* + - * Based on the example above for software engineering pathway apprentice creating a portfolio item to be used as an example within a training document. Repeat the process with a cybersecurity pathway based on a **Team Collaboration Reflection Log Within the underlying principles theme and allocated KSBS both core and for the ones that are associated with the cybersecurity pathway make sure you apply the criteria for the professional discussion underpinned by portfolio  
          
         Assessment plan can be found here** <https://skillsengland.education.gov.uk/apprenticeship-standards/st0119-v1-2>

Here’s a full **portfolio item example** for a **Cybersecurity pathway apprentice**, designed to fit within a **training document**. It follows the same structure as your software engineering example, but focuses on a **Team Collaboration Reflection Log** under **Theme A: Underlying Principles**, and aligns with the **ST0119 v1.2 assessment plan** for the **Professional Discussion underpinned by a Portfolio**.

Portfolio Item: Team Collaboration in Cybersecurity Incident Response

**Title: My Role in Coordinating a Cybersecurity Incident Response Team**

**Overview**

In this portfolio item, I demonstrate my understanding of **team collaboration and organisational context** within a cybersecurity environment. I reflect on my role in a coordinated response to a simulated phishing attack, highlighting how I applied cybersecurity principles, worked effectively with cross-functional teams, and demonstrated leadership and professional behaviours. This example aligns with **Theme A: Underlying Principles**, covering both **core KSBs** and **cybersecurity-specific KSBs**.

**Insert Diagram 1**: *Cybersecurity Incident Response Workflow*  
*A visual showing the stages of incident response and team roles.*

**Situation**

During a cybersecurity training exercise, our organisation simulated a phishing attack targeting internal staff. I was assigned to the incident response team, which included IT support, network engineers, and compliance officers. The goal was to identify, contain, and remediate the threat while maintaining communication and documentation.

**Task**

My responsibility was to coordinate with team members, contribute to threat analysis, and ensure that our response aligned with organisational policies and cybersecurity best practices. I also documented the process and reflected on team dynamics and leadership approaches.

**Actions**

**Understanding the Organisational Context (K7):**

I began by reviewing the organisation’s cybersecurity policies and escalation procedures. I analysed how different departments contributed to the response and how our actions aligned with business continuity goals.

**Insert Diagram 2**: *Team Roles and Escalation Pathways*  
*A flowchart showing how different roles interact during incident response.*

**Supporting Evidence**:

* Cybersecurity Policy Summary (PDF)
* Incident Escalation Flowchart

*“I demonstrated my understanding of the organisational context by analysing how our response aligned with business continuity and compliance requirements.”*

**Working Effectively in a Team (K8, S7, B4, B6, B7):**

I participated in daily briefings, shared threat intelligence findings, and collaborated on containment strategies. I used Microsoft Teams and SharePoint to communicate and share documentation.

**Insert Diagram 3**: *Team Collaboration Timeline*  
*A timeline showing key collaboration points and decisions.*

**Supporting Evidence**:

* Teams Chat Log (Redacted)
* Threat Intelligence Report (PDF)

I adapted my communication style to suit technical and non-technical colleagues, and I encouraged open discussion during debriefs. I also supported junior team members by explaining technical concepts and guiding them through the response process.

*“I demonstrated my ability to work effectively in a team by contributing to threat analysis, adapting communication styles, and supporting knowledge sharing.”*

**Applying Leadership and Management Principles (K9, K10, S8):**

I took initiative to lead the documentation effort, ensuring that all actions were logged and justified. I prioritised tasks using a risk-based approach and coordinated with compliance to ensure regulatory alignment.

**Insert Diagram 4**: *Risk-Based Prioritisation Matrix*  
*A matrix showing how tasks were prioritised based on impact and urgency.*

**Supporting Evidence**:

* Incident Response Log (PDF)
* Compliance Checklist

I reflected on the leadership styles observed during the exercise and evaluated how they influenced team morale and decision-making. I also practiced self-leadership by setting goals for improving my incident response skills and seeking feedback from senior analysts.

*“I applied leadership principles by managing documentation, prioritising tasks based on risk, and reflecting on team leadership dynamics.”*

**Results**

The incident was contained within 24 hours, and no data was compromised. The team received commendation for clear communication and rapid response. My documentation was used as a template for future exercises.

**Supporting Evidence**:

* Post-Incident Review Summary
* Team Commendation Email

**Reflection and Lessons Learned**

This experience reinforced the importance of structured collaboration in cybersecurity. I learned that clear communication and documentation are critical during high-pressure situations. In future, I would introduce earlier tabletop exercises to improve readiness and refine escalation protocols.

*“I evaluated the outcomes of our response and identified improvements such as earlier simulation exercises and clearer escalation paths.”*

**KSBs Demonstrated**

**Core KSBs**

* **K7**: I analysed organisational roles and their impact on cybersecurity response.
* **K8, S7**: I worked effectively in a team using collaboration tools and shared intelligence.
* **K9, K10, S8**: I applied leadership and management principles in coordinating documentation and prioritisation.
* **B4, B6, B7**: I demonstrated professional behaviours including adaptability, collaboration, and continuous improvement.

**K11**: I applied knowledge of cybersecurity threats and response strategies.

* **S9**: I contributed to threat analysis and containment.
* **B8**: I showed integrity and accountability in handling sensitive information.