GRUPA 1: SIEM programske komponente (softver) i edukacija

1.1. Opis

Softver mora imati funkcionalnost prikupljanja log zapisa, prikupljanja sigurnosnih podataka na druge načine, normalizacije podataka, arhiviranja svih podataka te korelacije sigurnosnih događaja. Nadalje, softver mora moći nadzirati sljedeće dijelove IT infrastrukture: poslužitelje, vatrozide (engl. *firewall*), mrežne uređaje, aplikacije i baze podataka. Softversko rješenje treba biti distribuirano, skalabilno i sastojati se od sljedećih komponenti:

1. Softverskih komponenti u obliku virtualnih poslužitelja (engl. *virtual appliance*) za realizaciju potrebnih funkcionalnosti,
2. Potrebnih plugin-a za inicijalnu instalaciju. Ako proizvođač softvera ne podržava neki od navedenih plugin-a, odabrani ponuditelj ga je dužan isporučiti tijekom provedbe ugovora kao dodatno napisanu i testiranu komponentu.

1.2. Opis arhitekture

U okviru nabave, Naručitelj nabavlja jedno SIEM softversko rješenje koje treba biti skalabilno i sastojati se od odvojenih funkcionalno specijaliziranih komponenti u obliku virtualnih poslužitelja (engl. *virtual appliance*):

- dva virtualna poslužitelja specijalizirana za prikupljanje dnevničkih zapisa (engl. *senzor, receiver*),
- jednog virtualnog poslužitelja specijaliziranog za obradu i korelaciju sigurnosnih događaja te
- jednog virtualnog poslužitelja za pohranjivanje izvornih dnevničkih zapisa.

Dodatno, Naručitelj za cjelokupno SIEM softversko rješenje nabavlja **edukaciju** za njegovo korištenje te podršku prilikom instalacije i konfiguriranja softvera.

1.3. Tehnička specifikacija SIEM programskih komponenti

SIEM sustav mora zadovoljavati sljedeće funkcionalnosti:

Naziv tražene robe		Količina	Ponuđeni proizvod *(Ispunjava ponuditelj)*	
1. SIEM programske komponente		1		
Tehnička specifikacija		**Ponuđeno (DA/NE) *(Ispunjava ponuditelj)***	**Oznaka poglavlja ponude (točke/stranice) gdje je tražena specifikacija jednoznačno vidljiva *(Ispunjava ponuditelj)***	**Bilješke/ Napomene *(Ispunjava ponuditelj)***
PRIKUPLJANJE I OBRADA LOG ZAPISA				
1.1.	Sustav se sastoji od dvije zasebne komponente, virtualnih poslužitelja, specijaliziranih za prikupljanje i obradu log zapisa			
1.2.	Sustav se sastoji od zasebne komponente, virtualnog poslužitelja, specijalizirane za trajnu pohranu izvornih log zapisa			
1.3.	Obrada log zapisa u vremenu bliskom stvarnom vremenu (engl. „near real time“) u regularnim uvjetima rada			
1.4.	Pohrana log zapisa u izvornom i nepromijenjenom obliku s kontrolom integriteta			
1.5.	Pohrana izvornih log zapisa u komprimiranom obliku			
1.6.	Agregiranje ulaznih log zapisa minimalno prema izvorišnoj i odredišnoj IP adresi te broju ponavljanja			

Tehnička specifikacija		Ponuđeno (DA/NE) *(Ispunjava ponuditelj)*	Oznaka poglavlja ponude (točke/stranice) gdje je tražena specifikacija jednoznačno vidljiva *(Ispunjava ponuditelj)*	Bilješke/ Napomene *(Ispunjava ponuditelj)*
1.7.	Mogućnost prilagodbe kriterija agregiranja			
1.8.	Mogućnost enkripcije log zapisa tijekom prijenosa s agenta na uređaju pod nadzorom			
1.9.	Prikupljanje log podataka nije ograničeno brojem uređaja s kojih se prikupljaju podaci			
1.10.	Prikupljanje log podataka putem sljedećih protokola: syslog, syslog-ng, WMI			
1.11.	Prikupljanje log zapisa brzinom od minimalno 2500 događaja u sekundi (EPS) bez ograničenja maksimalnog broja EPS-ova			
1.12.	Mogućnost proširenja sustava za prikupljanje podataka sa uređaja koji nisu podržani softverom i log datoteka koje generiraju korisničke aplikacije na način da se sa tvornički nepodržanih uređaja i korisničkih aplikacija mogu prikupljati podaci			
1.13.	Definiranje vremenskog intervala prikupljanja podataka iz datoteka na nadziranim uređajima pomoću agenata na istim uređajima			
1.14.	Odvajanje dijelova nadzirane mreže u zasebne grupe			
1.15.	Odvajanje nadziranih uređaja u zasebne grupe			
1.16.	Sustav mora biti izveden na način da vršna opterećenja neće onemogućiti naknadnu obradu dolaznih log zapisa			

Tehnička specifikacija		Ponuđeno (DA/NE) *(Ispunjava ponuditelj)*	Oznaka poglavlja ponude (točke/stranice) gdje je tražena specifikacija jednoznačno vidljiva *(Ispunjava ponuditelj)*	Bilješke/ Napomene *(Ispunjava ponuditelj)*
1.17.	Provjera maliciozne reputacije IP adresa			
1.18.	Mogućnost utvrđivanja geolokacije IP adresa			
1.19.	Agenti moraju imati mogućnost detekcije izmjena na zadanim datotekama nadziranog resursa			
NORMALIZACIJA				
1.20.	Mogućnost normalizacije standardnih log zapisa podržanih od strane sustava			
1.21.	Normalizacija podataka bez njihovog gubitka u vršnim opterećenjima sustava			
1.22.	Mogućnost prilagodbe postojećih pravila za normalizaciju			
1.23.	Mogućnost dodavanja novih pravila za normalizaciju log zapisa koji nisu podržani od strane sustava			
1.24.	Normalizirani podaci se moraju moći kategorizirati prema protokolu, IP adresi izvorišta i odredišta, nadziranom uređaju, servisu			
1.25.	Normalizirani podaci se pohranjuju u bazu podataka			
1.26.	Normalizacija log podataka nije ograničena brojem uređaja čiji podaci se normaliziraju			
KORELACIJA				

Tehnička specifikacija		Ponuđeno (DA/NE) *(Ispunjava ponuditelj)*	Oznaka poglavlja ponude (točke/stranice) gdje je tražena specifikacija jednoznačno vidljiva *(Ispunjava ponuditelj)*	Bilješke/ Napomene *(Ispunjava ponuditelj)*
1.27.	Korelacijski sustav se temelji na analizi normaliziranih podataka uz ocjenu rizičnosti pojedinih događaja			
1.28.	Sustav se sastoji od zasebne komponente, virtualnog poslužitelja, specijalizirane za obradu i korelaciju sigurnosnih događaja			
1.29.	Korelacija se provodi odmah po primitku i normalizaciji log zapisa			
1.30.	Sustav ima mogućnost detekcije napada uzastopnog pogađanja (engl. brute force) na elemente nadziranog informacijskog sustava (u daljnjem tekstu IS)			
1.31.	Sustav mora moći korelirati događaje između više uređaja u nadzoru			
1.32.	Sustav ima mogućnost detekcije uspješnog spajanja na određeni element IS-a nakon nekoliko uzastopnih neuspješnih pokušaja s iste IP adrese			
1.33.	Sustav ima mogućnost detekcije skeniranja portova (engl. port scan) (FTP/HTTP/HTTPS/SMB/ ICMP/UDP/SNMP) na jedan ili više elemenata IS-a s iste IP adrese			
1.34.	Sustav ima mogućnost detekcije uspješnog spajanja s istim korisničkim podacima iz različitih zemalja na jednu ili više komponenti IS-a			
1.35.	Sustav mora moći detektirati uspješno spajanje na određeni element IS-a iz zemalja iz kojih se ne očekuje spajanje			

Tehnička specifikacija		Ponuđeno (DA/NE) *(Ispunjava ponuditelj)*	Oznaka poglavlja ponude (točke/stranice) gdje je tražena specifikacija jednoznačno vidljiva *(Ispunjava ponuditelj)*	Bilješke/ Napomene *(Ispunjava ponuditelj)*
1.36.	Postupak korelacije ne smije biti obustavljen pri povećanom opterećenju sustava			
1.37.	Mogućnost prilagodbe postojećih korelacijskih pravila, dodavanje novih i onemogućavanje postojećih			
1.38.	Izrada i uređivanje korelacijskih pravila se obavlja korištenjem vizualnog alata			
1.39.	Korelacija ima mogućnost referenciranja na važnost pojedinog resursa informacijskog sustava			
1.40.	Korelacijski sustav sadrži skup podržanih i automatski ažuriranih korelacijskih pravila			
1.41.	Distribuirana arhitektura koja omogućava raspodjelu opterećenja na više hardverskih i/ili softverskih komponenti			
1.42.	Korelacija log podataka nije ograničena brojem uređaja čiji podaci se koreliraju			
OBAVJEŠTAVANJE I ALARMIRANJE				
1.43.	Sustav ima mogućnost obavještavanja administratora o detektiranim događajima u sustavu u skladu s definiranim pravilima			
1.44.	Sustav ima mogućnostslanja obavijesti e-mailom			
ANALIZA SIGURNOSNIH DOGAĐAJA				
1.45.	Postoji sučelje za pretraživanje pohranjenih događaja			

Tehnička specifikacija		Ponuđeno (DA/NE) *(Ispunjava ponuditelj)*	Oznaka poglavlja ponude (točke/stranice) gdje je tražena specifikacija jednoznačno vidljiva *(Ispunjava ponuditelj)*	Bilješke/ Napomene *(Ispunjava ponuditelj)*
1.46.	Sučelje posjeduje mogućnost odabira parametara za prikaz detalja događaja			
1.47.	Sučelje omogućava pristup do izvornih log zapisa koji su elementarni dijelovi pojedinog događaja			
1.48.	Sučelje omogućava pokretanje postupka stvaranja i rješavanja incidenata temeljenih na sigurnosnim događajima			
UPRAVLJANJE IZVORNIM LOG ZAPISIMA				
1.49.	Sustav posjeduje mogućnost trajne pohrane izvornih log zapisa prije postupka normalizacije			
1.50.	Izvorni log zapisi se komprimiraju prije pohrane			
1.51.	Implementirana je kontrola integriteta pohranjenih izvornih log zapisa			
1.52.	Implementirana je kontrola korisničkog pristupa pohranjenim izvornim log zapisima			
1.53.	Sustav posjeduje funkcije za pretragu i dohvat pohranjenih izvornih log zapisa u svrhu provođenja istrage ili pravnih akcija			
IZVJEŠTAVANJE (REPORTING)				
1.54.	Sustav ima mogućnost izrade izvještaja na temelju pohranjenih sigurnosnih događaja i izvornih log zapisa			
1.55.	Sustav za izradu izvještaja ima ugrađene predloške izvještaja			

Tehnička specifikacija		Ponuđeno (DA/NE) *(Ispunjava ponuditelj)*	Oznaka poglavlja ponude (točke/stranice) gdje je tražena specifikacija jednoznačno vidljiva *(Ispunjava ponuditelj)*	Bilješke/ Napomene *(Ispunjava ponuditelj)*
1.56.	Ugrađeni predlošci izvještaja sadrže predloške primjerene za izvještavanje sukladno zahtjevima norme ISO 27001 i sa standardom PCI DSS			
1.57.	Izvještaji se generiraju u formatima prikladnim za prijenos, čitanje, strojnu obradu i ispis (PDF, HTML, CSV)			
1.58.	Moguća je izrada korisnički definiranih formata izvještaja			
1.59.	Mogućnost definicije intervala u kojima sustav automatski izrađuje izvještaje			
1.60.	Sustav omogućava slanje izvještaja e-mailom			
NADZOR I UPRAVLJANJE SUSTAVOM				
1.61.	Centralno grafičko web sučelje za upravljanje svim komponentama sustava neovisno o tehnologijama s učestalim sigurnosnim problemima (Flash, Java)			
1.62.	Postoji kontrola korisničkog pristupa upravljačkom sučelju sustava			
1.63.	Postoji mogućnost definicije korisničkih grupa s odvojenim ovlastima za administraciju sustava u odnosu na grupe s ovlastima za pristup podacima i izvještajima			
1.64.	Autentikacija korisnika se obavlja putem kriptiranog komunikacijskog kanala			
1.65.	Autentikacija korisnika je moguća putem lokalnih korisničkih računa u sustavu			

Tehnička specifikacija		Ponuđeno (DA/NE) *(Ispunjava ponuditelj)*	Oznaka poglavlja ponude (točke/stranice) gdje je tražena specifikacija jednoznačno vidljiva *(Ispunjava ponuditelj)*	Bilješke/ Napomene *(Ispunjava ponuditelj)*
1.66.	Autentikacija korisnika je moguća putem vanjskog LDAP imenika			
ODRŽAVANJE SOFTVERA				
1.67.	Omogućen neograničen broj prijava softverskih pogrešaka odnosno grešaka u funkcioniranju SIEM sustava			
1.68.	Podrška za uklanjanje softverskih grešaka koje potpuno onemogućuju rad SIEM sustava, s odgovorom unutar 4 sata od prijave greške, kontinuirano do njenog otklanjanja			
1.69.	Podrška za uklanjanje softverskih grešaka koje znatno umanjuju funkcionalnosti SIEM sustava, s odgovorom unutar 8 sati od prijave greške, kontinuirano do njenog otklanjanja			
1.70.	Podrška za uklanjanje softverskih grešaka koje umanjuju deklariranu funkcionalnost SIEM sustava ali ne utječu znatno na normalno funkcioniranje, s odgovorom unutar 24 sata od prijave greške, u periodu od 8 do 20 sati radnim danima			
1.71.	Podrška za uklanjanje manjih softverskih grešaka koje ne utječu znatno na normalno funkcioniranje SIEM sustava, s odgovorom unutar 36 sati od prijave greške, u periodu od 8 do 20 sati radnim danima			
1.72.	Omogućen neograničen broj tehničkih upita			
1.73.	Odgovor na tehničke upite vezane za instalaciju, konfiguraciju i administriranje sustava unutar 6 sati od postavljanja upita			

1.74.	Osigurane redovite zakrpe i nadogradnje svih softverskih komponenti proizvođača tijekom 3 godine od isporuke			

1.4. Podrška za procesiranje dnevničkih zapisa (logova)

Isporučeno SIEM softversko rješenje treba imati podršku za procesiranje logova sa sljedećih izvora:

R.br.	Popis tipova uređaja koji moraju biti podržani SIEM sustavom	Ponuđeno (DA/NE) *(Ispunjava ponuditelj)*	Oznaka poglavlja ponude (točke/stranice) gdje je tražena specifikacija jednoznačno vidljiva	Bilješke/ napomene
	Mrežni uređaji			
1.	Cisco usmjerivači			
2.	Cisco ASR			
3.	Cisco Nexus			
4.	Cisco ASA			
5.	F5 Load balancing			
6.	Fortinet Fortigate			
	Operativni sustavi			
7.	Microsoft Windows Event Log zapisi (System, Security, Application)			
8.	Linux Syslog			
	DNS poslužitelji			
9.	ISC Bind DNS			
	Web poslužitelji			
10.	Microsoft IIS			
11.	Apache			
12.	Squid (proxy)			
	Baze podataka			
13.	Microsoft SQL server			
	E-mail poslužitelji			
14.	Microsoft Exchange			
15.	Postfix			

16.	Spamassassin			
17.	ClamAV			
	Neflow			
18.	Cisco Netflow v9			
19.	sFlow			
	Ostali servisi			
20.	OpenLDAP			
21.	Iptables			
22.	Samba			
23.	RSA			
24.	SAP			
25.	VMware ESXi			
26.	Sudo			

Ponuđeni softver u trenutku predaje ponude mora podržavati barem 80% izvora logova iz gornje tablice.

U slučaju da SIEM ne podržava određeni izvor podataka, odabrani ponuditelj će napisati i isporučiti zajedno s ostalim softverskim komponentama potrebnu podršku (plug-in).

Za izvore podataka koji se nalaze u prethodnoj tablici, a koji nisu standardno podržani SIEM sustavom, odabrani ponuditelj mora napisati i integrirati komponente prilagođene potrebama Naručitelja. SIEM sustav u trenutku isporuke treba podržavati rad sa svim navedenim izvorima podataka.

Dodatno, odabrani ponuditelj mora pružiti potrebnu **konzultantsku podršku djelatnicima Naručitelja u procesu instalacije** u ukupnom angažmanu ne većem od 10 radnih dana (čovjek dana, odnosno 8 sati). Ukoliko prilikom instalacije ili konfiguracije sustava djelatnici Naručitelja naiđu na probleme koje ne mogu riješiti ili imaju pitanja oko nastavka instalacije ili konfiguracije, odabrani ponuditelj mora pružiti podršku koja dovodi do rješavanja problema. Podrška može biti u obliku konzultacija putem telefona ili elektroničke pošte, udaljenog konfiguriranja sustava ili dolaska u prostorije Naručitelja u svrhu rada na otklanjanju problema zajedno s djelatnicima Naručitelja, ovisno o tome koji je oblik najprikladniji, a što će biti dogovoreno tijekom provedbe ugovora između Naručitelja i odabranog ponuditelja.

Odabrani ponuditelj je dužan **osigurati edukaciju za ponuđeno softversko rješenje**.

Cilj edukacije je upoznati djelatnike Naručitelja uključene u procese vezane za sigurnost servisa (sistemski i mrežni inženjeri, programeri) sa SIEM rješenjem, prikupljanjem i obradom podataka te izvještavanjem i administracijom sustava.

Edukacija se provodi na lokaciji Naručitelja u trajanju pet (5) radnih dana. Nakon edukacije polaznici trebaju biti osposobljeni za samostalno korištenje isporučenog sustava te prilagođavanje istog vlastitim potrebama. Naglasak treba biti na kreiranju parsera i korelacijskih pravila za nestandardne servise i specifične aplikacije razvijene za potrebe Naručitelja.

Osobe koje educiraju moraju imati potvrdu o znanju ponuđenog SIEM sustava, minimalno tri (3) godine iskustva u radu s dotičnim sustavom te barem jednu (1) održanu edukaciju o sustavu. Ovaj uvjet će se provjeravati tijekom provedbe ugovora na način da će prije održavanja edukacije odabrani ponuditelj dostaviti Naručitelju na potvrdu životopise osobe/-a koja/-e će držati edukaciju i koja/-e kumulativno moraju ispunjavati navedene uvjete.

Edukacija treba biti provedena po "hands-on" principu, odnosno pored prezentacijskog (teoretskog) dijela, potrebno je demonstrirati mogućnosti sustava, a polaznici trebaju isprobati na testnoj instanci koju osigurava izvođač edukacije, odnosno odabrani ponuditelj. Logistiku (učionica, računala i mrežna povezanost) za održavanje edukacije osigurava Naručitelj.

R.br.	Teme **koje je potrebno obuhvatiti** edukacijom
1.	Uvod, pregled komponenti i funkcionalnosti sustava
2.	Osnovna instalacija i konfiguracija

3.	Održavanje i nadogradnja sustava
4.	Upravljanje resursima i izvorima podataka
5.	Korelacija događaja i mrežnih aktivnosti
6.	Detekcija i obrada sigurnosnih incidenata
7.	Izvještavanje i vizualizacija
8.	Kreiranje vlastitih parsera i korelacijskih pravila
9.	Integracija s vanjskim aplikacijama

U _____, dana _____ 2016. god.	
Ime i prezime ovlaštene osobe ponuditelja:	
Vlastoručni potpis ovlaštene osobe ponuditelja i pečat:	