



certSIGN

SERVICII ȘI SOLUȚII DE SECURITATE CIBERNETICĂ



De ce certSIGN?

certSIGN acoperă întregul spectru al securității cibernetice, de la analiză și evaluare, până la implementare, testare, monitorizare și suport operațional.

Serviciile specializate sunt combinate cu **soluții tehnologice consacrate** și **servicii profesionale asociate**, pentru a construi arhitecturi de securitate coerente, eficiente și ușor de gestionat. Accentul este pus pe claritate, responsabilitate și un parteneriat pe termen lung, nu pe soluții generice sau implementări formale.

Membrii echipei certSIGN dețin **certificări profesionale** recunoscute la nivel internațional, care atestă atât competențele tehnice, cât și experiența practică, plus respectarea standardelor de conduită profesională în domeniul securității cibernetice.



certSIGN



Servicii NIS2

1. Notificare / Înregistrare DNSC și Evaluare nivel de risc

Serviciul ajută organizația să pregătească și să transmită notificarea către DNSC și să finalizeze corect procesul de evaluare a nivelului de risc, asigurând conformitatea cu cerințele legale în vigoare.

2. Analiză Inițială

Serviciul oferă o analiză a măsurilor de securitate existente în organizație, în vederea identificării acțiunilor necesare conformării cu OUG nr. 155/2024, precum și a pașilor practici de urmat de către companie.

3. Responsabil NIS "as a Service"

Serviciul ajută organizația prin externalizarea rolului de responsabil NIS, incluzând coordonarea comunicării cu DNSC, supravegherea măsurilor de securitate și raportarea periodică către conducere.

4. Evaluare nivel de maturitate

Specialiștii certSIGN ajută organizația să își evalueze nivelul de maturitate în securitate cibernetică, stabilind totodată măsurile de remediere care se impun, cu respectarea reglementărilor legislative în vigoare.

5. Implementare măsuri de securitate

Serviciu de consultanță pentru elaborarea sau actualizarea și adaptarea politicilor și procedurilor de securitate cibernetică existente, în vederea mapării la reglementările curente în domeniu.

Respectarea cerințelor Directivei NIS2 este fundamentală pentru companiile care gestionează infrastructuri critice sau servicii esențiale.

Prin serviciile complete de consultanță NIS, certSIGN ajută organizațiile vizate să asigure conformitatea cu legislația europeană și să își întărească securitatea rețelelor și a sistemelor informatice, garantând un nivel ridicat de protecție, încredere și reziliență digitală.

Servicii și soluții de securitate cibernetică certSIGN



Servicii de Audit / Consultanță

1. Audit NIS2

Serviciul ajută organizația să identifice gradul de conformitate față de cerințele OUG nr. 155/2024, primind de asemenea recomandări adecvate în vederea reducerii riscurilor și atingerii nivelului impus prin cerințele NIS2.

2. Audit Norma 4 ASF

Acest serviciu sprijină companiile autorizate/avizate/înregistrate, reglementate și/sau supravegheate de către ASF (Autoritatea de Supraveghere Financiară) în implementarea prevederilor Normei 4 ASF, respectiv identificarea, prevenirea și reducerea impactului potențial negativ al riscurilor operaționale generate de utilizarea tehnologiei informației și comunicărilor la nivel de oameni, procese, sisteme și mediu extern, inclusiv pentru fapte ce țin de criminalitatea informatică.

3. Consultanță ISO 27001

Serviciul conține activități specifice necesare implementării ISO27001 în cadrul unei companii. De asemenea include evaluarea situației actuale și propunerea măsurilor ce sunt necesare pentru implementarea unui sistem de management al securității informațiilor care ajută organizația să-și stabilească și să realizeze politicile de securitate informațională și obiective în concordanță cu cerințele legale aplicabile activității desfășurate.



Servicii tip SOC / CSIRT

1. Monitorizarea de Securitate

Monitorizarea alertelor generate de soluțiile de securitate ale companiei, trierea și investigarea alertelor, alertarea beneficiarului în cazul detectării unui posibil incident de securitate, suport pe durata răspunsului la incident din perspectiva investigării alertelor monitorizate.

Pentru prestarea serviciului este necesară utilizarea unei soluții SIEM, puse la dispoziție de beneficiar sau care poate fi implementată de certSIGN.

2. Teste de Penetrare

Realizarea unei testări a securității la nivelul rețelei IT și a sistemelor informatice ale companiei prin scanarea componentelor acestora în vederea identificării vulnerabilităților existente și identificarea posibilității de exploatare a acestora.

Serviciul ajută organizația să testeze rezistența sistemelor la atacuri cibernetice simulate și să descopere riscurile ascunse.

3. Scanare de Vulnerabilități

Realizarea unei testări a securității la nivelul rețelei IT și a sistemelor informatice ale companiei prin scanarea componentelor acestora în vederea identificării vulnerabilităților existente.

Serviciul ajută organizația să identifice vulnerabilitățile tehnice din rețele și sisteme și să primească recomandări de remediere.



Unified Endpoint Management (UEM)

1. Zimperium

Soluție de securitate mobilă de tip Mobile Threat Defense (MTD), bazată pe inteligență artificială, care detectează și previne atacurile în timp real – inclusiv malware, phishing și vulnerabilități de rețea. Funcționează direct pe dispozitiv, fără a compromite confidentialitatea utilizatorului. Creată pentru a proteja endpoint-urile mobile împotriva amenințărilor moderne – de la aplicații malițioase, la atacuri de rețea și exploatari de vulnerabilități.

2. Trust4Mobile

Aplicație de comunicare securizată, dezvoltată de certSIGN, care oferă mesagerie instant, apeluri și schimb de fișiere protejate prin criptare avansată (criptare dublă, simetrică și asimetrică), bazată pe certificate digitale. Aplicația este concepută pentru organizații care au nevoie de un canal de comunicare privat, conform cu cerințele de securitate și confidențialitate ale mediilor corporate și guvernamentale.

3. Samsung Knox Suite

Samsung Knox oferă un nivel avansat de securitate pentru dispozitivele mobile din mediul de business. Conceput pentru protecția completă a endpoint-urilor mobile, Knox asigură criptare la nivel hardware, control granular al politicilor de securitate și gestionare centralizată a dispozitivelor. Este soluția ideală pentru companiile care doresc să prevină accesul neautorizat, pierderile de date și atacurile cibernetice, menținând în același timp productivitatea mobilă. O alegere optimă pentru flote mari de dispozitive în medii corporate sau guvernamentale.

4. Ivanti

Platformă unificată de Mobile Device Management, care combină automatizarea IT, conformitatea și protecția datelor într-o singură interfață. Asigură onboarding rapid, politici de securitate flexibile și integrare facilă cu infrastructura IT existentă.

Oferind vizibilitate end-to-end, control avansat al politicilor și protecție împotriva amenințărilor cibernetice, Ivanti ajută organizațiile să prevină breșele de securitate și să asigure conformitatea, indiferent de locația sau tipul dispozitivului. Mobilitatea rămâne sigură, controlată și eficientă.

5. SOTI

Soluție robustă de Enterprise Mobility Management (EMM), care permite gestionarea centralizată a dispozitivelor mobile, indiferent de platformă sau locație. Oferă control granular, actualizări de la distanță și monitorizare în timp real.

6. Google Zero-Touch

Google Zero-Touch Enrollment este o metodă oferită de Google pentru configurarea automată și în masă a dispozitivelor Android destinate firmelor și instituțiilor. Ea permite ca telefoanele și tabletele Android compatibile să fie livrate direct către angajați gata configurate, fără ca departamentul IT să fie nevoit să le pregătească manual.

Pentru toate platformele de mai sus, certSIGN oferă servicii de suport, implementare și mentenanță.

Servicii și soluții de securitate cibernetică certSIGN



Security Awareness

KnowBe4

KnowBe4 este cea mai mare platformă integrată la nivel mondial pentru training-uri de awareness combinate cu atacuri simulate de phishing. Soluția oferă instruirea angajaților prin programe interactive de conștientizare în securitate, acoperind toate subiectele esențiale din domeniul securității cibernetică. Include simulări realiste de phishing, testarea periodică a vigilenței utilizatorilor și rapoarte detaliate care măsoară nivelul de conștientizare și progresul în timp.



certSIGN Academy

Cursuri de securitate

Destinate specialiștilor din domeniul IT, structurate pe niveluri diferite de competențe, cu certificare recunoscută la nivel internațional după absolvirea examenelor:

- **CompTIA PenTest+**, pentru profesioniștii în securitate cibernetică, nivel intermediar
- **CompTIA Cybersecurity Analyst (CySA +)**, pentru analiștii de securitate cibernetică, nivel intermediar
- **Security+ 501**, atestarea abilităților de bază necesare pentru îndeplinirea atribuțiilor specifice funcțiilor din domeniul securității IT
- **Certified Ethical Hacker**, atestarea cunoașterii celor mai noi instrumente, tehnici și metodologii de hacking de nivel comercial utilizate atât de hackeri, cât și de profesioniștii în securitatea informațiilor

Întrebări suplimentare despre serviciile și soluțiile de securitate cibernetică certSIGN?

Echipa noastră vă stă la dispoziție, pentru a descoperi împreună instrumentele optime adaptate specificului organizației!

