Read this https://skillsengland.education.gov.uk/apprenticeship-standards/st0119-v1-2  
  
as an example for here is one created for Software engineer Which covers the four themes from the apprenticeship standard  
  
Theme A: Underlying Principles Theme B: Technical Solutions Demonstrates   
  
Theme A: Underlying Principles Demonstrates foundational understanding of Cyber Security Analyst concepts, methodologies, and team dynamics

* Software Development Lifecycle Overview
* Agile Methodology Application
* Requirements Gathering and Analysis
* Software Design Documentation
* Estimation and Planning Techniques
* Risk and Opportunity Assessment
* Team Collaboration Reflection
* Leadership and Management Techniques

Theme B: Technical Solutions Focuses on the practical application of software development, testing, and implementation.  
  
Software Component Build and Test

* + - * Code Review and Quality Assurance
      * Version Control and Release Management
      * Network Design and Implementation
      * Data Product Development
      * Security Implementation in Software
      * Use of Development Frameworks and Tools
* Debugging and Troubleshooting Logs  
    
  Theme C: Innovation & Response Highlights adaptability, continuous improvement, and the use of emerging technologies.   
    
  Sprint Retrospective and Adaptation
* Research on Emerging Technologies
* Lessons Learned and Continuous Improvement
* Response to Changing Requirements
* Evaluation of New Tools or Methods
* Innovation in Software Architecture
  + - Problem Solving and Critical Thinking

Theme D: Legal, Ethics & Landscape Covers compliance, ethical practice, and awareness of the broader professional environment.

* Security Risk Assessment Report
* Compliance with Data Protection Regulations
* Ethical Considerations in Software Development
* Accessibility and Inclusion Review
* Legal Standards Mapping to Project Work
* Professional Conduct and Integrity Reflection

Can you give me a list of between five and eight Potential portfolio it items for each of the themes **Full the knowledge skills and behaviours both core and ones that focus on Cyber Security Analyst**

In the grading section <https://skillsengland.education.gov.uk/apprenticeship-standards/st0119-v1-2> Use the table captioned Professional Discussion underpinned by a portfolio Identify and align the both the core and cyber security analysis KSB's to theme lists just given

Based on the Cyber Security Analyst apprenticeship standard[[1]](https://skillsengland.education.gov.uk/apprenticeship-standards/st1021-v1-0)[[2]](https://skillsengland.education.gov.uk/apprenticeship-standards/st0119-v1-2), here are **potential portfolio items** for each of the four themes, designed to demonstrate the **knowledge, skills, and behaviours (KSBs)** required by both the **core standard** and the **Cyber Security Analyst specialism**.

### **Theme A: Underlying Principles**

Demonstrates foundational understanding of Cyber Security Analyst concepts, methodologies, and team dynamics.

**Portfolio Items:**

* + - * **Security Architecture Overview Document**
      * **Cyber Risk Assessment Report**
      * **Agile Sprint Planning for Security Features**
      * **Stakeholder Engagement Summary**
      * **Security Requirements Specification**
      * **Team Collaboration Reflection Log**
      * **Security Governance and Compliance Mapping**
      * **Leadership in Incident Response Simulation**

1. **Security Architecture Overview Document**
   * Explains the principles of secure system design and how they align with business needs.
2. **Cyber Risk Assessment Report**
   * Includes threat identification, vulnerability analysis, and mitigation strategies.
3. **Agile Sprint Planning for Security Features**
   * Shows how agile methods are used to integrate security into development cycles.
4. **Stakeholder Engagement Summary**
   * Reflects collaboration with technical and non-technical stakeholders.
5. **Security Requirements Specification**
   * Captures functional and non-functional security requirements.
6. **Team Collaboration Reflection Log**
   * Documents contributions to team discussions and decisions.
7. **Security Governance and Compliance Mapping**
   * Maps organisational policies to legal and regulatory standards.
8. **Leadership in Incident Response Simulation**
   * Demonstrates leadership in managing a simulated cyber incident.

### **Theme B: Technical Solutions**

Focuses on the practical application of cyber security tools, techniques, and systems.

**Portfolio Items:**

* + - * **Security Monitoring Dashboard Setup**
      * **Incident Response Playbook**
      * **Penetration Testing Report**
      * **Secure Network Configuration Documentation**
      * **Malware Analysis Case Study**
      * **Security Patch Management Log**
      * **Code Review for Security Vulnerabilities**
      * **Security Tool Evaluation Matrix**

1. **Security Monitoring Dashboard Setup**
   * Configuration and use of SIEM tools to monitor threats.
2. **Incident Response Playbook**
   * Step-by-step guide for responding to various types of cyber incidents.
3. **Penetration Testing Report**
   * Includes methodology, findings, and remediation actions.
4. **Secure Network Configuration Documentation**
   * Details firewall rules, access controls, and segmentation.
5. **Malware Analysis Case Study**
   * Investigation and reverse engineering of a malware sample.
6. **Security Patch Management Log**
   * Records updates and vulnerability remediation.
7. **Code Review for Security Vulnerabilities**
   * Identifies and resolves insecure coding practices.
8. **Security Tool Evaluation Matrix**
   * Compares tools like IDS/IPS, antivirus, and endpoint protection.

### **Theme C: Innovation & Response**

Highlights adaptability, continuous improvement, and the use of emerging technologies.

**Portfolio Items:**

* + - * Emerging Threats Research Brief
      * Security Retrospective Report
      * Zero-Day Vulnerability Response Plan
      * Security Automation Script
      * Evaluation of New Security Frameworks
      * Innovation in Threat Detection Techniques
      * Continuous Improvement Log
      * Adaptive Security Policy Update

1. **Emerging Threats Research Brief**
   * Analysis of new attack vectors and defensive strategies.
2. **Security Retrospective Report**
   * Lessons learned from a completed security project or incident.
3. **Zero-Day Vulnerability Response Plan**
   * Strategy for handling unknown threats.
4. **Security Automation Script**
   * Automates repetitive tasks like log analysis or alert triage.
5. **Evaluation of New Security Frameworks**
   * Compares traditional vs. modern approaches (e.g., Zero Trust).
6. **Innovation in Threat Detection Techniques**
   * Proposes novel methods for identifying threats.
7. **Continuous Improvement Log**
   * Tracks personal and team improvements over time.
8. **Adaptive Security Policy Update**
   * Shows how policies evolve in response to changing risks.

### **Theme D: Legal, Ethics & Landscape**

Covers compliance, ethical practice, and awareness of the broader professional environment.

**Portfolio Items:**

* + - * GDPR Compliance Audit Report
      * Ethical Hacking Policy Document
      * Security Awareness Campaign Materials
      * Accessibility and Inclusion Review
      * Professional Conduct Reflection
      * Legal Standards Mapping to Security Controls
      * Third-Party Risk Assessment Report

fbsdbsdsbbdsb

1. **GDPR Compliance Audit Report**
   * Assesses adherence to data protection regulations.
2. **Ethical Hacking Policy Document**
   * Defines boundaries and responsibilities for ethical testing.
3. **Security Awareness Campaign Materials**
   * Posters, presentations, or videos promoting secure behaviour.
4. **Accessibility and Inclusion Review**
   * Ensures security tools and policies are inclusive.
5. **Professional Conduct Reflection**
   * Reflects on ethical dilemmas and decision-making.
6. **Legal Standards Mapping to Security Controls**
   * Links controls to laws like NIS2, ISO 27001, etc.
7. **Third-Party Risk Assessment Report**
   * Evaluates vendor compliance and security posture.
8. **Security Policy Review and Update Log**
   * Documents changes based on legal or ethical considerations.

**References**

[1] [Cyber security technologist (2021) / Skills England](https://skillsengland.education.gov.uk/apprenticeship-standards/st1021-v1-0)

[2] [Digital and technology solutions professional / Skills England](https://skillsengland.education.gov.uk/apprenticeship-standards/st0119-v1-2)