ATLAS FEDECS

Platformă cyber range distribuită

Securitatea cibernetică reprezintă o provocare ce necesită eforturi ridicate pentru pregătirea specialiștilor și dezvoltarea de mecanisme de protecție adecvate pentru a face față la atacuri din ce în ce mai complexe. Platformele de tip cyber range permit organizațiilor să creeze medii izolate în care să emuleze infrastructuri informatice și de comunicații reale pentru instruirea specialiștilor, testarea eficienței mecanismelor de protecție existente sau dezvoltarea unor noi soluții de securitate.

ATLAS FEDECS

FEDECS este un cyber range versatil, realizat în cadrul proiectul ATLAS și implementat la nivelul universităților partenere în proiect. Interconectarea acestor platforme permite universităților să partajeze resursele, să deruleze în comun exerciții de apărare cibernetică și să colaboreze în proiectele de cercetare. FEDECS are la bază tehnologii moderne pentru virtualizare, automatizare, managementul configurațiilor și orchestrare ce asigură scalabilitate și obținerea unor performanțe ridicate. Arhitectura FEDECS este una flexibilă, platforma putând fi ușor reconfigurată sau modificată pentru a adăuga funcționalități noi. Avantajele soluției propuse sunt multiple, platforma FEDECS fiind un instrument extrem de util pentru orice universitate sau companie.

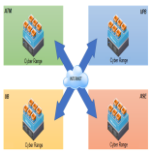
De ce ATLAS FEDECS?

Mediu izolat pentru instruire și experimentare în domeniul securității cibernetice

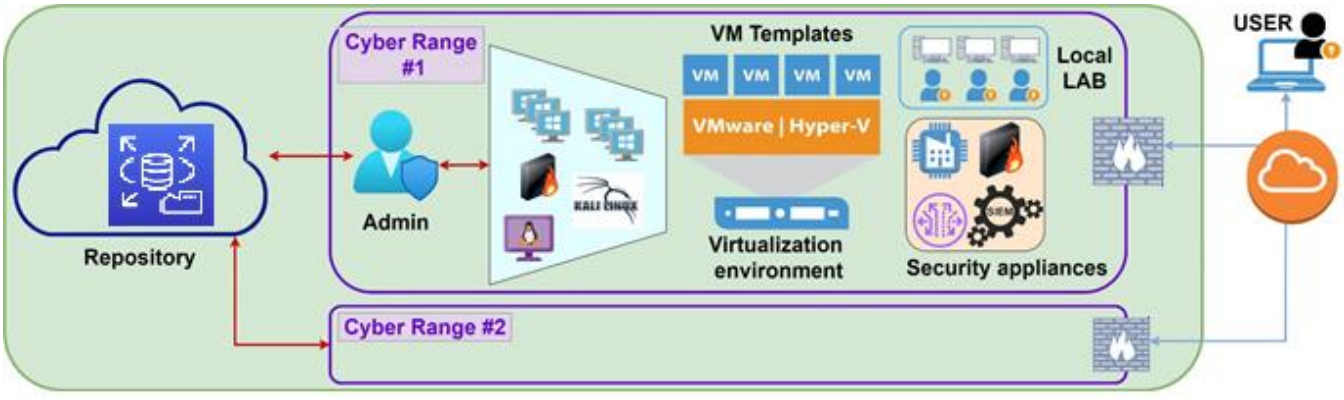
Training realist prin emularea de echipamente, rețele, servicii și aplicații informatice

Arhitectură versatilă ce poate fi folosită pentru derularea de laboratoare, exerciții, și competiții

Partajare de resurse, scenarii pentru exerciții și competențe în domeniul securității cibernetice.



Federalizare prin interconectarea mai multor platforme cyber range-uri de același tip.



ATLAS FEDECS

Mediu de instruire ce reflectă condițiile reale

Majoritatea profesioniștilor în securitate cibernetică nu experimentează niciodată un atac cibernetic din viața reală, până când nu se produce unul. Pe lângă pregătirea teoretică, experiența practică este esențială în contracararea atacurilor cibernetice. FEDECS permite organizațiilor să combine modul tradițional de învățare cu formarea practică pentru a îmbunătăți abilitățile și competențele specialiștilor. FEDECS poate fi folosit pentru a crea rapid medii de laborator, care imită rețelele și sisteme informatice organizaționale, pentru a simula diferite tipuri de atacuri, oferind astfel o experiență cât mai apropiată de realitate pentru cursanți.

Economisirea timpului și reducerea costurilor

Construirea și implementarea manuală a mediilor de antrenament pentru exercițiile cibernetice necesită foarte mult timp, în special pentru scenarii complexe și pentru un număr mare de participanți la exerciții. De obicei, exercițiile cibernetice durează câteva ore sau zile, însă faza de pregătire durează câteva săptămâni sau luni din cauza efortului necesar pentru a defini scenariile, pentru a configura și instala mașinile virtuale și pentru a replica resursele necesare pentru fiecare participant sau echipă în parte. Prin intermediul unor scripturi special concepute, FEDECS automatizează etapele de configurare și replicare ale mașinilor virtuale, reducând timpul de deployment la nivelul minutelor. În plus, odată create imaginile pentru mașinile virtuale, acestea sunt stocate într-un repository local putând fi refolosite pentru a repetarea exerciíului sau implementarea altor tipuri de scenarii.

Partajarea scenariilor

Dezvoltarea scenariilor pentru exerciții necesită timp și presupune un nivel ridicat de expertiză în domenii diferite. Partajarea între organizații a acestor scenarii economisește timp și efort. Pentru a rezolva această problemă, în cadrul proiectului ATLAS a fost creat un repository comun în care sunt publicate scenarii dezvoltate de universitățile partenere. În acest mod, un exercițiu desfășurat în cadrul unei universități poate fi reluat în altă universitate iar scenariile pot fi reutilizate ori de câte ori este nevoie.

Partajarea resurselor

Organizarea de exerciții complexe necesită, de multe ori, resurse specializate pentru simularea atacurilor, a traficului și serviciilor de rețea, a dispozitivelor IoT sau a sistemelor de control industrial. Aceste resurse pot fi costisitoare și greu de achiziționat. Prin urmare, este mult mai eficient ca resurse existente să fie partajate și folosite în comun. Interconectarea prin VPN a platformelor cyber range FEDECS rezolvă această problemă și, în plus, permite crearea de scenarii distribuite în care fiecare entitate poate juca un anumit rol (de exemplu, red team vs. blue team).

Cercetare și experimentare

Pentru a face față la atacuri cibernetice din ce în ce mai evoluate, cercetătorii trebuie să dezvolte noi tehnologii și produse de securitate cibernetică. Înainte ca aceste soluții să poată fi implementate în rețele organizaționale, trebuie testate și validate. FEDECS permite crearea de bancuri de testare pentru a evalua, valida și compara performanțele diferitelor soluții de securitate cibernetică. De asemenea, FEDECS poate fi utilizat de cercetători pentru a studia noi tehnici de atac sau pentru a analiza aplicații malițioase (malware) în medii sigure și izolate.

Despre ATLAS

Proiectul “Hub inovativ pentru tehnologii avansate de securitate cibernetică (ATLAS)” își propune îmbunătățirea performanțelor de cercetare și de colaborare în domeniul securității cibernetice, adresând teme de mare interes: securitatea aplicațiilor și sistemelor de operare, securitatea IoT și cloud.

Proiectul ATLAS este finanțat printr-un grant acordat de Ministerul Cercetării și Inovării din România, CCCDI - UEFISCDI, proiect nr. PN-III-P1-1.2-PCCDI-2017-0272, în cadrul PNCDI III.

