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 dual ă 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**

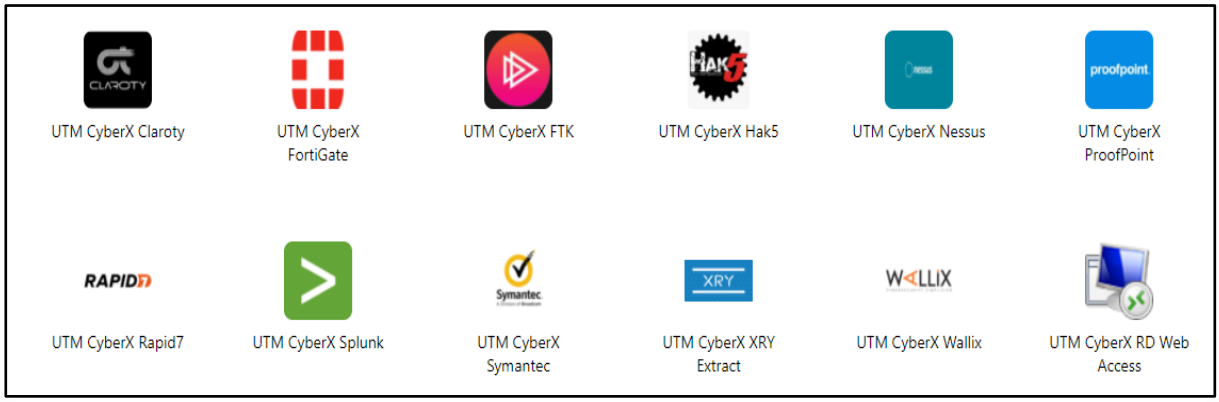
CENTRUL DE EXCELENTA
IN SECURITATE CIBERNETICA IN CLOUD
CyberX

August, 2021

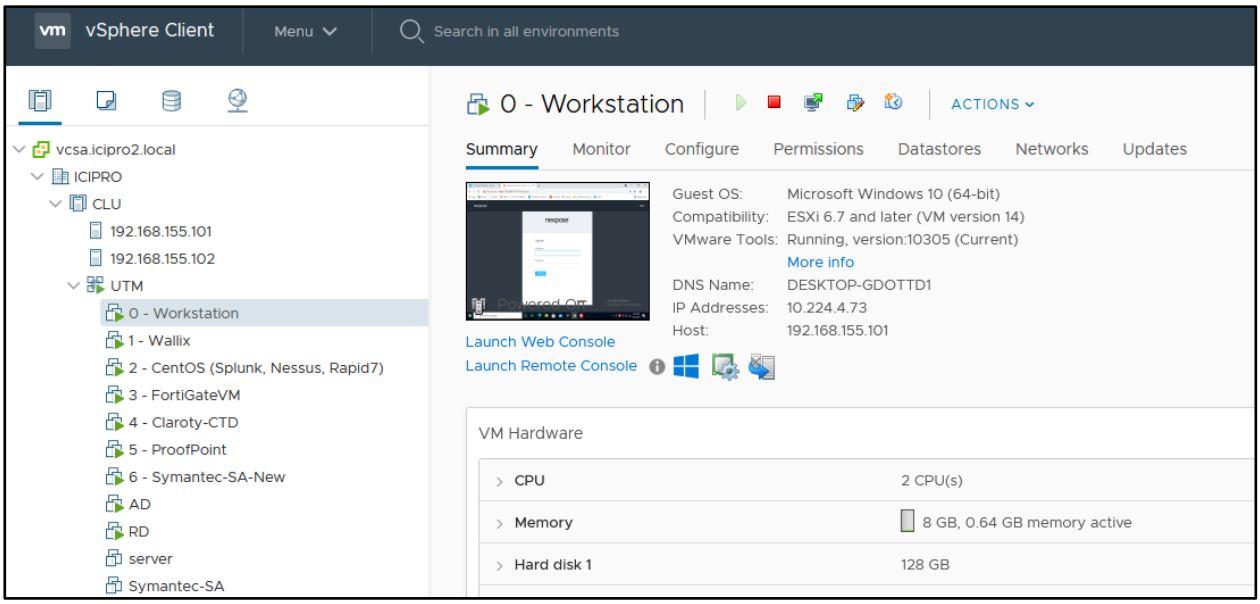
MINISTERUL EDUCAȚIEI ȘI CERCETĂRII
UNIVERSITATEA "TITU MAIORESCU" DIN BUCUREȘTI
Calea Văcărești nr. 187, sector 4, București, cod 040051
tel.: 021 316 16 46, fax: 021 311 22 97, e-mail: rectorat@univ.utm.ro, www.utm.ro

INTERFAȚA LABORATORULUI CYBERX

My Apps (microsoft.com)



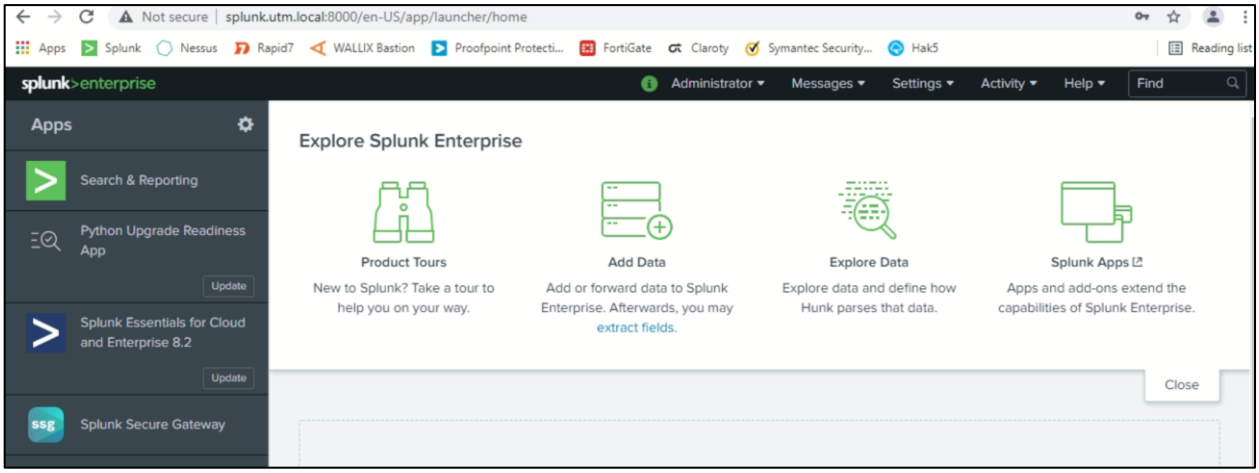
ARHITECTURA DIN CLOUD A CYBERX



DESCRIEREA APLICAȚIILOR SOFTWARE:

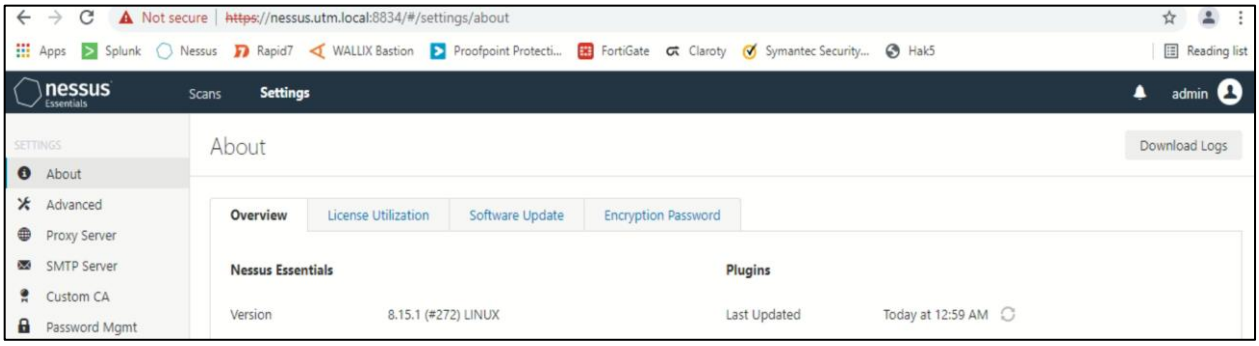
Splunk (Splunk | Turn Data Into Doing):

În cadrul unei organizații, resursele și componentele infrastructurii IT pot fi numeroase, complexe atât în ceea ce privește funcționalitatea lor, cât și al modului lor de operare. *Splunk Enterprise* este un produs software care permite operațiile atât de uzuale și necesare, precum căutarea, analizarea și vizualizarea datele colectate pentru componentele infrastructurii IT, într-o manieră eficientă. Practic, ,Splunk Enterprise colectează informații utile de pe site-uri web, aplicații, senzori, dispozitive etc. permițând o indexare eficientă a fluxului de date și parsându-l într-o serie de evenimente ce pot fi căutate și vizualizate cu ușurință.



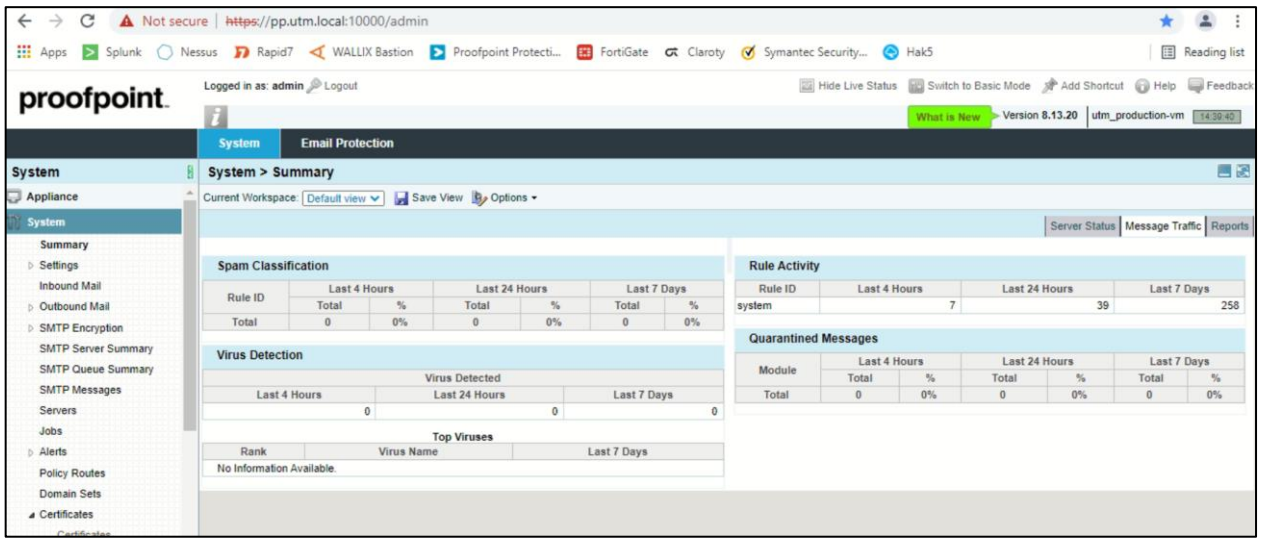
Nessus (https://www.tenable.com/):

În scopul de a asigura securitatea unei platforme, a unui dispozitiv sau a unei aplicații software, o analiză a vulnerabilităților este imperios necesară. *Nessus Professional* reprezintă un instrument puternic ce permite o analiză complexă și eficientă pentru identificarea punctuală a vulnerabilităților, oferind inclusiv soluții de remediere a acestora. În industrie, Nessus oferă cea mai bună precizie în procesul de scanare și identificare a vulnerabilităților, cu o precizie de 0.32 defecte la un milion de scanări, având o largă acoperire prin cele peste 130.000 pulgin - uri oferite, care se actualizează automat în timp real.



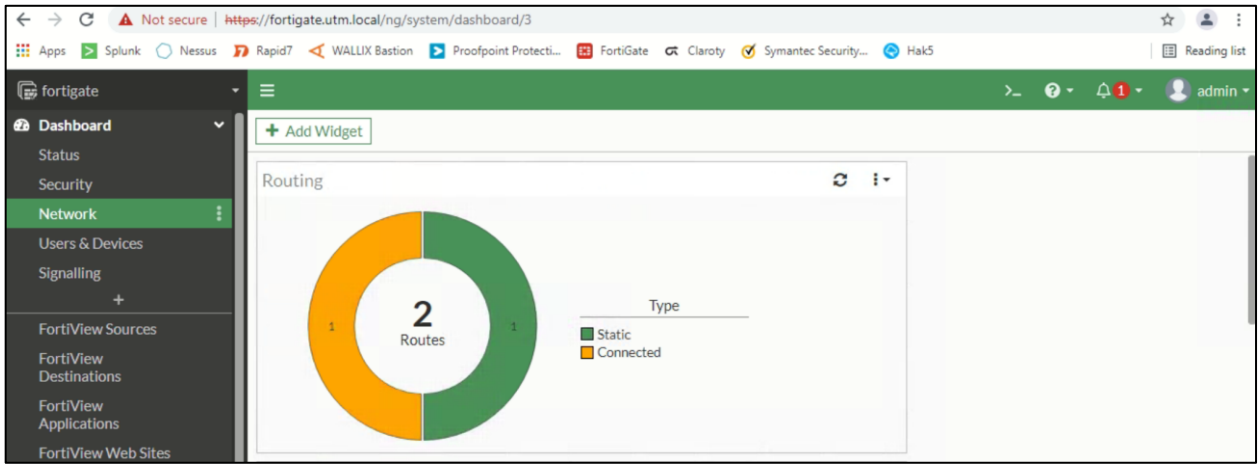
ProofPoint (https://www.proofpoint.com/):

Soluția *Proofpoint* oferă un grad înalt de securitate împotriva amenințărilor malware și non-malware, utilizând un mecanism elaborat și eficient de filtrare în scopul de a controla SPAM-ul. Astfel, oferă o protecție ridicată împotriva atacurilor vizate, detectând și blocând amenințările avansate, inclusiv pe cele de tip ransomware. În scopul de a clasifica cu precizie e-mailuri despre impostori, phishing, malware, spam etc, tehnologia ProofPoint conține instrumente avansate de învățare automată (machine learning).



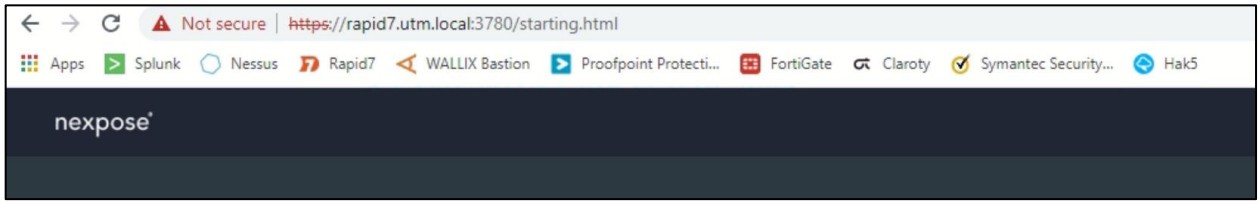
FortiGate VM (https://www.fortinet.com/):

Dispozitivele virtuale FortiGate oferă toate serviciile de securitate și de rețea comune dispozitivelor FortiGate tradiționale bazate pe hardware. Odată cu adăugarea de dispozitive virtuale, se poate implementa o combinație de hardware și dispozitive virtuale, care funcționează împreună și care sunt gestionate de la o platformă comună de management centralizat. Solutia propusă *Fortigate VM FG-VM01* este una integrată de protectie în rețea cu capabilități de rutare, precum și capabilități avansate de securitate precum scanare antivirus, scanare antispam, permitâmd un control avansat la nivel de aplicatie, prevenirea intruziunilor, filtrarea WEB etc. Componentele inteligente IA utilizate oferă soluții avansate de protecție, detecție, precum și de atenuare a atacurilor avansate în doar câteva minute.



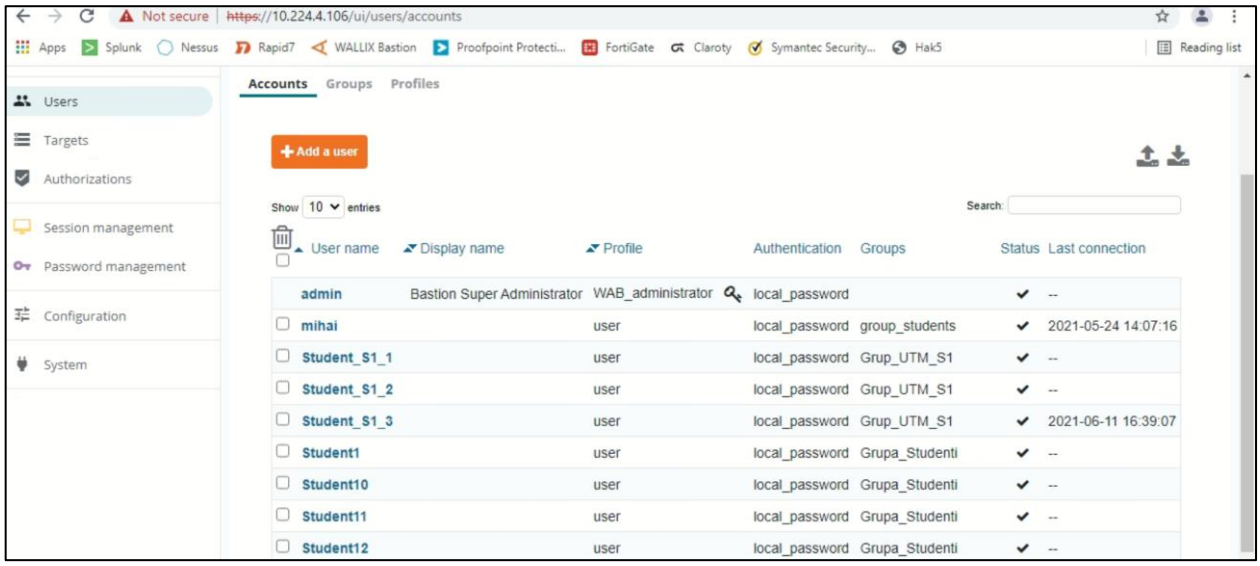
Rapid7 ([Cybersecurity & Compliance Solutions & Services | Rapid7](https://www.rapid7.com/) **):**

Rapid7 Nexpose oferă un sistem de scanare expert bazat pe motoare de inteligente pentru colectarea de informații care emulează tehnici utilizate de hackerii umani în scopul de a definii diferite scenarii de atac. Pe baza informațiilor extrase și analizate din exploatările anterioare soluția identifica vulnerabilități suplimentare, realizând și o evaluare a riscurilor mai completă.



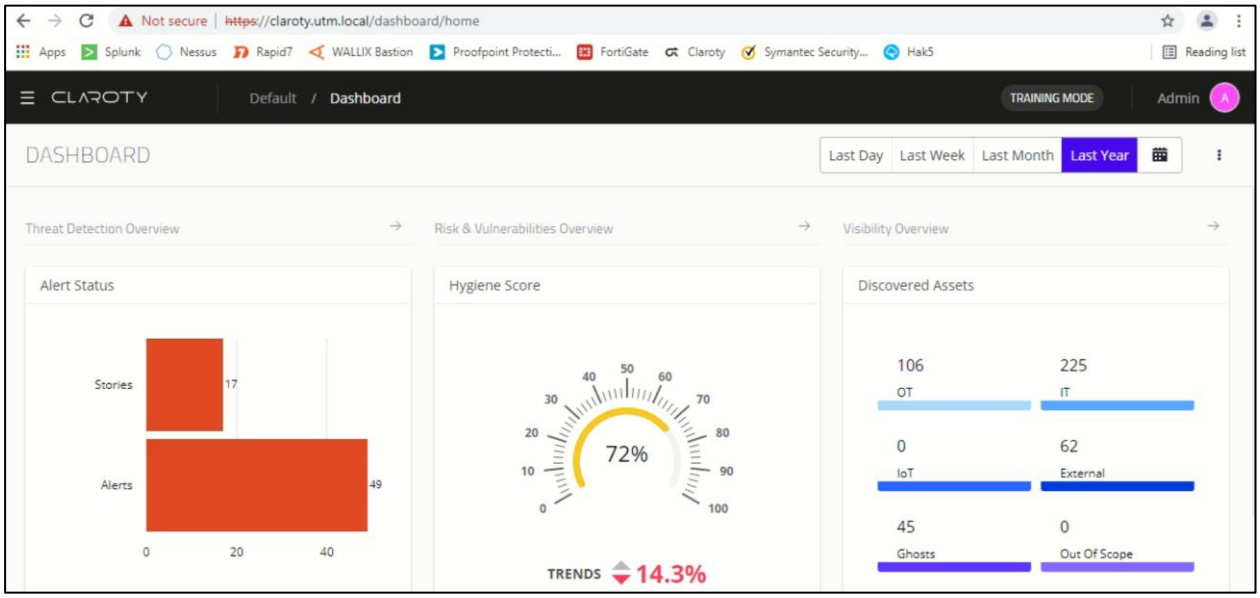
Wallix Bastion (https://www.wallix.com):

Un punct stringent pentru securitatea unei organizații îl reprezintă managementului accesului la resursele sale. WALLIX este o soluție eficientă care protejează identitățile și accesul la infrastructura IT, la aplicații și date, fiind specializat în gestionarea accesului privilegiat în conforrmitate cu cele mai recente standarde de securitate IT. Astfel, soluțiile WALLIX oferă un grad înalt de protecție împotriva atacurilor cibernetice, a furtului de date, fiind pactic un scut puternic pentru tentative de a obține malițios acreditări sau privilegii asupra activelor sensibile ale unei organizații. Soluția Bastion asigură, de asemenea, trasabilitatea sesiunilor administratorilor, oferind posibilitatea de a revizui sesiuni privilegiate în scopuri de audit, depanare sau identificarea cauzelor evenimentelor rău intenționate, având un sistem de alertă în timp real pentru a semnala utilizatorii care încalcă politica de securitate corporativă.



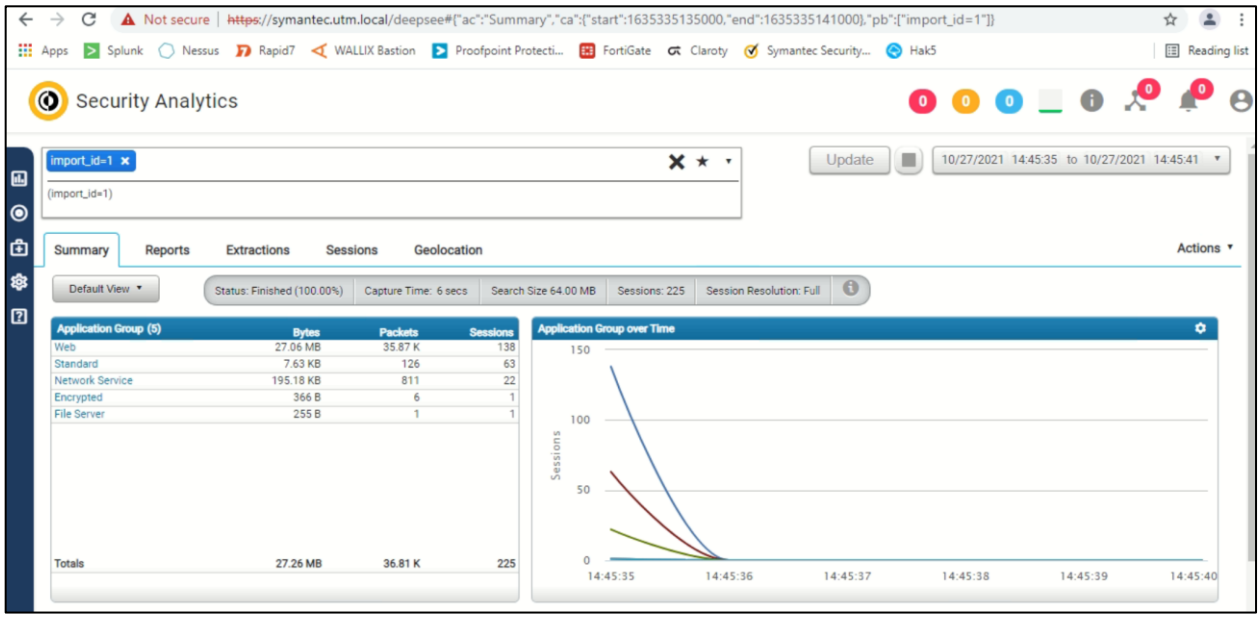
Claroty (Claroty: The Industrial Cybersecurity Company):

Platforma *Claroty* este o soluție completă de securitate OT care cuprinde sistemele Claroty de detectare continuă a amenințărilor (CTD), Enterprise Management Console (EMC) și sisteme de acces securizat la distanță (SRA). Această soluție unică, oferă cea mai extinsă gamă de controale de securitate a tehnologiei operaționale (OT) din industrie în patru domenii: vizibilitate, detectarea amenințărilor, managementul vulnerabilităților de triaj și atenuare. Platforma Claroty este, de asemenea, singura soluție de acest fel din industrie care oferă capabilități complet integrate de gestionare a incidentelor de la distanță, care acoperă întregul ciclu de viață al incidentului.



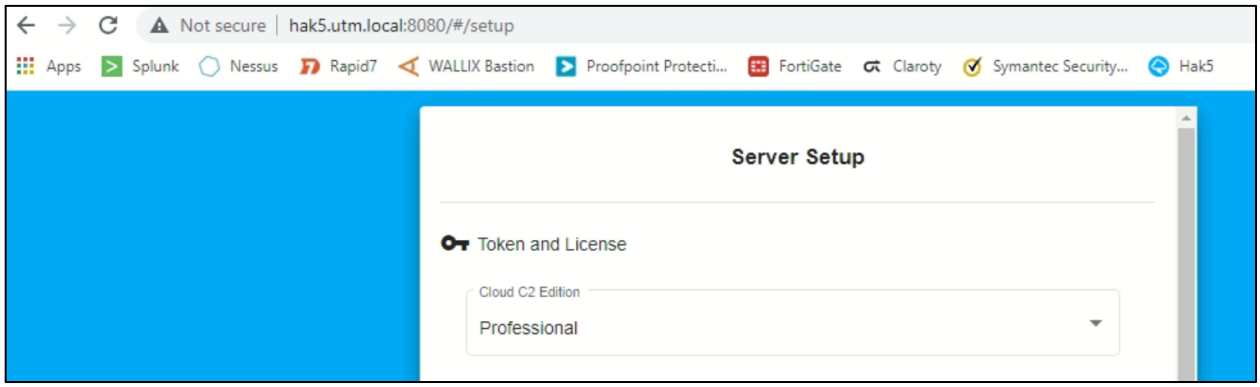
Symantec Security Analytics (Symantec Cyber Security (broadcom.com)):

Soluția permite vizibilitate completă și investigații de tip forensic pentru datele aflate în cloud. Funcționalitățile de bază ale soluției *Symantec Security Analytics* sunt cele de a captura, a inspecta, a indexa, a clasifica și a îmbogăți întregul trafic de rețea (inclusiv pachetele complete) în timp real. în scopul de a obține date ce sunt stocate într-un sistem de fișiere optimizat pentru analiză rapidă, recuperare instantanee și reconstrucție completă, sprijinin astfel toate activitățile de răspuns la incident și de remediere.



Hak5 (Hacking Gear & Media | Hak5 Official Site):

Sunt unele dintre cele mai recunoscute dispozitive în testele de penetrare – de la intruziunea WiFi la implanturi de rețea și atacuri USB. Soluția HAK5 C2 ofera o vizualizare completă a peisajului Wi-Fi, oferind o monitorizare pasivă, continua și în timp real. Conține platforme extensibile pentru teste de penetrare folosind automatizarea USB, acces fizic, acces remote Ethernet și tipologii “man in the middle” .



Forensic Toolkit® (FTK®) (Forensic Toolkit (FTK) version 7.1.0 | AccessData):

AccessData® Forensic Toolkit® (FTK®) vă permite să efectuați examinări criminalistice amănunțite pe calculator. Acesta include o funcționalitate puternică de filtrare și căutare a fișierelor și acces la sistemele la distanță din rețea.
Instrumentele software de investigare criminalistică AccessData ajută funcționarii de aplicare a legii, profesioniștii din domeniul securității corporative șiIT să acceseze și să evalueze valoarea probatorie a fișierelor, folderelor și a computerelor.
AccessData Imager este un instrument de achiziție software. Poate previzualiza rapid dovezile. În cazul în care dovezile justifică investigații suplimentare, se poate crea o imagine de disc criminalistică a unității sau a sursei de probe. Acesta face un duplicat bit-cu-bit , si redă o imagine de disc identică în orice mod cu originalul.
Puteți procesa dovezi statice și puteți obține date în direct de la mașinile de rețea locale pentru procesare. De asemenea, puteți vizualiza și previzualiza dovezi pe unități la distanță, inclusiv CD-uri și DVD-uri.

XRY ([XRY - Extract - MSAB](#)):

XRY este o aplicație software concepută pentru a rula pe sistemul de operare Windows care vă permite să efectuați o extragere criminalistică sigură a datelor dintr-o mare varietate de dispozitive mobile. Extragerea datelor de pe telefoanele mobile este o abilitate specializată și nu același lucru cu recuperarea datelor de la calculatoare tradiționale. Majoritatea dispozitivelor mobile nu partajează aceleași sisteme de operare și sunt proprietare de dispozitive încorporate care au configurații unice. XRY a fost proiectat și dezvoltat pentru a face procesul ușor pentru dvs., cu suport pentru mii de diferite dispozitive mobile și versiuni de aplicații pentru smartphone. Furnizăm o soluție totală pentru a vă ajuta să vă asigurați datele de care aveți nevoie. Software-ul nostru intuitiv vă ghidează prin procesul pas cu pas pentru a-l face ca ușor posibil.