safetech

Your trusted security partner

PROFIL COMPANIE

safetech
Your trusted security partner

CINE SUNTEM?

- Safetech Innovations a fost înființată în 2011, peste 30 angajați, peste 100 clienți, peste 250 proiecte de securitate informatică finalizate cu succes în România, Uniunea Europeană, Statele Unite, Moldova, etc.
- Companie dedicată 100% Securității Informației, din România.
- Singura companie înființată de experți în Securitatea Informației, cu o experiență deosebită în domeniul Financiar – Bancar, din România.
- Fondatorul, deținătorul și operatorul unuia dintre cele două Centre **Private** operaționale de Monitorizare și Răspuns la Incidente de Securitate Cibernetică, din Europa de Est – **STI CERT**
- Una dintre cele mai competente si certificate echipe de Penetration Testing din România si Sud –Est UE
- Portofoliu nostru conține cele mai inovative soluții de securitate cibernetică din România

safetech
Your trusted security partner

MISIUNE ȘI STRATEGIE

SAFETECH INNOVATIONS adresează toate cele 3 componente majore ale securității unei companii:

CONFIDENȚIALITATE – SAFETECH INNOVATIONS a implementat pentru **Agenția Uniunii Europene pentru Securitatea Rețelelor și a Informațiilor (ENISA)** proiectul "Formalizarea unui cadru standardizat privind măsuri de securitate adecvate pentru companiile mici si mijlocii pentru prelucrarea datelor cu caracter personal". Ghidul poate fi accesat de la link-ul urmator: https://www.enisa.europa.eu/publications/guidelines-for-smes-on-the-security-of-personal-data-processing

INTEGRITATE – suntem prima companie din România și printre puținele companii din Europa, înregistrată pe lista partenerilor de încrede ai NATO **(NATO Trusted Industry Partner Roster)** și membru activ în **Parteneriatul NATO - Industrie în domeniul Securității Cibernetice (NICP-NATO Industry Cyber Partnership)**. Totodată, compania deține **Codul NCAGE (NATO Commercial And Governmental Entity)** care certifică faptul că SAFETECH INNOVATIONS îndeplinește toate cerințele necesare pentru organizarea și desfășurarea de activități în domeniul apărării.

DISPONIBILITATE – **STI CERT** a fost conceput pentru a sprijini companiile, instituțiile și organizațiile care doresc să fie protejate împotriva atacurilor cibernetice prin monitorizare continuă (24/7), răspuns prompt și recuperare rapidă după incidentele de securitate cibernetică.

safetech
Your trusted security partner

DIFERENTIATORI CHEIE SAFETECH INNOVATIONS

Prin profesionalism, solutii practice si eficiente din punctul de vedere al costurilor, **SAFETECH INNOVATIONS** s-a remarcat intr-un timp scurt pe piata Securitatii Informatiei din Romania.
Ca o recunoastere a competentelor pe aceasta tematica, echipa **SAFETECH INNOVATIONS** a fost invitata sa participe si a participat la exercitiile cibernetice organizate de catre **NATO: CYBER COALITION 2015**, **CYBER COALITION 2016, CYBER COALITION 2017** si **CYBER EUROPE 2016**, organizat de catre **Agentia Uniunii Europene pentru Securitatea Retelelor si a Informatiilor (ENISA).**

SAFETECH INNOVATIONS a implementat o serie de proiecte de penetration testing/vulnerability assessment/ethical hacking la peste 15 banci si institutii financiare si de asigurari din Romania si din alte tari din Europa precum: **Raiffeisen Leasing, Raiffeisen Bank, OTP Bank, BRD Groupe Societe Generale, Volksbank, ING Life Assurance, Alpha Bank, Idea Bank, Legal & General** etc.

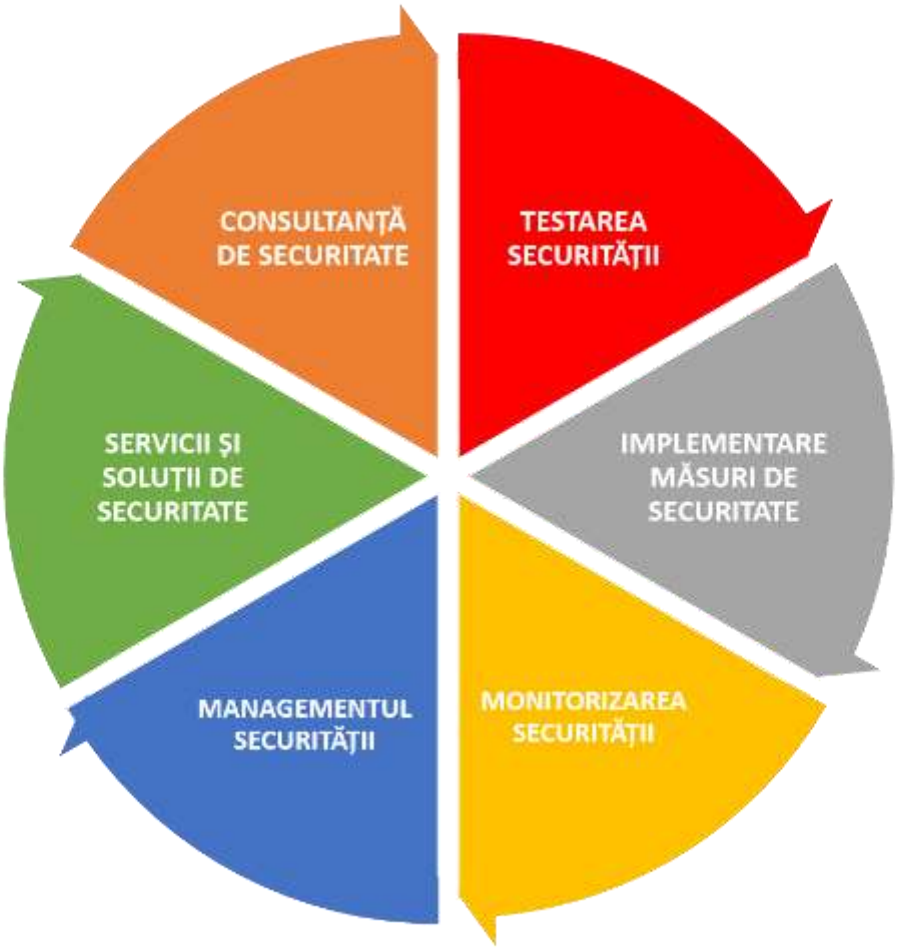
De asemenea, STI CERT este acreditat de către organizații internaționale (ex. The Trusted Introducer Service, https://www.trusted-introducer.org/directory/teams/sticert.html).

safetech
Your trusted security partner

CERTIFICĂRI RELEVANTE

safetech
Your trusted security partner

CUM VĂ PUTEM AJUTA?

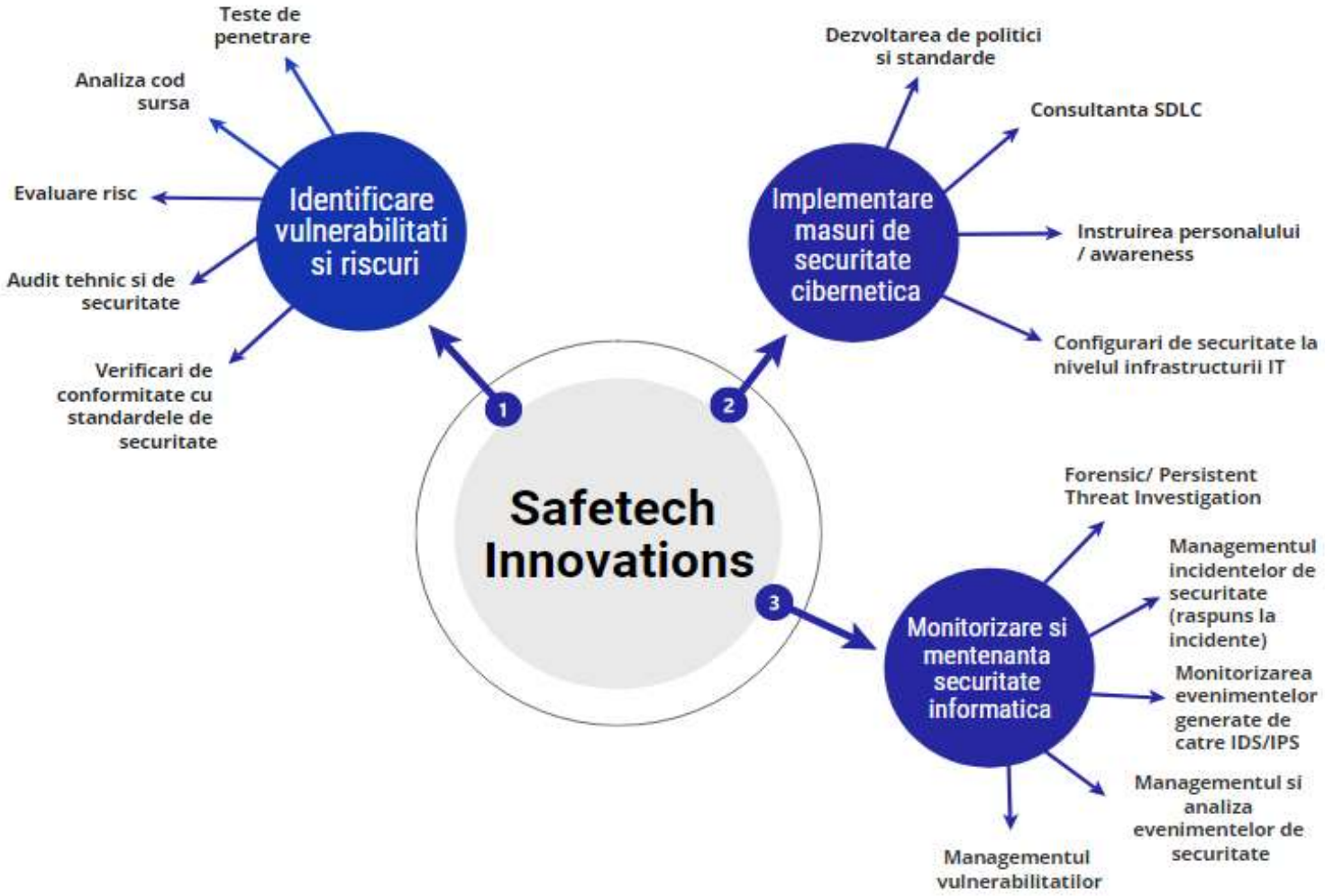


1. Consultanță de securitate
2. Testare de securitate
3. Implementare măsuri de securitate
4. Monitorizare de securitate
5. Managementul securității
6. Servicii & soluții de securitate

safetech
Your trusted security partner

PARTENER UNIC PENTRU SERVICII SI SOLUTII DE SECURITATE

Portofoliul de servicii de securitate cuprinde:



MONITORIZARE CONTINUĂ ȘI RĂSPUNS LA INCIDENTE DE SECURITATE

Oferim pachete de servicii care pot fi personalizate în funcție de nevoile clienților:

- **DIAGNOZĂ**: Forensic / Persistent Threat Investigation; Compliance checking – verficare conformitate cu standard international; Dezvoltare / actualizare standard si politici de securitate

- **INTERVENȚIE**: Remote administration echipamente de securitate informatica; Managementul incidentelor de securitate; Managementul si analiza evenimentelor (SIEM); Hardening – analiza configuratiilor de securitate a infrastructurii.

- **MONITORIZARE 24/7**: Managementul vulnerabilitatilor si urmarire process patch-management; Monitorizarea evenimentelor generate de catre IDS / IPS; Monitorizarea sistemelor antivurus (raport virusi identificati si eliminate sau neeliminati); Status monitoring disponibilitatea sistemelor; Raportarea lunara a nivelului de securitate (vulnerabilitati, incidente, metrici, riscuri)

safetech
Your trusted security partner

SOLUȚII INOVATIVE DE SECURITATE CIBERNETICĂ

safetech
Your trusted security partner

INOVARE ÎN CERCETARE ȘI DEZVOLTARE

Partener în securizarea proiectelor strategice.	Dosarul de Sănătate Electronic (DES)
	Centrul de Guvernare Electronică (E-Government) al Republicii Moldova
Proiecte finanțate de către UE.	Universitatea “Ștefan cel Mare” din Suceava – Laborator de Securitate Cibernetică
	ENISA – Recomandări pentru IMM în securitatea și procesarea Datelor cu Caracter Personal.
Membru în Clustere	Prima companie de Securitatea Informației invitată să adere la **Măgurele High Tech Cluster (MHTC)**
	Danube Cyber Security Alliance - DACSA – Membru fondator și coordonator
	SMART ALLIANCE – Membru fondator
	CLARA KET Cluster – Membru fondator Centru de Excelență al UE în Laser și Radiație.
Cooperare cu Institute de Cercetare și Universități din România	Universitatea Națională de Apărare "Carol I" (UNAp)
	Universitatea “Politehnica” București (UPB)
	Institutul Național de Cercetare – Dezvoltare în Informatică (ICI)

safetech
Your trusted security partner

REFERINTE SERVICII ȘI SOLUȚII DE SECURITATE

Administrație publică

Financiar - Bancar

Infrastructură critică – Energie/ Utilități

Companii internaționale

Integratori IT

safetech
Your trusted security partner

PROVOCĂRILE 2018

REGULAMENTUL (UE) 2016/679 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date

DIRECTIVA (UE) 2016/1148 privind măsuri pentru un nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în Uniune

“masuri adecvate tehnice si organizatorice”

safetech
Your trusted security partner

Masuri ADECVATE

=

Managementul Securitatii

safetech
Your trusted security partner

safetech
Your trusted security partner

DIRECTIVA NIS

Directiva NIS va impune in Romania

- Cerințele minime de securitate (CAPITOLUL IV, Secțiunea 1)
- Notificarea incidentelor de securitate (CAPITOLUL IV, Secțiunea 2)
- Managementul incidentelor de securitate (CAPITOLUL IV, Secțiunea 3)
- amendă în cuantum de până la 2% din cifra de afaceri, iar, în cazul unor încălcări repetate, cu amendă în cuantum de până la 5% din cifra de afaceri.

Trebuie implementata in legislatia pana in 10 mai 2018 (inainte de intrarea in forta a GDPR)

MINISTERUL COMUNICAȚIILOR ȘI SOCIETĂȚII INFORMAȚIONALE

Legea care va implementa directiva inca este in stadiu de proiect la MCSI

safetech
Your trusted security partner

DOMENIU DE APLICABILITATE

DIRECTIVA NIS

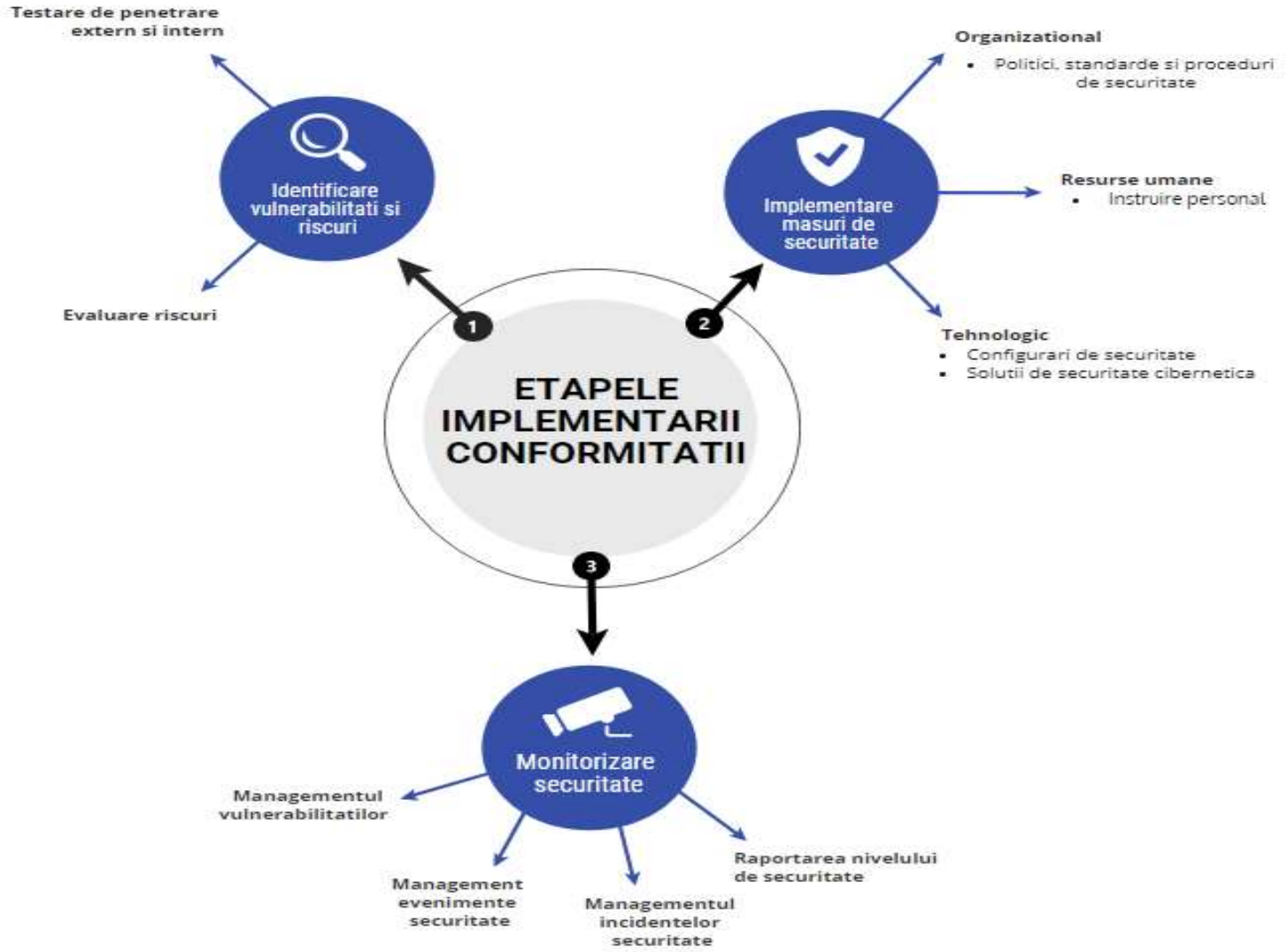






safetech
Your trusted security partner

ETAPELE IMPLEMENTARII CONFORMITATII



safetech
Your trusted security partner

SOLUTIA STI CERT

Sources of Threat Intelligence

STI CERT
Research Team

STI CERT

Nivel de escaladare superior sau
Management end to end

DIRECTIVA NIS

Notificarea incidentelor de securitate (CAPITOLUL IV, Secțiunea 2)

Managementul incidentelor de securitate (CAPITOLUL IV, Secțiunea 3)

Security Operation Center Client

Analisti Securitate

Linia de business

IBM Radar

DARKTRACE

- Security analytics
- Management Vulnerabilitati
- Detectie anomalii securitate

- Detectie anomalii securitate OT (scada)
- Management Vulnerabilitati
- Vizibilitate operationala

CyberX

Retea de Business IT

Senzor

Retea Operationala (Scada)

safetech
Your trusted security partner

safetech
Your trusted security partner

safetech
Your trusted security partner

Noul Regulament GDPR, un set de reguli care le schimbă pe cele aflate în vigoare, după 20 de ani!

- GDPR se va aplica direct in toate statele membre UE
- Noul set de reguli intra in efect incepand cu 25 Mai

- Vor fi nevoiti sa se conformeze atat cei care proceseaza cat si care stocheaza sau transfera date, indifferent de locatie

- GDPR :
  - Acordă drepturi sporite persoanelor vizate
  - Adăugă obligații suplimentare pentru operatorii de date și procesatori
  - Introduce o evaluare a impactului asupra vieții private ca o obligație de diligență obligatorie

safetech
Your trusted security partner

GDPR

De ce este important **GDPR**? Creșterea drepturilor și a obligațiilor, plus o creștere semnificatiă mai a amenzilor pentru încălcări

Drepturi consolidate pentru persoanele vizate	
Obiectul procesării și profilării	• Cu excepția cazului în care controlorul demonstrează motive convingătoare pentru prelucrare și dacă nu există consimțământul clienților sau autorizație prin contract sau lege
Dreptul de a fi “uitat”	• Atunci când datele nu mai sunt necesare sau persoanele vizate își retrag consimțământul
Portabilitatea datelor	• În format electronic și transmiterea directă către un alt controlor
Solicitări de acces la subiecte	• **Drepturile de a solicita date personale pe care controlorii le stochează**

Obligații suplimentare ale controlorilor / prelucrătorilor de date	
Privacy by Design și by Default	• Produsele noi trebuie să include protectia datelor cu caracter personal, prin design și implicit. Evaluarea impactului asupra vieții private (PIA)
Registru de date	• Controlorii și procesatorii trebuie să mențină un registru care să identifice și să documenteze activitățile cheie de prelucrare a datelor
Consimțământ	• În cazul în care consimțământul este invocat pentru prelucrarea unor categorii speciale de date cu caracter personal, este necesar consimțământul explicit
Notificare breșă de securitate	• Autoritățile de supraveghere și persoanele vizate trebuie informate despre o încălcare a datelor cu caracter personal în termen de 72 de ore
Ofițer Protecția Datelor	• Controlorul și procesatorul desemnează, în anumite cazuri, un responsabil cu protecția datelor (DPO)

safetech
Your trusted security partner

Principii fundamentale

Privacy by Design

încearcă să prevină evenimentele invazive înainte ca acestea să se întâmple, în loc să aștepte apariția unor probleme, care ar trebui apoi să fie tratate reactiv

safetech
Your trusted security partner

CUM VĂ PUTEM AJUTA ÎN VEDEREA CONFORMĂRII ACTIVITĂȚII COMPANIEI CU PREVEDERILE GDPR?

ETAPA I – Analiza activității actuale a companiei din perspectiva riscurilor de securitate

În cadrul acestei etape vom identifica modul în care compania prelucrează datele cu caracter personal și vom stabili în ce măsură activitatea pe care o desfășoară la momentul actual, în raport și de activitățile viitoare preconizate, este conformă cu prevederile GDPR, precum și riscurile asupra securității operațiunilor de prelucrare a datelor.

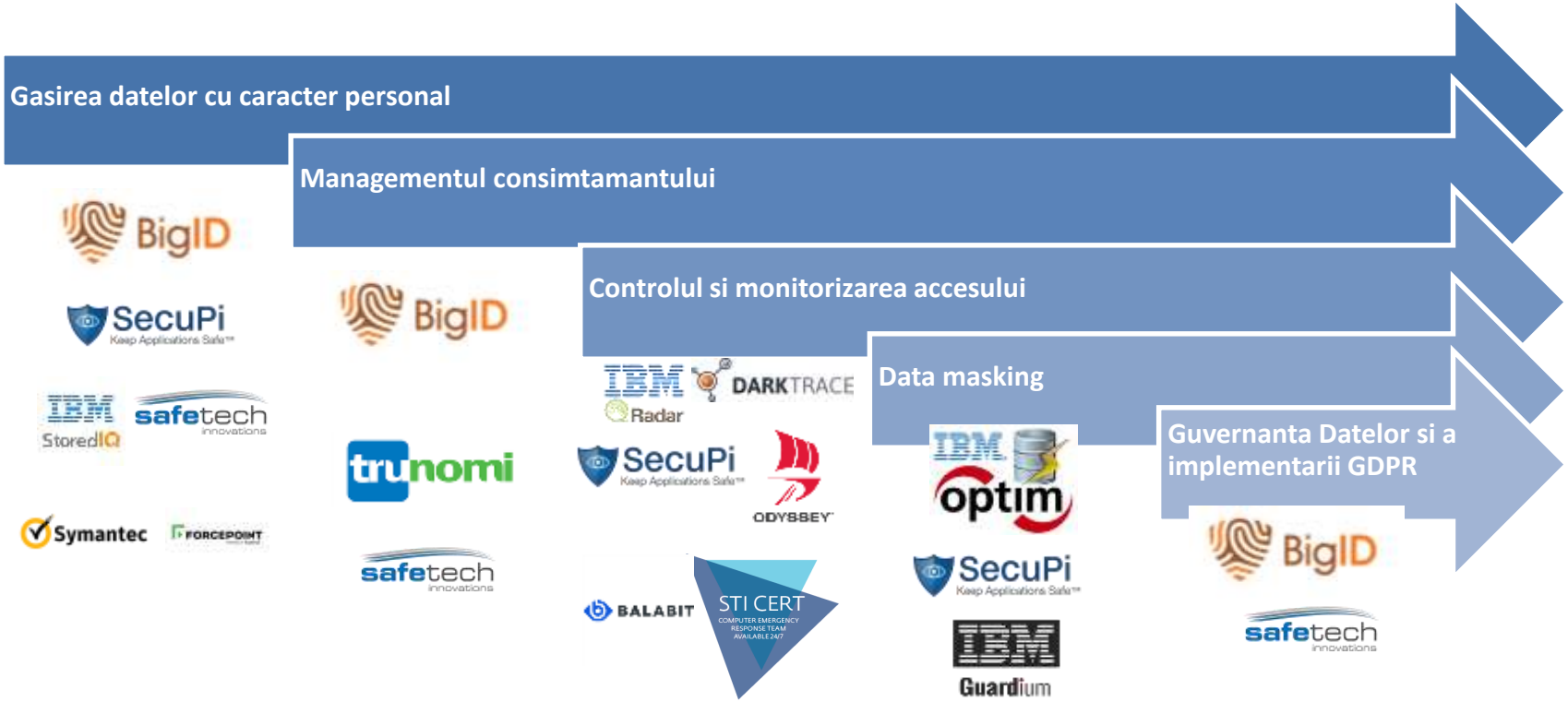
safetech
Your trusted security partner

IDENTIFICAREA NIVELULUI DE CONFORMITATE ȘI A RISCURILOR DE SECURITATE A DATELOR

- **Identificarea** categoriilor de **date cu caracter personal** prelucrate și **scopul prelucrării acestora**.
- Identificarea proceselor de business care utlizează aceste date
- Identificarea fluxurilor de date (colectare, procesare, stocare, transfer și arhivare)
- Identificarea sistemelor informatice utilizate pentru prelucrarea datelor
- Identificarea măsurilor de securitate existente precum și rezistența acestora la atacurile informatice
- **Analiza de risc**: identificarea amenințărilor la adresa datelor personale și evaluarea nivelului de risc în funcție de măsurile de securitate implementate și a vulnerabilităților identificate.

safetech
Your trusted security partner

CATALIZATORI DE IMPLEMENTARE RAPIDA IN MEDII COMPLEXE DE BUSINESS



safetech
Your trusted security partner

GDPR

ANALIZA DE IMPACT ASUPRA CONFIDENTIALITATII datelor cu caracter personal in sistemele informatice utilizate pentru prelucrarea datelor, **măsurile de securitate existente** și **rezistența acestora la atacurile cibernetice**.

În raport cu elementele identificate, de eventualele lipsuri sau neconcordanțe semnalate, în continuare vom elabora **un raport** ce va cuprinde **toate măsurile** și **soluțiile de securitate a datelor** ce trebuie implementate de către companie în vedere conformării cu noile cerințe.

safetech
Your trusted security partner

PLAN DE MĂSURI

1. Guvernanta protectiei datelor cu caracter personal
2. Inventarierea datelor cu caracter personal si mecanismele de transfer
3. Politica interna de protectie a datelor cu caracter personal
4. Protectia datelor personale in cadrul operatiunilor de procesare
5. Programul de instruire si constientizare a angajatilor
6. Managementul riscului privind securitatea informatiilor
7. Managementul riscului privind entitatile externe (transfer de informatii)
8. Implementarea conceptului “Privacy by Design” in cazul unor noi prelucrari de date
9. Managementul incidentelor privind protectia datelor personale
10. Monitorizarea accesului la informatii si a atacurilor cibernetice

safetech
Your trusted security partner

ETAPA II - IMPLEMENTAREA MĂSURILOR DE SECURITATE

Misiunea noastră este de a oferi clienților **soluții de securitate complete și adaptate specificului fiecărei companii**, prin care să asigurăm implementarea noului cadru legal și creșterea nivelului de securitate în domeniul prelucrării datelor cu caracter personal.

Implementarea măsurilor de securitate cibernetică se realizează pe 3 nivele:

1.Organizațional
- Dezvoltarea de politici, standarde și proceduri de securitate si protectie date cu caracter personal

2. Resurse umane
- Instruirea personalului în ceea ce priveste protectia datelor cu caracter personal si securitatea informatiei

3. Tehnologic
- Configurarea infrastructurii IT si implementarea de solutii conform planului de masuri

safetech
Your trusted security partner

ETAPA III - MENTENANTA SI MONITORIZARE

VERIFICAREA PERIODICĂ A POLITICILOR DE PRELUCRARE ȘI MONITORIZAREA SECURITĂȚII DATELOR CU CARACTER PERSONAL

După implementarea tuturor măsurilor tehnice impuse de **Regulament**, venim în ajutorul clienților noști cu **măsuri de mentenanță** pentru a reduce riscurile generate de: distrugerea, pierderea, modificare, prelucrarea sau divulgarea neautorizată, accesul neautorizat la datele cu caracter personal, precum cele care ar afecta securitatea datelor.

STI CERT
COMPUTER EMERGENCY RESPONSE TEAM AVAILABLE 24/7

Monitorizare 24/7 a nivelului de securitate, servicii de identificare a breșelor de securitate, managementul vulnerabilităților, monitorizarea continuă a jurnalelor generate de echipamentele de comunicații, a serverelor și stațiilor de lucru în scopul detectării intruziunilor, generarea alertelor și a avertizărilor referitoare la evenimentele de securitate, precum și managementul incidentelor de securitate;

ETAPA III - MENTENANTA SI MONITORIZARE

Intervenție și răspuns la incidentele de securitate raportate de către companie sau identificate de experții noștri IT, servicii privind investigarea cauzei care a dus la apariția respectivului incident și un plan de măsuri pentru redresarea cât mai rapidă a companiei și preîntâmpinarea unor evenimente similare.

- Monitorizare evenimente (detectare intruziune rețea, detectare intruziune endpoint)
- Răspuns la incidente de Securitate
- Investigarea incidentelor de Securitate
- Managementul vulnerabilităților
- Verificarea conformității cu standardele de Securitate
- Protejarea aplicațiilor compromise și web
- Întărirea și revizuirea periodică a configurării de securitate (rețea, sistem de operare) și propunere măsuri de Securitate
- Administrare soluții de securitate

safetech
Your trusted security partner

”SISTEM INFORMATIC INTEGRAT PENTRU MANAGEMENTUL ACTIVITĂȚILOR”

- **SAFETECH ESTE IMPLICAT IN REALIZAREA TUTUROR CELOR 10 MODULE:**
- **M1. MODUL DE MANAGEMENT INTEGRAT DE IDENTITATE ȘI DREPTURI DE ACCES. SISTEM UNIC DE AUTENTIFICARE.**
- **M2. MODULUL DE MANAGEMENT AL PROCESELOR, PROCEDURILOR ȘI ACTIVITĂȚILOR**
- **M3. MANAGEMENTUL PROGRAMELOR ȘI PROIECTELOR INSTITUȚIEI**
- **M4. MANAGEMENTUL RESURSELOR INSTITUȚIEI**
- *- M5. MANAGEMENTUL DOCUMENTELOR ȘI AL COMUNICAȚIEI*
- *M6. HĂRȚI (GIS)*
- *M7. ANALITICS ȘI DASHBOARD (BI)*
- *M8. NOTIFICĂRI*
- *M9. MONITORIZARE PARAMETRILOR TEHNICI PLATFORMĂ*
- *M10. MONITORIZARE DISPONIBILITATE PLATFORMĂ*

safetech
Your trusted security partner

ACTIVITATI

E1. CERCETAREA ȘI ANALIZA CADRULUI TEORETIC ȘI PRACTIC PRIVIND PROIECTAREA, DEZVOLTAREA ȘI IMPLEMENTAREA UNUI SIIMA LA NIVELUL AUTORITĂȚILOR PUBLICE ȘI A INSTITUȚIILOR DIN CADRUL SNAOPS

-A1.1. CERCETAREA ȘI ANALIZA MEDIULUI TEHNOLOGIC

A1.3.CERCETAREA ȘI ANALIZA FUNCȚIONĂRII ȘI SPECIFICULUI INSTITUȚIILOR PUBLICE (ENTITĂȚILOR PUBLICE COMANDITARE), IDENTIFICAREA CERINȚELOR ȘI CONDIȚIONĂRILOR OPERAȚIONALE APLICABILE .

A1.4. IDENTIFICAREA SOLUȚIILOR INFORMATICE (APLICAȚII, MODULE) DE GESTIONARE A ACTIVITĂȚILOR, RESURSELOR, INFORMAȚIILOR ȘI COMUNICĂRII INSTITUȚIEI PUBLICE (IDENTIFICAREA SOLUȚIILOR APLICABLIE)

E2. REALIZAREA MODELULUI CONCEPTUAL AL SIIMA DEZVOLTAREA SOFTWARE A MODELULUI SOFTWARE CONCEPTUAL AL SIIMA

-A2.1. STABILIREA CERINȚELOR OPERAȚIONALE ȘI DE SECURITATE ALE SIIMA.

A2.3. STABILIREA ARHITECTURII SIIMA. ȘI A SISTEMULUI DE COMUNICAȚII NECESAR, INCLUSIV A SOLUȚIILOR TEHNICE DE INTERCONECTARE. REALIZAREA TIPARULUI (MODELULUI) SIIMA

A2.5. DEZVOLTAREA VERSIUNII INIȚIALE (VERSIUNEA BETA) DE SOFTWARE A2.6.COLECTAREA ȘI ÎNCĂRCAREA DATELOR DE TEST, ELABORAREA SCENARIILOR DE TEST ȘI ÎNCĂRCAREA DATELOR

A2.7. TESTAREA DE LABORATOR A VERSIUNII BETA DE SOFTWARE,

safetech
Your trusted security partner

ACTIVITATI

E3. VALIDAREA ȘI EVALUAREA OPERAȚIONALĂ A MODELULUI SOFTWARE A SIIMA. DEFINITIVARE VERSIUNE FINALĂ.

-A3.2. PREGĂTIREA MEDIULUI DE INSTALARE ȘI TESTARE A SIIMA. CONFIGURAREA ȘI PUNEREA ÎN FUNCȚIUNE A ECHIPAMENTELOR ȘI A SUBSISTEMULUI DE COMUNICAȚII, CONFIGURAREA/INSTALAREA BAZELOR DE DATE, SOLUȚIILOR DE SECURITATE, PLATFORMELOR SUPORT ȘI APLICAȚILOR INFORMATICE, ELABORAREA SCENARIILOR DE TEST ȘI A MATERIALELOR PENTRU RAPORTUL PRIVIND MEDIUL DE TESTARE

-A3.3. INSTALAREA ȘI TESTAREA VERSIUNII INIȚIALE (BETA) A SIIMA.,

-A3.4. COLECTAREA, ANALIZA ȘI IMPLEMENTAREA REACȚIILOR DE FEEDBACK

A3.5. OPTIMIZARE FINALĂ HARDWARE/SOFTWARE ȘI ELABORAREA DOCUMENTAȚIILOR TEHNICE DE ADMINISTRARE, EXPLOATARE, UTILIZARE ȘI MENTENANȚĂ A SIIMA.

A3.6. CERTIFICARE OPERAȚIONALĂ, DEMONSTRAREA FUNCȚIONALITĂȚII PROTOTIPULUI (SIIMA. LA SCARĂ REALĂ)

A3.7. VALORIFICAREA REZULTATELOR PROIECTULUI. ELABORARE RAPORT DE EVALUARE ȘI VALIDARE OPERAȚIONALĂ, CERTIFICAREA FEZABILITĂȚII ȘI ACCEPTANȚĂ.

safetech
Your trusted security partner

CARACTERISTICILE DE SECURITATE LA NIVEL DE PLATFORMĂ

PRIN MANAGEMENTUL INTEGRAT AL IDENTITĂȚII ȘI POLITICILOR DE SECURITATE (E.G VALABILITATE PAROLĂ), REGULILOR DE AUTORIZARE ȘI AUTENTIFICĂRII MULTIFACTOR

PRIN STIVA DE INSTRUMENTE DIN GAMA WSO2 CARE OFERĂ CARACTERISTICI PRECUM:

CRIPTAREA PAROLELOR ÎN FIȘIERELE DE CONFIGURARE [45],

TLS LA NIVEL DE TRANSPORT CU DEZACTIVARE ALGORITMI DE CRIPTARE SLABI, ANONIMIZARE HEADERE HTTP AFERENTE TIPULUI DE SERVER, JAVA SECURITY MANAGER

UTILIZAREA SEMNĂTURII DIGITALE PENTRU DOCUMENTE,

MECANISME DE CRIPTARE [53] A DATELOR ÎN BAZA DE DATE LA NIVEL DE COLOANĂ ȘI CONEXIUNI SECURIZATE CĂTRE ACEASTA [52],

CRIPTAREA FIȘIERELOR BACKUP AUTENTIFICAREA STAȚIILOR DE LUCRU CU CERTIFICATE DIGITALE

IZOLAREA LA NIVEL DE REȚEA A ACCESIBILITĂȚII COMPONENTELOR PLATFOMEI CONFORM NECESITĂȚII STRICTE.

safetech

Your trusted security partner

VĂ MULȚUMIM!

Safetech Innovations
Str. Frunzei nr.12-14, et.1 - 3, sector 2 , cod poștal 021533
București, România

Tel/Fax: +4 021 316 0565 e-mail: office@safetech.ro

www.safetech.ro