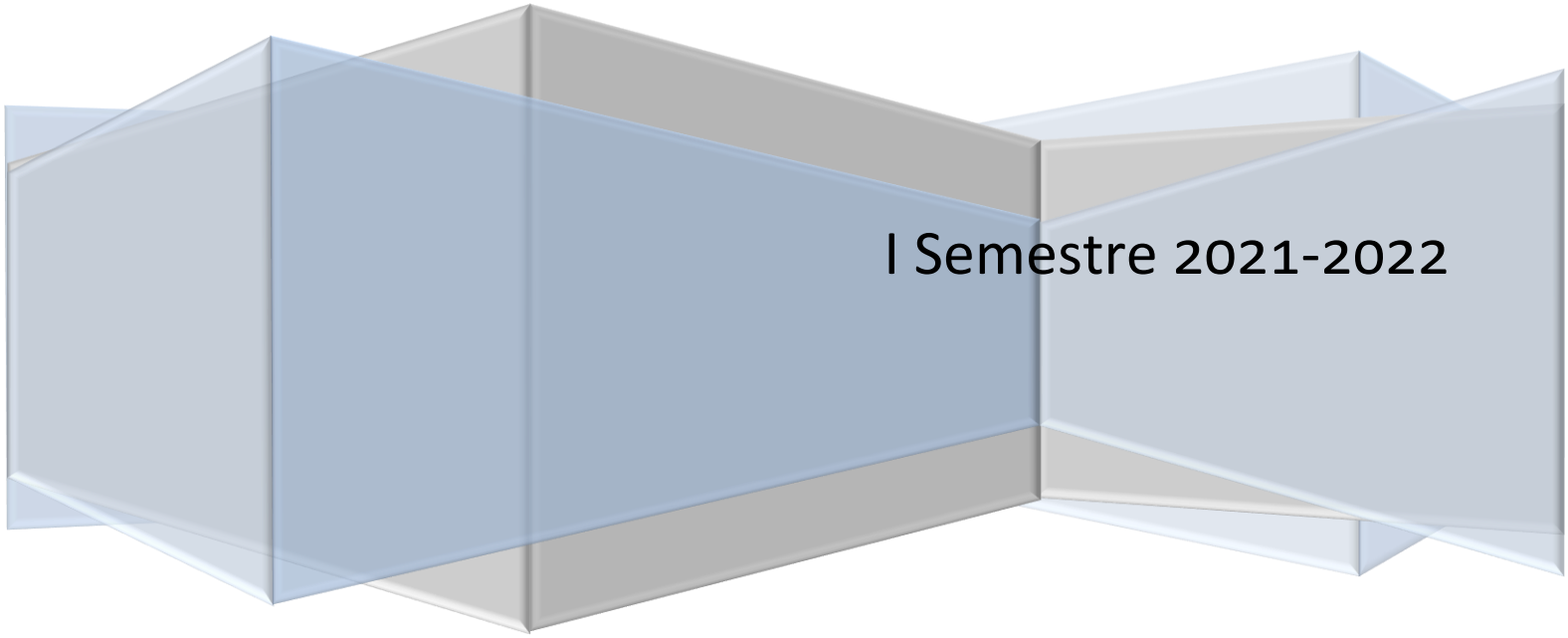
Memòria TFM

Model teòric de creació d'un SOC per a entorns al núvol amb les eines natives d'AZURE.

Autor: Jaume Jofre Bravo

Professor col·laborador: Erik de Luis Gargallo



I Semestre 2021-2022

Contingut

Índex de taules

Índex il·lustracions

FITXA DEL TREBALL FINAL

Títol del treball:	Model teòric de creació d'un SOC per a entorns al núvol amb les eines natives d'AZURE
Nom de l'autor:	Jaume Jofre Bravo
Nom del professor col·laborador:	Erik de Luis Gargallo
Nom del PRA:	Jordi Serra Ruiz
Data d'entrega:	01/01/01
Titulació:	Màster ciberseguretat i Privadesa
Àrea del treball final:	Seguretat en xarxes i sistemes
Idioma del treball:	Català
Paraules clau:	Cloud, SOC, registres, seguretat
Resum del treball:	

Aquesta memòria presenta un model teòric d'implementació de serveis SOC al núvol per la prestació de sistemes de seguretat d'infraestructures, hostatjades a Microsoft Azure.

Es presenta un model d'infraestructura d'un client fictici anomenat ACME: es descriu breument el funcionament d'un SOC i les eines que pot fer servir, es revisen alguns possibles orígens de dades de seguretat de la plataforma i es planteja com es pot fer arribar aquesta informació al SOC pel seu tractament.

La metodologia seguida ha estat una descripció teòrica, ometent conscientment referències comercials específiques més enllà dels recursos propis existents al núvol de Microsoft Azure, per tal de fer un redactat agnòstic a les eines que, finalment, siguin implementades per desplegar els serveis i funcionalitats del SOC.

El resultat ha estat una memòria estructurada en 7 capítols, on s'ha presentat cadascun dels components mencionats i s'ha procurat proporcionar al lector totes aquelles referències necessàries per poder aprofundir en cadascun dels elements tractats.

La conclusió final del treball és que la quantitat d'informació que es pot generar dels recursos d'Azure, tant a nivell de registres com de mètriques, ofereix dues possibilitats diferents de tractament: una primera on es filtrarà en origen la informació crítica de seguretat i una segona en la que es farà un enviament massiu de tots els esdeveniments pel posterior tractament del SOC.

Abstract (in English)

The current thesis exposes a theoretical model for cloud SOC implementation services, on cloud-hosted Microsoft Azure infrastructure.

It presents a common infrastructure for unreal client named ACME and describes an outsourced SOC services, with some tools that could be used, lists some available data sources, and considers how this information can be delivered to the SOC for their processing.

The methodology followed has been to write a theoretical description, omitting specific business references beyond Microsoft Azure's own resources in the cloud, in order to present an agnostic description of the tools that would be finally implemented to carry out SOC tasks.

The result has been a report structured in 7 chapters where each of the mentioned components has been presented. The reader will gain all necessary references to be able to delve into each of the elements treated.

The final conclusion of this thesis, is that the amount of information that can be generated from Azure resources both in terms of records and metrics, offers two different treatment possibilities, the first one will send the critical security information filtered at source, and the second option, in which all events will be forwarded massively to the SOC for their analysis and processing.

1. Introducció

1.1. Context i justificació

Aquest Treball de Final del Màster de Ciberseguretat i Privadesa presentarà al lector una guia estructurada de com, a partir de les eines natives de la infraestructura al núvol de Microsoft Azure, es pot obtenir la informació necessària per tal que un SOC (*Security Operation Center*) pugui realitzar les seves funcions.

Les funcions d'un SOC es podrien resumir en els següents punts:

- Gestionar les operacions, monitoritzar i actualitzar els diversos dispositius de defensa perimetrals.
- Detectar i coordinar respostes, dur a terme investigacions de ciberatacs i ciberamenaces així com resoldre els incidents de seguretat que es puguin produir.
- Coordinar el Servei d'Atenció Tècnica (SAT) d'alertes de seguretat a les connexions a Internet, a xarxes interadministratives comuns i, a petició, a xarxes corporatives de les entitats.
- Realitzar l'anàlisi de vulnerabilitats d'aplicacions i serveis.
- Serveis contra l'abús d'identitat digital.
- Fer una evolució progressiva del SOC per garantir l'adaptació a l'entorn dinàmic.

En definitiva, es cerca donar resposta al repte que ha d'afrontar un SOC en el seu objectiu de monitoritzar la seguretat de la xarxa i un sistema informàtic al núvol. Més concretament, aquest treball vol arribar a un model teòric de creació d'un SOC per a un entorn al núvol de Microsoft Azure, determinant les tecnologies de seguretat necessàries a desplegar en aquest entorn.

1.1.1. Estat de l'art

Entenem per estat de l'art, en el context d'aquest treball, com la versió més innovadora de tecnologia o producte. Així doncs, a continuació es descriurà quines són les últimes tendències en seguretat a l'entorn de computació al núvol d'Azure, analitzant les diferents eines utilitzades a la infraestructura trobem els següents components:

- Azure Sentinel: administració d'esdeveniments i informació de seguretat (SIEM) centralitzada per obtenir visibilitat sobre els registres a tota l'empresa. Tal i com afirma un dels proveïdors[1] que ofereix suport en el desplegament i gestió de Sentinel:

  "Microsoft Azure Sentinel is a state-of-the-art cloud native technology that helps you see and stop cyber threats before they cause harm."

- Azure Security Center: generació d'alertes automatitzades a partir dels estàndards tecnològics adaptats, utilitza el quadern d'estratègies de seguretat en resposta a un avís i, a més, amb el panell de compliment de regulacions (Regulatory Compliance[2]) es pot comprovar si la infraestructura aplica i compleix els estàndards tècnics establerts. Concretament:
  - Azure CIS: CIS[3] és una organització independent i sense ànim de lucre amb la missió de crear confiança en el món connectat. Al seu lloc web

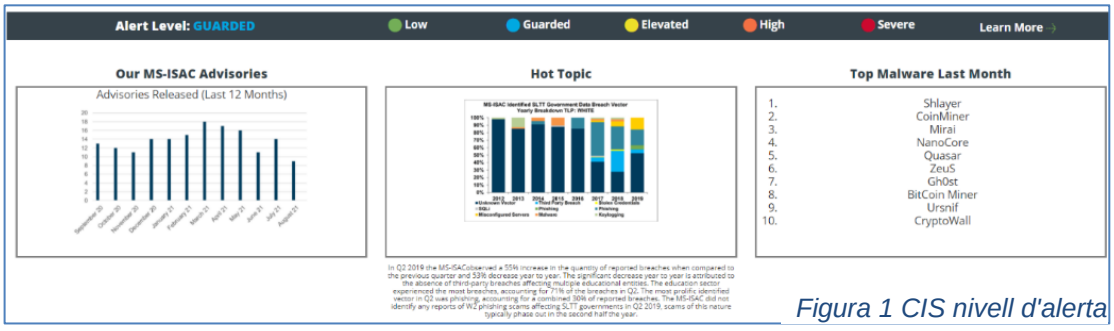


Figura 1 CIS nivell d'alerta

[1] COMTACT (Cloud, Security, Delivery); Data consulta: 24/09/2021;
URL: https://comtact.co.uk/azure-sentinel/
[2] Panel compliment regulacions Azure; Data consulta: 24/09/2021;
URL: https://azure.microsoft.com/es-es/blog/regulatory-...-center-now-available/
[3] Web oficial CIS; Data consulta: 24/09/2021;
URL: https://www.cisecurity.org/cybersecurity-threats/

podem trobar l'estat actual d'alerta quant a ciberseguretat a les infraestructures d'Azure.

- PCI DSS 3.2: és l'estàndard de seguretat de dades de la indústria de les targetes de pagament (PCI DSS). Es va desenvolupar per fomentar i millorar la seguretat de les dades dels titulars de targetes i facilitar-los l'adopció àmplia de mesures de seguretat de dades a nivell mundial. Proporciona una base de requisits tècnics i operatius dissenyada per protegir les dades dels comptes. S'aplica a totes les entitats que participen en el processament de targetes de pagament: els comerciants, els processadors, els compradors, els emissors i proveïdors de serveis a més de totes les altres entitats que emmagatzemen, processen o transmeten dades del titular de la targeta (CHD) i / o dades d'autenticació sensibles (SAD).

PCI Data Security Standard – High Level Overview

Build and Maintain a Secure Network and Systems	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Protect all systems against malware and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need to know 8. Identify and authenticate access to system components 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel

Figura 2 Resum regulació PCI DSS

- ISO 27001[4]: la norma ISO / IEC 27001 és àmpliament coneguda per proporcionar requisits per a un sistema de gestió de seguretat de la informació (ISMS), tot i que hi ha més d'una dotzena d'estàndards a la família ISO / IEC 27000. El seu ús permet a organitzacions de qualsevol tipus gestionar la seguretat d'actius com: informació financera, propietat intel·lectual, dades dels empleats o informació confiada per tercers.

[4] ISO ORG web oficial; Data consulta: 28/09/2021;
URL: https://www.iso.org/isoiec-27001-information-security.html

- SOC TSP: desenvolupat per l'American Institute of CPAs (AICPA), SOC2 defineix criteris per gestionar les dades dels clients basant-se en els principis de servei de confiança: seguretat, disponibilitat, integritat del processament, confidencialitat i privadesa.

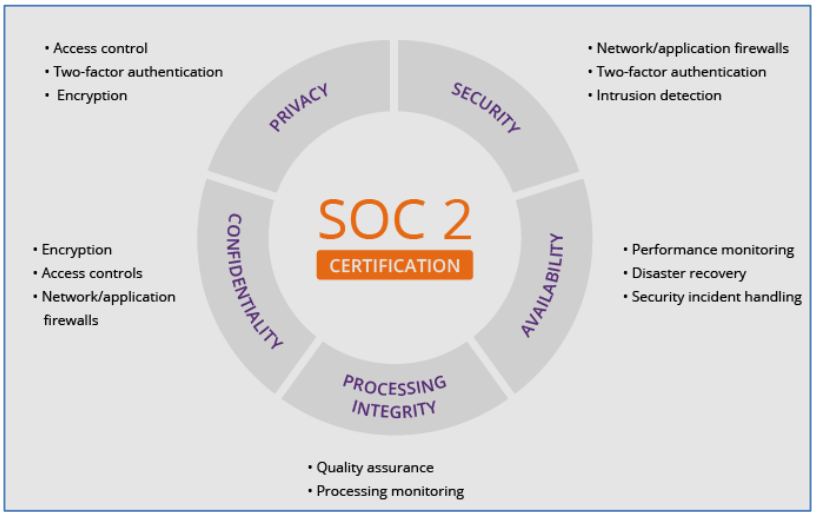


Figura 3 SOC2 Principis de confiança (TSP)

- Azure Monitor: registres d'esdeveniments d'aplicacions i serveis d'Azure.
- Network Security Group (NSG): visibilitat sobre les activitats de xarxa.
- Azure Information Protection: protegeix el correu electrònic, els documents i les dades confidencials que comparteix fora de la seva companyia.

Per altra banda, es presenta el resum dels plans de suport existents en aquesta URL[5] i els resumim a la taula següent:

[5] Plans de suport Azure; Data consulta: 24/09/2021;
URL: https://azure.microsoft.com/en-us/support/plans/

Concepte \ Model	Basic	Desenvolupador	Estàndard	Professional
Preu	Inclòs per tots els clients	29$/mes	100$/mes	1000$/mes
Àmbit	Inclòs per tots els clients	Entorns test i desenvolupament	Entorns de producció	Entorns amb dependències crítiques
24x7 autoajuda amb recursos públics d'Azure	✔	✔	✔	✔
Opció de creació de tiquets il·limitada	✔	✔	✔	✔
Azure advisor[6] – guia de pràctiques recomanades	✔	✔	✔	✔
Azure Health status[7] (estat de la infraestructura) i notificacions	✔	✔	✔	✔
Suport per software de tercers		✔	✔	✔
Accés a suport per correu o telèfon 24x7		Només correu en hores laborals	✔	✔
Gravetat dels incidents i temps de resposta. (C=mínim, B=moderat, A=crític)		C: en 8 hores laborals	C: en 8 hores laborals B: en 4 hores A: en 1 hora	C: en 4 hores laborals B: en 2 hores A: en 1 hora
Suport arquitectura		Guia general	Guia general	Guia directe de enginyers d'Azure

Taula 1 Plans de suport Microsoft Azure

[6] Recomanacions d'Azure; Data consulta: 24/09/2021
URL: https://azure.microsoft.com/en-us/services/advisor/
[7] Estat de salut de la infraestructura; Data consulta: 24/09/2021;
URL: https://status.azure.com/en-us/status

1.2. Objectius

La llista d'objectius que cal assolir un cop finalitzat el projecte és la següent:

- Presentar una arquitectura prototipus de recursos al núvol d'Azure per fer-la servir com a plataforma a protegir per part del SOC.
- Proposar un perfil de SOC el qual es presentarà el treball.
- Recollir tots els orígens d'informació de seguretat disponibles a la infraestructura i definir com gestionar-ne la recollida i el tractament.
- Presentar la normativa vigent, de les diferents associacions professionals i entitats tecnològiques referents, per ajustar la proposta als estàndards establerts.

1.3. Enfocament i mètode seguit

La memòria ha de ser desenvolupada com una referència teòrica que inclogui només els propis recursos de la solució Azure de Microsoft al núvol.

Altres productes o solucions de seguretat de programari lliure o comercials de tercers han de quedar exclosos, per tal de mantenir el punt de vista teòric i evitar inferir en la presa de decisions del lector alhora de implementar solucions específiques per cada cas. Fent-ho així es pretén presentar un punt de vista agnòstic a cap programari concret i permetrà l'adopció de la solució més convenient en cada cas.

Per altra banda, el mètode a seguir consistirà en descripcions dels eixos troncals des del punt de vista de la seguretat, però sense obviar que caldrà donar una visió global d'altres components tècnics que conformen qualsevol infraestructura de les tecnologies de la informació, per guiar en una millor comprensió de la solució que es presentarà.

1.4. Planificació del treball

1.4.1. Tasques a desenvolupar

Per tal de poder assolir els objectius definits caldrà dur a terme les següent tasques:

- Presentar una arquitectura prototipus de recursos al núvol d'Azure per fer-la servir com a plataforma a protegir per part del SOC.
    - Presentar una empresa fictícia amb un conjunt d'aplicacions i serveis íntegrament desenvolupats al núvol d'Azure, així com el seu Tenant (acord empresa – Azure).
    - Descriure cadascun dels components d'aquestes solucions dividits en subscripcions.
    - Detallar els nivells de seguretat IAM d'aquestes subscripcions.
    - Llistar i descriure cadascun dels grups de recursos i recursos membres de les diferents subscripcions. Per exemple:
        - autenticació al núvol amb Azure Active Directory.
        - bases de dades (SQL, MariaDB, MongoDB)
        - dispositius de seguretat: tallafocs, IDS, etc..
        - àrees d'emmagatzematge: Datastore o Datalake gen 2.
        - components de xarxa com vnets, application gateways, etc.

- Proposar un perfil de SOC:
    - Organigrama global del SOC.
    - Objectius generals del SOC incloent els serveis que proporcionarà.
    - Eines disponibles pel SOC: SIEM, SOAR i Datalake.

- Analitzar la normativa vigent de les diferents associacions professionals i entitats tecnològiques referents per ajustar la proposta als estàndards vigents.
    - ISO / IEC 27001
    - NIST: Cybersecurity framework

- ATT&CK
- CCN-CERT

- Establir tots els possibles orígens d'informació disponibles a la infraestructura i definir com gestionar-ne la recollida i el tractament. Cal trobar un mètode per filtrar els successos interessants i realitzar-ne la transferència al SOC minimitzant el màxim possible el volum, per reduir els costos vinculats a les transferències de dades i simplificar l'anàlisi dels registres rebuts.

    - Registres d'activitat i esdeveniments.
        - Metadades disponibles d'Azure per cadascun dels recursos de la infraestructura proposada.
        - Registres propis de cadascun dels elements de la infraestructura. Això inclou, per exemple, entrades dels visors de successos de les màquines virtuals o diferents recursos SaaS disponibles.
    - Registres generats per els dispositius Firewall, balancejadors de càrrega, serveis DDoS i grups de seguretat de xarxa (*Network Security Groups*).
    - Anàlisi de costos, és a dir, recollida periòdica dels informes d'anàlisi de costos per monitoritzar i controlar la infraestructura i els seus consums.
    - Polítiques, informes d'aplicació i detecció d'incidències.

1.4.2. Diagrama de Gantt

El ritme del projecte quedarà emmarcat dins les dates límit del semestre i les entregues parcials de las PACs 1, 2 i 3, per finalitzar amb la memòria, els vídeos amb la presentació del projecte i la defensa del treball.

En el següent diagrama queda detallada la planificació inicial.

#	Name	Duration	Start	Finish	Cost
1	**Definir prototip arquitectura al núvol**	**10,0 d**	**13/09/2021**	**24/09/2021**	**€ 0,00**
2	Crear esquemes disseny	8,0 d	13/09/2021	22/09/2021	€ 0,00
3	Descriure els esquemes	3,0 d	22/09/2021	24/09/2021	€ 0,00
4	**Entrega PAC1**	**25,0 d**	**20/09/2021**	**22/10/2021**	**€ 0,00**
5	Redactar document	5,0 d	20/09/2021	24/09/2021	€ 0,00
6	Diagrama de Gantt	6,0 d	24/09/2021	01/10/2021	€ 0,00
7	**Especificar elements SOC**	**25,0 d**	**20/09/2021**	**22/10/2021**	**€ 0,00**
8	Organigrama general	6,0 d	20/09/2021	27/09/2021	€ 0,00
9	Definir objectius	5,0 d	27/09/2021	01/10/2021	€ 0,00
10	Descripció eines a utilitzar	10,0 d	04/10/2021	15/10/2021	€ 0,00
11	Encaix en estàndards existents	5,0 d	18/10/2021	22/10/2021	€ 0,00
12	**Entrega PAC2**	**35,0 d**	**25/10/2021**	**10/12/2021**	**€ 0,00**
13	**Fonts d'informació i tractament**	**35,0 d**	**25/10/2021**	**10/12/2021**	**€ 0,00**
14	Registre activitats i events elements Azure	10,0 d	25/10/2021	05/11/2021	€ 0,00
15	Logs firewall	15,0 d	01/11/2021	19/11/2021	€ 0,00
16	Logs DDoS	10,0 d	08/11/2021	19/11/2021	€ 0,00
17	Logs NGS	10,0 d	15/11/2021	26/11/2021	€ 0,00
18	Analitiques costs i consums	5,0 d	22/11/2021	26/11/2021	€ 0,00
19	Incidencies politiques aplicades a les	10,0 d	29/11/2021	10/12/2021	€ 0,00
20	**Entrega PAC3**	**5,0 d**	**22/12/2021**	**28/12/2021**	**€ 0,00**
21	Memoria	5,0 d	22/12/2021	28/12/2021	€ 0,00
22	Video + slides	3,0 d	31/12/2021	04/01/2022	€ 0,00
23	Defensa TFM	5,0 d	10/01/2022	14/01/2022	€ 0,00

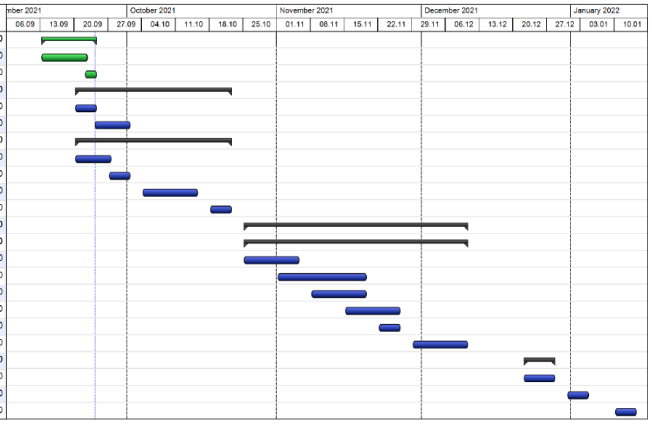


Figura 4 Diagrama Gantt

La disponibilitat horària de l'únic recurs disponible per l'elaboració d'aquesta memòria s'ha definit amb una dedicació diària de 4 hores de dilluns a divendres deixant lliures els caps de setmana. Realment, la distribució horària s'anirà adaptant durant el semestre a la disponibilitat, sempre procurant d'assolir les fites marcades per les PAC en el temps establert. Per altra banda, algunes de les tasques es podran desenvolupar en paral·lel, tot i haver-ne planificat l'execució en sèrie, per tal de mostrar més clarament la dedicació estimada prevista.

1.5. Sumari de productes obtinguts

Essencialment, el que aquesta memòria pretén proporcionar és una guia de referència per la implementació d'una infraestructura genèrica al núvol, un exemple de SOC que proveirà els serveis de seguretat i com articular l'intercanvi de dades entre ambdues parts: client i proveïdor.

1.6. Descripció capítols de la memòria

La memòria està formada per 7 capítols: s'iniciarà presentant un client fictici per tenir clar el disseny de la infraestructura al núvol a la que ha de donar servei el SOC; a continuació s'exposarà el funcionament global del SOC i les eines de les que disposa; es presentaran els diferents elements generadors d'informació al núvol d'Azure; seguidament algunes de les eines habituals en un SOC; i finalment es revisarà com es pot enviar i filtrar tota la informació de seguretat generada per tal que el SOC pugui oferir els seus serveis al client fictici.

2. Arquitectura client ACME

Amb l'objectiu de presentar el model teòric del que tracta aquest treball es partirà d'una empresa fictícia anomenada ACME, que dedica els seus recursos al desenvolupament i comercialització d'aplicacions web, distribuïdes geogràficament a nivell mundial, pels seus clients. Per tal de poder proporcionar un de temps de resposta de qualitat, ACME ha cregut convenient fer el desplegament de la infraestructura on es desenvoluparan, provaran i executaran en mode productiu les seves aplicacions i serveis al núvol, ja que poden disposar d'accés geogràfic proper arreu del món, minimitzant el lag de les aplicacions. Entre els diferents candidats analitzats han optat per les solucions de Microsoft Azure ja que encaixen millor amb els coneixements previs dels enginyers de la companyia.

El model triat per aquest desplegament serà del tipus SaaS (*Software as a Service*), és a dir, la contractació dels serveis necessaris per proporcionar al client les solucions requerides adquirint els diferents components de programari exigits en cada cas.

Així doncs, cal que el disseny de la infraestructura que es faci servir sigui altament modular i permeti una clara segregació entre els diferents projectes i entorns. D'aquesta forma, ACME podrà garantir a cadascun dels seus clients que la informació hostatjada al núvol estarà disponible per aquelles persones que el client decideixi i podrà analitzar els costos específics de cada infraestructura per poder imputar els que correspongui a cada client.

Així mateix, aquest disseny també permetrà que els serveis de SOC contractats, que es presentaran en el punt següent, es puguin segregar clarament per cada un dels clients que contractin els serveis d'ACME.

2.1. Visió global, infraestructura d'ACME

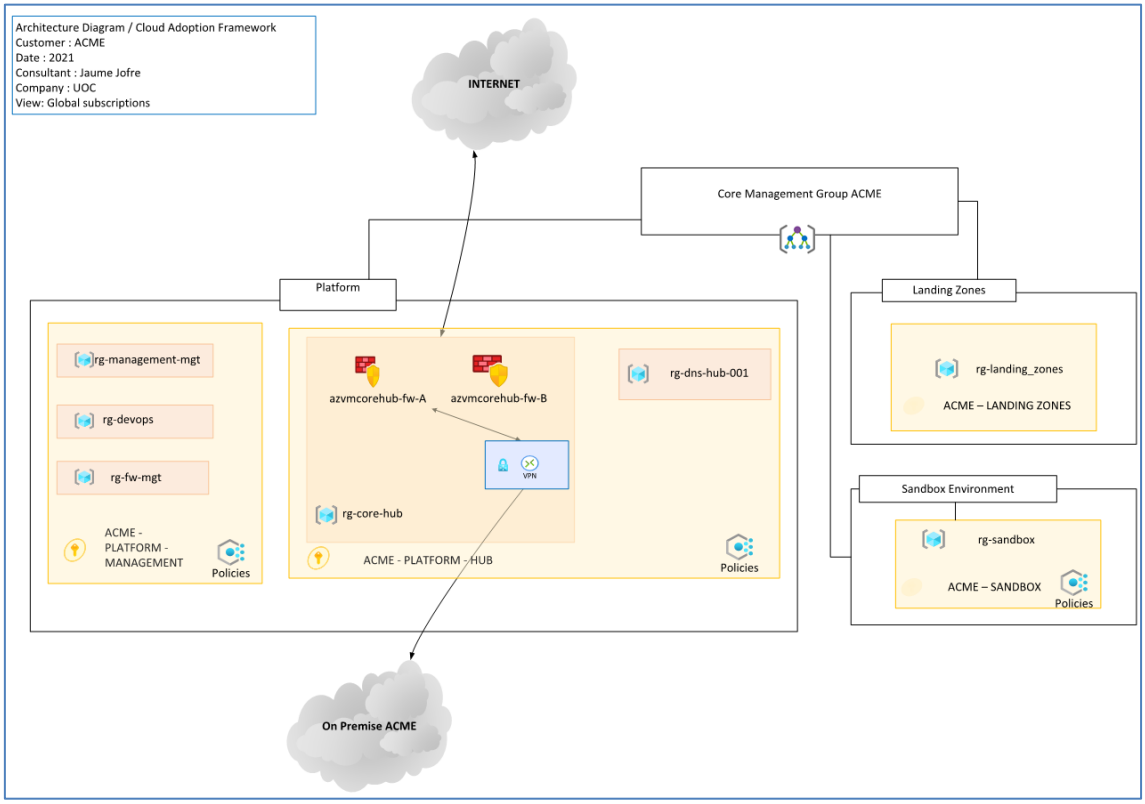


Figura 5 Visió global

2.2. Visió detallada

Observant la figura 5, el lector podrà veure un esquema més detallat dels diferents components de la infraestructura. Els punts 2.3 i 2.4 només fan un zoom de la plataforma i les zones d'aterratge per poder facilitar-ne la lectura.

En el punt 2.5 s'entra en detall de cadascun dels components i es raona el per què del disseny escollit.

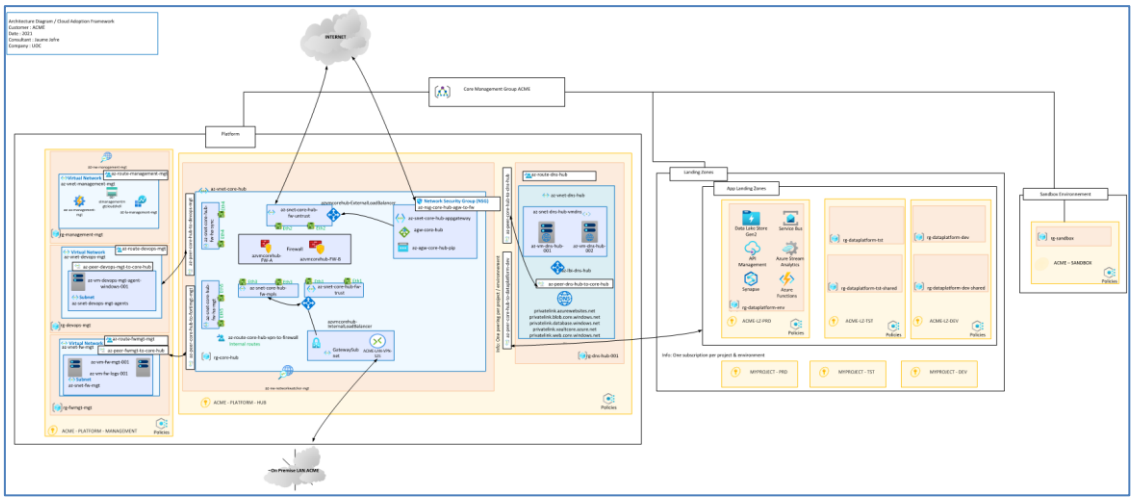


Figura 6 Vista completa de la infraestructura

2.3. Nucli i gestió

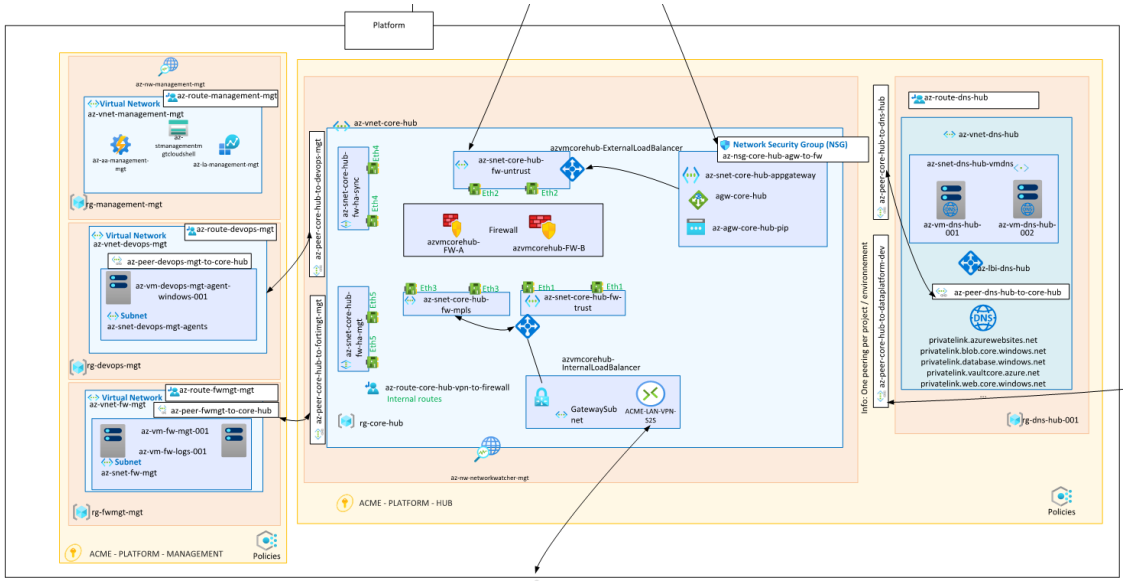


Figura 7 Zoom àrees nucli i gestió

2.4. Zones d'aterrada i entorn de proves

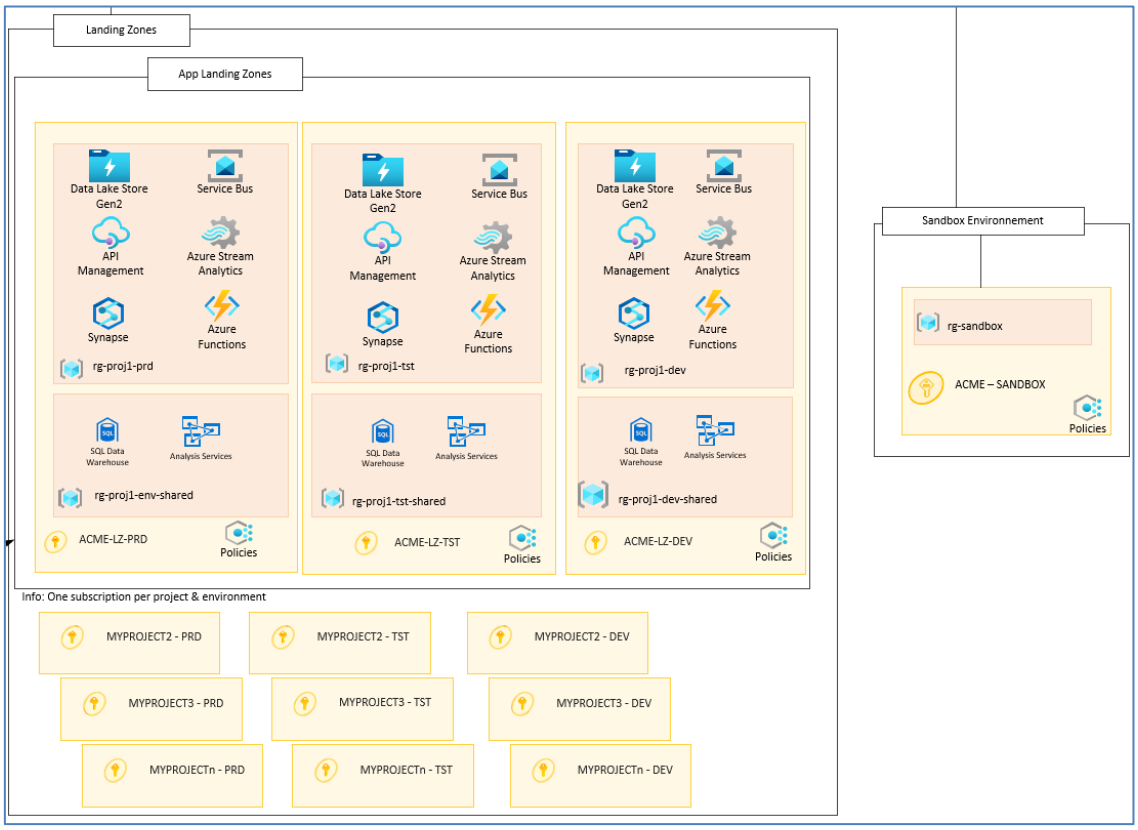


Figura 8 Zoom de les zones d'aterratge

2.5. Descripció

2.5.1. Organització jeràrquica

A cada un dels dissenys presentats des del punt d'2.1 al 2.4 es poden apreciar unes caixes etiquetades amb diferents sigles, per exemple *rg-* correspon a **grup de recursos** (*resource groups*), **subscripcions** identificades amb la icona d'una clau, i **grups d'administració**

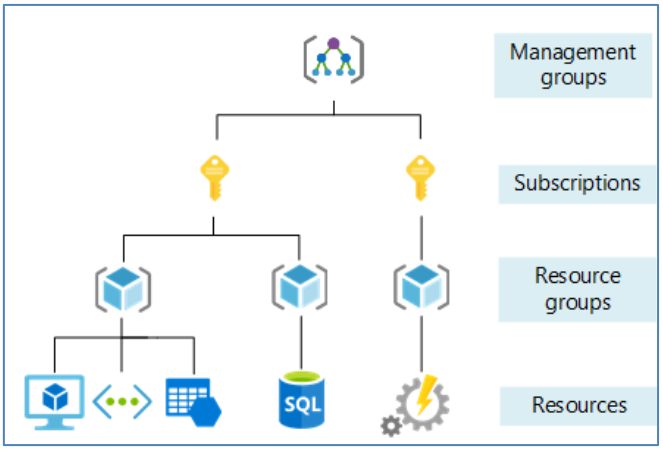


Figura 9 Jerarquia

(*Management Groups*) que són a la part més alta de la jerarquia. Es poden trobar les diferents icones i l'arbre de jerarquia a la figura 9.

ACME disposa d'un equip d'administradors de xarxa amb els privilegis necessaris per tal de gestionar tota la infraestructura, i a cadascun dels clients se'ls proporciona accés de lectura, per poder donar visibilitat dels recursos emprats per l'aplicació contractada i justificar així els costos dels recursos al núvol.

2.5.2. Subscripcions

A l'apartat 2 s'ha pogut observar un possible model teòric d'organització de la infraestructura al núvol d'Azure. A l'esquema, el primer que cal veure es la divisió de la infraestructura en plataforma, zones d'aterratge o *landing zones* i zona de proves o *sandbox.* La primera correspon a l'àrea de gestió i les segones són les que ACME farà servir per implementar els diferents serveis o aplicacions que vulgui hostatjar.

Les següents subscripcions són les unitats de facturació que es defineixen a Azure i que permeten als gestors agrupar els diferents recursos, aplicar polítiques i gestionar el control d'accés individualment per cadascuna d'elles. Entrant al detall de cadascuna d'elles, trobem:

- Plataforma de gestió - *Platform Management*
    - Administració general: inclourà aquells recursos necessaris per l'administració de totes les subscripcions que conformen la infraestructura, com per exemple, comptes d'emmagatzematge (*Storage Account*) o comptes d'automatització (*Automation Account*) per tasques de gestió i monitorització.
    - FW management: per la gestió des d'una consola única de tots els nodes FW desplegats per ACME.
    - DevOPS management: màquina virtual amb agents DevOPS pel desplegament de codi a les subscripcions d'aterratge. La

connectivitat es farà amb Noms de Servei Principals (SPN - *Service Principal Name*) per cada aplicació i cada entorn.

- Plataforma nucli - *Platform Hub*:
  - Màquines virtuals per hostatjar els nodes FW.
  - Balancejadors de càrrega entre zones.
  - Servei d'intercanvi (*peering service*) que fan la funció de connectors entre subscripcions.
  - Màquina virtual per la publicació dels serveis DNS al núvol.
- Zones d'aterratge - *Landing Zones*:
  - Projecte 1 Producció
    - Cada un d'aquests nodes pot incloure diferents components basant-se en quin projecte estan assignats. Per exemple, pot ser necessari un *DataLake* per l'emmagatzematge massiu de dades no relacionals, un motor de base de dades com MariaDB o SQLServer, components de PowerBI, etc...
  - Projecte 1 Desenvolupament
  - Projecte 1 Test
  - Projecte 2 Producció
  - Projecte 2 Desenvolupament
  - Projecte 2 Test
  - ...
  - Projecte n Producció
  - Projecte n Desenvolupament
  - Projecte n Test
- Banc de proves – *Sandbox*
  - Pot incloure tot o res. Es recomana tenir rutines automàtiques d'eliminació i neteja del contingut per minimitzar els costos que pugui generar.

Al punt 2.3 el lector pot observar el detall de les subscripcions Plataforma i nucli, mentre que la resta són visibles al punt 2.4.

En relació amb la divisió de subscripcions per projecte i entorns (producció, desenvolupament i test) a les zones d'aterratge, permet al propietari de la

infraestructura gestionar de forma independent els accessos, polítiques i costs associats a cada un d'ells. A més a més, les subscripcions com a tal no suposen cap cost recurrent al núvol d'Azure, sinó que el cost el genera el consum de recursos que es faci a cada una d'elles.

2.5.3. Components de seguretat

2.5.3.1. Dispositius de seguretat

Partint de la base que cal protegir cadascun dels elements de forma individual, per tal de proveir tota la infraestructura d'un nivell més alt de seguretat, ACME decideix adquirir un producte SaaS de tallafocs. La selecció escollida no és pertinent per aquesta memòria, hi ha una gran varietat de productes existents al mercat. Segons la consultora Gartner[8] algunes de les opcions existents són: CheckPoint, PaloAlto, Cisco, Sophos, Juniper, SonicWall, etc...

El disseny presentat proposa com a node central els dispositius de seguretat de tallafocs que fan de filtre entre les diferents zones:

- Gestió: connecta amb la subscripció de gestió per l'administració global de les diferents passarel·les amb funció de tallafocs. La xarxa complerta d'ACME està basada en un model SASE (*Secure Access Service Edge*) on les diferents seus del grup es connecten per SD-WAN entre elles, però això queda fora de l'àmbit d'aquest document.

- HA Sync: una *vnet* per la sincronització entre els dos nodes que treballen en mode actiu-passiu.

[8] Lloc web oficial Gartner - Network Firewalls Reviews and Ratings; Consultat: 20/09/2021
URL: https://www.gartner.com/reviews/market/network-firewalls

- Untrust: interfície de xarxa que connecta a Internet per la connexió de les diferents SD-WAN i habilita l'accés a les passarel·les. Aquesta mateixa interfície té un segon accés a Internet via un encaminador d'aplicació (*Application Gateway*) natiu d'Azure i un Grup de xarxa de Seguretat (NSG), que es presentarà més endavant.

- Trust: és l'enllaç amb les diferents zones d'aterratge (Landing Zones) on es publiquen les aplicacions web o serveis que proporciona la infraestructura.

- MPLS: interfície que protegeix la estructura física (on-premise) d'ACME.

2.5.3.2. Balancejadors de càrrega

Les comunicacions entre els diferents nodes connectats als tallafocs estan prèviament connectades als balancejadors de càrrega (*Load Balancers*) que asseguren l'alta disponibilitat als nodes de xarxa que els componen.

Qualsevol recurs publicat al núvol d'Azure disposa d'una alta disponibilitat garantida pel nivell de servei contractat (SLA - *Service Level Agreement*), però per tal de proporcionar-la cal que hi hagi un dispositiu virtual que detecti si algun dels nodes està fora de servei i en distribueixi el tràfic. A més d'aquesta funció, els balancejadors de càrrega aporten les següents funcionalitats[9]:

- **Simplificar l'equilibri de càrrega entre aplicacions:** amb l'equilibri de càrrega de les aplicacions, integrat pels serveis en el núvol i les màquines virtuals, es poden crear aplicacions escalables i d'alta disponibilitat en qüestió de minuts. Azure Load Balancer admet protocols basats en TCP /

[9] Lloc web oficial Microsoft Azure - Load Balancer; Visitat a: 20/09/2021; URL: https://azure.microsoft.com/es-es/services/load-balancer/

UDP, com HTTP, HTTPS i SMTP, així com protocols utilitzats per a aplicacions de missatgeria de vídeo i veu en temps real.

- **Alta disponibilitat i rendiment sòlid per a les aplicacions:** s'adapta automàticament al creixent trànsit de les aplicacions. Les aplicacions proporcionen una millor experiència de client sense necessitat de tornar a configurar el Load Balancer.

- **Equilibrador de càrrega intern:** utilitza l'equilibrador de càrrega intern pel trànsit entre màquines virtuals dins les seves xarxes virtuals privades o per crear aplicacions híbrides de diversos nivells.

- **Crear aplicacions molt fiables amb un front-end de difusió per proximitat (*anycast*) a escala mundial:** Load Balancer prova l'estat de les instàncies de l'aplicació, pren automàticament les instàncies incorrectes de rotació i les reinstal·la quan tornen a ser correctes. Es pot utilitzar l'equilibri de càrrega global que ofereix per distribuir el trànsit en funció de la latència entre diverses implementacions regionals, o bé, utilitzar-lo per millorar el temps d'activitat de les aplicacions amb redundància regional.

- **Protecció de les xarxes:** controla el tràfic de xarxa intern i extern i protegeix les xarxes privades mitjançant traducció d'adreces de xarxa integrada (NAT). Permet protegir la xarxa i integrar grups de seguretat de xarxa.

- **Ampliar abast amb IPv6:** habilita la connectivitat d'Internet IPv6 amb equilibri de càrrega fins als punts de connexió IPv6 nadius en Azure Virtual Machines. Els punts de connexió de doble pila nadius ajuden a complir els requisits normatius i solucionar el creixent nombre de dispositius en mercats mòbils i de IOT que busquen connectar-se als serveis basats en Azure.

2.5.3.3. Pla de protecció contra la denegació de servei

Conegut per l'acrònim *DDoS Protection*. A Azure en trobem dues versions: la bàsica, que està inclosa per defecte en qualsevol component que es desplega a la infraestructura, i la estàndard.

Feature	DDoS Protection Basic	DDoS Protection Standard
Active traffic monitoring & always on detection	●	●
Automatic attack mitigations	●	●
Availability guarantee		●
Cost Protection		●
Mitigation policies tuned to customers application		●
Metrics & alerts		●
Mitigation reports		●
Mitigation flow logs		●
DDoS rapid response support		●

Figura 10 DDoS comparativa[10]

En el cas de l'organització fictícia ACME es contracta i activa la versió estàndard per proveir el SOC de major visibilitat en la interfície pública del núvol.

2.5.3.4. Grup seguretat de xarxa - NSG

En relació amb la part exposada de la xarxa a internet és possible protegir el balancejador de càrrega amb un grup de seguretat a la xarxa o NSG (*Network Security Gro*up).

És possible fer servir NSG per filtrar el trànsit a una xarxa virtual d'Azure. Un grup de seguretat de xarxa conté regles de seguretat que permeten o deneguen el trànsit de xarxa entrant o el trànsit de xarxa de sortida de

[10] Lloc web oficial Microsoft Docs; Data edició: 09/09/2020; Data consulta: 25/09/2021
URL: https://docs.microsoft.com/en-us/azure/ddos-protection/ddos-protection-overview

diversos tipus de recursos d'Azure. Per a cada regla, és possible especificar l'origen i el destí, el port i el protocol, fent les funcions de tallafocs de nivell filtrat de paquets.

A l'exemple que presenta la figura 11, es pot veure com és possible habilitar l'accés pel port TCP 80 (tràfic HTTP) fent servir NSG.

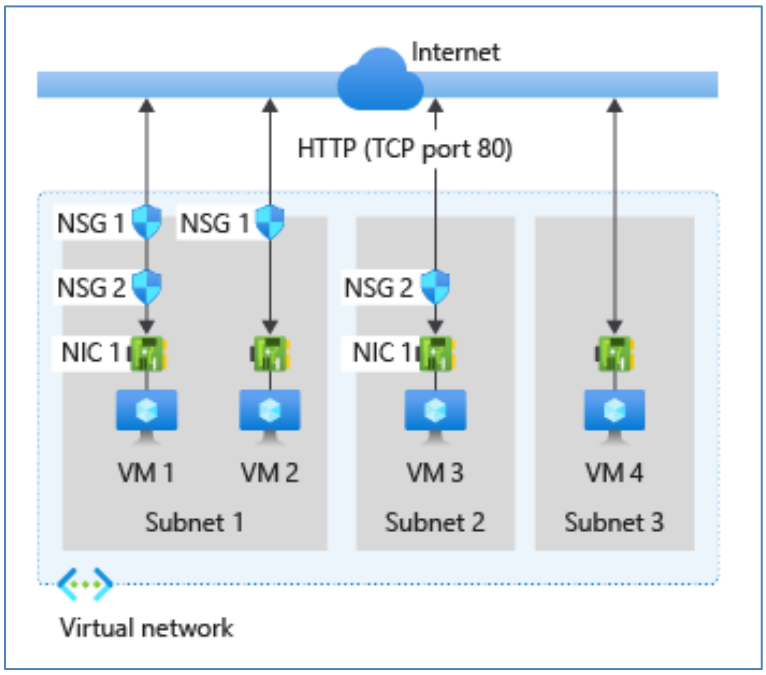


Figura 11 NSG

Per defecte els NSG[11] incorporen la regla DenyAllInbound (denegar tot el tràfic entrant), així doncs, per permetre qualsevol tràfic cal configurar-ho explícitament.

Per tal que VM1 pugui rebre el tràfic entrant, tant NSG1 com NSG2 han d'incorporar una regla que l'habiliti.

Quant al tràfic sortint, existeix AllowInternetOutbound (permetre tot el sortint) per defecte a tots els NSG, així doncs, no cal afegir una regla específica per permetre l'accés a webs des de les diferents VMs.

Per últim, és important saber que els NSG també afecten el tràfic entre VM dins la mateixa vnet (Virtual Network), i si una regla del NSG bloqueja el tràfic cap a Internet també ho farà entre VMs.

[11] Web oficial Microsoft Docs – Azure NSG; Data modificació: 24/08/2020; Data consulta: 25/09/2021
URL: Network security group - how it works | Microsoft Docs

3. Presentació model teòric d'un SOC

3.1. Introducció

Com que la funció central del SOC (*Security Operations Center*), que es descriurà en aquest punt, és limitarà a monitoritzar la seguretat de la xarxa i un sistema informàtic al núvol, només es descriuran les tecnologies de seguretat necessàries a desplegar per donar servei a aquest entorn. Un SOC pot fer ús de multitud d'utilitats i eines diferents, però moltes d'elles no seran presents en l'àmbit d'aquest projecte i s'ometran.

3.2. Organigrama

Des d'un punt de vista organitzatiu podem trobar tres tipologies de SOC: Distribuït, mixt i físic.

En el supòsit d'una organització distribuïda, el client subcontracte els serveis de monitoratge i control dels recursos completament a un tercer. Per contra, en el disseny organitzatiu físic, és el client qui disposa dels recursos suficients per gestionar el seu propi SOC, proveint un servei a temps complert tipus 24x7. Per últim, un sistema mixt serà aquell on trobarem que algunes de les funcions es duen a terme amb els recursos de l'empresa i d'altres es subcontracten.

Quant al projecte que aquest document presenta, el model escollit serà el distribuït ja que ACME arrendarà completament els serveis del SOC a un tercer per monitorar, detectar i prevenir els diferents riscos de seguretat que es puguin produir a la plataforma del núvol.

En el cas presentat, el SOC disposarà de tres nivells d'especialització en el personal:

- Nivell 1: format pels analistes encarregats del monitoratge i l'activació d'alertes en cas de trobar alguna anomalia en la informació rebuda.

- Nivell 2: hi pertanyen aquells analistes que realitzaran les auditories dels incidents detectats, acotant els possibles serveis i dades afectades i recomanant la resposta adequada a aplicar per cada cas.

- Nivell 3: on es trobaran els analistes més qualificats i amb un nivell més alt de titulació que s'ocuparan de resoldre els incidents i aportar les solucions necessàries per prevenir-los.

Finalment, tenint cura de la gestió de l'equip, del pressupost i del disseny dels serveis oferts es trobaran les figures del supervisor del SOC i l'enginyer de seguretat, que seran els principals interlocutors entre el client ACME i el seu equip tècnic. A la il·lustració 12[12] trobem un exemple del que aquest punt planteja.

Figura 12 Exemple rols equip SOC

[12] TechTarget – Search Security; Visitat a: 25/09/2021
URL: https://searchsecurity.techtarget.com/definition/Security-Operations-Center-SOC

3.3. Serveis proporcionats pel SOC

La principal tasca de qualsevol SOC és la detecció i resolució d'incidents de seguretat. A la taula següent es presenta l'annex A.16 de la norma ISO2701 que tracta com s'han de gestionar els incidents de seguretat.

A.16 Gestió d'incidents de seguretat de la informació		
A.16.1 Gestió d'incidents de seguretat de la informació i millores		
Objectiu: Assegurar un enfocament coherent i eficaç per a la gestió d'incidents de seguretat de la informació, incloent-hi la comunicació d'esdeveniments de seguretat i debilitats.		
A.16.1.1	Responsabilitats i procediments control	S'han d'establir les responsabilitats i procediments de gestió per garantir una resposta ràpida, efectiva i adequada als incidents de seguretat de la informació.
A.16.1.2	Notificació dels esdeveniments de seguretat de la informació control	Els esdeveniments de seguretat de la informació s'han de notificar pels canals de gestió adequats el més aviat possible.
A.16.1.3	Notificació de punts febles de la seguretat control	Tots els empleats, contractistes, terceres parts usuàries dels sistemes i serveis d'informació han de ser obligats a anotar i notificar qualsevol punt feble que observin o que sospitin que hi hagi, en els sistemes o serveis.
A.16.1.4	Avaluació i decisió sobre els esdeveniments de seguretat de informació control	Els esdeveniments de seguretat de la informació han de ser avaluats i s'ha de decidir si es classifiquen com incidents de seguretat de la informació.
A.16.1.5	Resposta a incidents de	Els incidents de seguretat de la informació han de ser respostos d'acord amb els procediments documentats.

	seguretat de la informació control	
A.16.1.6	Aprenentatge dels incidents de seguretat de la informació control	El coneixement obtingut a partir de l'anàlisi i la resolució d'incidents de seguretat de la informació s'ha d'utilitzar per reduir la probabilitat o l'impacte dels incidents en el futur.
A.16.1.7	Recull d'evidències control	L'organització ha de definir i aplicar procediments per a la identificació recollida, adquisició i preservació de la informació que pot servir d'evidència.

Taula 2 ISO2701 Annex A.16

Així doncs, la ISO2701[13] (vigent amb data edició 2017-05-24) emmarca quines són les tasques a dur a terme. Es poden resumir en els següents punts:

- Comunicar els incidents.
- Alertar sobre els punts febles detectats.
- Avaluar els incidents de seguretat que es produeixin.
- Aplicar les correccions prèviament documentades als incidents.
- Crear una base de coneixement dels incidents detectats per minimitzar els nous possibles incidents.
- Recollida d'evidències.

L'arxiu amb el contingut complert de la norma el podem trobar a l'annex:

une-en_iso-iec_27001.pdf

Complementàriament, i per donar una visió més complerta de les tasques que ha de dur a terme un SOC, es presenta una infografia d'una de les companyies més importants en matèria de seguretat informàtica, la nord-americana

[13] Aenor lloc web oficial; Data consulta: 27/09/2021
URL: https://tienda.aenor.com/norma-une-en-iso-iec-27001-2017-n0058428

McAfee[14], que il·lustra les passes a dur a terme en l'anàlisi dels incidents de seguretat.

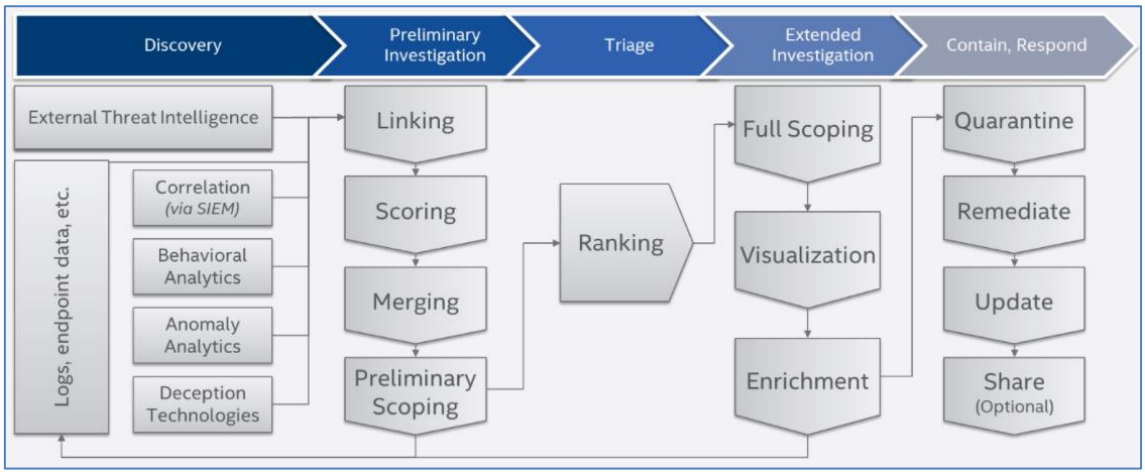


Figura 13 Fases anàlisis incidents

3.4. SIEM en un SOC

SIEM és l'acrònim de *Security Information and Event Management* que es pot traduir com a seguretat de la informació i gestió d'esdeveniments. De fet, està format per dos components: per una banda productes SEM (gestió d'esdeveniments de seguretat) i per l'altra SIM (gestió d'informació de seguretat). Els primers s'encarreguen de detectar patrons estranys d'accés i analitzar en temps real tot el que succeeix, mentre que els segons agrupen aquestes dades en un repositori central per ser explorades i generar informes per proporcionar informació que permeti prendre decisions als responsables del sistema.

Degut a l'augment d'incidents de seguretat arrel de la pandèmia i molts d'ells relacionats amb l'increment del teletreball, tal i com afirmen Lallie et al.[15], 2021, l'increment en l'ansietat causada per SARS Cov2 ha fet créixer la probabilitat que

[14] Lloc web oficial McAfee - What is a security operations center?; Data consulta: 27/09/2021
URL: https://www.mcafee.com/enterprise/es-es/security-awareness/operations/what-is-soc.html
[15] Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic; acceptat el 22 febrer 2021.

els ciberatacs resultin exitosos, traduint-se en una explosió en nombre i gamma dels mateixos.

Això fa que, ara més que abans de la pandèmia, les solucions SIEM siguin indispensables per la gestió de la seguretat de qualsevol empresa o entitat amb una certa complexitat a la seva infraestructura tecnològica.

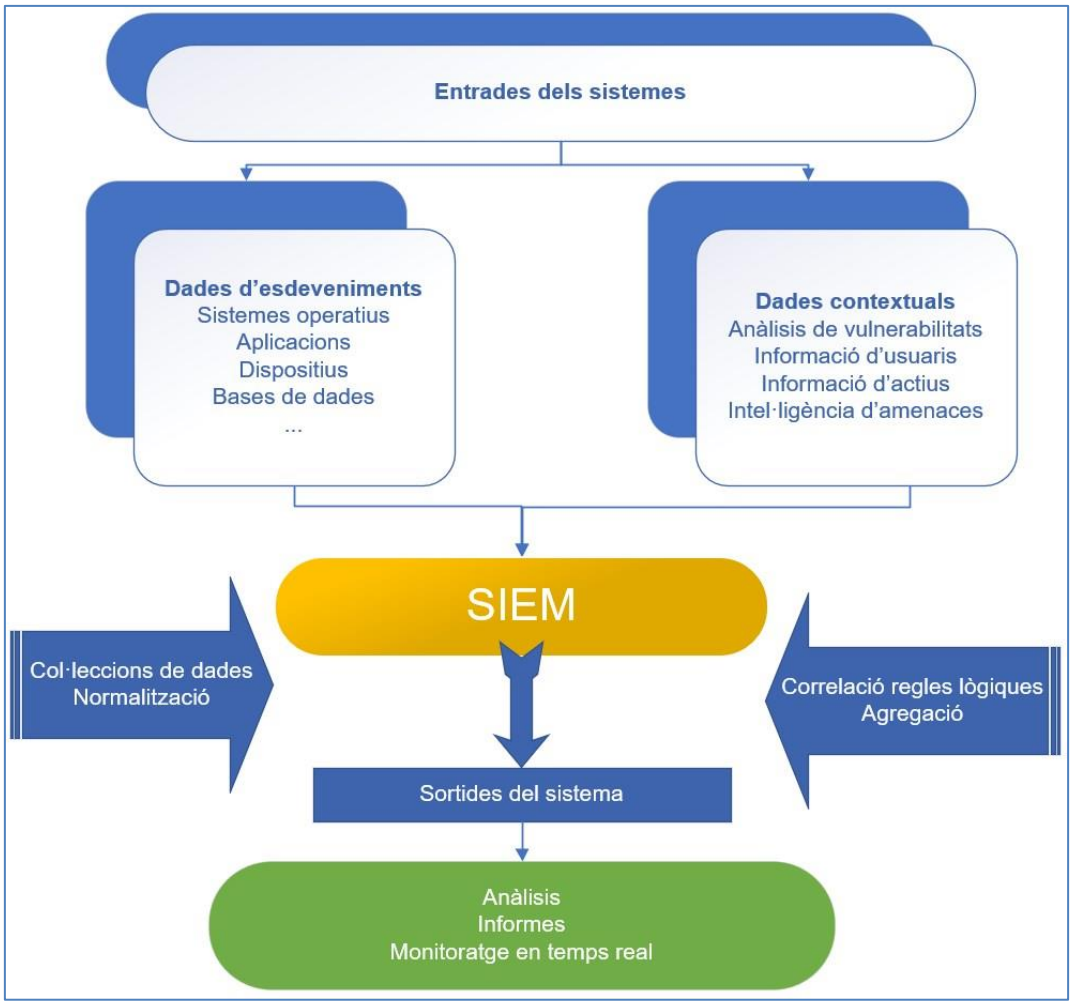


Figura 14 Arquitectura SIEM

Tal i com es mostra a la figura 14, per aconseguir l'objectiu final del SIEM es disposa d'entrades d'informació a partir dels esdeveniments que composen els diferents elements de l'arquitectura i, per altra banda, dades contextuals del entorn (usuaris, dispositius, etc.). És necessari dur a terme una classificació en col·leccions de dades, normalitzar-ne el contingut i, en base a sèries de correlacions de regles lògiques i operacions d'agregació, obtenir-ne les sortides pertinents.

Amb l'objectiu d'aconseguir gestionar les dades recollides, cal recordar que habitualment es tractarà de grans volums de dades, els SIEM disposen d'una gran varietat d'eines que n'unifiquen la gestió. Hi ha multitud de solucions al mercat de diferents fabricants que proporcionen aquestes funcionalitats, el quadrant màgic de Gartner presenta algunes dels fabricants líders al mercat.

Figura 15 Seguretat de la informació i gestió d'esdeveniments

3.5. SOAR en un SOC

L'acrònim SOAR correspon a l'orquestració de seguretat, automatització i resposta (*Security Orchestration, Automation and Response*). Consisteix en un conjunt d'eines que, com el seu nom indica, faciliten l'automatització de processos i milloren les operatives d'un SOC.

La clau per entendre el seu funcionament està en la automatització de processos, eliminant la intervenció humana allà on sigui possible, pel que cal una sèrie de procediments prèviament establerts o tasques recurrents per generar entrades d'informació de forma automatitzada.

Com tot sistema té una sèrie d'avantatges i inconvenients. Entre els primers està la capacitat d'automatització, l'augment de la productivitat derivat de l'automatització i alliberar al SOC de les tasques relatives a la operativa diària permetent que es centri en la cerca de les amenaces. Per altra banda, com a inconvenients, es pot mencionar el cost que serà més elevat, es requereix de programació i especialistes en el desenvolupament de codi per l'adaptació a cada cas concret o el temps de desplegament que sol ser més llarg.

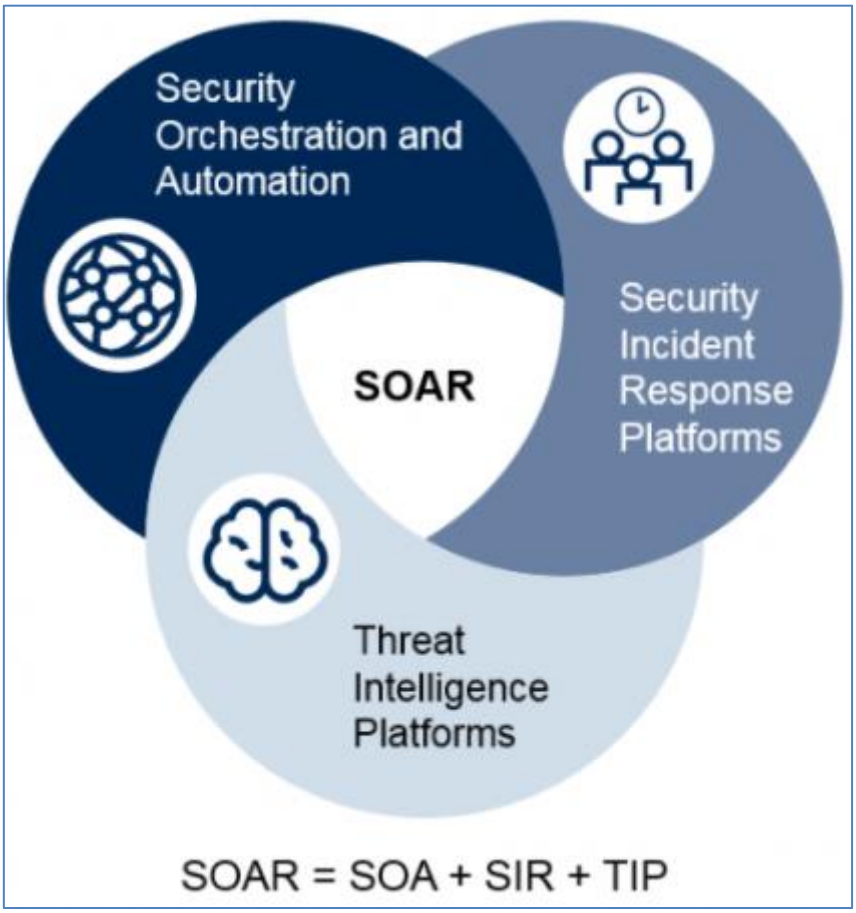


Figura 16 Gartner 2019 ID379047 - Tipus de SOAR

Incidint en cadascun dels tres components que formen el SOAR[16], hi ha:

Security Orchestation: possibilitat de coordinar eines de seguretat i altres tipus de tecnologies, que no han de ser necessàriament de seguretat, que normalment s'usen de forma independent, fins i tot de diferents fabricants, perquè s'integrin i comuniquin per establir un flux de treball de resposta a incidents efectius, eficients però sobretot iterables.

Security Automation: mètode d'automatitzar tasques i processos manuals, és a dir, sense la intervenció humana. En aquest punt és molt comú l'ús del terme *playbooks* que no són més que tasques lineals o passos que contenen accions bàsiques basades en condicionals.

Security Response: amb la consolidació de l'orquestració i l'automatització, la presa d'accions específiques com ara col·locar en quarantena una estació de treball, bloquejar una adreça IP, deshabilitar un compte d'usuari, etc. es redueix dràsticament el temps mitjà de resposta.

En resum, utilitzar SOAR dins d'una estratègia de seguretat, permet:

- Minimitzar el risc com a resultat a un incident de seguretat.
- Reduir el temps des que una escletxa és descoberta fins que es resol.
- Millorar l'efectivitat o l'eficiència de les operacions de seguretat o d'un programari.

Hi ha diverses solucions comercials disponibles al mercat per ajudar als SOC en la implementació del SOAR, però el quadrant màgic de Gartner mostrat per altres solucions com SIEM no està disponible pel SOAR i no és possible incloure una comparativa independent de les diferents solucions existents.

[16] Lloc web: LaSalle Blogging; Article: Que és un SOAR?;
Data publicació 20/05/2021; Data consulta: 06/12/2021;
URL: https://blogs.salleurl.edu/es/que-es-soar

4. Gestió dels recursos d'Azure

La plataforma de serveis al núvol de Microsoft Azure incorpora a la majoria de recursos que es poden usar a les subscripcions, opcions de monitoratge diferents depenent del recurs triat, la taula 3 mostra algunes d'elles.

Màquina virtual (*Virtual Machine*) Servidor virtual que pot ser de sistema operatiu Windows (10 o 11, Server 2016, 2019, etc...) o Linux (Ubuntu, Centos, distros de PostgreSQL, etc.). És el recurs que inclou més opcions de monitorització.	Insights Alerts Metrics Diagnostic settings Logs Connection monitor (classic) Workbooks
Compte d'emmagatzematge (*Storage account*) Conté tots els objectes de dades d'Azure Storage: blobs, recursos compartits de fitxers, cues, taules i discos. El compte d'emmagatzematge proporciona un espai de noms únic per a les dades d'Azure Storage que és accessible des de qualsevol lloc del món mitjançant HTTP o HTTPS.	Insights Alerts Metrics Workbooks Diagnostic settings (preview) Logs (preview)
Xarxes virtuals (*Virtual networks*) Proporciona un entorn aïllat i altament segur per executar les màquines i aplicacions virtuals.	Alerts Metrics Diagnostic settings Logs Connection monitor (classic) Diagram
Interfície de xarxa (*Network Interface*) Una interconnexió entre una màquina virtual i la xarxa de programari subjacent.	Alerts Metrics Diagnostic settings

Zona privada DNS (*Private DNS Zone*)	Alerts Metrics
SQL Server	Logs
Bases de dades SQL & Fàbrica de dades (*SQL Database & Data Factory*) Gestor de bases de dades natiu de Microsoft i serveis ETL al núvol per a la integració de dades sense servidor i la transformació de dades a escala.	Alerts Metrics Diagnostic settings Logs

Taula 3 Eines monitorització per recurs a Azure

En els següents apartats es revisarà les característiques principals de les eines de monitorització a Azure inclosos els diferents recursos.

Abans que res, cal apuntar que la documentació oficial existent sobre totes aquestes eines és molt complerta i està disponible per tothom, sense necessitat de disposar d'un compte d'accés. Per exemple, el document "Supervisió de màquines virtuals d'Azure amb Azure Monitor" explica en detall totes les dades que es poden recollir d'una màquina virtual en execució a Azure i revisa totes les eines existents. Als punts següents se'n fa un petit resum de cadascuna d'elles.

4.1. Estadístiques (*Insights*)

VM Insights supervisa el rendiment i l'estat de les màquines virtuals inclosos els processos en execució i les dependències d'altres recursos. Ajuda a oferir un rendiment predictible i la disponibilitat de les aplicacions, identificant els colls d'ampolla de rendiment i els problemes de xarxa, així com ajudar a comprendre si un problema està relacionat amb altres dependències.

4.2. Alertes (Alerts)

Aquesta és l'eina que permet definir regles d'alerta pels objectes a Azure. L'usuari d'Azure disposa d'una consola centralitzada d'alertes on pot veure si alguna de les que té definides s'han activat o revisar les que té creades.

Cada alerta que es defineix té un cost mensual fix, independentment del nombre de vegades que s'executa, però depenent de la complexitat en la definició de l'alerta (es poden definir llindars estàtics o dinàmics) aquest cost varia entre 0,10$/mes o 1,50$/mes. Això es pot verificar amb la calculadora de costs d'Azure[17].

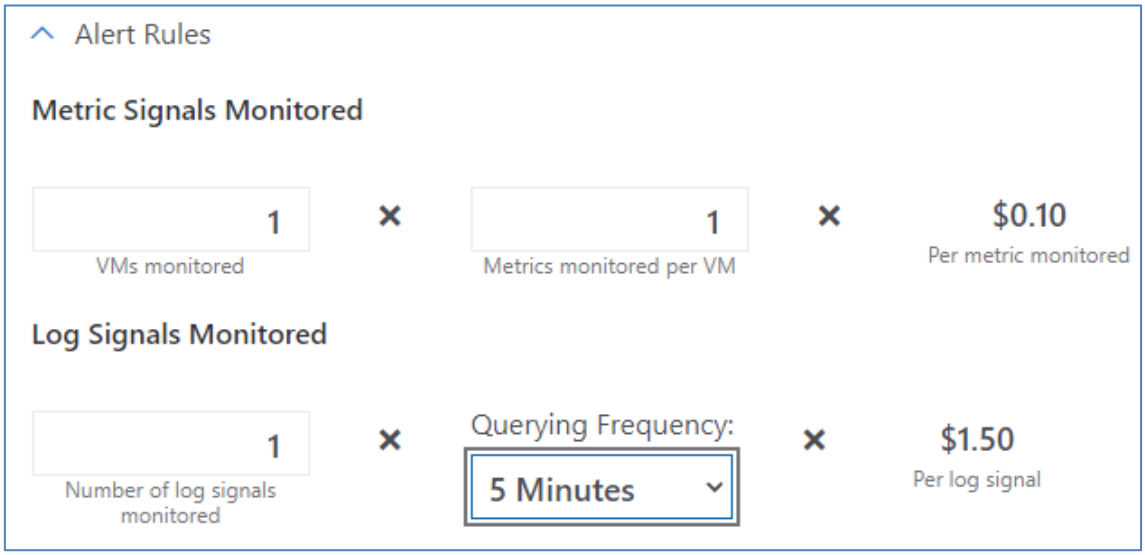


Figura 17 Calculadora Azure

A més, per cada alerta és possible assignar grups d'accions que poden incloure tant notificacions via correu electrònic, SMS o trucada telefònica, com accions prèviament definides per Azure.

Aquestes són:

- Automation runbook: reiniciar VM, aturar-la, redimensionar-la augmentant o disminuint recursos, o eliminar-la.
- Azure Function: permetre definir accions a realitzar sobre el recurs amb codi Visual Basic.
- ITSM: crear un tiquet automàtic a la plataforma de control d'incidències que hi hagi definida.
- Logic App: associar flux de treball automatitzats que integrin aplicacions, dades, serveis i sistemes.

[17] Azure pàgina oficial - Calculadora de preus; Consultat a 10/10/2021;
URL: https://azure.microsoft.com/en-us/pricing/calculator

- Secure Webhook: enviar notificacions API HTTP autenticant amb *AAD*.
- Webhook: enviar notificacions a una API HTTP sense autenticar.
- EventHub: enviar missatges al concentrador de esdeveniments.

4.3. Mètriques (Metrics)

L'eina de mètriques ens permet visualitzar de forma gràfica els diferents valors de consum dels recursos del sistema. Per exemple, en el cas d'una màquina virtual permetrà obtenir dades sobre l'ús del disc, consum de memòria, tràfic de xarxa, etc.

A més, ofereix diferents tipus de representacions gràfiques de les dades, descarrega les dades per ser tractades amb un full de càlcul o creació de regles associades a les dades mostrades.

4.4. Paràmetres de diagnòstic (Diagnostic Settings)

Per defecte, Azure només fa recull de mètriques a nivell de host com, per exemple: CPU, disc, xarxa, etc... Si es vol recollir altre tipus de registres, hi ha l'opció d'instal·lar un agent al recurs que permeti obtenir més informació com els comptadors de rendiment, registres, bolcats de memòria en cas d'error, pics d'ús o metadades del propi agent.

Un altre exemple seria el cas d'un adaptador de xarxa on ens permetria comprendre quins fluxos de trànsit s'acceptaran o es denegaran, juntament amb informació detallada per a la depuració.

4.5. Registres (Logs)

Tots els recursos que inclouen la opció de Logs disposen d'una consola on executar consultes amb el llenguatge Kusto (KQL)[18] per obtenir informació detallada a demanda de l'usuari. A grans trets, les consultes Kusto fan servir

[18] Lloc oficial Microsoft Docs; Introducció a les consultes Custo; Data consulta 10/10/2021
URL: https://docs.microsoft.com/es-es/azure/data-explorer/kusto/query/

entitats d'esquema organitzades en una jerarquia similar a les de les bases de dades, taules i columnes de SQL. La sentència consta d'una seqüència d'instruccions de consulta delimitades per un punt i coma (;) i al menys una d'elles és una instrucció d'expressions tabulars, que genera dades organitzades en una malla tabular de columnes i files.

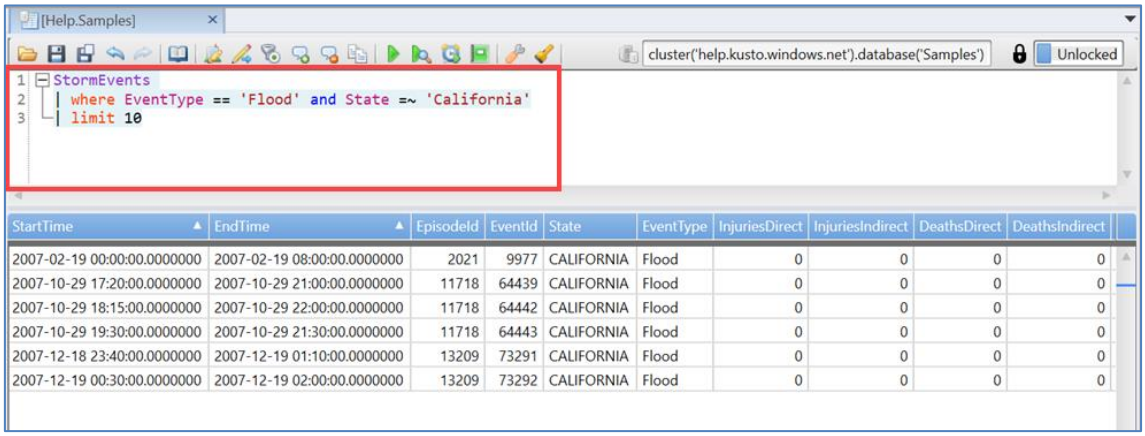


Figura 18 Exemple consulta Kusto

Una de les grans avantatges que proporciona *Log Analytics* és la quantitat de consultes prefabricades existents i disponibles per l'usuari. Si no es troba la consulta exacte que retorni les dades cercades, segurament és possible trobar alguna similar, que amb petits retocs, permeti obtenir el resultat esperat. A més, existeix una gran comunitat "Azure Monitor" a *Github* amb consultes ja desenvolupades i compartides pels membres de la comunitat.

4.6. Llibres de treball (Workbooks)

Tal i com estan descrits, a la documentació oficial d'Azure[19], proporcionen un llenç flexible per a l'anàlisi de dades i la creació d'informes visuals complets al portal d'Azure. Permeten accedir a diversos orígens de dades des d'Azure i combinar-los en experiències interactives unificades.

En altres paraules, habiliten a l'usuari la creació de punts d'accés únics per la consulta de diferents anàlisis mètriques o alertes definides per un recurs.

[19] Lloc oficial Microsoft Docs – Llibres d'Azure Monitor; data consulta 11/10/2021;
URL: https://docs.microsoft.com/es-es/azure/azure-monitor/visualize/workbooks-overview

4.7. Monitor de connexions (Connection Monitor)

D'una forma molt senzilla, el monitor de connexions permet, pel recurs seleccionat, veure les dades (IP origen i port, IP destí i port, estat de la connexió, interval en segons), de les connexions actives.

Aquesta funcionalitat ha sigut discontinuada des de l'1 de juliol de 2021 permeten els usuaris seguint fent ús dels monitors de connexió existents creats prèviament a aquesta data, però recomanant la migració a la nova solució Azure Network Watcher.

Network Watcher apareix configurat de forma automàtica per cada subscripció activa existent. A més de proporcionar les funcionalitats de monitorització abans llistades pel monitor de connexions incorpora altres utilitats com:

- Verificació flux IP (IP flow verify): comprovar si un paquet està permès o denegat, donades IPs i ports d'origen i destí.

- Diagnòstics Grup Seguretat de xarxa (NSG Diagnostic): retornar totes les regles aplicades per un tràfic definit, de nou per IPs i ports d'origen i destí.

- Salt següent (Next hop): retornar la següent IP a assolir per una connexió. El símil a nivell de sistema operatiu Windows seria el `tracert` o en Linux el `traceroute`.

- Regle de seguretat efectiva (Effective Securiy rule): per cada dispositiu de xarxa virtual es pot assignar un o més grups de seguretat de xarxa, el que pot provocar que sigui una mica complex esbrinar quines restriccions hi ha aplicades. Amb aquesta utilitat podem veure què hi ha aplicat.

- Solució problemes Xarxa Privada Virtual (VPN trobleshoot): proporcionar una eina de test que retorni un diagnòstic complert d'una connexió VPN establerta entre Azure i una xarxa local.

- Capturador de paquets (Packet capture): tal i com es podria fer amb utilitats com *WireShark*, permetrà capturar d'una forma molt limitada, ja que no es poden aplicar filtres, el tràfic que travessa una connexió de xarxa.

- Solució problemes de connexió (Connection trobleshoot): obtenir un diagnòstic de connectivitat entre IPs donat un protocol (TCP o ICMP) i un servei seleccionat.

5. Orígens de la informació per recurs

Arribats a aquest punt, el lector es pot preguntar si, ja disposant d'una sèrie d'eines natives a Azure pel monitoratge de la plataforma, hi ha necessitat real de cercar eines alternatives o serveis externs.

Primer cal analitzar la complexitat de la infraestructura a monitoritzar. Si els serveis SaaS contractats al núvol d'Azure resideixen en una única subscripció i són molt reduïts quant a quantitat i ús, les eines natives d'Azure poden ser suficients. Cal tenir present que Microsoft ja incorpora per les seves solucions al núvol, Azure Monitor que engloba els serveis de monitoratge, alertes, control, etc.

Com s'ha definit en el capítol 1 d'aquesta memòria, el model d'empresa fictícia d'exemple ACME estableix un disseny complex de diferents subscripcions, amb previsió de creixement a mesura que s'incorporin nous clients. Això convida a cercar solucions globals que centralitzin el control de la infraestructura, a més, en el cas teòric que s'està plantejant es volen subcontractar completament tots els serveis de SOC.

Així doncs, en aquest apartat s'establirà que cal fer, donats els recursos definits per l'empresa fictícia ACME i donat els serveis que ofereix el SOC fictici descrit al capítol 3 d'aquesta memòria, per posar en funcionament aquesta delegació de serveis de seguretat.

Els subapartats següents presentaran per cadascun dels recursos (tallafocs, xarxes, màquines virtuals, gestors de bases de dades, etc.) quines seran les mètriques, els registres i els protocols usats per la recollida de dades que durà a terme el SOC i com cal configurar aquests enviaments. Prèviament es descriuran dues eines bàsiques per gestionar les transferències d'informació: l'SNMP i el SysLog.

5.1. Protocol SNMP

El Protocol simple d'administració de xarxa o SNMP (*Simple Network Management Protocol*) és un protocol de la capa d'aplicació de la pila TCP/IP que facilita l'intercanvi d'informació d'administració entre dispositius de xarxa.

SNMP permet als administradors supervisar el funcionament de la xarxa, cercar i resoldre els seus problemes i planificar el seu creixement[20].

Basat en els estàndards RFC 1157 (SNMP, 1990) i RFC 3410 (SNMPv3, 2002), actualment la versió del protocol més segura és la v3 ja que inclou opcions d'autenticació i privacitat. Tot i així, la versió que encara segueix sent més usada és la v2.

Tot i que queda fora de l'àmbit d'aquesta memòria, per entendre mínimament com funciona el protocol cal saber que es composa de 3 elements bàsics: Sistemes Administrats de Xarxa (NMS), Dispositius Administrats on s'instal·len els agents i Agents que fan la funció d'aplicatius col·lectors d'informació.

Aquest intercanvi d'informació es fa usant Bases d'Informació de Gestió (MIB *Management Information Base*) i col·leccions d'informació que està organitzada jeràrquicament incloent Identificadors d'Objectes (OID *Objecte Identification*).

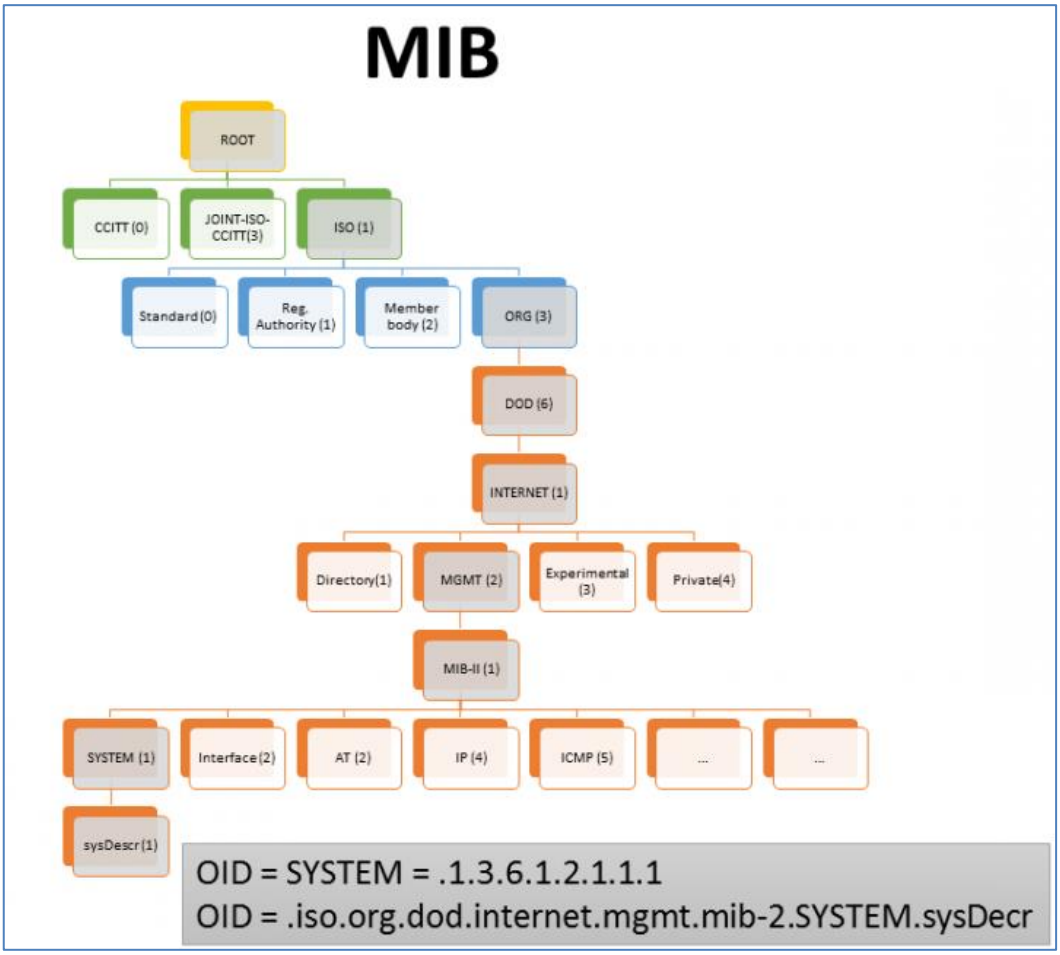


Figura 19 Esquema gràfic SNMP MIB (font Incibe)

[20] Wikipedia - Protocolo simple de administración de red; Data darrere actualització: 20/05/2021; URL: https://es.wikipedia.org/wiki/Protocolo_simple_de_administraci%C3%B3n_de_red

5.2. Serveis SYSLOG

A diferència del protocol SNMP revisat a l'apartat anterior, els serveis de Syslog inclouen tant el protocol que defineix el format de les transmissions com l'aplicació o biblioteca que envia els missatges de registre. Un missatge de registre sol tenir informació sobre la seguretat del sistema encara que pot contenir qualsevol informació. Juntament amb cada missatge s'inclou la data i l'hora d'enviament.

A la imatge[21] mostrada a continuació es pot veure esquemàticament els elements que composen Syslog i el RFC 5424 del *Network Working Group* que estableix els paràmetres i comportaments del protocol.

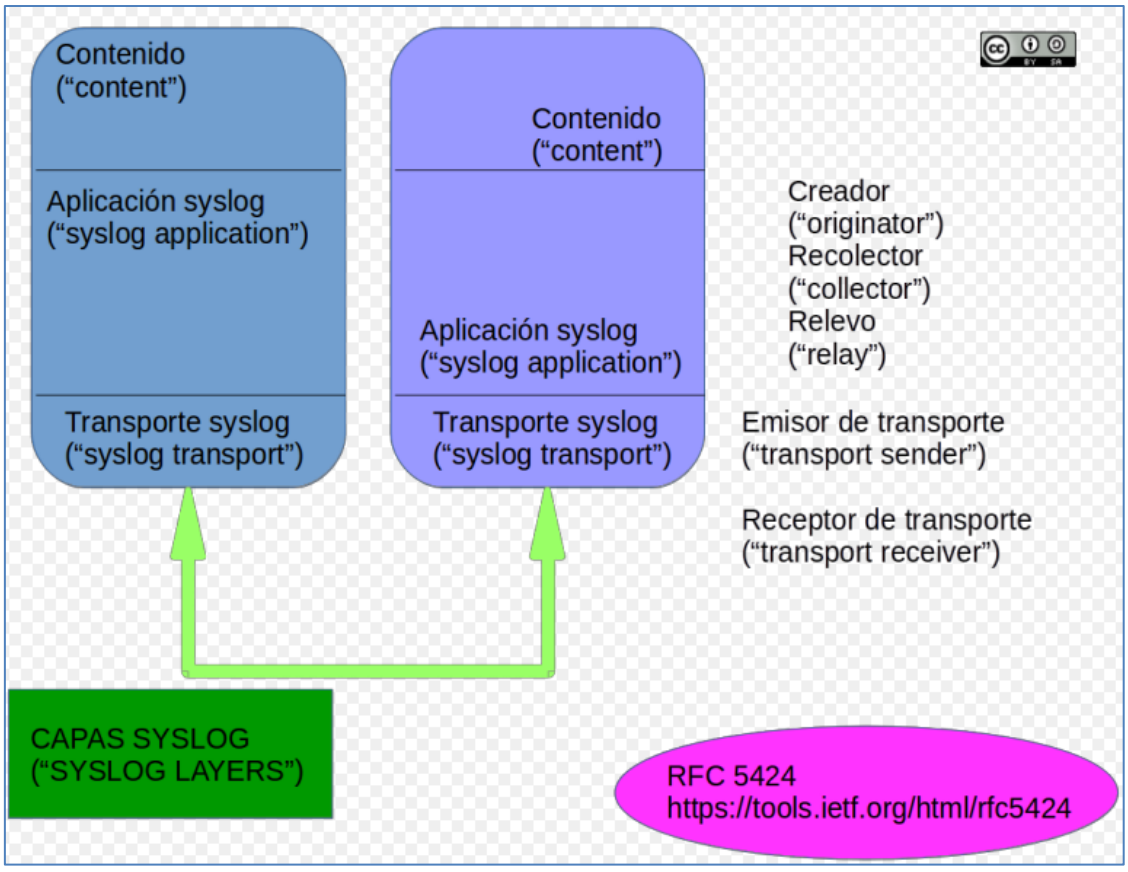


Figura 20 Descripció Syslog

Fent ús de Syslog podem recuperar, no només informació de l'estat dels dispositius sinó, registres d'aplicació encapsulats dins paquets syslog amb tot el contingut original dels mateixos. Un clar exemple d'ús són els registres de tràfic que genera un sistema tallafocs.

[21] Pàgina oficial Wikipedia; entrada syslog; darrera edició 09/10/2021; https://es.wikipedia.org/wiki/Syslog#/media/Archivo:Syslog_layers_RFC5424.png

5.3. Cas d'ús SNMP i SYSLOG

Tal i com s'ha mencionat prèviament, un cas d'ús pel que fa els protocols d'enviament d'esdeveniments de seguretat són els tallafocs. En aquest tipus de dispositius trobem dos nivells de recol·lecció d'informació: SNMP per obtenir l'estat bàsic i Syslog que permetrà enviar al SIEM els esdeveniments que es registren.

En el cas de les dades SNMP els propis dispositius tallafocs habitualment incorporen plantilles d'autoconfiguració SNMP que estan disponibles per la descàrrega. A més, és habitual que permetin seleccionar els ports locals i remots per cadascuna de les 3 versions disponibles de configuració del protocol, així com els esdeveniments que es recolliran.

Per altre banda, els dispositius tallafocs, tant en les seves versions físiques com virtuals, tenen la capacitat d'enviar els registres generats a més d'un servidor syslog. Habitualment, a les seccions de gestió de registres apareix disponible l'opció d'activar el reenviament de tots els esdeveniments que genera el sistema a un syslog extern introduint l'adreça IP o el FQDN.

Evidentment, caldrà habilitar les regles de filtrat de tràfic necessàries per tal que els paquets HTTPS entre els dispositius i la URL de destí estiguin permeses.

5.4. Registres de seguretat als recursos d'Azure

Tal i com s'ha vist en els primers apartats de la memòria, les subscripcions d'Azure no només contenen serveis SaaS o PaaS sinó que també requereixen de tota una sèrie de recursos que donen suport a aquest serveis. Als següents punts es revisaran alguns d'ells i es proposaran casos d'ús dels paràmetres de seguretat a monitoritzar per prevenir o detectar possibles atacs, intrusions o vulnerabilitats.

5.4.1. Obtenció de registres de màquines virtuals

Quan el client ACME vulgui activar la monitorització de qualsevol màquina virtual publicada a les seves subscripcions d'Azure, tant si es tracta d'instal·lacions amb sistema operatiu Windows com si són Linux, disposarà de dues vies per recollir les mètriques d'ús de memòria, disc, processador i xarxa.

La primera opció es fer ús de l'API d'Azure, mentre que la segona consistirà en la instal·lació d'un agent específic pel producte usat com a SIEM per part del SOC.

- Fent servir API: caldrà habilitar l'accés de lectura del SIEM triat pel SOC al nostre compte d'Azure (*Tenant*). Per fer-ho, cal disposar d'Azure Active Directory, crear-hi un registre d'aplicació (App registrations) i introduir-ho com a cadena de connexió per recuperar tota la informació que generin les diferents màquines virtuals publicades.

Aquesta opció habilita la recol·lecció casi immediata de registres però potser concedeix un nivell de visibilitat de la infraestructura massa ampli, pel que ACME disposa de la segona opció.

- Instal·lar agent: des del portal Azure es navega a cadascuna de les màquines virtuals que es desitja monitoritzar i a la secció d'extensions s'hi afegeix entre les diverses que hi ha disponibles. L'assistent ens demanarà la clau API de connexió a la compte de l'aplicació seleccionada per part de l'empresa gestora del SOC, d'ús restringit a ACME.

Amb aquesta segona opció, el client disposa d'una major capacitat de filtratge dels recursos que vol monitoritzar i addicionalment obté un major nivell d'informació, ja que no només recupera les mètriques habituals sinó que afegeix dades de les aplicacions en execució a la màquina virtual, com per exemple SQL Server o el servidor de pàgines web Internet Information Server (IIS), per mencionar-ne dos.

5.4.2. Obtenció de registres serveis (*SaaS* o *PaaS*).

És possible que, a més de monitoritzar els dispositius de seguretat i les màquines virtuals, el client tingui interès en que el SOC reculli dades dels diferents serveis SaaS desplegats a la infraestructura. Es revisarà algun d'ells a continuació i es descriurà com caldrà configurar l'enviament de registres en cada cas.

5.4.2.1. SaaS – SQL Server

SQL Server és el SGBD de Microsoft més reconegut i àmpliament estés a les infraestructures al núvol d'Azure. Permet emmagatzemar bases de dades relacionals i fer-ne una gestió complerta (còpies de seguretat, control d'accessos, auditoria, gestió d'índex, etc.).

Totes inclouen el prefix *azure.sql_servers_databases* i els paràmetres més comuns de monitorització a qualsevol instancia de SQL Server. La taula 4 en llista alguns exemples:

Mètrica	**Descripció**
cache_hit_percentage (mesura)	Percentatge d'accés a la memòria cau. S'aplica només als datawarehouse.
connection_failed (comptador)	Connexions fallides.
replication_links.count (mesura)	La quantitat d'enllaços de replicació per base de dades.
status (mesura)	Estat de les bases de dades d'Azure SQL.
storage (mesura)	Espai de dades utilitzat. No aplicable als magatzems de dades.

Taula 4 Mostra mesures monitor SQL Server

La llista és molt més extensa i susceptible de ser actualitzada ampliant el catàleg de possibles valors a monitoritzar, ja que és pràctica habitual dels diferents fabricants de programari millorar i ampliar les funcionalitats existents.

Els casos d'ús d'aquesta informació poden ser varis. Si el client Acme defineix els intervals acceptats com a vàlids per cadascuna de les mesures que es vol mantenir sota observació, el SOC fàcilment podrà definir alertes automatitzades seguint els criteris definits pel client. Serà habitual que el client estableixi diferents llistes de receptors de les alertes depenent dels horaris o del calendari de festius.

Per altra banda, també es pot donar el cas que Acme contracti serveis d'intervenció prèviament definits en detectar algun valor anormal. Per exemple, en cas d'esgotar l'espai disponible per l'arxiu de registre d'una base de dades (*storage*), es pot automatitzar l'ampliació del mateix des dels serveis contractats de SOC. Un altre cas d'ús podria consistir en detectar una quantitat anormal de connexions a la base de dades des d'una mateixa IP (*connection_failed*) o de rèpliques actives (*replication_links*), en aquest cas es podria indicar el SOC que cal bloquejar les IP d'origen ja que és susceptible de ser interpretat com un intent d'atac per injecció SQL.

Un dels casos d'ús més evidents, consistiria en monitoritzar l'estat (*status*) de la base de dades i, en cas de detectar-la fora de línia, realitzar les verificacions i accions corresponents per recuperar l'estat actiu l'abans possible. O, des del punt de vista de l'equip de desenvolupament, podria ser interessant definir un nivell de referència per detectar valors anormals d'accessos a memòria cau (*cache_hit_percentage*) indicant possibles dissenys erronis en les consultes que s'executen.

5.4.2.2. PaaS – Analysis Services

Azure Analysis Services és una plataforma com a servei (PaaS) totalment gestionada que proporciona models de dades de nivell empresarial al núvol.

Mètrica	**Descripció**
current_user_sessions (comptador)	Nombre actual de sessions d'usuari establertes.
memory_cleaner_current_price (comptador)	Preu actual de la memòria, $/byte/hora, normalitzat a 1000.
status	Estat d'Azure Analysis Services.
successfull_connections_per_sec	Percentatge de connexions finalitzades amb èxit. Es mostra com a connexió.

Taula 5 Mostra mesures monitor Analysis Services

Cal una tasca prèvia de definició per part del client de quins són els valors correctes esperats en el servei, per tal que el SOC pugui automatitzar la comprovació de les mètriques existents i generar les alertes adequades.

Un cas d'ús a aplicar pot ser monitoritzar un avís quan les connexions (*current_user_sessions*) superin un nombre que es consideri per sobre del màxim esperat, i preveure així possibles caigudes de rendiment per problemes de dimensionament del servei. També es poden definir valors màxims (*memory_cleaner_current_price*) del cost del servei per ser alertats en cas de sobrepassar l'estimat o, tal i com s'ha comentat en el cas de SQL Server, monitoritzar l'estat de servei (*status*) i definir les accions correctives en cas de rebre alerta d'estat incorrecte.

Per últim, destacar el paràmetre que ens permetrà saber amb antelació si les connexions entrants (*successfull_connections_per_sec*) al servei estan fallant més de l'esperat, anticipant així mancances en la disponibilitat dels serveis.

5.4.3. DataLake

Azure Data Lake permet emmagatzemar dades de qualsevol mida, forma i velocitat i fer tot tipus de processament i anàlisi.

Els espais d'emmagatzematge que proporciona DataLake poden ser monitoritzats recuperant els valors dels comptadors d'escriptura (*write_requests*) i lectura (*read_requests*) a l'espai, el que permetrà als administradors d'Acme tenir visibilitat de quin és l'ús que s'està fent dels magatzems de dades en tot moment. Aquesta informació també es pot enviar al SOC per tal de, donats uns paràmetres previs de llindars acceptables, poder generar l'alerta corresponent en cas de que no estiguin dins els marges.

5.4.4. Data Factory

Data Factory és el servei d'integració de dades sense servidor i totalment gestionat que integra visualment fonts de dades amb més de 90 connectors integrats sense manteniment ni cap cost afegit. Permet construir fàcilment processos ETL i ELT sense codi en un entorn intuïtiu a més de permetre desenvolupar codi personalitzat.

El primer cas d'ús serà monitoritzar l'estat (*status*) del servei, permetent que el SOC avisi al client instantàniament de qualsevol canvi. Es podrà mantenir un comptador (count) dels Data Factories existents o controlar els errors (*PipelineFailedRuns*) que generin els ETL en execució i SSIS (*SSISPackageExecutionFailed*) erronis.

5.4.5. Key Vault

És la solució que proporciona Azure com a servei al núvol per a l'emmagatzematge dels secrets i l'accés a aquests de forma segura. Un secret és tot allò que l'accés del qual es vol controlar de manera estricta. Per exemple: les claus API, les contrasenyes, els certificats o les claus criptogràfiques.

Així doncs, es tracta d'un component clau en la seguretat de la infraestructura que requereix poder ser auditat en qualsevol moment per revisar-ne els esdeveniments recents, així com afegir alertes de valors incorrectes de mètriques com disponibilitat, saturació del magatzem (*SaturationShoebox*) i nombre total de visites (*ServiceApiHit*).

Un cas d'ús molt evident podria ser avisar al SOC d'un accés no reconegut. Amb la següent sentència Kusto podem obtenir les IPs que accedeixen al nostre KeyVault i comunicar-ho al SOC regularment perquè comprovi si són o no autoritzades.

```
AzureDiagnostics
| where ResourceProvider =="MICROSOFT.KEYVAULT"
| summarize count() by CallerIPAddress
```

5.4.6. Application Gateway

Tal i com es pot veure a la següent figura[22], Application Gateway és un equilibrador de càrrega de trànsit web que permet administrar el trànsit a les aplicacions web. Els equilibradors de càrrega tradicionals operen a la capa de transport (OSI capa 4: TCP i UDP) i encaminen el trànsit en funció de l'adreça IP i port d'origen a una adreça IP i port de destinació.

En aquest cas, pot interessar monitoritzar les peticions fallides (*failed_requests*), ja que poden indicar possibles intents d'accés il·legítim per força bruta, o monitoritzar el comptador dels bloquejos realitzats pel tallafocs (*blocked_req_count*).

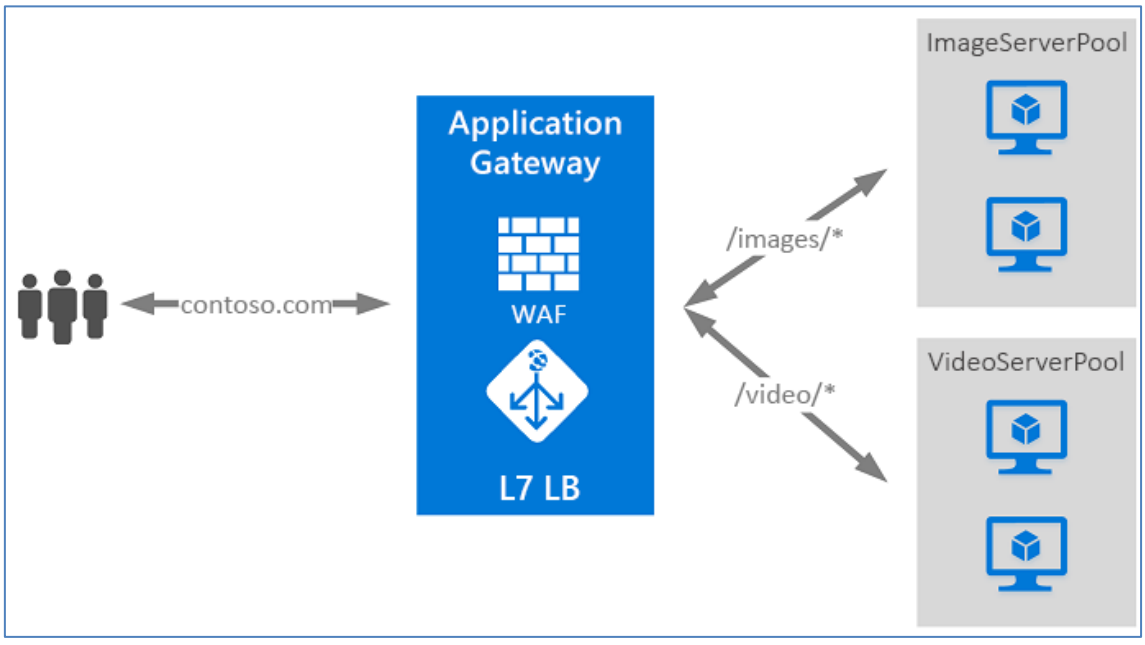


Figura 21 Application gateway

[22] Lloc web: Microsoft Docs; ¿Que es Azure Application Gateway?; data consulta 20/11/2021
URL: https://docs.microsoft.com/es-es/azure/application-gateway/overview

5.4.7. Container Service

Simplifica la implementació d'un clúster de Kubernetes administrat a Azure ja que descarrega la sobrecàrrega operativa a Azure. Com que és un servei de Kubernetes allotjat, Azure controla tasques crítiques com la supervisió de l'estat i el manteniment.

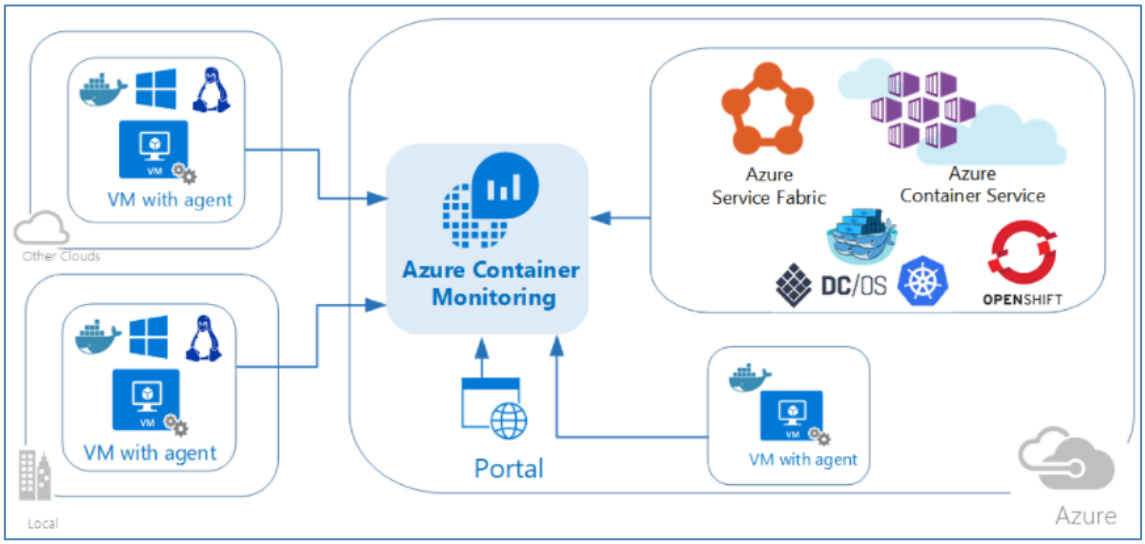


Figura 22 Monitorització de contenidors

El servei de monitoratge requereix de diferents instal·lacions de la solució desplegada per tal de disposar dels registres que generen a Azure Monitor. A la figura anterior a aquest paràgraf es mostrava l'esquema proposat per Microsoft[23] per la monitorització centralitzada dels serveis de contenidors. Depenent d'on estigui hostatjat el contenidor (Windows, diferents versions de Linux, etc.) caldrà instal·lar una versió diferent del Log Analytics Service executat en mode *Swarm*.

Això habilitarà la recollida de diferents mètriques cada 3 minuts. Per exemple, trobarem registres d'activitat (*ContainerLog*) o de servei (*ContainerServiceLog*), registre d'imatges disponibles (*ContainerImage Inventory*), etc.

De nou, tal i com s'ha apuntat en els punts anteriors, les dades per si soles no són susceptibles de generar alertes sinó es defineixen els límits acceptats com a vàlids o s'instrueix al SOC per detectar cadenes específiques d'errors dins dels registres generats.

[23] Lloc web: Microsoft Docs; Article: Container Monitoring solution in Azure Monitor; Data consulta: 20/11/2021; Darrere edició: 09/23/2021;
URL: https://docs.microsoft.com/en-us/azure/azure-monitor/containers/containers

5.4.8. Load Balancer

Opera a la capa 4 del model Interconnexió de sistemes oberts (OSI).

És l'únic punt d'accés disponible pels clients dels recursos als quals balanceja la càrrega.

Distribueix els fluxos de dades rebuts que arriben al frontend de l'equilibrador de càrrega a les instàncies del grup de backend, fent la funció de clúster distribuït de recursos.

Els balancejadors de càrrega[24] generen mètriques multidimensionals i alertes, així com estat de salut dels recursos. Una mètrica susceptible de ser monitoritzada i que generi alertes automàtiques, en cas de superar els llindars establerts, seria *Bytes Count,* o amb *TCP SYN packets* seria possible detectar atacs DDoS que estiguin succeint en un moment donat.

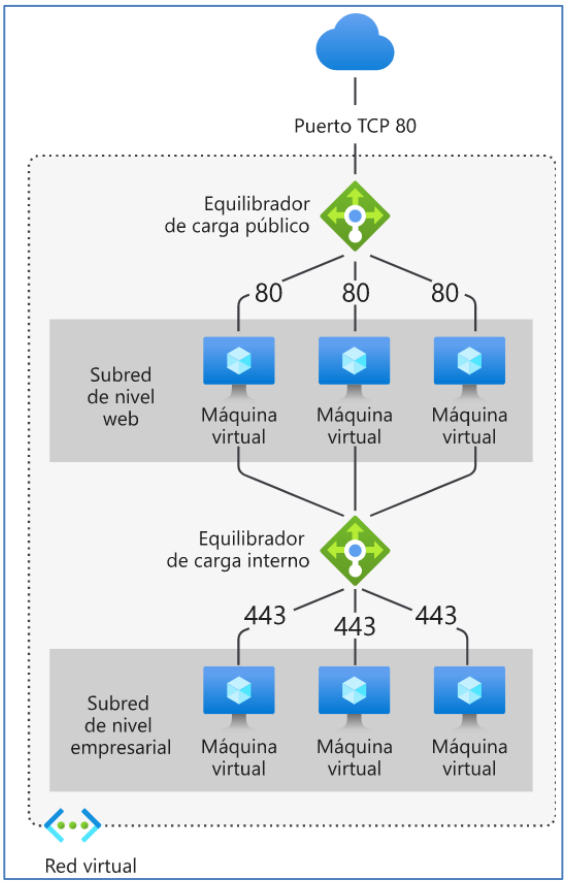


Figura 23 Exemple balancejador de carrega

5.4.9. API Management

Utilitat que permet crear portes d'enllaç d'API coherents i modernes per a serveis de back-end existents. Els productes són la manera de presentar les API als desenvolupadors. Els productes en Administració d'API tenen una o diverses API i es configuren amb títol, descripció i termes d'ús. Els productes poden ser de tipus Obert o Protegit, per poder utilitzar els productes protegits cal subscriure-s'hi abans mentre que els productes oberts es poden utilitzar sense subscripció.

Amb la següent sentència del llenguatge de Microsoft Kusto per l'accés a les metadades de la plataforma és possible obtenir els registres generats per *API Management* les darreres 24 hores.

[24] Lloc web: Microsoft Docs; Article: ¿Que es Azure Load Balancer?; Data consulta: 20/11/2021
URL: https://docs.microsoft.com/es-es/azure/load-balancer/load-balancer-overview

```
ApiManagementGatewayLogs
| where TimeGenerated > ago(1d)
```

Per altra banda, alguns exemples de mètriques a analitzar pel SOC són el nombre de peticions al servei fallides (*failed_requests*) o el nombre de peticions no autoritzades (*unauthorized_requests*) que podrien implicar un atac per força bruta, així com els esdeveniments rebutjats (*rejected_event_hub_events*).

Per suposat, també és possible visualitzar l'estat de les API creades des del portal amb l'opció del registre d'activitats o monitoritzant les mètriques que convingui. Per exemple, a la següent imatge es consulta la mètrica de resposta de porta d'enllaç:

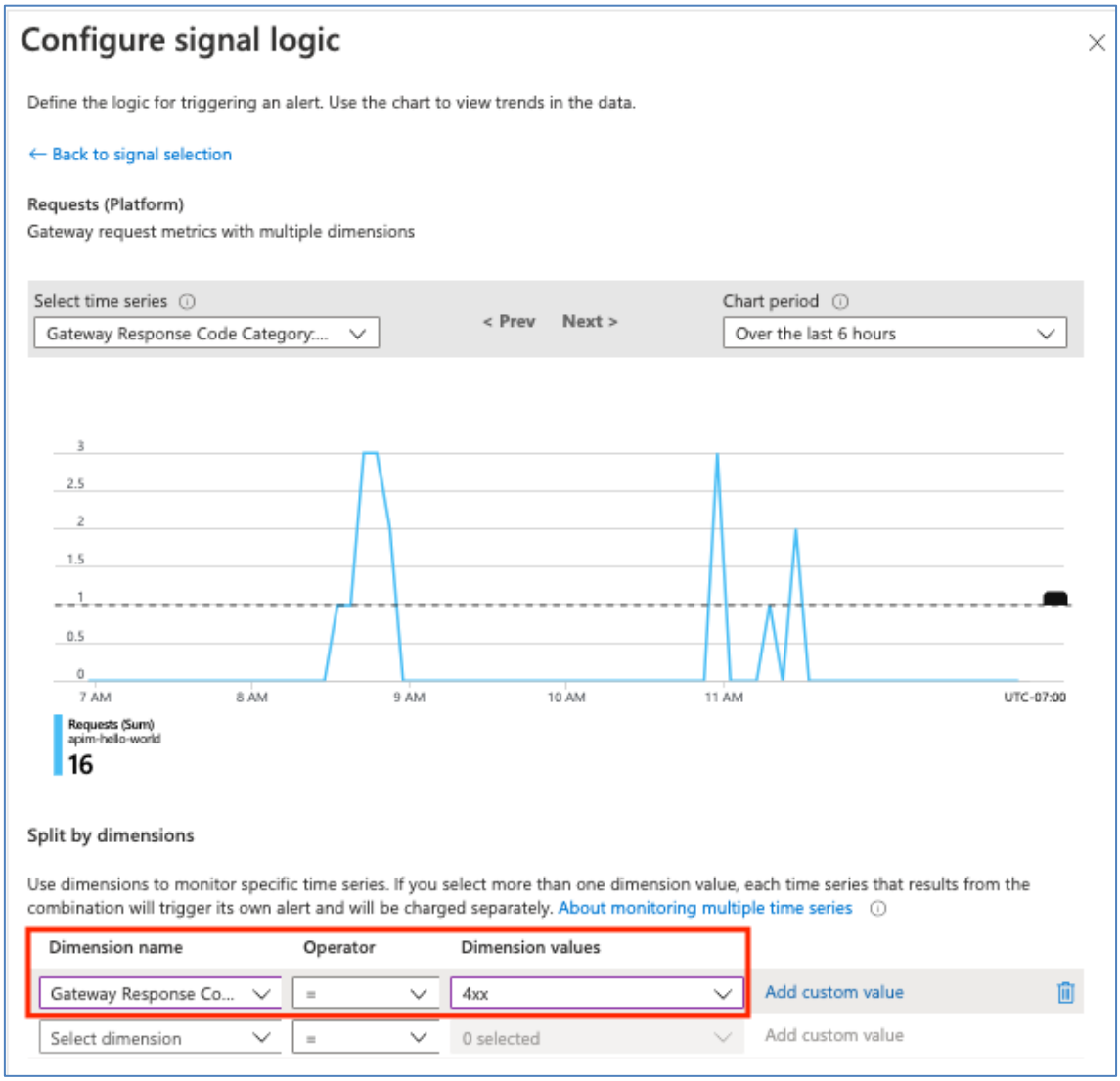


Figura 24 Exemple monitor de mètrica per una API

6. Recollida i enviament de dades

Tal i com s'ha detallat en capítols anteriors, els recursos d'Azure tant poden generar registres com mètriques. Els primers estan disposats en format XML i poden incloure diferents camps amb valors diversos, mentre que els segons són de tipus numèric per permetre l'anàlisi quantitatiu dels valors recollits. La taula següent mostra una comparativa d'ambdues opcions:

Atribut	Mètriques	Registres
Beneficis	Lleuger i capaç d'escenaris gairebé en temps real, com ara alertes. Ideal per a la detecció ràpida de problemes.	Analitzat amb un llenguatge de consultes ric. Ideal per a una anàlisi profunda i identificar la causa arrel.
Dades	Només valors numèrics	Dades de text o numèriques
Estructura	Conjunt estàndard de propietats que inclou el temps de mostra, el recurs que s'està supervisant i un valor numèric. Algunes mètriques inclouen diverses dimensions per a una definició més detallada.	Conjunt únic de propietats segons el tipus de registre.
Recol·lecció	Recollida a intervals regulars.	Es pot recopilar esporàdicament a mesura que els esdeveniments desencadenen la creació d'un registre.
Azure portal	Metrics Explorer	Log Analytics
Orígens de dades inclosos	-Mètriques de la plataforma recopilades dels recursos d'Azure. -Aplicacions supervisades per *Application Insights*. -Personalitzat definit per aplicació o API.	-Registres d'aplicacions i diagnòstic. -Solucions de monitorització -Agents i extensions de VM -Sol·licituds d'aplicacions i excepcions -Azure Security Center -API Data Collector

Taula 6[25] Azure, mètriques vs. registres

[25] Lloc web: Adinemie.com; Measuring Metrics: Log Analytics vs Azure Metrics;
Data consulta: 28/11/2021; Data creació: Juny 2019;
URL: https://adinermie.com/measuring-metrics-log-analytics-vs-azure-metrics-part-4-conclusion/

6.1. Emmagatzematge local

Per tal de poder recollir de forma centralitzada tots els registres que es generen a la infraestructura d'Azure és necessari disposar del recurs d'Azure anomenat *Log Analytics Workspace,* on es durà a terme la recollida general d'aquestes dades per després poder explorar-les i analitzar-les amb les diferents eines disponibles (consultes Kusto, exportació de dades a PowerBI, ...).

Aquest seria el primer punt de recollida general de registres de la infraestructura, tant pel que fa a registres de funcionament dels diferents recursos desplegats al núvol, que es podria etiquetar com a registres de gestió IT, com els específics de seguretat que caldrà destriar i filtrar per enviar al SIEM del serveis SOC contractats externament.

En el cas específic presentat en aquesta memòria pel client fictici ACME, el lloc on caldria emmagatzemar aquesta informació seria la subscripció de gestió, més concretament en el grup de recursos *rg-management-mgt* on es disposarà de la corresponent compte d'emmagatzematge (*Storage Account*). A més, també es podrà vincular aquest compte per guardar les consultes generades, els registres personalitzats i les alertes.

Dins aquest espai de treball Azure permet la creació de Workbooks que ja hem vist anteriorment, habilitant la gestió dels recursos que generen registres i estan connectats des de les diferents subscripcions i la possibilitat de descarregar agents per instal·lar a equips Windows i Linux d'una estructura on-premise en cas que existís. A més, inclou una opció per descarregar un agent per instal·lar equips sense accés directe als recursos Azure per tal d'actuar com a Proxy i facilitar l'enviament de registres.

Així mateix, també permet l'activació granular de recollida d'esdeveniments dels diferents sistemes operatius o de mètriques específiques, tal i com es pot veure a la següent imatge.

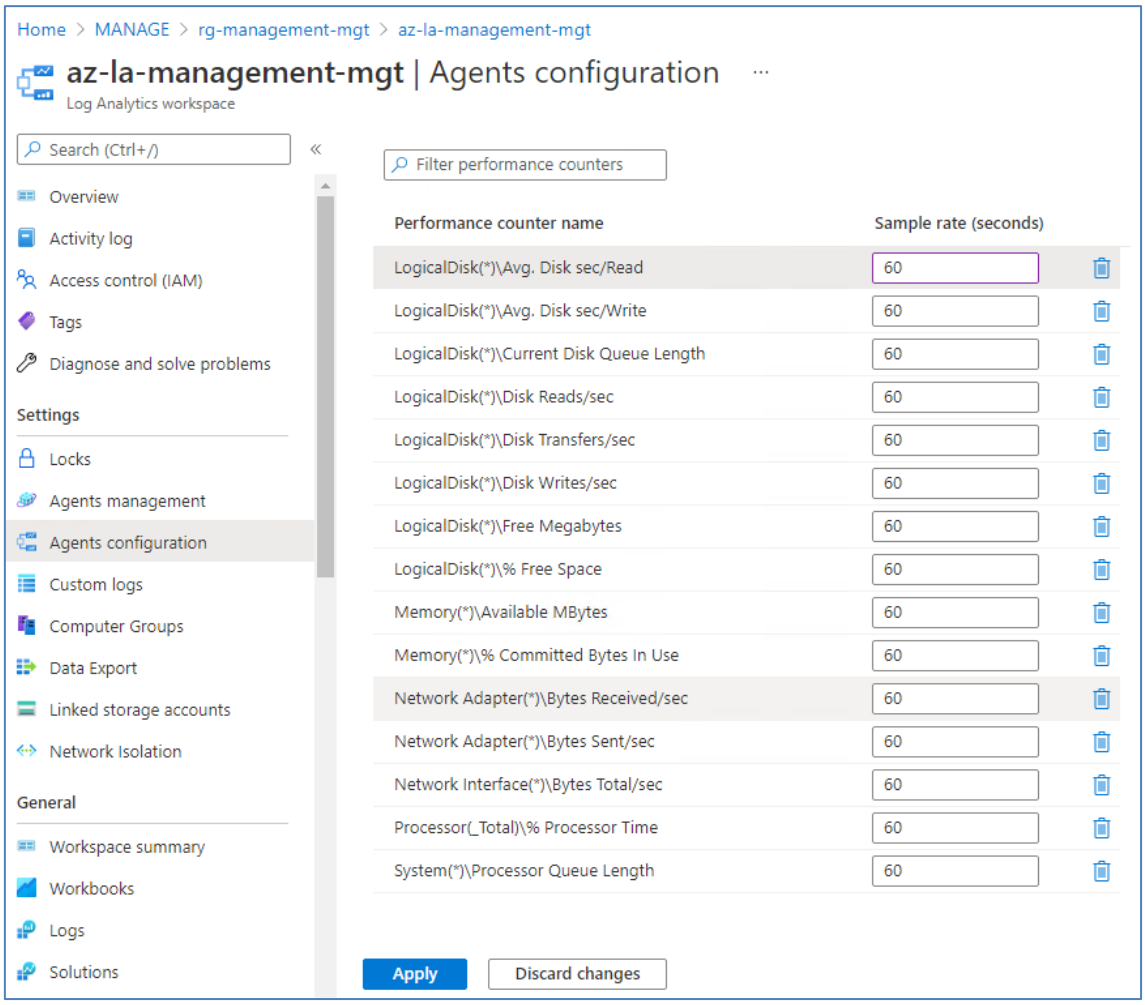


Figura 25 Selecció comptadors de rendiment

Si els gestors de l'empresa ACME volen exportar tota o part de la informació recollida al Log Analytics Workspace disposen d'una funció d'exportació on Azure habilita la opció de triar quins orígens de dades es volen exportar (mètriques, diagnòstics, esdeveniments de màquines virtuals, operacions registrades a Azure monitor, diagnòstics, etc.) i a quin destí es vol enviar, ja sigui a una compte d'emmagatzematge diferent a la que es tingui accés o un Event Hub per la posterior recollida de la informació per part d'un tercer que estigui subscrit al mateix.

Finalment, és important gestionar correctament el nivell de retenció de dades desitjat. Per defecte, la retenció està configurada en 30 dies. Aquest paràmetre es pot consultar a la secció General del Log Analytics Workspace. Aquest valor entra dins del pla contractat i no té cap cost addicional. Ampliar el nivell de retenció impactarà en el cost mensual de la eina. Aquesta informació està disponible a la secció d'ús i costs estimats on es detalla, pels diferents nivells de consum, quines serien les despeses associades.

6.2. Enviament filtrat SOC

6.2.1. Regles de filtrat

Un cop ACME disposa d'un punt centralitzat per la recol·lecció de tots els esdeveniments de la infraestructura tal i com s'ha vist en l'apartat anterior, es pot seleccionar aquelles mètriques i registres crítics que poden ser enviats al SIEM pel seu anàlisi, tractament i gestió si s'escau. És important fer una primera tasca de cribratge entre tota la informació generada a la plataforma per minimitzar les transferències de dades entre ACME i SOC, tant pel que fa al consum d'ample de banda i com això podria impactar al rendiment dels serveis publicats, com per l'impacte econòmic que pot suposar ja que, com s'ha presentat en apartats anteriors, cada alerta generada al sistema té un cost associat.

Definir regles d'enviament d'esdeveniments rellevants no deixa de ser res més que crear aquestes alertes al sistema pels recursos que es considerin crítics i definir-ne el llindar correcte. Cada client d'ACME pot considerar diferents nivells de criticitat pels seus recursos, potser en un cas només es considera com a crítica la plataforma de producció, mentre que altres usuaris de la plataforma poden considerar les subscripcions de desenvolupament vitals per la continuïtat del negoci, ja que es dediquen al disseny i creació de noves solucions.

Així doncs, no és adequat establir quins recursos i mètriques concrets cal analitzar, però sí descriure quin seria el procediment per triar-les. Per això cal seguir les següents recomanacions:

- El client que contracta els serveis a la plataforma, ACME com a arrendador de les subscripcions i un representant tècnic del SOC s'han de reunir per poder entendre i disposar d'una visió de conjunt dels recursos que s'han contractat, quins serveis ofereixen i quins nivells de disponibilitat (*SLA*) han de tenir associats.
- Caldrà acordar revisions periòdiques on es llistin els canvis aplicats a la plataforma i el funcionament global de la solució. Si el SOC no n'és conscient dificultarà enormement la seva tasca de monitorització de seguretat.

- Així mateix, caldrà periòdicament avaluar els costos associats a l'enviament d'alertes al SOC per tal de fer-ne les modificacions que calgui ajustant el màxim possible la despesa associada a la part de seguretat del servei.

- Un cop més, de forma recurrent cal analitzar que les alertes són realment útils per la detecció d'incidències de seguretat i la seva prevenció. És important que a les reunions periòdiques s'exposi tant allò que s'hagi detectat com els possibles incidents que han passat per alt i veure com es poden ajustar les alertes existents per optimitzar el servei ofert pel SOC.

- Una bona forma de garantir la visibilitat dels resultats obtinguts pel SOC es basa en informes. Acordar en les reunions preliminars a la posada en marxa quins KPI es consideren crítics (nombre d'esdeveniments detectats a posterior vs. a priori, quantitat d'alertes enviades, etc.), quins informes generarà periòdicament el SOC tant a nivell global per ACME com a nivell particular per cada client final i els quadres de comandament (*dashboards*) que es posaran a disposició per la monitorització de la plataforma.

- Finalment, i probablement un dels aspectes més importants a tractar, serà definir el marc d'actuació en cas de detecció d'un atac per part del SOC. Cal definir la estratègia de comunicació, quines són les accions que es duran a terme i qui les durà a terme. Al tractar-se de serveis subcontractats entre entitats diferents és bàsic establir els rols de cada una d'elles. Per exemple, si el SOC detecta un cryptolocker a un servidor del client hostatjat a la plataforma d'ACME, qui tindrà la responsabilitat d'aïllar aquest servidor i aturar-lo per evitar la propagació?.

6.2.2. Enviament

Com s'ha escrit anteriorment, es farà ús de les alertes per tal de detectar registres interessants pel SOC o mètriques incorrectes però, com s'ha d'executar aquest enviament? Quines opcions ens ofereix Azure per resoldre aquest punt?. En els següents subapartats se'n presentaran dues que es consideren les més adequades: EventHub i Azure Function. Depenent de com vulgui recollir la informació el SOC, serà més interessant fer-ne servir una o l'altra.

6.2.2.1. EventHub

EventHub consisteix en, tal i com defineix Microsoft[26], una plataforma de streaming de macrodades i un servei d'ingesta d'esdeveniments. Es pot rebre i processar milions d'esdeveniments per segon. Les dades enviades a un centre d'esdeveniments es poden transformar i emmagatzemar amb qualsevol proveïdor d'anàlisi en temps real o adaptadors de processament per lots i emmagatzematge.

Així doncs, sembla que és l'eina correcte pel tractament massiu d'esdeveniments, que és la solució cercada per enviar al SOC les alertes detectades per ACME.

Fent ús de la calculadora d'Azure podem obtenir un cost orientatiu de la solució:

Descripció	Estimated monthly cost
Nivell estàndard: 1 unitat de processament x 730 hores, 1 milió d'entrades d'esdeveniments.	$21,93
Total	$21,93

Com es pot observar, es pot considerar un cost mensual assumible ja que si la tasca de filtrat en origen es fa adequadament difícilment s'hauria d'assolir la quantitat d'1 milió d'esdeveniments enviats.

El següent que cal plantejar-se és, com funciona un concentrador d'esdeveniments?. Per això ens pot ser útil la següent il·lustració extreta de la pròpia documentació de Microsoft. En ella es pot observar que hi ha una sèrie de productors d'esdeveniments que mitjançant diferents protocols de comunicacions com HTTPS o AMQP (Servei avançat de cues de missatgeria - *Advanced Message Queuing Protocol*) s'encarreguen d'enviar les dades al concentrador i després hi ha una sèrie de receptors que s'ocupen de la recollida asíncrona de les mateixes.

A més, permet la distribució en particions dins el propi concentrador per tal d'evitar la saturació en la recollida.

[26] Lloc web: Microsoft Docs; Entrada: EventHub; Data creació: 25/08/2021; data consulta: 06/12/2021; URL: https://docs.microsoft.com/es-es/azure/event-hubs/event-hubs-about

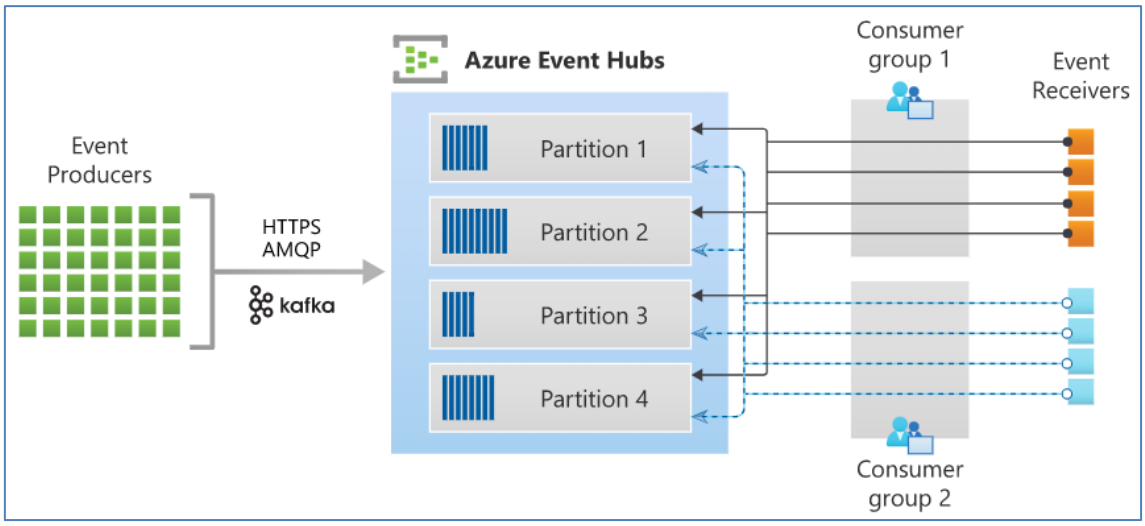


Figura 26 Arquitectura d'EventHub

Un cop presentat el funcionament, cal veure com crear aquest Eventhub i com s'ha de configurar la plataforma per enviar-hi els esdeveniments. La creació es pot dur a terme fàcilment seleccionant Eventhub al menú principal del portal Azure. Només sol·licitarà els següents detalls:

Subscripció: en el disseny presentat a aquesta memòria correspondria a la que hem definit com a Gestió MANAGEMENT.

Grup de recursos: RG-MANAGEMENT-MGT

Nom de l'espai de noms (namespace): qualsevol seria vàlid, però és recomanable escollir-ne un que sigui identificatiu del propòsit d'ús.

Ubicació: és important triar correctament el centre de dades on estigui ubicat ja que això en determinarà la latència d'accés i el cost.

Preu: Standard (20 grups de consumidors + 1000 connexions al concentrador), Basic (1 consumidor i 1000 connexions), Premium (100 grups de consumidors i 10K connexions.).

Quant a connexions, EventHub les descriu com a *Brokered Connections,* que es poden definir com a connexions AMQP d'un client a una subscripció de Service Bus, una cua o un centre d'esdeveniments, una crida HTTP per rebre un missatge d'un tema o una cua de Service Bus que tingui un valor de temps d'espera de recepció superior a zero.

Un cop es disposa del namespace s'hi pot crear tots els Eventhubs que es considerin necessaris per la infraestructura d'ACME per exemple, pot convenir disposar de dos concentradors diferents: un per l'enviament d'esdeveniments

massius que pot fer servir ACME per l'analítica IT i un altre específic per l'enviament filtrat d'esdeveniments de seguretat que farà servir el SOC.

Per dur a terme aquest esdeveniment filtrat es farà servir les alertes d'Azure i a cada una d'elles s'hi vincularà un Action Group que serà l'encarregat de l'enviament. En ell es pot escollir com a destí el namespace i Eventhub que s'hagi creat.

A més, aquest Action Group permet encadenar diferents accions per cada alerta detectada, és a dir, es pot donar el cas que un mateix esdeveniment tingui associades diverses accions (notificació per correu electrònic o SMS, enviament a Eventhub d'ACME, enviament a Eventhub de seguretat pel SOC, etc.)

Finalment, cal veure com es faria la recollida d'aquests esdeveniments. Hi ha múltiples opcions per fer-ho amb implementacions de codi específiques per multitud de llenguatges de programació. Es mostra un exemple a continuació:

```
class Program
  {
    const string EvHConnectString = "<youreventhub connectstring>";
    static void Main(string[] args)
    {
      MainAsync().Wait();
    }
    private static async Task MainAsync()
    {
      Console.WriteLine("Connecting to the Event Hub...");
      var EvHCli =
        EvHCli.CreateFromConnectionString(EvHConnectString);
      var runtimeInformation = await
ZvHCli.GetRuntimeInformationAsync();
      var partitionReceivers =
runtimeInformation.PartitionIds.Select(partitionId =>
          EvHCli.CreateReceiver("$Default",
          partitionId, DateTime.Now)).ToList();
      Console.WriteLine("Waiting for incoming events...");
      foreach (var partitionReceiver in partitionReceivers)
      {
        partitionReceiver.SetReceiveHandler(
          new
SecurityDataPartitionReceiveHandler(partitionReceiver.PartitionId));
      }
      Console.WriteLine("Press any key to shutdown");
      Console.ReadLine();
      await EvHCli.CloseAsync();
    }
  }
```

Hi ha versions del codi per C#, Java, Python, etc. Un cop rebuda la cadena de dades el SOC hauria de desenvolupar el codi associat per emmagatzemar-la i tractar-la, però això queda fora de l'àmbit d'aquesta memòria.

6.2.2.2. Azure Function

Una alternativa a EventHub consisteix en la gestió dels esdeveniments fent ús de les Azure Functions[27]. Enlloc d'enviar tots els registres complerts tal i com estan creats a Azure, podem crear línies de codi que s'executin a l'activar l'alerta i modificar les dades recollides. Un exemple de codificació d'Azure Function podria ser el següent:

```
using namespace System.Net

# Input bindings are passed in via param block.
param($Request, $TriggerMetadata)

# Write to the Azure Functions log stream.
Write-Host "PowerShell HTTP trigger function processed a request."

$alert = $request.body

#extract Affected cI
$affectedCI                                                    =
$alert.body.data.alertContext.AffectedConfigurationItems
write-host "Affected CI" $affectedCI

#Extract projected fields from Log Search Alert
$computer                                                      =
$alert.body.data.alertContext.SearchResults.tables.rows[0]
$svcname = $alert.body.data.alertContext.SearchResults.tables.rows[1]
$svcstate                                                      =
$alert.body.data.alertContext.SearchResults.tables.rows[2]
$svcdisplayname                                                =
$alert.body.data.alertContext.SearchResults.tables.rows[3]
$TimeGenerated                                                 =
$alert.body.data.alertContext.SearchResults.tables.rows[4]

write-host "Computer" $computer "svc name" $svcname "svcstate"
$svcstate "svc displayname" $svcdisplayname "TimeGenerated"
$timegenerated
```

El que estem fent en aquestes línies de codi és extreure dels registre d'Azure els camps $computer. $svcstate, $svcdisplayname i $TimeGenerated amb el que es podria monitoritzar l'estat dels serveis de cada un dels equips de la infraestructura.

Aquest exemple només envia per pantalla el detall del registre capturat amb la comanda write-host, caldria doncs modificar-la per executar l'acció d'enviament

[27] Lloc web: Cloud, Systems, Management and Automation; Article: Azure Monitor Alert with Azure Functions; Autor: Billy York; Data creació: setembre 2019; Data consulta: 06/12/2021; URL: https://www.cloudsma.com/2019/09/azure-monitor-alert-azure-functions/

al SOC, per exemple via crida a un web Service que estigui en escolta en el SIEM.

Alternativament, també podríem recollir les mètriques amb el següent codi:

```
using namespace System.Net

# Input bindings are passed in via param block.
param($Request, $TriggerMetadata)

# Write to the Azure Functions log stream.
Write-Host "PowerShell HTTP trigger function processed a request."

# Interact with query parameters or the body of the request.
$alert = $request.body

# get alert rull, severity and time
$alertrule = $alert.body.data.essentials.alertRule
$severity = $alert.body.data.essentials.severity
$firedDateTime = $alert.body.data.essentials.firedDateTime

#get metric type and value
$metric = $alert.body.data.alertContext.condition.allOf.metricName
$metricValue                                                        =
$alert.body.data.alertContext.condition.allOf.metricValue

#get affected CI
$affectedCI                                                         =
$alert.body.data.alertContext.condition.allOf.dimensions.value[1]

write-host    "Rule"    $alertRule    "Severity"    $severity    "Time"
$fireddateTime "metric" $metric "value" $metricvalue "Affected CI"
$affectedCI
```

Les dues peces de codi permetrien la generació i enviament d'avisos via API (caldria modificar de nou el write-host pel codi corresponent). Només cal afegir a l'*Action Group* associat a l'alerta, l'opció Azure Function prèviament creada amb el codi del requadre anterior.

És una opció molt més costosa de configurar ja que caldria un important desenvolupament de totes les diferents alertes que es volen tractar per part d'ACME, però al mateix temps s'aconseguiria un enviament granular al SIEM de la informació amb un gran nivell de detall i molt filtrada.

Cal comparar ambdues alternatives i avaluar quina d'elles pot ser més interessant, ja que depenent de quin sigui l'escenari a tractar pot convenir més una opció o l'altra.

7. Analítica d'esdeveniments al SOC

Fins ara s'ha presentat la infraestructura al cloud d'ACME, s'ha descrit el funcionament d'un SOC, s'han presentat els diferents recursos que es troben disponibles a Azure, s'ha vist com aquests recursos generen registres i s'ha vist quines opcions són disponibles a Azure per la recol·lecció i enviament d'aquesta informació al SOC.

L'últim aspecte que queda per tancar aquest model teòric consisteix en descriure com el SOC ha d'emmagatzemar i processar aquesta informació. Cal partir de la premissa que el SOC no tindrà un únic client (ACME en el cas d'aquesta memòria) sinó que disposarà de diferents fonts de dades recollides per analitzar, que li poden servir per fer sinèrgia entre els diferents clients. En el supòsit que diversos clients amb serveis contractats a Acme pateixin d'un atac específic que pot ser evitat aplicant alguna mesura correctiva, té sentit que el SOC emeti una alerta a la resta dels clients avisant-ne, evidentment mantenint anònims els detalls dels clients que han estat atacats.

Així doncs, com es pot aconseguir aquesta funcionalitat?. El més lògic seria pensar que la infraestructura del SOC també està hostatjada al núvol, en aquest cas no té per què ser d'Azure, qualsevol de les opcions existents al mercat serien vàlides per exemple: AWS, Google cloud, IBM, etc. Però, alternativament, també es pot donar el cas que el SOC disposi d'infraestructura on-premise o en un cloud privat en el que operar.

Fos quina fos la plataforma escollida sí que hauria de disposar d'espai d'emmagatzematge suficient per recollir i tractar tota la informació rebuda pels clients, a més d'assegurar la confidencialitat de les dades entre els diferents clients. És evident que si el SOC té contractes de serveis de seguretat amb dues entitats bancàries rivals, els clients no poden tenir visibilitat dels quadres de comandament i informes de seguretat que es generin per cadascun d'ells, així tampoc, com els espais d'emmagatzematge on resideixin les dades dels registres en cru de cada client.

Aquest espai d'emmagatzematge, en el cas d'estar a Azure, hauria de ser un Storage Account DataLake2 amb diferents contenidors per cadascun dels clients que contractin els serveis del SOC. D'aquesta forma es podria garantir la confidencialitat de les dades emmagatzemades via ACL o polítiques d'accés específiques pel recurs. Habitualment, s'assignen SPN amb permisos d'escriptura i de lectura associats als diferents processos d'enviament o recollida de dades.

7.1. SIEM vs. SOAR

Tal i com s'ha vist en la descripció de les eines disponibles per un SOC se n'han presentat dues: el SIEM i el SOAR. El primer que cal indicar és que no són eines excloents l'una de l'altra, just al contrari, es complementen i poden conformar la caixa d'eines principal emprada pel SOC.

Els SIEM estan pensants per la detecció i la resposta ràpida enfront incidents i vulnerabilitats de seguretat, mentre que els sistemes SOAR es centren en el filtrat d'aquests esdeveniments, descarten els falsos positius i automatitzen les respostes als mateixos alliberant al SOC d'aquestes tasques repetitives i poc productives.

En el model teòric que es planteja es recomana la utilització d'ambdues eines per part del SOC, donant així als clients, en particular a ACME, tots els serveis de seguretat per poder garantir la continuïtat del negoci i la seguretat de les seves dades i serveis.

Un cop revisats els costos associats d'enviar tots els esdeveniments generats per la infraestructura d'ACME es pot optar per dos models:

1. Enviament filtrat de la informació generada via Azure Function. Aquesta opció requereix un treball previ a la plataforma d'ACME per definir regles i implementar el codi que recollirà la informació a enviar. Serà més costós d'implementar, però els gestors d'ACME disposaran d'un nivell més alt de control sobre la informació generada a la plataforma i enviada al SOC. En aquest cas el SOC probablement només necessitaria fer ús del SIEM per recollir els esdeveniments, ja que estaran prèviament filtrats. Es corre el risc d'excloure informació important en el filtrat.

2. Enviament massiu de la informació d'infraestructura generada a Azure via EventHub. En aquest cas no s'implementarien filtres en origen, no caldria definir regles, simplement s'associaria tots els registres generats a la plataforma i s'enviaren sense cap filtre, i així seria SOAR l'encarregat de fer-ne el tractament i posterior filtrat, si s'escau.

   Per fer-ho, només caldria anar al portal Azure i per cada una de les subscripcions activar l'enviament a: Monitor – Activity Log – Diagnostic Settings – seleccionar tots els Log Types – enviar a stream or Event Hub.

   A la imatge següent podem veure els diferents tipus de registre que es podrien seleccionar i destins disponibles. Com es pot apreciar, és possible seleccionar més d'un destí simultàniament permetent, en cas que es

consideri necessari, mantenir els registres dins el LogAnalytics de la subscripció creada per la gestió d'ACME i al mateix temps enviar a un EventHub pel posterior tractament del SOC amb el SOAR. Inclús, en cas de que el SOC disposi de solucions comercials específiques per fer la tasca de recollida de dades, la podrem seleccionar via *Send to partner solution*, que en el moment d'escriure aquest document inclou les solucions Apache Kafka, Datadog, Elastic i Logz.io.

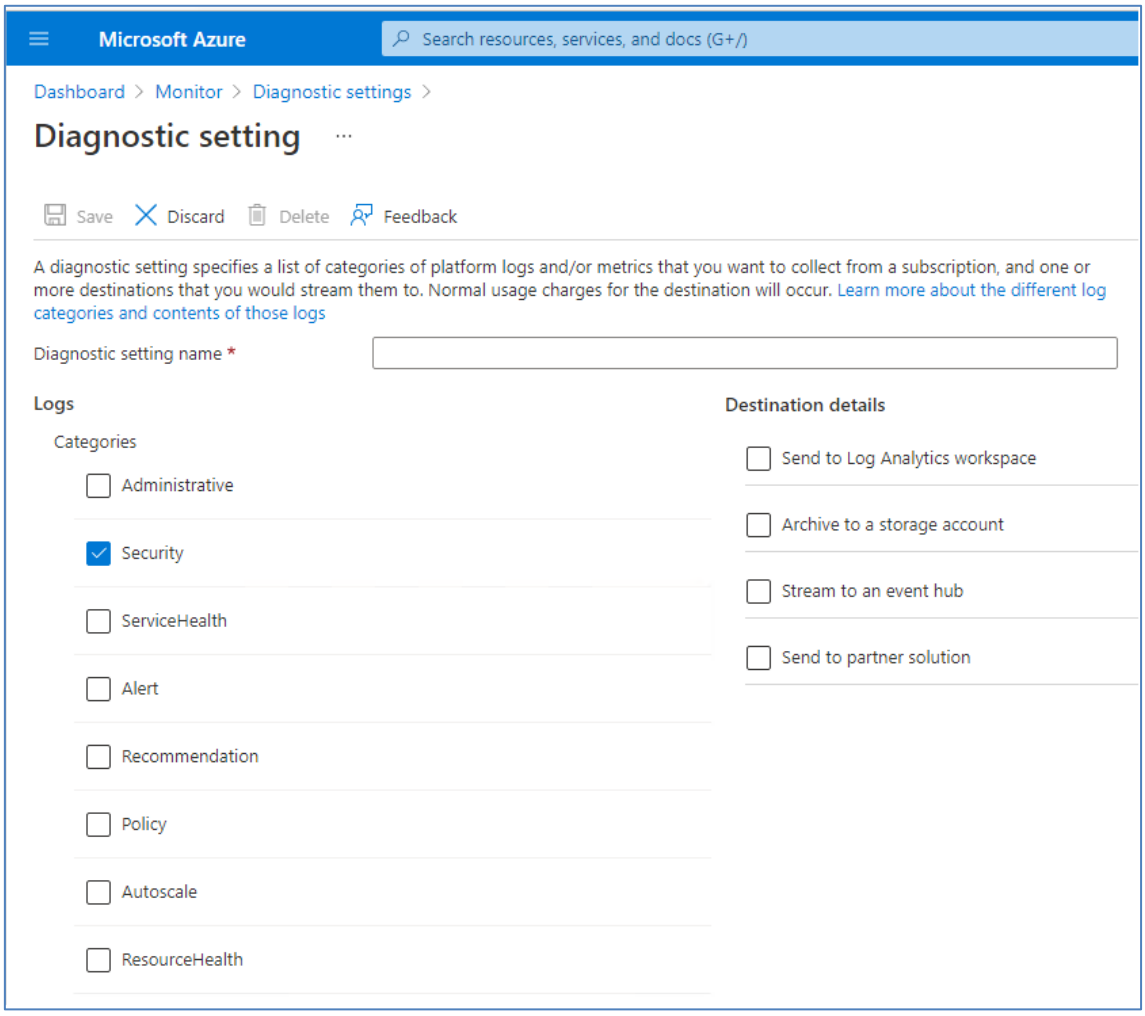


Figura 27 Selecció esdeveniments per enviament massiu

No hi ha una opció correcte o incorrecte entre les presentades, les dues són igual de vàlides. Cal ponderar els recursos humans disponibles a l'organització, coneixements dels mateixos, maduresa existent en matèria de ciberseguretat, anàlisi dels costos de les diferents solucions, política de seguretat existent a la companyia, etc. En qualsevol cas, triar un o altre model serà una opció important per ACME però no reversible. Els contractes es revisen de forma cíclica i les realitats de les empreses varien, el que pot semblar correcte avui, pot no ser-ho demà i sempre es poden renegociar els terminis de l'acord i modificar-ne alguns aspectes si convé.

7.2. GDPR al SOC

Cal assegurar que la informació que ACME enviarà al SOC compleix amb la normativa vigent quant a protecció de dades. L'actual legislació europea al respecte, es basa en el Reglament (UE) 2016/679 relatiu a la protecció de les persones físiques pel que fa al tractament de dades personals i a la lliure circulació d'aquestes dades (aquest text inclou la correcció d'errades publicada al DOUE de 23 de maig de 2018).

Durant tota memòria s'ha presentat com un client fictici subcontractarà la seguretat de la infraestructura al núvol a un tercer, més concretament, un SOC que disposarà d'eines com SIEM o SOAR. Un dels aspectes que ACME ha de considerar per seleccionar amb qui arrendarà aquests serveis es la regulació GDPR i el nivell de compliment de la mateixa.

Florian Menges, et. al[28] afirma que:

"SIEM systems work with data from highly heterogeneous sources. As a result, different requirements need to be met in order to enable data protection in accordance with the GDPR. Establish data protection through the full encryption of all data would be the most intuitive and legally compliant way to process the data. However, since the GDPR only requires the protection of personal data, the data can also be classified according to protection requirements and partially peudonymized in this context."

És a dir, la GDPR protegeix especialment les dades personals pel que caldrà analitzar i tenir cura de quina informació s'envia el SOC i en cas de que sigui considerada com a protegia anonimitzar-la adequadament. La opció més ràpida seria la complerta encriptació de totes les dades però, si se'n fa una classificació prèvia es pot ser molt més selectiu.

Per tal de dur a terme aquesta tasca, es proposa passar d'una arquitectura inicial del SIEM on s'encripta massivament tota la informació rebuda (figura 28), a una segon disseny on s'analitza el tipus de dades que s'està enviant i es fa una pseudo-anonimització de la mateixa (figura 29) per fer-ne el posterior tractament i generar els informes corresponents. Cal destacar que no s'anonimitzen completament les dades ja que les convertiria en dades no útils per l'anàlisi posterior del SOC i que la pseudo-desanonimització només es pot aplicar quan s'estudia un incident de seguretat concret que implica aquelles dades.

[28] Towards GDPR-compliant data processing in modern SIEM Systems; data publicació: 31 desembre 2020

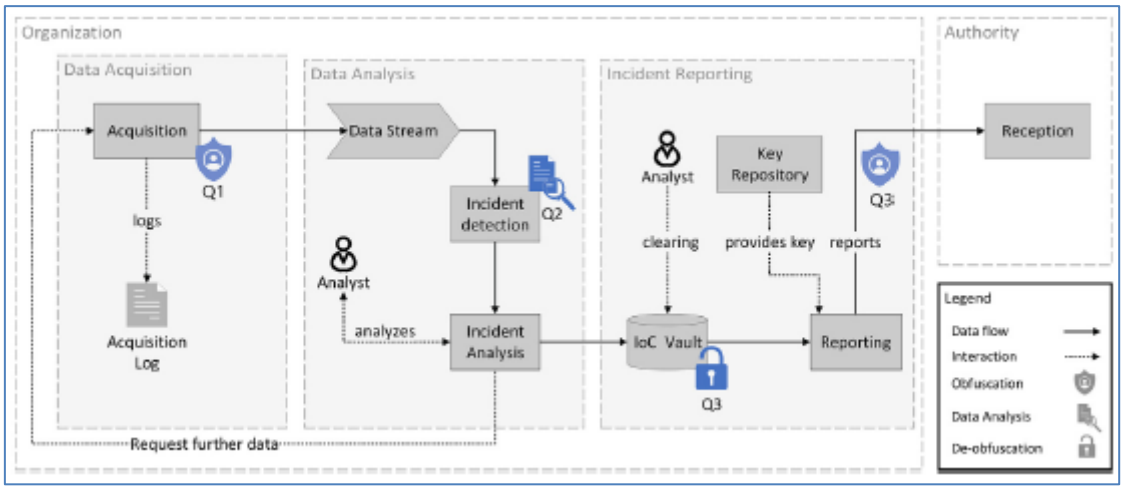


Figura 28 DINGfest Base Architecture

DINGfest és un projecte de recerca que té com a objectiu millorar la detecció, l'anàlisi forense i la notificació d'incidències detectades. Consta de tres mòduls principals: l'adquisició de dades, l'anàlisi de dades i la notificació d'incidents ubicats dins d'una organització i mostra una possible notificació a una autoritat externa per a la recepció d'incidències detectades.

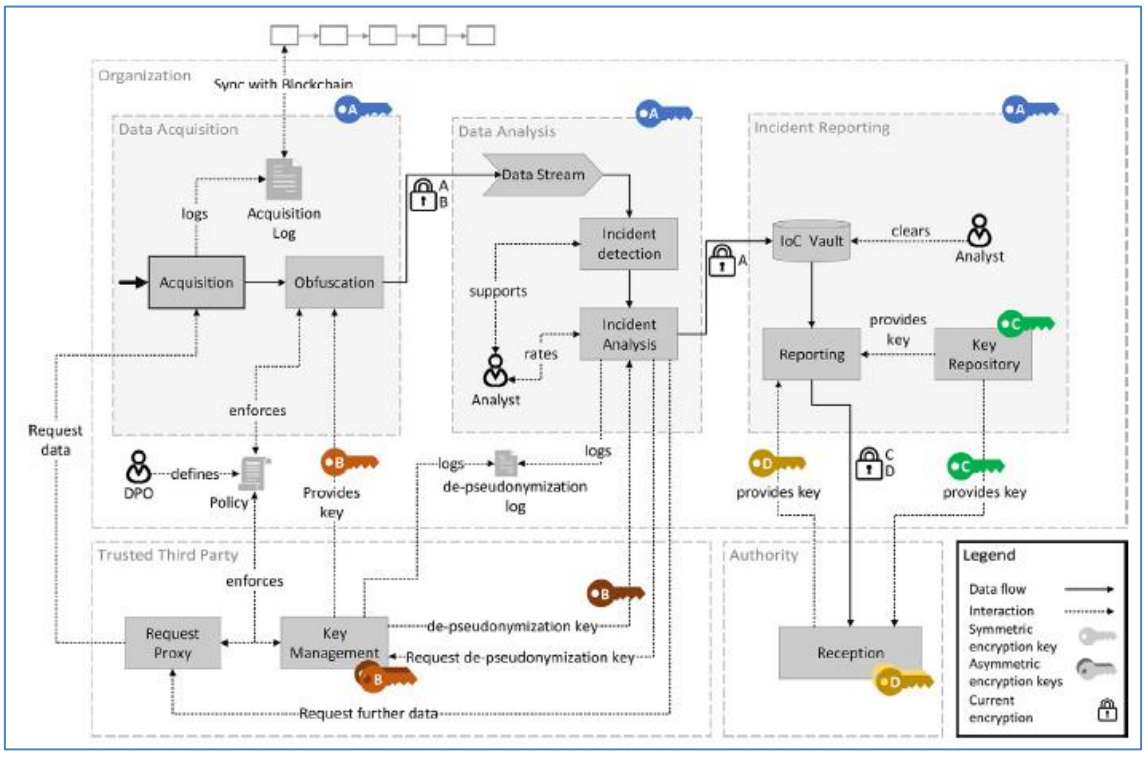


Figura 29 DINGfest GDPR Architecture

Com s'aprecia a la arquitectura de la figura 29, s'afegeix al disseny original la pseudo-desanonimització de les dades per què, en cas d'incident, en quedi evidencia de la mateixa i complir això amb la normativa establerta per la GDPR.

Conclusions

Hi ha varies conclusions a les que s'ha arribat a l'acabar el redactat d'aquesta memòria, però potser la principal és que l'enviament i compartició dels esdeveniments de seguretat de la plataforma al SOC es pot fer filtrada o complerta. Depenent del model triat implicarà la contractació de diferent tipus de serveis de seguretat repercutint també en els costs derivats. La tria d'una o altre opció està supeditada a diversos factors que cal ponderar en cada cas.

Addicionalment a aquesta conclusió central es pot afegir:

- Les infraestructures al núvol operen diferent de les tradicionals i els coneixements previs que es puguin tenir són molt útils però no suficients per desplegar i gestionar la infraestructura. Cal renovar i ampliar els coneixements adquirits en matèria de gestió de seguretat al núvol.

- L'externalització de serveis de seguretat a un SOC no implica que l'empresa contractant dels serveis es pugui desentendre completament de la gestió de seguretat. Si no existeix una comunicació transparent i fluïda entre ambdues, el perill de la pèrdua del *know-how* en la gestió prèvia feta pot implicar importants riscs de seguretat.

- Cal analitzar quines dades es considera necessari recollir i filtrar els registres i mètriques propis d'IT dels relacionats amb seguretat, per tal de limitar les tasques del SOC. Però, cal fer-ho amb la coordinació dels especialistes de seguretat per tal de no ometre informació que pot semblar innecessària pel client, però en realitat sí ser-ho per un agent amb expertesa en matèria de seguretat.

Pel que fa als assoliments del model teòric, es creu que s'ha establert un bon disseny d'infraestructura al núvol i s'han definit les bases per poder externalitzar els serveis de seguretat a un SOC establint diferents recursos disponibles. Queda pendent, però, una important tasca a realitzar definint quina informació cal enviar al SIEM i al SOAR per tal que siguin analitzades i gestionades pel SOC. Això només es pot detallar quan s'estableixin quins seran els recursos que es desplegaran a la infraestructura i quins seran els riscos reals que caldrà evitar.

La metodologia aplicada i la planificació han sigut adequades. S'ha redactat la memòria de forma progressiva i continuada durant el temps assignat al projecte, sense haver de fer grans modificacions al plantejament inicial. Sí

que cal mencionar que hi ha hagut una correcció en l'orientació del treball ja que inicialment s'han mencionat marques de productes comercials, que al tractar-se d'un model teòric no tenien sentit d'aparèixer a la memòria, i finalment s'han eliminat del redactat.

Per últim, per futures línies de treball en les que poder ampliar aquest model teòric, caldria aprofundir en solucions de seguretat específiques per productes concrets com les màquines virtuals. Incloure programaris antivirus, tallafocs, anàlisi de continguts per la navegació web, agents de detecció de patrons de risc als clients finals, agents per l'inventari automatitzat dels recursos IT tipus MDM (Mobile Device Management), etc.

Glossari

AAD: Azure Active Directory és el servei de gestió d'accessos i identitats basat en núvol de Microsoft que ajuda als usuaris a iniciar sessió i accedir als recursos.

Add-ons: petits components de programari que permeten ampliar la gamma de funcions de les aplicacions on s'instal·len. Instal·lant el complement adequat, es pot adaptar l'aplicació a les necessitats personals de l'usuari i actualitzar-lo perquè disposi de funcions i utilitats addicionals.

API: de l'acrònim *Application Programming Interfaces* (interfícies de programació d'aplicacions) és un conjunt de definicions i protocols que s'utilitza per desenvolupar i integrar el programari de les aplicacions, permetent la comunicació entre dos components de programari a través d'un conjunt de regles.

Blobs: de l'acrònim *Binary Large Object* (objecte binari gran) s'entén com a emmagatzemar un element gran de dades en una base de dades que està en codi binari. Aquest codi binari és llegible per al programari però per a les persones només sembla una combinació de 0 i 1.

CAPEX: inversions en béns de capital o despeses en capital. És una contracció de l'anglès *capital expenditure* i s'executa quan un negoci inverteix en la compra d'un actiu fix o per afegir valor a un actiu existent amb una vida útil que s'estén més enllà de l'any imposable.

Datawarehouse: sistema informàtic que afegeix i combina informació de diferents fonts en un magatzem de dades únic i centralitzat per donar suport a funcionalitats diverses com l'anàlisi empresarial, la mineria de dades, la intel·ligència artificial (IA) o l'aprenentatge computacional (*Machine Learning*).

DDoS: atacs de denegació distribuïda de servei són aquells on un lloc web rep multitud de sol·licituds simultànies desbordant la capacitat de servir respostes.

Docker Swarm: consisteix en un grup de màquines físiques o virtuals que executen l'aplicació Docker i que s'han configurat per unir-se en un clúster proporcionen així alta disponibilitat dels serveis publicats.

ETL: de l'acrònim *Extract, Transform, and Load* (extreure, transformar i carregar). Qualsevol eina que fem servir per realitzar aquestes tres funcions amb les dades entre diferents orígens i destins.

FQDN: de l'acrònim *Fully Qualified Domain Name*, (Nom de domini qualificat complert) es refereix a l'adreça completa i única necessària per tenir presència a

Internet. Està composta pel nom d'amfitrió i el de domini i s'utilitza per localitzar hosts específics a Internet i accedir-hi mitjançant la resolució de noms.

Github: un portal creat per allotjar el codi de les aplicacions de qualsevol desenvolupador i que va ser comprada per Microsoft al juny del 2018. La plataforma està pensada per tal que els desenvolupadors pugin el codi de les seves aplicacions i eines i que, com a usuari, no només es pugui descarregar l'aplicació sinó també entrar al perfil per llegir sobre ella o col·laborar amb el seu desenvolupament.

KPI: de l'acrònim *Key Performance Indicator* (indicadors claus de rendiment) són aquell conjunt de mètriques considerades com a més rellevants per l'estratègia del que s'està analitzant i que ajuden a determinar l'èxit o el fracàs de la tasca que s'estudia.

Machine Learning: terme anglosaxó per l'aprenentatge computacional que defineix un tipus d'intel·ligència artificial (IA) que permet que les aplicacions de programari siguin més precises a l'hora de predir els resultats sense haver-les programat explícitament. Els algoritmes d'aprenentatge automàtic utilitzen dades històriques com a entrada per predir nous valors de sortida.

On-premise: una traducció vàlida és "en local" i es refereix a qualsevol instal·lació d'una solució de programari o maquinari que es porta a terme dins dels servidors físics i la infraestructura (TIC) de l'empresa. Amb el model on-premise l'empresa és la responsable de la seguretat, disponibilitat i gestió del programari.

OPEX: acrònim d'*Operational Expenditures* (despeses operacionals) és el cost permanent associat al funcionament d'un producte, negoci o sistema. També es pot traduir com a despesa de funcionament o despeses operatives.

Outlier: concepte d'origen estadístic definit com a valor atípic dins una sèrie que és numèricament diferent de la resta de valors de la sèrie.

SaaS: de l'acrònim *Software As a Service* (programari com a servei) és un model de distribució de programari on el suport lògic i les dades que es gestionen s'allotgen en servidors d'una companyia de tecnologies d'informació i comunicació, als quals s'accedeix via Internet des d'un client.

Shell: És la interfície més externa dels sistemes operatius i proporciona una sèrie de comandes per poder interactuar amb el sistema. Cada sistema té un o varis propis, com per exemple Linux té BASH, Korn, TSCH, etc. o Windows DOS, PowerShell, etc.

SLA: acrònim de *Service Level Agreement* o nivell d'acord de servei. Defineix clarament quins són els acords entre dues parts quant als nivells de servei oferts i els temps de resposta.

SPN: acrònim de *Service Principal Name* o també conegut com a comptes de servei. Són comptes de xarxa que es fan servir, sobretot en l'entorn Microsoft, per associar a aplicacions o serveis que necessiten credencials per la seva execució i no estan vinculades a persones físiques.

PaaS: acrònim de *Platform As a Service* (Plataforma com a servei) és un entorn de desenvolupament i implementació complet al núvol amb recursos que permeten lliurar-ho tot, des d'aplicacions senzilles basades en el núvol fins a aplicacions empresarials sofisticades habilitades per al núvol.

Privacy Shield: Escut de privacitat entre la Unió Europea i els Estats Units per garantir el compliment de la normativa Europea sobre el tractament de les dades personals dins del marc de la GDPR.

WireShark: Eina gratuïta molt usada en la informàtica forense que permet interceptar el tràfic d'una xarxa i el converteix en un format llegible per les persones.

Bibliografia i Web grafia

1. COMTACT Cloud, Security, Delivery;
Data consulta: 24/09/2021;
URL: https://comtact.co.uk/azure-sentinel/

2. Panel compliment regulacions Azure;
Data consulta: 24/09/2021;
URL: https://azure.microsoft.com/es-es/blog/regulatory-compliance-dashboard-in-azure-security-center-now-available/

3. Web oficial CIS;
Data consulta: 24/09/2021;
URL: https://www.cisecurity.org/cybersecurity-threats/

4. ISO web oficial; UNE-EN ISO/IEC 27001 Mayo 2017;
Data consulta: 28/09/2021;
URL: https://www.iso.org/isoiec-27001-information-security.html

5. Plans de suport Azure;
Data consulta: 24/09/2021;
URL: https://azure.microsoft.com/en-us/support/plans/

6. Recomanacions d'Azure;
Data consulta: 24/09/2021;
URL: https://azure.microsoft.com/en-us/services/advisor/

7. Estat de salut de la infraestructura;
Data consulta: 24/09/2021;
URL: https://status.azure.com/en-us/status

8. Lloc web oficial Gartner - Network Firewalls Reviews and Ratings;
Data Consultat: 20/09/2021;
URL: https://www.gartner.com/reviews/market/network-firewalls

9. Lloc web oficial Microsoft Azure - Load Balancer;
Data consulta: 20/09/2021;
URL: https://azure.microsoft.com/es-es/services/load-balancer/

10. Lloc web oficial Microsoft Docs;
Data edició: 09/09/2020; Data consulta: 25/09/2021
URL: https://docs.microsoft.com/en-us/azure/ddos-protection/ddos-protection-overview

11. Web oficial Microsoft Docs – Azure Network Security Groups;
Data edició: 24/08/2020; Data consulta: 25/09/2021
URL: https://docs.microsoft.com/es-es/azure/virtual-network/network-security-groups-overview

12. TechTarget – Search Security;
Data consulta: 25/09/2021;
URL: https://searchsecurity.techtarget.com/definition/Security-Operations-Center-SOC

13. Aenor lloc web oficial;
Data consulta: 27/09/2021;
URL: https://tienda.aenor.com/norma-une-en-iso-iec-27001-2017-n0058428

14. Lloc web oficial McAfee - What is a security operations center?;
Data consulta: 27/09/2021;
URL: https://www.mcafee.com/enterprise/es-es/security-awareness/operations/what-is-soc.html

15. Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic.
Autors: Harjinder Singh Lallie, Lynsay A. Shepherd, Jason R.C. Nurse, Arnau Erola, Gregory Epiphaniou, Carsten Maple, Xavier Bellekens;
Acceptat el 22 febrer 2021.

16. Lloc web: LaSalle Blogging; Article: Que és un SOAR?;
Data publicació 20/05/2021; Data consulta: 06/12/2021;
URL: https://blogs.salleurl.edu/es/que-es-soar

17. Azure pàgina oficial - Calculadora de preus;
Data consulta: 10/10/2021;
URL: https://azure.microsoft.com/en-us/pricing/calculator

18. Lloc oficial Microsoft Docs; Introducció a les consultes Custo;
Data consulta 10/10/2021;
URL: https://docs.microsoft.com/es-es/azure/data-explorer/kusto/query/

19. Lloc oficial Microsoft Docs – Llibres d'Azure Monitor;
Data consulta: 11/10/2021;
URL: https://docs.microsoft.com/es-es/azure/azure-monitor/visualize/workbooks-overview

20. Wikipedia - Protocolo simple de administración de red;
Data edició: 20/05/2021; Data consulta: 10/10/2021;
URL: https://es.wikipedia.org/wiki/Protocolo_simple_de_administraci%C3%B3n_de_red

21. Pàgina oficial Wikipedia; Article: Syslog;
Data edició 09/10/2021; Data consulta: 12/10/2021;
URL: https://es.wikipedia.org/wiki/Syslog#/media/Archivo:Syslog_layers_RFC5424.png

22. Lloc web: Microsoft Docs; ¿Que es Azure Application Gateway?
Data edició 13/05/2021; Data consulta 20/11/2021
URL: https://docs.microsoft.com/es-es/azure/application-gateway/overview

23. Lloc web: Microsoft Docs; Container Monitoring solution in Azure Monitor;
Data consulta: 20/11/2021; Darrere edició: 09/23/2021;
URL: https://docs.microsoft.com/en-us/azure/azure-monitor/containers/containers

24. Lloc web: Microsoft Docs; Article: ¿Que es Azure Load Balancer?;
Data consulta: 20/11/2021; Darrere edició: 28/10/2021
URL: https://docs.microsoft.com/es-es/azure/load-balancer/load-balancer-overview

25. Lloc web: Adinemie.com; Measuring Metrics: Log Analytics vs Azure Metrics
Data consulta: 28/11/2021; Data creació: Juny 2019;
URL: https://adinermie.com/measuring-metrics-log-analytics-vs-azure-metrics-part-4-conclusion/

26. Lloc web: Microsoft Docs; Article: EventHub;
Data creació: 25/08/2021; Data consulta: 06/12/2021;
URL: https://docs.microsoft.com/es-es/azure/event-hubs/event-hubs-about

27. Lloc web: Cloud, Systems, Management and Automation;
Article: Azure Monitor Alert with Azure Functions; Autor: Billy York;
Data creació: setembre 2019; Data consulta: 06/12/2021;
URL: https://www.cloudsma.com/2019/09/azure-monitor-alert-azure-functions/

28. Towards GDPR-compliant data processing in modern SIEM Systems;
Autors: Florian Menges, Tobias Latzo, Manfred Vielberth, Sabine Sobola, Henrich C. Pöhls, Benjamin Taubmann, Johannes Köstler, Alexander Puchta, Felix Freiling, Hans P. Reiser, Günther Pernul.
Data publicació: 31 desembre 2020;

Annexes

- Arxiu: une-en_iso-iec_27001.pdf
  Detall: Document Norma Española UNE-EN ISO/IEC 27001 Mayo 2017

- Arxiu: PAC1_Gantt.cdpz & PAC1_Gantt.pdf
  Detall: Diagrama de Gantt realitzat amb l'aplicació Concept Draw.

- Arxiu: Azure ACME infrastructure.vsd
  Detall: Representació gràfica global de la infraestructura de l'empresa fictícia ACME, realitzat amb l'aplicació Microsoft Visio Standard.

- Arxiu: Azure ACME subscriptions.vsdx
  Detall: Representació gràfica detallada de les subscripcions de la infraestructura de l'empresa fictícia ACME, realitzat amb l'aplicació Microsoft Visio Standard.

- Arxiu: Presentació_TFM.pptx
  Detall: Presentació del treball, realitzada amb Microsoft PowerPoint.

- Arxiu: Video_Presentacio_tfm.mp4
  Detall: Gravació format vídeo de la defensa del TFM.