

Hello, we are Randy Taylor and Christopher Villa, and we are the facilitators for today's conversation. I want to welcome each of you and thank you for being here. We are an evaluation team hired by San Jacinto College to conduct today's focus group session. The purpose of our discussion is to learn about your perspective and experience with the college's NSF Cyber Security Training program.

We want to **audio record** today's conversation unless any of you object to it. The recording is only for us—the evaluation team—and will not be shared with anyone, including San Jacinto College staff and administration. We will only use the audio recording for the purpose of writing our report. We want to make sure that we accurately report what you share with us today. That said, this conversation will be reported anonymously. In other words, your responses today will not be attributed to you in any report we produce. That said, we hope you feel comfortable speaking freely.

Do we have your permission to record today's session?

[Wait for all focus group participants to consent to the audio recording. If someone does not provide their permission, a facilitator will take notes.]

Our conversation today will be structured around four primary questions. The discussion will last no longer than one hour. Please keep in mind that this is not a test with right or wrong answers. Instead, we are seeking your opinions, reflections, and constructive feedback about the NSF Cyber Security program. That said, we realize that you may have had different experiences and opinions from each other; we would like to hear from ALL of you. So, please don't hesitate to share your thoughts!

Before we begin, there are a few ground rules. You do not need to speak in a certain order. We do ask, however, that you please stay on topic and do not interrupt each other, and please respect each other's ideas. We also ask to limit side conversations because they can interfere with the recording.

We would also like to remind you that what you say here is confidential. We ask that you do not share what was said in our discussion with anyone outside this room. Thank you!

Are there any questions thus far?

[Address all questions before more on to the next prompt.]

Let's start by introducing ourselves and saying one thing that is making you happy today.

Thank you for sharing. Next, we are going to start our planned questions and open discussion.

So, the first question is:

1. **What do you see as the major activities that have been conducted during PY1 implementation?**
    a. Probe activities towards curriculum/course development
        i. In what ways are these being aligned with national/local standards?
        ii. How are SOC and curriculum being integrated?
    b. Probe activities towards partnership (Houston CC or UH)/advisory council (community partners)
    c. Probe activities towards SOC deployment
        i. Work to align with industry identified needs/real world training to promote career attainment
    d. Probe activities towards faculty recruitment/training
    e. Probe activities towards student recruitment
    f. Probe activities towards or plans for implementation commencement

2. **What challenges has the program faced in the work conducted during PY1? And how were challenges managed or overcome?**
3. **What successes are you most proud of?**
4. **How do you envision the lessons learned from PY1 being carried forward into the upcoming years of implementation?**
    a. Are there any resources or areas of support that you envision being needed to support the program's implementation and achievement of its goals?
5. **Is there anything else you would like to tell us about the PY1 implementation of the Cyber Security program?**

Thank you for your time today. It has been great to meet and hear from you. We are just about out of time. Before we go, we'd like to quickly go around the room and allow everyone a chance to make any final comments or final reflections on today's focus group.

You can let us know whether you liked this discussion or not, tell us how we did as facilitators, talk about your plans for the future either as a student or your ideal job, or you don't have to say anything.

If anyone has any questions for us, we are happy to answer, otherwise, thank you again for your time today. We really appreciate your feedback.

Appendix C: Instructor Focus Group Script

San Jacinto Faculty Focus Group Script

Date: XXXXX

Hello, we are Randy Taylor and Christopher Villa, and we are the facilitators for today's conversation. I want to welcome each of you and thank you for being here. We are an evaluation team hired by San Jacinto College to conduct today's focus group session. The purpose of our discussion is to learn about your perspective and experience with the college's NSF Cyber Security Training program.

We want to **audio record** today's conversation unless any of you object to it. The recording is only for us—the evaluation team—and will not be shared with anyone, including San Jacinto College staff and administration. We will only use the audio recording for the purpose of writing our report. We want to make sure that we accurately report what you share with us today. That said, this conversation will be reported anonymously. In other words, your responses today will not be attributed to you in any report we produce. That said, we hope you feel comfortable speaking freely.

Do we have your permission to record today's session?

[Wait for all focus group participants to consent to the audio recording. If someone does not provide their permission, a facilitator will take notes.]

Our conversation today will be structured around four primary questions. The discussion will last no longer than 90 minutes. Please keep in mind that this is not a test with right or wrong answers. Instead, we are seeking your opinions, reflections, and constructive feedback about the NSF Cyber Security program. That said, we realize that you may have had different experiences and opinions from each other; we would like to hear from ALL of you. So, please don't hesitate to share your thoughts!

Before we begin, there are a few ground rules. You do not need to speak in a certain order. We do ask, however, that you please stay on topic and do not interrupt each other, and please respect each other's ideas. We also ask to limit side conversations because they can interfere with the recording.

We would also like to remind you that what you say here is confidential. We ask that you do not share what was said in our discussion with anyone outside this room. Thank you!

Are there any questions thus far?

[Address all questions before more on to the next prompt.]

Let's start by introducing ourselves and saying one thing that is making you happy today.

Appendix C:
Instructor Focus Group Script

Thank you for sharing. Next, we are going to start our planned questions and open discussion.

So, the first question is:

1. **What types of professional development or training have you participated in as part of the Cyber Security program?**
    a. [Tease out SOC and curriculum components if it does not happen naturally]
    b. How effective were these activities in building your confidence to use the curriculum and activities with your students?
2. **In what ways have you begun working with students, if at all?**
    a. What aspects of the curriculum or activities have students responded positively or negatively? What did they like or dislike?
    b. In what ways have you had to adapt or modify curriculum or activities based on your experience or student feedback?
        i. If no, ask about confidence/preparedness to work with students.
3. **What types of support (i.e., technical, administrative, peer, etc.) have been most helpful to you so far?**
    a. Have there been any areas where support was lacking or less effective?
    b. What areas of support would help you most moving forward?
4. **In what ways do you think that the Cyber Security program will help SJC students succeed in their future careers—whether in cybersecurity or related fields?**
5. **What suggestions do you have for improving the Cyber Security program for faculty, students, or the center as a whole?**
    a. How can the program better support teaching, learning, or engagement in cyber security?
    b. In other words, how can the program best prepare students for higher education learning and employment in cyber security?

Thank you for your time today. It has been great to meet and hear from you. We are just about out of time. Before we go, we'd like to quickly go around the room and allow everyone a chance to make any final comments or final reflections on today's focus group.

You can let us know whether you liked this discussion or not, tell us how we did as facilitators, talk about your plans for the future either as a student or your ideal job, or you don't have to say anything.

If anyone has any questions for us, we are happy to answer, otherwise, thank you again for your time today. We really appreciate your feedback.

Appendix D: Fidelity Matrix

Fidelity Matrix
Pipeline for Cybersecurity Careers Aligned to National Standards
San Jacinto Community College District

Fidelity Indicator	Definition	Unit of Implementation	Data Sources (Who, When)	Project Level of Implementation (Score – Fidelity Level: Description)	Adequate Threshold Score (Project Level)	Expected Years
Key Component 1: Develop an Enhanced Cybersecurity Curriculum Aligned with National and Local Standards						
1-1. Center of Academic Excellence (CAE) Designation	SJC Cybersecurity Programs earns the CAE designation	Documentation received from NSA	Designation documentation *Who: PIs* *When: Once in PY1*	**4 – Adequate Fidelity:** Designation earned **0 – Low Fidelity:** Designation not earned	4	PY1
1-2. Cybersecurity Advisory Committee	Meeting conducted with industry professionals and SJC faculty and staff	Number of meetings	Sign-in sheets, minutes, agendas, and/or personal notes *Who: PIs* *When: Annually*	**1 – Adequate Fidelity:** At least one meeting conducted **0 – Low Fidelity:** No meetings conducted	1	PY1–PY3
1-3. Curriculum Standards Alignment Report	A report documenting the Cybersecurity standards against the SJC curriculum	A completed internal report	Completed report *Who: PIs* *When: Annually*	**2 – Adequate Fidelity:** Report generated **0 – Low Fidelity:** No report generated	2	PY2
1-4. Update SJC syllabi	After review, SJC update the curriculum syllabi	Number of syllabi updated	Syllabi *Who: PIs & Faculty* *When: Annually*	**4 – Adequate Fidelity:** Syllabi updated* **0 – Low Fidelity:** Syllabi not updated* * If the review determined that course syllabi needed to be updated. Suppose the review determined that no course syllabi need to be updated, award 4 points.	4	PY2
			Key Component Score →	*Score range: 0–5*	*5*	*PY1*
				Score range: 0–7	*7*	*PY2*
				Score range: 0–1	*1*	*PY3*

HS Project No: 2023-41
Revision Date: May 6, 2025

1

Fidelity Matrix
Pipeline for Cybersecurity Careers Aligned to National Standards
San Jacinto Community College District

Fidelity Indicator	Definition	Unit of Implementation	Data Sources (Who, When)	Project Level of Implementation (Score – Fidelity Level: Description)	Adequate Threshold Score (Project Level)	Expected Years
Key Component 2: Establish a Security Operations Center (SOC) at SJC						
2-1. Build Security Operations Center (SOC)	SJC outfits a physical environment with equipment sufficient to serve as a SOC	A classroom with 15 student and 2 technician workstations as well as 1 instructor podium	Evaluator site visit and photographic documentation *Who: Evaluators* *When: End of PY1*	**8 – Adequate Fidelity**: SOC established **0 – Low Fidelity**: SOC not established	8	PY1
2-2. Software Purchase	The project maintains the SOC software (Splunk) license	Annual license	Purchase Orders *Who: PIs* *When: Annually*	**4 – Adequate Fidelity**: Software acquired **0 – Low Fidelity**: Software not acquired	4	PY1–PY3
2-3. Establish a process for data connections	The process by which required data sources are connected to the SOC environment	Number of product integrations	Documentation demonstrating product integrations *Who: PIs* *When: Annually*	**4 – High Fidelity**: More than seven data source integrations established **2 – Adequate Fidelity**: Seven data source integrations established **0 – Low Fidelity**: Fewer than seven data source integrations established	2	PY1
			Key Component Score →	*Score range: 0–16* *Score range: 0–4*	*14* *4*	*PY1* *PY2–PY3*
Key Component 3: Train SJC Faculty on Industry Recommended Tools and Software						
3-1. Meeting with Chief Information Security Officer* (CISO) and SJC faculty * Currently, the CISO is Josh Drary.	Meetings between faculty and CISO to update on the latest needs and trends of SOC	Number of meetings	Sign-in sheets, minutes, agendas, and/or personal notes *Who: PIs* *When: Annually*	**2 – High Fidelity**: ≥ 2 meetings per year **1 – Adequate Fidelity**: 1 meeting per year **0 – Low Fidelity**: 0 meetings per year	1	PY2-PY3

HS Project No: 2023-41
Revision Date: May 6, 2025

2

Appendix D: Fidelity Matrix

Fidelity Matrix
Pipeline for Cybersecurity Careers Aligned to National Standards
San Jacinto Community College District

Fidelity Indicator	Definition	Unit of Implementation	Data Sources (Who, When)	Project Level of Implementation (Score – Fidelity Level: Description)	Adequate Threshold Score (Project Level)	Expected Years
3-2. Faculty training	Faculty complete Splunk Core Power User Certification course	Number of faculty that completed certification course	Splunk system user documentation or certificate of completion *Who: PIs and Faculty* *When: Annually*	**6 – High Fidelity:** > 2 faculty completed certification **4 – Adequate Fidelity:** 2 faculty complete certification **0 – Low Fidelity:** < 2 faculty complete certification	4	PY2
				Score range: N/A	*N/A*	*PY1*
			Key Component Score →	*Score range: 0–8*	*5*	*PY2*
				Score range: 0–2	*1*	*PY3*
Key Component 4: Provide SJC Students with Hands-On Cybersecurity Workforce Experience to Build Industry-Based Skills and Knowledge						
4-1. Lab Activities	Lab activities integrated into six courses, creating opportunities for students to work on simulated threats/attacks based on real-world examples	Number of courses with a lab component	Course syllabi *Who: PIs* *When: Annually*	**6 – High Fidelity:** > 6 labs **4 – Adequate Fidelity:** 6 labs **0 – Low Fidelity:** < 6 labs	4	PY2
4-2. MOUs with partner institutions	MOUs with the University of Houston to facilitate student transfer or enrollment	Completed MOU	Signed MOUs *Who: PIs* *When: Annually*	**1 – Adequate Fidelity:** 1 MOU(s) completed **0 – Low Fidelity:** No MOU(s) was/were completed	1	PY2
			Key Component Score →	*Score range: N/A*	*N/A*	*PY1 & PY3*
				Score range: 0–7	*5*	*PY2*

HS Project No: 2023-41
Revision Date: May 6, 2025

3

Appendix D: Fidelity Matrix

Fidelity Matrix
Pipeline for Cybersecurity Careers Aligned to National Standards
San Jacinto Community College District

Fidelity Indicator	Definition	Unit of Implementation	Data Sources (Who, When)	Project Level of Implementation (Score – Fidelity Level: Description)	Adequate Threshold Score (Project Level)	Expected Years
Key Component 5: Disseminate Lessons Learned and Evidence-based Practices with Other Higher Institutions						
5-1. Post labs	Post labs modules and materials on existing SJC webpages	Number of labs	SJC website with posted modules and materials *Who: PIs* *When: Annually*	**2 – High Fidelity:** > 12 labs posted **1 – Adequate Fidelity:** 12 labs posted **0 – Low Fidelity:** < 12 labs posted	1	PY2–PY3
5-2. Post syllabi	Post course syllabi on existing SJC web pages	Number of syllabi	SJC website with posted syllabi *Who: PIs* *When: Annually*	**2 – High Fidelity:** > 6 six syllabi posted **1 – Adequate Fidelity:** 6 syllabi posted **0 – Low** Fidelity: < 6 syllabi posted	1	PY2–PY3
5-3. Conference presentations	Present at ATE conferences	Number of conference presentations conducted	Conference agenda and photographs *Who: PIs* *When: Annually*	**2 – High Fidelity:** >1 conference presentations **1 – Adequate Fidelity:** 1 conference presentation **0 – Low Fidelity:** 0 conference presentations	1	PY3
		Key Component Score →		*Score range: N/A*	*N/A*	*PY1*
				Score range: 0–4	*2*	*PY2*
				Score range: 0–6	*3*	*PY3*

HS Project No: 2023-41
Revision Date: May 6, 2025

4

Appendix D: Fidelity Matrix

Fidelity Matrix
Pipeline for Cybersecurity Careers Aligned to National Standards
San Jacinto Community College District

Fidelity Indicator	Definition	Unit of Implementation	Data Sources (Who, When)	Project Level of Implementation (Score – Fidelity Level: Description)	Adequate Threshold Score (Project Level)	Expected Years
				Score range: 0–21	***19***	***PY1***
			Project Score →	***Score range: 0–32***	***24***	***PY2***
				Score range: 0–13	**9**	***PY3***

HS Project No: 2023-41
Revision Date: May 6, 2025

5

Appendix E: Logic Model

SAN JACINTO COLLEGE

LOGIC MODEL: Pipeline for Cybersecurity Careers Aligned to National Standards

ULTIMATE GOAL: Develop a hands-on cybersecurity talent pipeline that fills regional and national shortage of qualified analysts by graduating job-ready SJC students from a CAE-aligned program anchored in real-world experience within a live Security Operations Center.

INPUTS

- National Science Foundation Advanced Technological Education (ATE) Funding
- San Jacinto College (SJC) Cyber Security Program Infrastructure
- SJC Faculty and Staff
- Program Partners
  - Cyber Security Advisory Committee
- SJC Funding and Resources
  - Security Operations Center (SOC) construction
  - Software funding
  - Existing curriculum

KEY ACTIVITIES

1. Develop an Enhanced Cybersecurity Curriculum Aligned with National and Local Standards
2. Establish a Security Operations Center (SOC) at SJC
3. Train SJC Faculty on Industry Recommended Tools and Software
4. Provide SJC Students with Hands-on Cybersecurity Workforce Experience to Build Industry-based Skills and Knowledge
5. Disseminate Lessons Learned and Evidence-based Practices with Other Higher-Education institutions

OUTPUTS

1-1: SJC cybersecurity program earns Center of Academic Excellence designation
1-2: Twice-yearly updates from cybersecurity advisory committee on current industry trends
1-3: Generate an internal report summarizing standards identification & alignment w/ existing curriculum
1-4: Update syllabi based on internal report findings

2-1: SJC constructs physical components of SOC: 15 student workstations, 2 technician workstations, and 1 instructor podium
2-2: Maintain Splunk (cybersecurity software) license
2-3: Establish a process to connect required data sources to SOC environment

3-1: Two meetings per year (fall/spring) between faculty and CISO to update on latest needs and trends of SOC*
3-2: Two faculty members complete Splunk Core Power User certification training by PY2

4-1: 6 Semester-long courses with two labs per semester-course by end of PY2
4-2: SJC to facilitate student internships*
4-3: A signed Memorandum of Understanding with partner institution to facilitate student transfer/enrollment
4-4: Students build résumés based on SOC experiences*
4-5: SJC to offer a Bachelor of Applied Technology in IT with an emphasis in Cybersecurity*
4-6: Students complete the Splunk training modules*

5-1: Post lab modules on existing SJC websites
5-2: Post course syllabi on existing SJC websites
5-3: Present at a minimum of one ATE conference per year

OUTCOMES

SHORT-TERM

- Faculty remain updated on latest trends and developments in cybersecurity industry skills/tools
- Develop students' skills & knowledge that are needed for employment in direct cybersecurity role (not just help desk)

MEDIUM-TERM

- Students more easily transition from Associates of Applied Science to Bachelor Degree programs
- Students gain applicable SOC working experience that can be used to obtain a cybersecurity role

LONG-TERM

- Increase the number of students entering cybersecurity workforce in the gulf coast region
- SJC designation as a National Center of Academic Excellence in cybersecurity by the NSA

Notes:
* Output activity will not be tracked in the project's fidelity matrix.
Date: May 6, 2025
HS Project No.: 2023-44