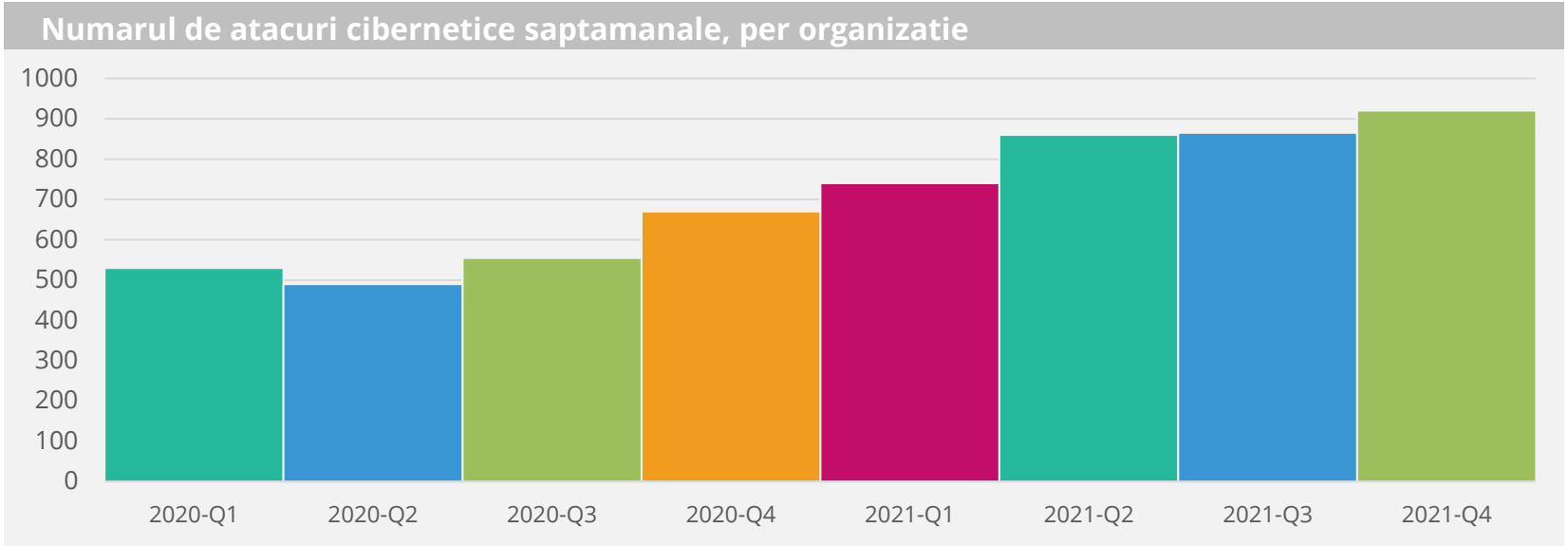
SPARTAN IDS

Solutie inovativa
pentru detectia intruziunilor in infrastructura critica

OMEGA TRUST

Evolutia atacurilor cibernetice

Conform unui studiu efectuat de Check Point

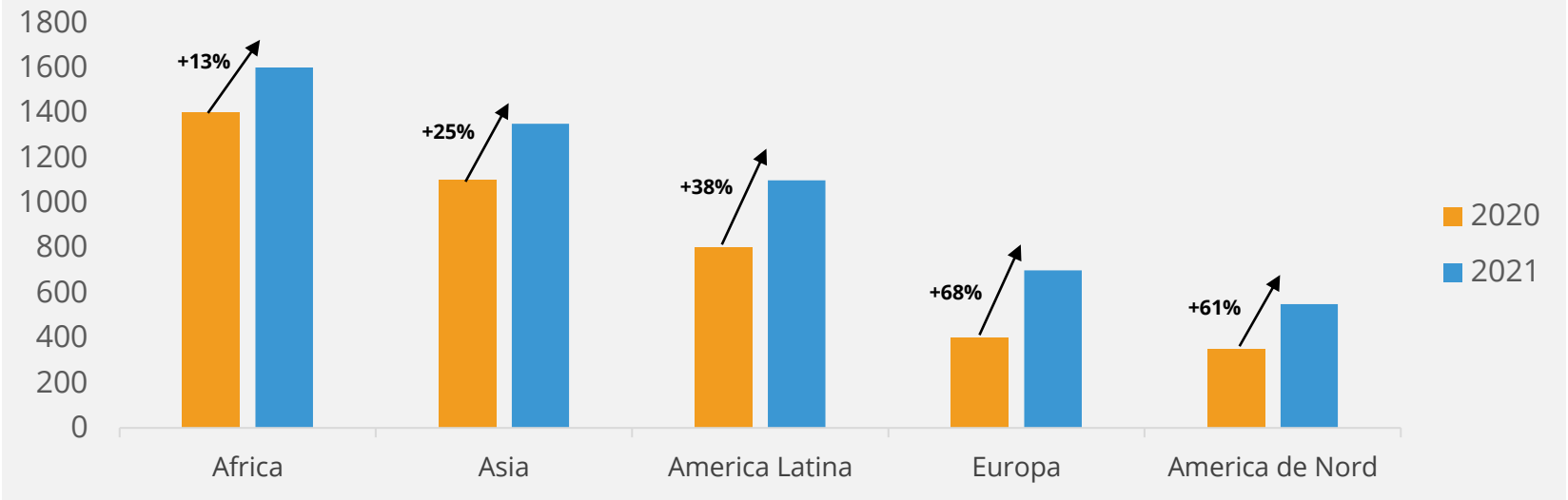


OMEGA TRUST

Evolutia atacurilor per regiune

Conform unui studiu efectuat de Check Point

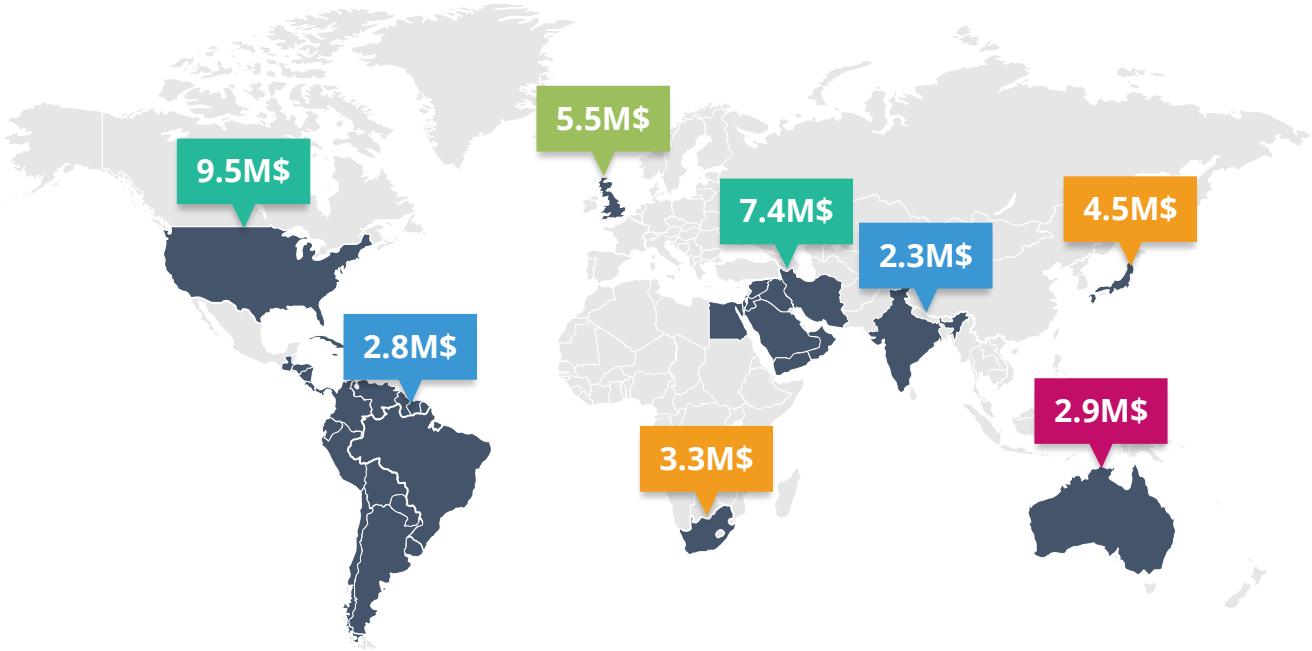
Numarul de atacuri cibernetice saptamanale, la nivel de organizatie, per regiune



OMEGA TRUST

Costul unei brese de date

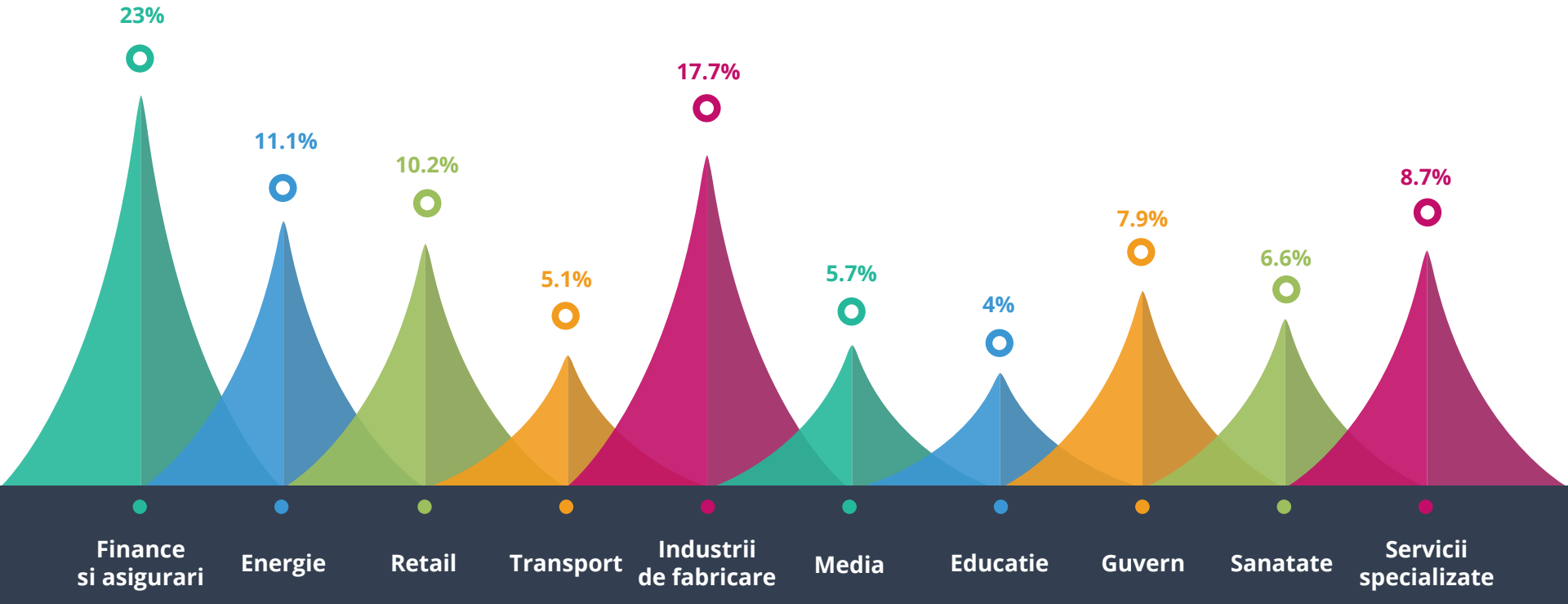
Costul unei brese de date, per regiune



OMEGA TRUST

Industrii afectate

Distributia atacurilor cibernetice, per domeniu de activitate



Directiva NIS

- **Directiva** (UE) 2016/1148
- **Legea 362/2018 (NIS) -** privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice
- **Ordinul 1323/2020 -** Normele tehnice privind cerintele minime

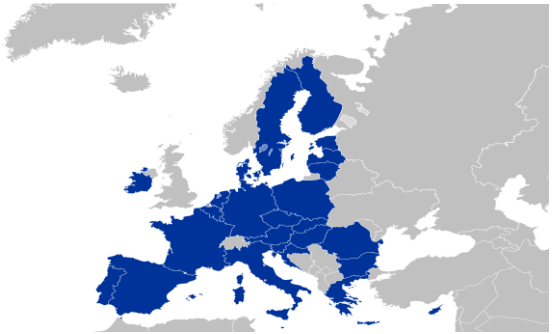
au drept scop cresterea nivelului de pregatire a statelor UE pentru a face fata la incidentele de securitate informatica.

Se adreseaza:

Operatorilor de Servicii Esentiale (OSE) din 7 sectoare de activitate economica: **Energie, Transport, Sectorul bancar, Infrastructuri ale pietei financiare, Sectorul sanatatii, Furnizarea si distribuirea de apa potabila, Infrastructura digitala** si unor categorii de furnizori de servicii digitale.

OMEGA TRUST

Directiva NIS - obligatii



Ordinul 1323/2020:

ARTICOLUL 28 Managementul vulnerabilităţilor şi alertelor de securitate [C11]

....

“2. OSE instituie un **sistem de detectare a incidentelor şi alertelor de securitate**.

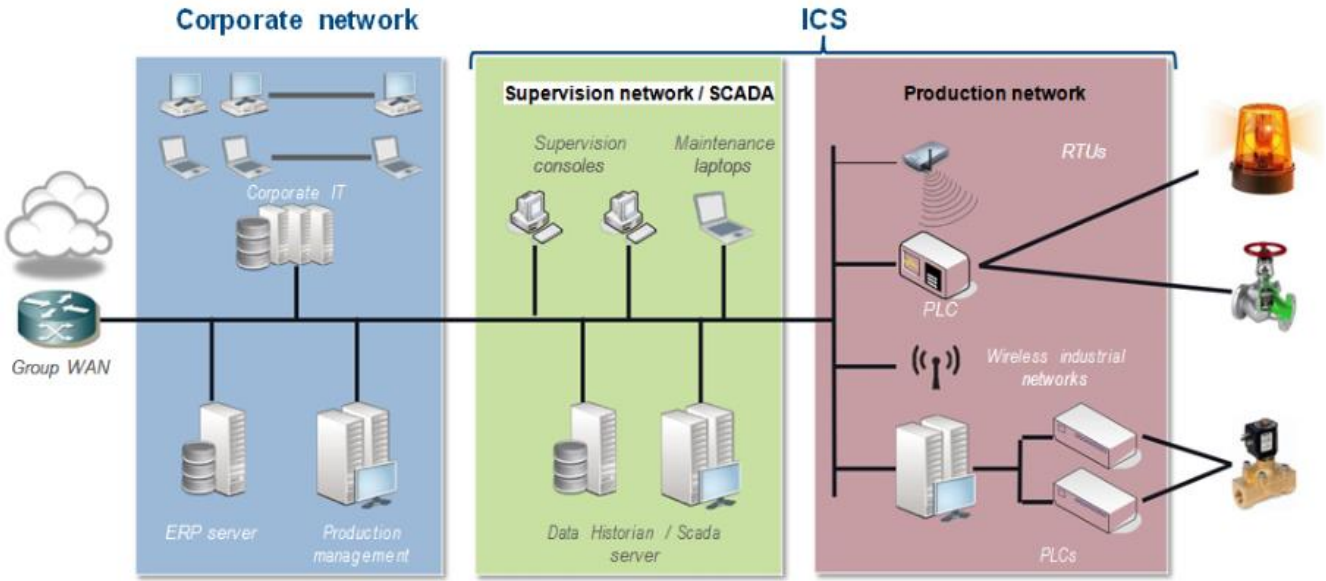
- Dispozitivele de detecţie analizează fluxurile de date care tranzitează reţelele şi sistemele informatice pentru a identifica evenimente care ar putea afecta reţelele şi sistemele informatice.

- Atunci când acest lucru nu este posibil din motive tehnice, operatorul descrie motivele tehnice care au împiedicat utilizarea dispozitivelor de detecţie.”

OMEGA TRUST

Infrastructura ICS vs IT

Industrial Control System (ICS) – SCADA (Supervisory Control and Data Acquisition), DCS (Distributed Control System



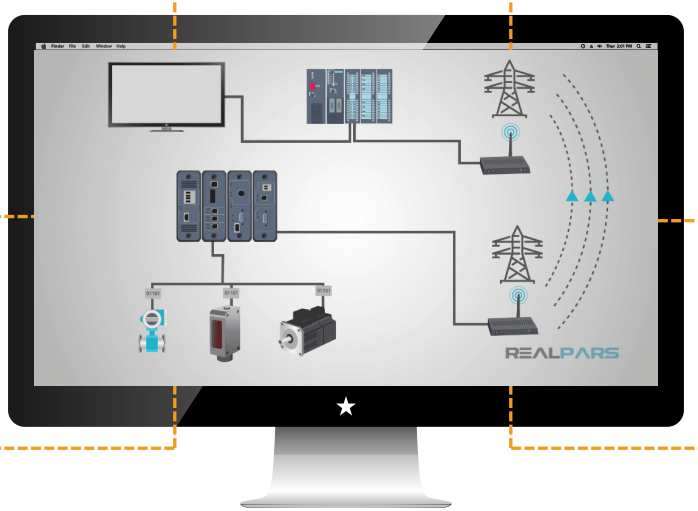
Vulnerabilitati ale sistemelor industriale

Securitatea sistemelor industriale este mult in urma celor IT

Software invechit

Credentiale default

Comunicatii necriptate



Lipsa instrumentelor de monitorizare

Lipsa mentalitatii orientata spre securitate

Lipsa patch-urilor de securitate

OMEGA TRUST

Sistemul inovativ IDS

Caracteristici principale

Detectia intruziunilor de securitate

Obiectivul este detectia intruziunilor de securitate in organizatii prin analiza traficului generat in retele

Acopera infrastructuri ICS dar si IT

Sistemul detecteaza atacuri specifice atat echipamentelor ICS cat si IT

Pasiv, nu Activ

Sistemul este gandit complet pasiv astfel incat sa capteza traficul fara sa afecteze echipamentele din mediul in care opereaza

Machine Learning

Sistemul foloseste algoritmi de detectie avansati de Machine Learning

Poate opera in retele complet inchise

Poate opera atat in retele inchise cat si deschise la internet. Practic, functionalitatile principale nu au nevoie de acces la internet

Scalabil

Sistemul este scalabil si poate acoperi infrastructuri mari, distribuite territorial

OMEGA TRUST

Sistemul inovativ IDS

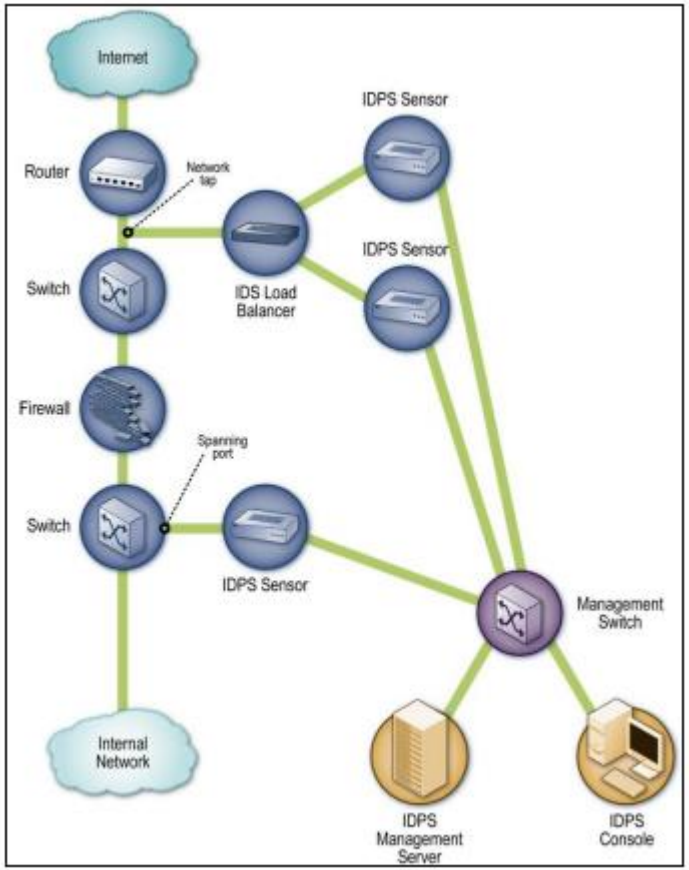
Arhitectura sistemului

Arhitecura este formata din:

- **Senzori (Conectori)**
- **Server de management**
- **Console de monitorizare**

In functie de nevoi, se pot instala mai multi conectori cate unul pentru fiecare segment de retea analizat

Traficul in segmentul respectiv de retea este mirrorat si captat de catre Conector pentru detectia atacurilor



OMEGA TRUST

Sistemul inovativ IDS

Capabilitati principale

Realizeaza detectia atacurilor si anomaliilor

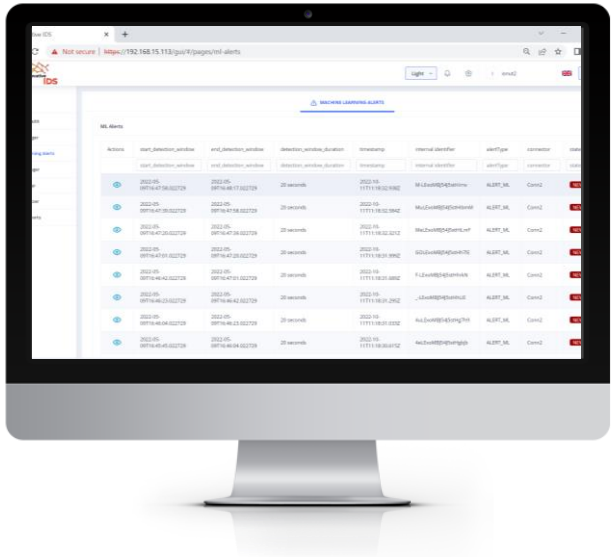
Alerteaza responsabilul de securitate

Permite investigarea detaliata a incidentului

Permite raportarea pe perioada de timp analizata

OMEGA TRUST

Detectia



Detectia se realizeaza prin 2 mecanisme

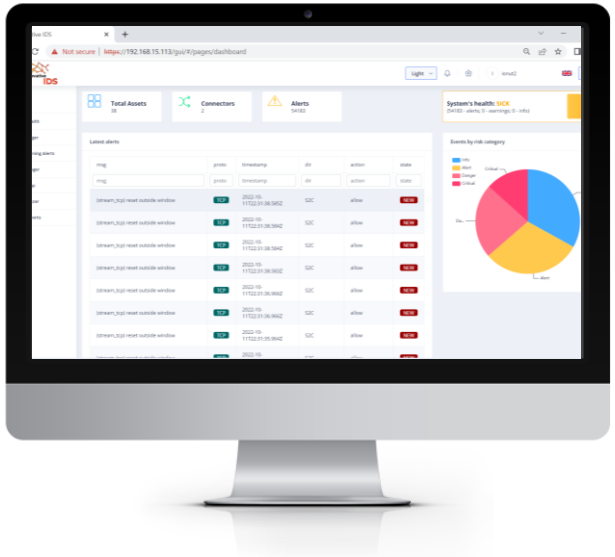
Pe baza de reguli

Detectia se realizeaza pe baza de reguli de semnaturi de atacuri, predefinite si/sau customizate

Pe baza de algoritmi Machine Learning

Detectia anomaliilor se realizeza pe baza de algoritmi puternici de Machine Learning care detecteaza deviatiile de la nivelul de baza

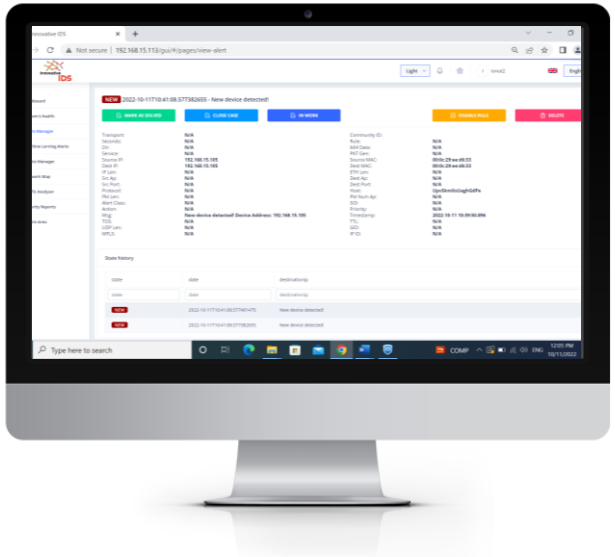
Alertarea



Odata identificat evenimentul, acesta este prezentat in modulul Alerts Manager, unde ii este asociat un status de criticalitate

Sistemul permite cautarea si filtrarea alertelor dupa diversi factori, cu ajutorul engine-ului Elastic Search

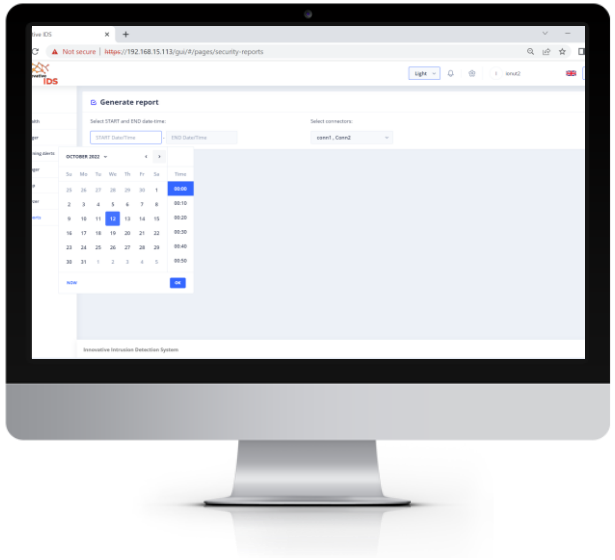
Investigarea



Sistemul permite operatorului sa investigheze parametri specifici ai evenimentului, precum IP-urile sursa si destinatie, protocolul, semnatura atacului, momentul in timp etc.

Operatorul poate trece alerta in diverse stari de lucru, poate inchide alerta in cazul in care considera ca este false pozitiv si poate dezactiva sau imbunatati regula care a dus la detectia respectiva

Raportarea



Sistemul permite generearea de rapoarte grafice de analiza

Se pot genera si exporta rapoarte pentru management sau personal care nu are acces direct la sistem

OMEGA TRUST

Avantajele solutiei noastre

Dorim a ne remarca pe piata, in baza urmatoarelor avantaje competitive

Tehnologie avansata

Detectie pe baza de reguli dar si algoritmi de machine learning

Pret competitiv

Pretul redus comparativ cu competitia

Licenta flexibila

Licenta adaptata la nevoile clientului, cu posibilitate achizitie licenta perpetua

OMEGA TRUST

Model de licentiere

Oferim modele de licente dupa nevoile tuturor clientilor

Licenta perpetua	Licenta anuala
Se plateste o singura data	Plata anuala
Licenta pe termen nelimitat	Licenta cu valabilitate anuala
Suport pe perioada limitata	Suport cu valabilitate anuala

Cost mare initial
Se preteaza companiilor care au buget “one-time”

Cost mic initial, dar licenta trebuie reinnoita.

OMEGA TRUST

DEMO...

INTREBARI