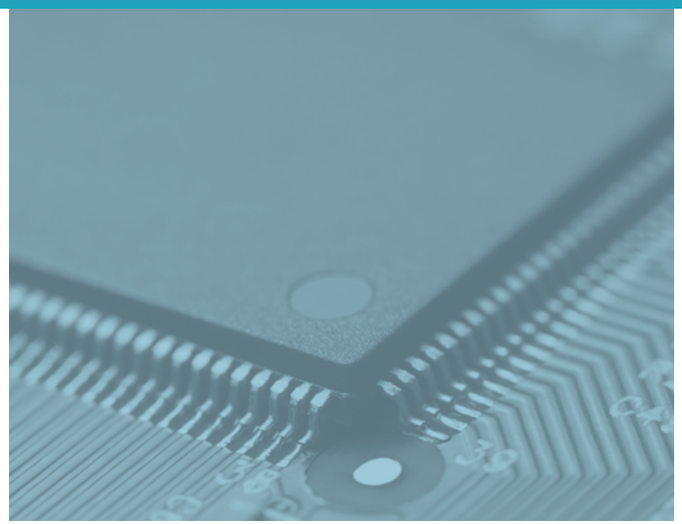
CoMSec

MANAGED SECURITY SERVICES

KOLIKO JE SIGURNA VAŠA TVRTKA?



Na tržištu funkcioniraju dvije vrste kompanija. One koje već znaju da su napadnute i one koje za to još nisu saznale. Razvojem novih, sve boljih i sofisticiranijih metoda sigurnosnih napada, poslovna okruženja više nisu u mogućnosti pratiti trendove sigurnosti u IT svijetu. Stoga se poslovni subjekti sve više okreću IT tvrtkama specijaliziranim upravo za sigurnost. COMBIS kao Managed Security Services Provider (MSSP) pouzdan je partner koji pruža vrhunski izbor objedinjenih sigurnosnih usluga! Naša misija je pojednostaviti i ubrzati IT procese, a da pri tome poboljšamo vašu produktivnost i umanjimo troškove.

LJUDI
TEHNOLOGIJA
PROCESI

MI U COMBISU OSIGURAVAMO TRI KLJUČNA ELEMENTA:

STRUČNJAKE
Koji vladaju specijaliziranim znanjima i vještinama iz različitih područja informacijske sigurnosti.

VRHUNSKU TEHNOLOGIJU
Koja je u mogućnosti identificirati najkompleksnije sigurnosne ugroze.

PROCESE
Koje možemo prilagoditi svim potrebama i željama unutar bilo kojeg radnog okruženja.

NAŠ PRISTUP

Vaš *in-house* tim stručnjaka može analizirati samo prijetnje koje se događaju u okruženju za koje je nadležan. S druge strane, **COMBISov tim stručnjaka** se svakodnevno susreće s raznovrsnim prijetnjama u mnogobrojnim okruženjima. Praćenje aktualnih sigurnosnih prijetnji, tehnoloških noviteta i kompleksnosti prepustite nama jer je to naš primarni posao.

NUDIMO VAM SLJEDEĆE USLUGE

UPRAVLJANJE PRIJETNJAMA I INCIDENTIMA

PRAĆENJE INCIDENATA

Raspolažete s velikim brojem sigurnosnih uređaja? Niste u mogućnosti pravovremeno pratiti sve sigurnosne događaje u sustavu? Teško razlikujete bitne od nebitnih incidenata? Sve se čini tako kompleksno...? Prepustite nadzor nama! Aktivnim praćenjem događaja u sustavu pouzdano možemo izdvojiti ključne događaje i pravovremeno vas upozoriti.

ODGOVOR NA INCIDENTE

Zaprimanjem incidenta tek započinje borba protiv malicioznih događaja. Detaljnom analizom i povezivanjem događaja iz više izvora možemo preciznije utvrditi pravi uzrok problema, a jasnim preporukama i brzim djelovanjem suzbijamo daljnje širenje ugroze u sustavu.

PODEŠAVANJE SUSTAVA

Sustav generira prevelik broj alarma? Ne funkcionira prema očekivanjima? Procijenili ste da tehnologija s kojom raspolažete nije maksimalno iskorištena? Svaki sustav je dinamičan i potrebne su stalne prilagodbe kako bi se postigla zadovoljavajuća razina efikasnosti. Konstantnim poboljšanjima, sigurnosne komponente možemo iskoristiti znatno bolje.

DINAMIČKA ANALIZA MALICIOZNOG SADRŽAJA

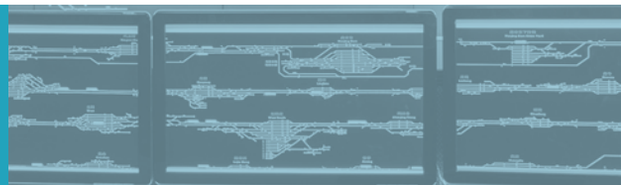
Stigao je e-mail upitnog sadržaja, sumnjivi prilog ili internetski link? Oni u sebi mogu sadržavati maliciozan kôd pa je tako ponekad dovoljan i jedan klik koji će ugroziti poslovanje cijele tvrtke. Na zahtjev, možete zatražiti dinamičku analizu upitnih datoteka te se na taj način uvjeriti u njihovu ispravnost i prije nego ih aktivirate na računalu tvrtke.

RUČNA ANALIZA MALICIOZNOG SADRŽAJA

Želite li znati kontekst napada? Ručna analiza upitnih datoteka korak je više u odnosu na dinamičku analitiku. Često prilikom ručnog pregledavanja koda imamo uvid u detaljan tijek i rad malicioznog koda, možemo shvatiti njegovu svrhu i samim time dodatno preventivno prilagoditi vlastiti sustav zaštite s ciljem povećanja efikasnosti.

IZVJEŠTAVANJE

Izvještavanje je iznimno bitno. Kombinacijom grafičkih, tabličnih i tekstualnih elemenata podaci se moraju prikazati na svima jasan, pregledan i čitljiv način. Bitno je da izvještaj sadrži ključne informacije, čime se uz utrošak minimalnog vremena, pruža kvalitetan uvid u povijest sigurnosnih događaja u sustavu.



SAVJETOVANJE

Planiranje razvoja i rasta infrastrukture ključan je element za poboljšanje poslovanja. Naše savjetodavne usluge prije integracije željenog sustava, odabira metodologije, boljih procesa, nove tehnologije, pomoći će vam da osigurate najbolje rješenje za vaše poslovanje.

USMJERAVAMO VAS DA PAMETNO I SMISLENO ULAŽETE U SVOJU INFRASTRUKTURU.

PRUŽAMO ŠIRU SLIKU POTENCIJALNIH PROBLEMA, A NE SAMO UVID U ODREĐENOM TRENUTKU.

UPRAVLJANJE RANJIVOSTIMA

SKENIRANJE RANJIVOSTI

Skeniranje ranjivosti s vrhunskim alatom uključuje analizu rezultata, konzultacije i preporuke za uklanjanje detektiranih ranjivosti. Skenovi su najčešće periodički i mogu udovoljiti potrebnim sigurnosnim standardima, no djeluju reaktivno, a ne proaktivno.

PRAĆENJE RANJIVOSTI i EXPLOITa

Kao nadogradnja klasičnom skeniranju ranjivosti, više ne morate čekati periodičke skenove ranjivosti da biste otkrili nove sigurnosne propuste. Na dnevnoj bazi aktivno pratimo pojavu novih sigurnosnih propusta i pripadajućih exploita koji su u vašem sustavu. Izrađujemo plan hitnog uklanjanja, eliminiramo i sigurnosnim testom potvrđujemo efikasno uklonjenu ranjivost.

PENETRACIJSKI TESTOVI

Penetracijski testovi uključuju i ljudski faktor u analizu. Kombinacijom ručnih i automatiziranih metoda možemo pružiti bolji uvid u trenutnu razinu sigurnosti, uz izradu detaljnog izvještaja s pronalascima i sugestijama za njihovo uklanjanje. Svaki penetracijski test uključuje i ponovni test nakon ispravaka, a s ciljem utvrđivanja efikasnosti svih primijenjenih korekcija. Penetracijske testove provodimo vodeći se priznatim metodologijama kao što su OWASP, ISSAF i druge.

ODMAH IMATE SAZNANJE O POJAVI JAVNO DOSTUPNOG EXPLOITA, NEMA ČEKANJA PERIODIČKIH SKENOVA.

IZVRŠAVANJE PENETRACIJSKIH TESTOVA PO POTREBI I TO ODMAH NAKON IZMJENA NA SUSTAVU.

RUČNA ANALIZA POTENCIJALNIH RANJIVOSTI DAJE DODATNU DIMENZIJU I UVID U STANJE SUSTAVA. AUTOMATIZIRANI ALATI ZA DETEKCIJU RANJIVOSTI IPAK NEMAJU MAŠTU NAPADAČA.

OSIGURAVANJE USKLAĐENOSTI

PODEŠAVANJE SIEMa

Naše iskustvo govori da je SIEM sustav koji zahtjeva kontinuiran rad i poboljšanja. Često u nedostatku vremena, ovaj iznimno bitan element nije u potpunosti iskorišten. Pravilnom integracijom te analizom korisničkih potreba možemo definirati kompleksne zahtjeve okruženja i podesiti sustav da radi pametnije.

REVIZIJA KONFIGURACIJSKIH POSTAVKI i OSNAŽIVANJE SUSTAVA

Pregledom konfiguracijskih postavki na operacijskim sustavima, bazama podataka, raznovrsnim servisima i mrežnim uređajima možemo uočiti nedostatke, predložiti moguće scenarije dodatnih prilagodbi, izraditi odgovarajuće izvještaje i sugerirati korekcije na sustavu s ciljem poboljšanja. Revidiranje i korekcije vršimo s ciljem usklađivanja s potrebnim sigurnosnim standardima, ali i radi unapređenja preventivnih mjera.

PRIPREMA ZA AUDIT

Priprema za revizijske nadzore često može biti vremenski iznimno zahtjevna: točno specificirani izvještaji, odgovarajuće upravljanje podacima, adekvatno provedeni procesi i brojni drugi zahtjevi. Konzultirajte se s nama, iskoristite naše znanje i iskustvo kako bi priprema bila sistematična, temeljita i potpuna!

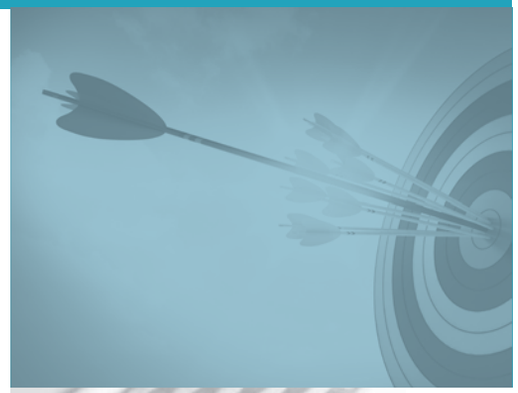
OPTIMIZACIJA I KONSTANTNA PRILAGODBA SIEMA, MAKSIMALNO ISKORIŠTAVANJE FUNKCIONALNOSTI.

DETALJAN UVID U AKTIVNOSTI SUSTAVA.

TEMELJITA PRIPREMA ZA REVIZIJSKI NADZOR.

ISPUNJENA "REVIZIJSKA KVAČICA" NEĆE OSTATI SAMO NA TOME, JER MI MOŽEMO PRUŽITI VIŠE.

KLJUČNE POSLOVNE PREDNOSTI



SMANJEN SIGURNOSNI RIZIK

Primjenom vrhunske tehnologije, znanjem i maksimalnim iskorištavanjem svih potencijala koji su nam na raspolaganju, povećavamo efikasnost detekcije sigurnosnih ugroza. Mi imamo know-how, a upravo to je najbitnija karika u lancu sigurnosti.

FOKUS NA POSLOVANJE

Angažiranjem COMBISa kao MSS Providera moći ćete se fokusirati na vaš *core business*, a sve ostalo prepustite nama!

KONTINUIRANI NADZOR

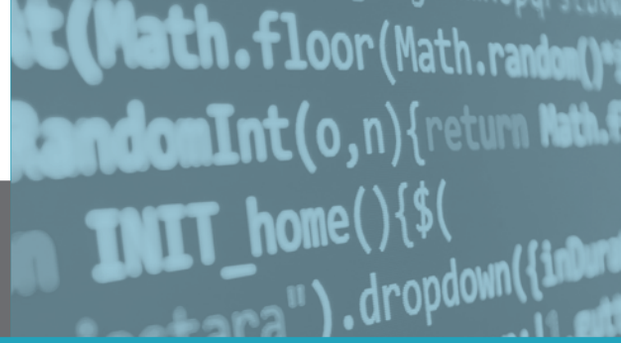
Kontinuiranim nadzorom incidenti se uočavaju i preuzimaju odmah pa je vrijeme reakcije i rješavanja svedeno na minimum.

SMANJENI TROŠKOVI

Biti u korak s vremenom znači konstantno ulagati u specijalizirana školovanja i skupa tehnološka rješenja, što stvara dodatne troškove. Uz COMBIS vrhunsko znanje i tehnologija uvijek su vam na raspolaganju!

KOME SU NAMIJENJENE USLUGE?

Svaka ozbiljna tvrtka svjesna je važnosti zaštite poslovnog sustava. Naše usluge namijenjene su poslovnim subjektima i organizacijama svih veličina, a dobiti su višestruke! COMBISove usluge osiguravaju vrhunsku zaštitu uz optimalan trošak!



ZAŠTO COMBIS?

NAŠ TIM JE I VAŠ TIM

Kao nadogradnja vašem timu, uspostavom kvalitetne komunikacije, funkcionirat ćemo kao cjelina. Iskoristite prednost velikog broja naših stručnjaka i smatrajte naš tim vašim timom.

AKTIVNO PRAĆENJE OPASNOSTI

Neprekidno pratimo događanja vezana uz sigurnost. U mogućnosti smo iznimno brzo upozoriti na potencijalne opasnosti i negativne trendove koje smo uočili ne samo kod vas, već i kod drugih korisnika. Sve s ciljem pravovremene prevencije i vrhunske zaštite!

KONTINUIRANO ULAGANJE

COMBIS kontinuirano ulaže u edukaciju svojih djelatnika kroz stručna usavršavanja, seminare i edukacije. Posjedujemo zavidnu kolekciju priznatih industrijskih certifikata s područja računalne sigurnosti: CISSP, CCIE Security, OSCE, GMON, GREM, GSNA i mnoge druge.

ISO CERTIFIED

COMBIS posjeduje certifikat ISO 27001 koji jamči da s podacima postupamo odgovorno!

S NAMA JE VAŠE POSLOVANJE SIGURNO! ZATO NAM SE SLOBODNO I VI OBRATITE S POVJERENJEM!

Za dodatne informacije o uslugama upravljanja sigurnošću slobodno nam se obratite na:
T: +385 1 3651 222, E: security@combis.eu
www.combis.hr