



ATL

Ens d'Abastament
d'Aigua Ter-Llobregat

1.13 MONITORITZACIÓ

10.10.2024

1.13 Monitorització

Índex de continguts

1.	Introducció	4
1.1.	Requisits de projecte	4
1.1.1.	Situació actual	4
1.1.2.	Punts de millora	5
2.	Estudi de mercat	6
2.1.	Anàlisis d'eines de monitorització	6
2.2.	Detalls de les solucions d'eines monitorització	7
2.2.1.	Solució Nagios XI	8
2.2.2.	Solució PRTG Network Monitor	8
2.2.3.	Solució SolarWinds	8
2.2.4.	Solució ManageEngine OpManager	8
2.2.5.	Solució Zabbix	8
2.2.6.	Solució Centreon	8
2.3.	Anàlisis d'eines de SIEM	9
2.4.	Detall de les solucions d'eines SIEM	10
2.4.1.	Solució Splunk	10
2.4.2.	Solució IBM QRadar	10
2.4.3.	Solució ArcSight	10
2.4.4.	Solució Securonix	10
2.4.5.	Solució LogRhythm	11
2.4.6.	Solució McAfee Enterprise Scurity Manager	11
2.5.	Conclusions de l'estudi de mercat	11
2.5.1.	Elecció de la solució monitorització IT	12
2.5.2.	Elecció de la solució de monitorització Telecontrols	12
2.5.3.	Elecció de la solució SIEM	13
3.	Punts de control	15
3.1.	Relació de variables monitorització amb PLC	18
3.1.1.	Configuració de l'estat de l'estació PLC	19

1.13 Monitorització

4.	Passarel·la d'intercanvi d'informació.....	20
4.1.	Procés d'importació de dades Scada.....	20
4.1.1.	Flux general	21
4.1.2.	Eines utilitzades	21
4.2.	Procés d'importació de dades SIEM	22
5.	Requisits maquinari	23
6.	Programa de tasques	24

Llista de taules

Taula 2-1: Llista de programari	7
Taula 2-2: Anàlisi de les eines SIEM	9
Taula 3-1: Punts de Control	18
Taula 3-2: Variables monitoritzades del PLC	19
Taula 3-3: Configuració de l'estat de l'estació PLC.....	20

Llista de figures

Figura 4-1: Flux d'informació del procés.....	21
---	----

1.13 Monitorització

1. INTRODUCCIÓ

En el present document s'analitzen les millors pràctiques, normatives i tecnologies per garantir un entorn de treball segur i eficient en els centres d'ATL, amb l'objectiu de protegir els treballadors, els béns i la continuïtat operativa.

1.1. Requisits de projecte

L'aplicació de les directrius de seguretat al projecte "Pilot pel disseny i renovació del sistema d'automatització i telecomandament de l'Ens d'abastament d'ATL" es durà a terme tenint en compte una sèrie de requeriments essencials.

En primer lloc, es garantirà l'aplicació dels requeriments descrits al plec i a l'oferta tècnica, assegurant que es compleixen totes les especificacions prèviament acordades. També es vetllarà pel compliment de la normativa interna d'ATL en matèria de seguretat, assegurant que els procediments propis de l'organització es respecten en totes les fases del projecte.

A més, es compliran les exigències de la normativa de l'Esquema Nacional de Seguretat (ENS) en el seu nivell alt, una regulació fonamental per garantir la protecció de la informació i la infraestructura crítica. Així mateix, s'assegurarà l'aplicació dels estàndards internacionals de gestió de la seguretat de la informació, seguint la normativa ISO27001, reconeguda mundialment com a referent en aquest àmbit.

Finalment, s'aplicaran les bones pràctiques indicades pels fabricants dels diferents components utilitzats al projecte, assegurant que les tecnologies desplegades funcionin d'acord amb les seves especificacions tècniques i maximitzant la seva seguretat i eficiència. D'aquesta manera, es garantirà un alt nivell de protecció i compliment normatiu durant tot el desenvolupament del projecte.

1.1.1. Situació actual

ATL disposa d'una plataforma de monitorització per tota la seva infraestructura IT, incloent serveis, sistemes operatius, protocols de xarxa, mètriques de sistemes i elements de la infraestructura de xarxa. Aquesta plataforma utilitza la solució tecnologia Nagios XI, una eina àmpliament utilitzada en el món de les tecnologies de la informació.

Aquesta eina es focalitza principalment en l'estat de CPU, memòria, serveis de SO i altres paràmetres dels servidors SCADA i bases de dades, oferint una visibilitat limitada pel que fa als altres components crítics del sistema d'automatització i telecontrol. Actualment, no es disposa d'una solució que cobreixi aspectes com la redundància del sistema SCADA, la recuperació de dades en cas de fallada de les comunicacions, o la connexió entre l'SCADA i l'eina de monitorització.

A més, es fa evident la necessitat de disposar d'un sistema de monitorització propi per als centres de control de les plantes de tractament d'aigües (PTT), plantes de tractament del Llobregat (PTLL), estacions remotes i

1.13 Monitorització

centres de contingència. Aquest sistema ha de permetre incorporar, modificar i eliminar nous punts de control de manera àgil i sense dependències externes. Aquesta flexibilitat és essencial per assegurar que qualsevol canvi en la infraestructura o en els processos de monitorització pugui ser gestionat internament, garantint així una resposta ràpida i efectiva davant qualsevol necessitat operativa.

Per altra banda, és imprescindible la incorporació d'un sistema de monitorització tipus SIEM (Security Information and Event Management) amb l'objectiu de complir amb els requisits de seguretat del ENS en el nivell alt. Aquest sistema permetria una auditoria contínua de la seguretat, així com la generació d'alertes de ciberseguretat, garantint una protecció més robusta de les comunicacions i dades dels sistemes SCADA i OT. D'aquesta manera, es milloraria la capacitat de resposta davant qualsevol incident de ciberseguretat, assegurant el compliment de la normativa vigent i mantenint la integritat del sistema.

Aquesta situació deixa evidents mancances en la monitorització proactiva de les comunicacions OT, així com en la capacitat de detectar i reaccionar a anomalies que podrien afectar el bon funcionament dels sistemes de control, amb possibles repercussions en la continuïtat del servei. Per aquest motiu aquest proveïdor presentarà una proposta de millora en el present document.

1.1.2. Punts de millora

S'han identificat diversos aspectes de millora rellevants per a l'eficàcia i la seguretat del sistema de monitorització d'ATL. Un dels principals punts és la limitació de la plataforma actual (Nagios XI), que només cobreix aspectes bàsics com l'estat de CPU, memòria i serveis de sistema operatiu dels servidors SCADA i bases de dades.

A més, la manca de punts de control per la solució que proporcioni redundància al sistema SCADA o la capacitat de recuperar dades en cas de fallada de comunicacions és un altre punt que s'ha de millorar. Aquestes mancances limiten la capacitat de monitorització proactiva, deixant buits en la detecció d'anomalies i afectant la continuïtat del servei.

Finalment, s'ha identificat la necessitat de disposar d'un sistema de monitorització propi i flexible per als centres de control, així com la incorporació d'un sistema SIEM per complir amb el nivell alt de l'ENS. Aquestes millores permetrien gestionar nous punts de control de manera àgil i incrementar la seguretat amb alertes de ciberseguretat i auditories contínues.

Així, els principals aspectes de millora són l'ampliació de la cobertura de monitorització incorporant nous punts de control, la implementació d'un sistema de monitorització propi dels Telecontrols i la integració d'un sistema SIEM.

1.13 Monitorització

2. ESTUDI DE MERCAT

A continuació, es plantegen els requisits clau que serviran com a base per a la selecció d'una nova eina de monitorització. En primer lloc, és essencial que la solució compleixi amb les especificacions tècniques detallades en el plec, assegurant l'adequada monitorització de les infraestructures IT i OT, així com la seva adaptació a les normatives de seguretat, com l'Esquema Nacional de Seguretat (ENS) en el seu nivell alt, i l'ISO 27001. Es requereix que la solució seleccionada sigui on-premise, garantint el control complet sobre la infraestructura i el seu desplegament dins del centre de dades corporatiu, la qual cosa assegura una major privacitat i seguretat en la gestió de dades crítiques.

A més, es busca que l'eina estigui actualitzada en els darrers anys, per assegurar la seva compatibilitat amb les tecnologies modernes i la seva resiliència davant noves amenaces. També és important que la solució tingui un ús extensiu tant a la comunitat europea com mundial, el que oferirà garantia de suport, escalabilitat i una àmplia experiència d'ús. En aquest sentit, s'ha de centrar la selecció en les solucions de monitorització líders a nivell mundial, totes elles amb una gran comunitat d'usuaris i amb una adopció significativa en entorns industrials i corporatius. Això assegurarà la capacitat de gestionar de manera eficaç els nous reptes de monitorització i ciberseguretat que les infraestructures actuals requereixen.

2.1. Anàlisis d'eines de monitorització

Per tal de millorar la gestió de la infraestructura crítica, s'ha proposat l'adopció d'una eina especialitzada en la monitorització dels components del centre de control, SCADA, frontals de comunicació i PLCs. Aquesta eina haurà de ser capaç de proporcionar una visibilitat més profunda i específica per a la xarxa OT, integrant-se amb els sistemes existents i oferint capacitats de monitorització avançada.

Després de consultar diferents consultores IT i amb la nostra experiència en projectes similars, s'ha identificat la següent llista de programari que compleix els requeriments de monitorització de la infraestructura d'ALT.

1.13 Monitorització

Característiques	Nagios XI	PRTG Network Monitor	Solar Winds	Manage Engine Op Manager	Zabbix	Centreon
Tipus de Llicència	Comercial	Comercial	Comercial	Comercial	Open Source	Open Source
Monitoratge	Xarxes, aplicacions, serveis, sistemes operatius	IT/OT	IT/OT	IT/OT	IT/OT	IT/OT
Interfície d'Usuari	Web amb personalització	Alta	Moderada	Alta	Alta	Alta
Notificacions	Correu electrònic, SMS, trucades	Sí	Sí	Sí	Sí	Sí
Escalabilitat	Moderada	Alta	Alta	Alta	Alta	Alta
Suport de Comunitat	Activa	Moderada	Moderada	Moderada	Alta	Alta
Data de Creació	1999	1997	1999	2003	2001	2005
Cota de Mercat	Mitjana	Mitjana	Alta	Mitjana	Alta	Alta
Facilitat d'Instal·lació i Desplegament	Fàcil amb guia pas a pas	Moderada	Alta	Moderada	Moderada	Moderada
Col·lecció de Mètriques	Completa però requereix configuració	Alta	Alta	Alta	Avançada	Alta
Arquitectura	Modular amb plugins	Distribuïda	Centralitzada	Modular	Distribuïda	Distribuïda
Disseny UI & UX	Personalitzable	Avançada	Avançada	Senzilla	Intuitiva	Avançada
Documentació i Suport	Completa i comunitat activa	Bona	Bona	Bona	Excel·lent	Excel·lent
Cota de Mercat	Mitjana	Mitjana	Alta	Mitjana	Alta	Alta

Taula 2-1: Llista de programari

2.2. Detalls de les solucions d'eines monitorització

Totes les solucions identificades en l'apartat anterior, com Nagios XI, Zabbix, SolarWinds, PikaAlert, entre d'altres, compleixen amb les especificacions tècniques indicades en el plec de condicions. Així mateix, aquestes eines s'ajusten a les normatives aplicables, incloent l'Esquema Nacional de Seguretat (ENS) en el seu nivell alt, així com a les bones pràctiques de seguretat de la informació segons la normativa ISO 27001. Aquestes solucions ofereixen la flexibilitat i escalabilitat necessàries per garantir una monitorització eficient i segura en entorns IT i OT.

1.13 Monitorització

2.2.1. Solució Nagios XI

Nagios XI és una eina de monitorització creada l'any 2009, amb la seva última actualització el 2023. Es tracta d'una solució de codi obert (Open Source) molt popular per a la monitorització bàsica d'infraestructures IT, incloent servidors, xarxes i aplicacions. Nagios XI ofereix una interfície modular i ampliable a través de complements, la qual cosa la fa flexible per a petites i grans infraestructures. Tot i això, la seva interfície d'usuari és més limitada comparada amb altres solucions més modernes.

2.2.2. Solució PRTG Network Monitor

PRTG Network Monitor és una eina comercial de monitorització fundada el 1997, amb la seva última actualització el 2023. Està dissenyada per monitoritzar xarxes IT i OT amb una interfície fàcil d'utilitzar i desplegament ràpid. És ideal per a empreses de mida mitjana i gran que busquen una solució ràpida d'instal·lar i configurar, oferint una àmplia cobertura de monitorització.

2.2.3. Solució SolarWinds

SolarWinds és una altra solució comercial, creada el 1999 i actualitzada el 2023. Ofereix una àmplia gamma de funcionalitats per a la monitorització d'infraestructures IT i OT, amb una interfície d'usuari intuïtiva i capacitats avançades per a empreses grans. És molt coneguda i utilitzada en entorns corporatius per la seva eficiència en el monitoratge d'infraestructures complexes.

2.2.4. Solució ManageEngine OpManager

ManageEngine OpManager és una eina comercial fundada l'any 2003, amb l'última actualització el 2023. Està enfocada a la monitorització d'infraestructures IT i OT, amb una interfície d'usuari senzilla però efectiva. És coneguda per la seva bona integració amb altres eines de gestió de TI, com ara la gestió d'actius i servidors, la qual cosa la fa popular en empreses que requereixen eines de gestió unificades.

2.2.5. Solució Zabbix

Zabbix és una solució de codi obert (Open Source) que va veure la llum l'any 2001 i es va actualitzar l'any 2023. Ofereix una arquitectura distribuïda que permet la monitorització tant de sistemes IT com OT, fent-la ideal per a infraestructures grans i complexes. Zabbix és altament escalable i molt valorada per la seva capacitat d'integració amb altres entorns i sistemes, sent una eina popular en entorns industrials i empresarials.

2.2.6. Solució Centreon

Centreon és una solució de codi obert (Open Source) molt utilitzada a Europa, especialment per a la monitorització d'infraestructures IT i OT. Creada l'any 2005, i amb la seva última actualització el 2023, Centreon destaca per la seva interfície moderna i intuïtiva, així com per la seva capacitat de gestionar grans volums de dades, sent molt popular en entorns empresarials.

1.13 Monitorització

2.3. Anàlisi d'eines de SIEM

A continuació, es presenta l'anàlisi de les principals eines SIEM (Security Information and Event Management) disponibles al mercat. Aquestes solucions són fonamentals per a la monitorització, detecció i resposta davant d'incidents de seguretat en temps real, oferint una visibilitat completa sobre les infraestructures IT i OT. L'anàlisi se centra en les eines més utilitzades a nivell mundial i amb una forta presència a Europa, avaluant aspectes com l'escalabilitat, la capacitat de correlació d'esdeveniments, la facilitat de desplegament i el suport comunitari. A més, es posa especial atenció en solucions actualitzades recentment, assegurant que compleixen amb les necessitats de seguretat actuals i les normatives vigents.

Característica	Splunk	IBM QRadar	ArcSight	Securonix	Log Rhythm	McAfee Enterprise Security Manager
Tipus de llicència	Comercial	Comercial	Comercial	Comercial	Comercial	Comercial
Tipus de monitorització	IT/Seguretat	IT/Seguretat	IT/Seguretat	IT/Seguretat	IT/Seguretat	IT/Seguretat
Interfície d'usuari	Alta	Alta	Moderada	Alta	Alta	Moderada
Notificació	Sí	Sí	Sí	Sí	Sí	Sí
Escalabilitat	Alta	Alta	Alta	Alta	Alta	Alta
Suport comunitat	Alta	Alta	Moderada	Moderada	Moderada	Moderada
Data de creació	2003	2005	2000	2008	2003	2010
Cota de mercat	Ampli	Ampli	Ampli	Mitjana	Mitjana	Mitjana
Facilitat d'instal·lació i desplegament	Alta	Moderada	Moderada	Moderada	Alta	Moderada
Col·lecció de mètriques	Alta	Alta	Alta	Alta	Alta	Alta
Arquitectura	Centralitzada	Centralitzada	Modular	Distribuïda	Modular	Modular
Disseny UI/UX	Avançada	Avançada	Moderada	Avançada	Avançada	Moderada
Documentació i suport	Excel·lent	Excel·lent	Bona	Bona	Bona	Bona
Puntuació Gartner	Molt alta	Molt alta	Alta	Alta	Alta	Alta

Taula 2-2: Anàlisi de les eines SIEM

1.13 Monitorització

2.4. Detall de les solucions d'eines SIEM

Aquestes son les solucions SIEM més destacades a nivell mundial, seguidament realitzarem una breu descripció de les principals característiques, implantació, darrera actualització entre altra informació.

2.4.1. Solució Splunk

Splunk es va presentar per primera vegada l'any 2003 com una solució comercial destinada a la gestió i monitorització de grans volums de dades, especialment en l'àmbit de la seguretat IT i l'anàlisi de registres. Splunk destaca per la seva escalabilitat i la seva capacitat d'integrar-se amb una àmplia gamma de sistemes, proporcionant una visibilitat en temps real i una resposta ràpida davant incidents de ciberseguretat. Amb una implantació global, Splunk té una forta presència tant a Europa com a nivell mundial, sent una de les solucions més utilitzades en grans corporacions. La seva última actualització va ser el 2023, mantenint-se al dia amb les necessitats emergents en ciberseguretat.

2.4.2. Solució IBM QRadar

IBM QRadar, llançat l'any 2005, és una solució comercial desenvolupada per IBM que destaca per la seva capacitat d'anàlisi i correlació d'esdeveniments de seguretat en temps real. QRadar és àmpliament utilitzat per empreses que necessiten monitoritzar grans infraestructures i detectar amenaces de manera eficient. És una de les eines preferides a Europa i a nivell mundial per la seva integració amb altres eines de seguretat i pel suport que ofereix IBM. L'última actualització d'IBM QRadar va ser el 2023, oferint noves funcionalitats per millorar la seguretat en entorns complexos.

2.4.3. Solució ArcSight

ArcSight, presentat l'any 2000, és una solució comercial coneguda per la seva capacitat modular i per ser una eina robusta en la correlació d'esdeveniments de seguretat. Desenvolupat per Micro Focus, ArcSight té una forta implantació a nivell mundial, incloent Europa, on és utilitzat en sectors governamentals i grans corporacions. Tot i que és una eina més antiga, es manté rellevant gràcies a les contínues actualitzacions. La seva última actualització va ser el 2023, millorant les capacitats d'anàlisi d'amenaces en entorns IT i OT.

2.4.4. Solució Securonix

Securonix és una solució comercial que es va llançar l'any 2008. És coneguda per la seva excel·lent capacitat de detecció d'amenaces avançades i per utilitzar tècniques d'aprenentatge automàtic per identificar anomalies en grans volums de dades. Securonix ha guanyat una popularitat creixent tant a Europa com a nivell mundial, especialment en sectors que requereixen un alt nivell de seguretat. La seva última actualització es va realitzar el 2023, afegint millores significatives en la seva interfície i capacitats d'anàlisi de seguretat.

1.13 Monitorització

2.4.5. Solució LogRhythm

LogRhythm va ser llançat l'any 2003 com una solució comercial que proporciona una gestió avançada d'incidents de seguretat. Destaca per la seva facilitat d'ús i la seva capacitat per integrar-se amb sistemes IT i OT, cosa que la fa molt popular entre empreses de mida mitjana a gran. Té una presència forta tant a Europa com a nivell mundial, gràcies al seu bon equilibri entre funcionalitats i facilitat de desplegament. L'última actualització de LogRhythm es va dur a terme el 2023, assegurant-se que la solució estigui alineada amb les noves necessitats del mercat.

2.4.6. Solució McAfee Enterprise Security Manager

McAfee Enterprise Security Manager, introduït el 2010, és una solució comercial que ofereix una excel·lent correlació d'esdeveniments i una resposta ràpida a incidents de seguretat. McAfee ha aconseguit una implantació significativa a nivell global i a Europa, sent utilitzat per empreses que busquen una solució integrada de seguretat. La seva força resideix en la seva capacitat de gestionar grans volums de dades de seguretat en temps real. La seva última actualització va ser el 2023, incorporant noves funcionalitats per millorar la protecció contra amenaces avançades.

2.5. Conclusions de l'estudi de mercat

Els criteris utilitzats per seleccionar les solucions de monitorització i seguretat s'han basat en diversos factors clau. En primer lloc, s'ha valorat la capacitat d'integració amb infraestructures IT i OT, així com la compatibilitat amb tecnologies de control industrial com SCADA i PLCs. A més, s'ha considerat la flexibilitat i escalabilitat de les solucions per adaptar-se a les necessitats actuals i futures de l'organització. També ha estat determinant l'eficàcia en la gestió de seguretat i la seva capacitat per detectar i respondre ràpidament davant incidents de ciberseguretat. Per últim, s'ha tingut en compte el compliment normatiu, com l'Esquema Nacional de Seguretat (ENS), i el suport de la comunitat o dels proveïdors de les solucions.

Per les raons anteriorment indicades s'ha seleccionat les següents solucions :

- Solució seleccionada per la monitorització IT. Nagios ha estat triat per la seva eficàcia en la supervisió d'infraestructures IT, gràcies al seu caràcter de codi obert, que facilita la personalització i expansió segons els requeriments de l'organització. Aquesta eina s'està utilitzat actualment i no hi ha motius tècnics pel seu canvi.
- Solució seleccionada per monitoritzar els Telecontrols. Zabbix ha estat seleccionat per la seva excel·lent capacitat d'integració amb sistemes de telecontrol com SCADA i PLCs, convertint-lo en una solució òptima per a la monitorització d'infraestructures OT.
- Solució seleccionada per monitoritzar esdeveniments o solució SIEM. Splunk es destaca com una eina líder en la gestió d'esdeveniments de seguretat (SIEM), oferint una anàlisi en temps real i una detecció d'amenaces avançada, cosa que el fa imprescindible per garantir la seguretat i el compliment normatiu

1.13 Monitorització

en els entorns críptics i industrials. Aquesta eina tindrà un ús transversal i per tant la decisió final recau en el departament de ciberseguretat.

Aquestes tres solucions conjuntament cobreixen de manera integral les necessitats de l'organització en termes de monitorització.

2.5.1. Elecció de la solució monitorització IT

La selecció de Nagios XI com a eina de monitorització per a la infraestructura IT es justifica per diverses raons tècniques i funcionals. En primer lloc, es tracta d'una solució de codi obert, la qual cosa permet una major flexibilitat i adaptabilitat en entorns personalitzats. A més, és àmpliament coneguda per la seva capacitat de monitorització bàsica d'infraestructures IT, oferint visibilitat sobre paràmetres com l'estat de la CPU, memòria, ús del disc i serveis de sistema operatiu. Aquestes funcionalitats cobreixen les necessitats essencials d'un entorn IT tradicional, on es busca principalment controlar el rendiment dels servidors i dispositius de xarxa.

Nagios XI és conegut per ser una eina robusta amb una arquitectura modular, que permet una fàcil extensió mitjançant complements i plugins desenvolupats per la comunitat. Aquesta característica és especialment útil en infraestructures IT que evolucionen amb el temps, ja que permet adaptar la solució sense grans inversions addicionals. La seva interfície d'usuari és moderada, però la seva facilitat d'instal·lació i configuració permet que els equips tècnics puguin gestionar-lo sense una corba d'aprenentatge massa elevada. A més, la seva àmplia comunitat de suport garanteix que qualsevol problema pugui ser resolt ràpidament, oferint una gran documentació i assistència en línia.

En termes de compliment normatiu, Nagios XI compleix amb les expectatives requerides per les normatives com l'Esquema Nacional de Seguretat (ENS) i les bones pràctiques d'ISO 27001, proporcionant una capa de seguretat que facilita la gestió de la infraestructura IT, garantint que els sistemes es monitoritzin de manera constant i eficient. Aquesta solució és una opció provada i fiable en entorns corporatius i ofereix un equilibri perfecte entre funcionalitat, escalabilitat i cost, fent-la ideal per a la monitorització d'infraestructures IT.

2.5.2. Elecció de la solució de monitorització Telecontrols

La selecció de Zabbix com a eina de monitorització per a entorns OT, especialment per a la monitorització de sistemes de telecontrol com els SCADA, frontals de comunicació i PLCs, es basa en la seva capacitat d'adaptar-se a entorns complexos d'automatització industrial. Zabbix, a diferència d'altres eines, ofereix una arquitectura distribuïda que és ideal per monitoritzar infraestructures OT, on la disponibilitat i la resposta en temps real són essencials.

Un dels principals punts forts de Zabbix és la seva capacitat per recollir dades avançades i en temps real des de diferents punts de control, incloent SCADA. Zabbix permet recollir i analitzar aquestes dades de manera distribuïda, assegurant que qualsevol canvi o anomalia en el rendiment es detecti immediatament, la qual cosa és vital en entorns d'alta criticitat com el control d'aigua i infraestructures industrials.

1.13 Monitorització

Zabbix és una eina de codi obert, la qual cosa proporciona una gran flexibilitat per personalitzar la monitorització segons les necessitats específiques del sistema SCADA i les comunicacions amb PLCs. L'eina ofereix una interfície intuïtiva i amigable per a l'usuari, la qual cosa facilita la configuració de punts de control específics i sondes per a la detecció d'anomalies, augmentant l'eficiència de la supervisió dels processos industrials. La seva capacitat per gestionar grans volums de dades, juntament amb la seva alta escalabilitat, el fa adequat per entorns que creixen en complexitat o que necessiten agregar més punts de control en el futur.

Un altre avantatge de Zabbix és la seva capacitat per enviar notificacions en temps real sobre qualsevol problema o alerta crítica, així com la seva facilitat d'integració amb altres sistemes de notificació o eines de resposta a incidents. Aquesta característica és essencial en un entorn de telecontrol com aquest, on el temps de resposta és clau per evitar interrupcions del servei. Zabbix també ofereix una col·lecció avançada de mètriques, la qual cosa permet una visibilitat completa sobre l'estat dels SCADA, els PLCs i els frontals de comunicació.

Zabbix compleix amb les normatives de seguretat com l'ENS i les bones pràctiques d'ISO 27001, proporcionant un entorn segur per monitoritzar sistemes OT, amb capacitats per protegir les dades i garantir la disponibilitat contínua dels sistemes de control. Així doncs, Zabbix s'adapta perfectament als requisits de telecontrol en entorns complexos com els descrits, oferint una monitorització completa i segura dels sistemes SCADA, PLCs i frontals de comunicació.

2.5.3. Elecció de la solució SIEM

Splunk ha estat seleccionat com a solució SIEM (Security Information and Event Management) per la seva escalabilitat, robustesa i per ser una de les eines més potents en l'àmbit de la ciberseguretat a nivell mundial. Splunk és una solució comercial desenvolupada per oferir una visibilitat completa sobre les infraestructures IT i OT, recopilant i correlacionant grans volums de dades en temps real, la qual cosa permet identificar anomalies i detectar possibles incidents de seguretat amb una alta eficàcia.

Un dels punts forts de Splunk és la seva capacitat per gestionar grans volums de dades, com els que es generen en sistemes SCADA o en xarxes industrials, proporcionant una anàlisi avançada i en temps real. Aquesta capacitat és essencial en un entorn com el descrit, on es manegen tant dades operatives com dades de seguretat. Splunk és reconegut per la seva capacitat de correlació d'esdeveniments de seguretat, identificant patrons que podrien passar desapercebuts amb altres eines. A més, la seva interfície d'usuari avançada facilita la visualització de dades i la creació de quadres de comandament personalitzats, permetent una gestió eficient de les amenaces de seguretat.

Splunk està àmpliament implantat a Europa i arreu del món, especialment en sectors industrials, financers i governamentals que requereixen una solució robusta per a la seguretat. La seva escalabilitat li permet adaptar-se a infraestructures de qualsevol mida, des de petites empreses fins a grans corporacions multinacionals. La solució també ofereix una excel·lent integració amb altres eines de seguretat, com les plataformes de resposta a incidents o solucions de firewall, creant un ecosistema de seguretat centralitzat.

1.13 Monitorització

La seguretat i el compliment normatiu són factors clau en la decisió d'utilitzar Splunk com a SIEM. La seva arquitectura permet complir amb normatives com l'ENS i les bones pràctiques d'ISO 27001, garantint que les dades estiguin protegides i que es disposi d'una auditoria contínua de seguretat. A més, Splunk ha estat constantment actualitzat, amb la seva darrera versió llançada el 2023, assegurant que la solució està al dia enfront les amenaces modernes i emergents.

Per tant, Splunk és la millor elecció per a una gestió integral de la seguretat a través d'un sistema SIEM, garantint una resposta ràpida davant incidents i oferint una visibilitat completa sobre les infraestructures crítiques.

1.13 Monitorització

3. PUNTS DE CONTROL

Un punt de control de monitorització és un element clau dins d'un sistema de supervisió i control, utilitzat per recopilar informació específica sobre l'estat o el funcionament d'un dispositiu, un sistema o un procés dins d'una infraestructura IT o OT. Aquests punts de control poden estar associats a una àmplia gamma de paràmetres, com ara l'ús de CPU, memòria, temperatura, estat de xarxa o, en el cas d'infraestructures OT, el rendiment d'un PLC o SCADA. Els punts de control permeten la recollida de dades en temps real i són crucials per identificar anomalies, predir possibles fallades o optimitzar el rendiment de la infraestructura.

Cada punt de control ha de ser configurat per monitoritzar meticulosament una variable o conjunt de variables determinades, i la seva informació és processada per les eines de monitorització, com Nagios o Zabbix, per oferir informes o alertes en cas de comportaments fora de la normalitat.

Amb la nova arquitectura que es planteja en aquest projecte, s'incorporaran nous punts de monitorització per supervisar elements com els SCADA, els frontals de comunicació i els PLCs. Aquests punts de control permetran una supervisió més granular del sistema, recollint dades específiques de les comunicacions, rendiment i estat d'aquests dispositius. A més, amb la incorporació de Zabbix per a la infraestructura OT, serà necessari establir noves sondes que permetin integrar aquestes dades de manera eficient. Aquest canvi implicarà una reconfiguració de les eines actuals, adaptant-les per a gestionar la informació que prové d'aquests nous punts de control, així com una revisió de les polítiques de notificació per assegurar que qualsevol anomalia detectada en aquests nous elements es pugui gestionar de manera ràpida i eficient.

Servei	Descripció	Àrea Tecnològica	Solució Nagios IT	Solució Zabbix Telecontrol	Solució SIEM ciber
Uptime	Monitorització del darrer reinici del servidor, aplicable a tots els servidors	IT	✓	✓	
CPU	Monitorització de l'ús de la CPU del servidor, aplicable a tots els servidors	IT	✓	✓	
Memòria	Monitorització de l'ús de la memòria del servidor, aplicable a tots els servidors	IT	✓	✓	
Espai a disc	Monitorització de l'espai a disc del servidor, aplicable a tots els servidors	IT	✓	✓	
Antivirus	Monitorització si l'antivirus està operatiu, aplica a tots els servidors	IT	✓	✓	

1.13 Monitorització

Servei	Descripció	Àrea Tecnològica	Solució Nagios IT	Solució Zabbix Telecontrol	Solució SIEM ciber
Comunicacions estacions	Monitorització de l'estat de les comunicacions amb els PLCs, aplica als tres centres	Comunicacions		✓	
Backups Scada	Monitorització de l'estat del backup diari de la BD del Scada, aplica als tres centres	IT		✓	
Exportació Backup	Monitorització del traspàs del backup Scada al centre destí	IT		✓	
Contingència	Monitorització de la replicació de la informació cap al centre de contingència, aplica als tres centres	IT		✓	
Tasques Scada	Monitorització de les tasques Scada ANA, ANAC, BI, MEGA, CNSL, DANA, FT, LIN, MEB, MNC, MTC, PLC, PVW, RALR, SP, ANADIF, ESCO, CIMIO, aplica als tres centres	OT		✓	
Logs Scada	Monitorització de la mida dels logs de l'Scada, aplica als tres centres	OT		✓	
Tasques Històriques	Monitorització de les tasques Scada, aplica als tres centres	OT		✓	
Drive E	Monitorització espai de la unitat E, aplica als tres centres	IT	✓	✓	
Drive S	Monitorització espai de la unitat E, aplica als tres centres	IT	✓	✓	
Drive G	Monitorització espai de la unitat E, aplica als tres centres	IT	✓	✓	
CPU disponible per les comunicacions PLC	Monitorització de la CPU disponible per realitzar les comunicacions al PLC, aplica a tots els PLCs	OT		✓	
Memòria PLC	Monitorització de la memòria utilitzada pel PLC, aplica a tots els PLCs	OT		✓	
Cicles general de programes PLC	Monitorització dels cicles general d'execució dels programes, aplica a tots els PLCs. Alerta por	OT		✓	

1.13 Monitorització

Servei	Descripció	Àrea Tecnològica	Solució Nagios IT	Solució Zabbix Telecontrol	Solució SIEM ciber
	sobrecarrega de temps de cicle principal				
Estat dels diferents mòduls que conformen un xassís de PLC	Monitoritzar els slots del PLC, caldrà monitoritzar el status i el codi d'error.	OT		✓	
Data darrera compilació i versió	Monitoritzar el valor de la data de compilació i la versió de l'objecte. Recol·lecció des del software de gestió d'actius	OT		✓	
Logs errors PLC	Monitoritzar els registres d'errors o avisos generats pel PLC, solament és comptabilitzaran els errors majors. Tindrem una matriu amb els camps tipus, codi	OT		✓	
Estat de l'estació	Monitorització de l'estat de la estació	OT		✓	
Fonts de dades	Monitorització que les fonts de dades s'estiguin enviant correctament al SIEM, començarà a partir del router	IT/OT/ Comunicacions /Configuració			✓
Seguretat Telecontrol	Monitorització d'esdeveniments relacionats amb la seguretat, intents d'accés no autoritzat, detecció d'anomalies, intents d'injecció SQL, escanejos de ports	IT/OT			✓
Seguretat PLCs	Monitorització l'activitat dels firewalls dels PLCs, detecció d'intrusions IDS	OT			✓
Correlació esdeveniments	Detectar esdeveniments anòmals o patrons de comportament inusuals	IT/OT/ Comunicacions /Configuració			✓
Detecció de vulnerabilitats	Supervisar i gestionar la identificació de vulnerabilitats a través del SIEM	IT/OT/ Comunicacions /Configuració			✓*

1.13 Monitorització

Servei	Descripció	Àrea Tecnològica	Solució Nagios IT	Solució Zabbix Telecontrol	Solució SIEM ciber
Logs auditoria	Monitoritzar la recollida i emmagatzematge dels logs de seguretat. Assegurar que es mantenen els requisits de retenció de dades segons les normatives legals (com l'ENS o ISO 27001)	IT			✓
Monitorització versions hardware i firmware PLC	Monitoritzar la versió actual del hardware i del firmware del PLC	Configuració		✓	
Monitorització versions objectes PLC i SCADA	Monitoritzar la versió actual dels objectes despleats al PLC i SCADA.	Configuració		✓	
Monitorització estat API	Monitoritzar estat API	OT		✓	
Monitorització càrrega de peticions	Monitoritzar la darrera càrrega de peticions	OT		✓	
Monitorització estat ETL	Monitoritzar estat de les càrregues ETL	IT		✓	

Taula 3-1: Punts de Control

*L'eina SIEM no detecta vulnerabilitats.

3.1. Relació de variables monitorització amb PLC

Les variables que es monitoritzen des del PLC, es mostren a la següent taula:

Servei	Descripció	Variable PLC	Unitats
CPU disponible per les comunicacions PLC	Monitorització de la CPU disponible per realitzar les comunicacions al PLC, aplica a tots els PLCs	TimeSlice	Sencer del 10 al 90 en percentatge
Memòria PLC	Monitorització de la memòria utilitzada pel PLC, aplica a tots els PLCs	Memoria	Sencer del 0 a 100 en percentatge
Temps de cicle dels programes del PLC	Monitorització del temps de cicle que supera el temps màxim. Alerta por sobrecarrega de temps de cicle principal.	TempsCicleMaxim	Temps de cicle dels programes del PLC

1.13 Monitorització

Servei	Descripció	Variable PLC	Unitats
Temps de cicle mitjà	Monitorització del temps de cicle mitjà.	TempsCicleMigReal	Coma flotant
Temps de cicle actual	Monitorització del temps del cicle actual.	TempsCicleActual	Doble sencer
Estat dels diferents mòduls que conformen un xassís de PLC	Monitoritzar els slots del PLC, caldrà monitoritzar el status i el codi d'error.	Sys_IOS	Monitoritzar els slots del PLC, caldrà monitoritzar el status i el codi d'error.
Data darrera compilació i versió	Monitoritza el valor de la data de compilació i la versió de l'objecte. Recol·lecció des del software de gestió d'actius	versioAquestPrograma	Monitoritza el valor de la data de compilació i la versió de l'objecte. Recol·lecció des del software de gestió d'actius
Logs errors PLC	Monitoritza els registres d'errors o avisos generats pel PLC, solament és comptabilitzaran els errors majors. Tindrem una matriu amb els camps tipus, codi	Sys_RegistreErrorsMajors	Matriu amb la informació de les 10 errades que afecta a la CPU del PLC
Estat de l'estació PLC	Monitorització de l'estat de la estació	xxx.ActualitzacioFlashEnCurs	Matriu amb la informació

Taula 3-2: Variables monitoritzades del PLC

3.1.1. Configuració de l'estat de l'estació PLC

Taula de la configuració de la matriu de l'estat de l'estació PLC.

Descripció	Variable PLC	Unitats
AOI_ExtreureStatus	aoi_ExtreureStatus	Binari
Status Informació	Status	Binari
Actualització Flash en curs	ActualitzacioFlashEnCurs	Binari
Mode Fallada	ModeFallada	Binari
Flash Incorrecte	FlashIncorrecte	Binari
Mode Run	ModeRun	Binari
Mode Program	ModeProgram	Binari
Fallada Menor Recuperable	FalladaMenorRecuperable	Binari
Fallada Menor No Recuperable	FalladaMenorNoRecuperable	Binari
Fallada Major Recuperable	FalladaMajorRecuperable	Binari

1.13 Monitorització

Descripció	Variable PLC	Unitats
FalladaMajorNoRecuperable	FalladaMajorNoRecuperable	Binari
InterruptorEnRun	InterruptorEnRun	Binari
InterruptorEnProgram	InterruptorEnProgram	Binari
InterruptorEnRemote	InterruptorEnRemote	Binari
CanviantDeMode	CanviantDeMode	Binari
ModeDepuracio	ModeDepuracio	Binari

Taula 3-3: Configuració de l'estat de l'estació PLC

4. PASSAREL·LA D'INTERCANVI D'INFORMACIÓ

Per intercanviar informació de manera efectiva entre un sistema SCADA i la solució de monitorització del telecontrol amb l'eina Zabbix, és important utilitzar mètodes que siguin robustos, segurs i compatibles amb els estàndards industrials. Després de analitzar diferents alternatives s'ha conclòs que el millor mètode d'intercanvi d'informació es a través d'un procés d'exportació des del SCADA fins a l'eina de monitorització.

Caldrà generar un nou processos de traspàs d'informació des de diferents aplicacions cap a la monitorització. Aquesta aplicació centralitzarà totes les alertes i informació rellevant associada als Centres de Control. La informació podrà arribar des de diferents orígens, la pròpia dels agents de l'aplicació de monitorització però també tindrem orígens com Scada, SIEM. Per l'intercanvi d'informació utilitzarem APIs.

L'ús d'APIs per intercanviar informació entre aplicacions millora significativament la seguretat i l'eficiència del flux de dades. Les APIs permeten establir canals de comunicació controlats, on es poden aplicar autenticació, xifratge i control d'accés per assegurar que només usuaris i sistemes autoritzats accedeixin a les dades. A més, les APIs faciliten una integració estandarditzada, la qual cosa redueix errors i millora la interoperabilitat entre sistemes.

Seguidament s'identifiquen els intercanvis necessaris i les aplicacions involucrades. Per millorar la claredat i control de l'intercanvi, incorporarem una procés de cadascun d'ells.

- Procés d'importació de dades des del Scada
- Procés d'importació de dades des del SIEM

4.1. Procés d'importació de dades Scada

L'intercanvi d'informació entre l'aplicació SCADA i l'eina de monitorització Zabbix permet integrar la supervisió dels sistemes industrials amb una plataforma centralitzada de monitoratge. Gràcies a aquesta connexió, és possible obtenir dades en temps real de l'SCADA, com ara alarmes, tendències i estats d'equipaments, per ser analitzades i gestionades des de Zabbix. Això facilita la detecció de problemes i l'optimització del rendiment,

1.13 Monitorització

millorant així la capacitat de resposta davant incidents. A més, l'automatització d'avisos i la generació d'informes completen l'administració eficient de la infraestructura.

A continuació es detallen les característiques principals del procés d'intercanvi d'informació entre SCADA i Zabbix:

- Nom del procés : TRASPAS_SCADA_MONIT
- Descripció : Tasca d'exportació dades Scada i importació a l'eina de Monitorització
- Freqüència d'extracció : Cada 5 minuts
- Format de les dades : API
- Gestió d'errors : logs monitoritzats
- Compliment normatiu : ENS nivell mitjà (auditoria de processos i traçabilitat)

4.1.1. Flux general

Seguidament s'implementa el flux d'informació del procés:

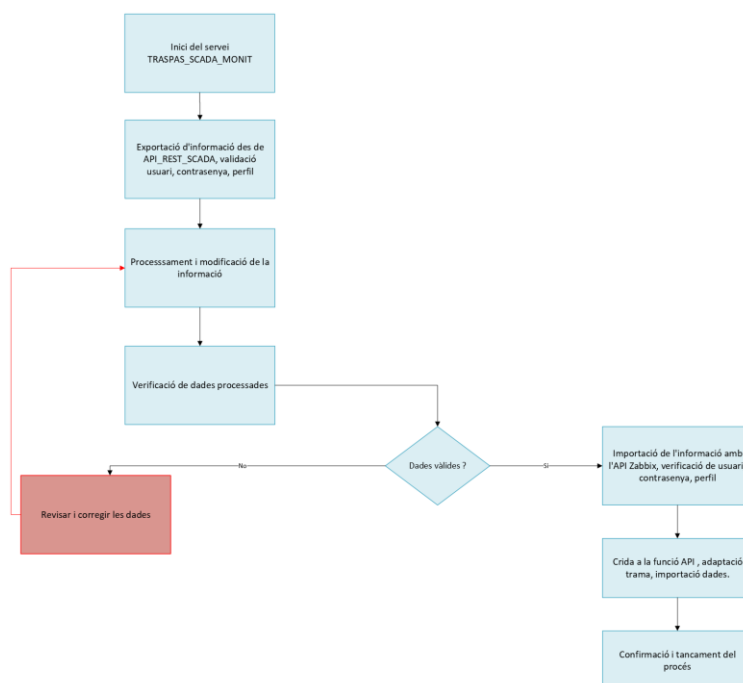


Figura 4-1: Flux d'informació del procés

4.1.2. Eines utilitzades

- Eines extracció : API Scada.
- Eines de transformació : scripts i eines ETL.
- Eines de càrrega : API Monitorització aplicació Zabbix.

1.13 Monitorització

4.2. Procés d'importació de dades SIEM

L'intercanvi d'informació entre el SIEM i l'eina de monitorització Zabbix permet integrar la supervisió dels esdeveniments de seguretat en una plataforma centralitzada de monitoratge. Això facilita la detecció proactiva de vulnerabilitats i amenaces, millorant així la capacitat de resposta davant incidents de seguretat. A més, l'automatització d'avisos i la generació d'informes asseguren una gestió eficient de la seguretat de la infraestructura.

A continuació es detallen les característiques principals del procés d'intercanvi d'informació entre el SIEM i Zabbix:

- Nom del procés: TRASPAS_SIEM_MONIT
- Descripció: Tasca d'extracció i traspàs de dades de seguretat del SIEM cap a Zabbix.
- Freqüència d'extracció: Cada 10 minuts
- Format de les dades: API
- Gestió d'errors: Logs monitoritzats per assegurar la correcta execució i detectar anomalies.
- Compliment normatiu: ENS nivell mitjà (auditoria de processos i traçabilitat).

Per poder definir el flux i les eines SIEM caldrà més informació, no obstant, es deixarà implementada l'API de l'eina de monitorització per poder realitzar l'intercanvi d'informació amb el SIEM escollit pel departament de ciberseguretat d'ATL.

1.13 Monitorització

5. REQUISITS MAQUINARI

La solució escollida per incorporar la monitorització dels telecontrols i xarxa OT s'ha d'instal·lar a un maquinari en la infraestructura del client ATL. Per aquesta raó caldrà analitzar la volumetria de la màquina virtual que albergarà la solució de monitorització **Zabbix**, cal tenir en compte diversos factors, com el nombre de punts de control que es monitoritzaran, la freqüència de les consultes, el volum de dades que es recolliran, i els requisits d'escalabilitat per al futur.

A continuació, es presenta una estimació basada en una infraestructura típica que inclou la monitorització d'entorns IT i OT:

- CPU : 4- vCPUs
- Memòria RAM 16 GB
- Espai a disc 500 GB de disc SSD
- Xarxa mínim 1 Gbps
- Sistema operatiu CentOS
- Caldrà realitzar backup
- Agent Antivirus
- Agent SIEM

1.13 Monitorització

6. PROGRAMA DE TASQUES

El programa de tasques del projecte d'integració de nous punts de control en la plataforma Zabbix té com a objectiu ampliar les capacitats de monitoratge de l'eina, garantint una supervisió més completa i detallada dels sistemes crítics.

Aquest projecte inclou la configuració, implementació i validació de nous ítems de monitoratge, així com la integració amb fonts de dades externes.

Les tasques s'organitzen en diferents fases per assegurar un desplegament eficient i un seguiment òptim del rendiment i la seguretat de la infraestructura.

Cal indicar que per adaptar la solució a les necessitats reals del client i millorar en la qualitat de la solució s'han realitzat els següents canvis :

- L'oferta incorporava la integració de nous punts de control en les diferents àrees Preventiva IT, perspectiva OT, perspectiva de comunicacions, perspectiva de configuració amb l'eina Nagios. Finalment l'eina on s'integraran les sondes serà Zabbix.
- Queda exclòs d'aquests treballs la instal·lació de la nova eina i la migració de les sondes existents.

Per tal de complir amb els objectius establerts en el projecte, s'incorporaran les noves sondes de monitorització segons els criteris indicats. Aquestes sondes permetran una vigilància més exhaustiva i eficient dels sistemes, alineada amb les necessitats del client.

No obstant això, per dur a terme aquestes tasques, serà imprescindible disposar de l'entorn Zabbix completament operatiu, ja que és l'eina central que gestionarà la recollida, processament i visualització de les dades proporcionades per les sondes.

Per aquest motiu la instal·lació, migració de sondes existents, el traspàs d'informació i la formació es realitzarà prèviament a la creació de nous punts de control a l'eina de monitorització Zabbix.

Durant la creació de nous punts de control a Zabbix, es realitzaran les següents activitats:

- Identificació dels nous dispositius i sistemes que s'han d'incorporar al sistema de monitorització, especialment en l'àmbit OT (PLC, SCADA, servidors frontals).
- Creació de nous punts de control per a aquests dispositius, incloent la supervisió de paràmetres com latència de comunicacions, rendiment dels PLC, estats de SCADA, etc.
- Configuració de les alertes personalitzades segons els requeriments operatius i de ciberseguretat.
- Test de funcionament dels nous punts de control i verificació que totes les dades es recullen i processen correctament a Zabbix.