NETALERT

“Instrumente automate de detecție a

comportamentelor anormale în rețelele de calculatoare”

Acest proiect a fost susținut prin grantul acordat de
Ministerul Cercetării, Inovării și Digitalizării, CNCS/CCCDI - UEFISCDI

Proiect:

PN-III-P2-2.1-SOL-2021-0036, în cadrul PNCDI III.

Autoritatea Contractantă:

Unitatea Executivă pentru Finanțarea Învățământului Superior,
a Cercetării, Dezvoltării și Inovării

UNIVERSITY OF BUCHAREST
VIRTUTE ET SAPIENTIA

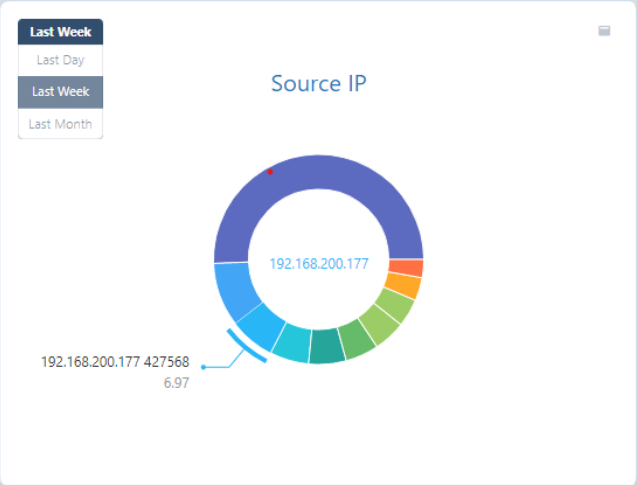
nextgen

NETALERT

SOLUȚIA DE ULTIMĂ GENERAȚIE PENTRU DETECTAREA ȘI RĂSPUNSUL ÎN REȚEA (NDR)

CE ESTE NETALERT?

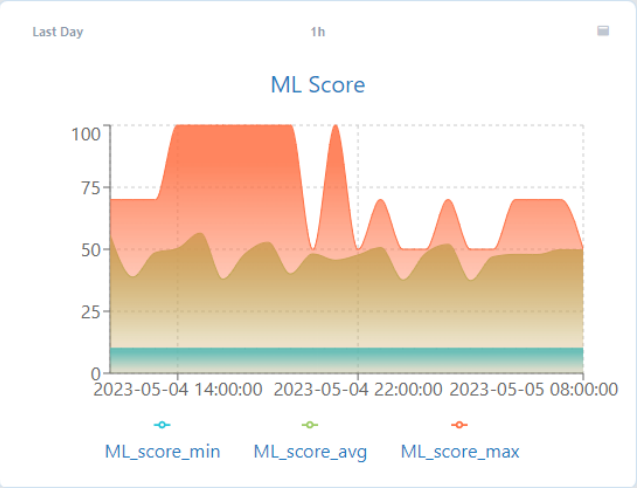
NETALERT este o soluție avansată de securitate cibernetică tip NDR (Network Detection and Response) pentru a monitoriza, analiza și răspunde la amenințările de rețea în timp real. În contextul actual, în care atacurile cibernetice devin tot mai sofisticate și frecvente, devine critică implementarea sa.



CE DETECTEAZĂ NETALERT?

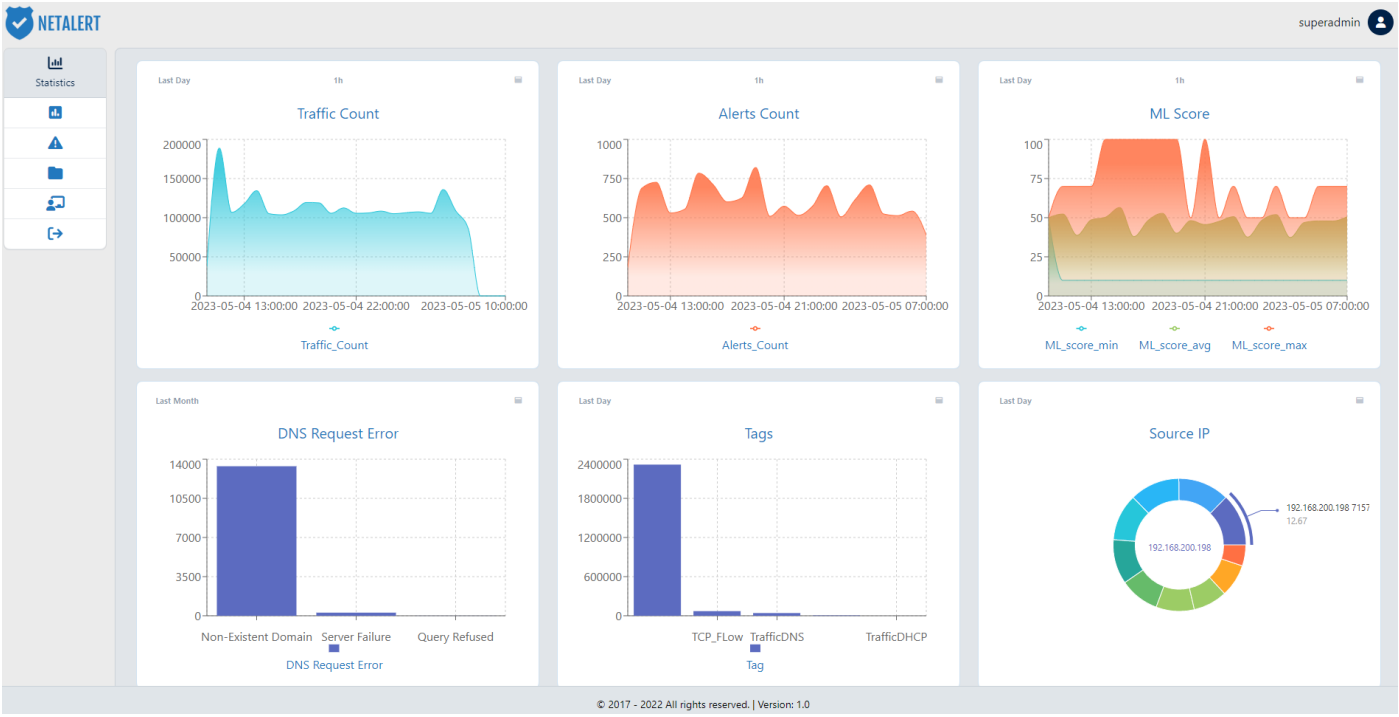
NETALERT se concentrează pe identificarea unor serii de amenințări și puncte sensibile, folosind analiza statică și tehnici de inteligență artificială/ machine learning. Printre acestea se numără:

- Atacuri DDoS
- Conexiuni către endpoint-uri TOR
- Cereri DNS eșuate
- Exploit-uri de tip Heartbleed
- Conexiuni cu certificate SSL invalide
- Atacuri de tip brute force
- Scanări de porturi și adrese
- Dynamic DNS
- Activități de crypto-mining
- Conexiuni cu indicatori de compromis (IOC)
- Comportament specific atacurilor APT (Advanced Persistent Threats) cu detecție la nivel de rețea
- Detectarea tipurilor de fișiere transferate, inclusiv fișiere .exe și alte tipuri
- Mișcări laterale în rețea a malware-ului
- Conexiuni anormale de rețea
- Comportament anormal al dispozitivelor
- Anomalii DNS
- Monitorizarea traficului SMTP



NETALERT este un sistem NDR care monitorizează și analizează în timp real traficul de rețea, oferind o protecție robustă împotriva amenințărilor cibernetice. Soluția capturează în mod pasiv traficul de rețea prin intermediul unui dispozitiv TAP, având suport și pentru span port în medii VMware/ fizice.

NETALERT



CUM FUNCȚIONEAZĂ NETALERT?

- Capturează în mod pasiv traficul de rețea pentru a nu impacta mediul monitorizat.
- Scanează traficul obținut, folosind analiza statică de fluxuri și inteligența artificială/ machine learning.
- Alertare: sistemul generează alerte în timp real atunci când detectează comportamente anormale/ anomalii în traficul de rețea, conexiuni către zone de rețea cu posibile activități suspecte.
- Înregistrarea traficului de rețea până la 32 KB în format PCAP.
- Decodează protocoale binare, precum DNS, SMTP și HTTP, pentru analize specifice.
- Trimite alerte către sisteme terțe, cum ar fi soluții SIEM (Security Information and Event Management), pentru o analiză și gestionare centralizată a alertelor de securitate generate.

CUM SE INTEGREAZĂ NETALERT ÎN ARHITECTURA DE SECURITATE?

NETALERT poate fi implementat în diferite configurații, în funcție de necesitățile organizației:

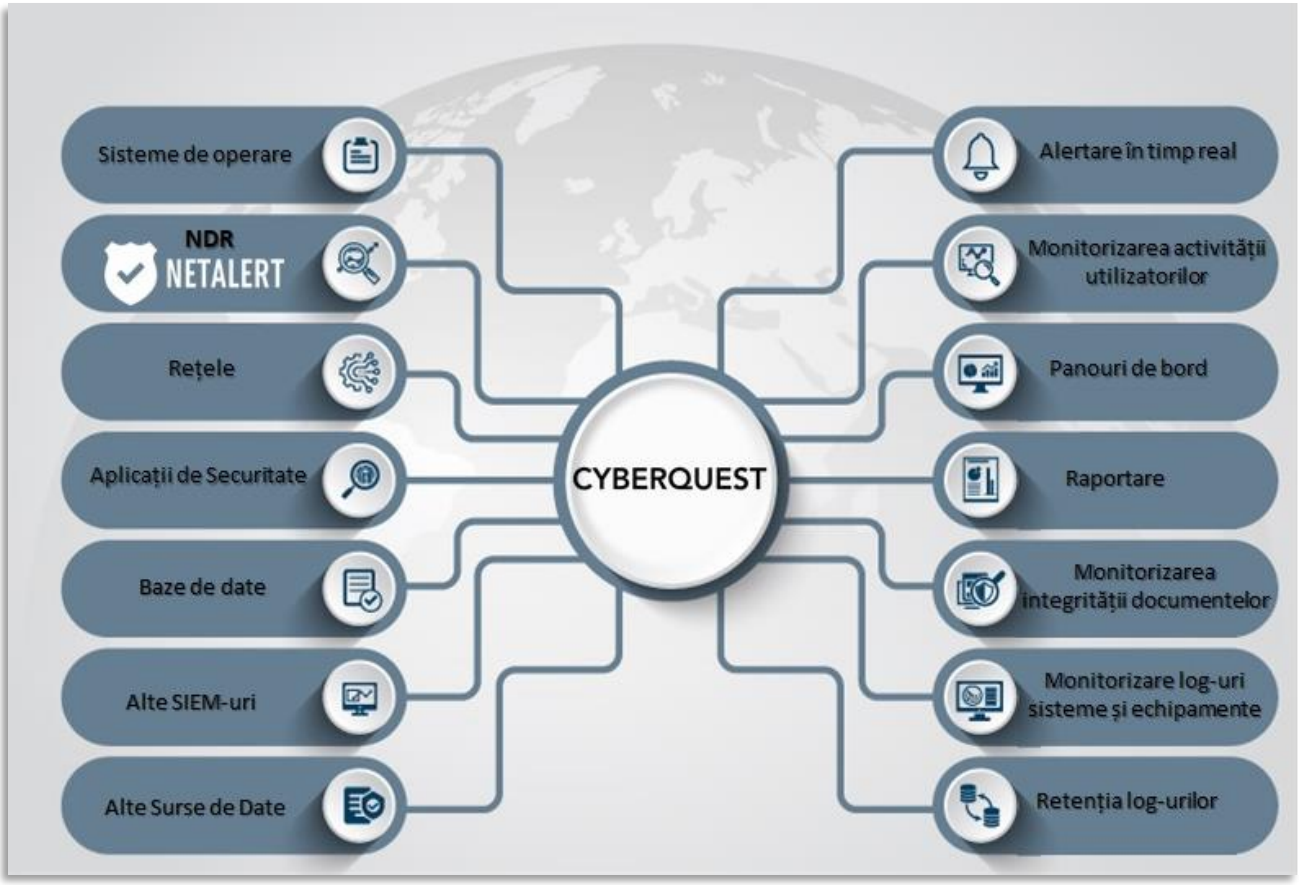
- **Standalone:** Senzorul și interfața de management sunt 100% independente și nu necesită integrare cu alte sisteme de securitate.
- **Integrat cu SIEM:** Alertele generate de NETALERT pot fi transmise către CYBERQUEST sau altă soluție SIEM, prin intermediul unui Forwarder, pentru o analiză și gestionare centralizată a alertelor.

Prin adaptabilitatea sa, NETALERT poate fi integrat cu ușurință în infrastructura de securitate existentă a unei organizații, oferind protecție împotriva unei game largi de amenințări cibernetice și contribuind la menținerea conformității cu reglementările din domeniul securității informațiilor.

NETALERT

INTEGRARE NETALERT CU CYBERQUEST PENTRU VIZIBILITATE ÎN REȚEA

CYBERQUEST și **NETALERT** sunt soluții de securitate complementare care pot fi integrate, pentru a oferi o acoperire completă a securității rețelei unei organizații.



www.nextgensoftware.eu
office@nextgensoftware.eu
Str. Clucerului nr.55, sector 1, București