Consorci
Administració Oberta
de Catalunya

Plec de prescripcions tècniques.

Servei d'implantació del Centre d'Operacions de Ciberseguretat pel Consorci AOC

Generalitat
de Catalunya

Consorci de governs locals
per a la societat de la informació

Contingut

1. Objecte del contracte

1.1. Introducció

El Consorci AOC està immers en un procés de millora de les eines de ciberseguretat integrades en els seus Sistemes d'Informació que fa que hagin augmentat considerablement la quantitat de registres que han de ser revisats per detectar events significatius que hagin de ser tractats per la unitat de ciberseguretat.

Per tal de poder gestionar aquesta gran quantitat de registres, es fa necessari un sistema de recol·lecció i correlació automàtic de registres. Aquests tipus d'eines, anomenades SIEM per l'acrònim en anglès de *Security Information and Event Managemet,* centralitzen els registres de totes les eines de ciberseguretat, i extreu els events que han de ser investigats pel personal de ciberseguretat, reduint considerablement l'esforç de revisió de registres.

A més és necessari un servei de SOC, acrònim en anglès de *Security Operation Center*, per tal d'operar, mantenir i monitoritzar els events de seguretat que proporciona l'eina SIEM. Aquest servei serà un dels pilars de la Unitat de Ciberseguretat del Consorci AOC, ja que serà l'encarregat de monitorització i investigació dels events de seguretat.

La necessitat d'una eina SIEM i un servei SOC s'evidencia encara més perquè, tant el marc de seguretat de l'Esquema Nacional de Seguretat, com en el de l'Agència de Ciberseguretat de Catalunya, inclouen mesures de seguretat obligatòries per sistemes de criticitat alta, que indiquen la obligatorietat de tenir sistemes de centralització i correlació de registres.

Per aquests motius, el Consorci AOC ha decidit implantar una eina SIEM i un servei SOC dins dels seus sistemes de ciberseguretat i desplegar-la en tots els seus Sistemes d'Informació.

El SOC del Consorci AOC formarà part de la xarxa de SOCs de Catalunya liderada per l'Agència de Ciberseguretat de Catalunya.

1.2. Objecte del contracte

L'objecte del contracte és la contractació del servei per a la **Implantació del Centre d'Operacions de Ciberseguretat** (servei SOC, pel seu acrònim en anglès de Security Operation Center), suportat per les eines del CCN-CERT "MONICA NGSIEM" i "SAT-INET" en suport físic.

La integració amb sistemes del CCN-CERT, inicialment sobre sistemes virtualitzats de les eines del CCN-CERT "LUCIA" i "REYES", així com el desplegament de l'eina del CCN-CERT "microCLAUDIA" sobre equips de punt final, de manera que permeti al Consorci AOC la recol·lecció i emmagatzematge centralitzada de logs, la gestió eficaç de les alertes sobre ciberamenaces (detecció i gestió avançada d'amenaces, resposta àgil i anàlisi forense) que potencialment afectin els sistemes d' informació de l' AOC i, en particular, d' aquells que suporten

els seus serveis d' administració electrònica, amb el propòsit de donar adequada resposta amb caràcter previ a que arribin a materialitzar-se.

La integració amb sistemes de l'Agència de Ciberseguretat de Catalunya, inicialment l'exportació d'incidents de seguretat al SOC/CERT de l'Agència per integrar el SOC del Consorci AOC en la xarxa de SOCs de Catalunya.

El SOC del Consorci AOC ha d'englobar un conjunt de mesures encaminades a millorar la seguretat de la informació del Consorci AOC, permetent disposar de capacitat de detecció, anàlisi i resposta davant incidents de seguretat que puguin succeir a les xarxes i sistemes d' informació de l' AOC.

Els requisits generals d' aquest servei per a la **Implantació del Centre d' Operacions de Ciberseguretat** són:

- Desplegament d'un node de MONICA NG-SIEM format per dos servidors backend-frontend, i un emmagatzematge secundari extern.
- Provisió de les llicències lliures de cost per a AAPP MONICA NG-SIEM per a TRETZE fonts de logs i esdeveniments.
- Serveis tècnics especialitzats per a la instal·lació i configuració de TRETZE fonts de logs i esdeveniments, casos d'ús i optimització del sistema subministrat.
- Serveis de suport de fabricant en nivell 2 i en nivell 3, en modalitat 8x5, prestats per l'empresa adjudicatària del present plec, basat en els serveis especialitzats en la tecnologia instal·lada per al manteniment i assistència in-situ en cas necessari.
- Serveis de CiberSOC o Advanced SOC en modalitat 24x7 per a la gestió d'incidents i ciberamenaces des d'un Centre Expert Certificat.
- Formació a l'equip tècnic d' AOC sobre les eines de treball.
- Desplegament d' una sonda del Sistema d' Alerta Primerenca SAT iNet del CCN-CERT en format físic.
- Integració sobre entorn virtualitzat d'AOC, de les eines "LUCIA" i cloud "REYES".
- Instal·lació de l'eina "microCLAUDIA" sobre 100 equips de punt final.
- Instal·lació d'una solució de remediació automatitzada en punt final, contra atacs de ransomware, que realitzi contenció i remediació de l'equip de punt final, sense realització de back-up.
- El SOC/CERT de l'Agència de Ciberseguretat de Catalunya haurà de tenir visibilitat de l'activitat gestionada per el SOC del Consorci AOC, els atacs rebuts i el grau d'exposició a l'amenaça que permeti a l'Agència monitoritzar l'estat de l'AOC respecte a les amenaces, atacs i incidents.

2. Abast de desplegament i operació

Són objecte d'aquest contracte els treballs necessaris per a instal·lació i parametrització de l'eina MONICA NG-SIEM, així com l'administració i operació posterior de la infraestructura instal·lada. El personal de l' equip tècnic d' AOC tindrà accés igualment a l' operació de la plataforma.

L' explotació haurà de permetre mantenir un equilibri entre la detecció d' alertes de seguretat i l' esforç precís per solucionar-les i documentar-les. La Unitat de Ciberseguretat del Consorci AOC haurà de tenir accés en temps real directament sobre els quadres de comandament de la plataforma SIEM per realitzar consultes dinàmiques per tècniques de drill-down sobre l' estat de la seguretat de la seva plataforma. L' accés pel Consorci AOC haurà de ser en nadiu sobre la plataforma SIEM, i no s' admetran solucions de façana interposada contra la plataforma SIEM desplegada, ni consultes a través que utilitzin un API de la plataforma SIEM.

En general, haurà de ser possible:

- Recollir, analitzar i presentar informació de dispositius de xarxa i de seguretat.
- Facilitats d'identificació d'accessos (logs)
- Detecció de vulnerabilitats i comprovació de compliment de polítiques de seguretat.
- Capacitat d' incloure informació de NDR i EDR.
- Possibilitat d'inclusió del context de l'activitat de la xarxa, el context dels usuaris/actius, registres d'aplicacions i reducció d'incidents en alertes reals.
- Traçabilitat d' informació de la infraestructura objecte de l' abast.
- Detecció, anàlisi, gestió i contenció/remediació d'incidents de seguretat.
- Reenviament d' incidents cap a l' Agència de Ciberseguretat de Catalunya, incloent-hi les oportunes llicències. El format dels incidents s'haurà d'adaptar per a que pugui ser consumit per CiberSOC de l'Agència.

També haurà de ser possible configurar diferents panells d' informació, casos d' ús personalitzats i models d' informes en formats explotables externament.

Addicionalment, els licitadors hauran de contemplar en la seva proposta de serveis:

- Desplegament d' un node de SAT-INET en format físic.
- Integració sobre entorn virtualitzat d'AOC, de les eines "LUCIA" i cloud "REYES"
- Instal·lació de l'eina "microCLAUDIA" sobre 100 equips de punt final.
- Instal·lació d'una solució de protecció addicional en punt final, contra atacs de ransomware, que no precisi de còpies de seguretat per a la recuperació de l'equip, sobre 100 equips de punt final i 80 servidors, tots dos amb tecnologia Windows.

En el cicle de vida de la prestació dels serveis contractats es distingiran tres fases:

- Fase 1: Instal·lació, parametrització i formació de l'eina MONICA NG-SIEM.

- Fase 2: Prestació dels serveis avançats en modalitat 24x7 de Gestió d' Incidents de Seguretat sobre l' eina MONICA NG-SIEM.
- Fase 3: Serveis de suport en modalitat 8x5 de MONICA NG-SIEM.

2.1. Entorn existent i requisits d' integració

En l'actualitat, el Consorci AOC presta els seus serveis d'IT des de cinc nodes[1] geogràficament disjunts. Es requereix que la solució proposada ingesti logs des dels sistemes cedents en cada node, sobre un col·lector de logs desplegat.

El col·lector de logs haurà de desplegar-se sobre maquinari físic dedicat per a AOC ("bare-metal") que suportarà el servei que es requereix per al contracte. Serà responsabilitat de l'adjudicatària del seu manteniment, suport i deguda resposta durant la vida del contracte, sense que aquest maquinari resulti de titularitat de l'AOC.

Es pretén que l'equip del CiberSOC de l'adjudicatària abordi investigacions completes sobre esdeveniments potencialment perillosos, per la qual cosa la solució proposada haurà d'escalar logs a nivell de registre fins al CiberSOC de l'adjudicatària, no admetent-se solucions que només escalin esdeveniments en temps real des dels col·lectors fins al CiberSOC de l'adjudicatària.

L'empresa adjudicatària aportarà el maquinari necessari per a la prestació del servei. Les característiques mínimes que haurà de complir el maquinari per al node MONICA NG-SIEM sobre els quals prestar els seus serveis seran:

Per al col·lector:

- Esdeveniments per segon: capaç de resoldre pics de 36.000 EPS.
- Ingestió de logs: 115 GB/dia.
- Capacitat de procés: 48 cors a 2.4MHz
- Memòria: 512 GB
- Emmagatzematge local:
    - RAID1: 2TB
    - RAID5: 16TB
    - Latència rotacional de lectura: millor o igual a 5 mil·lisegons.
    - Latència rotacional d' escriptura: millor o igual a 3 mil·lisegons.
    - Mida de blocs per a lectura/escriptura: 8.192 KB.
- Connectivitat:
    - 2x 10GE
    - 1x 1GE

Retenció de dades:

- En emmagatzematge a part per a un mínim de 12 mesos.
    - Capacitat igual o superior a 24TB.
    - Connectivitat:

[1] Els licitadors poden demanar aquesta informació sota acord de confidencialitat, conforme al procediment previst en aquest expedient.

1. 2x 10GE
2. 1x 1GE

Es requereix la integració de les següents eines del CCN:

- LUCIA - bidireccional.
- REIS 4.0.
- microCLAUDIA (per a un mínim de 100 equips de punt final)
- SAT-INET.

Les característiques mínimes per al desplegament de la sonda SAT-INET són:

- Capacitat de procés: 16 cors.
- Memòria: 16 GB
- Memòria: 16 GB
- Emmagatzematge local:
  - RAID1: 2x 146GB
- Connectivitat:
  - 2x 1GE
- Compatible amb CentOS 7.3.

S'aprofitaran els enllaços existents d'AOC, per establir la comunicació entre els col·lectors i entre els nodes; així mateix, l'AOC posarà a disposició de l'adjudicatària, un enllaç de comunicacions entre el col·lector i el CiberSOC de l'adjudicatària.

Durant tot el temps d'execució del contracte, el maquinari aportat per l'adjudicatari haurà tenir la suficient capacitat computacional i de retenció d'informació per donar compliments al present plec.

2.2. Fase 1: Instal·lació, parametrització i formació de l'eina MONICA NGSIEM

En tractar-se d'una eina integrada i compacta, els requisits a aportar per part del Consorci AOC per a la instal·lació en aquesta fase inicial d'implantació seran:

- Es provisionarà espai per a l' allotjament de dos nodes de MONICA NG-SIEM en els emplaçaments físics dels centres de dades que utilitza AOC, així com per al node físic de la sonda SAT-INET. Igualment, es provisionarà espai virtual per a l'allotjament de les eines "LUCIA" i "REYES"
- Connexió VPN des dels dos nodes de MONICA NG-SIEM al centre d'operacions.
- Full Excel de requisits per a la Integració de les fonts de Logs a monitoritzar.
- Procediment operatiu de gestió d' incidents d' AOC.
- El termini per aportar aquests requisits per part d' AOC serà inferior a deu dies laborables.

En aquesta fase del servei s' emmarquen les següents activitats per part de l' adjudicatari, llevat dels casos en què expressament s' indiqui que seran realitzades per AOC:

- Disseny de l'arquitectura de l'eina MONICA NG-SIEM a instal·lar definitivament, incloent requisits maquinari en base a logs monitoritzats.
- Definició dels requeriments tècnics sobre els quals s'instal·larà les eines MONICA NG-SIEM, SAT-INET, LUCIA, REYES, microCLAUDIA, així com la solució de protecció addicional contra ransomware.
- Preparació, documentació i desplegament dels nodes MONICA NG-SIEM i SAT-INET en format físic dins d' un centre de dades que utilitza AOC.
- Desplegament de les eines MONICA NG-SIEM, SAT-INET, LUCIA, REYES, microCLAUDIA, així com la solució de protecció addicional contra ransomware.
- Integració de les fonts acordades en l' arrencada del projecte en l' eina MONICA NG-SIEM i que tindran un abast de TRETZE fonts[2] de log diferents.
- Definició del quadre de comandaments de les fonts d' informació integrades.
- Aplicació d'intel·ligència mitjançant casos d'ús, personalització i desenvolupament de nous casos d'ús.
- En finalitzar la fase d'instal·lació i implantació, s'haurà de proporcionar al personal de l'equip tècnic d'AOC, accés a la consola de gestió de l'eina MONICA NG-SIEM amb rol d'operació i la formació necessària sobre les eines de treball.

2.2.1 Reenviament d' incidents cap a l' Agència de Ciberseguretat de Catalunya

L'Agència de Ciberseguretat de Catalunya haurà d'estar informada en temps real dels incidents de seguretat que afectin al Consorci AOC. Amb aquests objectiu, l'eina MONICA NG-SIEM haurà de publicar els incidents per a que el SIEM de l'Agència de Ciberseguretat recol·lecti aquesta informació.

2.2.2 Documentació a lliurar en aquesta fase

La documentació lliurada per l' adjudicatari i validada pel Consorci AOC servirà com a punt de partida per a la fase d' instal·lació i haurà d' incloure:

- Pla detallat de posada en marxa i configuració, incloent estimació de temps per a cadascuna de les tasques. Procés d'instal·lació, que inclogui tots els elements que són necessaris per disposar de l'equipament i les eines totalment operatives.
- Identificació de parts involucrades en el desplegament i dependències entre elles: necessitats d' infraestructura maquinari, connectivitat de xarxa, adreçament IP necessari.
- Pla de configuració del sistema.
- Proposta d' integració amb sistemes externs.
- Proposta de polítiques generals de configuració.

[2] Los licitadores pueden solicitar esta información bajo acuerdo de confidencialidad, conforme al procedimiento previsto en este expediente.

- Proposta de definició d' alertes i incidents.
- Arquitectura del sistema desplegat. Diagrames físics i lògics.

2.3. Fase 2: Prestació dels serveis avançats en modalitat 24x7 de Gestió d' Incidents de Seguretat sobre l' eina MONICA NG-SIEM.

Aquest servei vindrà suportat pel personal adscrit al CiberSOC de l' adjudicatari. Els serveis de gestió de la seguretat desenvolupat pel CiberSOC inclouran les funcions següents:

- Servei de detecció i resposta (Nivell 1 d'operació) en modalitat 24x7:
    - Monitoratge d' esdeveniments de seguretat mitjançant la plataforma MONICA NG-SIEM.
    - Correlació i anàlisi d' esdeveniments.
    - Operació i notificació d' alertes.
    - Coordinació de respostes a incidents.
- Gestió d' esdeveniments i incidents de seguretat:

Resposta davant incidents, englobant la notificació dels incidents detectats, conforme als procediments establerts, així com la gestió del cicle complet dels mateixos, coordinant, de forma alineada i sota la supervisió de l'equip tècnic del Consorci AOC, les actuacions necessàries sobre els sistemes/xarxes entre els grups que els administren.

A la vegada, el Consorci AOC es coordinarà amb l'Agència de Ciberseguretat de Catalunya per alinear l'estratègia de detecció, protecció, prevenció i resposta davant amenaces que el SOC/CERT de l'Agència defineixi.

Així, entre d'altres el SOC/CERT de l'Agència:

- Proposarà regles de correlació per detectar les principals amenaces de l'AOC.
- Proposarà polítiques de seguretat a desplegar.
- Proposarà contramesures a desplegar a les eines de detecció/protecció de l'AOC sobre amenaces actives.
- Proporcionarà informació d'intel·ligència operativa.
- Proposarà estratègies de resposta davant incidents.

Per aquests motius, el SOC del Consorci AOC es coordinarà operativament amb el SOC/CERT de l'Agència amb un seguiment periòdic.

2.3.1 Documentació a lliurar en aquesta fase

La documentació lliurada per l' adjudicatari i validada per AOC haurà d' incloure:

- Protocols d' actuació davant d' alertes de seguretat: Del funcionament habitual del sistema de gestió centralitzada de la seguretat s' extrauran informacions conseqüència del monitoratge i de la correlació d' esdeveniments. Prenent com a base el procediment operatiu de gestió d'incidents d'AOC i la guia del CCN "CCN-STIC 817. Gestió de ciberincidents" es definirà una classificació de severitats per a

les alertes de seguretat, així com els protocols d'actuació associats per a cadascuna d'elles.

- Informe d'incident: En cas de que es produeixi un incident de seguretat, l'adjudicatari es compromet a lliurar un informe on inclogui la descripció de l'incident, afectació (objecte o servei afectat, temps total, temps d'inici i fi d'incidència), antecedents, causa arrel de l'incident, solució i accions realitzades. El temps màxim per lliurar l'informe està fixat en el punt 4.1Temps d'atenció a incidents.

Quan es detectin esdeveniments que puguin resultar un incident de seguretat, l'adjudicatari haurà d'haver iniciat el tractament dels esdeveniments amb els següents temps màxims:

1 hora per incidents greus.

24 hores per incidents lleus.

L' adjudicatari es compromet ha complir aquests terminis en un 90% del casos.

Entrega d' informes d'incidents

- Informe mensual d' incidents: L' adjudicatari lliurarà informes incloent el resum mensual d' incidents.

2.4. Fase 3: Suport i Manteniment eina MONICA NG-SIEM 8x5

El servei de suport i manteniment de l' eina MONICA NG-SIEM inclourà:

- Actualitzacions de la seva instal·lació.
- Administració i operació de la configuració de la plataforma MONICA NG-SIEM
- Recepció d' incidències 8x5.
- Manteniment de les fonts d'informació i implantació de noves fonts en cas de ser necessari.

La implantació de l'eina MONICA NG-SIEM (FASE 1) i la posada en marxa del servei de gestió d'amenaces de seguretat (FASE 2), englobant els aspectes inicials de reconeixement o posada en context de les persones que l'integren amb l'entorn tecnològic i organitzatiu del Consorci AOC, i la formalització del procés de gestió d'incidents de seguretat, tindran començament com a màxim en cinc (5) dies després de la formalització del contracte, amb una reunió de llançament del servei, i tindrà una durada màxima de quatre (4) setmanes des de l'esmentada formalització del contracte.

3. Formació

L'adjudicatari haurà d'incloure en la seva proposta una sessió de capacitació d'almenys cinc (5) hores. La formació ha d' incloure:

- Arquitectura del sistema desplegat. Funcionalitats dels seus components.
- Administració bàsica de la plataforma.
- Administració i gestió de casos d' ús.
- Administració i gestió de recol·lecció de dades.
- Gestió d' alerta primerenca.

El nombre d' assistents a aquestes sessions serà com a mínim de 5 persones. S' expedirà certificat d' assistència al curs als assistents. Les sessions de capacitació seran realitzades a les instal·lacions d'AOC.

Aquesta formació es prestarà a la finalització de la fase d'instal·lació, com a finalització d'aquesta etapa, abans de començar la fase de Gestió d'Incidents de Seguretat, llevat de modificacions aprovades juntament amb el responsable d'AOC.

4. Acords de nivell de servei

L'adjudicatari s'haurà de comprometre a respectar els SLAs pactats amb el Consorci AOC. Durant el temps del contracte es podran ajustar els SLA o definir nous SLA sempre i quan les dues parts estiguin d'acord.

No obstant, com a mínim hi hauran els següents SLAs inicials:

4.1. Temps d'atenció a incidents.

Quan es detectin esdeveniments que puguin resultar un incident de seguretat, l'adjudicatari haurà d'haver iniciat el tractament dels esdeveniments amb els següents temps màxims:

- 1 hora per incidents greus.
- 24 hores per incidents lleus.

L' adjudicatari es compromet ha complir aquests terminis en un 90% del casos.

4.2. Entrega d' informes d'incidents.

Quan es produeixi un incident que afecti als sistemes d'informació monitoritzats per l'adjudicatari, aquest haurà de fer un informe tal i com es detalla en la descripció del servei. El temps màxim d'entrega de l'informe serà:

- 48 hores per incidents greus.
- 10 dies per incidents lleus.

L’ adjudicatari es compromet ha complir aquests terminis en un 90% del casos.

5. Devolució del servei

En el cas de finalització de la relació contractual entre el Consorci AOC i l’adjudicatària, abans del desmantellament de la solució, l’adjudicatària haurà de donar suport per a la exportació i/o migració de la informació històrica propietat del Consorci AOC.

Tota la informació històrica del Consorci AOC haurà de ser eliminada de manera que sigui irrecuperable.

El Consorci AOC es compromet a donar facilitats a l’adjudicatària per a la retirada i entrega del seu maquinari a la empresa adjudicatària.

6. Requisits exigibles.

- La empresa adjudicatària haurà de ser una empresa certificada pel CCN-Cert en la gestió d’events de seguretat amb l’eina MONICA NGSIEM.
- La empresa adjudicatària haurà d’estar adherida a la Xarxa Nacional de Centres d’Operacions de Ciberseguretat (RNS) en nivell Gold.
- La empresa adjudicatària un certificat de conformitat de l’Esquema Nacional de Seguridad de nivell ALT en l’àmbit dels seus processos interns.

Barcelona,

Ivan Caballero
Responsable de Sistemes de Seguretat