CyberSecurity Ovidius Camp

Aspecte practice privind interceptarea și monitorizarea traficului în Cloud folosind aplicațiile CyberX

Conf. univ. dr. ing. Iustin Priescu
Conf. univ. dr. Daniela Joița
Conf. univ. dr. ing. Mironela Pîrnău

Securitate cibernetică

Complexitatea unui sistem depinde de nivelul de competență al forței de muncă implicată. Firmele care folosesc strategii de securitate cibernetică, programe automatizate pentru analize avansate ale traficului de date, inteligență artificială (AI) și învățare automată, pot face față **eficient** **amenințărilor cibernetice**.

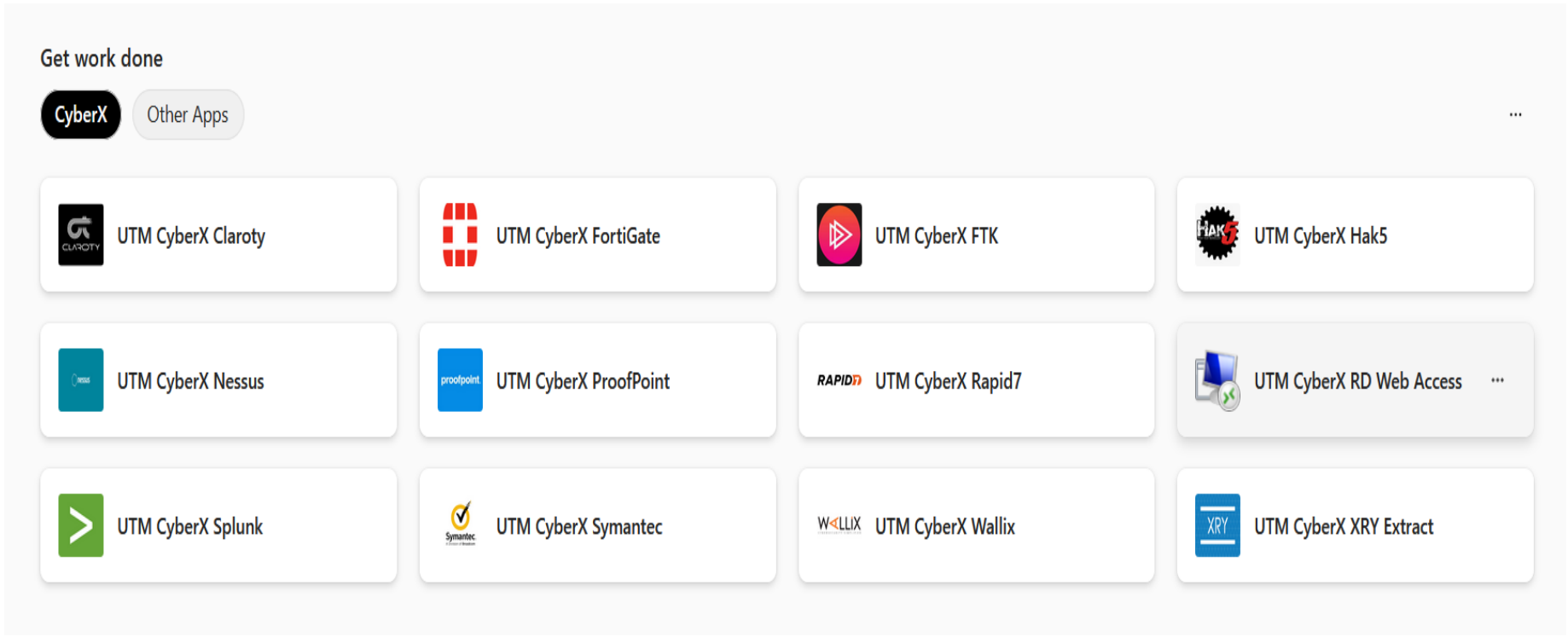
Symantec Security Analytics → efectueaza in timp real o analiză a traficului de rețea și ofera răspuns la incidentele de Securitate care apar in Cloud.

Symantec Security Analytics –permite investigații de tip forensic în timp real pentru datele din cloud cu scopul de a bloca amenintarile de securitate;

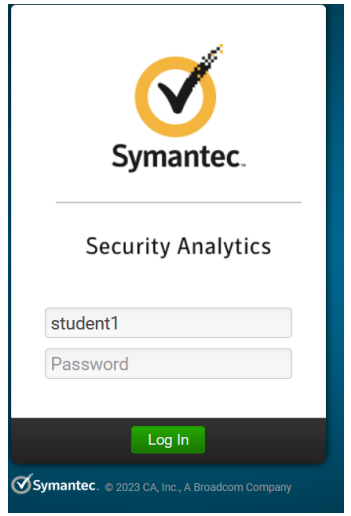
Symantec Security Analytics→ utilizeaza filtre complexe/puternice pentru analiza traficul selectat.

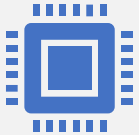
https://www.broadcom.com/info/symantec/security-analytics-key-features

https://techdocs.broadcom.com/us/en/symantec-security-software/web-and-network-security/security-analytics/8-2-6.html



https://www.microsoft365.com/apps?auth=2&home=1





*Pentru analiza traficului de rețea și răspuns la incidentele de securitate pentru sarcinile de lucru din **cloud**, Symantec Security Analytics poate fi implementat în Amazon Web Services, Microsoft Azure și Oracle Cloud;*

Symantec Security Analytics permite efectuarea de investigații amănunțite și căutare proactivă a amenințărilor pentru a descoperi sursa și amploarea unei amenințări sau a unui atac și pentru a furniza dovezi clare, indiferent dacă amenințarea vizează rețeaua dvs. locală sau volumul de lucru din cloud.

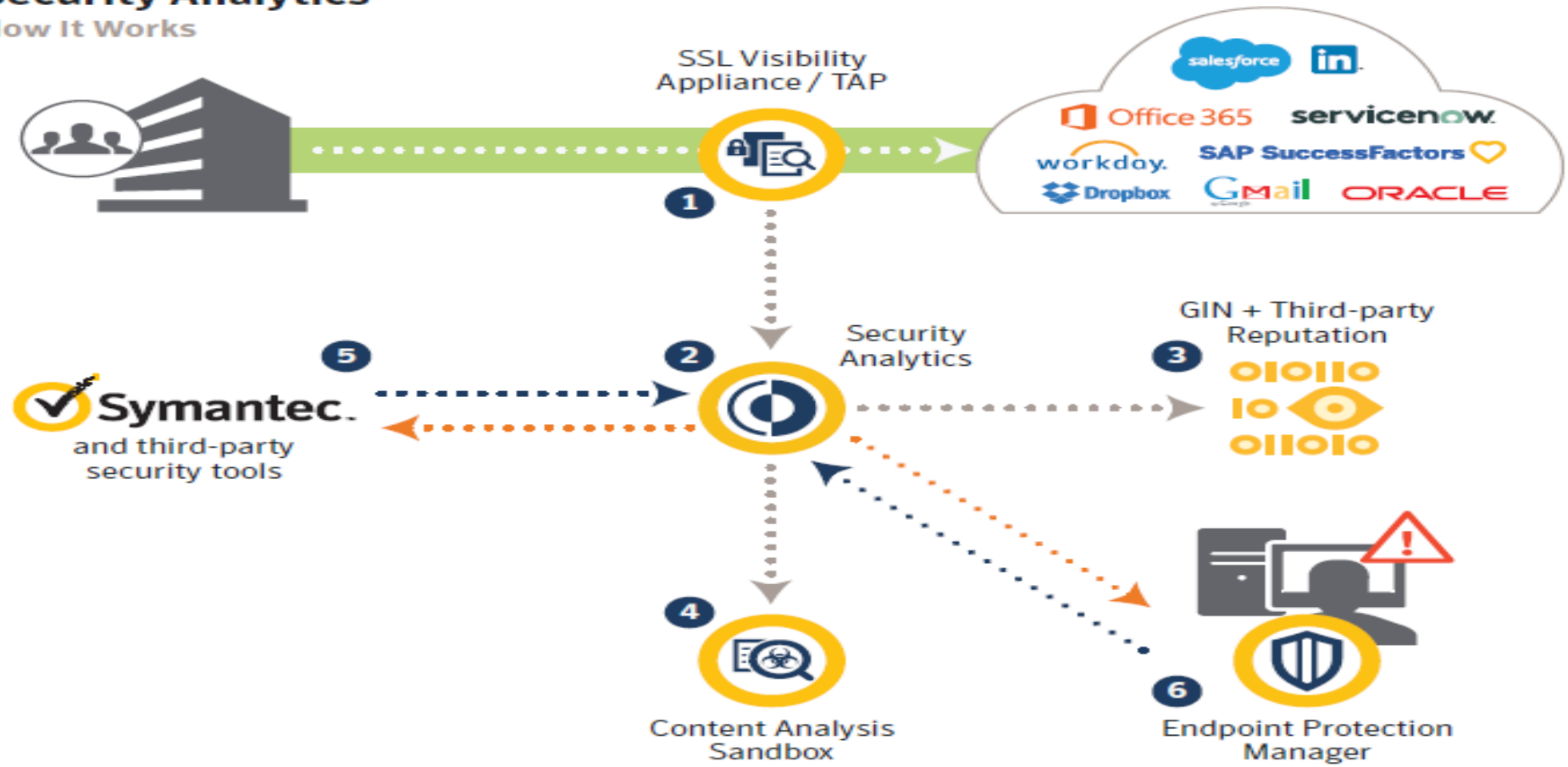
Intelligent Capture

- Tot traficul capturat este trimis prin conducta de analiză, cu generarea de metadate, extragerea artefactelor și detectarea anomaliilor, fiind păstrate numai pachetele considerate necesare pentru stocarea pe termen lung.
- In Symantec Security Analitics se pot crea **reguli** pentru capturarea traficului dar si pentru a stabili care pachete din traficul analizat se stocheaza.

- https://knowledge.broadcom.com/external/article/161687/what-is-a-threat-artifact.html - exemple artefacte de amenintare

Security Analytics

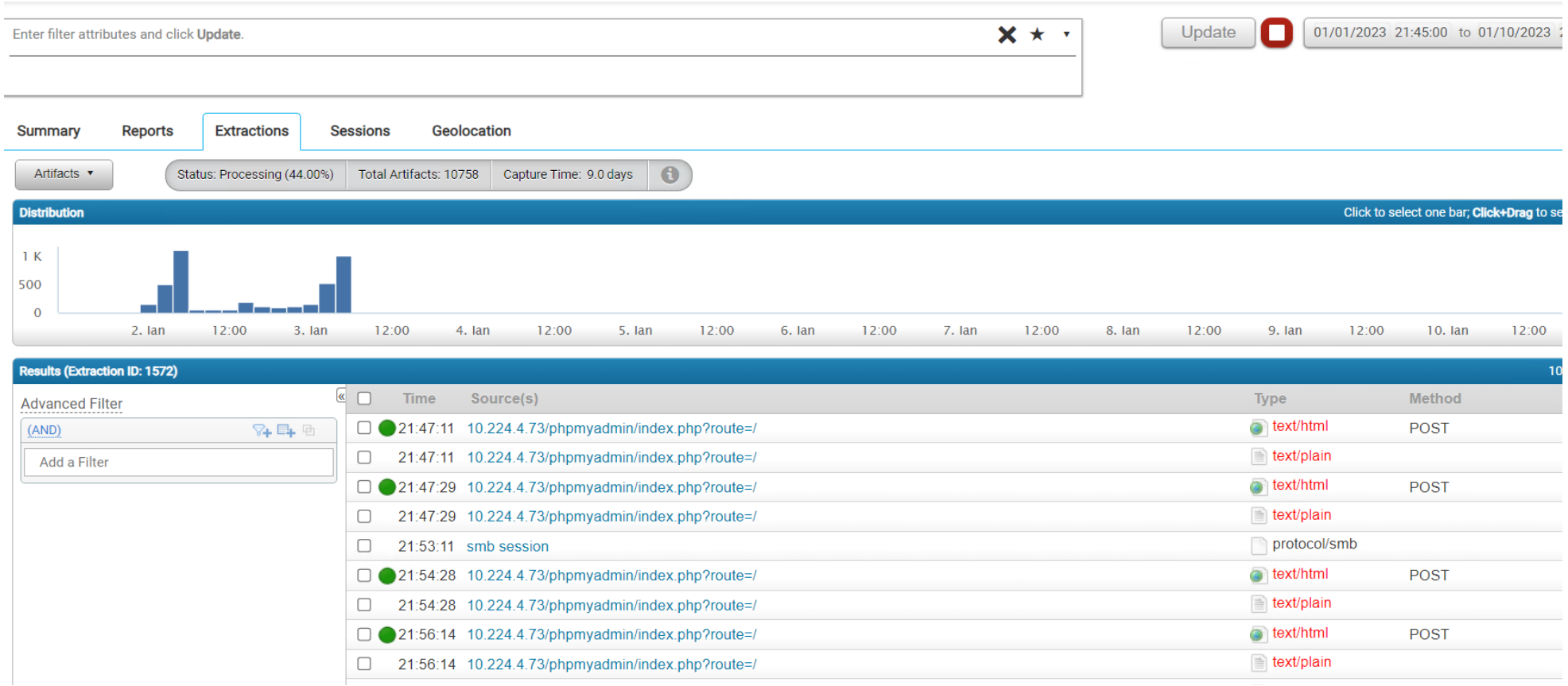
How It Works



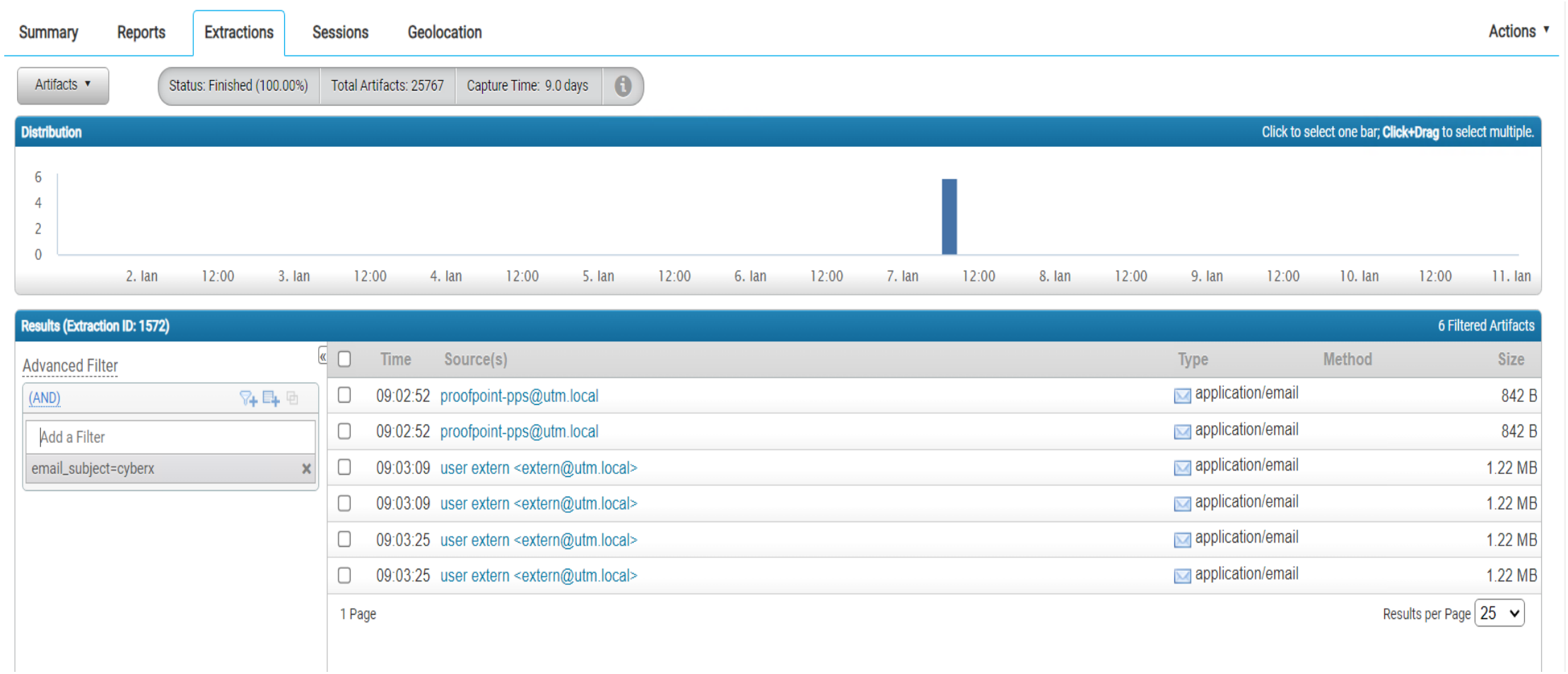
1. Security Analytics sits passively off the network (SSLV or TAP)
2. Captures all network traffic (packet header/payload)
3. Taps GIN and outside threat intelligence to enrich packet data
4. Unknown files sent to Content Analysis/3rd party to Sandbox
5. Alerts from SA or other tools may trigger an investigation
6. Incident response team finds source/scope of attack, resolves

Studiu de caz

Să se analizeze traficul din perioada 01-10 ianuarie 2023



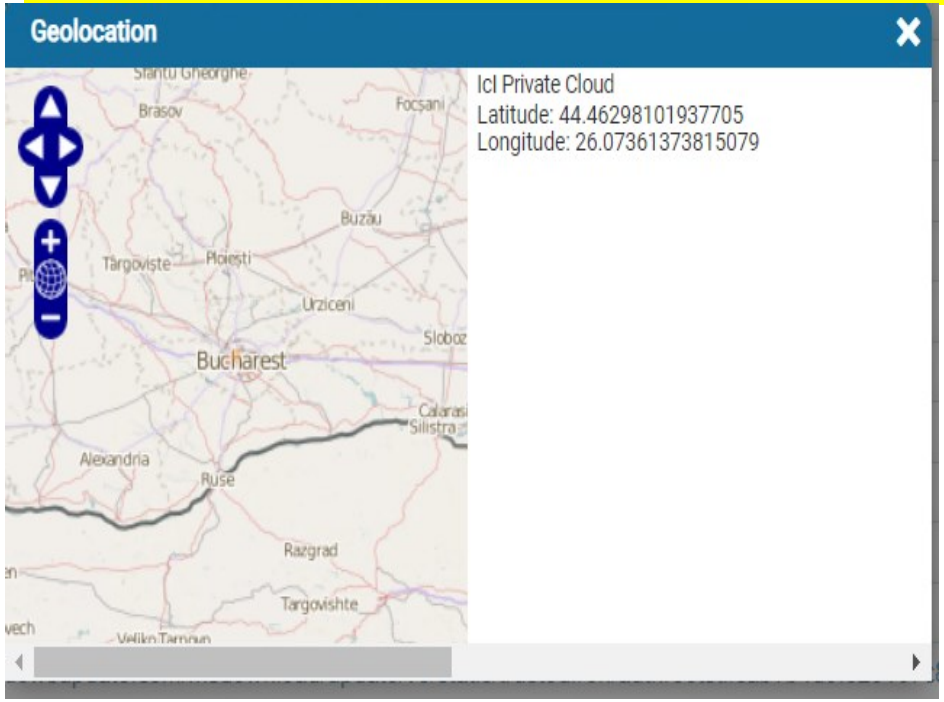
Să se filtreze traficul pentru email-urile cu subiect cyberx.



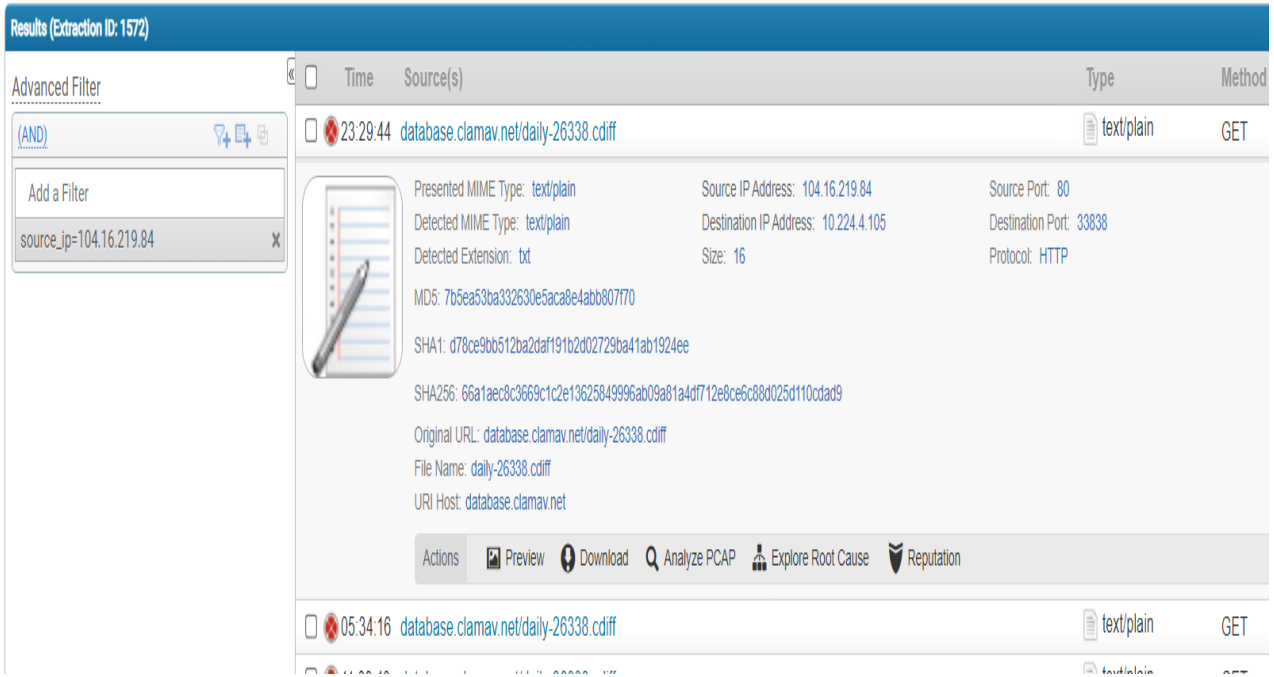
Să se identifice IP-sursă și destinație

Dacă s-au identificat fișiere **exe** să se analizeze reputația acestora cât și **IP sursă/destinație**

Să se identifice pentru un IP→ locația



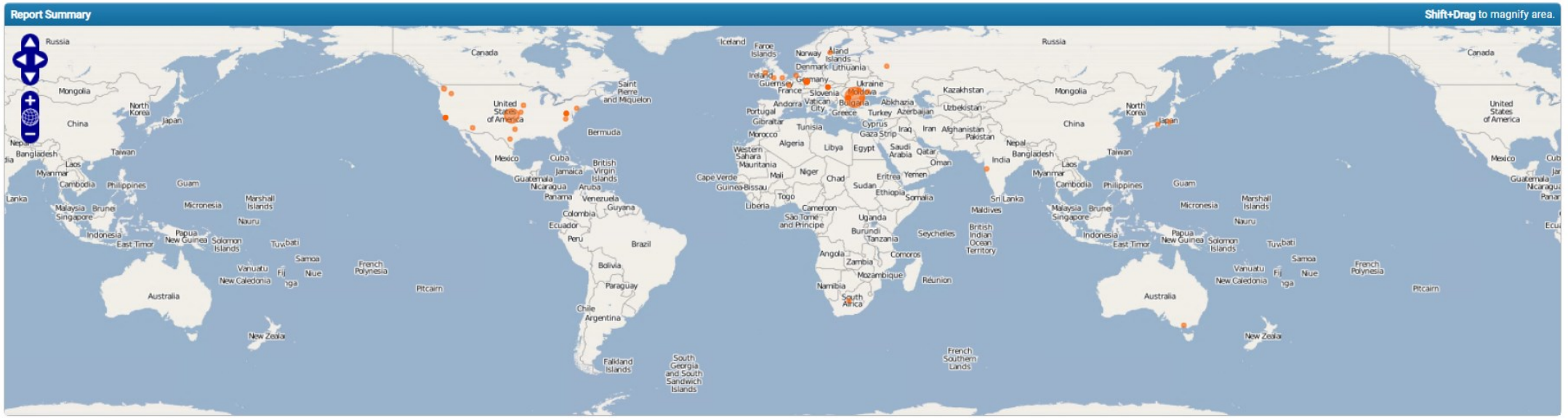
Să se filtreze traficul după IP-ul sursa:104.16.219.84 și să se identifice locația



Să se vizualizeze harta ip-urilor din comunicația analizată

Summary | Reports | Extractions | Sessions | Geolocation | Actions

World | Status: Finished (100.00%) | Capture Time: 9.0 days | Sessions: 212.61 K | Session Resolution: Full



Results

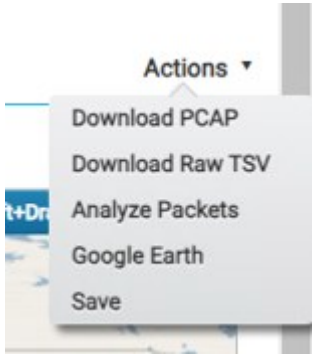
Advanced Filter

(AND)

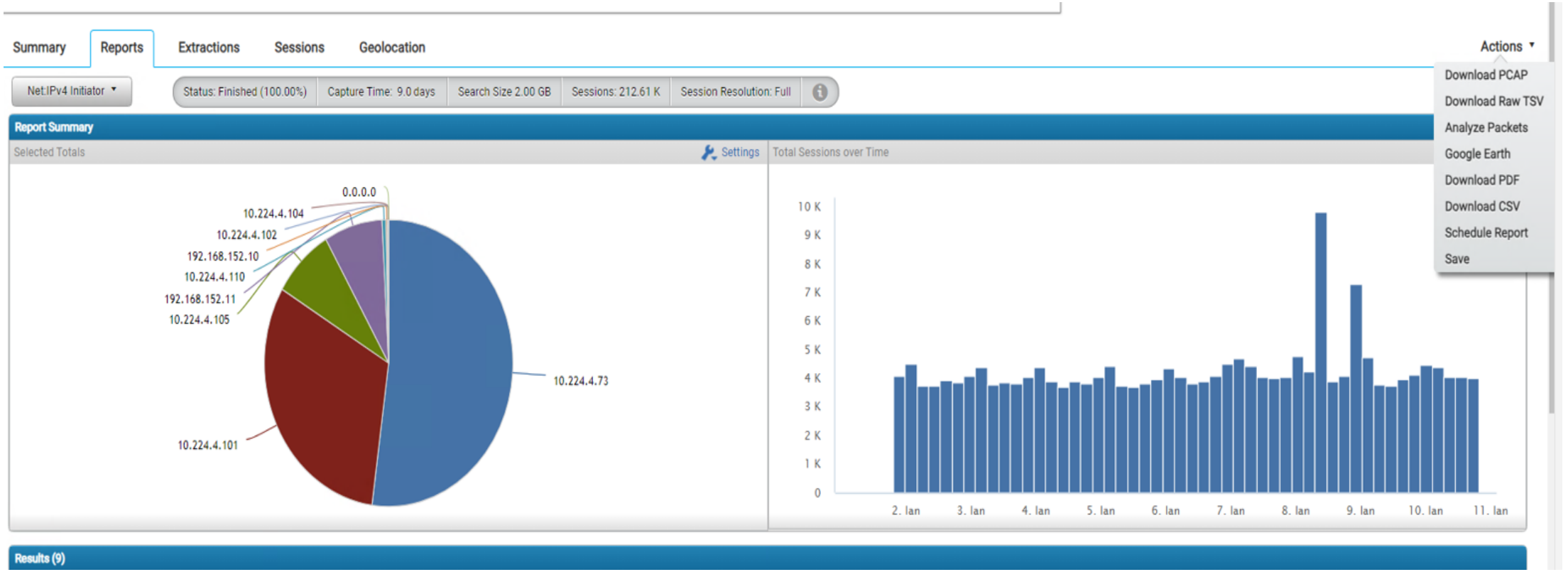
Add a Filter

Location	# IP Addresses		Bytes	
Icl Private Cloud	8	1.51%	1.75 GB	51.37%
United States	93	17.55%	1.17 GB	34.27%
Frankfurt am Main, Hesse, Germany	3	0.57%	124.25 MB	3.55%
Washington, United States	11	2.08%	65.15 MB	1.86%
Romania	14	2.64%	17.01 MB	0.49%

Să se exporte traficul analizat



Să se obțină un raport de tip IPv4 Inițiator și apoi să se exporte fisierul pdf



Tema

Folosind Pcap-ul → malware1.pcap

- Filtrați artefactele după extensia fișierelor cu valoarea exe / png;
- Analizați fișierele filtrate cu extensiile exe/ png inclusiv reputatia acestora tinând cont și de informațiile de la https://docs.clamav.net/ ;
- Realizati un raport după “Geo Country Responser”.

Folosind Pcap-ul→ Set2 să se analizeze acesta, folosind succesiv diverse filtre (http_method!~get; business consulting services; keyword="business consulting services"; keyword=mezzo_web_scroll_bottom.js).

https://www.cvedetails.com/cve/CVE-2016-9092/
https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=symantec
https://cve.report/vendor/symantec

Nexpose

https://docs.rapid7.com/

Rapid7 oferă două produse de bază pentru gestionarea vulnerabilităților:

- InsightVM (este o componenta complexă care se bazeaza pe Cloud cu următoarele facilități: Dashboards dinamic cu actualizări în timp real; sarcini de remediere în sistemele IT etc);
- Nexpose (este o soluție locală pentru companii de orice dimensiune).

https://www.rapid7.com/products/nexpose/download/

Scanarea și analiza vulnerabilităților este procesul care detectează și evaluează vulnerabilitățile care există într-o infrastructură de rețea.

O vulnerabilitate este o caracteristică a unui activ pe care un atacator o poate exploata pentru a obține acces neautorizat la date sensibile.

Pentru a preveni breșele de securitate, este important să identificați și să remediați găurile de securitate și vulnerabilitățile care pot expune un activ la un atac.

Cu Nexpose se poate scana o rețea pentru vulnerabilități.

- Nexpose identifică serviciile active, porturile deschise și aplicațiile care rulează pe fiecare computer și încearcă să găsească vulnerabilități care pot exista pe baza atributelor serviciilor și aplicațiilor cunoscute.
- Nexpose dezvăluie rezultatele într-un raport de scanare, care vă ajută să prioritizați vulnerabilitățile pe baza factorului de risc și să determinați cea mai eficientă soluție de implementat.

Nessus vs Nexpose?

Nexpose și Nessus Professional sunt ambele instrumente excelente și pot fi folosite pentru a scana o infrastructura IT.

- https://owasp.org/www-community/Vulnerability_Scanning_Tools
- https://allabouttesting.org/nexpose-vs-nessus-which-one-is-better/
- https://docs.rapid7.com/metasploit/vulnerability-scanning-with-nexpose/
- https://docs.rapid7.com/metasploit/installing-metasploit-pro

What is OWASP?

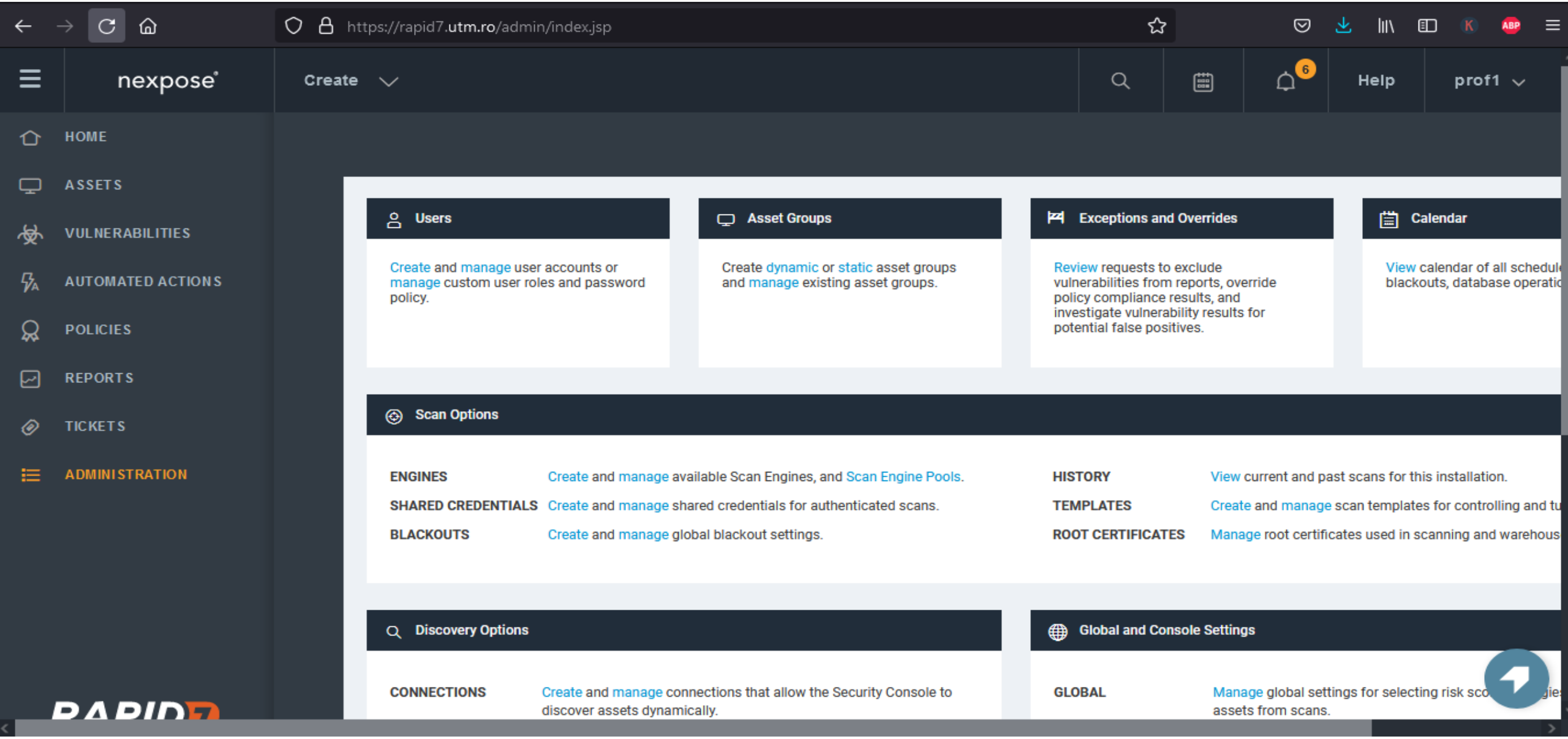
The Open Web Application Security Project (OWASP) is a worldwide nonprofit organization that focuses on improving software security. The main mission of OWASP is to ensure that software security is visible, and to provide insights and tools to help improve application security globally. through the top 10 lists for various categories, so that organizations can use the Top 10 lists to make informed decisions.

https://www.barracuda.com/glossary/owasp

Terminologie Nexpose:

- **Activ** - O gazdă într-o rețea.
- **Site** - Un grup logic de active care are un motor de scanare dedicat. Un site poate rula pe o perioadă lungă de timp și vă poate oferi date istorice, tendințe și este similar cu un proiect din Metasploit.
- **Scanare șablon** - Un șablon care definește nivelul de audit pe care Nexpose îl utilizează pentru a efectua o scanare a vulnerabilităților.

Ciclul de viață al programului de Securitate


https://rapid7.utm.ro/admin/index.jsp
nexpose
Create
6
Help
prof1
HOME
ASSETS
VULNERABILITIES
AUTOMATED ACTIONS
POLICIES
REPORTS
TICKETS
ADMINISTRATION
Users
Create and manage user accounts or manage custom user roles and password policy.
Asset Groups
Create dynamic or static asset groups and manage existing asset groups.
Exceptions and Overrides
Review requests to exclude vulnerabilities from reports, override policy compliance results, and investigate vulnerability results for potential false positives.
Calendar
View calendar of all schedul
blackouts, database operatic
Scan Options
ENGINES
Create and manage available Scan Engines, and Scan Engine Pools.
SHARED CREDENTIALS
Create and manage shared credentials for authenticated scans.
BLACKOUTS
Create and manage global blackout settings.
HISTORY
View current and past scans for this installation.
TEMPLATES
Create and manage scan templates for controlling and tu
ROOT CERTIFICATES
Manage root certificates used in scanning and warehous
Discovery Options
CONNECTIONS
Create and manage connections that allow the Security Console to discover assets dynamically.
Global and Console Settings
GLOBAL
Manage global settings for selecting risk sc
assets from scans.

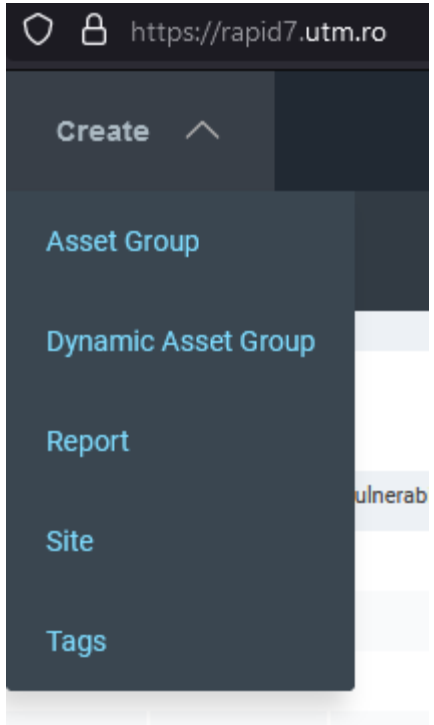
Ce este un site?

- Un site este o colecție de active pentru care se realizeaza o operație de scanare.

- Un site este format din:
  - active țintă (opțional)
  - un șablon de scanare
  - unul sau mai multe motoare de scanare

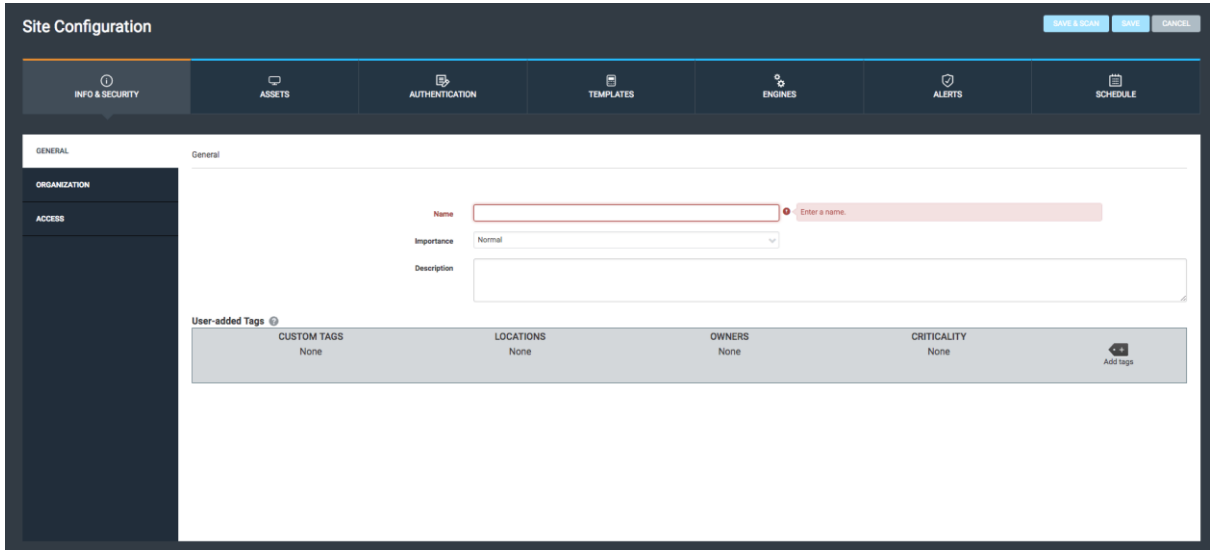
Prin ce diferă site-urile de grupurile de active?

- Grupurile de active oferă diferite modalități prin care membrii organizației pot acorda acces, vizualiza, scana și raporta informații despre active. Aveți posibilitatea să creați grupuri de active care conțin active pe mai multe site-uri.
- **Scenariu pentru creare unui site.**



Create Your First Site

From the **Home** page of your Security Console, click the **Create** dropdown and select **Site**. The Security Console displays the “Site Configuration” screen.



https://docs.rapid7.com/nexpose/create-and-scan-a-site/

- **“Info & Security”**
- On the **General** tab, name and describe your site. While common names include department titles or office locations for the assets being scanned, you can name this site after your target asset or “sample site” for easy reference.
- **“Assets”**
- The **Assets** tab is where you specify which of your assets should be included in the site, and if necessary, which should be excluded as well. You can specify individual assets by their Fully Qualified Domain Name (FQDN) or IP address, but IP address ranges are the most effective method. Site configurations accept a variety of IPv4 and IPv6 range notations, including Classless Inter-Domain Routing (CIDR).

“Authentication”

The **Authentication** tab allows you to configure different sets of credentials depending on the type of asset you target for a scan.

Configure Credentials

Click the **Add Credentials** tab to configure a set of credentials for your site to use:

1. On the **General** sub-tab, name and optionally describe your credentials.

   This name will identify these credentials on the **Manage Authentication** tab when saved.

2. On the **Account** tab, select the authentication service you want to use.

While several options are available here for a variety of scenarios, Rapid7 recommends the following two services as a good starting point for authenticated scans:

- **Microsoft Windows/Samba (SMB/CIFS)** for Windows machines
- **Secure Shell (SSH)** for Linux and Mac machines

You can read more about authentication on the following pages:

- Authentication on Unix and related targets: best practices
- Authentication on Windows: best practices

Complete the username and password fields as required.

Default ports for SSH and SMB/CIFS

By default, Nexpose attempts SSH communication through port 22 and SMB/CIFS communication through port 445.

Click **Test Credentials** when finished.

Credential Test Results Explained

Successful credential tests show a green confirmation message. Failed tests appear in red and may show the following text:

- **Invalid credentials** - Your username and/or password were incorrect.
- **Connection refused** - You specified the wrong port number, the port is not open on the host, or a firewall actively blocked the connection.
- **Host not found** - The IP address or FQDN specified was not found on the network. This means that you entered the wrong address, the host network cannot be reached from the network subnet hosting the console, or the host is not connected.

After you've successfully tested your credentials, click **Create** to save them.

“Templates”

- Sites must be configured to use a specific Scan Template during the scanning process. You can think of the Scan Template as the method by which the Scan Engine probes your assets.
- On the **Select Scan Template** tab, select **Full Audit without Web Spider**.
- Generally considered as the default Scan Template for the Security Console, **Full Audit without Web Spider** has the following traits:
    - Performs only safe checks
    - Looks for network-based vulnerabilities
    - Checks for patches and hotfixes
    - Audits at the application layer
    - Scans only default ports

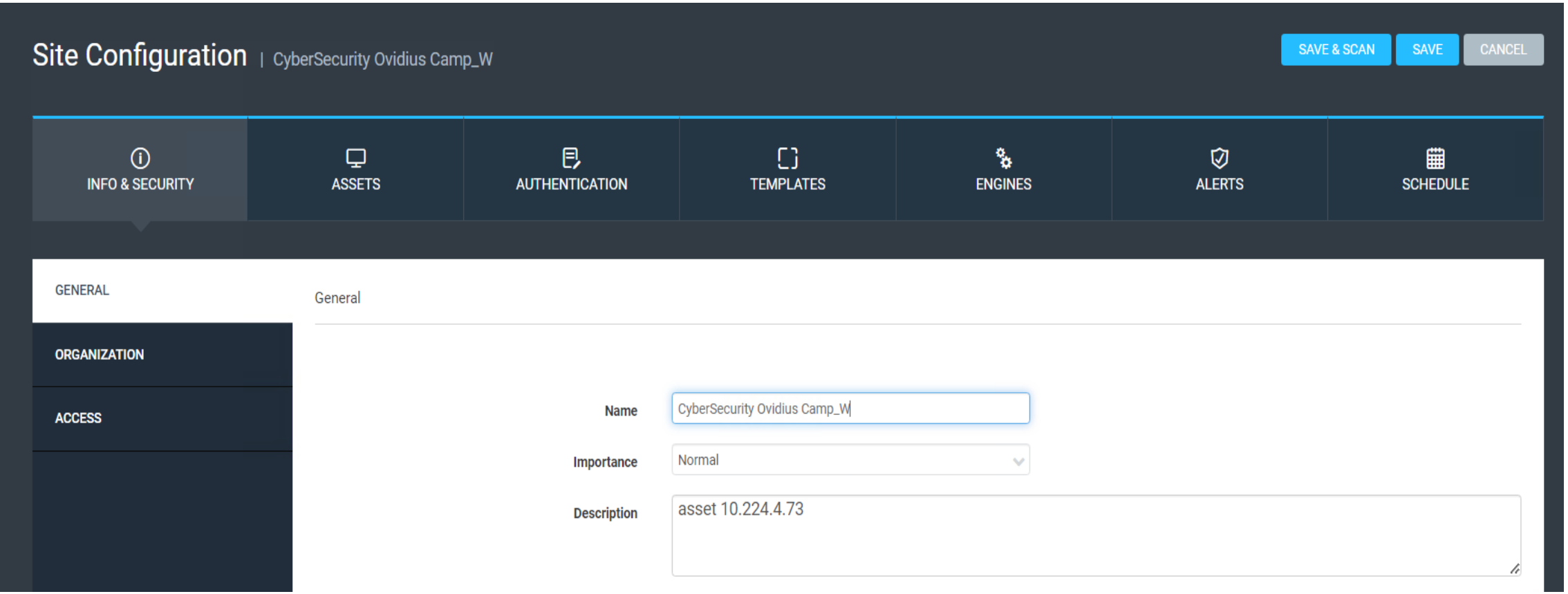
This template also excludes policy checking and web spidering, hence its name. As a consequence, it’s fast, broadly scoped, and reliable.

Save and Scan Your Site

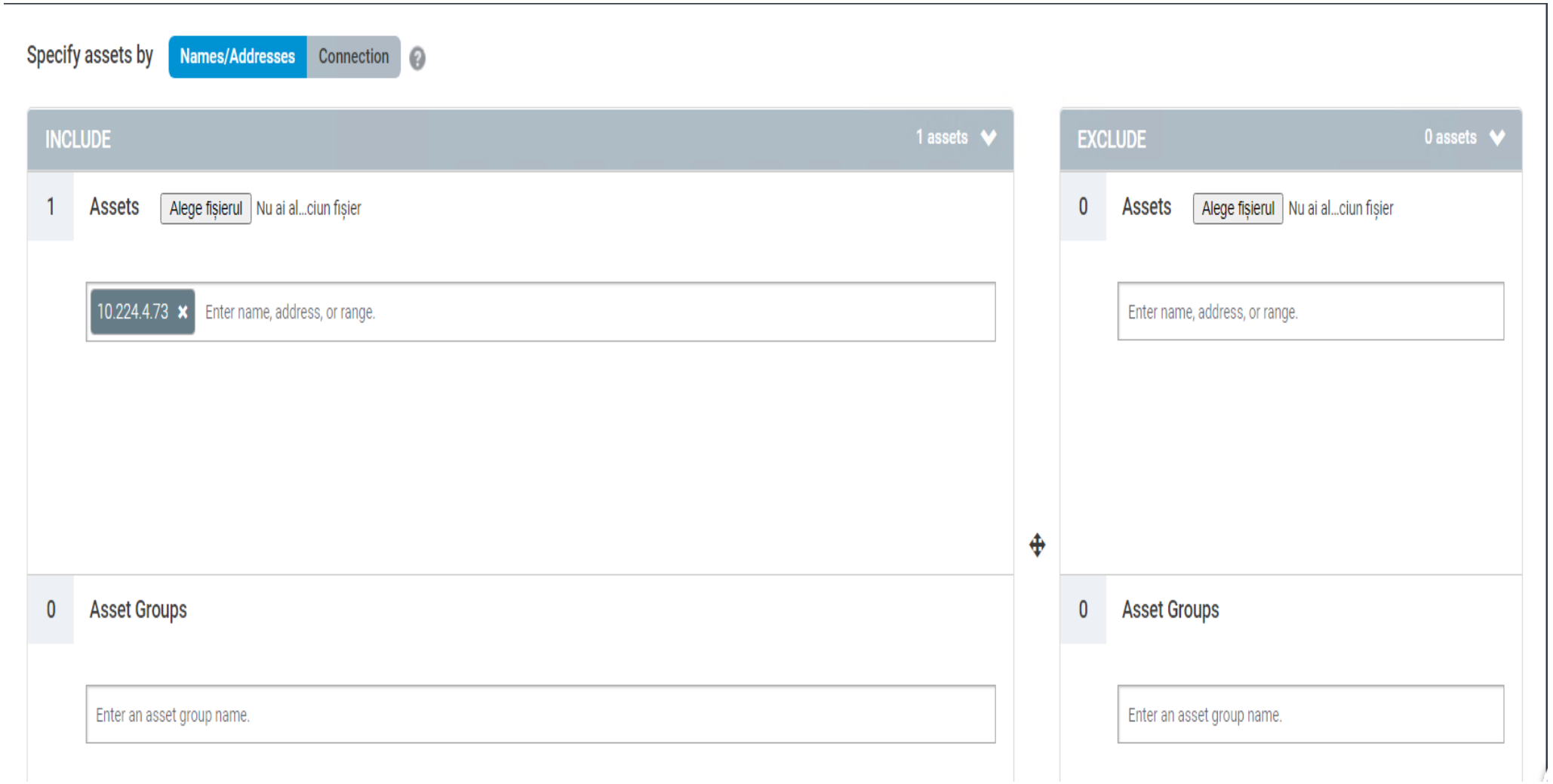
- You should now have all the information required for your first basic site. Keep in mind that there are many other options for site configurations that were not covered here, but this basic configuration is suitable for your first scan.
- Click **Save & Scan** in the upper right corner of your screen to save your site configuration and scan it immediately.
- If you would like to learn more about site configuration capabilities, the Site creation scenarios page is a good place to start.
- **Scan Progress**
- After initiating your first scan, the Security Console displays the site details page. The “Scan Progress” section at the top gives you a live look at the progress of the ongoing scan as it runs.

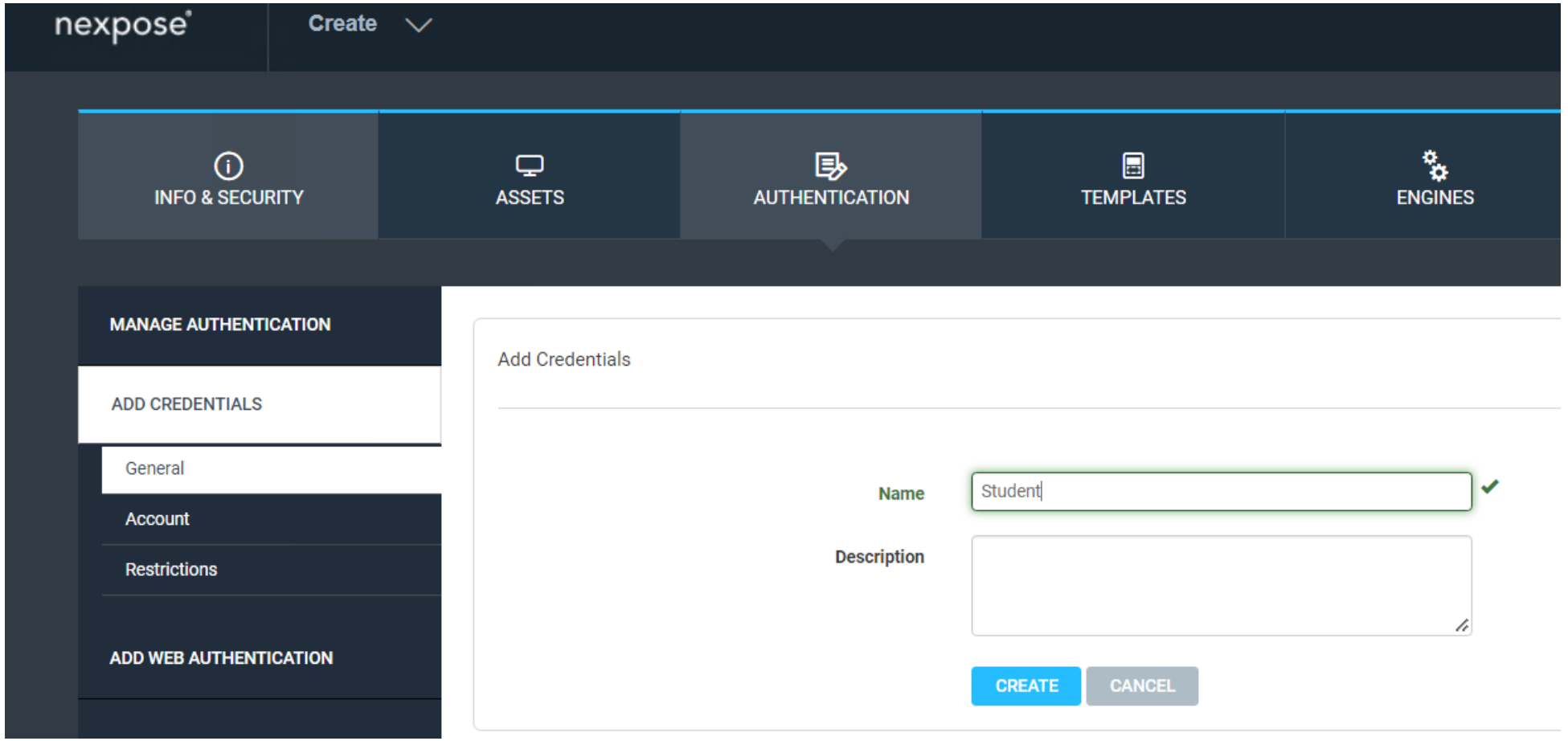
Studiu de caz

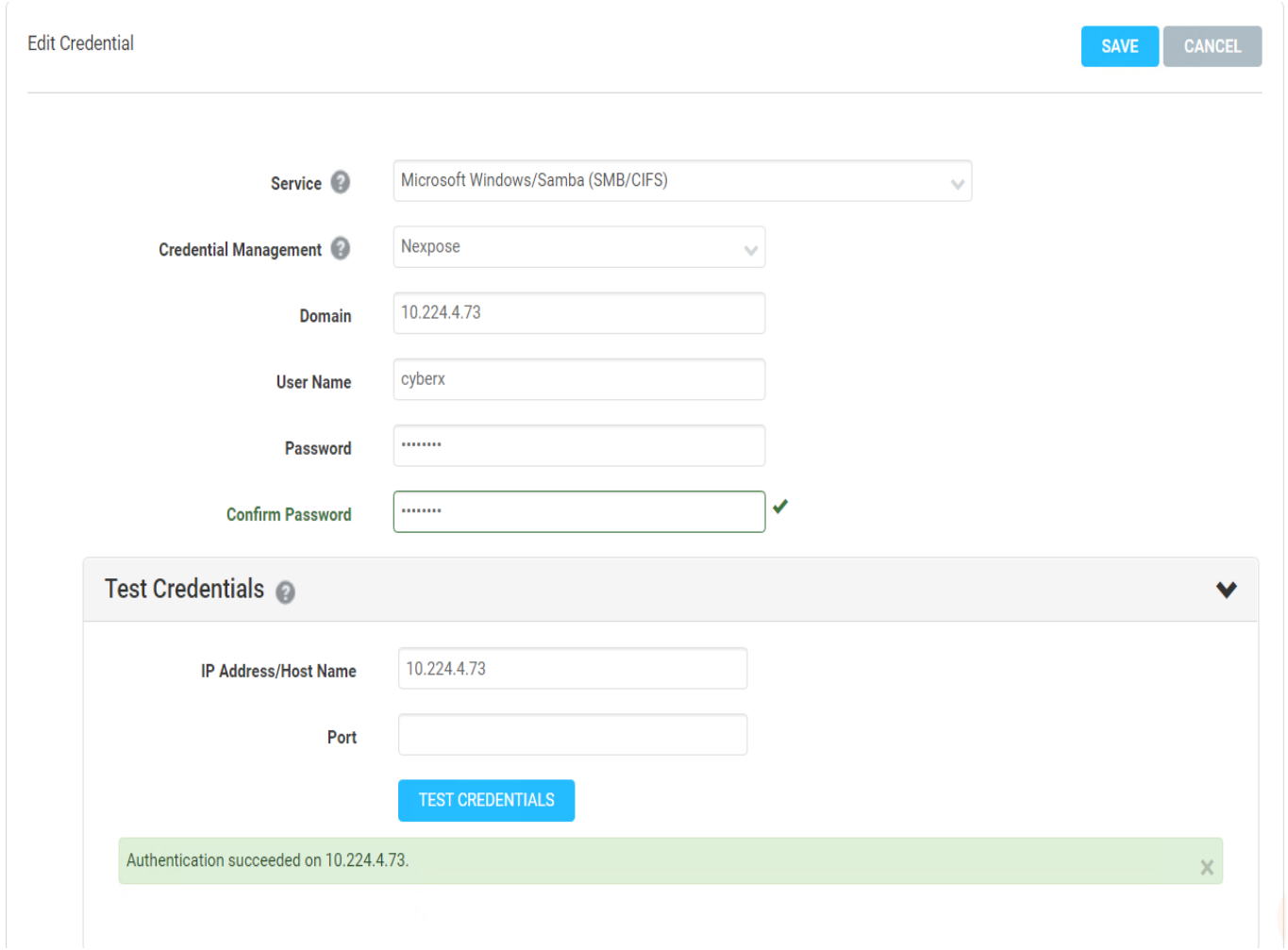
1. Crearea și configurare site



2. Assets


Specify assets by
Names/Addresses
Connection
INCLUDE
1 assets
1
Assets
Alege fișierul
Nu ai al...ciun fișier
10.224.4.73
Enter name, address, or range.
0
Asset Groups
Enter an asset group name.
EXCLUDE
0 assets
0
Assets
Alege fișierul
Nu ai al...ciun fișier
Enter name, address, or range.
0
Asset Groups
Enter an asset group name.


nexpose
Create
INFO & SECURITY
ASSETS
AUTHENTICATION
TEMPLATES
ENGINES
MANAGE AUTHENTICATION
ADD CREDENTIALS
General
Account
Restrictions
ADD WEB AUTHENTICATION
Add Credentials
Name
Student
Description
CREATE
CANCEL



Credentialele sunt

Windows

a. Un: cyberx
b. Pw: P@ssw0rd

Metasploitable (SSH)

a. Un: msfadmin
b. Pw: msfadmin

Site Configuration

SAVE & SCAN | SAVE | CANCEL

INFO & SECURITY | ASSETS | AUTHENTICATION | TEMPLATES | ENGINES | ALERTS | SCHEDULE

SELECT SCAN TEMPLATE

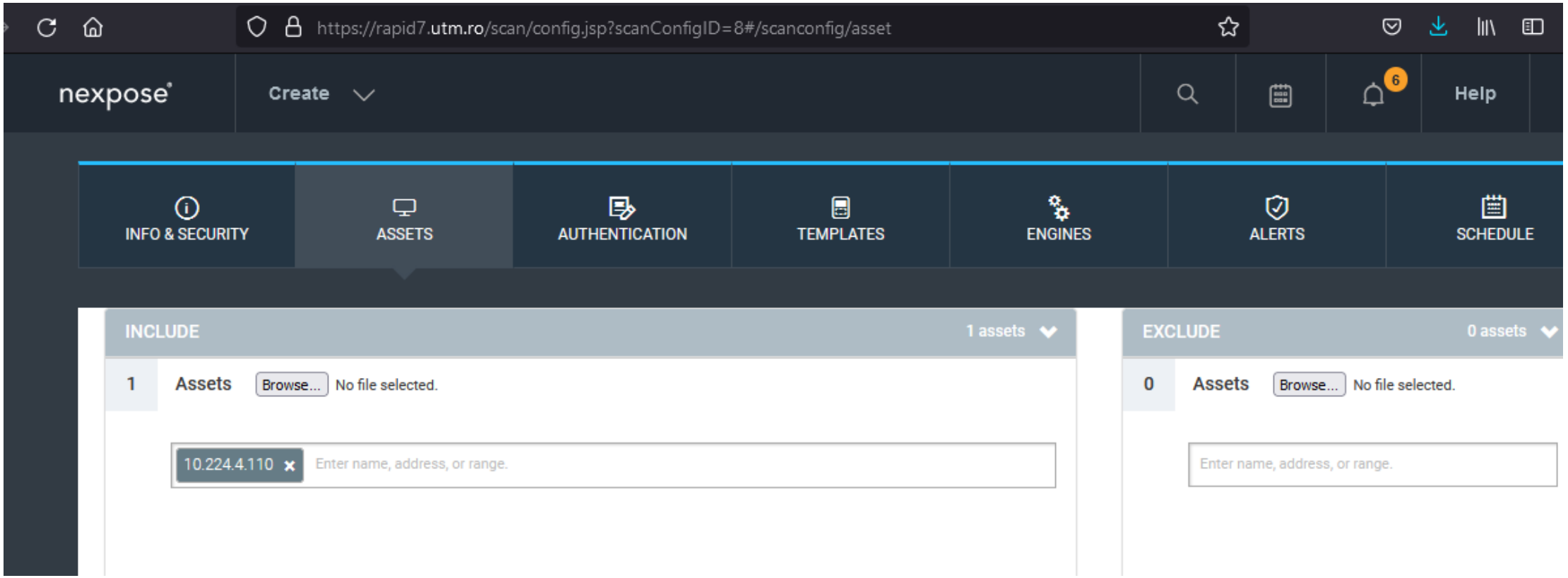
CREATE SCAN TEMPLATE

Selected Scan Template: Full audit without Web Spider

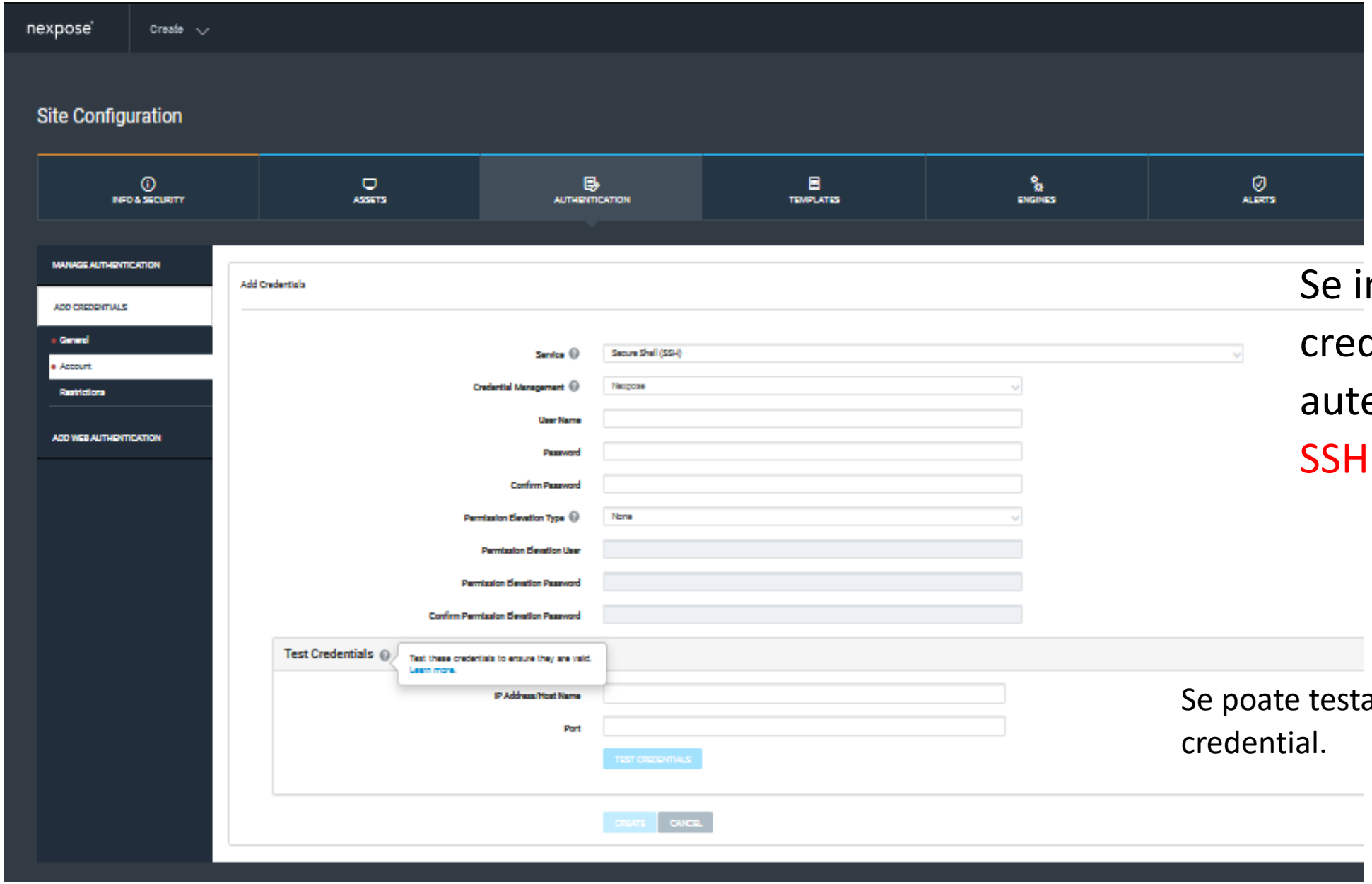
Scan Templates

Filter...

	Name	Asset Discovery	Service Discovery	Checks	Source	Copy
○	DISA	ICMP, TCP	Custom TCP	Safe Only		
○	Discovery Scan	ICMP, TCP, UDP	Custom TCP, Custo...	Disabled		
○	Discovery Scan - Aggressive	ICMP, TCP, UDP	Custom TCP, Custo...	Disabled		
○	Exhaustive	ICMP, TCP, UDP	Full TCP, Default UDP	Custom		
○	FDCC	ICMP, TCP	Custom TCP	Safe Only		
○	Full audit	ICMP, TCP, UDP	Default TCP, Default ...	Custom		
○	Full audit enhanced logging without Web Spider	ICMP, TCP, UDP	Default TCP, Default ...	Custom		
◉	Full audit without Web Spider	ICMP, TCP, UDP	Default TCP, Default ...	Custom		
○	HIPAA compliance	ICMP, TCP, UDP	Default TCP, Default ...	Custom		

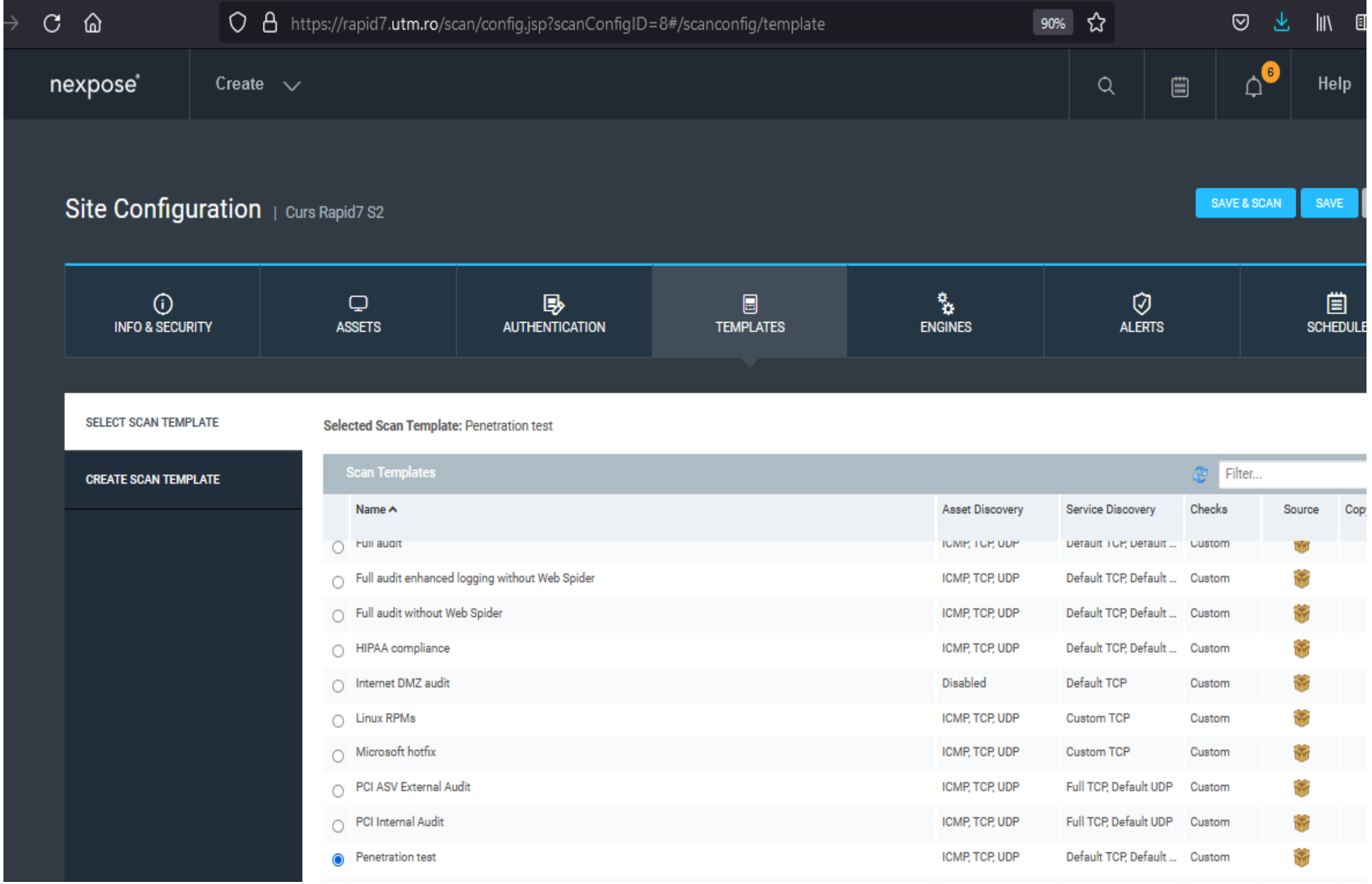


Se adauga “Assets”

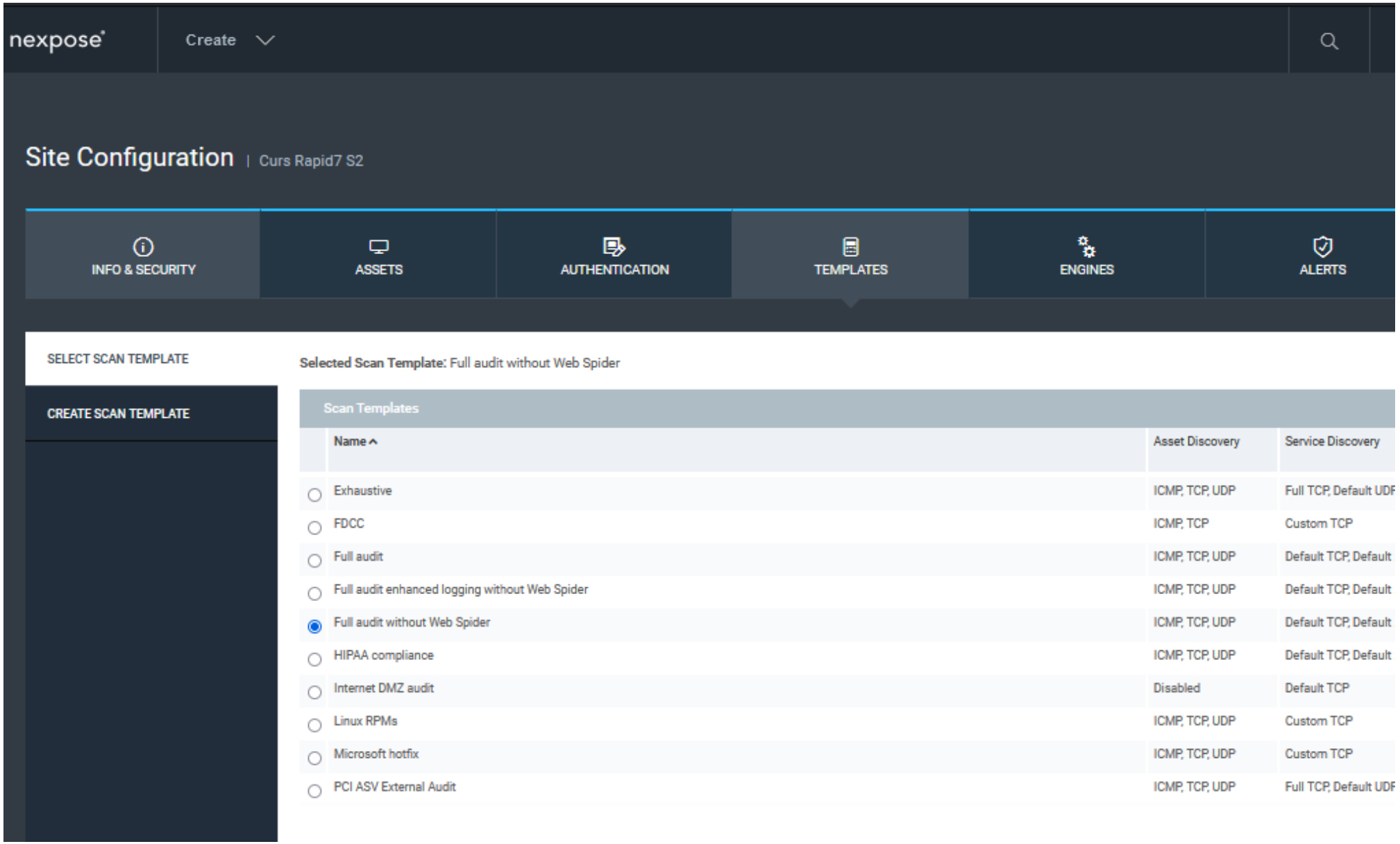


Se introduc credentialele de autentificare de tip SSH (ID / Pass)

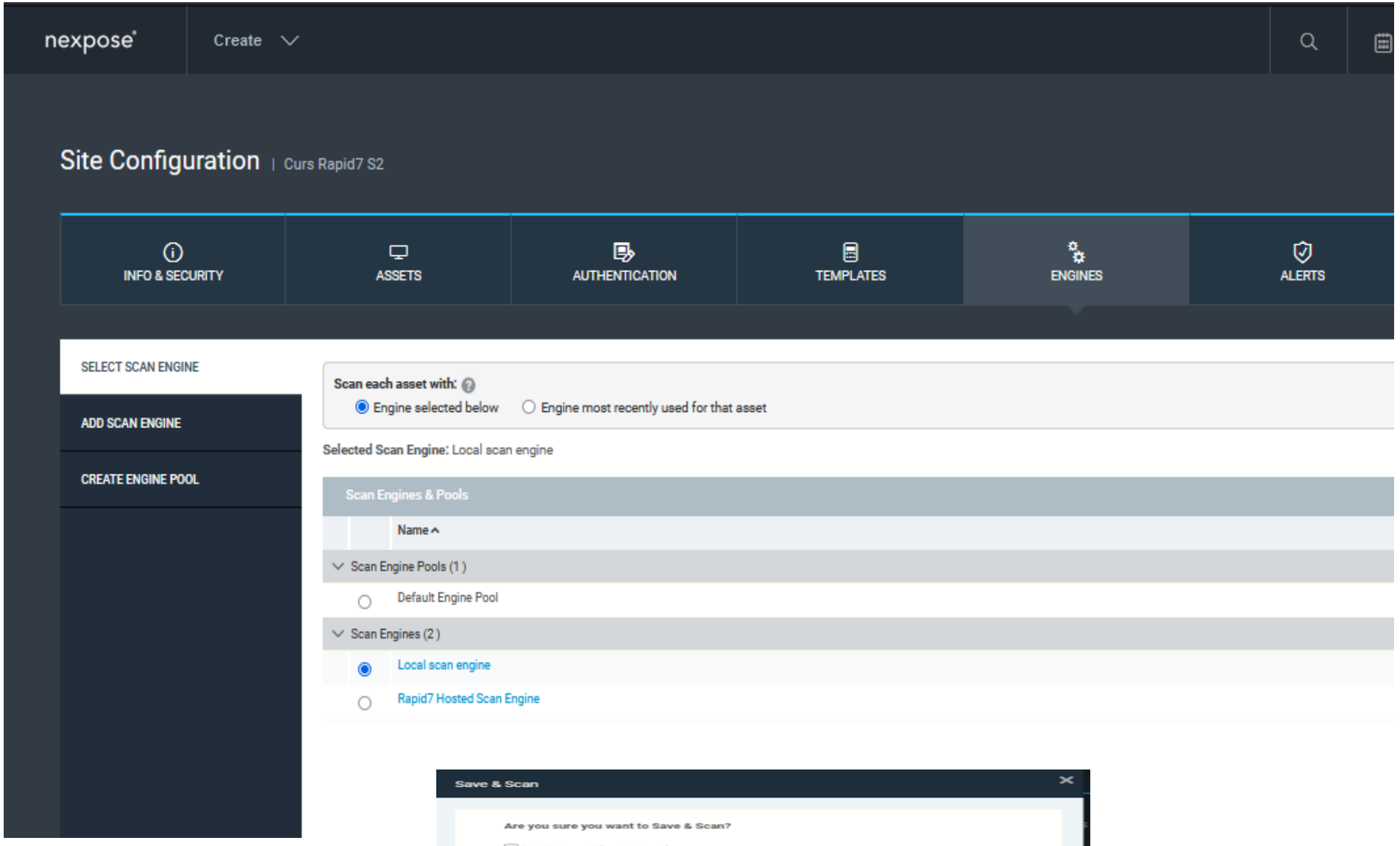
Se poate testa corectitudinea unui credential.



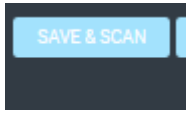
Se aleg “Template”-ul/ șabloanele de scanare

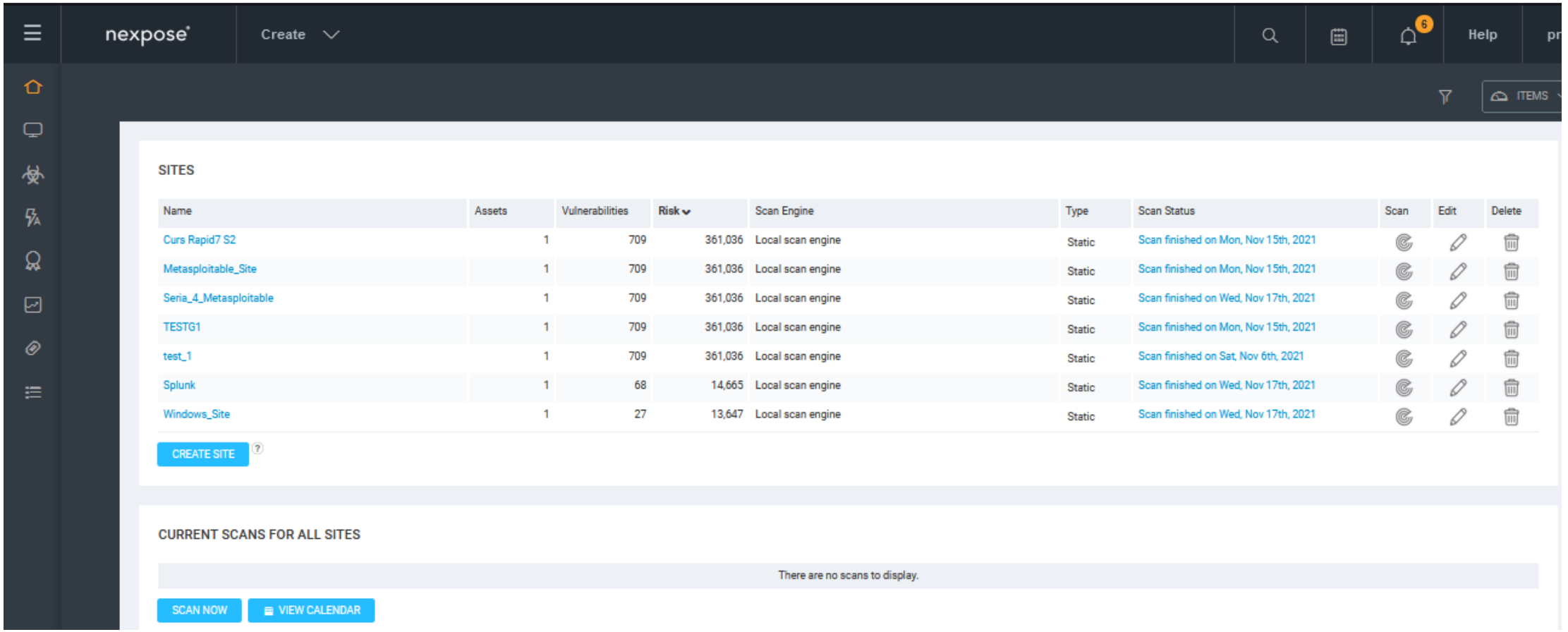


Se aleg “Template”-ul/ sabloanele de scanare


nexpose
Create
Site Configuration | Curs Rapid7 S2
INFO & SECURITY
ASSETS
AUTHENTICATION
TEMPLATES
ENGINES
ALERTS
SELECT SCAN ENGINE
ADD SCAN ENGINE
CREATE ENGINE POOL
Scan each asset with:
Engine selected below
Engine most recently used for that asset
Selected Scan Engine: Local scan engine
Scan Engines & Pools
Name
Scan Engine Pools (1)
Default Engine Pool
Scan Engines (2)
Local scan engine
Rapid7 Hosted Scan Engine

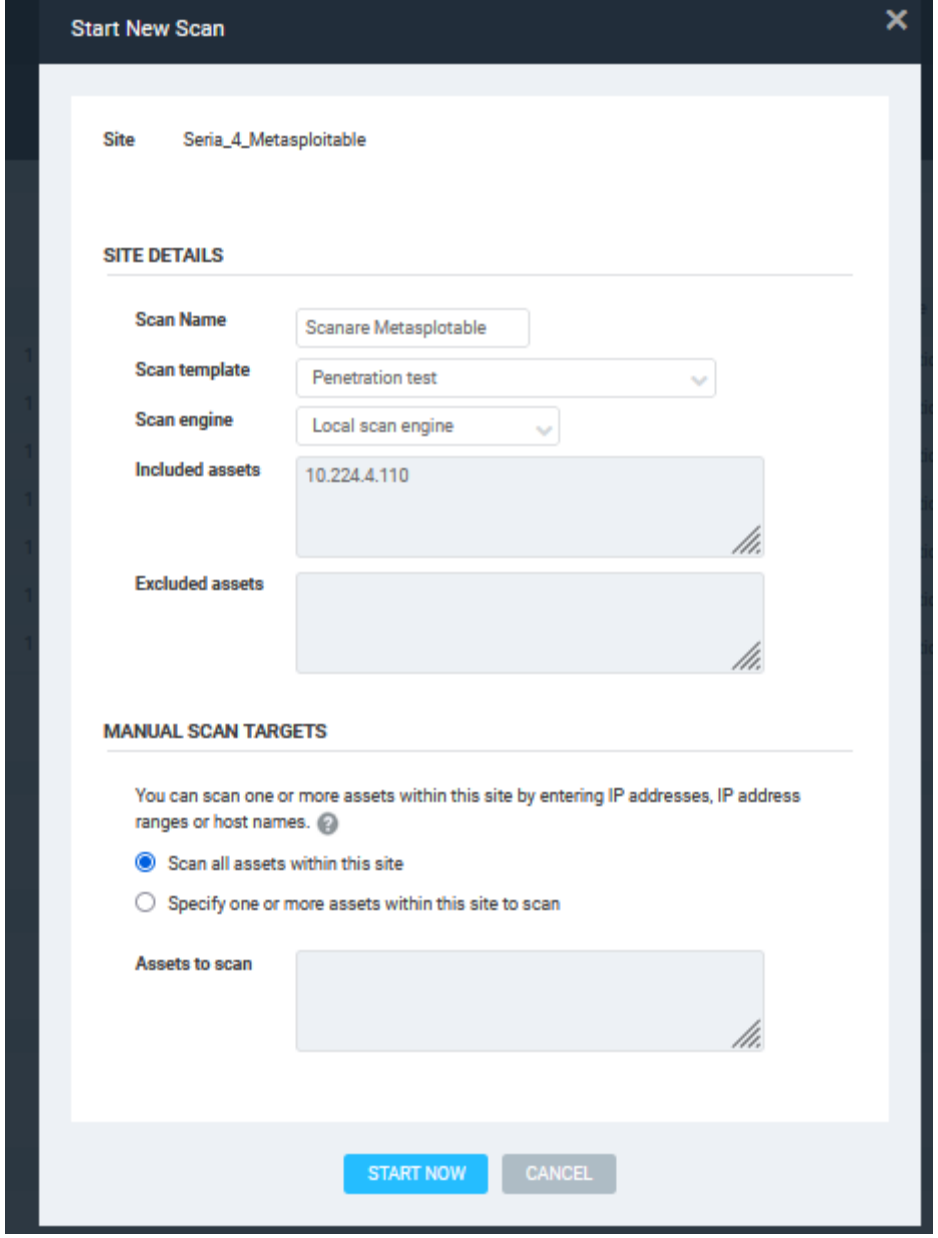
Save & Scan
Are you sure you want to Save & Scan?
Don't show this alert again.
SAVE & SCAN
SAVE ONLY


SAVE & SCAN



Lista site-uri pentru scanare

Pornirea ulterioara a unei scanari



- https://docs.rapid7.com/nexpose/creating-reports-based-on-sql-queries/
- https://docs.rapid7.com/nexpose/understanding-the-reporting-data-model-overview-and-query-design/
- https://docs.rapid7.com/nexpose/fingerprint-certainty/
- https://nvd.nist.gov/vuln-metrics/cvss# https://www.cvedetails.com/;

Studiu de caz

- *Ordonați vulnerabilitățile dupa criteriul “Severity”;*
- *Pentru vulnerabilitatile: PHP Vulnerability: CVE-2007-6039 si USN-1397-1: MySQL vulnerabilities indicați soluțiile de remediere.*
- *Pentru fiecare subcategorie din **Remediatos** analizați cel puțin 2 elemente care vă sunt cunoscute.*
- *Să se realizeze un raport de tip PCI Host Details pentru site-ul CyberSecurity Ovidius Camp_I; daca exista vulnerabilitate de nivel inalt pentru instance: protocol: tcp port: 22, să se explice în detaliu aceasta, folosind informațiile găsite la: https://nvd.nist.gov/vuln-metrics/cvss# si https://www.cvedetails.com/;*