SOC usluge

Upravljane usluge iz domena operativne bezbednosti – SecOps / SOC

Unicom Systems

Security Operations Center (SOC) je organizacija bazirana na ljudima, procesima i tehnologijama, čiji je cilj prevencija, detekcija, odgovor na sajber-bezbednosne incidente. Postoje i drugi slični termini koji se koriste u praksi često kao sinonimi - Computer Security Incident Response Team (CSIRT), Computer Emergency Response Team (CERT).

SOC/CERT predstavlja holistički pristup informacionoj bezbednosti, u smislu da su pored tehnologije/rešenja uključeni ljudski resursi u vidu operativnog praćenja i ekspertize, upravljani procedurama zasnovanim na preporukama i dobroj praksi. Često se u praksi prilikom rešavanja bezbednosnih problema pribegava kupovini ili upotrebi kroz uslugu samo tehnoloških rešenja. Uz nedostatak odgovarajućih ljudskih kapaciteta koji mogu da prate 24/7 (incidenti se događaju 24 časa dnevno 7 dana u nedelji i nemaju radno vreme) i ekspertize tehnološka rešenja ne donose očekivane rezultate. Sa druge strane upošljavanje operativnog tima i eksperata zahteva velike izdatke, koje često ni velike kompanije ne mogu da priušte. SOC/CERT usluge pored tehnološke komponente stavljaju fokus na operativnu bezbednost (*SecOps*) kao i na raspoloživu ekspertizu kroz uslugu kao autsorsing ili deo upravljane usluge i time znatno snižavaju troškove u odnosu da slične funkcije sprovode kroz interne resurse (koje često i ne postoje). Pored smanjenih troškova, ovaj pristup je efikasniji tj. donosi rezultate u smanjivanju bezbednosnih rizika u odnosu na „klasičan“ tehnološki fokusiran pristup.

Opis usluge

SOC/CERT usluge ne predstavljaju jedno univerzalno rešenje, već se kroz sve raspoložive gradivne elemente uklapaju u odnosu na potrebe, mogućnosti i regulatorne zahteve. Krajnja usluga koja može da zadovolji sve kriterijume predstavlja kombinaciju potrebnih gradivnih elemenata.

Kroz 6 gradivnih elemenata u mogućnosti smo da pokrijemo ceo spektar potreba u informacionoj bezbednosti:

UniSEC usluge

UniSEC usluge

- EDR – Zaštita radnih stanica
- APP – Zaštita aplikacija
- INFRA – Zaštita infrastrukture
- DLP – Zaštita informacija
- WEB – Mrežna bezbednost
- MAIL – Email bezbednost

UniSec usluge predstavljaju zasebne i zaokružene usluge sa ciljem rešavanja specifičnih bezbednosnih rizika. One takođe samo po sebi uključuju SOC/CERT usluge u vidu operativne bezbednosti, ekspertske analize i podrške u odgovoru na incidente. Sa druge strane, zajedno sa ovde nabrojanim SOC/CERT uslugama doprinose boljoj i kvalitetnijoj detekciji i odgovoru na incidente povećavajući vidljivost nad informacionim sistemom. Na primer, kroz zaštitu radnih stanica dobija se mogućnost sagledavanja svih događaja na radnim stanicama iz bezbednosnog aspekta čime se dobija kvalitetnija slika o sveukupnim pretnjama po organizaciju što inače ne bi bilo moguće. Ista je situacija sa povećanjem vidljivosti na infrastrukturi, web i mail kanalima i kretanju informacija. Što je kvalitetnija slika o sistemu, time se povećava i kvalitet detekcije i mogućnost odgovora na incident. Više informacija UniSEC uslugama je dostupno kroz zasebne brošure ili preko web-a: http://unicom.systemsIsporuka SIEM-a

Isporuka SIEM-a

Isporuka SIEM-a

- On-premise – na lokaciji korisnika
- Cloud – infrastruktura u okviru UniCERT-a
- Hybrid – kombinovano
- UEBA – User and Entity Behaviour Analytics

SIEM (Security Incident and Event Management) predstavlja osnovni alat za detekciju incidenata. SIEM vrši prikupljanje logova iz različitih izvora sistema (Firewall, IDS/IPS, anti-virus, AD, sistemi za zaštitu web i mail saobraćaja, baze podataka, web serveri…), mrežnog saobraćaja i drugih tipova informacija iz IT sistema i korelacijom tih podataka sa „ugrađenom inteligencijom“, dinamičkim obaveštajnim podacima i podešenim pravilima detektuje potencijalne pretnje i incidente. SIEM predstavlja centralnu tačku za sva bezbednosna rešenja gde se kroz koji se jedinstveno sagledavaju sve informacije vezane za bezbednost informacionog sistema. Samim tim, operativna bezbednost (SecOps) ne može da se zamisli bez ovakvog sveobuhvatnog pristupa. SIEM se može isporučiti na različite načine, u zavisnosti od potreba, mogućnosti i regulatornih ograničenja:

On-premise – svi elementi SIEM rešenja, u potpunosti na lokaciji korisnika. Ovo je najčešći scenario kada postoje regulatorna ograničenja i kada korisnik sam želi da upravlja rešenjem.

Cloud – svi elementi SIEM rešenja se nalaze u okviru UniCERT-a. Prednosti ovog pristupa su jednostavna i brza realizacija, kako nije potrebna instalacija korisničke opreme i samim tim i jeftinija.

Hybrid – pristup koji kombinuje prednosti oba gore navedena modaliteta. Prikupljanje podataka kao i skladištenje ostaje u perimetru korisnikovog sistema (najčešće iz regulatornih razloga) dok se centralno upravljanje vrši iz UniCERT-a, najčešće u kombinaciji sa uslugom upravljanja SIEM-om i drugim SOC/CERT uslugama.

User & Entity Behaviour Analytics (UEBA) – (analiza ponašanja korisnika i drugih entiteta) predstavlja naprednu tehnologiju detekcije incidenata (kroz mašinsko učenje, algoritme i statističku analizu) stavljanjem u fokus korisnika i drugih entiteta, praćenjem njihovog ponašanja i detekcijom nepravilnosti i odstupanja. Ova funkcionalnost je modularna u odnosu na bilo koje SIEM rešenje i donosi značajan doprinos u pravovremenom otkrivanju pretnji.

UniCERT može da isporuči SIEM rešenja različitih proizvođača, ukoliko postoji preferenca od strane korisnika za nekim određenim rešenjem.

Upravljanje SIEM-om

Upravljanje SIEM-om

- Potpuno upravljanje (Fully managed)
- Hibridno / deljeno upravljanje (Hybrid / Co-managed)

Upravljanje SIEM-om podrazumeva sve operacije vezane za efikasno funkcionisanje SIEM rešenja – od praćenja infrastrukture na kojoj se izvršava, konfiguraciju rešenja, postavljanje i redovno prilagođavanje pravila. Najčešće se kombinuje sa drugim SOC/CERT uslugama, bilo da se radi o već postojećem SIEM-u kod korisnika ili u okviru usluge isporuke SIEM-a., kroz različite modalitete u zavisnosti od zahteva korisnika:

Fully Managed – Potpuno preuzimanje operativne odgovornosti nad SIEM rešenjem. Korisnik može da traži promenu ili dodavanje novih pravila po zahtevom, bez potrebe za poznavanjem rešenja i bez potrebe za direktnim pristupom SIEM rešenju. Takođe, korisnik može u potpunosti da prepusti i ažuriranje pravila u odnosu na potrebe i pretnje, najčešće u kombinaciji sa drugim uslugama (Monitoring i detekcija, odgovor na incidente)

Hybrid / Co-managed – Hibridno upravljanje podrazumeva deljenje upravljanje između klijenta i UniCERT-a. Korisnik zadržava kontrolu i vidljivost nad sistemom u skladu sa potrebama i mogućnostima, dok se proizvoljne odgovornosti i funkcije autsorsuju u okviru usluge (uglavnom složenije operacije koje zahtevaju ekspertizu ili operacije koje zahtevaju redovno praćenje 24/7)

Monitoring i detekcija

Monitoring i detekcija

- SOC Monitoring – Operativno praćenje 24/7
- Security Analyst – Analiza incidenata

Usluge monitoringa i detekcije uz odgovor na incidente predstavljaju ključne elemente operativne bezbednosti (SecOps) koje je teško ili neisplativo izgraditi kao interne resurse unutar organizacije. Sa druge strane upravo operativan pristup obezbeđuje najveću efikasnost u sprovođenju bezbednosne politike. Usluge monitoringa i detekcije stavljaju na raspolaganje 24/7 dostupan operativni tim, kao i ekspertski tim koji nadzire i reaguje u slučaju pretnji i incidenata.

SOC Monitoring – operativno 24/7/365 praćenje informacionog sistema najčešće kroz SIEM rešenje i eskalacija u slučaju pretnje ili incidenta.

Security Analyst – podrazumeva sprovođenje trijaže nad detektovanim pretnjama i incidentima, utvrđivanje lažnih pozitiva (false psitive) tj. da detektovani događaj zapravo nije pretnja ili incident, sprovođenje dublje analize po potrebi i komunikacija sa ostalim timovima koji vrše operativno praćenje, upravljanje SIEM-om (u svrsi dodavanja novih pravila ili izmene) i odgovor na incidente. Najčešće se usluga Security Analyst kombinuje sa uslugom podrške u odgovoru na incident (IR Support) kroz preporuke u vidu mera koje treba da se sprovedu kako bi se otklonile negativne posledice incidenta i sprečili budući slični incidenti.

Odgovor na incidente

Odgovor na incidente

- IR Support – Preporuke u odgovoru na incidente
- IR Execution – Sprovođenje odgovora na incidente
- Threat Hunting – Pronalaženje pretnji
- Forensic Analysis – Forenzička analiza

I pored najboljih mehanizama prevencije, incident može da se dogodi. Blagovremeni odgovor na incidente i blagovremeno otklanjanje posledica incidenta je druga ključna komponenta (pored detekcije i prevencije) efikasne zaštite. Opšte je prihvaćena krilatica da nije pitanje da li će se incident dogoditi, već kada.

Usluge odgovora na incidente pokrivaju različite modalitete angažovanja:

Incident Response Support – uz sprovedenu detaljnu analizu podrška u okviru odgovora na incident podrazumeva pravovremenu izradu preporuka za: suzbijanje dejstva incidenta, sprovođenje mera eradikcije (potpuna eliminacija svih tragova incidenta), oporavak sistema i mere koje treba sprovesti kako se sličan incident ne bi ponovo dogodio. Kroz ovu uslugu se ne sprovode direktne mere na informacionom sistemu korisnika, već se putem preporuka savetuje korisnik koje mere treba da preduzme, kako UniCERT nema mogućnost upravljanja nad informacionim sistemom korisnika.

Incident Response Execution – podrazumeva isti obim aktivnosti kao i kod podrške u odgovoru na incidente, ali uz delimičnu ili potpunu mogućnost sprovođenja mera nad informacionim sistemom korisnika. Ova usluga je moguća ukoliko je korisnik preneo delimično ili u celosti ovlašćenja upravljanja nad sistemom korisnika, ili po potrebi uz dozvolu korisnika u situacijama koje to zahtevaju putem bezbedne udaljene veze ili na lokaciji korisnika.

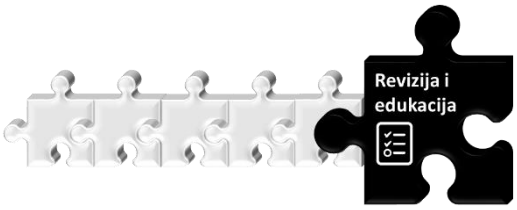
Forensic Analysis – Forenzička analiza u zavisnosti od potreba može da obuhvati prikupljanje digitalnih dokaza (sakupljanje, skladištenje, dokumentaciju) i analizu artefakata (memorija, disk, mreža…) kompromitovanih delova sistema sa ciljem rekonstrukcije incidenta. Forenzička analiza se sprovodi u cilju produbljivanja informacija o incidentu i uzročnicima incidenta kako bi se na osnovu te analize sproveli dalji koraci koje će poboljšati bezbednost sistema. Uglavnom se sprovodi kao ad-hoc usluga i kao podrška u odgovoru na incidente.

Posebno možemo da izdvojimo forenzičku analizu zlonamernih programa – malvera (***Malware Analysis***).

Revizija i edukacija

Revizija i edukacija

- Risk Assessment – Bezbednosna revizija
- Vulnerability assessment – Testiranje na ranjivosti
- Penetration testing – Testiranje iz ugla napadača
- Awareness trainings – Obuke za zaposlene
- Security trainings – Obuke za IT/bezbednosne kadrove
- Blue teaming / war games – Simulacije napada



Usluge iz domena revizije i edukacije dalje učvršćuju bezbednost sistema fokusirajući se ispitivanje trenutnog stanja sistema, pravila i procedura kao i na ljudski faktor koji je najčešće predstavlja najslabiju kariku. Iz domena revizija nudimo sledeće usluge:

Risk Assessement – je usluga bezbednosne revizije sistema bazirana na analizi politika vezanih za bezbednost, pravila, dokumentacije, arhitekture i dizajna informacionog sistema, konfiguracije uređaja, rešenja i aplikacija, intervjuima sa zaposlenima, utvrđivanju neregularnosti iz log poruka itd. Cilj revizije utvrđivanje neregularnosti u odnosu na dobru praksu i regulativu kao i predlog mera u otklanjanju neregularnosti u skladu sa poslovnim potrebama, informacionim sistemom i mogućnostima.

Vulnerability Assessement – Ispitivanje/skeniranje sistema na ranjivosti upotrebom odgovarajućih alata uz ekspertsku analizu konsultantskog tima. Cilj je dobijanje realnog izveštaja ranjivosti sa jasno definisanim preporukama u saniranju istih, sa fokusom i prioritetom, bez nepotrebnih i irelevantnih detalja (koji su često deo izveštaja koji se generiše samo uz pomoć alata).

Penetration Testing (PenTest) – je najefikasniji mehanizam utvrđivanja ranjivosti, korišćenjem metoda i pristupa kojom se koriste sajber-kriminalci. Za razliku od usluge skeniranja na ranjivosti, PenTest ide korak dalje i nakon utvrđenih ranjivosti vrši se zloupotreba istih sa ciljem infiltracije u sistem. Na taj način se dobija realna slika o ranjivostima i propustima u informacionom sistemu. Za razliku od pravih napada, u toku „etičkog hakinga“ se poklanja naročita pažnja da aktivnosti ne naruše rad informacionog sistema. U sklopu PenTest usluga možemo da ponudimo različite pristupe u zavisnosti od potrebe: PenTest informacionog

sistema u celosti, PenTest web aplikacija, PenTest mobilnih aplikacija, PenTest bežične mreže kao i PenTest koji uključuje socijalni inženjering. Cilj je dobijanje izveštaja koji će pokazati sve slabosti sistema, kroz transparentno prikazane metode kako su napadi sprovedeni i kako su ranjivosti zloupotrebljene sa odgovarajućim preporukama.

Sve ove usluge mogu se sprovoditi ad-hoc po zahtevu ili regularno (polugodišnje, kvartalno…) u skladu sa učestalošću promena u informacionom sistemu.

Kako je ljudski faktor najslabija karika u sajber-bezbednosti sistema, efikasna edukacija može značajno da doprinese povećanju sajber-bezbednosne svesti i time smanji rizike. Usluge iz domena edukacije su:

Awareness Training – imaju za svrhu povećanje svesti zaposlenih o mogućim rizicima i o opštim pravilima sajber-bezbednosne higijene. Ovakvi treninzi imaju kratku formu i namenjeni su svim zaposlenima bez obzira na njihov profil i edukaciju. Edukacija vrši uz realne primere moguće zloupotrebe (npr. pokazuje se šta se dešava u pozadini kada se klikne na neki link koji predstavlja virus, kao funkcioniše socijalni inženjering itd.)

Security Training – treninzi namenjeni sajber-bezbednosnim i IT profesionalcima. Nudimo različite treninge od tehnoloških (veznih za određena rešenja ili univerzalna znanja iz bezbednosne operative) do organizacionih.

Blue Teaming / War Games – Sajber vežbe omogućavaju testiranje i razvoj kapaciteta timova i pojedinaca kroz simulaciju realnih pretnji i napada. Sajber vežbe, za razliku od stvarnih napada, omogućavaju učesnicima kroz podršku organizatora i odgovarajućih alata, da bez pritiska od stvarnih rizika analitički pristupe problemu. Rezultat sajber vežbe treba da bude bolje poznavanje različitih pretnji, anatomije napada, sticanje primenjivih znanja u efikasnom odgovoru na incident kao i poboljšanju mehanizama prevencije i detekcije.

Primeri usluga

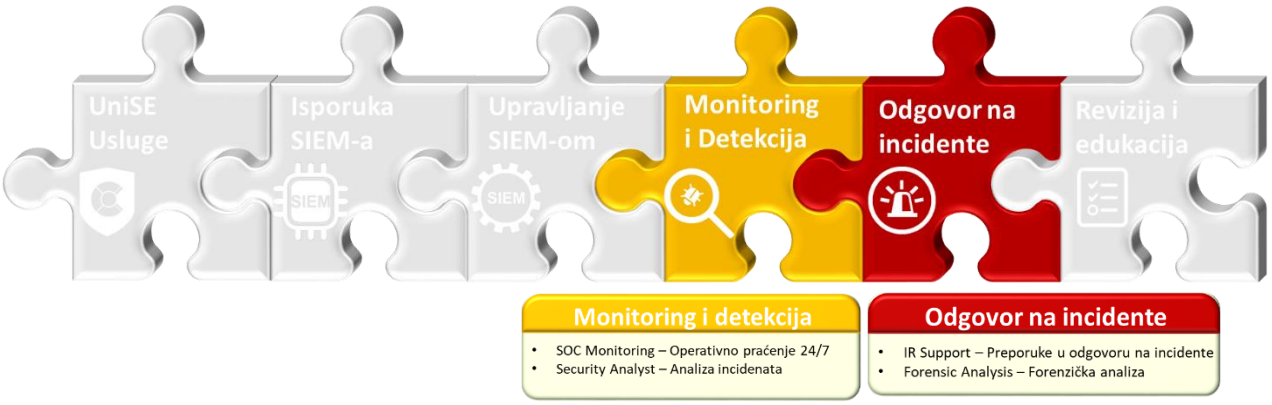
Uz pomoć gore navedenih gradivnih elemenata daćemo nekoliko primera usluga koje se uklapaju u specifične potrebe korisnika imajući u vidu trenutno stanje informacionog sistema i resursa, potrebe i ograničenja.

Primer 1a.

Korisnik u ima IT službu i kadrove zadužene za informacionu bezbednost. Takođe ima SIEM sistem u upotrebi. Zbog velike opterećenosti IT službe i službe za bezbednost, nisu u mogućnosti da adekvatno prate događaje na SIEM sistemu, javlja se velika lažnih incidenata (false positive) što unosi još dodatni šum.

Alternativa bi bila zapošljavanje dodatnih kadrova koji bi mogli operativno da prate događaje, da analiziraju incidente na osnovu kojih bi mogli da preduzmu odgovarajuće korake kao odgovor na incidente i „kalibrišu“ SIEM sistem kako bi minimizovali lažne pozitive. Takav scenario bi bio suviše skup, kako je za 24/7 operativni centar potrebno izdvojiti minimum 5 ljudi, plus eksperta koji bi mogao da vrši analizu.

Kroz SOC/CERT uslugu korisnik može da ostvari svoje potrebe uz znatno manje troškove, a dodatno se i oslobađa od odgovornosti vođenja operacija, koje se vode sa striktno zadatim SLA (Service Level Agreement) parametrima.



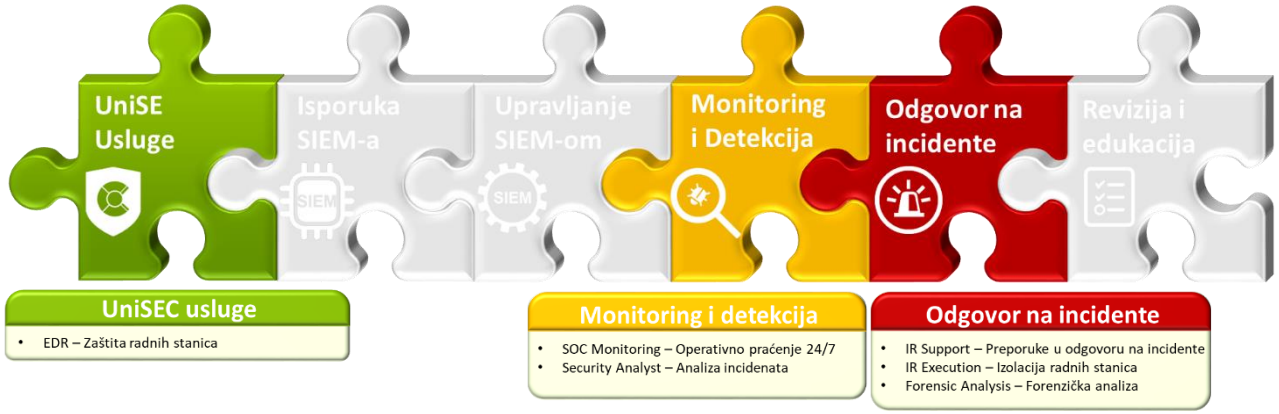
U ovom scenariju incidenti sa korisničkog SIEM-a preusmeravaju na UniCERT ili se kroz siguran kanal daje pristup UniCERT-u. Obaveze UniCERT-a su da operativno 24/7 prate incidente i vrše trijažu i analizu. U slučaju lažnih pozitiva ekspertski tim daje preporuke u konfiguraciji SIEM-a kako bi se eliminisali lažni pozitivi, a u slučaju da se analizom utvrdi da je došlo do incidenta – obaveštava se relevantno osoblje korisnika uz podršku i preporuke u odgovoru na incident. Po potrebi se vrši forenzička analiza malvera.

Ovakav scenario znatno eliminiše rizike značajno smanjujući broj incidenata pravovremenom reakcijom, kao i negativne posledice ukoliko se incident ipak dogodi, uz znatno manje troškove u odnosu na interne operacije.

Primer 1b.

Sličan scenario kao u Primeru 1a. što se tiče kapaciteta i potreba korisnika, ali se pojavljuje sve više incidenata na radnim stanicama pre svega ransomware-a, koji prolaze i pored postojećih sistema zaštite.

Pored navedenih prednosti kroz usluga monitoringa, detekcije i odgovora na incidente, usluga zaštite radnih stanica omogućava efikasnu odbranu od naprednih oblika napada (između ostalog i ransomware-a), pruža bolju vidljivost u sistem u smislu bezbednosti, omogućava forenzičku analizu radnih stanica, kao i mogućnost momentalne izolacije radne stanica u slučaju incidenta što predstavlja ujedno efikasan korak u odgovoru na incident.

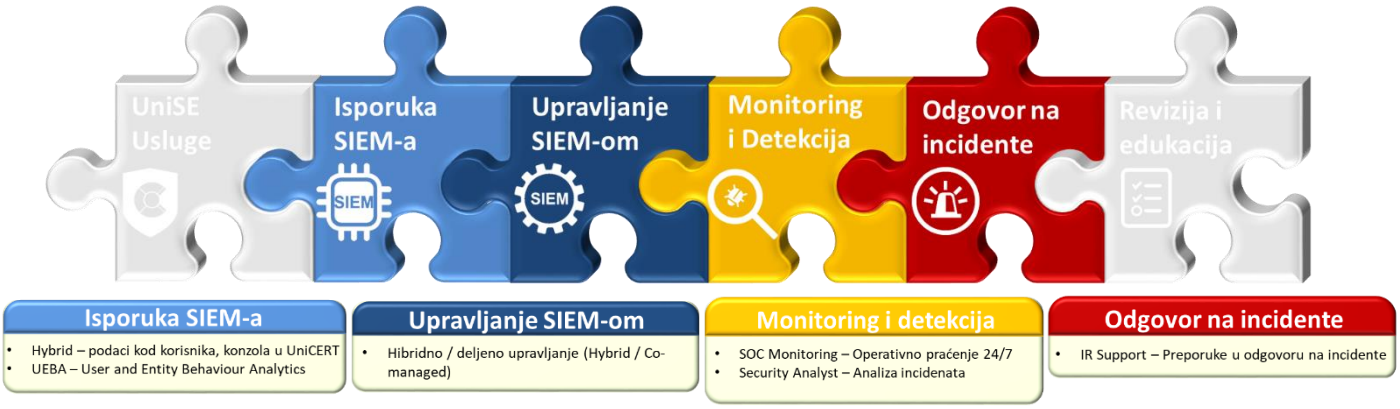


Primer 2.

Korisnik ima stari SIEM sistem koji više ne odgovara potrebama i planira da ga zameni. Nema raspoložive resurse koji se mogu baviti operativnom bezbednošću. Zahteva se brza implementacija, bez dugotrajnih testiranja i uklapanja. Pored toga želi da zadrži kontrolu nad sistemom i da autsorsuje operacije za koje nema kapacitete.

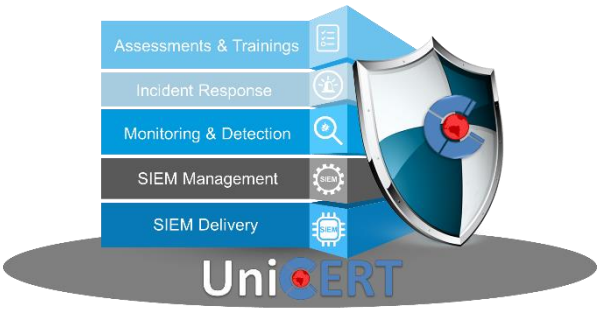
Kroz uslugu se isporučuje SIEM u hibridnoj arhitekturi – prikupljanje i skladištenje podataka na lokaciji korisnika (ovaj elemenat SIEM sistema se instantno instalira na postojeću virtuelnu infrastrukturu) u skladu sa regulativom, dok je upravljačka konzola u UniCERT-u. Inicijalnu konfiguraciju SIEM-a sprovodi UniCERT u skladu sa zahtevima korisnika, kao i dalje upravljanje (dodavanje novih pravila, eliminacija lažnih pozitiva…), dok korisnik zadržava potpuni pristup i kontrolu nad SIEM rešenjem. Po zahtevu korisnika deo SIEM rešenja je i UEBA analitika čime se postiže značajno bolja mogućnost detekcije pretnji i incidenata. UniCERT obavlja poslove operativne bezbednosti 24/7 monitoring, analizu i podršku u odgovoru na incident, slično kao u Primeru 1.

Korisnik bez potreba za inicijalnim ulaganjima, dobija uslugu koju plaća na mesečnoj bazi, po striktno zadatim servisnim uslovima SLA.



O UniCERT-u

UniCERT predstavlja organizacionu jedinicu unutar kompanije Unicom Systems čiji je cilj pružanje usluga iz domena sajber bezbednosti. Ključne delatnosti iz ovog domena su pružanje usluga operativne sajber-bezbednosti, odgovora na incidente i konsultativne usluge. UniCERT je registrovana CERT organizacija kod nadležne agencije (RATEL) u skladu sa zakonom o informacionoj bezbednosti.



Misija UniCERT-a je da kroz svoje usluge na pragmatičan i efikasan način pomogne korisnicima sa ciljem da se smanje rizici od sajber-bezbednosnih incidenata i njihovih posledica, što podrazumeva prevenciju, detekciju i odgovor na incidente. Usluge UniCERT-a treba da omoguće u širokom obimu ili delimično preuzimanje odgovornosti iz domena sajber-bezbednosti kako u organizacionom tako i u operativnom smislu sa naglaskom na ekspertizu i iskustvo koje UniCERT može da ponudi. Usluge predstavljaju pravu meru između ljudske ekspertize i prilagođene automatizacije procesa.

Šta je prednost naših usluga ?

Trenutna implementacija
Implementacija u istom danu od trenutka aktivacije servisa. Jednostavno puštanje u rad, tehnologija, procedure i ljudi spremni za pružanje usluge.

Vodeće tehnologije
Tehnologije koje se koriste u sklopu usluge prestavljaju vodeća rešenja iz svojih oblasti, odabrana da pruže najviši kvalitet i najbolju mogućnost integracije sa ostalim elementima usluge.

Operativni centar 24/7
U sklopu usluge na raspolaganju je stalno dostupan 24/7 operativni tim u okviru savremenog sigurnosnog operativnog centra (SOC)

Ekspertski tim
Pored operativnog tima, stručni tim sa višegodišnjim iskustvom iz domena sajber bezbednosti može uspešno da odgovori na sve izazove !

Bezbednost
Kako je naša osnovna delatnost informaciona bezbednost, pobrinuli smo se da vaši podaci budu bezbedni. Cela infrastruktura kao i data centar je pod našom direktnom kontrolom na teritoriji Republike Srbije.

Isporuka usluge - SLA
Precizno definisan nivo servisa (SLA), sa odgovarajućim ključnim indikatorima performansi (KPI). Kroz servisni model *garantujemo* efikasnu isporuku usluge !

Jasna komunikacija
Portal servisa i ticketing omogućavaju sledljivost međusobne komunikacije bez obzira na kanal – automatika sistema, portal, email ili usmena komunikacija. Pored dostupne tehnologije, naš tim je uvek spreman da direktno pomogne !

Smanjenje troškova
Sve gore navedene prednosti doprinose krajnjem cilju – smanjenju troškova. Bezbedniji sistem znači manje gubitaka, a uz efikasnu isporuku usluge smanjuje se potreba za ulaganjem u (skuplje) interne resurse.

Dodatne informacije o usluzi

Ukoliko želite da dobijete dodatne informacije u vezi usluge možete da nas kontaktirate putem email-a services@unicom.systems ili na telefon 011 / 735-7150. Moguće je i zakazivanje sastanka sa prodajnim timom u okviru kog možemo odgovoriti na sva vaša pitanja, ukazati na sve detalje naše usluge i demonstrirati samu uslugu kroz realne situacije.