**Fondul Social European**

**Programul Operațional Capital Uman 2014-2020**

Axa prioritară **Educatie si Competente (AP6)**

Prioritatea de investiții: ***10.iv - Sporirea relevanţei pe piaţa forţelor de muncă a educaţiei şi a sistemelor de formare, facilitarea tranziţiei de la educaţie la piaţa forţelor de muncă  şi consolidarea formării  şi a sistemelor de formare profesională, precum şi a calităţii lor, inclusiv prin mecanisme de anticipare a competenţelor, adaptarea programelor de învăţământ şi instituirea şi dezvoltarea unor sisteme de învăţare la locul de muncă, inclusiv a unor sisteme de învăţare duală  şi programe de ucenicie***

Beneficiar: **Universitatea Titu Maiorescu din Bucuresti**

Titlul proiectului: „**STAGII DE PRACTICA IN CENTRUL DE EXCELENTA IN SECURITATE CIBERNETICA IN CLOUD - CyberX**”

Contract de finanțare nr. **24093/ 25.11.2020** Cod SMIS: **133276**

**ACTIVITĂȚI DESFĂȘURATE**

**PE PARCURSUL STAGIULUI DE PRACTICĂ**

***Etapa de lucru pe platforma***

***CENTRUL DE EXCELENTA IN SECURITATE CIBERNETICA IN CLOUD – CyberX***

**Lucrări practice**

**STUDENT:**

**................Parfion Vladut...............**

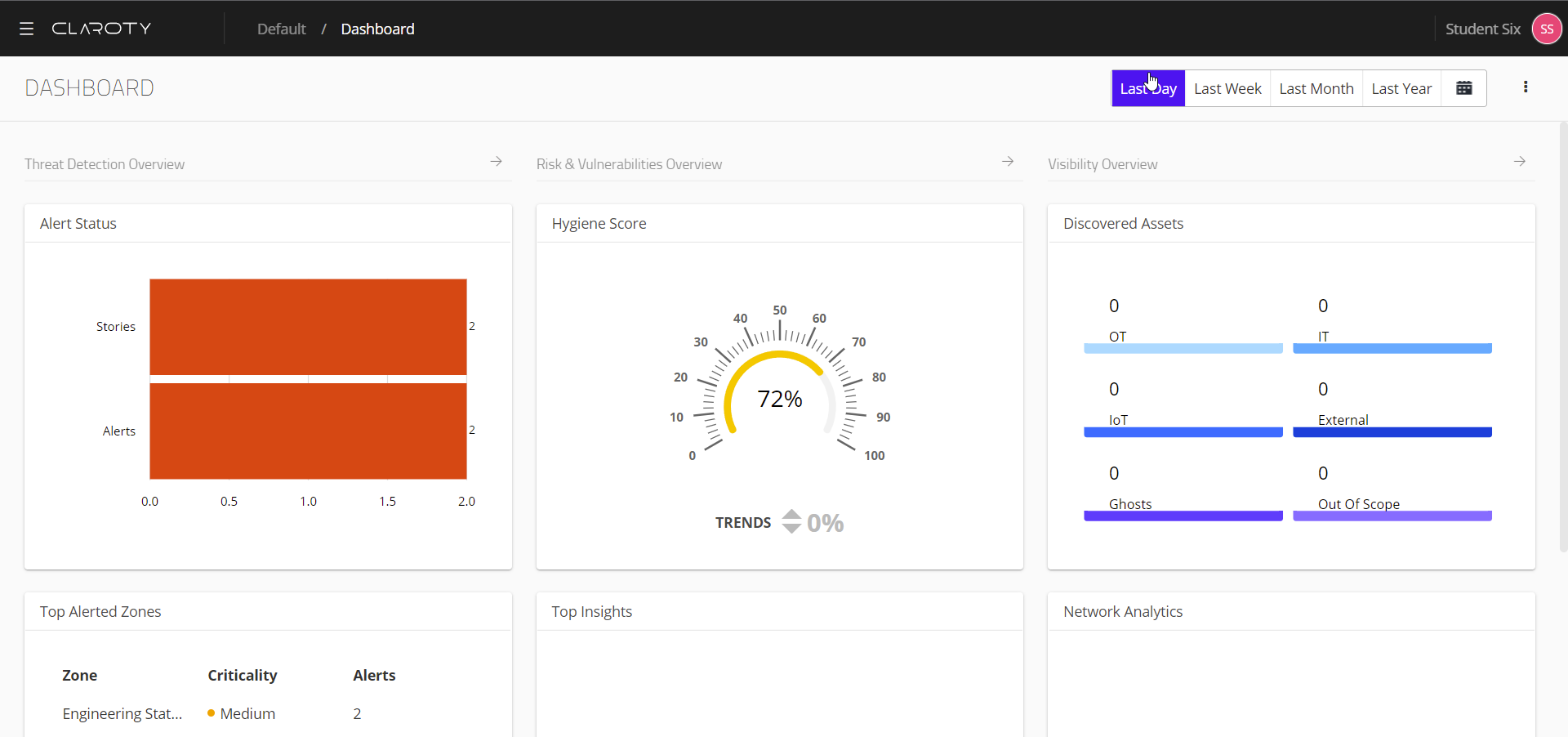
COMPONENTA 3 - Claroty Secure Remote Access v. 3.1.

REDUCEREA COMPLEXITĂȚII CYBERSECURITĂȚII INDUSTRIALE

Platforma Claroty oferă cea mai largă gamă de controale de securitate cibernetică industrială din industrie într-o singură soluție care se implementează fără probleme și se integrează perfect cu infrastructura existentă.

Platforma de Cyber Security destinata infrastructurilor industriale.

Pagina de start reprezinta starea generala a sistemului:



<https://claroty.com/blog/>

Securitatea cibernetică industrială eficientă începe cu a ști ce trebuie securizat. Platforma Claroty vă oferă aceste cunoștințe prin dezvăluirea și contextualizarea 100% din conținutul rețelei dvs., inclusiv conținutul său invizibil. Rezultatul este un inventar centralizat, ușor de gestionat și mereu actualizat al tuturor activelor, proceselor și căilor de conectivitate OT, IoT și IIoT din rețeaua dvs., precum și o perspectivă definitivă a modului în care arată normalul. Vizibilitate

Acoperirea de neegalat a protocolului OT și tehnologia de scanare activă, pasivă și AppDB permit platformei Claroty să ofere vizibilitate deplină asupra tuturor celor trei variabile, care sunt integrante pentru evaluarea și reducerea eficientă a riscurilor în mediile OT. Acestea includ 1) Vizibilitatea activelor; 2) Vizibilitatea sesiunii de rețea; și 3) Vizibilitatea procesului operațional. Claroty este singurul furnizor care oferă acest calibru de vizibilitate OT.

Detectarea amenințărilor

Platforma Claroty utilizează cinci motoare de detectare pentru a profila automat toate activele, comunicațiile și procesele din mediile OT, pentru a stabili o linie de bază comportamentală care caracterizează traficul legitim și pentru a elimina falsele pozitive și pentru a oferi o acoperire cuprinzătoare și continuă de monitorizare a securității și integrității OT - totul fără a necesita expertiza OT. Aceste motoare includ: Detectare anomalii, Comportamente de securitate, Amenințări cunoscute, Comportamente operaționale și Reguli personalizate.



Scenariu Profesor:

Data Sources – Play PCAPS🡪pentru a “injectat” trafic in aplicatie

Graphical user interface, application

Description automatically generated A screenshot of a computer

Description automatically generated

Scenariu laborator - STUDENT

1. Se conecteaza la aplicatie

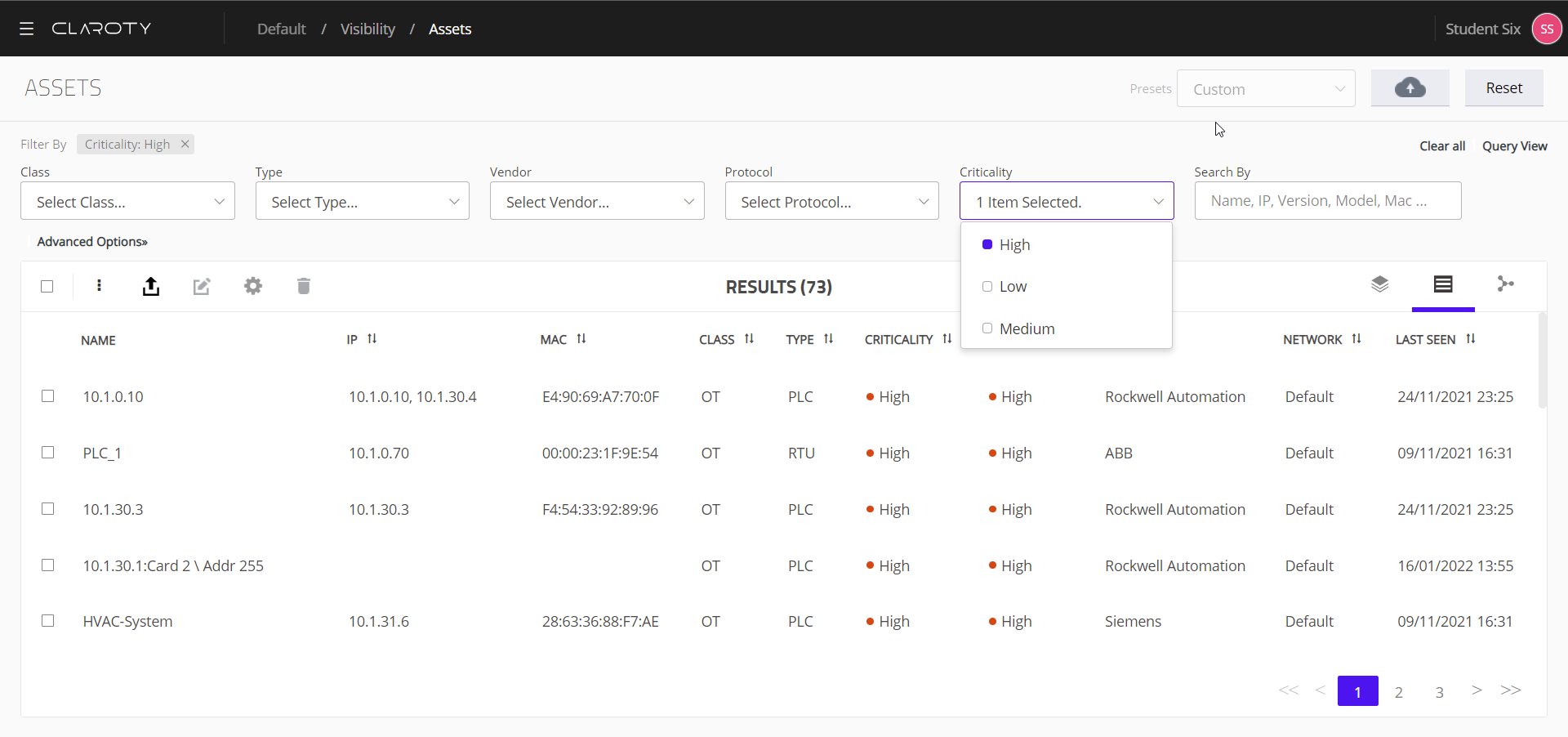
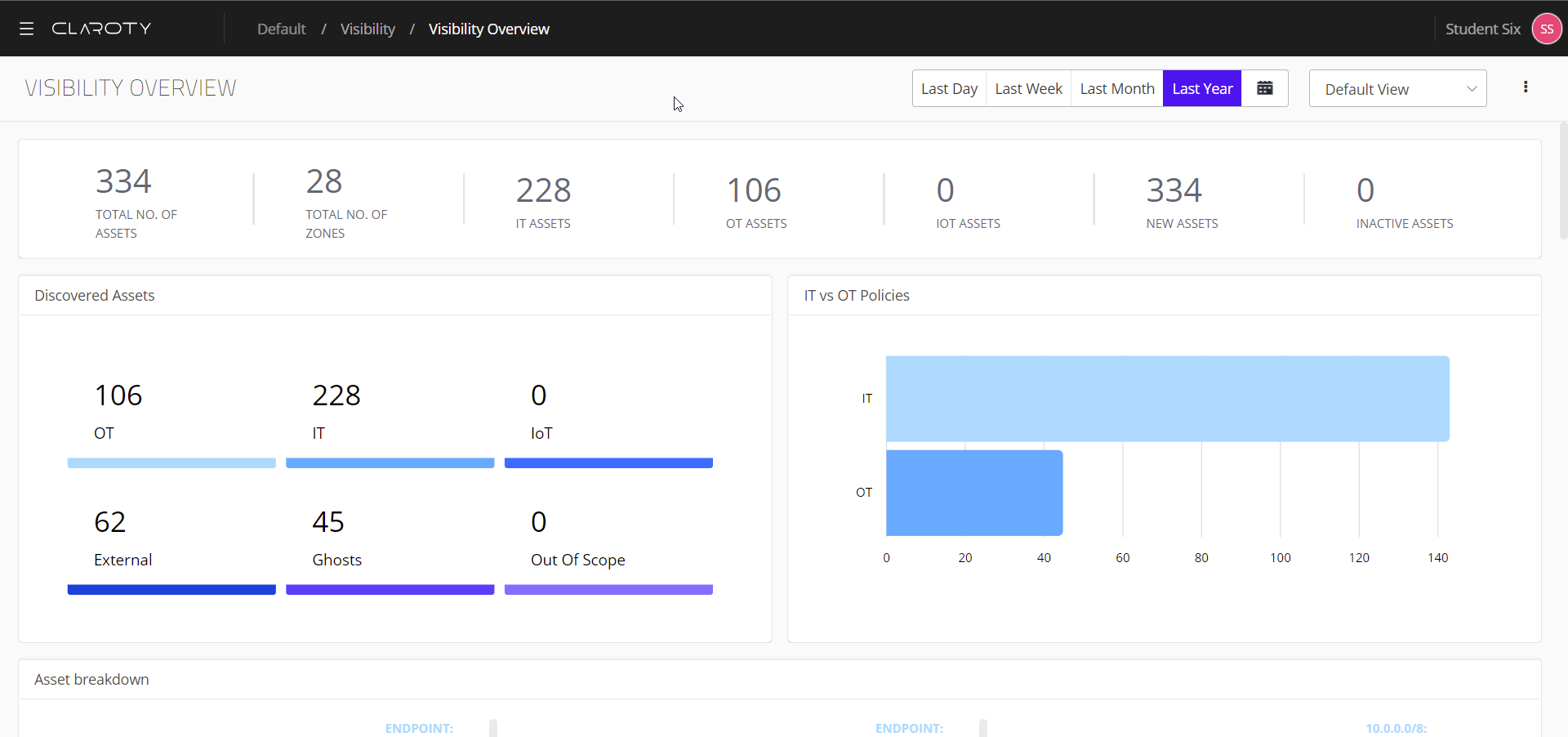
<https://10.224.4.103>



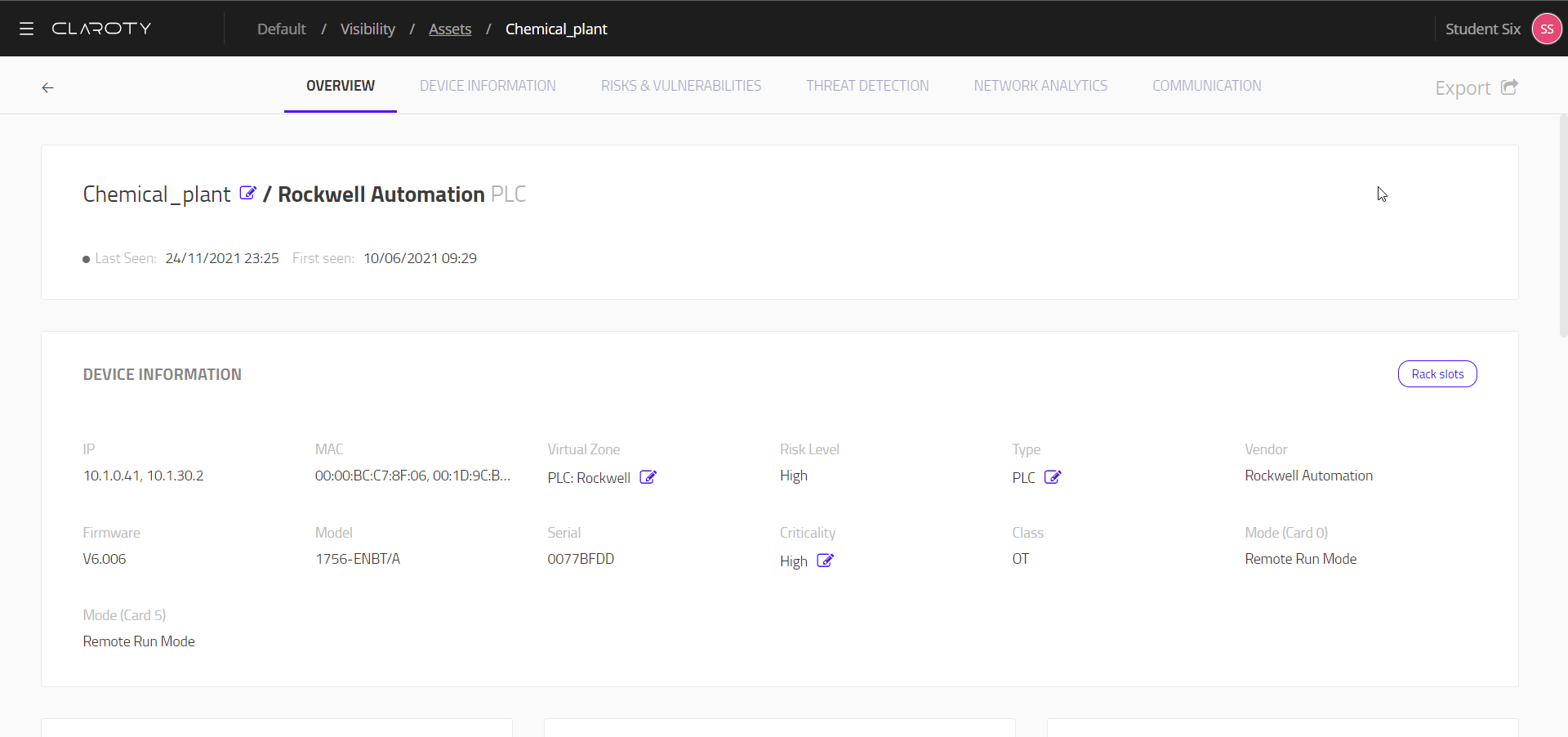
Se analizeaza elementele aplicatiei A picture containing text

Description automatically generated

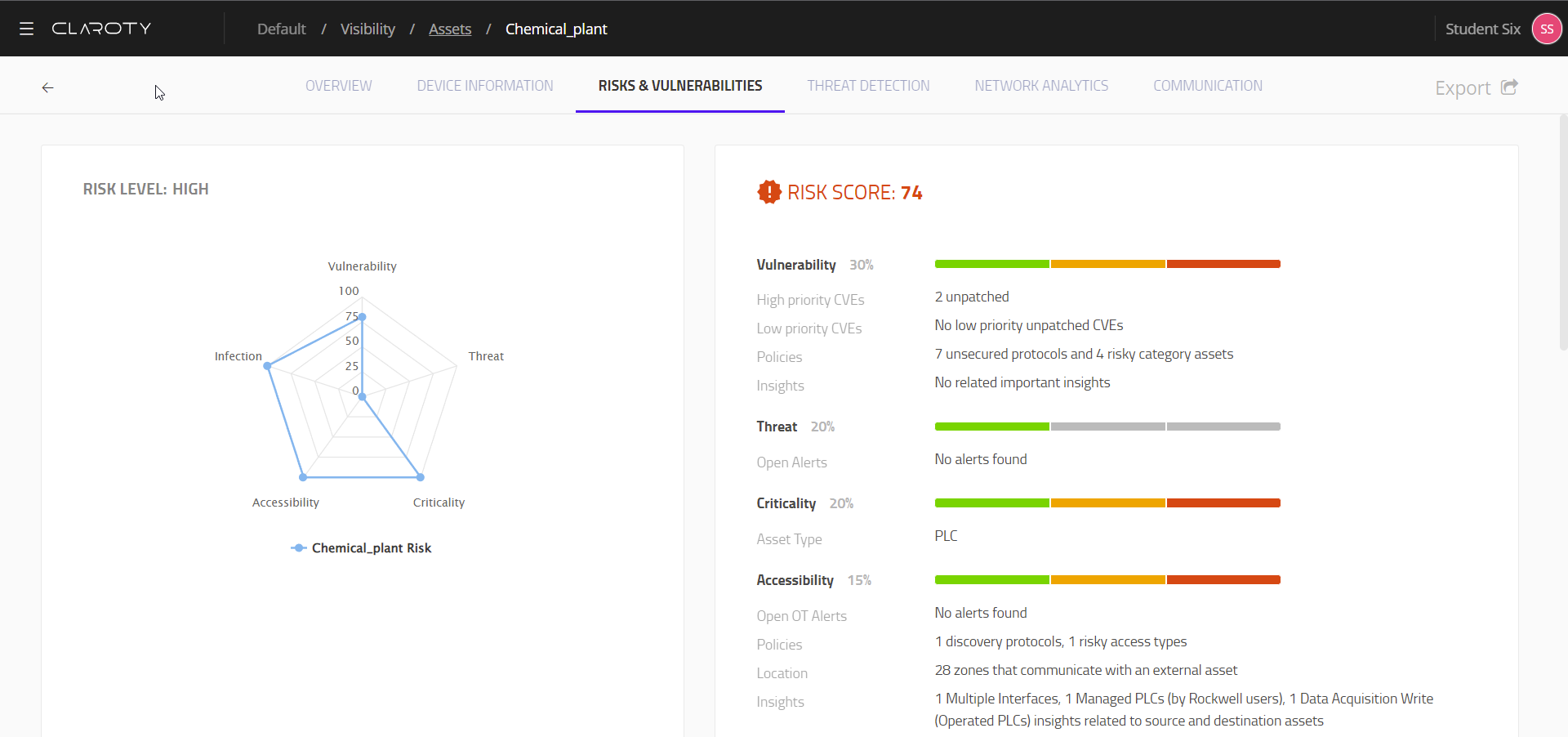
1. Visibility – Overview🡪 OT Assets pentru analiza traffic



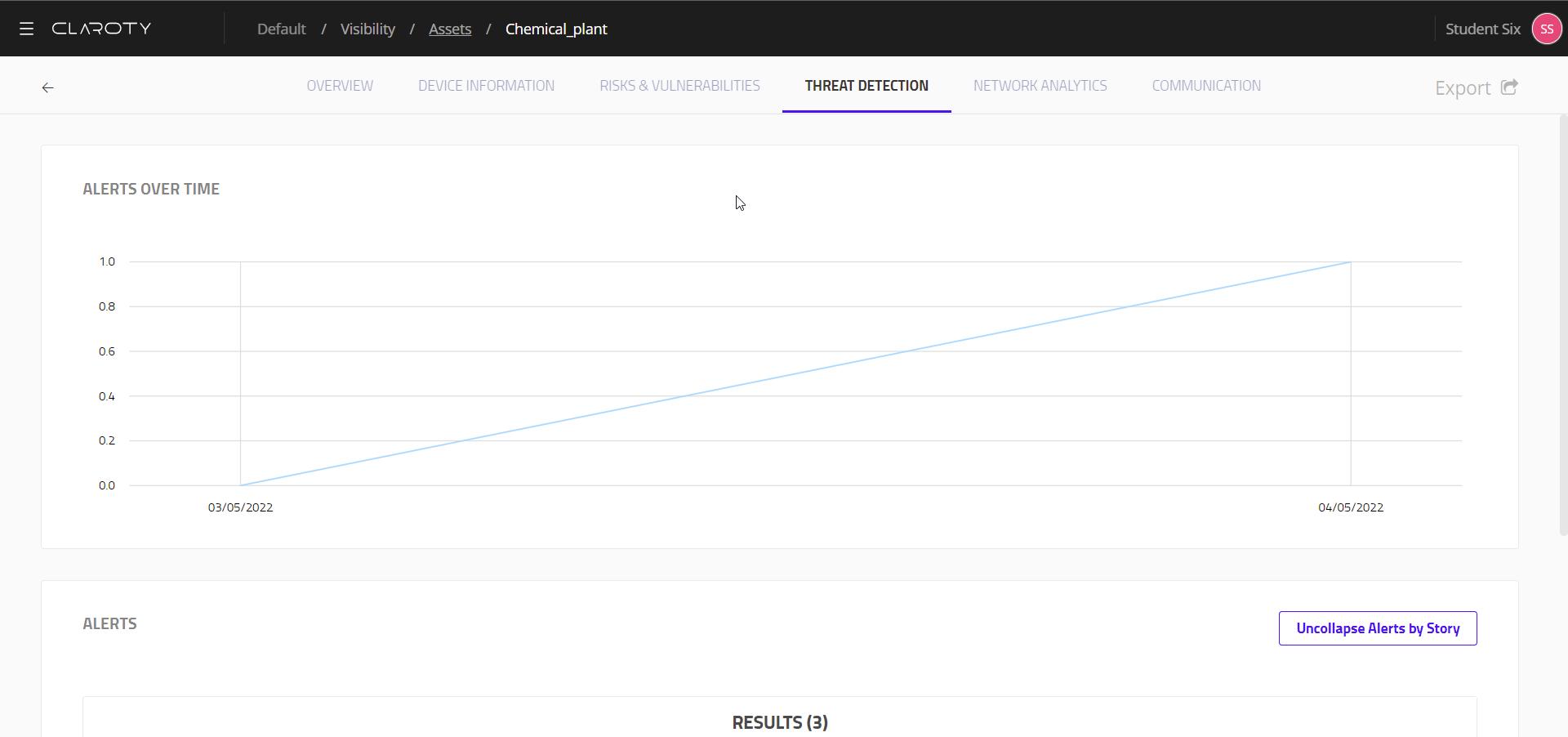
Ca exemplu alegem🡪 Chemical\_plant 🡪 are risc ridicat



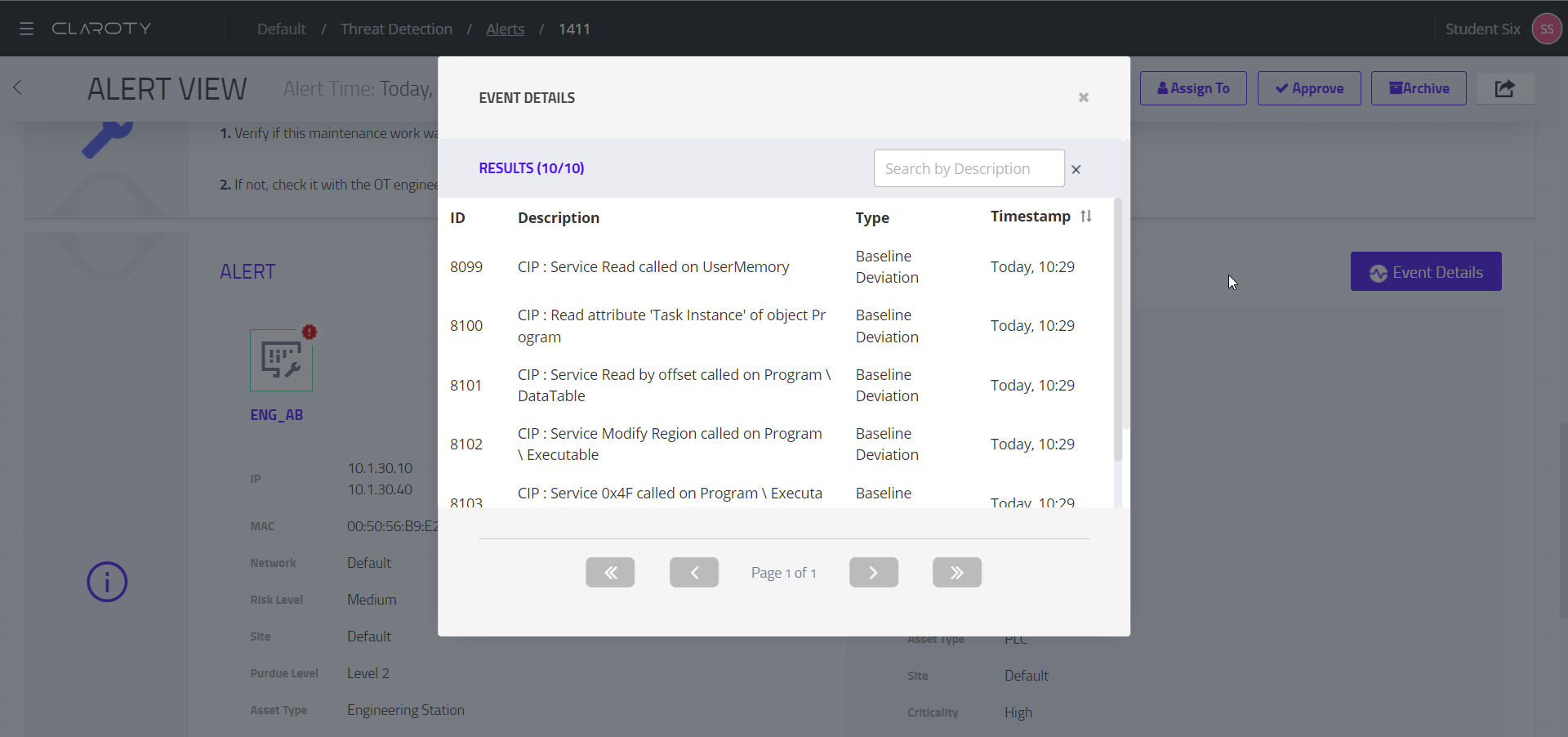
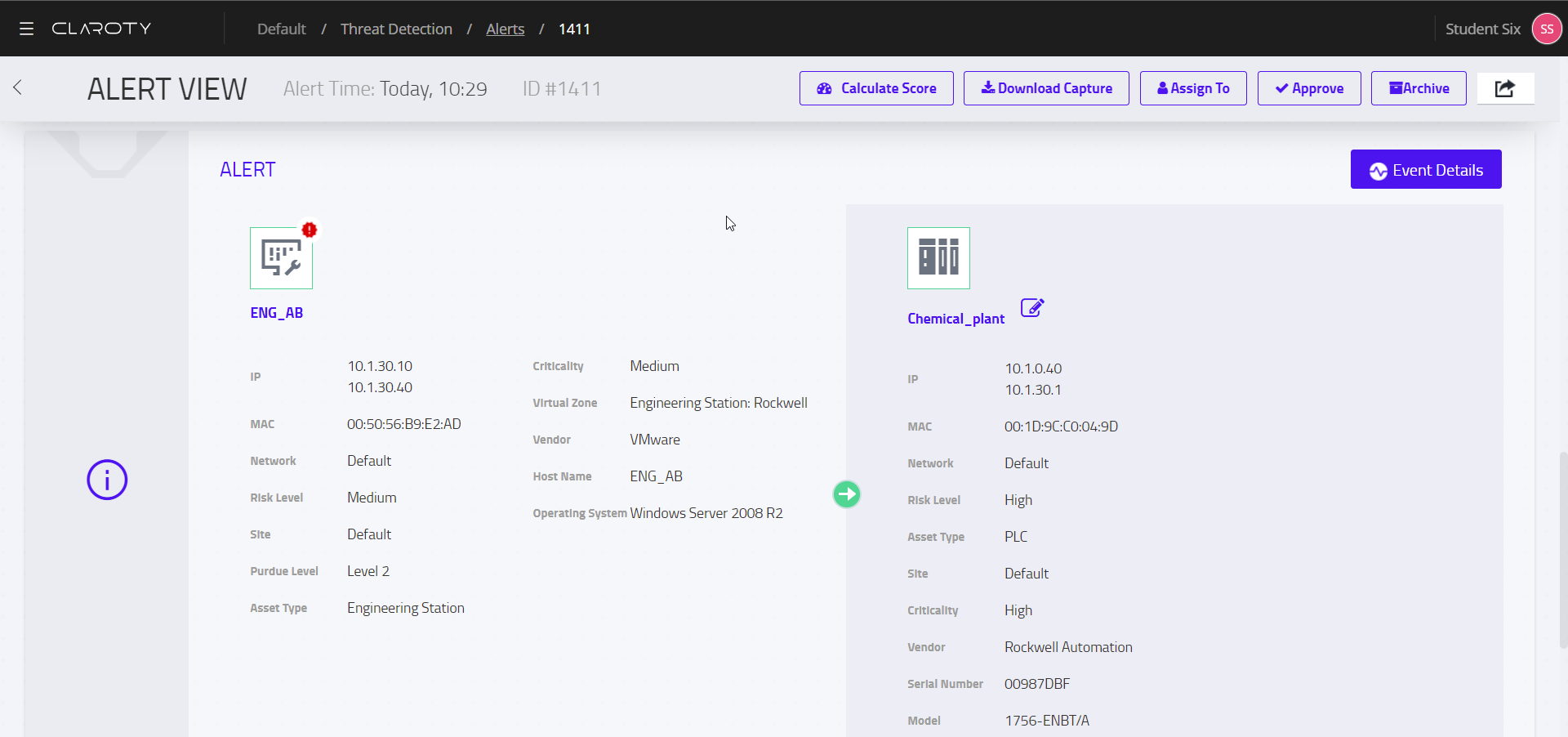
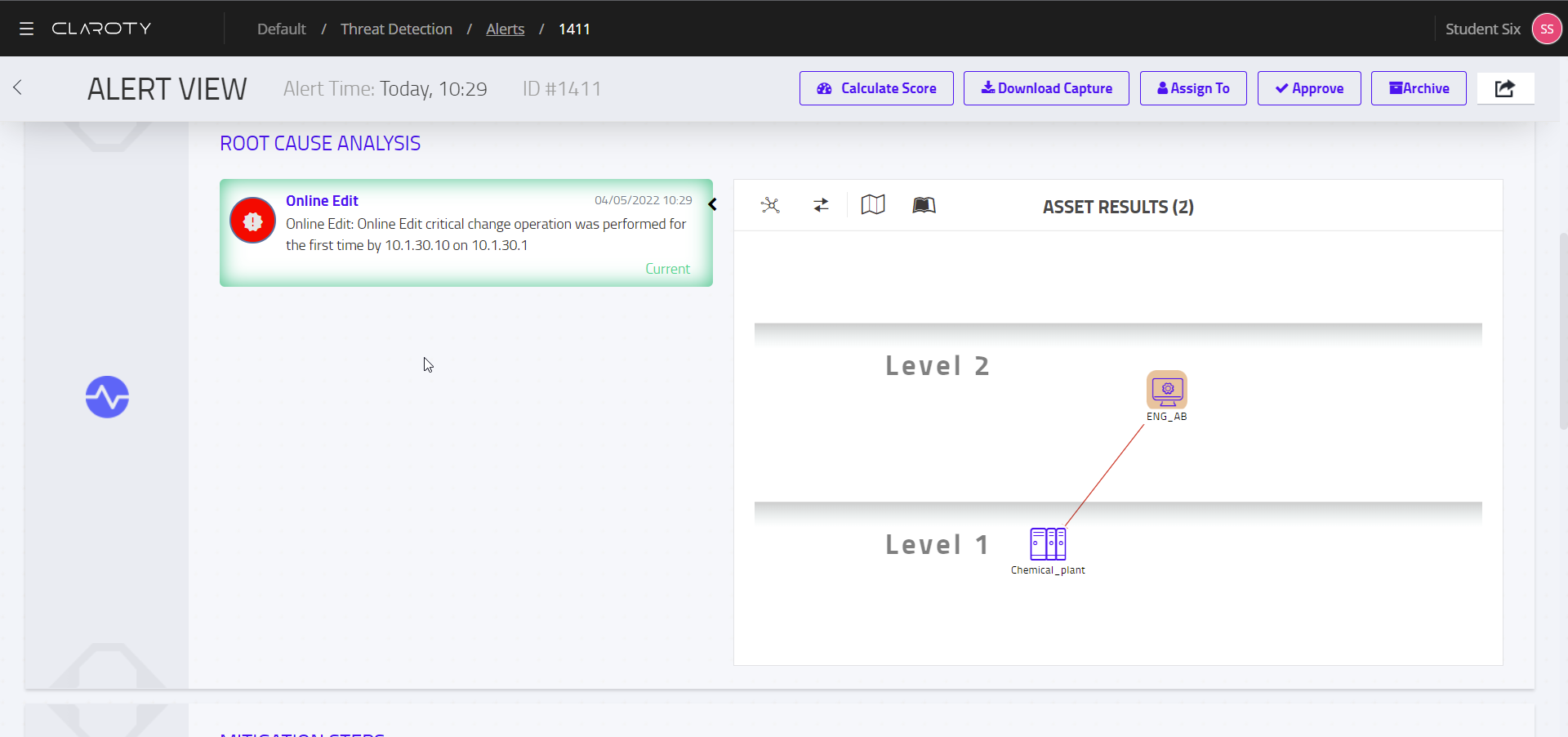
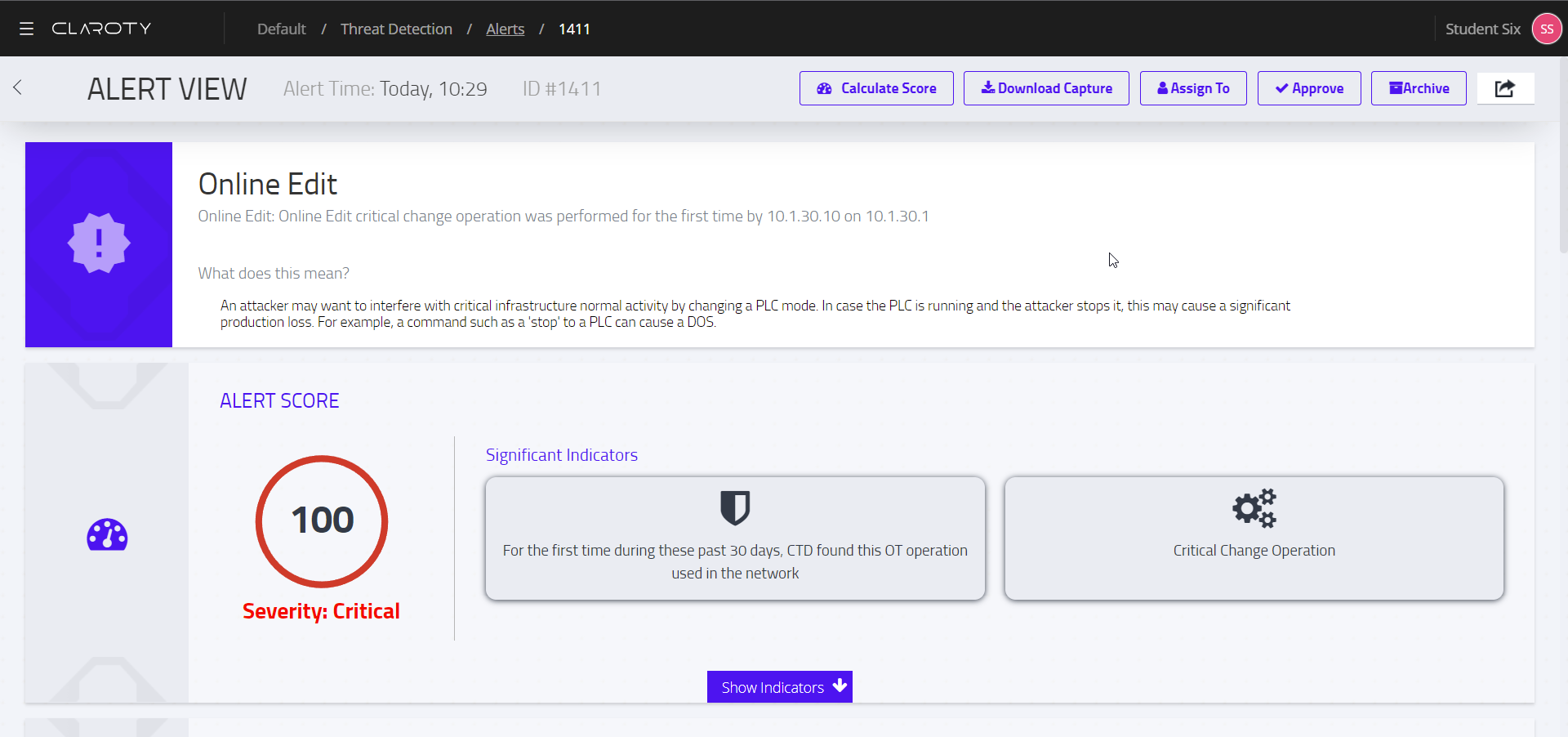
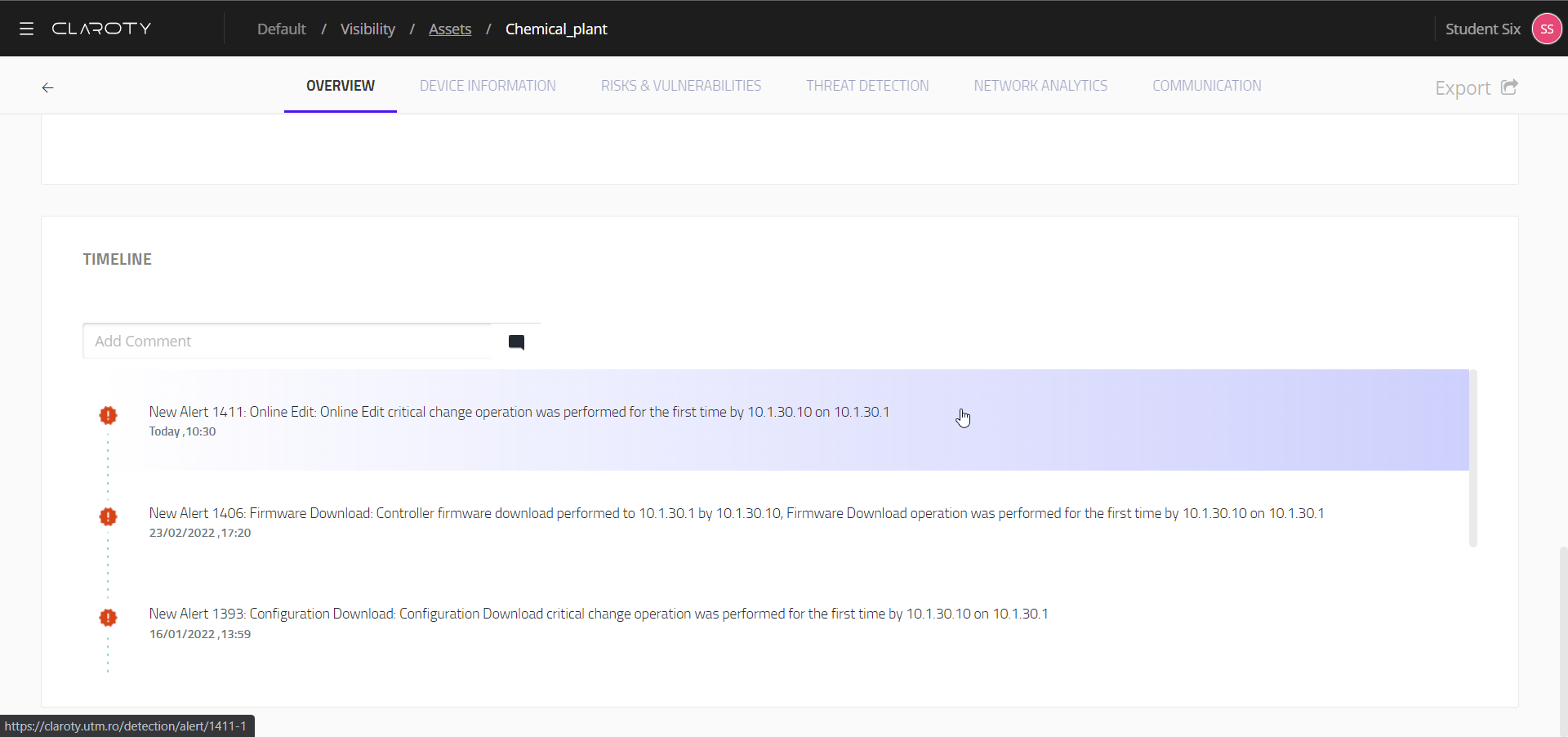
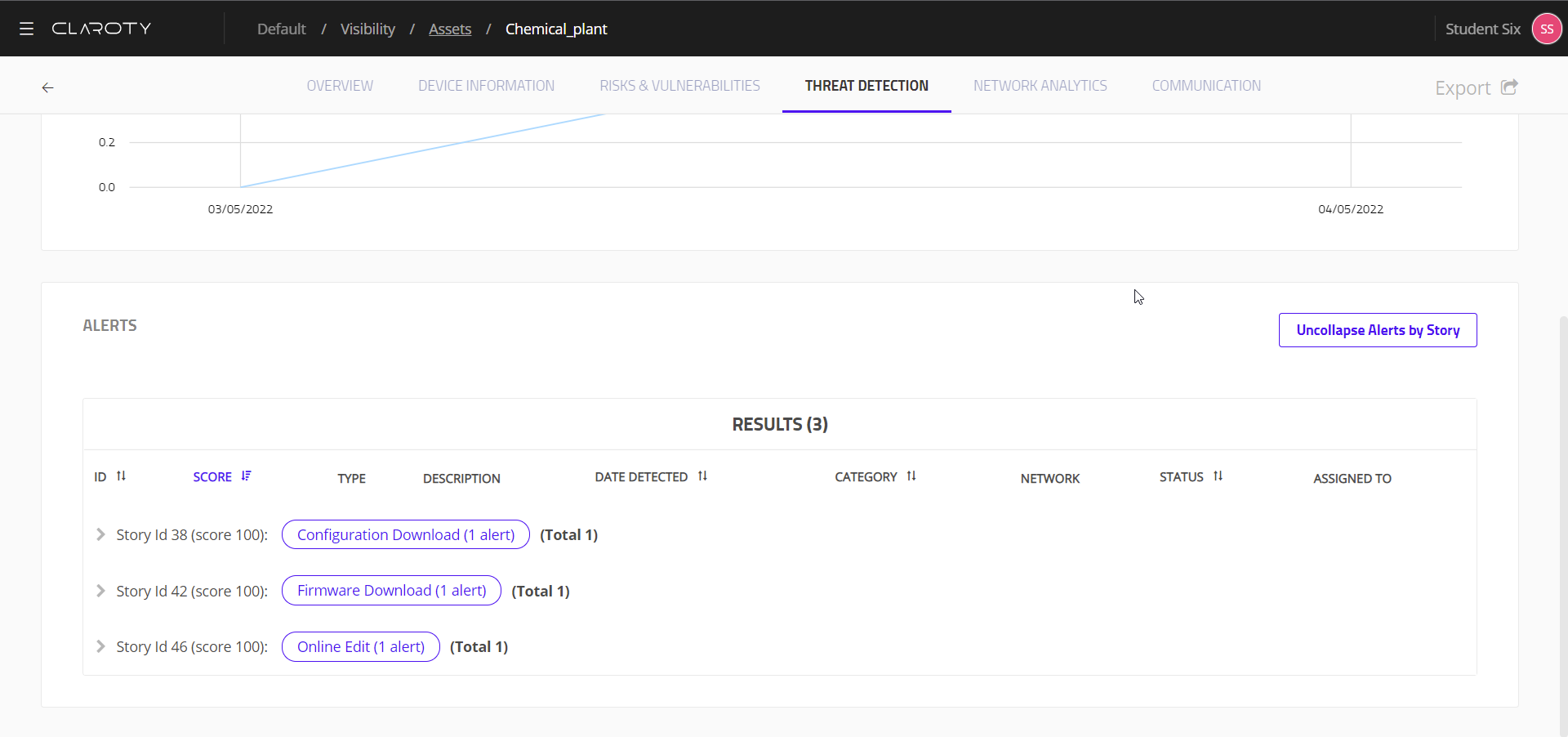
1. La Risk & Vulnerability 🡪se analizeaza detalii despre scorul primit:



1. Threat Detection 🡪 pentru a vedea alertele de pe echipamentul respectiv:

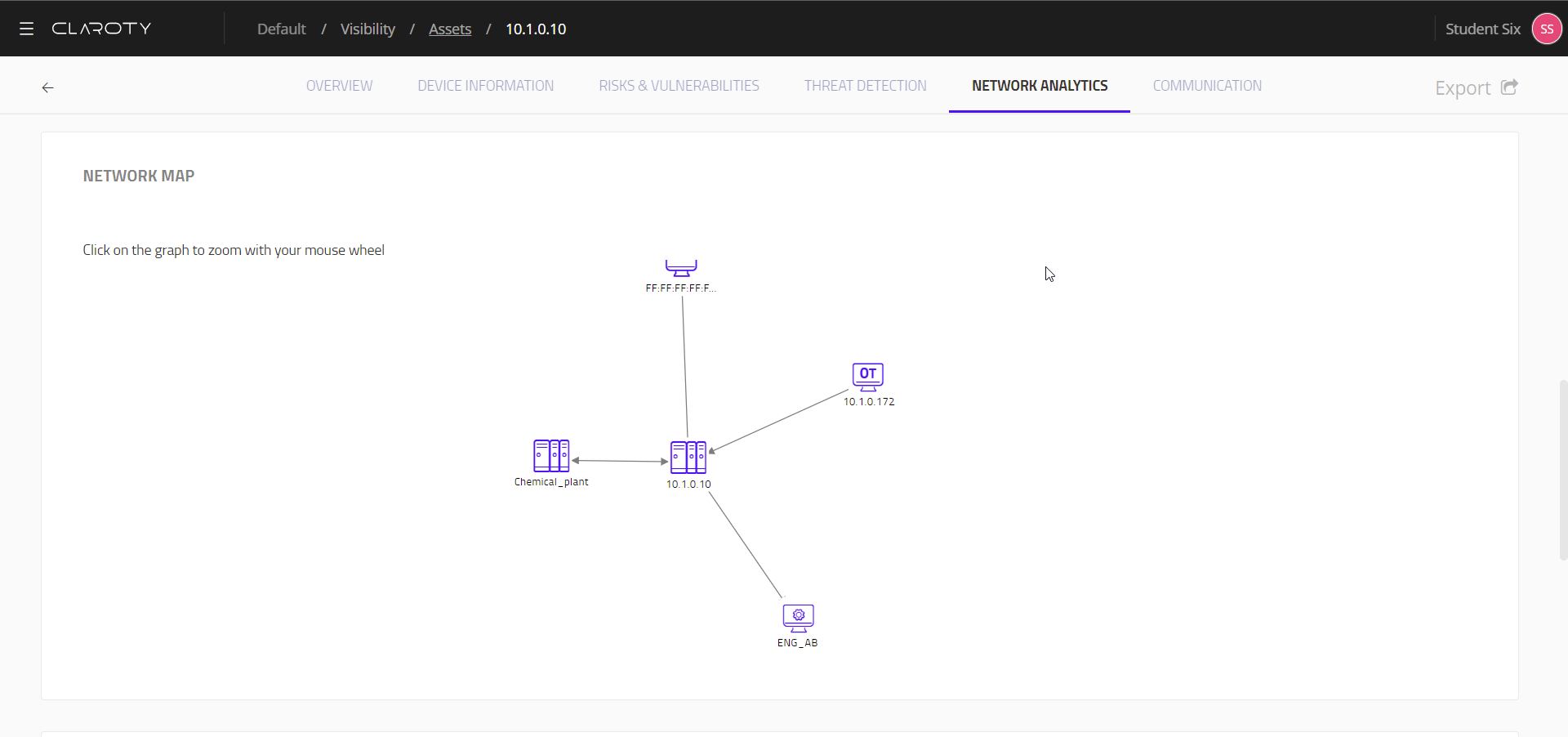


1. Pentru a vedea detalii🡪 click pe o alerta🡪 scroll pentru nivelul de detaliu al alertei

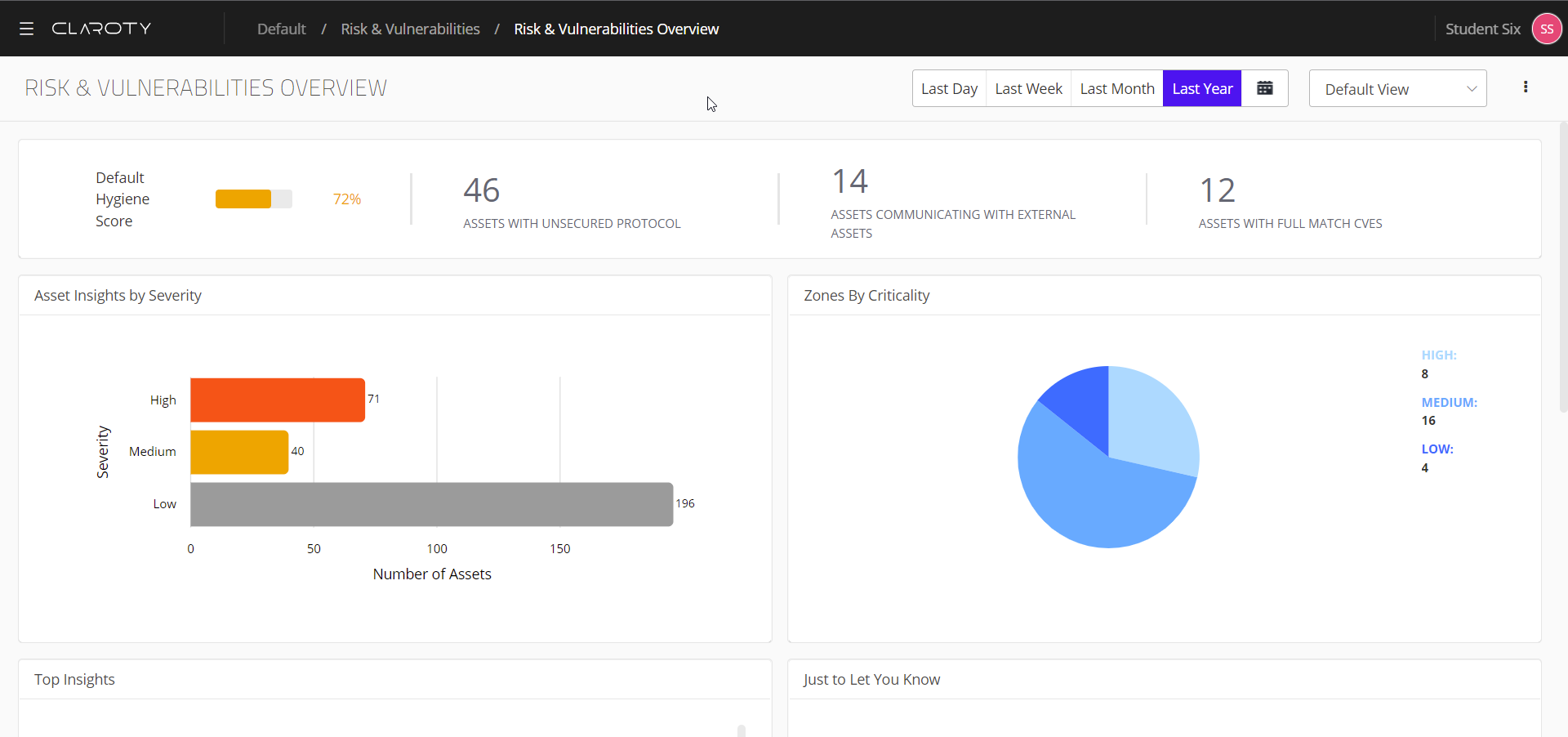


1. Visibility – Assets 🡪

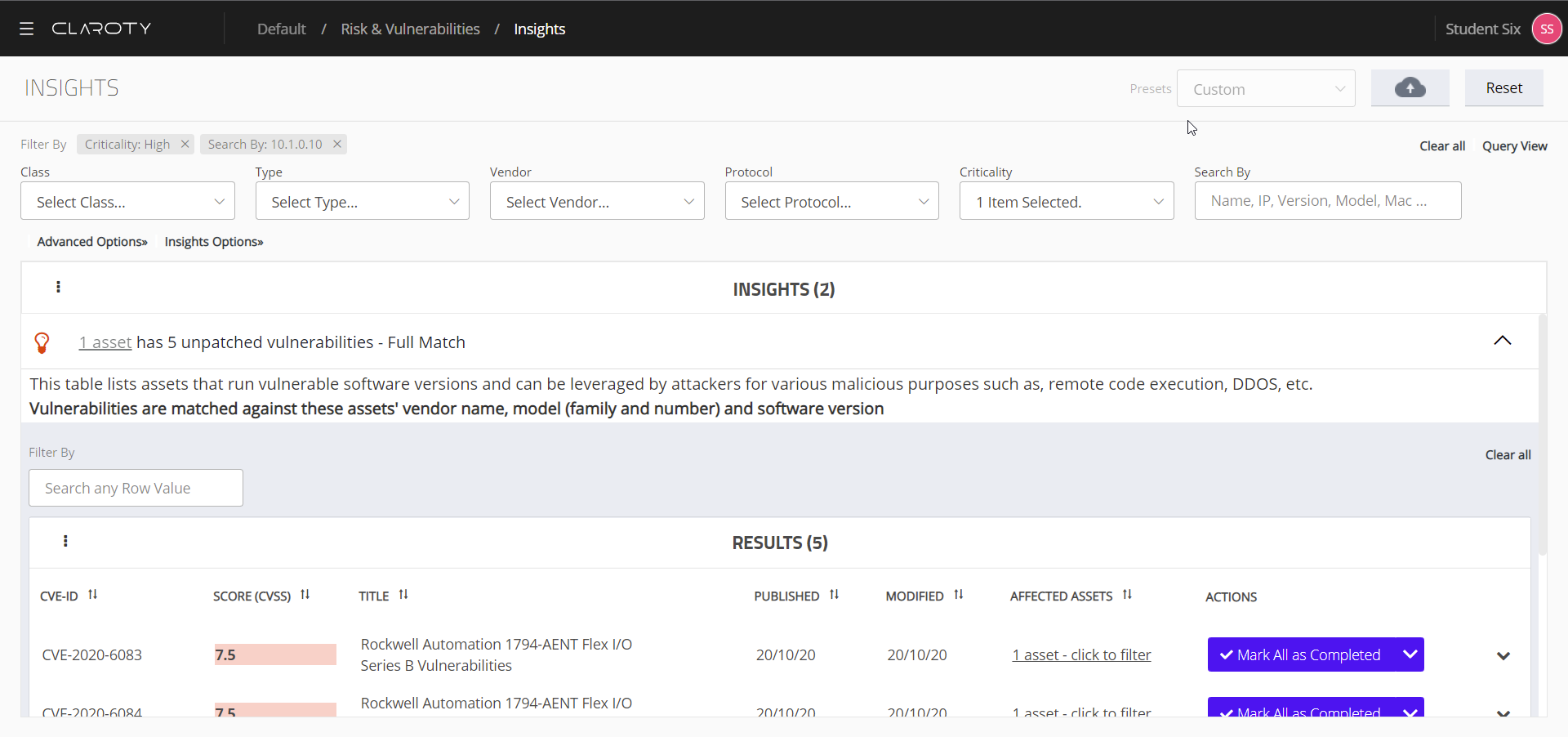
* Topologia pe straturi,
* Lista de asset-uri,
* Conexiunile de retea



1. La Risk & Vulnetabilities:



Se poate naviga pana la lista echipamentelor care (de exemplu) folosesc protocoale considerate vulnerabile.



1. Realizare🡪 Reports

Graphical user interface, text, application, chat or text message

Description automatically generated

Se obtine automat raportul in PDF:

