# Digital Product Risk Management(DPRA)


**CURIUM Digital Product Risk Management(DPRA)**

*The CURIUM project is supported by the European Cybersecurity Industrial, Technology and Research Competence Centre (ECCC) under Grant Agreement No. 101190372. Views and opinions expressed are those of the author(s) only and do not necessarily reflect those of the European Union or the ECCC*

## DPRA Overview

DPRA is an evidence-driven, step-wised dynamic approach which aims to determine the compliance of ICT products based on the associated assets and their risks and controls to mitigate the risks. The tool provides capabilities to the organisations for managing their security risks in a holistic and cost-effective manner by assessing both individual and cascading risk taking into account the vulnerabilities and threats that are linked with the ICT product. The tools adopt open intelligence in real time to identify the vulnerabilities and threats that are linked with the assets and standards like NIST 800-53 and ISO/IEC 15408 for an unified security declaration and control.

The tool exhibits following key features:

- Open intelligence facilitates the DPRA to adopt and incorporate a variety of security relating open source information from CPE, CAPEC, and CVE as well as standards and specifications like NIST 800-53 and ISO/IEC 15408 for vulnerability and threat identification as well as control and security declaration.
- The asset inventory includes internal and external assets , their related components, vulnerabilities and threats along with dependency modelling to visualize the dependencies among the assets for the discovery of attack paths given a specific set of assets.
- The ICT product declaration feature allows to declare the products of the organization that are required to achieve compliance. The features includes security declaration for the product and allows to link with the asset along with the risk level and control for the assets so that overall compliance assessment can be done.
- The Vulnerabilities Management feature identifies the possible vulnerabilities from the CVEDetails portal that are relevant with the identified asset in real time. All the vulnerability information is based on the CVE naming standard and are organized according to severity determined by the Common Vulnerability Scoring System Version 3 (CVSSv3) standard.
- The Threats feature acts as a comprehensive dictionary of known threats based on the MITRE attack identifiers and associates the identified vulnerabilities with one or more weakness identifiers.

## DPRA User Manual

**User Login :** User needs to obtain credential to access the system. The login screen is presented in Figure 1 introduces the initial **access gateway** to access the Digital Product Risk Management / Cyber Resilience Assessment. This process is the first critical step in ensuring that only legitimate users can access the system. The sign in includes user name or email address and password.

*The CURIUM project is supported by the European Cybersecurity Industrial, Technology and Research Competence Centre (ECCC) under Grant Agreement No. 101190372. Views and opinions expressed are those of the author(s) only and do not necessarily reflect those of the European Union or the ECCC*

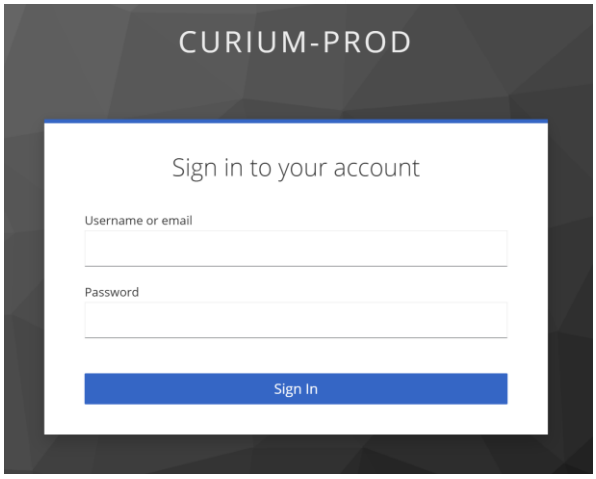


**Figure 1:User login prompt**

User dashboard: Upon successful login , the legitimate user is immediately directed to the main dashboard, as shown conceptually in Figure 2. It acts as the main interface for all activities related with the tool. The dashboard includes necessary components through a clear navigation sidebar that groups related functions, including asset inventory, components, vulnerabilities, threats and product.


**Figure 2: User Dashboard**

**Asset Inventory :** The initial step to trigger the DPRA is the inventory of asset where users are allowed to add the asset relevant with the organization. There are two different types of assets can be added into DPRA as shown in Figure 3. The asset can be added by following the open intelligence CPE detailed or using SBOM files that include information about the assets. To do that, the user selects “Add Asset” in the “Assets” section and proceeds accordingly.

*The CURIUM project is supported by the European Cybersecurity Industrial, Technology and Research Competence Centre (ECCC) under Grant Agreement No. 101190372. Views and opinions expressed are those of the author(s) only and do not necessarily reflect those of the European Union or the ECCC*

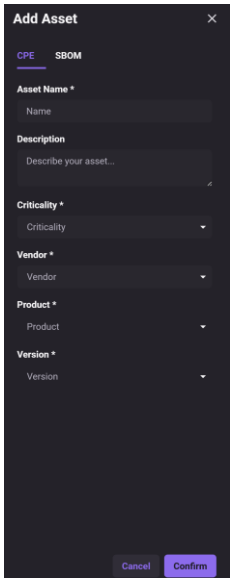


**Figure 3: Asset Addition**

Figure 4 illustrates the interface for an asset inventory once all assets are added. Hence, it is the outcome of the ass asset function shown here is the ability to easily add new assets using an **"Add Asset"** button.

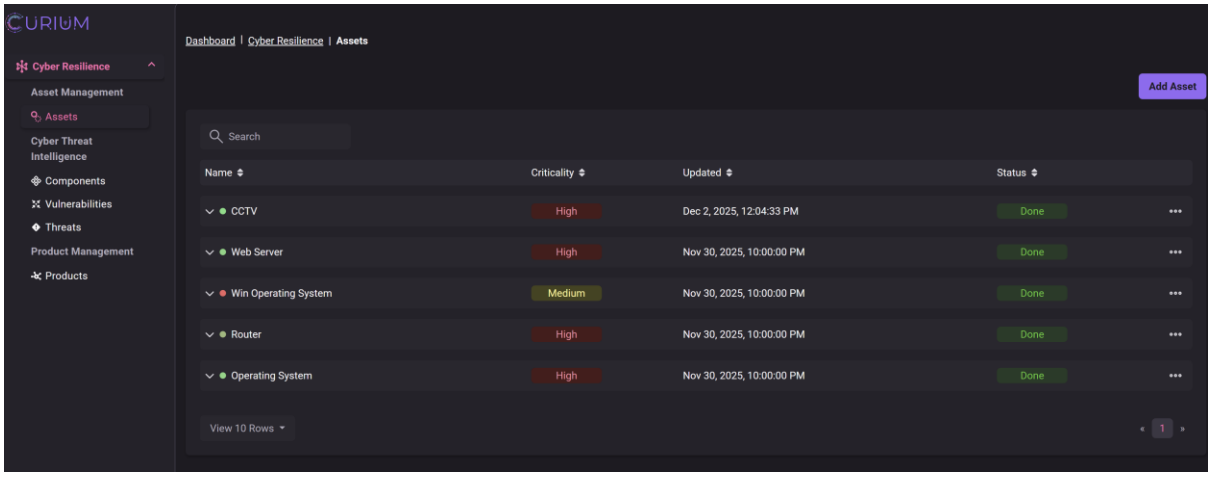


**Figure 4: Asset Inventory**

**Vulnerability Management**: The DPRA lists the vulnerabilities as a core function of its vulnerability management capabilities. It achieves this by automatically importing published vulnerability reports from open repositories like CWE (Common Weakness Enumeration) and the NVD (National Vulnerability Database), linking them to the manufacturer's identified assets. **Error! Reference source not found.** shows the list of vulnerabilities with each vulnerability detailed includes CVE ID, severity level, base and EPSS score(usually from CVSS) and library. The tool notably includes the EPSS score, which specifies the exploitation probability of a vulnerability within a given period, allowing for risk-based prioritization. Moreover, as shown in Figure 6, the system allows users to add confirmed vulnerabilities those already present in the NVD and link them to the relevant component or asset for comprehensive tracking.

*The CURIUM project is supported by the European Cybersecurity Industrial, Technology and Research Competence Centre (ECCC) under Grant Agreement No. 101190372. Views and opinions expressed are those of the author(s) only and do not necessarily reflect those of the European Union or the ECCC*


**Figure 5: List of Vulnerabilities**

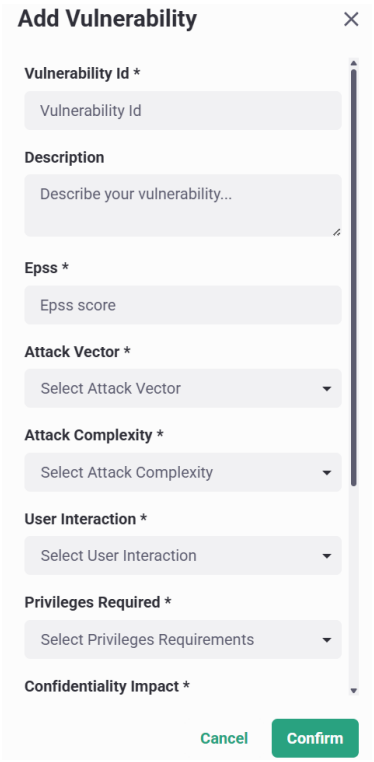


**Figure 6: Vulnerability Addition**

**Cyber threat intelligence:** Similar to the Vulnerability Management process, A pool that collects and analyses information about existing and emerging cyber threats, including attack-types, and asset vulnerabilities based on prominent open repositories.

*The CURIUM project is supported by the European Cybersecurity Industrial, Technology and Research Competence Centre (ECCC) under Grant Agreement No. 101190372. Views and opinions expressed are those of the author(s) only and do not necessarily reflect those of the European Union or the ECCC*

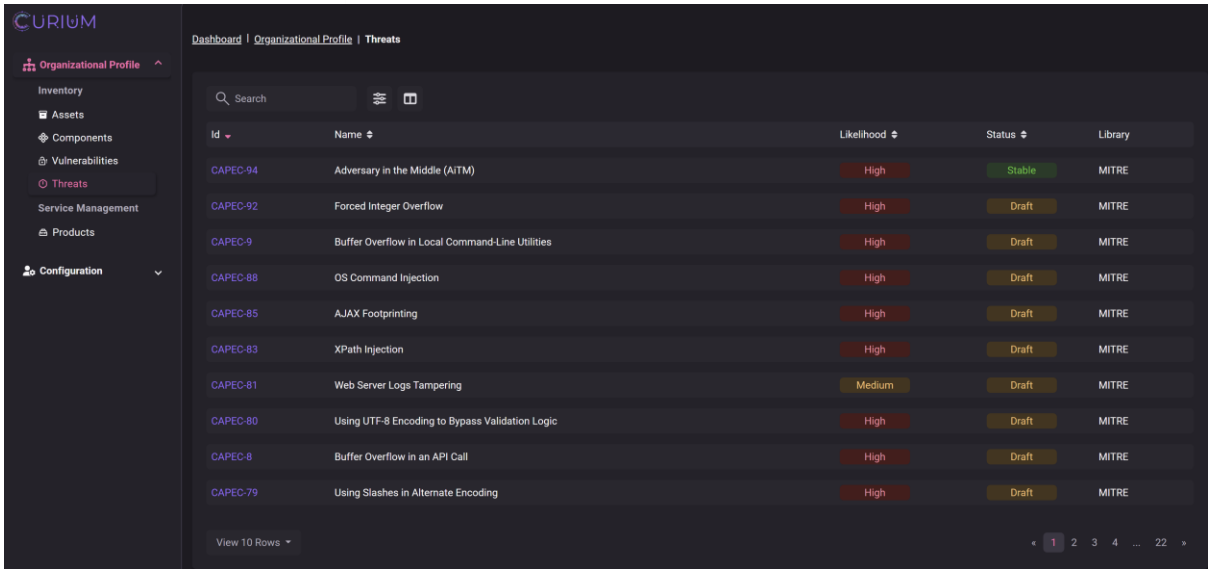


**Figure 7: Threat Detailed**

**Product declaration:** This feature initiates with adding product with Digital Elements that are relevant with the organization and required to achieve compliance. Figure 8 shows how user can add product and define specific assurance level for the product. It includes

- **Product Name:** A required field for assigning a unique and recognizable name to the product
- **Description:** An open text field for providing a brief overview of the product's function, scope, and intended environment
- Assurance Level: Allow user to choose specific assurance level derived from the Common Criteria (ISO/IEC 15408) including
    - AL1 (Functionally Tested): The lowest level; testing is limited to the product's basic functions.
    - EAL2 (Structurally Tested): Basic security assurance gained through testing and review of the design structure.
    - EAL3 (Methodically Tested and Checked): Requires more rigorous testing and structured design methods.
    - EAL4 (Methodically Designed, Tested and Reviewed): Considered the highest practical level of assurance for commercial products, requiring rigorous methods and testing.
    - EAL5 (Semi-formally Designed and Tested) to EAL7 (Formally Verified, Designed and Tested): These represent progressively higher levels of assurance, typically reserved for high-risk applications (e.g., security kernels, smart cards) where formal verification methods are mandated.

*The CURIUM project is supported by the European Cybersecurity Industrial, Technology and Research Competence Centre (ECCC) under Grant Agreement No. 101190372. Views and opinions expressed are those of the author(s) only and do not necessarily reflect those of the European Union or the ECCC*

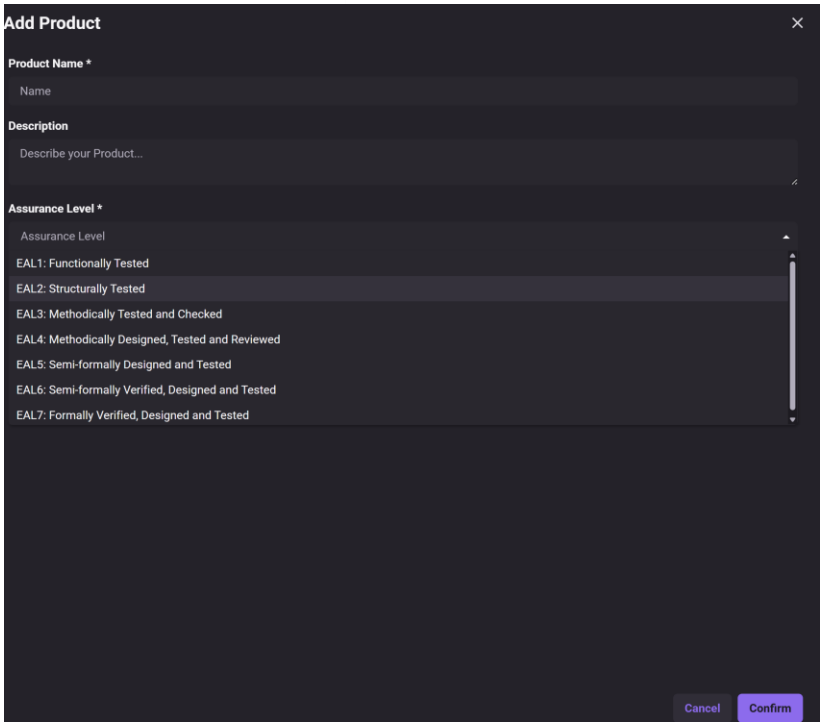


**Figure 8: Adding product**

Once the product is added to the system, the user is navigated to the Product Details screen, as shown in Figure 9. This allows user to add all relevant information from asset listing to the security objective , requirements necessary to support the assessment. It includes

- Assets: Asset related with the product
- Security Objectives: This tab is used to declare the specific security objectives relevant to the product.
- Security Requirements: This section details the specific security requirements (the mechanisms or functions needed to achieve the declared security objectives
- Questionnaires: This final tab represents the launch point for the core CyReA Assessment Wizard. Once assets, objectives, and requirements are defined, the user proceeds here to complete the structured, questionary-based assessment that verifies compliance against the CRA mandates.

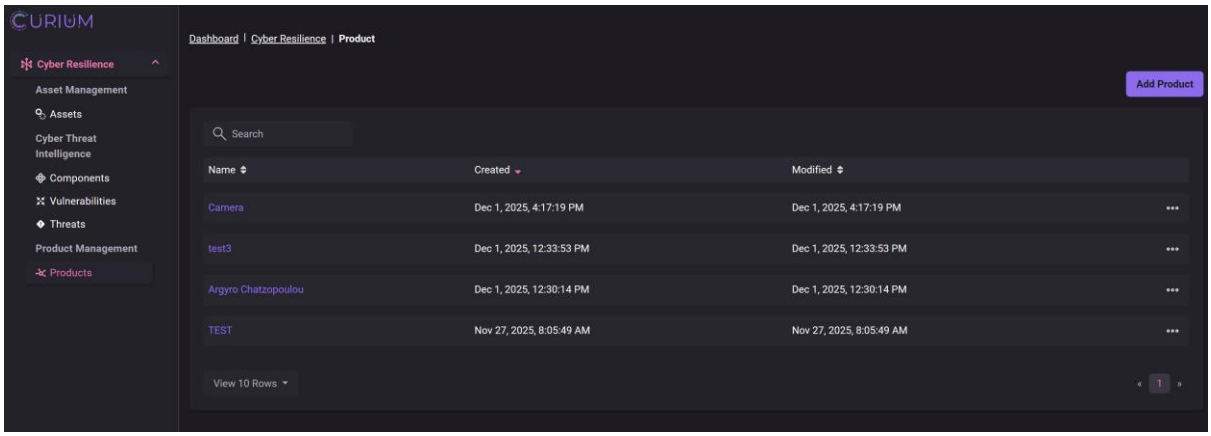


**Figure 9 Product Detailed**

*The CURIUM project is supported by the European Cybersecurity Industrial, Technology and Research Competence Centre (ECCC) under Grant Agreement No. 101190372. Views and opinions expressed are those of the author(s) only and do not necessarily reflect those of the European Union or the ECCC*

Figure 10 shows the security requirements tab within the Product Details view . These requirements are typically extracted from recognized standards such as the Common Criteria (ISO/IEC 15408), serving as a standardized method for defining the product's security posture. Each requirement is identified by a unique Id ,name and applicant as status .The appliance is a clear visual indicators to show whether the requirement is fully or partially applied to the product.

Definition of Security Requirements. Security Requirements can be defined on the assets of the product with digital elements from the “DPRA: Security Requirements” tab in the product management environment of DPRA. Security requirements are mapped with security objectives, as mentioned in the beginning of this section. Specifically, each security objective can be addressed by the satisfaction of one or more security requirements. Upon selecting the security objectives of the product’s assets, a list of all interrelated requirements appears in the “DPRA: Security Requirements” tab.

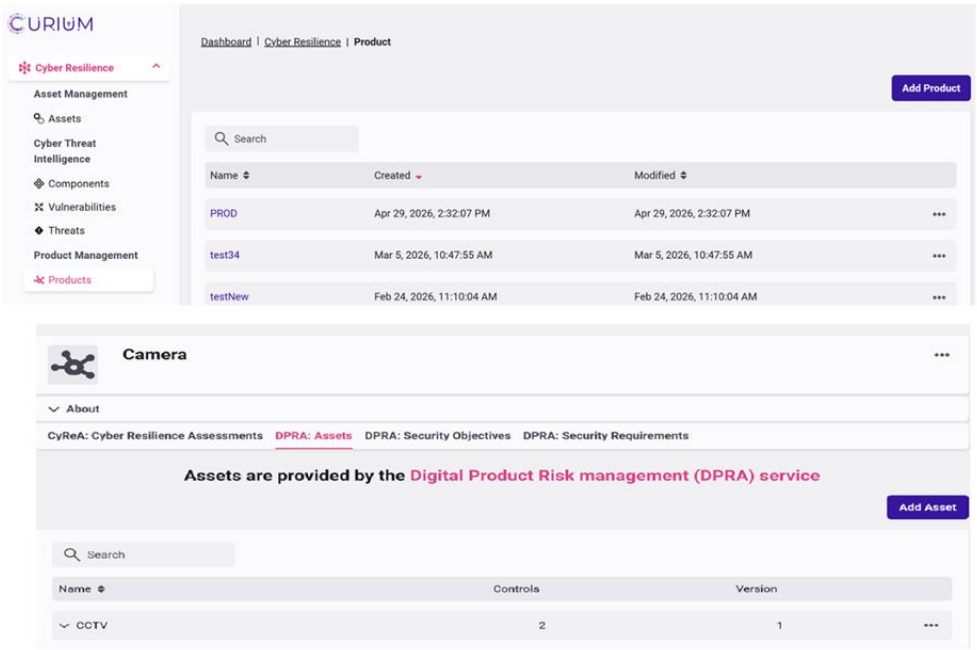


**Figure 10: Product Specific Security Requirements**

The user can view the security requirements per product’s asset and deselect those that he/she wants to exclude from the security evaluation process of an individual asset by navigating to the respective options of the 3-dot menu, depicted at the right part of each requirement as shown in Figure 11.

*The CURIUM project is supported by the European Cybersecurity Industrial, Technology and Research Competence Centre (ECCC) under Grant Agreement No. 101190372. Views and opinions expressed are those of the author(s) only and do not necessarily reflect those of the European Union or the ECCC*

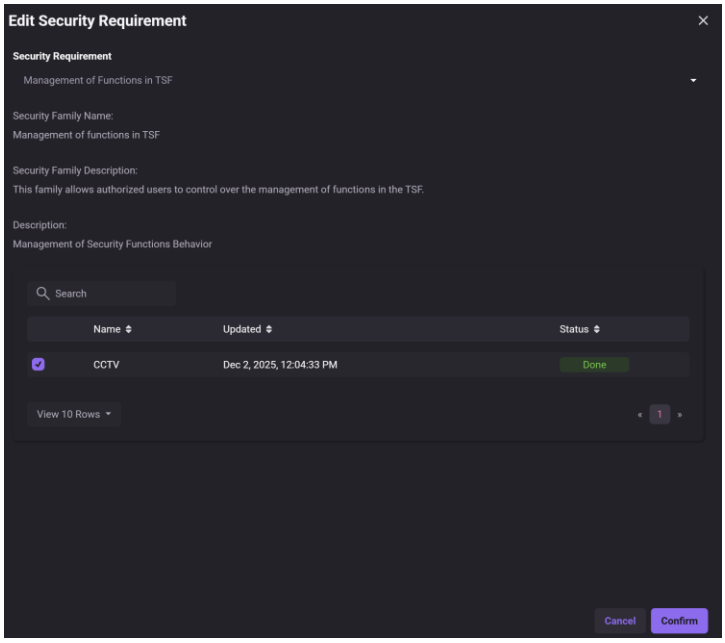


**Figure 11: Security Requirements Amendment**

Security Control Management

Security requirements are interrelated with security controls to address these requirements. To add/manage security controls on assets, the user selects the preferred asset in the Product Management environment and by clicking on the 3-dot menu , he/she selects the “Manage Control” option. Then, the Control tab appears depicting all security requirements defined for the specific asset. To assign security controls on the product’s asset, the user selects a security requirement and clicks from the 3-dot menu the option “Assign NIST Controls”. Afterwards, from the “Manage NIST controls” tab, the user selects the security controls implemented to satisfy the specific requirement from a default list, as shown in Figure 12.

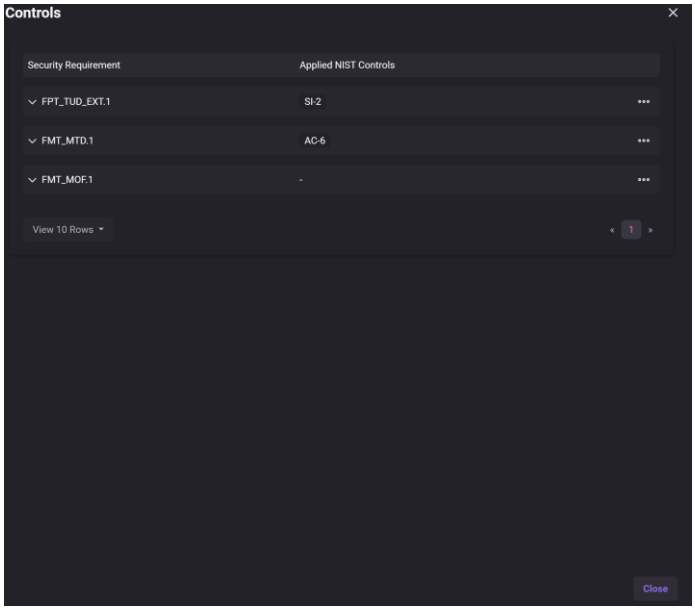


**Figure 12: Security Control Management**

*The CURIUM project is supported by the European Cybersecurity Industrial, Technology and Research Competence Centre (ECCC) under Grant Agreement No. 101190372. Views and opinions expressed are those of the author(s) only and do not necessarily reflect those of the European Union or the ECCC*

View Product's Protection Profile

After defining all the proper technical and security information of the product and its embedded elements (assets), the user can review the product's protection profile. To achieve this, the user selects the preferred product from the products' list in the product management environment of DPRA and then, he/she selects the "View Protection Profile" as shown in Figure 13 option from the 3-dot menu appearing at the right side in the product's tab.

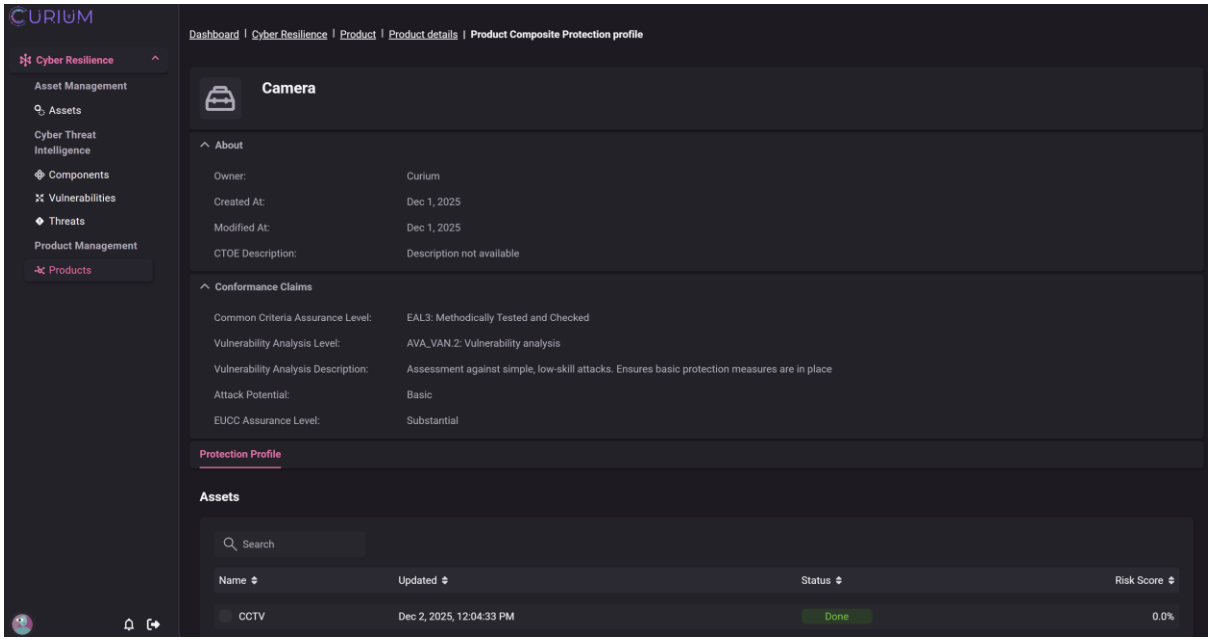


**Figure 13: Protection profile**

*The CURIUM project is supported by the European Cybersecurity Industrial, Technology and Research Competence Centre (ECCC) under Grant Agreement No. 101190372. Views and opinions expressed are those of the author(s) only and do not necessarily reflect those of the European Union or the ECCC*