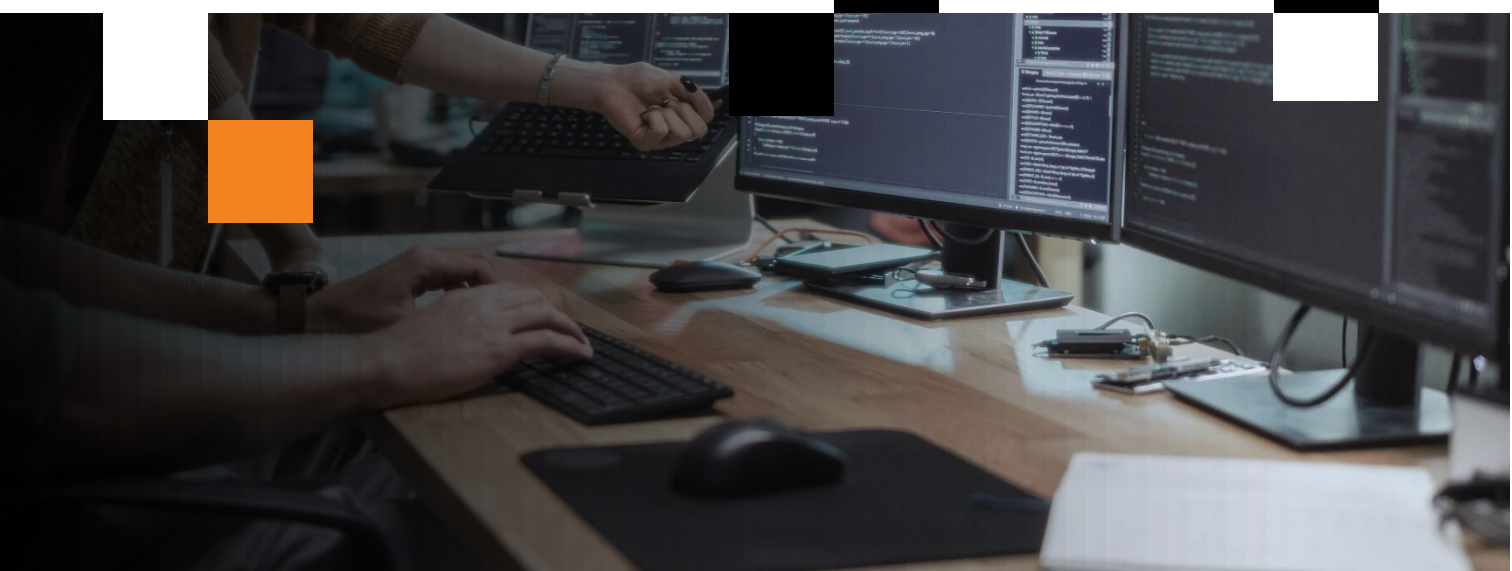
orange™ Business

Ai nevoie de MDR?

Un self-check pentru organizațiile de toate dimensiunile



De ce deschidem acum discuția despre MDR în compania ta?

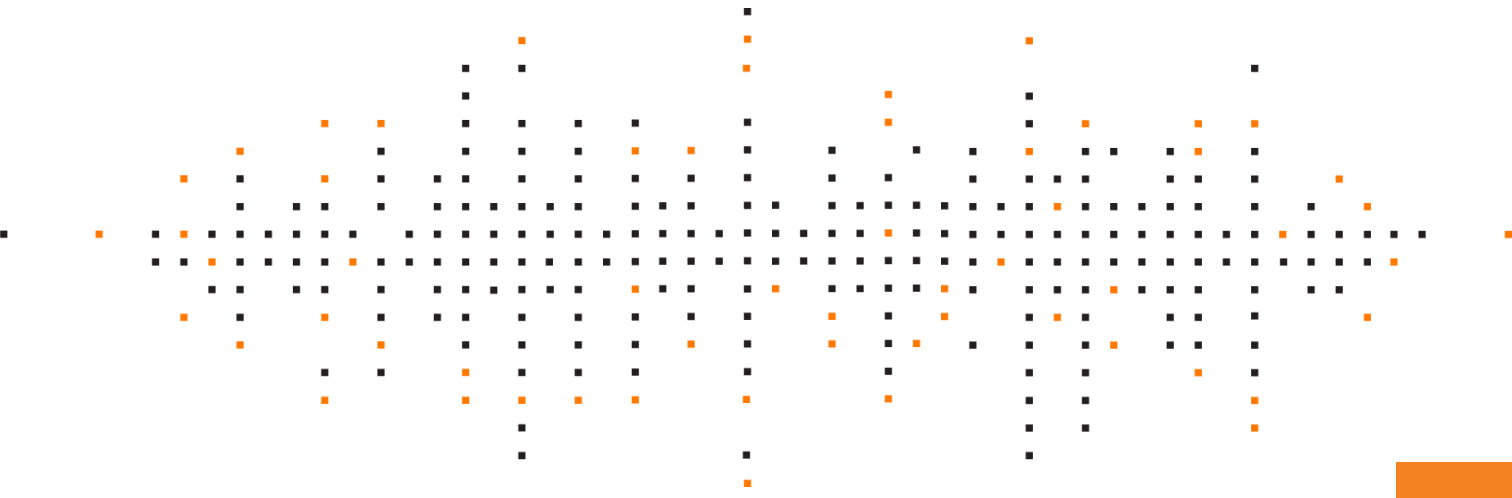
În ultimii ani, tot mai multe companii au ajuns în același punct: nu mai este suficient să ai soluții de securitate instalate. Atacurile pot începe noaptea sau în weekend, iar diferența dintre un incident limitat și o criză de business nu o face doar tehnologia, ci cât de clar este stabilit cine vede primul un semnal important, cine îl înțelege corect și cine poate reacționa la timp.

Dacă ești încă în punctul în care abia pui la punct aceste măsuri de bază, poți folosi acest material ca reper pentru pasul următor: momentul în care infrastructura și aplicațiile devin critice pentru business și începi să ai nevoie nu doar de soluții instalate, ci și de o funcție clară de monitorizare și răspuns la incidente.

Business-ul a schimbat viteza. Securitatea trebuie rescrisă pentru noul ritm.

Apar constant aplicații noi, integrări cu furnizori, automatizări și lucrul hibrid, iar suprafața de atac se modifică de la o lună la alta, nu o dată la câțiva ani. Multe companii au deja un minim de securitate: antivirus, firewall, VPN, politici interne, backup. Problema reală nu mai este dacă există tehnologie, ci dacă aceasta reușește să scoată la suprafață, la timp, alertele critice din zgomotul de zi cu zi și dacă există o echipă care să le urmărească și să intervină rapid. Cu alte cuvinte, întrebarea nu mai este doar „ce soluții avem instalate?”, ci „putem conta pe ele și operațional, atunci când apare o situație reală?”. În acest punct începe, de obicei, discuția despre o funcție de monitorizare și răspuns continuu la incidentele de securitate.

De aici apare discuția despre Managed Detection & Response (MDR): nu ca încă un produs de securitate, ci ca o funcție operațională de monitorizare, prioritizare și răspuns 24/7, construită peste ceea ce aveți deja. Scopul acestui material nu este să explice arhitectura unui serviciu MDR, ci să te ajute să vezi, în situația reală a organizației tale, dacă nivelul actual de protecție mai este suficient sau dacă există deja un decalaj între risc și capacitatea de reacție.



Un pas mic în plus, ca să îți ții planurile mari în siguranță

Ne-am dorit ca acest material să îți facă mai ușor ceea ce oricum aveai deja în minte, nu să îți mai adauge ceva pe listă. Știm că vezi riscurile, urmărești reglementările și, de multe ori, chiar îți face plăcere să te ocupi de zona de securitate, dar pur și simplu nu ai mereu timp să pui totul în ordine. De aceea, am adunat noi la un loc întrebările și reperele esențiale, ca să le poți folosi rapid în discuțiile interne și să fie mai clar dacă și unde ai nevoie de mai mult sprijin, ca partener pentru noi și ca om de referință în echipa ta.

Orientare rapidă pentru organizații în creștere, cu echipe IT restrânse sau externalizate

- nu aveți funcție de monitorizare a incidentelor de securitate în afara programului
- IT înseamnă 1–2 oameni sau furnizor extern „best effort”
- Business-ul depinde critic de e-mail, facturare, ERP sau e-commerce
- în ultimele 12 luni a existat un atac de tip phishing reușit sau a fost compromis un cont de utilizator
- există backup, dar nu este testat periodic
- MFA nu este aplicată consecvent pe conturile critice
- afacerea nu are un plan minim, clar definit, de răspuns la incidente de securitate

Câte situații bifezi?
≤1 - măsuri de baz; **≥2** - risc vizibil; **≥4** - MDR foarte relevant.

Chiar dacă nu bifezi, merită să mergi mai departe. Următoarele capitole arată cum funcționează în realitate ceea ce aveți deja în momentele tensionate.

Întrebări de self-check, fără răspuns corect sau greșit

Parcurge întrebările de mai jos ca să îți dai seama cat de bine e protejat business-ul tău. În plus, în pagina 6, ți-am pregătit un set scurt de întrebări pentru o discuție sinceră în echipă.

Lipsa monitorizării reale, 24/7

- Avem monitorizare activă a securității și în afara programului?
- Dacă un incident începe seara sau în weekend, cum ajunge informația la persoana potrivită?
- Avem un flux clar de monitorizare și escaladare sau doar alerte verificate când permite contextul?

Volumul alertelor și claritatea lor

- Câte alerte de securitate ajung într-o zi sau într-o săptămână la echipă?
- Există un mod clar de prioritizare a alertelor cu impact real?
- Cât de repede știm dacă o alertă este fals pozitivă sau incident real?
- Dacă într-o zi nu primim nicio alertă explicită, avem totuși o modalitate clară de a observa comportamente anormale în rețea sau pe conturile utilizatorilor?

Oameni, roluri și priorități

- Câți din echipă se ocupă efectiv de securitate cibernetică, zi de zi, nu doar „pe lângă restul”?
- Cât din timpul lor este alocat strict pentru securitate și cât pentru alte proiecte IT?
- De câte ori s-a întâmplat să amânăm activități de securitate (monitorizare, actualizări, verificări) din lipsă de timp?

Reacția coordonată în caz de incident

- Există un proces clar pentru ce se întâmplă atunci când este identificat un incident?
- Știm cine vede primul o alertă critică, cine decide ce se întâmplă mai departe și cine coordonează acțiunile?
- Există scenarii pregătite pentru situații precum endpoint compromis, ransomware, cont accesat neautorizat sau exfiltrarea datelor?
- Avem exemple recente în care am rezolvat înainte ca impactul să fie vizibil în business?

Audit, raportare și presiunea din exterior

- Suntem confortabili dacă un auditor întreabă cum monitorizăm securitatea 24/7 și cum documentăm incidentele?
- Putem demonstra, prin rapoarte sau istoric, cum au fost gestionate incidentele relevante?
- Există solicitări din partea auditorilor, partenerilor sau clienților privind timpii de reacție și trasabilitatea?
- Avem o imagine de ansamblu asupra stării de securitate sau doar semnale izolate, greu de pus în context?

Ce arată răspunsurile la self-check, în business?

Răspunsurile la întrebările de auto-verificare din pagina anterioară sunt un bun indicator al maturității în detecția și răspunsul la incidente. Dacă multe răspunsuri sunt „nu”, „nu știu” sau „doar parțial”, următorul pas logic este să iei în calcul o funcție dedicată de monitorizare și răspuns, care să sprijine echipa internă și să protejeze mai bine operațiunile de business.

Nevoia de MDR devine însă cu adevărat vizibilă atunci când legi securitatea de situații concrete de business:

- **În producție**, o întârziere de detecție poate însemna propagarea unui incident dintr-o zonă izolată către procese critice și oprirea activității.
- **În servicii sau financiar**, un cont compromis poate duce la exfiltrare de date, facturi false, blocaje operaționale și presiune suplimentară din zona de conformitate.
- **În retail și e-commerce**, o breșă sau compromiterea unui server expus poate afecta direct vânzările, încrederea clienților și continuitatea platformelor digitale.

Indiferent de industrie, impactul ajunge rapid în business: întreruperi de activitate, pierderi financiare, clienți afectați, timp consumat de echipe și presiune pe management. Diferența dintre un IMM și o companie mare nu ține de existența impactului, ci cum arată el: în unele cazuri lipsesc resursele, în altele lipsesc coerența și viteza de coordonare. În practică, înseamnă că, în cazul unui incident, reacția va depinde de disponibilitatea oamenilor și de decizii ad-hoc, nu de un proces clar, repetabil, aliniat între IT și management.

În acest context, o capabilitate dedicată de monitorizare și răspuns 24/7 nu mai este un „nice to have”, ci un pas firesc pentru a reduce riscul ca un incident tehnic să se transforme într-o problemă de continuitate de business.

Set scurt de întrebări pentru o discuție sinceră în echipă

Uneori diferența vine din încărcarea de zi cu zi sau din lucruri mici care pur și simplu scapă. Mai jos ai o sugestie de întrebări care poate scoate la suprafață exact aceste nuanțe și poate deschide o discuție umană, onestă, despre cum stă organizația ta cu adevărat. Folosește-le ca să vezi, împreună cu echipa, cât din ceea ce crezi și știi chiar se întâmplă în practică.

Managerii văd impactul în business, echipa vede unde se sar pașii

- Sunt activități de securitate pe care simțiți că le tot amânăm, deși știm că sunt importante?
- Sunt momente în care vedeți clar un risc, dar nu aveți timp sau spațiu să îl aduceți în față?
- Dacă ați avea câteva ore în plus pe săptămână, ce ați face diferit în zona de securitate?
- Unde simțiți că avem nevoie de ajutor: de mai mult timp, mai mulți oameni, mai multă automatizare sau suport extern?
- Ce v-a îngrijorat cel mai mult, în ultimele luni, legat de cum tratăm incidentele?

Dacă observi că răspunsurile predominante sunt „Nu” sau „Nu știm”, nu înseamnă că ai făcut ceva greșit, ci că riscurile au crescut mai repede decât resursele interne.
Pentru companiile mari, asta poate însemna că există deja o echipă de securitate, dar are nevoie de suport operațional. Pentru IMM-uri, de multe ori, înseamnă că securitatea este doar una dintre multele responsabilități ale unei echipe mici de IT.
Tocmai de aceea, merită să avem o discuție scurtă despre cum poți organiza, în contextul organizației tale, o funcție de monitorizare și răspuns 24/7, disponibilă la Orange Business prin soluția **SCUT Managed Detection & Response.**

IT-ul tău
e pe mâini bune

Un parteneriat complet pentru întregul tău ecosistem digital.

www.orange.ro/business

orange™ Business