SAFETECH INNOVATIONS SOC AS-A-SERVICE

Securitate cibernetică fără compromisuri!

SAFETECH INNOVATIONS

Cuprins

Despre serviciu

Safetech Innovations SOC as-a-Service Securitate cibernetică fără compromisuri!

Chiar dacă securitatea cibernetică este o prioritate, multe organizații se confruntă cu o lipsă acută de competențe, ceea ce le crește expunerea în fața avalanșei de atacuri informatice.

Serviciile Safetech Innovations de externalizare a activităților specifice de Security Operations Center oferă monitorizare permanentă și gestionarea optimă a incidentelor, contribuind la îmbunătățirea constantă a posturii de securitate.

Valorificând tehnologia de ultimă generație și expertiza Safetech, organizațiile elimină costurile și complexitatea gestionării unui SOC intern, beneficiind de scalabilitate și viteză de reacție.

SAFETECH INNOVATIONS

Securitatea cibernetică, o prioritate critică în economia modernă

Conform datelor sintetizate de **Ministerul Digitalizării** și prezentate la Bucharest Cybersecurity Conference 2024, **România se confruntă zilnic cu o medie cuprinsă între 25.000 și 50.000 de atacuri cibernetice. (*)**

Pe măsură ce economia modernă realizează tranziția către mediul digital și modelele de lucru online, amenințările cibernetice depășesc tot mai frecvent abordările tradiționale de securitate. Pe fondul unui mediu de business din ce în ce mai competitiv, mediul IT se diversifică și crește în complexitate, odată cu extinderea serviciilor cloud, adoptarea lucrului de la distanță și creșterea numărului de aplicații și dispozitive utilizate.

Atacatorii cibernetici se adaptează rapid la această realitate cu ajutorul tehnologiilor de inteligență artificială, amenințările devenind mai sofisticate și mai dificil de detectat. În ultimii ani, organizațiile din România au înregistrat o creștere semnificativă a atacurilor cibernetice pe toate palierele, dar mai ales DDoS și Ransomware, cele mai vizibile în spațiul public afectând industrii critice precum administrația publică, sănătatea și sectorul financiar.

(*) Sursă: https://gov.ro/ro/stiri/briefing-de-presa-la-finalul-edintei-de-guvern-sustinut-de-ministrul-economiei-radu-oprea-ministrul-digitalizarii-bogdan-ivan-i-purtatorul-de-cuvant-al-guvernului-mihai-constantin1708086975&page=163

Toate statisticile confirmă însă creșterea constantă a numărului de atacuri, precum și al pagubelor provocate de fenomenul cybercrime. De altfel, în România, costul unui incident de securitate suportat de o organizație medie era estimat de Directoratul Național de Securitate Cibernetică, la peste 150.000 EUR.
(Cîmpean (DNSC): Un incident cibernetic pentru o organizație medie, în România, ajunge la un cost de circa 750.000 de lei | AGERPRES • Actualizează lumea.) (*)

Totodată, conformitatea cu reglementări ca Directiva NIS 2 și DORA – Digital Operational Resilience Act) pune o presiune în creștere pe echipele de securitate, prin cerințele tot mai stricte de monitorizare a mediului digital și raportare a incidentelor către autorități.

Organizațiile care nu prioritizează securitatea cibernetică devin vulnerabile și riscă să se confrunte cu scurgeri de date costisitoare, întreruperea operațiunilor, amenzi și penalizări pentru nerespectarea reglementărilor, afectarea reputației, pierderea încrederii clienților și partenerilor, dar și costuri mari de remediere.

(*) Sursă: https://www.agerpres.ro/economic-intern/2022/12/09/cimpean-dnsc-un-incident-cibernetic-pentru-o-organizatie-medie-in-romania-ajunge-la-un-cost-de-circa-750-000-de-lei--1026965

De ce este necesar un Security Operations Center?

Un Security Operation Center (SOC) este esențial pentru organizațiile care doresc să mențină un nivel ridicat de securitate cibernetică și să se apere proactiv împotriva amenințărilor. Acesta funcționează ca o unitate centralizată unde analiștii de securitate și instrumentele de ultimă generație lucrează împreună pentru a monitoriza, detecta, analiza și răspunde în timp real incidentelor de securitate cibernetică pe întreaga suprafață de atac a unei organizații. Prin utilizarea sistemelor de Management al Informațiilor și Evenimentelor de Securitate (SIEM), un SOC poate agrega și corela datele din jurnale provenite din diverse surse, precum firewall-uri, sisteme de detecție a intruziunilor (IDS) și instrumente de detecție și răspuns la nivel de endpoint (EDR), oferind astfel o vizibilitate completă și detectarea anomaliilor.

Echipele SOC folosesc fluxuri avansate de informații despre amenințări pentru a se menține informate cu privire la cele mai recente tehnici, tactici și proceduri (TTP) de atac. Această integrare sprijină îmbogățirea în timp real a alertelor, sporind acuratețea detecțiilor. Instrumentele automate, inclusiv AI și algoritmi de învățare automată, ajută la analizarea unor cantități mari de date legat de trafic și evenimente pentru a identifica modele care indică amenințări sofisticate. Aceste instrumente prioritizează alertele prin alocarea unui scor de severitate și impact potențial, reducând alarmele false și concentrând eforturile analiștilor pe incidente de prioritate înaltă.

Pentru a întări răspunsul la incidente, SOC-urile implementează playbook-uri automate în combinație cu platforme de Orchestrare, Automatizare și Răspuns în Securitate (SOAR). Aceste playbook-uri coordonează acțiuni precum izolarea endpoint-urilor compromise, inițierea scanărilor de malware sau blocarea adreselor IP, accelerând astfel timpul de răspuns și minimizând intervențiile manuale.

Pentru îmbunătățirea continuă, SOC-urile folosesc frecvent un proces de gestionare a vulnerabilităților, care include scanări regulate, managementul patch-urilor și exerciții de căutare a amenințărilor. Această abordare proactivă asigură un nivel de securitate întărit care se adaptează la noi suprafețe de atac, generate de adoptarea IoT sau a lucrului de la distanță.

SAFETECH INNOVATIONS

Provocările operării unui SOC intern

Costurile ridicate:
Crearea unui SOC intern presupune investiții inițiale substanțiale, în echipamente, aplicații și resurse umane specializate. În plus, este nevoie de o lungă perioadă de timp pentru a deveni funcțional. Toate aceste aspecte ajung să destabilizeze bugetele IT, făcând ca investiția într-un SOC să devină nejustificată din punct de vedere economic.

Accesul dificil la expertiză:
Operarea unui SOC intern necesită personal specializat, cu un nivel de expertiză dificil de găsit pe piața locală.

Nevoia de scalabilitate:
La fel de importantă este și scalabilitatea unui astfel de centru de operațiuni de securitate, care trebuie să aibă capacitatea de a se adapta dinamic cerințelor organizației sau evoluției infrastructurii IT, volumului de date și amenințărilor. Limitele de scalabilitate apar frecvent atunci când sistemele sau aplicațiile ating parametrii lor maximi, ceea ce impune înlocuirea acestora cu soluții mai performante, sau când echipa din SOC ajunge la capacitatea maximă de lucru, ceea ce necesită angajarea, instruirea și operaționalizarea unor noi specialiști.

Care este alternativa?

Pentru depășirea acestor provocări, tot mai multe companii optează pentru soluția externalizării – parțiale sau totale – a operațiunilor de securitate către un furnizor de servicii SOC.

Se elimină astfel din start problemele investiției inițiale, a recrutării de personal calificat, a ținerii sub control a costurilor de operare și a respectării cerințelor de conformitate.

6 semne că aveți nevoie de SOC as a Service

Frecvență crescută a incidentelor de securitate în sectoarele critice.
Organizațiile care activează în sectoare precum sănătate, finanțe, energie și infrastructură critică, sunt ținte frecvente ale atacurilor cibernetice și sunt obligate prin legislație (NIS2, DORA, PCI DSS) să dețină sisteme robuste și actualizate de securitate.

Presiune legislativă.
Organizația nu poate ține pasul cu schimbările legislative constante impuse de reglementările de securitate cibernetică. Gestionarea greoaie a rapoartelor și trasabilitatea incidentelor, necesare pentru respectarea acestor reglementări, provoacă risipă de resurse sau costuri neplanificate datorate neconformității cu reglementările.

Buget restrâns.
Organizația nu (mai) poate acoperi costurile asociate cu crearea/ operarea unui SOC intern (personal, infrastructură, software, întreținere). Accesul la tehnologii avansate de cybersecurity este limitat.

Presiunea timpului.
SOC-ul intern nu poate asigura răspunsul în timp real, crește timpul de răspuns la incidente. Un răspuns întârziat poate duce la pierderi importante, în unele situații, chiar și la închiderea afacerii.

Lipsă de personal calificat.
Dificultăți în găsirea, pregătirea continuă și păstrarea angajaților care dețin competențe avansate de securitate cibernetică. Personalul existent este depășit de volumul de lucru, nu poate asigura monitorizarea 24/7 a rețelelor și sistemelor.

Scalabilitate dificilă.
SOC-ul intern nu face față la expansiunea afacerii. Creșterea numărului de angajați, a numărului de locații și a complexității infrastructurii IT înseamnă un volum mai mare de evenimente de securitate, creșterea suprafeței de atac și a numărului potențialelor amenințări.

SAFETECH INNOVATIONS

SOC as a Service (SOCaaS) – beneficii și oportunități

Organizațiile care optează pentru SOC as a Service își externalizează funcțiile centrului de operațiuni de securitate către un furnizor extern. SOCaaS oferă aceleași capacități ca un SOC intern, dar fără investițiile în infrastructura tehnică și personal specializat.

- **Predictibilitatea costurilor.** Prin externalizarea SOC-ului sunt eliminate investițiile inițiale și costurile de operare ale unui SOC intern. Serviciile SOC avansate pot fi accesate fără costuri majore, pe bază de abonament.

- **Acces la experți cu înaltă calificare.** Beneficiarii au acces la o echipă de specialiști în securitate cibernetică mai numeroasă, mai bine pregătită, mai bine organizată, angajată de furnizor. Astfel, nu mai irosesc resurse pentru recrutarea, reținerea/motivarea întregului personal necesar într-un SOC intern.

- **Monitorizare continuă și timp de răspuns la incidente redus.** Un SOC externalizat monitorizează în mod real în regim 24/7/365 rețelele și sistemele organizației, detectând rapid amenințările. Timpul de reacție este redus și impactul asupra organizației (riscul de pierderi operaționale/ financiare) este minim.

- **Scalabilitate.** Un SOC externalizat este dimensionat pentru a servi un număr mare de clienți simultan și are o rezervă pentru vârfuri de activitate. Spre deosebire de un SOC intern, se adaptează rapid la schimbările de cerințe. Beneficiarul poate scala serviciile de securitate fără investiții suplimentare.

- **Acces la tehnologii avansate.** Furnizorii de SOC externalizat utilizează tehnologii avansate pentru detectarea și răspunsul la amenințări. Astfel, organizația beneficiază de aceste soluții complexe fără să le achiziționeze, implementeze sau întrețină.

- **Conformitate cu reglementările.** Furnizorii de servicii SOC externalizate sunt pregătiți să ajute organizațiile să respecte reglementările de securitate cibernetică, precum GDPR, NIS2 sau PCI DSS, evitând sancțiuni și protejând reputația companiei.

- **Focalizare pe activitatea de bază a organizației.** Serviciile SOCaaS eliberează resurse pentru activitățile principale ale organizației și îi permit să se concentreze pe obiectivele sale strategice, știind că securitatea sa este gestionată de profesioniști.

Safetech Innovations SOC as a Service

Serviciile SOC as a Service oferite de Safetech Innovations sunt furnizate de centrul Safetech Computer Emergency Response Team (STI CERT®). Acestea au o structură granulară, care permite organizațiilor să opteze doar pentru serviciile de care au nevoie, și includ:

- **Servicii de onboarding și integrare.**
- **Descoperire active, evaluarea vulnerabilităților, testare de securitate.**
- **Monitorizare, detectare și investigare.**
- **Răspuns la amenințări în regim 24/7, 365 zile pe an.**
- **Raportare și suport pentru conformitate cu normele reglementare.**
- **Guvernanță, Risc și Conformitate (GRC).**

Tehnologii și platforme utilizate de STI CERT

Echipa STI CERT are expertiza in utilizarea de tehnologii avansate de securitate cibernetică specifice centrelor SOC, precum SIEM, NDR, EDR, NGFW (Next-Generation Firewall), XDR, etc.

Strategia Safetech pune accentul pe folosirea a cat mai multe surse de date existente in reteaua clientului, inclusiv instrumente de securitate cibernetica si integrarea acestora intr-o consola unica. În cazul unei infrastructuri de securitate reduse a beneficiarului, Safetech recomandă și implementează soluții suplimentare pentru a mari gradul de eficienta si acuratete a serviciilor SOC, acestea putand fi achiziționate ca investiții sau furnizate în regim as-a-Service.

În baza experienței de peste 9 ani în domeniu, Safetech Innovations recomandă implementarea, cel puțin, a unei arhitecturi minimale formată din:

- **Firewall:** protejează liniile de legatură cu exteriorul ale rețelei organizației și permite aplicarea de politici și restricții de acces,
- **Endpoint Detection and Response (EDR):** protejează cele mai expuse puncte de intrare în rețeaua organizației,
- **Platformă multi-tehnologică bazată pe tehnologia eXtended Detection and Response (XDR):** integrează instrumente EDR dar și alte surse de alerte și jurnale într-un singur panou de monitorizare la nivel SOC.

Safetech Innovations pune la dispoziția organizațiilor și unelte de securitate de Vulnerability Management, Risk Management și Operational Technology Security.

SAFETECH INNOVATIONS

Platforme tehnologice incluse în pachetele Safetech SOC as a Service

Pachete cu abonament anual	Essential	Advanced	Elevate
Endpoint Detection & Response			
• Endpoint Protection (EPP)	√	√	√
• Endpoint Detection and Response (EDR)	√	√	√
• Sandbox	–	√	√
• Deception	–	–	√
• Mobile Threat Detection (MTD)	+	+	+
eXtended Detection & Response			
• EDR integration based on out-of-the box connectors (customer existing EDR)	√	√	√
• Next Generation Security Information and Event Management (NextGen SIEM)	√	√	√
• Intrusion Detection System (IDS)	√	√	√
• Case Management	√	√	√
• Network Detection and Response (NDR)	–	√	√
• User and Entity Behavior Analytics (UEBA)	–	√	√
• Automated Response	–	–	√
Vulnerability Management			
• Web/Network Vulnerability assessment (VA)	–	√	√
Risk Management			
• Asset inventory and business processes maping	–	√	√
• Security risk analysis and Management of Security Indicators	–	–	√
Operational Technology Security			
• OT Threat Detection	+	+	+
• OT Risk Management	+	+	+

Legendă:
√ inclus – neinclus + opțional

Servicii incluse în pachetele Safetech SOC as a Service

Pachete cu abonament anual	Essential	Advanced	Elevate
Servicii Startup			
• Servicii de onboarding	√	√	√
• Servicii de integrare	√	√	√
Planificare și prevenire			
• Descoperire de active	√	√	√
• Evaluare lunară a vulnerabilităților externe	–	√	√
• Evaluare lunară a vulnerabilităților interne	–	–	√
• Testare de securitate (*)	+	+	până la 2 activități pe an
Monitorizare, detectare și investigare			
• Monitorizare continuă 24/7	√	√	√
• Detectare și investigare a amenințărilor	√	√	√
• Root Cause Analysis	–	√	√
• Threat Hunting avansată	–	–	până la 2 activități pe an
• Monitorizarea activelor externe de internet	+	+	√
Răspuns			
• Acțiuni recomandate de remediere	√	√	√
• Contain / Shutdown Host (**)	–	√	√
• Coordonarea acțiunilor de remediere pentru incidente majore și critice	–	în limita a 24 de ore pe an	în limita a 40 de ore pe an
• Playbook-uri personalizate	–	până la 5	până la 10
Guvernanța serviciilor			
• Rapoarte lunare	√	√	√
• Evaluare trimestrială / Lecții învățate	–	√	√
• Suport pentru conformitate cu normele de audit / reglementare	+	+	până la 2 intervenții pe an
Servicii suplimentare (add-on)			
• Activități de Guvernanță, Risc și Conformitate (GRC) (***)	+	+	+

Note:

(*) Testare de securitate: penetration test, revizuire cod, inginerie socială, Red Teaming

(**) Dacă aceste acțiuni sunt posibile de pe platformele gestionate de Safetech și pe baza procedurilor convenite cu clientul

(***) Activități de guvernanță, risc și conformitate: dezvoltarea/revizuirea/actualizarea standardelor/politicilor/procedurilor, analiza de risc, analiza impactului afacerii, planurile de continuitate a afacerii și de recuperare în caz de dezastru, audit de conformitate.

De ce să alegeți Safetech SOCaaS? Principalii diferențiatori

- **Acoperirea extinsă a riscurilor de securitate.**
  Echipa STI-CERT oferă o gamă completă de servicii de securitate cibernetică și accesul la unele avansate de securitate și la servicii de Threat Intellligence. Portofoliul mare de clienți permite echipei dobândească o înțelegere profundă a celor mai noi tehnici și amenințări cibernetice și să aplice soluții personalizate.

- **Servicii certificate la cel mai înalt nivel.**
  Centrul STI CERT este acreditat de către Trusted Introducer, NICP (NATO Industry Cyber Partnership), ISO 9001 și 14001, ISO/IEC 20001 și 27001, precum și OHSAS 18001.

- **Accesul la o echipă numeroasă de specialiști experimentați.**
  Membrii echipei STI CERT dețin multiple certificări personale, incluzând, printre altele, SANS, MICROSOFT, (ISC)², ISACA, CREST, EC-Council. Aceștia lucrează în 3 schimburi pentru a asigura acoperire neîntreruptă.

- **Experiență de 9 ani în tratarea unui volum mare de evenimente/alerte/incidente și capabilități de analiză avansată.**
  Lunar, STI CERT primește, în medie, 100 de miliarde de evenimente, analizează 15.000 de alerte de securitate și tratează 200 de incidente de securitate. STI CERT servește clienți din domenii diverse, incluzând financiar-bancar, utilități, sănătate, tehnologie, retail, distribuție, consultanță, gaming.

- **Poliță de asigurare** cu clauze specifice pentru riscuri de evenimente de natură cibernetică, cu acoperire asupra tuturor serviciilor STI CERT.

- **Preț competitiv, costuri predictibile și stabilitate financiară.**
  Serviciile STI CERT permit companiilor să elimine problema bugetului necesar pentru dezvoltarea unui SOC intern și a costurilor asociate operării lui. Organizațiile pot profita de trei pachete de servicii de externalizare de SOC, care pot fi personalizate în funcție de nevoile și resursele fiecărui client.

- **Safetech Innovations a fost inclusă în prestigiosul Top 250 MSSPs 2024, realizat de CyberRisk Alliance, care recunoaște cei mai performanți 250 de furnizori de servicii gestionate de securitate la nivel global.**
  Safetech Innovations este prima clasată dintre companiile MSSP din România incluse în top, ocupând poziția 153.

STI CERT garantează îmbunătățirea continuă a calității și focalizarea pe nevoile și cerințele fiecărui client, aplicând următoarele măsuri:

1. **Întâlniri lunare de guvernanță**
   Se efectuează informări cu privire la numărul/tipul alertelor investigate, alertele per soluție monitorizată, procentul alertelor care au generat incidente, categoriile și criticitatea incidentelor. Se calculează nivelul de acoperire de către soluțiile de securitate a sistemelor din infrastructura clientului și procentul sistemelor neacoperite cu soluții de securitate.

2. **Raport detaliat pentru fiecare incident high și critical severity**
   STI CERT creează rapoarte de incident care conțin un sumar executiv, descriere tehnică, root cause analysis, concluzii și recomandări.

3. **Îmbunătățirea lunară a acurateții alertelor**
   STI CERT propune lunar măsuri de îmbunătățire a acurateții alertelor din cadrul soluțiilor monitorizate și le validează cu clienții. Măsurile agreate sunt ulterior implementate.

4. **Proces intern de asigurare a calității, efectuat de echipa de nivel 3 (expert)**
   Aceasta evaluează continuu răspunsul la incidente, adaptând metodele/procedurile la cerințele clienților și evoluția amenințărilor. Procesul include ședințe săptămânale pentru îmbunătățirea calității investigațiilor și capacităților tehnice și umane interne.

5. **Buletine transmise prin e-mail cu informații despre amenințări și vulnerabilități recente**
   Informațiile despre vulnerabilități specifice, inclusiv versiuni de software afectate și metode de exploatare, permit echipelor IT ale clienților Safetech să își prioritizeze corespunzător activitățile și să aplice actualizări de securitate/patch-uri înainte ca vulnerabilitățile să fie exploatate.

Concluzie

Modelul SOC as a Service oferă organizațiilor o modalitate proactivă și scalabilă de a proteja întreaga infrastructură IT fără investiții majore în resurse interne.

Serviciile SOC as a Service oferite de Safetech Innovations sunt un pachet complex construit din personal, procese și tehnologie. Acesta garantează un nivel înalt de siguranță, prin sinergia dintre specialiști certificați, procese/metodologii bine definite și validate și tehnologii avansate, la un preț competitiv. Această abordare asigură protecție completă, adaptată nevoilor complexe ale organizațiilor moderne.

SAFETECH INNOVATIONS

APPLIED CYBER INTELLIGENCE

SAFETECH INNOVATIONS S.A.

Strada Frunzei nr. 12-14, et. 1-3, sector 2,
021533 București, România

+40 21 3160565
sales@safetech.ro
www.safetech.ro