

V O G O D I G I T A L

FIȘĂ TEHNICĂ

VOGO eBS

VOGO-IDS

SECURITATE CIBERNETICĂ DE TIP IDS

VERSIUNEA 2.4

Produs	VOGO-IDS
Domeniu	Securitate cibernetică de tip IDS
Scop	Detectarea intruziunilor și avertizarea timpurie asupra activităților suspecte
Interfețe	Web responsive, API și aplicație mobilă, după profilul modulului
Execuție	On-premises, cloud privat sau hibrid; containere OCI ori mașini virtuale

1. Prezentare generală

VOGO-IDS monitorizează traficul și activitatea sistemelor pentru a detecta intruziuni, tipare cunoscute de atac și comportamente suspecte înaintea producerii unor efecte semnificative.

Modulul funcționează integrat cu serviciile de identitate, registratură, management al documentelor, fluxuri de lucru, arhivă electronică, notificări și raportare ale suitei VOGO eBS. Configurația se adaptează structurii și procedurilor organizației fără a fragmenta informația între aplicații izolate.

Formularele, integrările, volumele și nivelurile de serviciu sunt configurabile în funcție de structura, procedurile și responsabilitățile organizației beneficiare.

Modulul asigură

- Monitorizarea traficului și detectarea tiparelor cunoscute de atac.

2. Beneficii și rezultate

Analiza în timp real, corelarea cu activele protejate și prioritizarea alertelor reduc timpul necesar identificării și investigării incidentelor.

Modulul asigură

- Analiza anomaliilor și corelarea evenimentelor cu activele protejate.
- Reducerea timpului de procesare și a operațiunilor manuale repetitive.
- Acces unitar la informații și servicii, cu experiență coerentă pe web și mobil.
- Date și documente urmărite de la inițiere până la închidere.
- Configurare adaptabilă fără fragmentarea informației între aplicații izolate.

3. Experiența utilizatorului și fluxul operațional

Echipa de securitate urmărește alerte contextualizate, primește notificări configurabile și transmite evenimentele relevante către SIEM pentru investigație centralizată.

Modulul asigură

- Alerta prioritizată, notificări și transmiterea evenimentelor către SIEM.
- Interfață în limba română, responsive și adaptată rolului utilizatorului.
- Pași clari, validări la introducerea datelor și mesaje explicite de succes sau eroare.
- Salvare intermediară, reluare controlată și istoric al operațiunilor.
- Căutare, filtrare, sortare și export pentru listele operaționale.
- Notificări configurabile la evenimente, termene și schimbări de stare.

4. Date, configurare și administrare

Administratorii actualizează semnăturile, configurează listele de excludere și adaptează regulile proprii la riscurile și infrastructura organizației.

Modulul asigură

- Actualizarea semnăturilor, liste de excludere controlate și rapoarte de securitate.
- Nomenclatoare, tipuri, stări, termene și reguli configurabile.
- Metadate obligatorii și opționale, cu validări și valori controlate.
- Versionarea configurațiilor și promovarea lor între medii.
- Import și export controlat pentru inițializare, migrare și interoperabilitate.
- Administrare separată pe organizație, structură și rol.

5. Integrare și interoperabilitate

Integrarea transmite evenimente și alerte către SIEM și către serviciile autorizate prin API, webhook-uri și conectori jurnalizați.

Modulul asigură

- Modulul monitorizează în timp real activitatea rețelelor și sistemelor și identifică comportamentele neobișnuite și activitățile suspecte înainte ca atacurile sau breșele de securitate să producă efecte semnificative.
- Modulul colectează datele necesare analizei intruziunilor cu impact minim asupra performanței sistemelor monitorizate.
- Modulul analizează datele colectate pentru identificarea tiparelor și semnalelor de alarmă asociate unei posibile intruziuni.
- Modulul utilizează semnături de atac actualizate pentru cele mai recente amenințări și permite modificarea și crearea regulilor proprii ale organizației.
- Modulul generează alerte de la nivel informativ până la nivel critic și furnizează echipei de securitate contextul necesar investigației.
- Modulul transmite notificări prin e-mail și prin alte canale configurate, inclusiv atunci când personalul nu este conectat la platformă.
- API REST documentat și servicii securizate pentru integrare.
- Webhook-uri și evenimente pentru sincronizarea cu sisteme terțe.
- Conectori pentru e-mail, fișiere, baze de date și servicii web.
- Identificatori stabili, idempotență și mecanisme de reluare a operațiunilor.
- Jurnalizarea schimburilor și reconcilierea erorilor de integrare.

6. Identitate, acces și securitate

Accesul pe rol protejează configurațiile și datele IDS, iar comunicațiile criptate și separarea atribuțiilor limitează modificările neautorizate.

Modulul asigură

- Modulul compară activitatea observată cu semnături cunoscute de atac.
- Autentificare prin OpenID Connect, SAML, LDAP, Active Directory și, unde este aplicabil, ROeID sau eIDAS.
- Control al accesului pe roluri, structură, operație și obiect de business.
- Principiul privilegiului minim, delegare temporară și revocare explicită.
- Criptarea comunicațiilor și protejarea datelor sensibile.
- Separarea atribuțiilor administrative și verificarea accesului la nivelul serviciilor.

7. Audit, trasabilitate și conformitate

Auditul păstrează cine a consultat sau modificat regulile și alertele, iar analiza comportamentală identifică anomalii inclusiv în lipsa unei semnături cunoscute.

Modulul asigură

- Modulul utilizează tehnici de învățare automată pentru detectarea comportamentelor anormale inclusiv în lipsa unei semnături cunoscute.
- Jurnal complet pentru autentificare, consultare, creare, modificare, aprobare, transmitere și administrare.
- Păstrarea autorului, momentului, motivului și valorilor relevante pentru fiecare schimbare.
- Politici de retenție și acces la dovezi pentru controale și audit.
- Protecția datelor conform principiilor GDPR, inclusiv minimizare și acces justificat.
- Export de audit și rapoarte de conformitate fără alterarea înregistrărilor operaționale.

8. Raportare, notificări și analiză

Tablourile de bord și rapoartele sintetizează alertele, severitatea, activele afectate, durata și excepțiile și păstrează istoricul notificărilor.

Modulul asigură

- Tablouri de bord operaționale și indicatori configurați pe rol.
- Rapoarte filtrabile și exportabile în formate uzuale.
- Notificări prin e-mail, aplicație, notificări push, SMS sau webhook, în funcție de configurație.
- Indicatori de volum, durată, stare, termen și excepție.
- Istoric al notificărilor și dovada transmiterii.

9. Arhitectură, deployment și scalabilitate

Arhitectura dimensionează colectarea și analiza astfel încât impactul asupra performanței sistemelor monitorizate să rămână minim.

Modulul asigură

- Implementare on-premises, în cloud privat sau în arhitectură hibridă.
- Containere OCI și operare pe Kubernetes sau mașini virtuale.
- Separarea mediilor de dezvoltare, testare, acceptanță și producție.
- Scalare orizontală și componente fără stare acolo unde arhitectura o cere.
- Baze de date relaționale și stocare configurabilă, cu portabilitatea datelor.

10. Continuitate, backup și operare

Semnăturile, regulile, configurațiile și istoricul alertelor sunt incluse în backup, restaurare și monitorizarea funcționării serviciilor IDS.

Modulul asigură

- Backup periodic pentru date, configurații și documente.
- Restaurare testată și proceduri documentate de recuperare.
- Monitorizarea serviciilor, capacității, erorilor și performanței.
- Actualizări controlate, posibilitate de revenire și note de versiune.
- Politici de disponibilitate și recuperare adaptate criticității modulului.

11. Livrare, suport și evoluție

Livrarea configurează sursele, regulile și integrarea SIEM, documentează operarea și instruește utilizatorii și administratorii de securitate.

Modulul asigură

- Instalare, configurare, integrare și documentație tehnică și de utilizare.
- Instruirea utilizatorilor și administratorilor pe roluri.
- Punct unic de contact, sistem de tichete și escaladare pe niveluri de severitate.
- Actualizări de securitate și corecții pe perioada de suport.
- Extinderea controlată cu noi formulare, fluxuri, rapoarte și integrări.