Cum vă puteți înrola?

Oferim o **integrare pragmatică, pas cu pas, cu infrastructura dvs. existentă**, fără a necesita investiții suplimentare în echipamente sau licențe. După înregistrare, **SIEMBIOT** garantează confidențialitatea datelor dvs., utilizând procese și documentații validate de **Directoratul Național de Securitate Cibernetică**.

Pasul 1: Creare tenant și stabilire comunicații securizate. Implementăm cloud-ul privat SIEMBIOT, stabilim conexiunea securizată (S2S VPN / P2P) între LAN-ul dvs. și tenantul SIEMBIOT.

Pasul 2: Implementarea agenților de monitorizare: Instalăm agenți dedicați pentru a monitoriza și transmite evenimentele de securitate către SIEM-ul dvs. dedicat. Din acest moment, puteți începe să utilizați portalul SIEMBIOT, să monitorizați activele, alertele, vulnerabilitățile și amenințările.

Pasul 3: Implementarea dispozitivelor dedicate (Opțional): Instalăm mini-appliances în locațiile cheie pentru colectarea metricilor suplimentare de trafic și evenimente de rețea, îmbunătățind corelarea datelor în SIEM.

SIEMBIOT CyberAcademy

SIEMBIOT CyberAcademy oferă atât companiilor private, cât și mediului universitar o platformă avansată de training, concepută pentru a dezvolta abilități esențiale în protejarea infrastructurilor IT:

- **Cursuri interactive,** pentru toate nivelurile – de la bazele securității cibernetice până la tehnici avansate de protecție,
- **Scenarii reale și simulări,** și simulări pentru o pregătire practică,
- **Acces la experți în cybersecurity,** și sesiuni personalizate,
- **Certificări recunoscute** care atestă nivelul de competență al echipei tale.

Protejează-ți afacerea

Testează ACUM și beneficiază de 6-12 luni de acces GRATUIT!

Profită de oportunitatea de a utiliza **tehnologii avansate de protecție** și îmbunătățește-ți **postura de securitate**, conform cerințelor **Directivei NIS2**.

Cere un DEMO:

expertware.net
info@expertware.net
Expertware

Înscrie-te și începe perioada de gratuitate!
*Locurile sunt limitate!

siembiot.eu
siembiot@expertware.net
Siembiot

SIEMBIOT®

Powered by expertware

Securitate cibernetică end-to-end accesibilă pentru toate companiile

Programează un DEMO și transformă securitatea cibernetică a afacerii tale!

Misiunea noastră este să creștem reziliența națională și regională împotriva atacurilor cibernetice, sprijinind afacerile printr-o platformă de apărare și cercetare de nouă generație, flexibilă, modulară și reziliență.

Co-funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE
DIRECTORATUL NAȚIONAL DE SECURITATE CIBERNETICĂ

DESPRE NOI

Proiectul **SIEMBIOT**, dezvoltat de **Expertware** în parteneriat cu **Directoratul Național de Securitate Cibernetică**, a câștigat cel mai mare grant din cadrul programului de fonduri de inovare pentru securitate cibernetică **DIGITAL-EC-CC-2022-CY BER-03** finanțat de Uniunea Europeană, fiind singurul consorțiu 100% românesc.

Expertware este o companie de servicii IT, specializată în **securitate cibernetică** și operarea **Security Operations Centers (SOC),** având expertiză în **AI și machine learning**, dezvoltare full-stack, **arhitectură IT** și optimizarea afacerilor.

De **19 ani**, Expertware lucrează cu clienți mari și foarte mari din **Vestul Europei**, activând în domenii precum **bancar, asigurări, energie și telecomunicații**. Cu **99,99% dintre clienți având afaceri de peste 1 miliard EUR anual**, am perfecționat expertiza necesară pentru a crea **SIEMBIOT** – o soluție completă de **securitate cibernetică end-to-end**, accesibilă și eficientă, destinată organizațiilor care nu dispun de resursele marilor bănci sau operatorilor de telecomunicații.

Vrei să te încadrezi în standardele setate de Directiva NIS2? Accesează acum în mod gratuit platforma SIEMBIOT!

SIEMBIOT este o soluție complementară pentru detectarea și prevenirea atacurilor cibernetice, care te ajută să îndeplinești cerințele **Directivei NIS2**. Platforma inovativă, flexibilă și modulară te protejează împotriva vulnerabilităților, atacurilor zero-day și a erorilor de configurare.

Ce oferă SIEMBIOT?

- **Tenant privat SIEMBIOT:** Stocarea securizată și procesarea datelor într-un **data lake** dedicat.
- **SIEM dedicat, open-source**, cu peste **30 de conectori** pentru a extrage, îmbogăți și corela evenimente și jurnale relevante.
- **Peste 700 de reguli de detectare automată** a amenințărilor, aplicabile tuturor evenimentelor colectate în data lake-ul tău.
- **Threat Intelligence personalizat –** Acces la **> 15 miliarde de indicatori CTI**, cu integrare zilnică a **15.000 de indicatori noi**.
- **Audit de configurare** - Validarea securității sistemelor de operare conform standardelor SCAP și CIS (pentru Windows și Linux).
- **Explorarea activelor** din infrastructura ta din multiple unghiuri – Scanări de rețea bazate pe agenți și cloud.
- **Scanări și corelări continue ale vulnerabilităților** - Detectare și analiză folosind **agenți, scanări de rețea și evaluări manuale**.
- **Rapoarte pentru management** - Dashboard-uri în timp real cu alerte și detalierea incidentelor de securitate.
- **Modul de răspuns la incidente** - Urmărirea, gestionarea și calificarea alertelor de securitate cibernetică ca incidente de securitate.
- **Cercetare și instruire –** Interogări complexe **DQL** pe evenimente eterogene și crearea de seturi de antrenament **SOC (CTF, provocări).**
- **Data lake anonimizat** pentru instruirea analiștilor de securitate.

Servicii Premium Suplimentare

Dacă nu aveți echipe de securitate pentru a gestiona platforma SIEMBIOT, vă oferim echipe de securitate dedicate/ partajate pentru:

Răspuns la incidente L1 24/7: Echipa de nivel 1 monitorizează și califică alertele nesoluționate automat, corelând OSINT și CTI pentru a deschide incidente de securitate în cazul atacurilor confirmate.

Răspuns la incidente L2 24/7: Echipa L2 continuă eforturile echipei L1 pentru a găsi soluții sau măsuri de atenuare, urmărind implementarea acestora cu sau fără suportul echipelor operaționale ale clientului.

Simularea avansată a atacurilor L3: Realizăm simulări și atacuri orchestrate pentru a identifica vulnerabilități zero-day și configurări greșite, pentru a preveni posibile breșe de securitate.

Remedierea sau atenuarea vulnerabilităților: Prioritizăm riscurile și implementăm soluțiile necesare, inclusiv actualizări, modificări de configurare și ajustarea regulilor firewall-ului.

