

1. Prezentare generală

Modulul VOGO eBS SIEM colectează, corelează și analizează evenimentele de audit de securitate din întreaga infrastructură IT a organizației — servere, echipamente de rețea, aplicații, baze de date, sisteme de fișiere și servicii de identitate — și transformă alertele în incidente investigate și rezolvate.

VOGO eBS SIEM este un produs comercial integrat, aflat în circuitul comercial, dezvoltat, licențiat și susținut de VOGO Technology: agenții, receptoarele și parsele, motorul de corelare, depozitul online și arhiva, consola, UEBA, managementul cazurilor și motorul de playbook-uri funcționează ca un singur produs, cu o singură licență și un singur contract de suport. Produsul folosește ca biblioteci open source mature: Wazuh, OpenSearch, Shuffle și MISP.

- ▶ **Monitorizarea întregii infrastructuri:** evenimente de audit din toate echipamentele, aplicațiile și bazele de date.
- ▶ **Detectie:** alerte predefinite de bune practici, corelare în mai mulți pași, UEBA și feeduri de securitate.
- ▶ **Răspuns:** incidente, cazuri de investigație colaborative și playbook-uri declanșate automat.
- ▶ **Conformitate:** rapoarte predefinite pentru GDPR, ISO 27001, COBIT, FISMA, SOX și PCI-DSS.

2. Arhitectură, instalare și licențiere

Modulul VOGO eBS SIEM se instalează în infrastructura beneficiarului, ca appliance virtual, și crește odată cu volumul de date.

- ▶ **Instalare on-premise:** rulează în infrastructura beneficiarului; datele de securitate nu ies din organizație.
- ▶ **Appliance virtual:** livrat ca imagine de mașină virtuală, gata de import în platforma de virtualizare, cu sistemul de operare inclus, configurat și întreținut de VOGO prin actualizările produsului.
- ▶ **Arhitectură all-in-one:** toate serviciile și componentele pe aceeași mașină, pentru instalările compacte.
- ▶ **Distribuire pe orizontală:** colectarea, corelarea și depozitarea se pot separa pe noduri suplimentare din infrastructura existentă a beneficiarului, când volumul o cere.
- ▶ **Licență perpetuă:** dimensionată în evenimente pe secundă, de la 5.000 EPS, fără limită de licență pentru volumul depozitului online și al arhivei, care se scalează fără cost suplimentar de licențiere. Licența nu depinde de numărul de noduri: acoperă nodurile colectoare și pe cele de distribuire și funcționarea în centrul de date de rezervă, pe durata activării lui.
- ▶ **Implementare prin configurare:** funcțiile se obțin prin configurarea și personalizarea produsului, fără dezvoltări; toate funcțiile descrise sunt incluse în licență, fără module plătite separat.

3. Colectarea evenimentelor

Modulul VOGO eBS SIEM colectează evenimente prin agenți sau direct din sistemele sursă, din segmente diferite de rețea.

- ▶ **Agenți și colectare fără agent:** agenți pe Windows și Linux sau citire directă din sursă (API, conectori de bază de date).
- ▶ **Fluxuri de evenimente:** Syslog, NetFlow, sFlow și colectare prin sisteme de tip TAP.
- ▶ **Segmente diferite de rețea:** colectori de zonă, de exemplu în DMZ, care transmit către serverul de procesare.
- ▶ **Transport sigur:** agenții transmit datele în format comprimat și criptat, pe canal TLS autentificat.
- ▶ **Integritate:** protecție împotriva alterării datelor la colecție, în tranzit și în repaus, cu coadă locală persistentă.
- ▶ **Colectare filtrată:** agenții filtrează la sursă și execută preprocesare și postprocesare a datelor.
- ▶ **Aplicații și baze de date:** evenimente de aplicații din înregistrări text și din tabele de audit MS SQL, Oracle, MariaDB și PostgreSQL.
- ▶ **Echipamente:** mesaje syslog de la echipamente de rețea, echipamente de tipărire și sisteme de control al accesului.
- ▶ **Sistemul de fișiere:** evenimente de securitate pe fișiere și directoare, pentru Linux și Windows.
- ▶ **Metadata din sisteme terțe:** Active Directory, informații WMI, SNMP și sisteme de management al identităților, folosite în corelare.

- ▶ **Conectori avansați:** fișiere cu evenimente multiline (separate prin newline sau datetime), fișiere XML și fișiere free text; tipurile de evenimente comune sunt identificate automat.
- ▶ **API de integrare:** surse de date noi și logică proprie în colectare, corelare și alertare.

4. Agenți, surse și active

Modulul VOGO eBS SIEM administrează din consolă agenții, sursele de date și inventarul activelor.

- ▶ **Managementul agenților:** instalare, dezinstalare și configurarea parametrilor de funcționare, pentru un agent sau pentru mai mulți agenți în același timp.
- ▶ **Managementul surselor de date:** adăugarea surselor din interfața grafică, cu auto-discovery al surselor.
- ▶ **Auto-discovery al infrastructurii:** sistemele din rețea sunt descoperite și propuse pentru monitorizare.
- ▶ **Asset management de securitate:** nume, nivel de criticitate, adrese IP, adrese MAC, zonă de rețea și vulnerabilități identificate pentru fiecare activ.
- ▶ **Performanța mașinilor:** încărcarea procesoarelor, memoria și spațiul pe discuri ale mașinilor monitorizate, în timp real și istoric pentru minimum 24 de ore.
- ▶ **Starea produsului:** alerte asupra statusului serviciilor componente, cu restaurare automată în caz de oprire, și alerte pe praguri de ingestie și pe numărul de evenimente care așteaptă procesarea.
- ▶ **Evenimente proprii:** produsul generează evenimente pentru interpretarea unor situații specifice.

5. Depozitele de date

Modulul VOGO eBS SIEM stochează datele în două depozite, în formate deschise; datele aparțin beneficiarului.

- ▶ **Arhiva:** păstrare pe termen lung, comprimată, cu rată de compresie de minimum 1 la 20 și mecanisme anti-repudiere — criptarea și semnarea digitală a datelor.
- ▶ **Depozitul online:** date indexate, pentru căutare, corelare, raportare și investigație.
- ▶ **Fără tehnologii proprietare:** formate deschise, accesibile independent de subscripție, mentenanță sau suport.
- ▶ **Import din arhivă:** evenimentele din arhivă se importă în baza online, imediat sau programat, filtrat, din interfața grafică, fără aplicații terțe.
- ▶ **RTBF:** funcția right to be forgotten pentru evenimentele din baza online și din arhivă.
- ▶ **Scalare fără cost de licență:** depozitul online și arhiva cresc oricând, fără cost de licențiere pentru baza de date.
- ▶ **Filtrare la destinație:** drop event, trimitere doar în arhivă sau ocolirea motorului de corelare, cu trimitere doar în baza de date online și în arhivă.
- ▶ **Anonimizare și pseudonimizare:** câmpuri setate manual pe tipuri de surse sau detectate automat după formă și conținut (de exemplu CNP), pentru toate sau numai pentru anumite surse, cu posibilitate de excludere.

6. Căutare, vizualizare și panouri de bord

Modulul VOGO eBS SIEM oferă o interfață web pentru operare și administrare, compatibilă cu orice browser modern (Chrome, Microsoft Edge etc.).

- ▶ **Afișare tabelară:** toate evenimentele colectate, cu filtrări avansate și ordonare; utilizatorii aleg coloanele vizibile.
- ▶ **Vizualizare detaliată:** fiecare eveniment se deschide cu toate câmpurile lui.
- ▶ **Căutare:** operatori logici AND, OR și NOT, expresii complexe cu paranteze imbricate; o căutare după un singur criteriu în toată baza online răspunde în mai puțin de 10 secunde.
- ▶ **Filtre salvate:** filtrele se salvează pentru reutilizare și ca rapoarte, alerte sau dashboard.
- ▶ **Panouri de bord:** agregări grafice ale evenimentelor, configurabile pentru fiecare utilizator în limita permisiunilor, asociate în grupe de panouri, inclusiv pentru tehnologii diferite.
- ▶ **Filtrare comună:** filtrarea și afișarea în toate panourile relativ la un singur criteriu.
- ▶ **Comenzi din evenimente:** ping, traceroute, whois și nslookup rulate direct de la nivelul evenimentelor colectate.

7. Corelare și alertare

Modulul VOGO eBS SIEM include toate evenimentele ingerate în motorul de corelare și alerte predefinite pe scenarii de bune practici.

- ▶ **Alerte out of the box:** alerte de tip best practices pentru multiple tehnologii, pe o gamă largă de tehnologii.

- ▶ **Editor grafic:** alertele se definesc și se editează într-o interfață grafică, intuitivă.
- ▶ **Corelare în mai mulți pași:** din unul sau mai multe evenimente și secvențe de evenimente, cu praguri de activare pe reguli individuale; corelarea jurnalelor pentru toate seturile de date, indiferent de sursă și de tipul de jurnal.
- ▶ **Excludere din corelare:** per sursă de date sau per identificator de tip de eveniment.
- ▶ **Tipuri de reguli:** eveniment singular, evenimente corelate, cumul de evenimente, lipsa unui eveniment, lipsa unui eveniment corelat și reguli particularizate; fiecare regulă combină criterii singulare, corelate și de excludere.
- ▶ **Acțiuni automate:** implicite, pe tehnologii sau personalizate, cu elemente și câmpuri din evenimentele care au generat alerta.
- ▶ **Notificări:** alertele se transmit prin notificări.
- ▶ **Managementul alertelor:** marcare acknowledge one-by-one sau bulk, marcare automată după scorul de gravitate și notarea rezoluției, one-by-one sau bulk.
- ▶ **Export de alerte:** manual, una câte una sau selecție, și automat, cu criterii de export pe alertă sau bulk, prin Email, apeluri de API și syslog.
- ▶ **Redirecționarea evenimentelor:** către soluții terțe, în format brut sau normalizat (syslog, JSON, CEF), filtrat pe surse și tipuri, configurată din interfața grafică cu granularitate până la tip de eveniment și alertă.

8. UEBA și informații despre amenințări

Modulul VOGO eBS SIEM detectează comportamentele care ies din șablonul normal și legăturile cu indicatorii de compromitere.

- ▶ **UEBA:** identificarea și alertarea asupra acțiunilor care ies din șablonul de comportament considerat normal.
- ▶ **Autentificări:** monitorizarea logon-urilor interactive, a logon-urilor automate și a logon-urilor de la stații noi; detectarea automată a autentificărilor suspecte.
- ▶ **VPN:** detecția locațiilor noi de conectare (țări, orașe) pentru fiecare utilizator.
- ▶ **Servicii noi:** detecția serviciilor noi pornite, la nivel de organizație și la nivel de server.
- ▶ **Scor de risc:** pe tip de activ, pe grup de utilizatori și pe tip de evenimente, pentru detecția automată a acțiunilor cu risc mare.
- ▶ **Feeduri de securitate:** integrare nativă a feedurilor open source și pe subscripție, plus feedul propriu VOGO cu IP-uri, domenii și URL-uri malițioase.
- ▶ **Corelare cu IOC:** identificarea automată a sistemelor care comunică cu IOC-uri; alertare pentru traficul către IP-uri malițioase, în curs și retroactiv.
- ▶ **Verificarea IOC în baze:** căutare automată sau manuală, bulk, în baza online și în arhivă, la apariția unor vectori noi de risc.

9. Incidente, investigație și răspuns

Modulul VOGO eBS SIEM oferă un workflow complet pentru analiști, de la alertă la incidentul închis.

- ▶ **Incident management:** lucru colaborativ al personalului de securitate, cu grupuri de destinatari pe mai multe niveluri.
- ▶ **Alocare și escaladare:** alocări automate sau manuale către analiști și escaladarea automată către nivelurile următoare.
- ▶ **Cazuri de investigație:** deschise din alerte și din evenimente, cu acces granular la cazuri.
- ▶ **Playbook-uri:** create și declanșate automat, cu o serie de playbook-uri oferite out-of-the-box.
- ▶ **Vulnerabilități:** integrare nativă prin API cu un modul de scanare de vulnerabilități pentru sisteme, aplicații web și echipamente de rețea, direct din interfața de administrare; rapoartele scannerului intră în corelare, în alertare și în investigație.

10. Raportare și conformitate

Modulul VOGO eBS SIEM include un modul de rapoarte cu rapoarte predefinite și editor.

- ▶ **Rapoarte de conformitate:** GDPR, ISO 27001, COBIT, FISMA, SOX și PCI-DSS, plus rapoarte best practices pentru multiple tehnologii.
- ▶ **Personalizare:** rapoarte noi, editarea rapoartelor existente și a titlurilor; toate rapoartele predefinite pot fi personalizate.
- ▶ **Conținut:** prima pagină rezumă perioada și evenimentele cuprinse; rapoartele conțin grafice.

- **Planificare:** rularea și transmiterea programată a rapoartelor.
- **Export:** PDF, HTML, XLSX, XLS, CSV și XML; definițiile de rapoarte se exportă una câte una sau selecție.
- **GDPR și NIS 2:** implementarea respectă GDPR și Directiva NIS 2 privind securitatea rețelelor și a sistemelor informatice.

11. Securitate, administrare și servicii

Modulul VOGO eBS SIEM separă atribuțiile și înregistrează propriile operații.

- **RBAC:** permisiuni pe roluri pentru accesul în date și pentru configurațiile sistemului; operatorii nu pot modifica datele sistemului.
- **LDAP:** autentificare unitară prin integrarea cu LDAP.
- **Self-audit:** sunt auditate toate operațiunile utilizatorilor și ale serviciilor componente.
- **Instalare și configurare:** prin partenerii certificați VOGO sau prin VOGO; consultanță pentru activarea controalelor de securitate, astfel încât toate componentele să genereze evenimente de audit.
- **Transfer de cunoștințe:** instruirea utilizatorilor și a operatorilor; VOGO acordă certificarea de competențe pentru instalarea și configurarea produsului.
- **Servicii de scalare:** la tarif similar serviciilor de configurare.
- **Suport:** VOGO asigură suportul, actualizările de securitate, regulile și decodoarele noi, actualizările feedului propriu și instruirea; pachetele de actualizare se verifică prin amprenta publicată de VOGO înaintea instalării.

12. Capturi de ecran din VOGO eBS SIEM Console

Capturile de mai jos sunt făcute în VOGO eBS SIEM Console, pe date reale.



Fig. 1 VOGO eBS SIEM Console: indicatorii ultimelor 24 de ore și incidentele corelate

Incidente corelate						
Severitatea	Sursa	Motivul corelării	Alerte	Servere	Prima	Ultima
Critică	203.0.113.47	autentificare reușită după 104 încercări eșuate; aceeași sursă atacă și aplicația web	156	1	15:29:18	16:34:30
Ridicată	192.0.2.81	104 autentificări eșuate (forță brută)	104	1	15:29:18	16:34:30
Ridicată	198.51.100.23	65 cereri de atac către aplicația web	65	1	15:29:18	16:34:30

Fig. 2 Incidente corelate VOGO: autentificare reușită după încercări eșuate și atacuri asupra aplicației web, din aceeași sursă

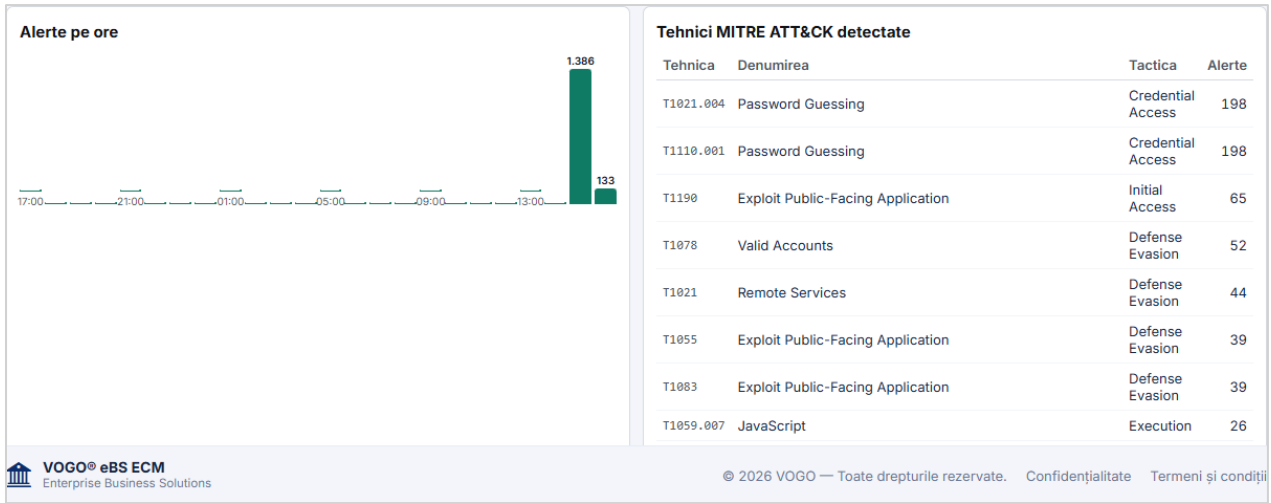


Fig. 3 Alertele pe ore, tehnicile MITRE ATT&CK detectate, regulile declanșate și agenții