Datanet SYSTEMSINTEGRATION
SOITRON GROUP

Cisco Partner
Gold Integrator

Ghid Datanet Systems pentru adoptarea soluției Cisco XDR

Creșterea volumului, diversității și complexității amenințărilor informatice obligă companiile să adopte mai multe soluții specializate de securitate pentru asigurarea protecției. În pofida investițiilor, detecția și răspunsul la amenințări rămân însă lente, eterogenitatea infrastructurilor de securitate limitând eficiența soluțiilor utililizate. Analiza izolată a datelor, compatibilitatea redusă a aplicațiilor de securitate și deficitul de specialiști IT[1] fac ca mai mult de jumătate dintre atacurile care penetrează sistemele de protecție să nu fie depistate[2].

Conceptul **XDR (Extended Detection and Response)** a apărut ca un răspuns la nevoile curente ale companiilor de a-și:

- îmbunătăți viteza de reacție la amenintari informatice;
- extinde vizibilitatea asupra sistemelor IT până la nivelul utilizatorului final;
- reduce nivelul de complexitate al sistemelor de securitate IT.

Analiștii Gartner definesc conceptul XDR ca „o platformă unificată de detecție și răspuns la incidentele de securitate, care centralizează și corelează date colectate de la mai multe soluții"[3].

Datanet Systems vine în sprijinul organizațiilor care se confruntă cu probleme legate de timpul de detecție și de reacție la amenințări informatice și de gestionarea complexității utilizării mai multor sisteme independente de securitate IT, transpunând conceptul XDR într-o ofertă de produse pre-integrate de securitate informatică ce reunește cinci dintre cele mai eficiente aplicații Cisco de protecție.
Soluțiile recomandate și livrate de Datanet sunt:

- **Cisco Secure Firewall (**noua denumire a produselor Firepower);
- **Cisco Secure Email** (fosta Email Security);
- **Cisco Secure Endpoint** (fosta AMP for Endpoints);
- **Cisco Umbrella**
- **Cisco SecureX.**

[1] Datele **Eurostat** arată că 90% dintre companiile locale întâmpină dificultăți în recrutarea de personal IT.
[2] Potrivit **Mandiant Security Effectiveness Report 2020**, 53% dintre atacurile care penetrează sistemele de securitate nu sunt descoperite, iar 91% nu generează nicio alertă directă.
[3] Conform raportului **Innovation Insight for Extended Detection and Response**.

Avantajele adoptării soluției Cisco XDR

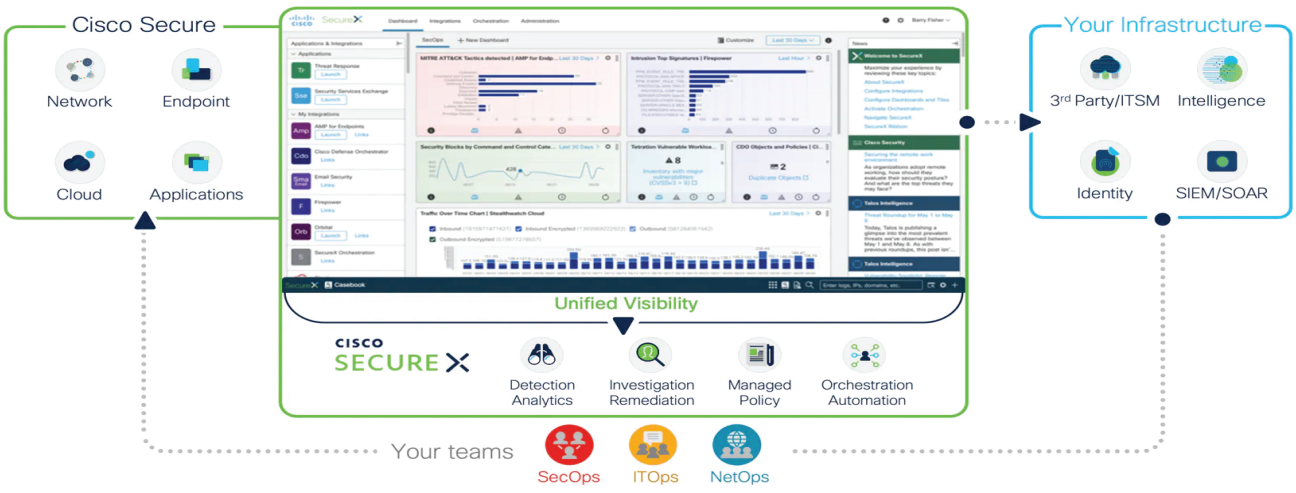
Această soluție integrează produse Cisco on-premises și servicii Cloud şi este concepută astfel încât să asigure protecție extinsă pe mai multe niveluri. Arhitectura recomandată acoperă de la nevoile de securitate ale utilizatorilor finali, până la cerințele de protecție ale infrastructurilor IT, oferind scalabilitate şi flexibilitate pentru cele mai diverse scenarii de lucru.

Totodată, prin integrarea celor patru produse de securitate cu serviciul Cloud SecureX asigură:

- creșterea eficienței soluțiilor de securitate;
- simplificarea proceselor operaționale de detecție, investigare și răspuns;
- reducerea nivelului de încărcare a departamentului IT și a costurilor operaționale.

Platforma SecureX este disponibilă gratuit oricărei companii, indiferent de ordinul de mărime sau nivelul competențelor IT interne, în baza achiziţiei produselor de securitate Cisco descrise în acest ghid pregatit de Datanet Systems.

Livrată ca serviciu Cloud, platforma integrează fluxuri de date colectate din toate cele patru produse Cisco recomandate, pe care le corelează și agregă, livrând informații contextuale utile în procesul de analiză al evenimentelor de securitate. SecureX simplifică și eficientizează astfel procesele de monitorizare, detecție și răspuns la amenințări. Prin intermediul platformei Cloud Cisco, operațiunile de securitate pot fi realizate centralizat dintr-o consolă unică, accesibilă de oriunde, iar elementele de automatizare și orchestrare integrate asigură creșterea vitezei de reacție.



Ce avantaje aduce oferta Datanet Systems

Valoarea pachetului propus de Datanet Systems stă în combinarea celor cinci componente, utilizarea împreună a soluțiilor Cisco recomandate fiind superioară însumării beneficiilor livrate separat. Principalele câștiguri asigurate sunt:

- **Îmbunătățirea securității la nivelul întregii companii**

Soluțiile Cisco recomandate asigură o protecție extinsă, pe mai multe niveluri. Selecția soluțiilor de securitate a fost realizată de specialiștii Datanet pe principiul complementarității produselor, astfel încât, prin integrarea lor, companiile beneficiază de o reducere a suprafeței de atac și îmbunătățirea capacităților de prevenție și răspuns. Conform evaluărilor Cisco, timpii de detecție și remediere scad astfel cu până la 85%.

- **Simplificarea procedurilor de investigare și răspuns la amenințări**

Prin integrarea nativă a produselor într-o arhitectură hibridă, monitorizarea și analiza evenimentelor de securitate devine mai simplă, nemaifiind necesare competențe specifice în operarea fiecărei soluții în parte. Totodată, partajarea informațiilor colectate din mai multe surse între echipele operaționale și responabilii cu securitatea informatică ajută companiile să obțină reducerea timpului de lucru al departamentelor IT.

- **Extinderea vizibilității asupra suprafeței de atac și potențialelor amenințări**

Integrarea soluțiilor de securitate Cisco prin intermediul SecureX permite companiilor să poate vizualiza dintr-o singură consolă orice potențial eveniment care poate semnala o situație de risc. Informațiile agregate în platformă pot fi corelate automat și cu date despre cele mai noi amenințări apărute, obținute din alte surse – precum serviciile de Security Intelligence Cisco Talos. Vizibilitatea unificată și elementele de automatizare ajută companiile să reducă la jumătate timpul necesar investigării incidentelor și depistării amenințărilor.

- **Creșterea eficienței**

Automatizarea activităților de rutină și metodele simple de creare a fluxurilor de lucru – prin intermediul interfețelor intuitive și a acțiunilor de tip drag-and-drop – îmbunătățesc eficiența proceselor operaționale, cu efecte directe în reducerea costurilor aferente. În același timp, identificarea rapidă a factorilor de risc ajută companiile să evite și limiteze pagubele directe și să blocheze potențialele riscuri, fără a afecta productivitatea utilizatorilor finali și randamentul serviciilor livrate.

- **Acoperirea unei game extinse de scenarii de lucru**

Flexibilitatea arhitecturii hibride (on-premises + Cloud), structura modulară a ofertei integrate, precum și funcționalitățile avansate de automatizare și orchestrare ale platformei Cloud simplifică procesul de dezvoltare de fluxuri și scenarii de lucru personalizate pe nevoile și cerințele specifice fiecărei companii.

Componentele ofertei integrate Datanet

Oferta integrată de soluții de securitate recomandată de specialiștii Datanet reunește patru dintre cele mai performante aplicații Cisco de protecție, integrate prin intermediul Cisco SecureX. Platforma Cloud transformă infrastructura de securitate dintr-o serie de produse individuale de protecție într-un ecosistem integrat, care acționează coordonat.

• Cisco Secure Endpoint
(fosta AMP for Endpoints)

Cisco Secure Endpoint ajută companiile să prevină situațiile critice, identificând și semnalând automat vulnerabilitățile aplicațiilor instalate pe dispozitivele IT pentru utilizatorii finali (ce ruleaza Windows, Mac, Linux, Android sau iOS), depistează atacurile monitorizând continuu activitatea dispozitivelor pentru a identifica comportamentele anormale ale programelor rulate și blochează amenințarea în timp real. Soluția integrează mai multe tehnologii avansate de detecție și protecție, precum File reputation, cu ajutorul cărora amenințările malware sunt recunoscute și introduse rapid în carantină, sau algoritmi de Machine Learning cu ajutorul cărora învață cum să identifice fișierele și activitățile cu potențial de risc pe baza atributelor malware cunoscute .

Prin integrarea cu SecureX, departamentele IT pot utiliza Secure Endpoint ca un senzor avansat pentru analiza statusului de securitate al echipamentelor mobile, dar și ca instrument de punere în aplicare a măsurilor de răspuns, în cazul detectării unei amenințări. Soluția poate fi folosită și pentru automatizarea fluxurilor de lucru și depistarea rapidă, direct din platforma Cloud, a fișierelor și resurselor din rețea care au fost accesate de mai multe terminale.

• Cisco Umbrella

Cisco Umbrella asigură protecția infrastructurii organizațiilor și a utilizatorilor mobili, stopând amenințările înainte ca ele să ajungă în rețea și/sau pe echipamente. Soluția analizează cererile DNS (Domain Name System) și determină nivelul de risc al conținutului on-line, blocând din start conținutul periculos, în timp ce URL-urile suspecte sunt analizate de serviciul Intelligent Proxy asigurat de Cisco în Cloud, care inspecteaza și traficul SSL. Rețeaua Umbrella analizează zilnic miliarde de solicitări DNS – verifică schimbări la nivel DNS, asocieri cu domenii care găzduiesc malware și/sau direcționează către IP-uri compromise, etc. – și depistează în timp real amenințări și tipare de atac. Soluția asigură confidențialitate (prin criptarea traficului DNS) și protecție utilizatorilor mobili cu ajutorul funcționalității IP Layer Enforcement.

Prin integrarea cu SecureX, Umbrella livrează informații detaliate despre URL-urile accesate, îmbogățind analizele cu informații contextuale despre reputația domeniilor solicitate. Soluția poate fi utilizată și pentru automatizarea fluxurilor de lucru și blocarea rapidă a adreselor cu potențial de risc.

Componentele ofertei integrate Datanet

• Cisco Secure Firewall

(fostul Firepower NGFW)

Soluțiile firewall de nouă generație de la Cisco se evidențiază prin capacitățile avansate de blocare a amenințărilor cunoscute și necunoscute, funcționalitățile de detecție a intruziunilor (NGIPS), ierarhizarea automată a riscurilor și uneltele integrate de detecție timpurie și remediere rapidă. Firewall-urile Cisco ajută departamentele IT să aplice consistent și uniform politicile de securitate la nivelul întregii companii, să creeze segmentări ale rețelei și reguli de acces dedicate și să monitorizeze traficul la nivel de aplicație și categorii de domenii accesate.

Prin integrarea cu SecureX, firewall-urile Cisco livrează în platforma Cloud informații detaliate despre adresele IP, URL-urile și domeniile accesate, echipamentele putând fi configurate pentru a bloca perimetral IP-urile malițioase. SecureX procesează și gestionează alertele de înaltă prioritate emise de firewall-uri, corelându-le cu informațiile colectate din alte surse. Departamentele IT pot obține astfel o vizibilitate extinsă, scăderea timpului de reacție și simplificarea operațiunilor de răspuns, prin coordonarea tuturor echipamentelor firewall dintr-o singură consolă.

• Cisco Secure Email

(fosta Email Security)

Cisco Secure Email ajută companiile să comunice în mod securizat și să blocheze amenințările, tentativele de phishing și Business Email Compromise (BEC), mesajele spam și transmiterea neautorizată a datelor cu caracter sensibil, asigurând protecție pe mai multe niveluri. Soluția Cisco are capacități avansate de detectare și blocare a amenințărilor susținute prin serviciul de Security Intelligence Talos, blochează amenințările ransomware ascunse în atașamentele email-urilor, elimină mesajele care conțin link-uri malițioase, limitează accesul la site-urile infectate, protejează conținutul email-urilor prin criptare și integrează funcționalități de Data Loss Prevention (DLP).

Prin integrarea cu SecureX, companiile pot vizualiza direct din platforma Cloud mail-urile pe care Secure Email le identifică drept potențiale amenințări, expeditorii și destinatarii acestora. Platforma permite realizarea de căutări detaliate după adrese, subiecte, mesaje și fișierele anexate pentru a ajuta administratorii să depisteze propagarea amenințărilor, a atacurilor phsihing, a tentativelor de tip BEC etc.

Componentele ofertei integrate Datanet

- **Cisco SecureX**

Cisco SecureX este un serviciu Cloud care permite integrarea mai multor soluții de securitate Cisco, dar și a celor provenind de la o serie de alți producători (prin intermediul API-urilor), pentru a asigura vizibilitate unificată asupra amenințărilor, automatizarea și orchestrarea fluxurilor de lucru și crearea de scenarii de lucru variate. Platforma asigură reducerea timpului de detecție prin centralizarea datelor colectate și vizualizarea răspunsului într-o singură interfață, permite realizarea dintr-o singură consolă a investigațiilor și blocarea simultană a atacurilor. Modulul central al platformei – „Threat response" –, asigură realizarea de investigații, monitorizând o serie extinsă de indicatori de compromitere (IoCs) pentru a depista ce utilizatori și/sau echipamente sunt afectate.

Cu ajutorul SecureX, responsabilii cu securitatea informatică pot realiza acțiunile de investigare și remediere dintr-o singură consolă, blocând fișiere și domenii suspicioase și izolând echipamentele compromise de restul rețelei, fără a fi nevoie să mai acceseze celelalte produse de securitate IT.

Servicii asigurate de Datanet Systems

O ofertă cu performanță garantată

Produsele de securitate Cisco recomandate de Datanet sunt soluții de top, cu tehnologii mature și performanțe confirmate. De altfel, conform institutului independent de cercetare **AV-TEST**, Umbrella este lider pe piața soluțiilor de detectare a amenințărilor și protejare a angajaților care lucrează la distantă. La rândul său, soluția Secure Endpoint a primit distincția Approved Business Security Award din partea **AV-Comparatives**. Totodată, Cisco este **lider pe piața firewall-urilor de nouă generație**, dar și a soluțiilor de securizare a serviciilor de email, conform clasamentelor **Radicati** și **Frost & Sullivan**.
Nu în ultimul rând, SecureX este tehnologia cu cea mai rapidă adopție din istoria companiei, ajungând la peste 9.000 de clienți la doar trei luni de la lansare.

Pentru a obține rezultate optime prin exploatarea produselor Cisco incluse în aceasta broşură, Datanet Systems vă oferă următoarele servicii:
• implementarea soluțiilor de securitate recomandate (Secure Firewall, Secure Email, Secure Endpoint și Umbrella);
• integrarea acestora în SecureX;
• configurarea fluxurilor de date transmise de aplicații în platforma Cloud, în funcție de specificul fiecărei organizaţii;
• personalizarea tablourilor de bord pentru a avea acces rapid la informații relevante.

Expertiza echipei Datanet este utilă sau, după caz, necesară şi pentru automatizarea şi orchestrarea proceselor cu ajutorul SecureX. Platforma Cloud Cisco integrează un modul dedicat pentru definirea unor seturi de acțiuni pentru automatizarea proceselor repetitive. Totodată, specialiștii Datanet vă pot ajuta să organizați și coordonați procesele – automatizate sau nu – prin instrumentele de orchestrare incluse în SecureX, creând astfel fluxuri de lucru configurate pe caracteristicile infrastructurii pe care o deținеți și pe cerințele specifice.

Automatizarea și orchestrarea proceselor de monitorizare, detecție și analiză a evenimentelor vă ajută să:
• Eliminați sarcinile repetitive;
• Reduceți riscul apariției erorilor umane;
• Scădeți nivelul de încărcare al departamentului IT și realocați personalul specializat;
• Diminuați cheltuielile operaționale;
• Creșteți viteza de detecție și de răspuns la amenințări;

Servicii asigurate de Datanet Systems

Un exemplu concret al modului în care Datanet și oferta integrată de soluții Cisco vă pot ajuta să îmbunătățiți securitatea companiei este crearea unui flux de lucru pentru protecția împotriva atacurilor de phishing.

Phishing-ul este în prezent una dintre cele mai cele mai răspândite amenințări, care crește constant ca volum și reprezintă principalul vector de propagare al malware-ului. 97% dintre angajații companiilor nu au însă competențele necesare pentru a recunoaște tentativele sofisticate de phishing, care sunt tot mai frecvente.

Pentru a ține sub control acest risc, specialiștii Datanet pot dezvolta un flux de lucru dedicat, prin care un utilizator care primește un mail suspect îl poate expedia – prin intermediul workflow-ului creat – către analiză în SecureX. Fluxul permite ca, în funcție de rezultatele analizei email-ului și regulile companiei, SecureX să realizeze automat mai multe acțiuni: deschiderea unui incident, emiterea unei alerte, etc. După semnalarea evenimentului, echipa IT poate realiza direct din platforma Cloud Cisco investigații detaliate – pentru a afla ce alți utilizatori au mai fost compromiși, de exemplu – și poate lua acțiunile adecvate, precum punerea lor în carantină, blocarea adreselor URL din mail-ul suspect, blocarea adresei de expediere etc.

Un astfel de workflow vă ajută să depistați și să blocați rapid amenințările şi valorifică la maxim potențialul soluțiilor Cisco recomandate, care colaborează între ele și acționează integrat prin intermediul SecureX.

Posibilitățile pe zona de automatizare și orchestrare ale ofertei integrate Datanet sunt, practic, nelimitate, iar specialiștii noștri vă pot ajuta să le realizați și personalizați pe diverse scenarii de lucru. În plus, oferta Datanet include servicii de training și transfer de cunoştinţe, prin intermediul căruia specialiștii IT beneficiari sunt învățați cum să opereze soluțiile, să realizeze automatizări, să creeze alerte și fluxuri de lucru personalizate etc.

Pentru mai multe informații tehnice și comerciale despre conceptul XDR, oferta integrată de soluții de securitate Cisco – Secure Email, Secure Endpoint, Umbrella, Secure Firewall, SecureX – și despre serviciile livrate de Datanet Systems, contactaţi-ne la sales@datanets.ro .

Servicii asigurate de Datanet Systems

Pachetul standard de servicii oferit de Datanet Systems include:

- analiza cerințelor tehnice ale clientului;
- definirea arhitecturii optime;
- realizarea proiectului de detaliu al soluției tehnice;
- instalarea, punerea în funcțiune și configurarea produselor;
- ajustarea și validarea caracteristicilor de sistem obținute;
- instruirea privind utilizarea soluțiilor;
- asistență tehnică și activitate de service cu timp garantat de remediere a defecțiunilor.

Datanet
SYSTEMSINTEGRATION
SOITRON GROUP

Datanet Systems SRL
Strada Sfântul Elefterie nr. 18
Clădirea Elefterie, Parter, etaj 1 parte A
București, 050525, România
Tel: +4 021 317 87 87 / Fax: +4 021 317 97 97
Cod Fiscal: R10363046; J40/2905/1998
office@datanets.ro / www.datanets.ro