

V O G O D I G I T A L

FIȘĂ TEHNICĂ

VOGO eBS

VOGO-SIEM

MANAGEMENTUL CENTRALIZAT AL EVENIMENTELOR DE SECURITATE

VERSIUNEA 2.2

Produs	VOGO-SIEM
Domeniu	Managementul centralizat al evenimentelor de securitate
Scop	Colectarea, corelarea, investigarea și răspunsul la evenimente de securitate
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-SIEM colectează, normalizează, corelează, investighează și gestionează centralizat evenimentele de securitate.

Modulul asigură

- VOGO-SIEM centralizează colectarea, corelarea, investigarea și răspunsul la evenimentele de securitate din întreaga infrastructură IT.
- Modulul asigură funcționalitățile în format COTS/out-of-the-box, fără a fi necesare dezvoltări, ci doar configurări sau personalizări,
- Modulul include integral capabilitățile tehnice, licențele și componentele necesare monitorizării de securitate.
- Modulul colectează evenimente de audit din echipamente, aplicații, baze de date și celelalte componente ale infrastructurii.
- Modulul oferă licențiere perpetuă și instalare în infrastructura organizației.
- Modulul oferă o interfață web de operare și administrare compatibilă cu browsere moderne, inclusiv Chrome și Microsoft Edge.
- Modulul stochează datele în două depozite complementare: arhivă comprimată pentru păstrare pe termen lung și depozit online indexat pentru investigații și raportare.
- Modulul asigură monitorizarea, detectarea și raportarea centralizată a incidentelor, intervenția rapidă și protejarea confidențialității, integrității și disponibilității datelor.

2. Colectarea și managementul surselor de date

VOGO-SIEM colectează evenimente din segmente distincte prin agenți, Syslog, NetFlow, sFlow și TAP și administrează sursele, conectorii și activele de securitate din interfața grafică.

Modulul asigură

- Modulul colectează evenimente din segmente de rețea distincte, prin agenți sau direct din sistemele-sursă.
- Modulul colectează fluxuri Syslog, NetFlow și sFlow și date preluate direct prin sisteme de tip TAP.
- Agenții transmit datele către serverul de procesare în format comprimat și criptat.
- Agenții filtrează și execută preprocesarea și postprocesarea datelor colectate.
- Agenții protejează datele împotriva alterării la colectare, în tranzit și în repaus.
- Modulul administrează instalarea, dezinstalarea și parametrii agenților individual sau în lot.
- Modulul adaugă sursele de date din interfața grafică, le descoperă automat și identifică tipurile comune de evenimente.
- Modulul descoperă automat infrastructura în care este instalat.
- Modulul include managementul activelor de securitate și păstrează numele, criticitatea, adresele IP și MAC, zona de rețea și vulnerabilitățile identificate.
- Modulul preia evenimente text și tabele de audit din baze de date Microsoft SQL Server, Oracle, MariaDB și PostgreSQL.
- Modulul preia mesaje Syslog din echipamente de rețea, echipamente de tipărire, sisteme de control al accesului și alte echipamente.
- Modulul colectează evenimente de securitate din sistemele de fișiere Linux și Windows.
- Modulul colectează metadate din Active Directory, WMI, SNMP și sisteme de management al identităților și le utilizează la corelare.
- Modulul generează evenimente interne pentru interpretarea situațiilor și a evenimentelor specifice identificate în infrastructură.
- Modulul configurează conectori pentru evenimente multilinie, fișiere XML și fișiere text liber.
- Modulul filtrează evenimentele la sursă și la destinație prin eliminare, trimitere exclusivă în arhivă sau ocolirea motorului de corelare cu păstrare online și în arhivă.

3. Depozite de date și protecția informațiilor

Arhiva comprimată și depozitul online indexat păstrează datele în tehnologii neproprietare, aplică protecția criptografică și permit importul controlat pentru investigații și raportare.

Modulul asigură

- Arhiva comprimă datele cu o rată de minimum 1 la 20 și oferă mecanisme de nerepudiare prin criptare și semnare digitală.
- Depozitul online păstrează datele indexate și le face disponibile rapid pentru investigații și raportare.
- Modulul utilizează depozite de date bazate pe tehnologii neproprietare, astfel încât datele organizației rămân accesibile și utilizabile independent de subscripția, mentenanța sau suportul soluției.
- Modulul anonimizează sau pseudonimizează datele prin selectarea manuală a câmpurilor pentru fiecare tip de sursă.
- Modulul identifică automat câmpuri sensibile, inclusiv CNP, aplică regulile pentru toate sursele sau numai pentru cele selectate și permite excluderi controlate.
- Modulul importă evenimentele din arhivă în depozitul online imediat sau programat și permite filtrarea evenimentelor importate.
- Importul din arhivă este administrat integral din interfața grafică a modulului.
- Modulul aplică funcția RTBF (right to be forgotten) pentru evenimentele din depozitul online și din arhivă.
- Licențierea include scalarea depozitelor online și a arhivei pe durata utilizării.

4. Căutare și experiența analistului

Analistii explorează evenimentele prin coloane și filtre configurabile, expresii logice complexe și căutări rapide și pot lansa verificări contextuale direct din eveniment.

Modulul asigură

- Modulul afișează tabelar toate evenimentele colectate și permite configurarea coloanelor, filtrarea avansată și ordonarea.
- Modulul returnează în mai puțin de 10 secunde rezultatele unei căutări simple după un criteriu în întregul depozit online.
- Modulul salvează filtrele pentru reutilizare și le transformă în definiții de raport, alertă sau tablou de bord.
- Modulul oferă o vizualizare detaliată pentru fiecare eveniment.
- Modulul combină operatorii logici AND, OR și NOT și acceptă expresii complexe cu paranteze imbricate.
- Modulul corelează jurnalele indiferent de sursă și tipul jurnalului.
- Modulul detectează automat autentificările suspecte.
- Modulul permite executarea controlată din contextul evenimentului a comenzilor ping, traceroute, whois și nslookup pentru obținerea informațiilor suplimentare.

5. Corelare, alertare și răspuns automat

Motorul corelează evenimente și secvențe în mai mulți pași, aplică reguli și praguri și declanșează alerte, acțiuni automate și playbook-uri pentru răspuns.

Modulul asigură

- Modulul include în motorul de corelare toate evenimentele ingerate și permite excluderea controlată după sursă sau identificatorul tipului de eveniment.
- Modulul execută corelări în mai mulți pași, din unul sau mai multe evenimente ori secvențe, cu praguri individuale de activare.
- Modulul execută acțiuni automate predefinite sau personalizate după declanșarea alertelor și utilizează în acțiuni câmpurile evenimentelor care au produs alerta.
- Modulul definește reguli pentru evenimente singulare, evenimente corelate, cumul de evenimente, absența unui eveniment, absența unui eveniment corelat și situații particularizate.

- Modulul marchează alertele individual sau în lot și aplică marcarea automată în funcție de scorul de securitate și gravitate.
- Modulul înregistrează rezoluția alertelor individual sau în lot.
- Modulul transmite notificări pentru alerte prin canalele configurate.
- Modulul include alerte de bune practici out-of-the-box pentru tehnologii multiple și permite definirea sau editarea acestora într-o interfață grafică intuitivă.
- Modulul oferă fluxuri complete pentru analiști și răspunde automat la incidente prin playbook-uri predefinite și personalizabile.

6. Analiză comportamentală, amenințări și vulnerabilități

UEBA, feedurile de amenințări, indicatorii IOC, scorurile de risc și scannerul de vulnerabilități identifică abateri, trafic malițios și expuneri relevante pentru investigație.

Modulul asigură

- Modulul integrează nativ feeduri de securitate open-source și pe bază de abonament și include un feed propriu cu adrese IP, domenii și URL-uri malițioase.
- Modulul corelează automat evenimentele cu indicatorii de compromitere (IOC) și identifică sistemele care comunică cu aceștia.
- Modulul alertează automat traficul către adrese IP malițioase atât pentru evenimente curente, cât și pentru evenimente istorice.
- Modulul verifică automat sau manual, inclusiv în lot, indicatorii de compromitere în depozitul online și în arhivă.
- Modulul UEBA detectează modificările tiparului normal pentru autentificări interactive, automate și de la stații noi.
- Modulul UEBA detectează țările și orașele noi utilizate de fiecare utilizator pentru autentificarea VPN.
- Modulul detectează serviciile nou pornite la nivelul organizației și al serverului.
- Modulul calculează scoruri de risc pentru active, grupuri de utilizatori și tipuri de evenimente.
- Modulul integrează nativ, prin API și direct din interfața de administrare, un scanner de vulnerabilități pentru sisteme, aplicații web și echipamente de rețea.
- Modulul utilizează vulnerabilitățile și rapoartele scannerului în procesele de corelare, investigare și alertare.

7. Managementul incidentelor și al cazurilor

Cazurile de securitate reunesc colaborarea, alocarea și escaladarea investigațiilor pornite din alerte și evenimente, cu acces granular pentru analiști.

Modulul asigură

- Modulul oferă un spațiu colaborativ de investigare a incidentelor și permite definirea grupurilor de destinatari pe mai multe niveluri.
- Modulul alocă automat sau manual cazurile analiștilor de securitate și le escaladează automat către nivelurile următoare.
- Analiștii deschid cazuri de investigație direct din alerte și evenimente.
- Modulul controlează granular accesul la cazurile de investigație.

8. Tablouri de bord și raportare

Tablourile configurabile și rapoartele de bune practici și conformitate agregă evenimentele, aplică filtre comune și exportă rezultatele și definițiile în formatele necesare.

Modulul asigură

- Modulul afișează agregările de evenimente în tablouri de bord configurabile și grupează în aceeași colecție tablouri asociate unor tehnologii diferite.

- Fiecare utilizator configurează propriile tablouri de bord în limitele permisiunilor atribuite.
- Modulul filtrează simultan toate tablourile de bord după un criteriu comun.
- Modulul include rapoarte de bune practici pentru tehnologii multiple și rapoarte de conformitate pentru GDPR, ISO 27001, COBIT, FISMA, SOX și PCI-DSS.
- Modulul creează rapoarte noi, editează rapoartele existente și planifică rularea și transmiterea lor.
- Modulul permite personalizarea și redenumirea tuturor rapoartelor predefinite.
- Prima pagină a raportului prezintă perioada și evenimentele incluse, iar corpul raportului include grafice relevante.
- Modulul exportă rapoartele în formatele PDF, HTML, XLSX, XLS, CSV și XML.
- Modulul exportă individual sau în selecție definițiile rapoartelor.

9. Administrare și monitorizarea platformei

Administrarea aplică RBAC și LDAP, controlează redirectionarea evenimentelor și alertelor și monitorizează serviciile, ingestia, resursele și operațiunile platformei.

Modulul asigură

- Modulul aplică permisiuni RBAC pentru accesul la date și configurații și rezervă modificarea datelor sistemului componentelor și rolurilor autorizate.
- Modulul se integrează cu LDAP pentru autentificare unitară.
- Modulul redirectionează evenimente brute sau normalizate în formatele Syslog, JSON și CEF și aplică filtre pe sursă și tip.
- Modulul exportă alertele manual sau automat, individual ori în lot, prin e-mail, apeluri API și Syslog.
- Modulul configurează redirectionarea din interfața grafică până la nivelul tipului de eveniment sau alertei.
- Modulul monitorizează starea serviciilor componente și le restaurează automat în caz de oprire.
- Modulul alertează la depășirea pragurilor de ingestie și a volumului de evenimente aflate în așteptare.
- Modulul auditează toate operațiunile utilizatorilor și serviciilor componente.
- Modulul monitorizează în timp real și păstrează minimum 24 de ore istoricul utilizării discului, memoriei și procesorului pentru mașinile-sursă.
- Modulul oferă un API pentru integrarea surselor noi și extinderea logicii de colectare, corelare și alertare.

10. Arhitectură, dimensionare și scalabilitate

Appliance-ul virtual susține arhitectură all-in-one sau distribuie orizontală și licențiere pentru minimum 5.000 EPS, 350 GB pe zi ori 1.500 de noduri, fără limitarea volumului depozitelor.

Modulul asigură

- Modulul este instalat în infrastructura organizației sub forma unui appliance virtual.
- Modulul oferă o arhitectură all-in-one, cu toate serviciile și componentele instalate pe aceeași mașină.
- Modulul distribuie orizontal serviciile și componentele atunci când scalarea necesită utilizarea infrastructurii existente.
- Licențierea acomodează minimum 5.000 EPS, 350 GB de date pe zi sau 1.500 de noduri, în funcție de parametrul de licențiere aplicat.
- Licențierea acoperă integral volumele bazelor de date online și ale arhivei, precum și scalarea capacității depozitelor.

11. Livrare, suport și conformitate

Livrarea acoperă instalarea, configurarea, activarea colectării și transferul de cunoștințe, iar funcționarea modulului respectă GDPR și Directiva NIS 2.

Modulul asigură

- Livrarea include instalarea și configurarea modulului.
- Livrarea include consultanță pentru activarea controalelor care generează și colectează evenimente de audit din toate componentele infrastructurii.
- Livrarea include transfer de cunoștințe pentru utilizatori și operatori, susținut de personal certificat de producător pentru instalarea și configurarea soluției.
- Modulul respectă GDPR și Directiva NIS 2 privind nivelul comun ridicat de securitate a rețelelor și sistemelor informatice.