

IMPLEMENTING A DIGITAL CREDENTIALS PROGRAM





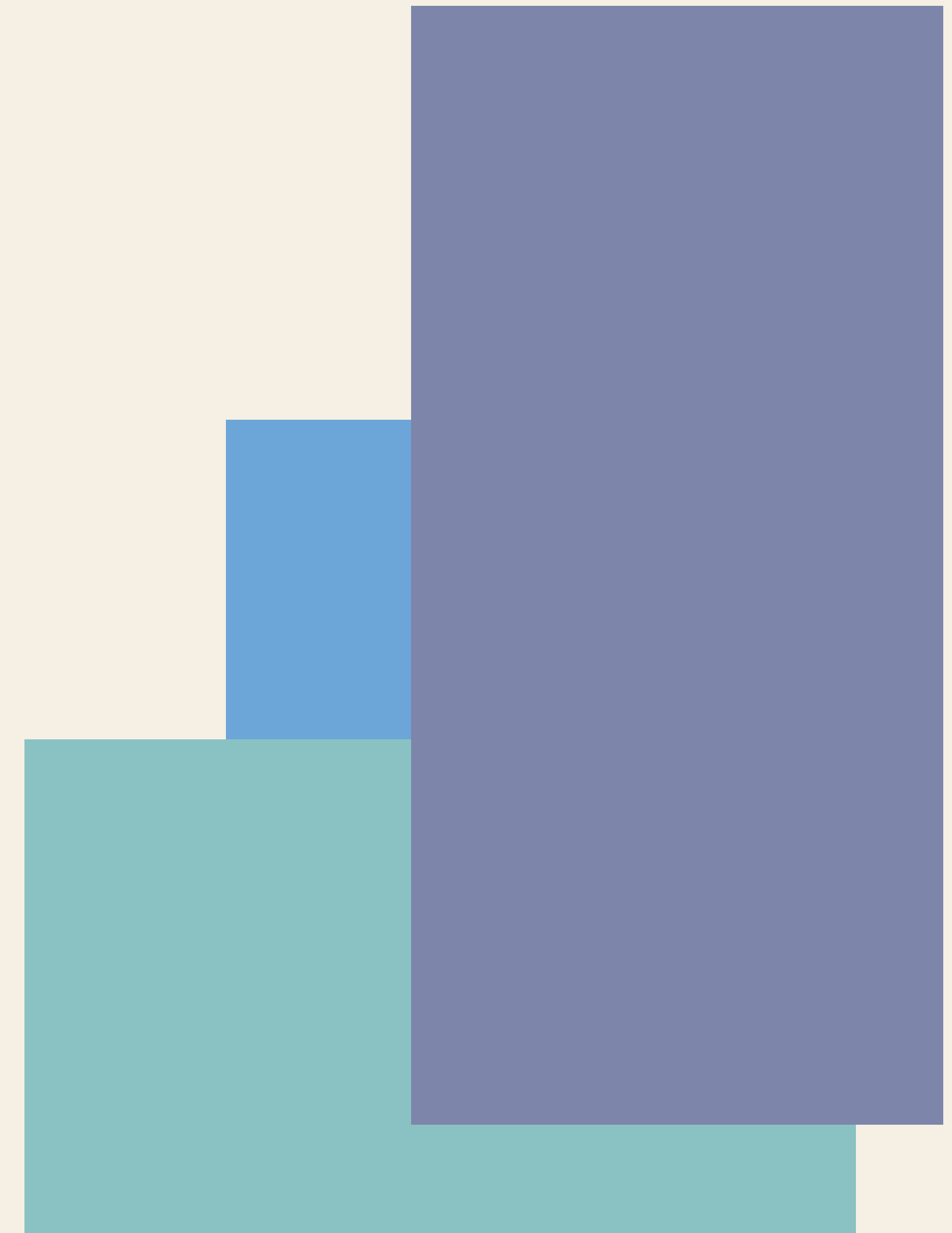
Introduction

Congratulations! As a project leader in the movement to revolutionize pathways to education and hiring outcomes, you now embark on a journey that is at the forefront of harnessing the power of innovation, collaboration, and opportunity. The work you do will not only shape the future of individuals but can redefine the future of industries, opening doors for talent, creativity, and growth in ways we've never seen before.

After following [SHEEO's Digital Credentials Design Template](#), the foundation of your digital credential program is set, the program's framework is standing, and now it is up to you and your collaborative partners to take this project from vision to reality. Within these pages, you will find strategies and operational next steps on the road to successful implementation.

Why a Digital Credentials Program?

As the leader of a digital credentials program, it's crucial to clearly communicate its value to stakeholders. Digital credentials are verifiable, web-based records of an individual's knowledge, skills, and competencies. As the digital credential ecosystem advances, there are several benefits to incorporating digital credentials for education/training, learner/employees, employers and governments. Education, training, and credentialing partners (hereafter **training partners**) benefit by improving employment outcomes for learners. For **learners/employees**, digital credentials provide greater control over their own career narrative, enabling them to easily access their records, identify growth opportunities, and showcase verified qualifications to employers. **Employers** will benefit by more efficiently completing credential verification processes and identifying qualified candidates whose skills have been validated by trusted experts, ensuring that new hires meet hiring standards. **Governments** benefit too, as digital credentials make it easier to collect accurate workforce data, better allocate resources for workforce development, and address emerging skill gaps. In short, a digital credentials program streamlines hiring, enhances educational alignment with industry needs, and empowers individuals while giving all stakeholders more reliable, transparent information to make informed decisions.



How to Use this Playbook

The pages within this playbook are interactive.

**bold
blue
words**

Click on any **bold, blue words** to take you to specific references in the real-world example.



PRO TIP!

Click on this button for information to help you avoid common frustrations that can occur as you work with the employers and training partners in meeting program objectives.



REAL-WORLD
EXAMPLE

Click this button for a real-world example of an employer and training partner working with granular details required to complete program objectives.



DEEP-DIVE

Click this button for a deep-dive into explanations and tools for evaluating digital credential platforms and wallets.



If this button is on the page, click to advance to more information.

Digital Credential Program Objectives

The goal of implementing a digital credential program is to streamline the connection between highly skilled individuals and employers. To achieve and scale this, the project leader collaborates with key partners from both employer and training organizations to:

1. Identify and define (using **essential skills**) the **competencies** required for job role(s).
2. Determine the competency levels for **employment level/classifications**.
3. Align training/program learning outcomes to essential skills and competency levels.
4. Develop assessment opportunities for individuals to demonstrate skill and competency.
5. Select a digital credentialing (badging) platform and digital wallet provider.



How To Achieve the Program Objectives

1. Employer(s) and training partner review **existing job description(s)** that include information about required hard skills (like technical skills) and soft skills (like leadership skills) embedded within job competencies with suggested level of skill mastery required for employment classification.
2. Employer(s) and the training partner align and **crosswalk** the identified and defined hard skills and soft skills with existing training curricula learning/program outcomes.
3. Employer(s) identify any industry standards and/or skill descriptors aligned to the job description at competency-levels. It can be useful to create a **skill and competency matrix** for reference throughout the project.



PRO TIP!

How To Achieve the Program Objectives

4. Using agreed-upon skills (learning/program outcomes) and competency matrix, employers make any relevant adjustments/revisions to job descriptions and **tag the job description with relevant skill descriptors**.
5. Create skill and competency-level assessments.
6. Design training materials for learners to achieve stated learning outcomes, demonstrate skills, and competency.
7. If not already determined, collaborate with relevant stakeholders to choose a digital credential platform and digital wallet.

**View Complete Example
of CyberVigilant, Inc.**



Program Launch Review

Before you launch your digital credentials project, review [SHEEO's Digital Credentials Design Template](#) and this Playbook to ensure you have successfully:

Defined and Designed Your Digital Credentials Program

- By establishing your project's parameters and conducting financial assessments.
- Developed career pathways grounded in skills and competency frameworks.
- Aligned employer job descriptions with training outcomes to meet workforce demands.

Built Key Components

- Designed opportunities for learning, mentorship, and apprenticeships to support skill acquisition, upskilling, and re-skilling.
- Prepared to deliver comprehensive navigational and career support services.
- Crafted outreach and marketing strategies to engage learners and employers effectively.

Program Launch Review

Selected and Implemented Technology

- Chosen a digital credentials platform and wallet to facilitate seamless credentialing and sharing.

Planned for Measuring Success and Ensuring Sustainability

- Created strategies to evaluate program effectiveness and assess impact.
- Planned a meaningful cost-benefit analysis to guide decision-making.
- Strategized for ongoing program improvement to ensure adaptability and relevance.

With these foundational steps complete, you, as the project leader, in collaboration with employer and training partners, are ready to move confidently toward piloting, evaluating, and scaling your digital credentials program.

Congratulations on taking significant strides to revolutionize the connection between the highly skilled workforce supply and demand. Your work is helping to build a future where skills-based hiring and career mobility are more accessible and equitable for all.

Thank You

Thank you to Walmart Foundation and Reach University for their funding support for this playbook and to the State Higher Education Executive Officers Association (SHEEO), and iQ4 for their collaboration and feedback on playbook content.



This playbook was created by:



REAL WORLD EXAMPLE

CyberVigilant Inc.

CyberVigilant Inc., a fast-growing company specializing in cybersecurity solutions for small and mid-sized businesses, is looking to hire a team of mid-level cybersecurity professionals to support its expanding client base. The company prides itself on offering tailored services, including risk assessment, vulnerability management, and incident response.

CyberVigilant Inc. has faced increasing difficulty in sourcing mid-level cybersecurity professionals who possess not only technical expertise but also practical, hands-on experience in real-world scenarios. To address this, the company conducted an internal review of its workforce development strategy. This included assessing its in-house training programs as well as evaluating existing training and education options available locally, such as those offered by nearby community colleges and continuing education programs.

The findings revealed notable gaps: many programs were too general, lacked alignment with CyberVigilant's specific needs, or were unable to keep pace with evolving cybersecurity challenges. Recognizing the need for a tailored approach, CyberVigilant partnered with **EduTech**, a regional leader in fast-track cybersecurity bootcamps, to create a customized training-to-hiring pipeline.

Through this partnership, CyberVigilant aims to:

1. **Define Key Competencies:** Collaboratively outline the skills and knowledge critical for success in the mid-level cybersecurity analyst role.
2. **Validate Training Alignment:** Ensure EduTech's bootcamp curriculum directly maps to the technical and practical skills CyberVigilant prioritizes.
3. **Streamline Talent Pipelines:** Use digital credentials to quickly identify candidates who meet hiring criteria.
4. **Promote Equity in Hiring:** Open pathways for non-traditional candidates by recognizing alternative training and certifications over traditional degree requirements.

CyberVigilant and EduTech began their collaborative work by first reviewing the **job description** for CyberVigilant's mid-level cybersecurity analyst job role.

Position Overview: Mid-Level Cybersecurity Analyst

Key Responsibilities:

- Monitor and respond to security incidents using advanced threat detection tools.
- Perform vulnerability scans and recommend remediation strategies.
- Assist in the development and enforcement of cybersecurity policies.
- Collaborate with internal teams to ensure compliance with industry standards like NIST and ISO 27001.

Qualifications:

- Bachelor's degree in Computer Science, Cybersecurity, or related field (or equivalent experience).
- At least 3 years of hands-on experience in cybersecurity operations.
- Familiarity with tools such as SIEM platforms, firewalls, and endpoint protection systems.
- Industry certifications like CompTIA Security+, CISSP, or CEH are a plus.

Notice how broad and vague CyberVigilant's initial job description is. The broadness of the job description might be one reason that CyberVigilant has had some difficulty in sourcing the highly skilled, mid-level cybersecurity professionals that meet their needs. Upon reviewing the job description, CyberVigilant and EduTech work together to better describe and define exactly what CyberVigilant stakeholders want in the mid-level cybersecurity analyst. EduTech is also able to refine existing curriculum, or design new curriculum, to align learning and program outcomes to the skills and competencies needed for a mid-level cybersecurity analyst.

The project leader facilitates discussions between the training partner and employer partner by asking stakeholders to first review credentials and standardized competencies for cybersecurity analysts on Credential Engine using the Credential Finder tool. After stakeholders spend time reviewing industry standards, the project leader, employer partner and training partner meet to discuss each line-item in the starting job description. As the project leader challenges stakeholders to explain and get specific- using many of the standardized credentials they agreed upon as vital to the role with CyberVigilant, they identify the following categories of competencies:

- Technical Knowledge
- Threat Detection
- Incident Response
- Regulatory Compliance

CyberSecurity Analyst Job Skill Matrix

For this job role, CyberVigilant is interested in hiring a mid-level analyst; however, to define mid-level, stakeholders need to differentiate emergent, entry-level, intermediate-level, mid-level, and executive-level. Discussions center on years of practical experience, formal training, and the combination of practical experience and formal training.

As discussions progress, the project leader facilitates development of the CyberSecurity Analyst [Job Skill Matrix](#).

Skills & Employment Level/Classification

Competency Area	Emergent (Less than 1 year)	Entry-Level (1-2 years)	Mid-Level (2-3 years)	Executive-Level (5+ years)
Technical Knowledge	<ul style="list-style-type: none"> • Basic understanding of networking and cybersecurity fundamentals. • Familiar with firewalls, antivirus software, and OS security settings. 	<ul style="list-style-type: none"> • Working knowledge of SIEM tools (e.g., Splunk) and scripting languages like Python or Bash. • Proficient in securing small networks. • Basic understanding of cloud security concepts. 	<ul style="list-style-type: none"> • Advanced knowledge of network architecture, penetration testing, and vulnerability assessment tools (e.g., Nessus). • Familiar with compliance frameworks like NIST and ISO 27001. • Proficient in cloud and hybrid environment security. 	<ul style="list-style-type: none"> • Expert in enterprise-wide security strategy and architecture. • Leads in deploying advanced encryption and forensic tools. • Designs global threat intelligence frameworks.

Skills & Employment Level/Classification

Competency Area	Emergent (Less than 1 year)	Entry-Level (1-2 years)	Mid-Level (2-3 years)	Executive-Level (5+ years)
Threat Detection	<ul style="list-style-type: none">• Identifies phishing attacks and simple malware behaviors.• Assists in monitoring network traffic under guidance.	<ul style="list-style-type: none">• Detects and analyzes threats using IDS/IPS systems.• Conducts basic log analysis.	<ul style="list-style-type: none">• Proficient in advanced threat detection using machine learning tools (e.g., CrowdStrike, Darktrace).• Evaluates and deploys emerging detection technologies.	<ul style="list-style-type: none">• Oversees threat intelligence programs.• Develops predictive threat models and supervises global SOC operations.

Skills & Employment Level/Classification

Competency Area	Emergent (Less than 1 year)	Entry-Level (1-2 years)	Mid-Level (2-3 years)	Executive-Level (5+ years)
Regulatory Compliance	<ul style="list-style-type: none">• Aware of common regulations (e.g., GDPR, HIPAA).• Basic understanding of compliance checklists.	<ul style="list-style-type: none">• Performs operational compliance tasks for specific frameworks (e.g., PCI-DSS).• Creates compliance audit reports.	<ul style="list-style-type: none">• Ensures compliance across departments.• Leads internal audits and remediation strategies for multiple frameworks.	<ul style="list-style-type: none">• Defines strategic compliance policies.• Represents the organization in regulatory discussions and audits.

Skills & Employment Level/Classification

Competency Area	Emergent (Less than 1 year)	Entry-Level (1-2 years)	Mid-Level (2-3 years)	Executive-Level (5+ years)
Project Management	<ul style="list-style-type: none">• Assists in managing tasks and documentation for small projects.• Tracks project deliverables.	<ul style="list-style-type: none">• Manages small-scale projects independently, including timeline and resource allocation.	<ul style="list-style-type: none">• Leads complex, multi-team projects (e.g., infrastructure upgrades).• Ensures alignment with organizational objectives.	<ul style="list-style-type: none">• Oversees an organization's cybersecurity portfolio.• Aligns cybersecurity initiatives with business strategy.

Skills & Employment Level/Classification

Competency Area	Emergent (Less than 1 year)	Entry-Level (1-2 years)	Mid-Level (2-3 years)	Executive-Level (5+ years)
Communication & Collaboration	<ul style="list-style-type: none">• Communicates technical findings in simple terms to teammates.• Collaborates effectively in small groups.	<ul style="list-style-type: none">• Delivers concise updates to stakeholders.• Participates in team problem-solving exercises.	<ul style="list-style-type: none">• Mentors junior analysts.• Collaborates with departments like IT, legal, and HR.	<ul style="list-style-type: none">• Speaks authoritatively with C-suite leaders and external partners.• Champions a security-conscious organizational culture.

Skills & Employment Level/Classification

Competency Area	Emergent (Less than 1 year)	Entry-Level (1-2 years)	Mid-Level (2-3 years)	Executive-Level (5+ years)
Degrees and Certifications	<ul style="list-style-type: none"> Pursuing or holds an Associate Degree in IT, Computer Science, or Cybersecurity. Working toward certifications like CompTIA Security+, Google IT Support Professional Certificate (digital credential). 	<ul style="list-style-type: none"> Holds a Bachelor's Degree in Cybersecurity or related field. Certifications: CompTIA Security+, CEH (Certified Ethical Hacker). Digital credentials: AWS Cloud Practitioner, Linux Essentials. 	<ul style="list-style-type: none"> Holds a Bachelor's or Master's Degree in Cybersecurity. Certifications: CISSP (Certified Information Systems Security Professional), GIAC Certifications (e.g., GSEC, GCIH). Digital credentials: SIEM Proficiency Badge, Incident Response Specialist Microcredential. 	<ul style="list-style-type: none"> Advanced degree (e.g., MBA with Cybersecurity Focus, Master's in Cybersecurity Leadership). Certifications: CISM (Certified Information Security Manager), CISSP-ISSAP. Digital credentials: Executive Cybersecurity Leadership Badge.

Using the details defined in the CyberSecurity Analyst Matrix, the employer revises the initial job description into one that more robustly describes what CyberVigilant wants in a mid-level cybersecurity analyst, including “**tagging**” it with Rich Skill Descriptors (RSDs). RSDs are machine-readable, searchable data that include the context behind a skill, giving users a common definition for a particular skill and help to make it understandable and transferable across the learning and employment landscape. These can be found using Credential Engine and/or through the Open Skills Network.

Position Overview: Mid-Level Cybersecurity Analyst

CyberVigilant Inc. is seeking a proactive and skilled Mid-Level Cybersecurity Analyst to join our team. The ideal candidate brings technical expertise, hands-on experience, and strong communication abilities to support our organization’s cybersecurity objectives.

Key Responsibilities

- **Threat Monitoring & Incident Response:**
 - Continuously monitor and respond to security incidents using advanced threat detection tools (e.g., SIEM platforms like Splunk or QRadar).
 - Analyze and interpret security events to identify trends and mitigate risks.
 - Document and communicate findings, ensuring timely escalation of critical issues.



- **Vulnerability Management:**

- Perform regular vulnerability assessments and penetration testing, identifying areas of risk in on-premises, cloud, and hybrid environments.
- Develop and recommend remediation strategies to minimize vulnerabilities.

- **Policy Development & Compliance:**

- Assist in drafting, updating, and enforcing cybersecurity policies and procedures in alignment with industry standards such as **NIST Cybersecurity Framework** and **ISO 27001**.
- Collaborate with internal and external stakeholders to ensure compliance with regulatory frameworks (e.g., GDPR, PCI-DSS).

- **Collaboration & Training:**

- Work cross-functionally with IT, DevOps, and legal teams to ensure secure system integration and data protection.
- Mentor junior cybersecurity staff and contribute to ongoing team training initiatives.
- Conduct security awareness training sessions for employees to reduce human factor risks.

Qualifications

- **Education & Experience:**

- Bachelor's degree in computer science, Cybersecurity, or related field (or equivalent experience).
- Minimum of 3 years of hands-on experience in cybersecurity operations, including threat

- **Technical Skills:**

- Proficient in tools such as SIEM platforms (Splunk, QRadar), firewalls, intrusion detection systems (IDS/IPS), and endpoint protection (e.g., CrowdStrike).
- Strong understanding of scripting languages (e.g., Python, PowerShell) for automation and custom tool development.
- Experience with vulnerability management tools (e.g., Nessus, OpenVAS) and cloud security platforms (e.g., AWS, Azure).

- **Soft Skills:**

- Strong problem-solving skills and the ability to make data-driven decisions under pressure.
- Excellent written and verbal communication skills for clear reporting and stakeholder collaboration.
- A proactive mindset with the ability to prioritize tasks and manage multiple projects simultaneously.

- **Certifications** (preferred but not required):
 - Industry-recognized certifications such as **CISSP, CompTIA Security+, Certified Ethical Hacker (CEH),** or **GIAC Certifications** (e.g., GSEC, GCIH).

By starting with the end results in mind, CyberVigilant and EduTech use an evidence-based practice for adult learners known as backward design: reviewing the job description for the mid-level security analyst role, included relevant competencies listed on Credential Engine's Credential Finder, and built the cybersecurity job role matrix to describe the ideal competencies for cybersecurity analysts at CyberVigilant by employment level. Now, EduTech can design the digital credential curriculum that fills learning outcome gaps that are missing by most applicants for CyberVigilant's mid-level cybersecurity analyst role.

EduTech crosswalks existing curricula outcomes to CyberVigilant's mid-level cybersecurity analyst requirements. For example, throughout the year, CyberVigilant offers professional development opportunities to its entry-level cybersecurity analysts. EduTech notices that one of the professional development opportunities that CyberVigilant regularly offers might prepare existing analysts to meet some requirements for the mid-level cybersecurity analyst role. The table below is a crosswalk showing how learners who successfully complete the CyberVigilant ID10T-101 training meet some specific requirements listed in the detailed job description.


Crosswalk Example: Existing Employer Training to Job Role Requirement(s)
 CyberVigilant CyberSecurity Training ID10T-101: Using Data Visualizations to tell Our Story.

ID10T-101: Learning Outcomes By successfully completing IDT010-1010, learners can:	Job Role Requirement
<p>Analyze potential security events that occurred last quarter</p> <p>Identify any trends in last quarter's security events</p>	<p>Analyze and interpret security events to identify trends</p>
<p>Use relevant statistical and presentation software to visualize trend data for documentation and communication of findings to stakeholders.</p> <p>Create written report on quarter security events, including suggestions for remediation/prevention.</p> <p>Present findings using data visualizations that tell a story to training classmates, trainer and CyberVigilant stakeholders</p>	<p>Document and communicate findings</p>
<p>Use relevant statistical and presentation software to visualize trend data for documentation and communication</p> <p>Present findings using data visualizations that tell a story to training classmates, trainer and CyberVigilant stakeholders</p>	<p>Excellent verbal and written communication skills for clear reporting and stakeholder collaboration</p>

Skills-aligned Training


Through a collaborative effort, EduTech and CyberVigilant stakeholders engage in structured discussions to align CyberVigilant's workforce needs with EduTech's course development strategy. These discussions include identifying learning opportunities not already offered in CyberVigilant's training curriculum, assessing the availability of CyberVigilant employees to participate as subject matter experts, and ensuring alignment with industry best practices. Together, they map key skills—such as advanced threat detection using machine learning tools like CrowdStrike and Darktrace—to specific course modules, ensuring that learners gain hands-on experience with technologies used in the field.

In addition, EduTech follows best practices for adult learners when determining course modality. Factors such as working professionals' schedules, the complexity of skill acquisition, and the need for real-time collaboration guide the decision between synchronous online, asynchronous online, or in-person instruction. For example, analyzing and interpreting security events may be best taught through asynchronous case studies, while documenting findings and escalating critical issues may require live role-play exercises in a synchronous or in-person setting.



By incorporating direct employer input and aligning instructional design with workforce demands, EduTech creates a learning experience that prepares participants to meet CyberVigilant's expectations, equipping them with the competencies to identify trends, mitigate risks, and recommend remediation strategies effectively.

To assess mastery of these competencies, EduTech designs a final course project that simulates a real-world security incident response scenario. Learner-employees are required to conduct a full threat analysis using machine learning detection tools, interpret security events to identify potential attack vectors, and develop a detailed incident response report. The final deliverable includes a written security assessment and a remediation plan, which learners present in a professional debriefing format. This project not only reinforces the technical and analytical skills developed in the course but also provides a tangible artifact that learner-employees can showcase to their current or future employers as evidence of their ability to assess risks, document findings, and implement effective security strategies in a professional setting.



DEEP-DIVE

Deep-dive into Choosing a Digital Credential Platform & Digital Wallet

A digital credential platform provides training partners with the tools to issue credentials (like badges). Digital credential platform subscriptions are available for purchase or they can be built using open-source resources. Often, training partners use digital credential platform(s) and their established use of the platform(s) can be used for your digital credential program.

Keep reading to learn the benefits of using a digital credential platform for employers, training partners, and learner-employees.

Digital Credential Platform Benefits

Employers

- **Enhanced Talent Acquisition:** Quickly identify and verify candidates with specific skills through authenticated digital credentials.
- **Skills Matching:** Filter candidates based on precise skillsets and competencies, reducing time-to-hire.
- **Workforce Development:** Track employee skill development and target training needs efficiently.
- **Improved Retention:** Provide employees with visible career progression paths tied to skill-based achievements.

Training Partners

- **Increased Credibility:** Showcase verified learning/program outcomes to demonstrate the value of their programs.
- **Broader Reach:** Attract more learners by identifying skills gaps, offering suggestions for pathways to address skills gaps, and by offering credentials that are portable and aligned with industry standards.
- **Data Insights:** Leverage analytics on credential issuance and usage to refine and improve program offerings.
- **Collaboration Opportunities:** Build stronger partnerships with employers by aligning credentials to workforce demands.

Digital Credential Platform Benefits

Employees/Learners

- **Career Advancement:** Use credentials to showcase verified skills and competencies to current and potential employers. Use information on any identified skills gaps to guide decisions related to additional training needs and opportunities.
- **Portability and Ownership:** Store credentials in a digital wallet, making them accessible anytime, anywhere.
- **Transparency:** Gain a clear understanding of required skills and achievements for career goals.
- **Motivation and Recognition:** Boost confidence and motivation through visual representation of accomplishments.

Choose a Digital Credential Platform

There are many key considerations when evaluating digital credential platforms for adoption. This decision can vary depending upon the employer, industry, training partner and long-term stakeholder vision for the digital credential project, as well as existing technology infrastructure; therefore, take time to give this key activity plenty of attention and invite other subject matter professionals such as information technology team leaders to join the conversations. Consider developing a **scoring matrix** that you can use to guide discussions regarding what is most important to stakeholders and least important when choosing a digital credential platform

The following criteria should be used to evaluate digital credential platforms with your employer

Issuance, Customization & Management

- Support for multiple credential types (e.g., badges, certificates, micro-credentials).
- Bulk issuance capabilities.
- Customization of credential designs, metadata (e.g., skill descriptions, evidence), and industry-aligned standards.
- Capability to embed metadata for rich skill descriptors and organizational needs.

Integration & Compatibility

- Compatibility with learning, talent, and business systems (e.g., LMS, HRIS, CRM, ERP).
- API availability for automation and scalability.
- Support for Single Sign-On (SSO) for secure and easy access.

Verification & Interoperability Standards

- Use of blockchain or other verifiable credential standards (e.g., W3C Verifiable Credentials).
- Real-time, tamper-proof verification for third parties without login requirements.
- Support for industry standards (e.g., Open Badges, CLR, Learning and Employment Records) with cross-platform compatibility.

User Experience

- Intuitive dashboard for credential issuers and recipients.
- Mobile-friendly functionality for credential access and management.
- Self-service options for recipients (e.g., reissue requests, profile updates).
- Customizable templates for notifications and email delivery.

Taxonomies & Metadata Interoperability

- Ability to address multiple taxonomies (e.g., O*NET, NICE Cybersecurity).
- Integration of job roles with knowledge, skills, and attributes (KSAs) within job families.
- Supports importing and tagging credentials with assessed skills from multiple third-party providers.

Cross-referencing (cross-walking) with metadata registries (e.g., Credential Engine) for exploration of:

- Competencies and skill frameworks;
- Learning outcomes and career pathways;
- Market value and demand for skills.

Analytics & Reporting

- Insight into credential issuance and engagement metrics (e.g., verifications, clicks).
- Customizable reports for tracking and decision-making.

Skill Development & Career Pathways

- Visual representation of skill gaps categorized by types (e.g., professional, business, technical).
- Recommendations for upskilling and reskilling resources based on skill gaps.
- Visual and textual presentation of career progression pathways with suggested steps for advancement.

Security & Compliance

- Compliance with data privacy regulations (e.g., GDPR, FERPA, HIPAA).
- Secure storage and encryption of sensitive data.
- Identity verification options to protect credential integrity.

Branding & Community Engagement

- White-label branding options for institutions.
- Strong community support, including user guides, forums, and best practices.
- Reliable technical support and feedback channels for continuous improvement.

Cost & Scalability

- Transparent pricing structure, including setup, usage (e.g., per credential issued), and maintenance fees.
- Licensing or subscription options that support scalability.

Choose a Digital Credential Wallet

A digital credential wallet stores and manages an individual's credentials, badges, and learning records. Some digital credential platforms include a wallet; however, depending upon the long-term vision for the digital credentials program, it is wise to carefully consider digital credential wallet options that are part of digital credential platforms as well as standalone wallets. Platform evaluation focuses more on credential issuance, management, verification, and integration with organizational systems. Wallet evaluation emphasizes user privacy, control, security, interoperability, and user experience in managing and sharing credentials.

Consider developing a scoring matrix, like the example scoring matrix used for the digital credential platforms, to guide discussions regarding what is most important to stakeholders and least important when choosing a digital credential wallet.

The following criteria should be used to evaluate digital wallets with your employer and training partner stakeholders:

User Control & Privacy

- Ownership of credentials by the individual user.
- Privacy-preserving architecture with no centralized data storage.
- User consent required before sharing credentials or data.
- Transparency in data storage and usage policies.

Compatibility & Interoperability

- Support for various credential formats (e.g., Open Badges, Verifiable Credentials).
- Interoperability with credential platforms, employer systems, and job boards.
- Standards compliance with protocols such as W3C Verifiable Credentials and DID protocols.
- API availability for integrations.

Ease of Use

- Intuitive, user-friendly interface with minimal learning curve.
- Mobile-first design for on-the-go access across devices.
- Simple credential import/export functionality.

Security

- Encryption of credentials and sensitive data.
- Multi-factor authentication (MFA) for access control.
- Protection against unauthorized credential alteration.
- Compliance with privacy regulations.

Sharing & Verification

- Flexible sharing options (e.g., QR codes, secure links, email).
- Ability to manage sharing permissions (e.g., public, private, restricted access).
- Instant, real-time verification by third parties without requiring login.
- Tamper-proof records for employers and credential issuers.

Storage & Organization

- Capability to store and organize a wide variety of credentials.
- Categorization, tagging, and visibility control (e.g., public, private).
- Support for notes or annotations on stored credentials.
- Support for multiple file types (e.g., PDFs, XML, CSV).

Evidence of Learning

- Ability to embed and display detailed metadata about skills, achievements, and learning outcomes.
- Searchable and verifiable metadata.
- Evidence/artifact upload options to provide additional context.

Portability & Scalability

- Adherence to portability standards, allowing users to export and migrate their credentials to other platforms.
- Support for both individual and enterprise users.
- Scalable infrastructure to accommodate increasing credential volumes and additional features over time.

Backup & Recovery

- Secure wallet recovery options (e.g., key management, backup codes).
- Clear, documented processes for restoring credentials in case of data loss or device failure.
- Sync capabilities to ensure data integrity between devices.

User Support & Documentation

- Comprehensive help resources (e.g., tutorials, FAQs).
- Responsive customer support for troubleshooting and technical issues.
- Feedback channels for continuous improvement.

Cost & Maintenance

- Clear pricing structure with transparent costs for setup, maintenance, and feature access.
- Options for free vs. subscription-based plans.
- Clear disclosure of any additional fees for advanced features.

Career Pathway & Job Integration (less common in most current wallets)

- AI or analytics-driven career recommendations based on stored credentials.
- Real-time job opportunities matched to credentialed skills and roles.
- Geo-location search for open job requisitions.
- Direct integration with job boards, career services, and networking platforms (e.g., LinkedIn).

Example Scoring System for Digital Platforms (and Digital Wallets)

Interpreting Scores Example

- **200-275:** Exceptional—strong candidate for implementation.
- **125-199:** Acceptable—meets most needs; evaluate limitations carefully.
- **Below 125:** Unsuitable—significant gaps in key functionalities.

Example Scoring Approach

	Weight	Platform A	Weighted Score	Platform B	Weighted Score
Issuance, Customization & Management	5	4	20	3	15
Integration & Compatibility	5	5	25	4	20
Verification & Interoperability Standards	4	3	12	5	20
User Experience	4	5	20	4	16
Taxonomies & Metadata Interoperability	4	3	12	3	12
Cross-referencing	4	5	20	5	20
Analytics & Reporting	5	5	25	4	20
Skill Development & Career Pathways	5	5	25	5	25
Security & Compliance	4	4	16	4	16
Branding & Community Engagement	4	4	16	3	12
Cost & Scalability	4	3	12	4	16
Total weighted score			203		192

Scoring Approach

Each criterion is scored on a scale of 1 to 5:

- **1 - Poor:** Fails to meet basic requirements or offers minimal functionality.
- **2 - Fair:** Meets some requirements but has significant limitations.
- **3 - Good:** Adequately meets most requirements, with minor issues or gaps.
- **4 - Very Good:** Meets all requirements with few limitations; exceeds expectations in some areas.
- **5 - Excellent:** Fully meets or surpasses all expectations with robust features.

Weighting Criteria

Not all criteria hold the same importance for every project. Assign weights (e.g., 1-5) to reflect priorities. For instance:

- **Critical (Weight = 5):** Security, interoperability, portability.
- **Important (Weight = 3):** Career pathway integration, sharing and access control.
- **Optional (Weight = 1):** Scalability, cost

Weighted Scoring Example

- Here's how to calculate the total score:
- Score each criterion (1-5).
- Multiply the score by its assigned weight.
- Add up the weighted scores to determine the wallet's overall performance.



PROTIPS!

PROTIP!

As an evolving ecosystem, the digital credential language is, in many ways, still in its infancy. For this reason, it is important that all key players begin this project with shared definitions for concepts and key terms used in digital credentialing. The digital credential project leader can facilitate discussions with the employer partner and training partner to identify agreed-upon terminology (i.e., wallet, credential or badge, tag, competency level, etc..) and might consider creating a glossary of terms and definitions for partner reference throughout the project.

At the time of this playbook's release, The LER Accelerator Coalition's (2024) LER Accelerator Inventory presents numerous resources that are relevant to guiding discussions regarding current definitions (some standardized/universal where they exist) of digital credentialing program keywords. In addition, [Credential Engine](#) offers a credential registry and credential finder tool that documents job competencies, learning and employment outcomes, as well as credential descriptors using standardized transparent identifiers (CTIDs).

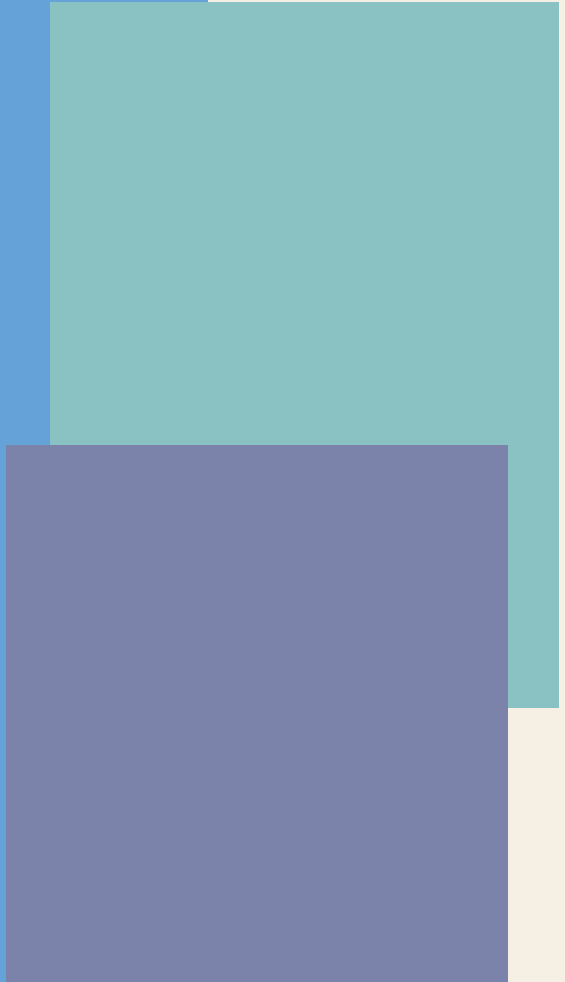
PROTIP!

Resources for Aligning Rich Skill Descriptors & Industry Standards to Training Outcomes, Job Descriptions & Competencies at Performance Levels

Some of the no-cost resources below can be helpful springboards for facilitating discussions on aligning current training outcomes, job descriptions, and competencies at performance levels to rich skill descriptors and/or industry standards. They can also be used for designing digital credential backward build training courses and projects.

- Achievement Standards Network (ASN aka D2L)
- Lightcast Openskills Library
- European Skills, Competencies, Qualifications, and Occupations (specific to EU Labor market)
- MedBiquitous (specific to competencies across U.S. medical industry)
- O*Net Online
- Open Skills Network

DEFINITIONS

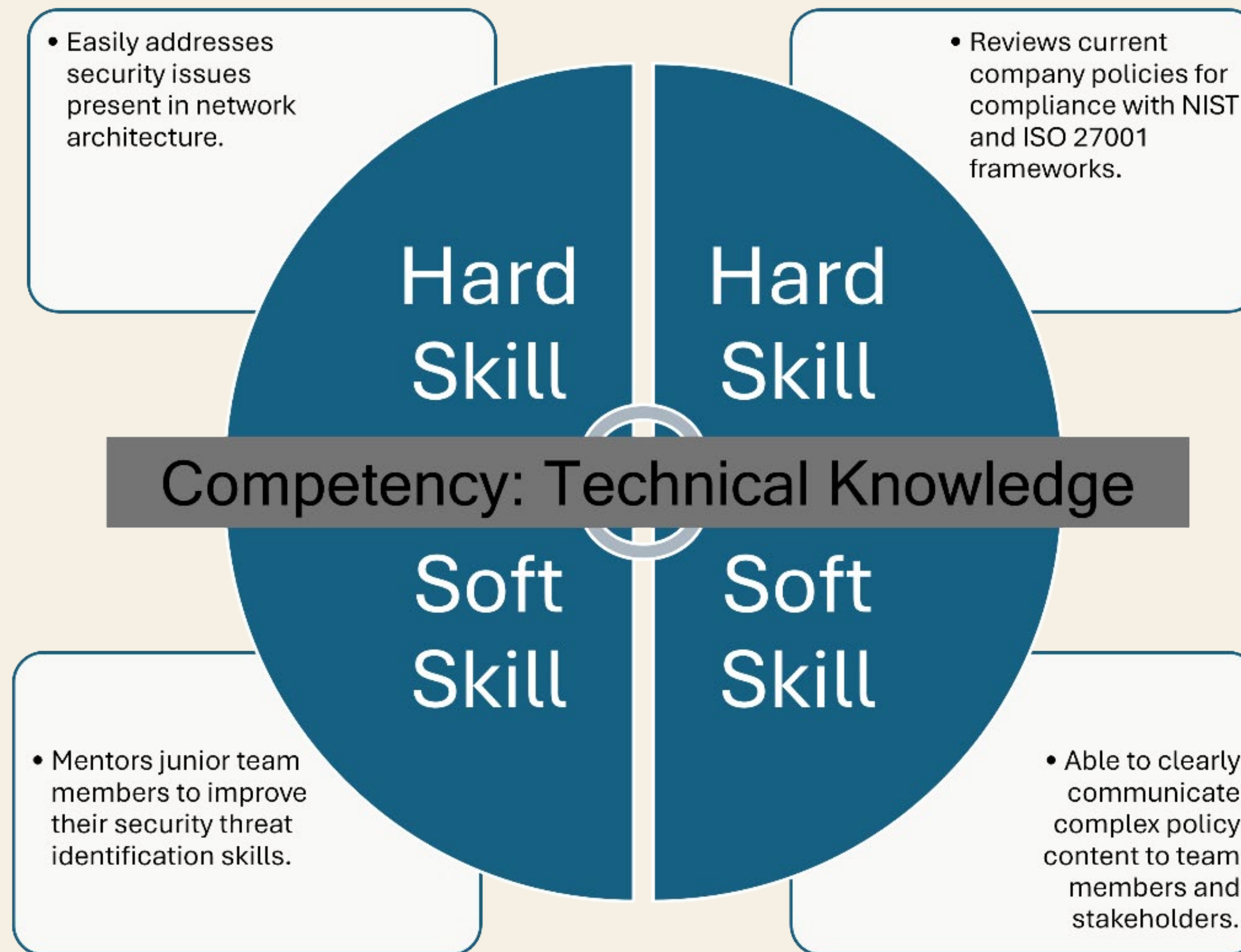


Essential Skills

Open Skills Network (OSN) works with industry leaders and training providers to develop a common, standardized, language that defines measurable “knowledge, abilities, or learned behaviors” required for individuals to demonstrate competencies in job roles. See the [OSN FAQs page](#) for more information.

Competencies

Within each competency are the hard and soft skills required to demonstrate that competency. A simple example:



Employment Level/Classifications

Most employers need a continuum of highly skilled individuals for various job roles. It is important to discuss with the employer and training partner how the employer classifies job role levels (i.e., entry-level, intermediate, supervisory, executive etc.). In the playbook vignette, the example employer CyberVigilant uses the following categories to group the amount of experience that employees have with each skill in a competency.

Skills & Employment Level/Classification				
Competency Area	Emergent (Less than 1 year)	Entry-Level (1-2 years)	Mid-Level (2-3 years)	Executive-Level (5+ years)