APĂRARE COORDONATĂ:
Cum construiești un SOC puternic, modern și susținut de AI

vodafone business

Microsoft Solutions Partner
Security

SOC DEVINE UN ACCELERATOR DE CONFORMITATE ȘI REZILIENȚĂ

Astăzi, securitatea cibernetică se schimbă mult mai repede decât pot ține pasul majoritatea organizațiilor. Atacatorii folosesc tactici complexe, adaptate mediului în care funcționează afacerea ta, iar extinderea utilizării cloud ului și a inteligenței artificiale le oferă noi oportunități de a acționa mai rapid și mai eficient.

De aceea, soluțiile de securitate care funcționează separat nu mai sunt suficiente. E nevoie de un mod nou de a privi lucrurile – un sistem în care toate instrumentele comunică între ele, iar AI și automatizarea ajută la detectarea și oprirea amenințărilor înainte să devină incidente.

DE CE SE SCHIMBĂ ATACURILE? CE TREBUIE SĂ ȘTII PENTRU A FI PREGĂTIT?

1 INGINERIE SOCIALĂ SUPER-PERSONALIZATĂ CU AI

Atacatorii folosesc AI pentru a crea mesaje care arată perfect autentic, fie că vorbim de e mailuri, mesaje pe Teams sau SMS-uri.

Acestea nu mai conțin mereu linkuri suspecte; în schimb, folosesc presiunea și urgența ca să te facă să acționezi impulsiv.

2 MALWARE CARE SE ADAPTEAZĂ SINGUR

Există programe malițioase care se rescriu automat în funcție de dispozitivul pe care îl infectează.

Fără să comunice cu internetul, pot învăța și evolua singure. Asta le face mult mai greu de detectat.

3 VULNERABILITĂȚILE VECHI – „DATORIA TEHNICĂ”

Deși actualizarea software-ului și implementarea MFA rămân măsuri esențiale de apărare, actorii rău intenționați profită tot mai mult de datoria tehnică (sisteme învechite, vulnerabilități neactualizate, infrastructură îmbătrânită etc.) pe care organizațiile au dificultăți în a o gestiona.

Chiar și organizațiile care stăpânesc bine măsurile tradiționale de securitate rămân vulnerabile, deoarece atacatorii vizează în mod deliberat aceste puncte slabe moștenite. Dispozitivele neadministrate și sistemele integrate mai puțin monitorizate au devenit ținte deosebit de atractive din cauza lacunelor de securitate frecvent trecute cu vederea.

4 ATACURI ASUPRA CONTURILOR PARTAJATE

Atacurile pe parole au explodat: de la 579 pe secundă în 2021 la 7.000.

Conturile administrative sau cele împărțite între mai mulți utilizatori sunt printre cele mai vulnerabile, în special dacă nu folosesc MFA sau au parole vechi.

CE AM ÎNVĂȚAT DIN ATACURILE RECENTE

Ultimele 12 luni au arătat un lucru clar: nu poți ține pasul dacă tratezi vulnerabilitățile una câte una. Trebuie privite ca un drum posibil către resursele critice, nu ca probleme separate.

Cea mai mare lecție? Datoria tehnică este vulnerabilitatea numărul 1. Infrastructura veche, configurările depășite și aplicațiile cu prea multe permisiuni sunt exploatate în mod repetat – chiar și atunci când restul mediului este bine securizat.

Pe măsură ce atacatorii devin mai bine finanțați și mai pregătiți, presiunea crește. Clienții Microsoft, de exemplu, se confruntă cu peste 600 de milioane de atacuri pe zi, de la ransomware la atacuri asupra identității. Totuși, companiile care folosesc soluții moderne au rezultate vizibile: organizațiile care utilizează Defender for Endpoint au înregistrat o scădere de 300% a atacurilor ransomware reușite, chiar dacă volumul total al întâlnirilor cu ransomware a crescut cu 275%.

CUM TE AJUTĂ O PLATFORMĂ UNIFICATĂ DE SECURITATE

O platformă modernă adună într-un singur loc toate elementele importante: protecție pentru dispozitive, identități, e mail, aplicații și cloud, plus detecție, răspuns și informații despre amenințări. În loc să gestionezi console separate și procese complicate, ai o imagine clară asupra riscurilor și poți acționa mai rapid, mai eficient și mai încrezător.

Este diferența dintre a reacționa la probleme și a preveni problemele.

OPERAȚIUNI DE SECURITATE UNIFICATE

O arhitectură unificată transformă operațiunile de securitate prin centralizarea datelor și utilizarea inteligenței artificiale pentru a amplifica expertiza umană, permițând scalare, adaptabilitate și îmbunătățire continuă pe tot parcursul ciclului de viață al amenințărilor.

1 Fundamentul: datele brute care îți arată realitatea

Platforma adună în același loc toate jurnalele de securitate, activitate și semnalele din infrastructură. În loc să cauți informații în zece sisteme, vezi totul într-o singură privire și poți lua decizii mai rapide.de la „pagină goală” sau să rezumi rapid o ședință.

2 Procesare & îmbogățire prin AI

Datele sunt standardizate și conectate între ele, apoi îmbogățite cu informații despre amenințări. AI-ul le transformă în insight uri clare: ce e cu adevărat important, ce trebuie verificat și unde poate apărea următorul risc.

3 Apărare proactivă, nu doar reacție

Platforma poate identifica atacuri în desfășurare, anticipa pașii următori ai atacatorilor și automatiza blocarea mișcărilor laterale. Vulnerabilitățile sunt prioritizate, astfel încât să știi ce trebuie remediat primul pentru a reduce riscurile reale.

4 Expertiză externă integrată natural

Dacă te bazezi pe servicii gestionate sau pe experți externi, platforma le oferă acces la aceleași date și context ca echipei interne. Colaborarea devine fluidă, iar timpul de răspuns scade semnificativ.

5 O experiență clară și simplificată pentru analiști

Toate alertele, incidentele și insight-urile apar într-o singură interfață. Automatizările reduc munca repetitivă, analiza devine mai rapidă, iar AI-ul ajută la investigare și raportare. În final, echipa poate preveni problemele înainte să devină incidente.

ABORDAREA „CLOSED LOOP”: PREVENȚIE → DETECȚIE → RĂSPUNS

O strategie modernă de securitate acoperă tot ciclul unui atac: prevenirea intrării, detectarea mișcărilor suspecte și răspuns rapid în caz de incident. O platformă unificată conectează toate aceste etape într-un circuit închis, astfel încât fiecare acțiune întărește apărarea generală a organizației.

Rezultatul este o strategie completă, coerentă și ușor de gestionat, indiferent de nivelul tău de resurse sau experiență tehnică.

PREVENIRE: PENTRU O APĂRARE MAI BUNĂ, GÂNDEȘTE CA UN ATACATOR

O platformă unificată de securitate îți arată, într-un singur tablou de bord, toate punctele vulnerabile ale afacerii tale. Practic, vezi întreaga suprafață de atac fără zone „oarbe”, ceea ce îți permite să înțelegi clar unde sunt riscurile și ce trebuie rezolvat cu prioritate.

Platforma analizează automat cum ar putea un atacator să combine vulnerabilitățile ca să ajungă la date critice – astfel știi exact ce trebuie remediat mai întâi pentru un impact maxim. În același timp, informațiile despre amenințări active îți arată ce tehnici folosesc atacatorii acum, astfel încât te pregătești pe baza realității, nu a presupunerilor.

Gândirea „ca un atacator” duce la o apărare mult mai proactivă. Integrând instrumente precum SIEM, XDR și managementul expunerii, platforma observă tiparele suspecte mai repede, corelează inteligent semnalele și automatizează o parte din răspuns. Rezultatul: detectezi mai devreme, reacționezi mai rapid și ții riscurile sub control fără efort suplimentar.

Beneficiile managementului unificat al expunerii

Atenuare a riscului, acolo unde contează cu adevărat: te concentrezi pe vulnerabilitățile cu impact mare, nu pe liste interminabile.

Identificare proactivă a breșelor: vezi și rezolvi slăbiciunile înainte ca cineva să profite de ele.

Reducerea suprafeței de atac: configurările devin consecvente, iar punctele de intrare scad.

Reziliență îmbunătățită: ai informații în timp real și răspunsuri automatizate, astfel încât afacerea se adaptează mai ușor la amenințările în schimbare.

DETECTARE:
COORDONEAZĂ APĂRAREA ȘI ÎNTRERUPE ATACURILE AFLATE ÎN DESFĂȘURARE

Oricât de bine ai securiza mediul, atacatorii vor încerca mereu să găsească o portiță. De aceea, pe lângă prevenție, ai nevoie și de detecție inteligentă, care se adaptează constant la noile tactici folosite de infractori.

Spre deosebire de soluțiile clasice care scanează periodic după malware cunoscut, tehnologia de **attack disruption** folosește AI și semnale din întregul ecosistem IT pentru a prezice care va fi următoarea mișcare a atacatorului. Astfel, platforma poate opri mișcarea laterală încă din primele minute – uneori chiar **în medie în trei minute** în cazul atacurilor ransomware.

Gândește-te la attack disruption ca la un set de „playbook-uri" inteligente: se actualizează mereu cu cele mai noi informații despre amenințări și reacționează automat, în timp real, indiferent cât de încărcată este echipa ta.

Beneficiile esențiale ale attack disruption

Răspuns foarte rapid la ransomware: blochează atacurile în medie în trei minute, înainte să producă pagube.

Izolare automată a amenințărilor: dispozitivele sau identitățile compromise sunt izolate imediat, pentru a opri extinderea breșei.

Inteligență predictivă: AI-ul anticipează pașii atacatorului și adaptează apărarea în timp real.

Vizibilitate completă: platforma folosește semnale din tot mediul (endpoint, identități, cloud etc.) pentru detectare mai precisă.

Apărare autonomă: răspunsurile sunt automatizate, ceea ce asigură un nivel constant de protecție.

Adaptare continuă: mecanismele de apărare se actualizează permanent cu cele mai noi informații despre amenințări.

INVESTIGARE ȘI RĂSPUNS:
REMEDIAZĂ RAPID AMENINȚĂRILE CU AJUTORUL AI GENERATIV

În business, timpul pierdut cu alerte inutile poate însemna riscuri uriașe. În multe companii, analiștii de securitate se pierd în sute de notificări și pot rata exact alerta critică ce duce la o breșă serioasă. Aici intervine valoarea unei platforme unificate, bazate pe AI generativ:

Grupează automat alertele și le transformă într-o singură listă deja prioritizată;

Oferă context și informații despre amenințări, fără să trebuiască să cauți în zeci de instrumente;

Ghidează pas cu pas investigația, astfel încât problemele reale să fie rezolvate rapid;

Automatizează acțiunile repetitive, economisind timp și resurse.

ABORDAREA INTEGRATĂ A SECURITĂȚII ÎN CELE MAI EXPUSE ZONE ALE BUSINESSULUI

O protecție eficientă nu se face cu soluții disparate. Atacatorii profită de fiecare „gol” dintre aplicații, dispozitive și identități. O platformă unificată de securitate te ajută să consolidezi apărarea în toate punctele sensibile. În eBook vei descoperi cinci zone esențiale și cum pot fi ele protejate inteligent, cu impact rapid:

1. **Protejarea dispozitivelor (endpoint-uri)**
2. **Protejarea identităților**
3. **Securizarea aplicațiilor cloud-native**
4. **Protecția organizației cu SIEM și XDR**
5. **Protejarea datelor**

SCENARIUL 1
PROTEJAREA ENDPOINT-URILOR

Endpoint urile sunt toate dispozitivele din compania ta: laptopuri, telefoane, tablete, servere. Ele sunt primul punct de intrare pentru atacuri precum ransomware, malware sau exploatarea dispozitivelor neadministrate.

Atunci când securitatea endpoint-urilor este tratată separat de restul sistemelor de apărare, apar breșe pe care atacatorii le pot exploata ușor. De aceea,o protecție eficientă presupune conectarea securității endpoint urilor cu celelalte mecanisme de apărare ale organizației.

Ransomware-ul este considerat principala amenințare externă de către decidenții IT cu responsabilități în zona de securitate.

Sursa: „The Unified Security Platform Era Is Here”, Microsoft, 2024

CE POȚI FACE PENTRU AFACEREA TA

Poți implementa o soluție care să protejeze fiecare dispozitiv și să funcționeze integrat cu restul sistemelor de securitate.

Microsoft Defender for Endpoint detectează și blochează ransomware ul direct la nivel de dispozitiv, oprind răspândirea atacului, mișcarea laterală în rețea și încercările de criptare.

Fiind parte din Microsoft Defender XDR, soluția se integrează cu Security Copilot pentru a analiza rapid atacurile și a oferi ghidare clară pentru remediere, astfel încât incidentele să fie întrerupte în mai puțin de trei minute.

Beneficiile managementului unificat al expunerii

- **Reduci semnificativ riscul atacurilor de tip ransomware și malware**
- **Protejezi toate dispozitivele companiei, inclusiv pe cele mai vulnerabile**
- **Reacționezi rapid la incidente, cu analiză și recomandări clare**
- **Eviți blocajele operaționale și pierderile financiare cauzate de atacuri**
- **Ai o protecție aliniată cu întreaga strategie de securitate, nu soluții izolate**

SCENARIUL 2
PROTEJAREA IDENTITĂȚILOR – PRIMUL PAS SPRE O AFACERE CU ADEVĂRAT SIGURĂ

Identitățile digitale (utilizatori, conturi, parole, acces) sunt una dintre cele mai frecvente ținte ale atacurilor cibernetice. Prin phishing și furt de credențiale, atacatorii pot prelua conturi legitime și se pot deplasa rapid în interiorul organizației.

O apărare eficientă presupune unificarea semnalelor de identitate, pentru a detecta din timp atacurile, a preveni preluarea conturilor și a bloca mișcarea laterală și amenințările interne.

CE POȚI FACE PENTRU AFACEREA TA

Poți adopta o abordare unificată de **Identity Threat Detection and Response (ITDR)**, care monitorizează și corelează continuu semnalele de identitate din întregul mediu.

Cum arată un atac și cum este oprit, pas cu pas:

LEGENDĂ: Acțiunea atacatorului | Cum ajută platforma unificată de securitate | Rezultatul acțiunii SOC

1 COMPROMITERE INIȚIALĂ

- Se trimit e mailuri către utilizatori pentru a-i păcăli (phishing).
- Detectarea bazată pe modele LLM scanează e-mailurile pentru a interpreta intenția.
- E-mailurile malițioase sunt marcate sau plasate în carantină înainte de a ajunge la utilizatori.

2 FURTUL DE CREDENȚIALE

- Utilizatorul răspunde la e-mail și aprobă o solicitare MFA primită.
- Răspunsul trimis este marcat ca suspect; solicitarea MFA este blocată.
- Activitatea suspectă este detectată timpuriu, blocând încercarea atacatorului.

3 PRELUAREA CONTULUI

- Atacatorul folosește credențiale furate pentru a se autentifica.
- ITDR detectează anomalii; credențialele sunt suspendate.
- Accesul neautorizat este prevenit sau activitatea atacatorului este perturbată.

4 MIȘCARE LATERALĂ

- Se încearcă deplasarea laterală în rețea pentru escaladarea privilegiilor.
- SIEM corelează semnalele și declanșează un playbook de răspuns.
- Mișcarea laterală este oprită; atacul este rapid limitat.

5 INVESTIGAȚIE ȘI REMEDIERE

- Se încearcă exfiltrarea datelor.
- Investigația asistată de AI oferă o vedere completă asupra incidentului și recomandări de acțiune.
- Remediere rapidă; riscurile viitoare sunt reduse în mod eficient.

6 CONFIRMARE ȘI RĂSPUNS

- Atacul este neutralizat, dar necesită confirmare și închidere.
- Analistul confirmă măsurile de remediere și întărește apărarea.
- Organizația se recuperează; lecțiile învățate îmbunătățesc postura de securitate.

Microsoft ITDR analizează în timp real semnalele de identitate, automatizează răspunsurile și oprește rapid amenințările. Security Copilot accelerează investigațiile și reduce impactul incidentelor, iar Microsoft Entra ID Protection completează apărarea prin MFA și autentificare fără parolă, optimizate continuu.

Beneficiile pentru tine și afacerea ta

- **Previi phishing-ul și furtul de credențiale**
- **Limitezi impactul atacurilor înainte să se extindă**
- **Construiești o protecție solidă și coerentă a identităților în întreaga organizație**
- **Blochezi rapid preluarea conturilor**
- **Reduci timpul de investigație și răspuns**

SCENARIUL 3
SECURIZAREA APLICAȚIILOR CLOUD NATIVE

Aplicațiile cloud native sunt esențiale pentru funcționarea afacerilor moderne, dar pot deveni rapid o țintă dacă există configurări greșite sau vulnerabilități neadresate.

O securitate cloud eficientă presupune o abordare unificată, care să detecteze din timp punctele slabe, să blocheze escaladarea privilegiilor și să oprească mișcarea laterală, protejând resursele critice din cloud.

CE POȚI FACE PENTRU AFACEREA TA

Poți implementa o soluție de securitate cloud unificată care monitorizează continuu infrastructura și aplicațiile tale, de la configurare până la rulare.

Cum arată un atac și cum este oprit, pas cu pas:

LEGENDĂ: ■ Acțiunea atacatorului ■ Cum ajută platforma unificată de securitate ■ Rezultatul acțiunii SOC

1 ACCES INIȚIAL

- Exploatează o vulnerabilitate cunoscută într-un serviciu cloud.
- CSPM și CWPP detectează configurările greșite și punctele slabe.
- Vulnerabilitățile sunt identificate și atenuate înainte de a fi exploatate.

2 PERSISTENȚĂ

- Stabilește persistență în mediul compromis.
- Protecția pentru workload urile din cloud detectează activitate neobișnuită.
- Anomaliile sunt marcate pentru investigație, reducând timpul în care atacatorul rămâne în sistem.

3 MIȘCARE LATERALĂ

- Se deplasează lateral pentru a compromite resurse cloud suplimentare.
- SIEM corelează logurile pentru a detecta tiparele mișcării laterale.
- Mișcarea laterală este oprită; resursele compromise sunt izolate.

4 ESCALADAREA PRIVILEGIILOR

- Încearcă să escaladeze privilegiile în cadrul sistemului cloud.
- Schimbările suspecte de roluri sau permisiuni sunt detectate.
- Credențialele utilizatorului sunt suspendate; atacatorul este blocat.

5 INVESTIGAȚIE ȘI RĂSPUNS

- Exfiltrează date sensibile sau perturbă serviciile cloud.
- Exfiltrarea este blocată; alertele sunt grupate într-un incident pentru analist.
- Amenințarea este neutralizată; analistul trebuie doar să confirme și să atenueze vulnerabilitățile.

Microsoft Defender for Cloud unifică protecția pe întreg ciclul de viață al aplicațiilor, de la cod la execuție, în toate mediile cloud. Security Copilot analizează continuu configurațiile și automatizează controalele de securitate pentru a preveni compromiterile.

Beneficiile pentru tine și afacerea ta

- **Identifici rapid vulnerabilitățile din cloud**
- **Blochezi mișcarea laterală și escaladarea privilegiilor**
- **Ai control și vizibilitate completă asupra securității cloud**
- **Reduci riscul breșelor și al configurărilor greșite**
- **Protejezi datele și serviciile critice din cloud**

SCENARIUL 4
PROTEJAREA ÎNTREGII ORGANIZAȚII CU SIEM ȘI XDR

Atacurile moderne nu se limitează la un singur punct de intrare. Ele folosesc mai multe canale – e-mail, identitate, rețea, endpoint – pentru a păcăli utilizatorii și a se infiltra în organizație.

Prin combinarea **SIEM și XDR într-o singură platformă**, echipele de securitate pot vedea întregul lanț al atacului, pot corela rapid alertele din surse diferite și pot investiga și răspunde fără întreruperi.

CE POȚI FACE PENTRU AFACEREA TA

Poți adopta o platformă unificată, cloud native, care corelează semnalele de securitate și oprește atacurile complexe, precum AiTM (adversary in the middle).

Cum arată un atac și cum este oprit, pas cu pas:

LEGENDĂ: Acțiunea atacatorului | Cum ajută platforma unificată de securitate | Rezultatul acțiunii SOC

1 ACCES INIȚIAL

- Trimite un e-mail de phishing cu un link către o pagină falsă de autentificare.
- Securitatea e-mail detectează mesajul; rețeaua detectează accesarea site-ului de phishing.
- Detectarea timpurie reduce probabilitatea interacțiunii utilizatorului.

2 ACCESAREA LINKULUI

- Utilizatorul accesează linkul de phishing, conectându-se la pagina falsă de autentificare.
- Securitatea rețelei detectează conexiunea către un site de phishing cunoscut.
- Detectarea timpurie a activității malițioase înainte de introducerea credențialelor.

3 FURTUL DE CREDENȚIALE

- Utilizatorul introduce credențialele pe pagina falsă; credențialele sunt furate.
- SIEM corelează semnalele de identitate, în timp ce protecția identității detectează autentificarea anormală; utilizatorului i se solicită MFA.
- Furtul de credențiale este atenuat sau prevenit.

4 MIȘCARE LATERALĂ

- Folosește credențialele furate pentru a accesa alte resurse.
- SIEM analizează tiparele de autentificare, în timp ce Zero Trust aplică principiul privilegiilor minime; segmentarea limitează mișcarea.
- Limitează capacitatea atacatorului de a se deplasa în rețea.

5 IMPACT (COMPROMITEREA CONTULUI)

- Contul este compromis și utilizat în scopuri malițioase.
- SIEM corelează semnalele din sistemele implicate; contul este blocat, accesul este revocat, iar un incident este creat pentru investigație
- Atacul este izolat; contul compromis este remediat.

6 INVESTIGAȚIE ȘI RĂSPUNS

- Atacul este izolat, dar necesită investigație.
- SIEM oferă o cronologie completă a atacului în timp ce analiștii investighează; AI recomandă acțiuni pentru întărirea apărărilor.
- Amenințarea este neutralizată; riscurile viitoare sunt reduse.

Microsoft Sentinel unifică semnalele de securitate din toate mediile cloud și platformele, expunând tiparele ascunse ale atacurilor avansate. Security Copilot cartografiază lanțurile complexe de atac și automatizează răspunsul la nivelul întregii organizații.

Beneficiile pentru tine și afacerea ta

- **Vizibilitate completă asupra atacurilor, dintr-un singur loc**
- **Detectarea rapidă a amenințărilor complexe, multi vector**
- **Răspuns coordonat, fără pierdere de timp între echipe și sisteme**
- **Reducerea impactului incidentelor asupra operațiunilor**
- **O postură de securitate solidă, coerentă, la nivelul întregii organizații**

SCENARIUL 5
PROTEJAREA DATELOR

Datele sunt unul dintre cele mai valoroase active ale unei organizații și, în același timp, una dintre cele mai frecvente ținte ale atacurilor — inclusiv din interior. Amenințările interne, accesul neautorizat sau exfiltrarea accidentală sau intenționată pot duce la pierderi majore de informații și reputație.

O protecție eficientă a datelor presupune o abordare unificată, care să detecteze comportamentele suspecte, să blocheze accesul neautorizat și să prevină exfiltrarea datelor la nivelul întregii organizații.

CE POȚI FACE PENTRU AFACEREA TA

Poți implementa o soluție de protecție unificată a datelor, care oferă vizibilitate completă asupra modului în care sunt accesate, mutate și utilizate informațiile sensibile.

Cum arată un incident de securitate a datelor și cum este gestionat, pas cu pas:

LEGENDĂ: ■ Acțiunea atacatorului ■ Cum ajută platforma unificată de securitate ■ Rezultatul acțiunii SOC

1 RECUNOAȘTERE

SEMNALE NATIVE ALE PLATFORMEI

- Un insider localizează date sensibile pentru o posibilă exfiltrare
- Monitorizarea comportamentului utilizatorului detectează anomalii.
- Activitate suspectă marcată pentru investigații suplimentare.

2 PREGĂTIREA DATELOR (DATA STAGING)

STRAT UNIFICAT DE DATE

- Copiază sau mută date sensibile într-o zonă de pregătire.
- Instrumentele de prevenire a pierderii datelor detectează și blochează mișcările neautorizate.
- Încercările de consolidare a datelor sunt identificate și întrerupte.

3 EXFILTRARE

DATE BRUTE ȘI INFORMAȚII

- Transferă datele pregătite în afara organizației.
- Monitorizarea rețelei detectează tipare neobișnuite de trafic.
- Încercările de exfiltrare sunt detectate și blocate în timp real.

4 EXFILTRARE

ANALITICĂ DE SECURITATE LA SCARĂ MARE (HYPERSCALE SECURITY ANALYTICS)

- Încearcă să escaladeze privilegiile în cadrul sistemului cloud.
- Schimbările suspecte de roluri sau permisiuni sunt detectate.
- Credențialele utilizatorului sunt suspendate; atacatorul este blocat.

5 INVESTIGARE, REMEDIERE ȘI PREVENȚIE

EXPERIENȚĂ UNIFICATĂ PENTRU ANALIȘTI

- Exfiltrarea este oprită; gradul pierderii de date este determinat.
- Analiștii folosesc instrumente AI pentru a investiga incidentele, a recupera datele și a consolida controalele de acces.
- Incidentul este rezolvat; viitoarele riscuri interne sunt reduse prin politici îmbunătățite și măsuri preventive.

Beneficiile pentru tine și afacerea ta

- **Detectezi rapid amenințările interne și comportamentele suspecte**
- **Previ accesul neautorizat și pierderea datelor sensibile**
- **Blochezi exfiltrarea informațiilor în timp real**
- **Reduci timpul de investigație și impactul incidentelor**
- **Îți întărești politicile de protecție a datelor pe termen lung**

CONCLUZIE

Viitorul operațiunilor de securitate înseamnă trecerea de la o apărare reactivă la una proactivă și coordonată.

O arhitectură SOC unificată face această schimbare posibilă, eliminând silozurile dintre soluții, permițând automatizarea bazată pe AI și creând un ciclu continuu de protecție și îmbunătățire.

Prin platforma sa integrată de securitate, Microsoft oferă fundația necesară pentru această transformare:

- **Detectare în timp real și răspuns automatizat la amenințări**
- **Vizibilitate unificată asupra întregului mediu digital**
- **Investigație și remediere accelerate cu ajutorul AI**
- **Optimizare continuă a posturii de securitate**

DOUĂ MODURI PRIN CARE ÎȚI POȚI CONSOLIDA SECURITATEA CU UN SOC UNIFICAT

1 Cu ajutorul soluțiilor Microsoft

O arhitectură completă, care acoperă toate scenariile critice:

- **Defender XDR & Defender for Endpoint** – protecția dispozitivelor și oprirea atacurilor ransomware
- **Sentinel** – SIEM și securitate la nivelul întregii organizații
- **Entra ID Protection** – protecția identităților și accesului
- **Defender for Cloud** – securitatea aplicațiilor cloud native
- **Purview** – protecția și guvernanța datelor
- **Security Copilot** – analiză și automatizare bazate pe AI, în toate scenariile

2 Cu ajutorul Managed Security Services de la Vodafone

Dacă nu ai o echipă internă dedicată sau buget pentru o infrastructură complexă, **SOC ul Vodafone** se ocupă de configurare, monitorizare și protecție continuă a mediului tău Microsoft.

Vodafone Managed Security – securitate enterprise, gestionată complet.

Vodafone Managed Security pentru Microsoft 365 Business Premium este o soluție dedicată companiilor mici și mijlocii, care oferă protecție completă pentru identitate, dispozitive, e mail și date. Totul este configurat și monitorizat 24/7 de echipa SOC Vodafone și integrat în platforma **Vodafone CyberHub.**

Ce îți oferim, pe scurt:

- **configurații de securitate standardizate, bazate pe best practices**
- **protecția identității prin MFA și Entra ID**
- **securizarea dispozitivelor cu Defender for Business**
- **protecția e mailului și a datelor prin Defender și Purview**
- **monitorizare 24x7x365 și evaluări periodice ale posturii de securitate**
- **vizibilitate și administrare simplificată prin CyberHub**

Pentru companiile foarte mici, care nu folosesc încă Microsoft 365 Business Premium, **Managed Security pentru Defender for Business** oferă protecție complet administrată pentru endpoint uri, cu monitorizare 24/7 și răspuns rapid la incidente, la un cost accesibil.

DE CE SĂ ALEGI VODAFONE

- securitate gestionată de experți, fără efort intern
- răspuns la incidente disponibil 24/7
- reducerea semnificativă a riscului de compromitere a conturilor
- mai puțină presiune pe echipa IT, prin automatizare
- costuri optimizate, cu acoperire completă într o singură soluție

Într-un peisaj digital în care atacurile evoluează constant, avantajul real nu este doar tehnologia, ci **echipa care o gestionează.** Vodafone Security Operations Centre îți oferă protecție continuă, intervenție rapidă și aplicarea celor mai bune practici de securitate, astfel încât tu să te concentrezi pe creșterea afacerii tale.

Cere detalii managerului tău de cont Vodafone.

vodafone business

Microsoft Solutions Partner
Security