SOLUCIÓN DE CIBERSEGURIDAD APLICADA AL VEHÍCULO CONECTADO

Universitat Oberta de Catalunya

Jordi Nogués López

Junio 2023

AGENDA

Objetivos y enfoque

Comprender los riesgos de ciberseguridad del Vehículo Conectado, y cómo abordarlos

Tecnologías de comunicación
Análisis de los protocolos DSRC, ITS-G5 y 5G-V2X desde el punto de vista de los riesgos vinculados a posibles intrusiones a través de las comunicaciones.

Marco regulatorio
Estudio de la normativa de seguridad UNECE WP.29, aplicable en la industria del automóvil, sus actuales retos y plazos de cumplimiento.

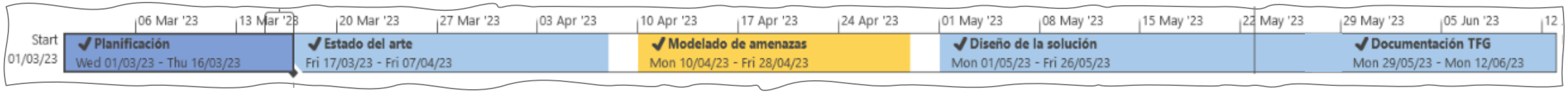
Solución de ciberdefensa
Evaluación de los requisitos, selección de la tecnología, definición de la arquitectura, e implementación de un caso de uso en el laboratorio.

Anatomía del vehículo
Análisis de la arquitectura de comunicaciones inter e intra-vehiculares y sus componentes principales: bus CAN, ECUs y OBU.

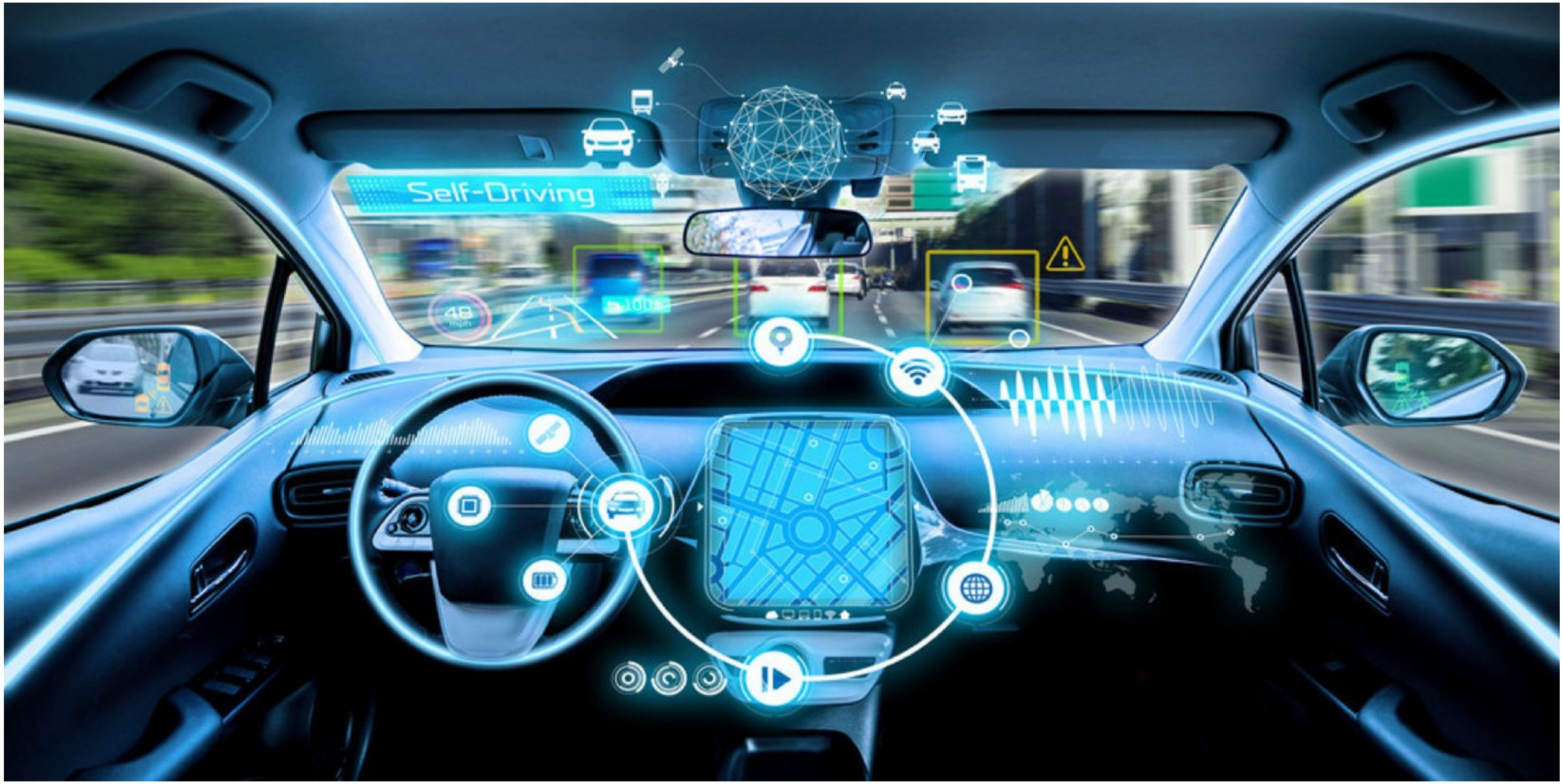
Amenazas de ciberseguridad
Investigación de las posibles vulnerabilidades y amenazas de ciberseguridad, y de las tácticas, técnicas y procedimientos de los adversarios.

Metodología – Fases y actividades

3 semanas	3 semanas	3 semanas	4 semanas	2 semanas
Definición de objetivos, enfoque, alcance y entregables. Elaboración del calendario de trabajo.	Estado del arte de las comunicaciones y del marco regulatorio. Selección de la línea de investigación.	Estudio de vulnerabilidades. Estrategias de gestión de riesgos. Análisis de dos casos de estudio.	Definición de los requisitos. Diseño de la arquitectura. Implementación de un caso de uso.	Elaboración de las conclusiones. Documentación de la memoria. Autoevaluación.

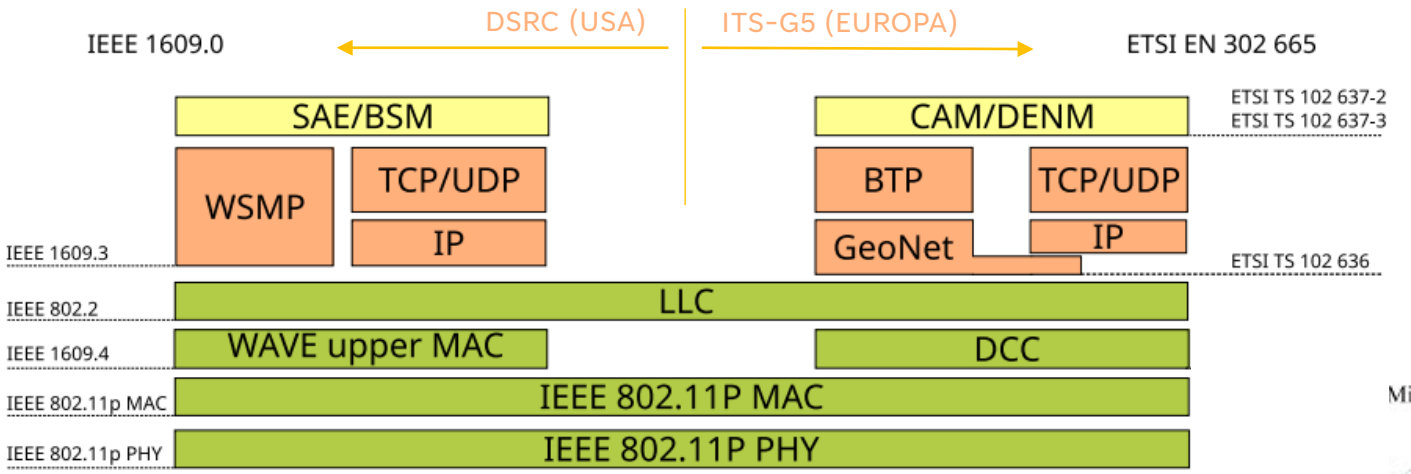


Tecnologías de comunicación v2x

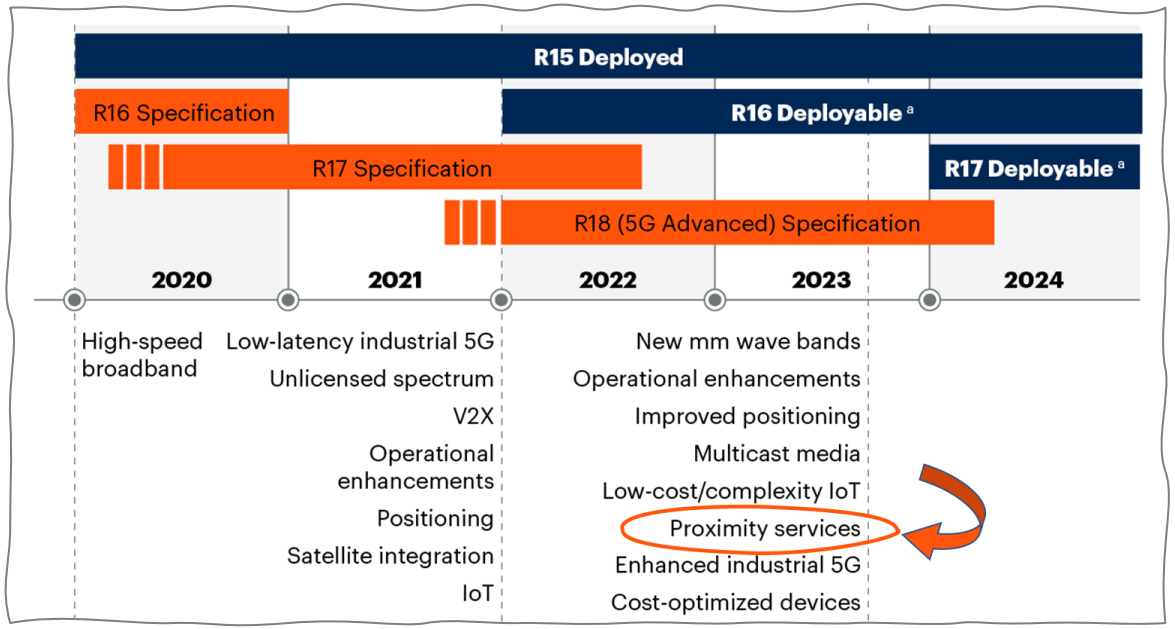


Tecnologías de comunicación V2X

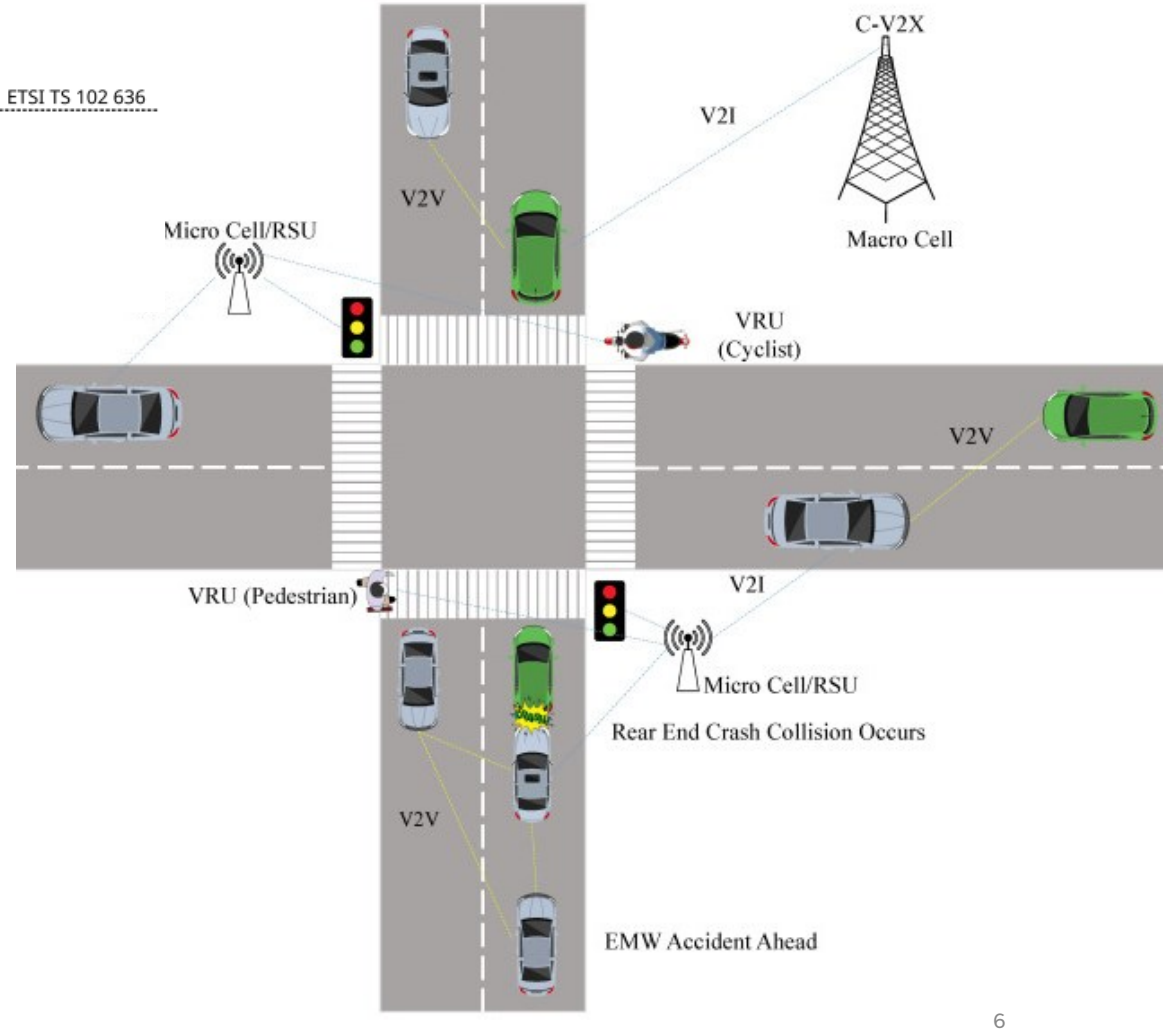
BASADAS EN WIFI



HOJA DE RUTA DEL 3GPP



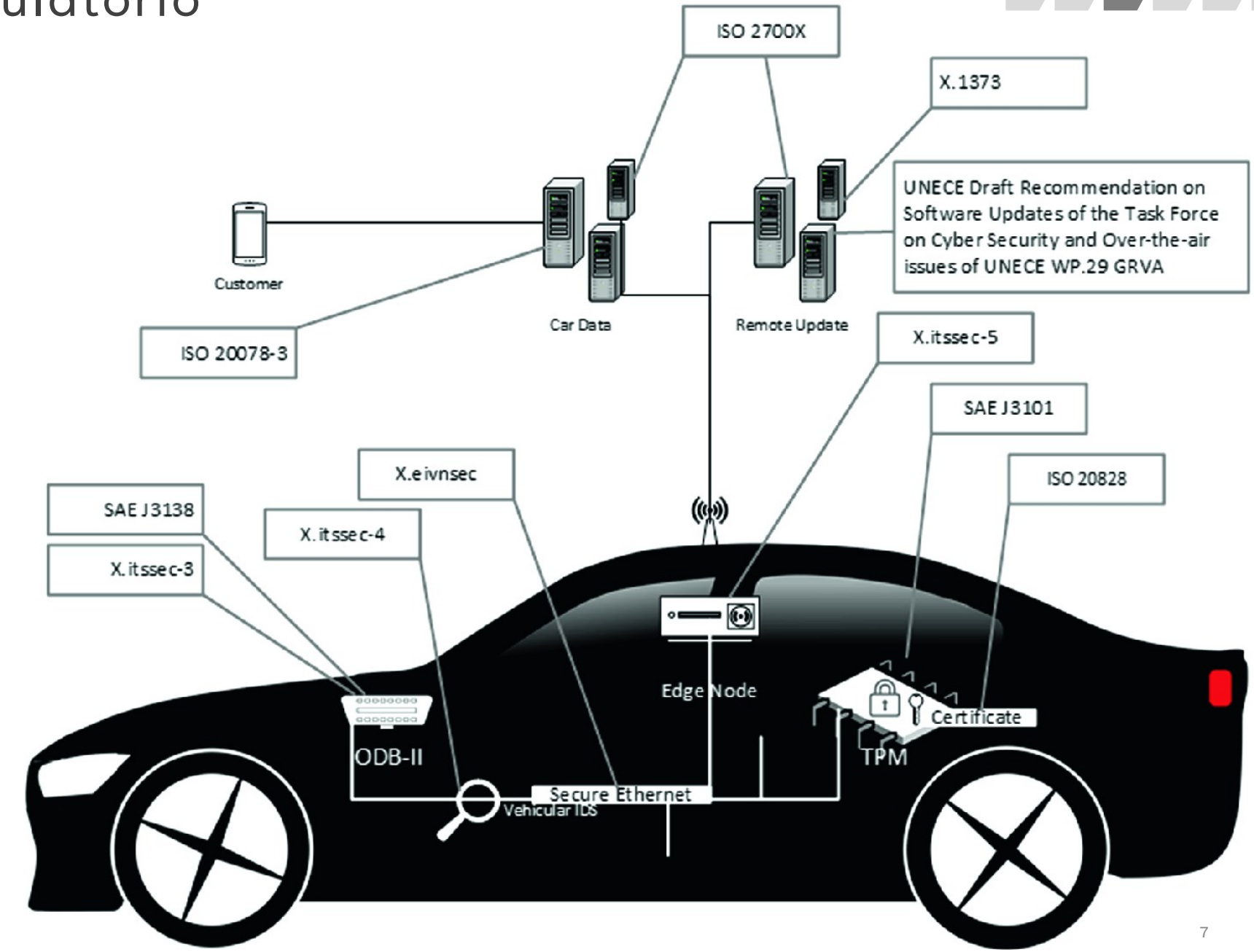
ESCENARIO V2X



Marco regulatorio

A lo largo del tiempo, diferentes organismos (ISO, SAE, ETSI, ITU…) han ido desarrollando distintos grupos de estándares a medida que aparecían nuevos elementos en el ecosistema de los Sistemas Inteligentes de Transporte.

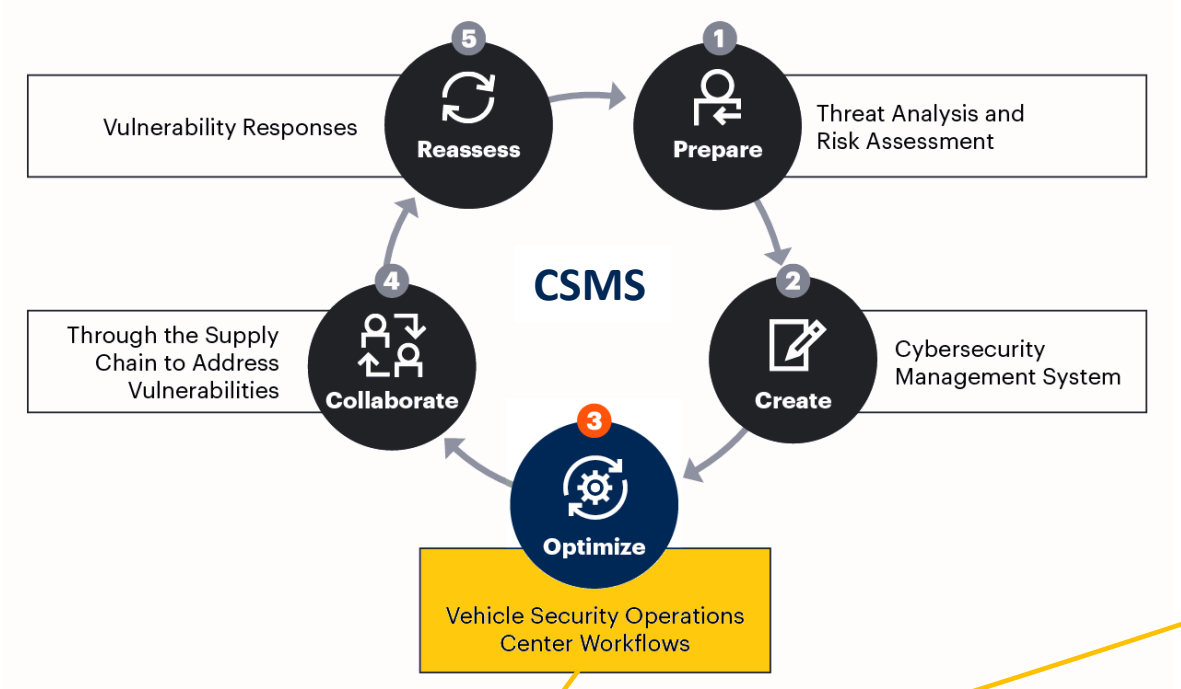
La falta de una regulación global ha provocado carencias y también solapes entre los distintos organismos, y por ese motivo la Comisión Económica de las Naciones Unidas para Europa ha desarrollado nuevos aspectos en su acuerdo **UN ECE WP.29** para la armonización de la reglamentación sobre Vehículos, centrados principalmente en la **implantación de un Sistema de Gestión de la Ciberseguridad.**

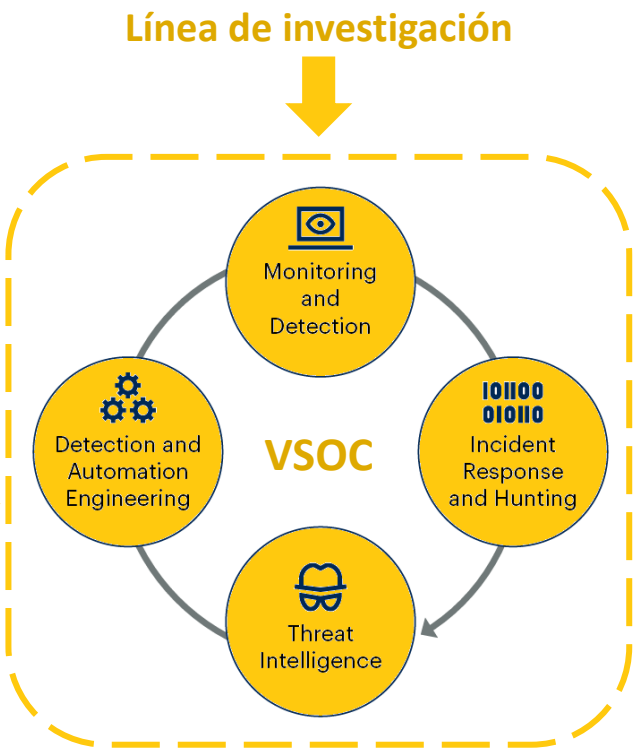


Marco regulatorio

La normativa **UN ECE WP.29** establece 2 requisitos de **cumplimiento obligatorio** para todos los vehículos que se fabriquen a partir de **julio de 2024**:

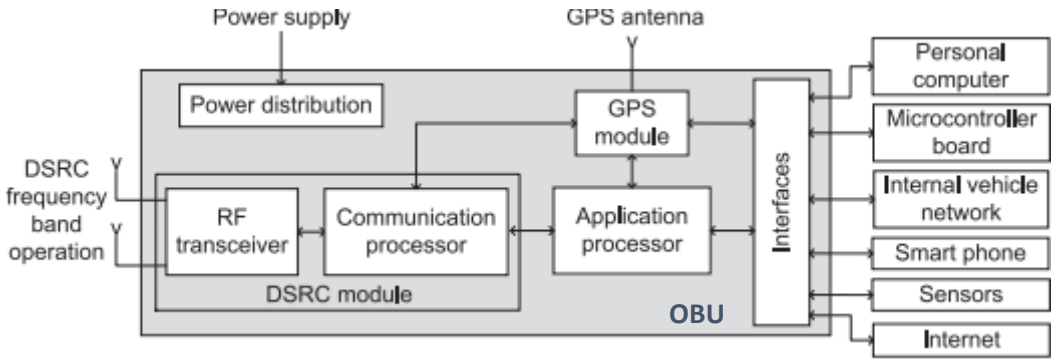
- **R155** (CSMS): Gestión de la ciberseguridad
- R156 (SUMS): Gestión de las actualizaciones del software

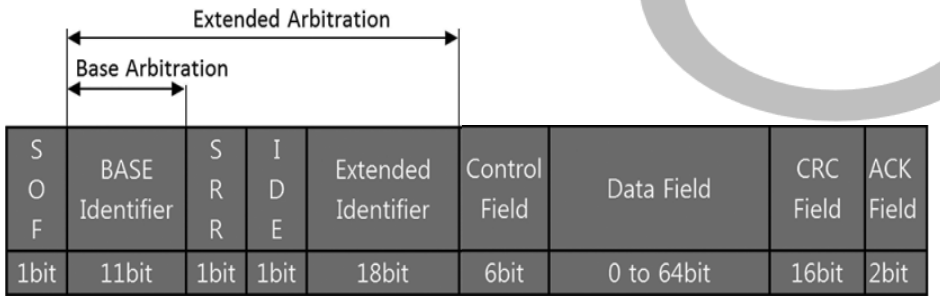




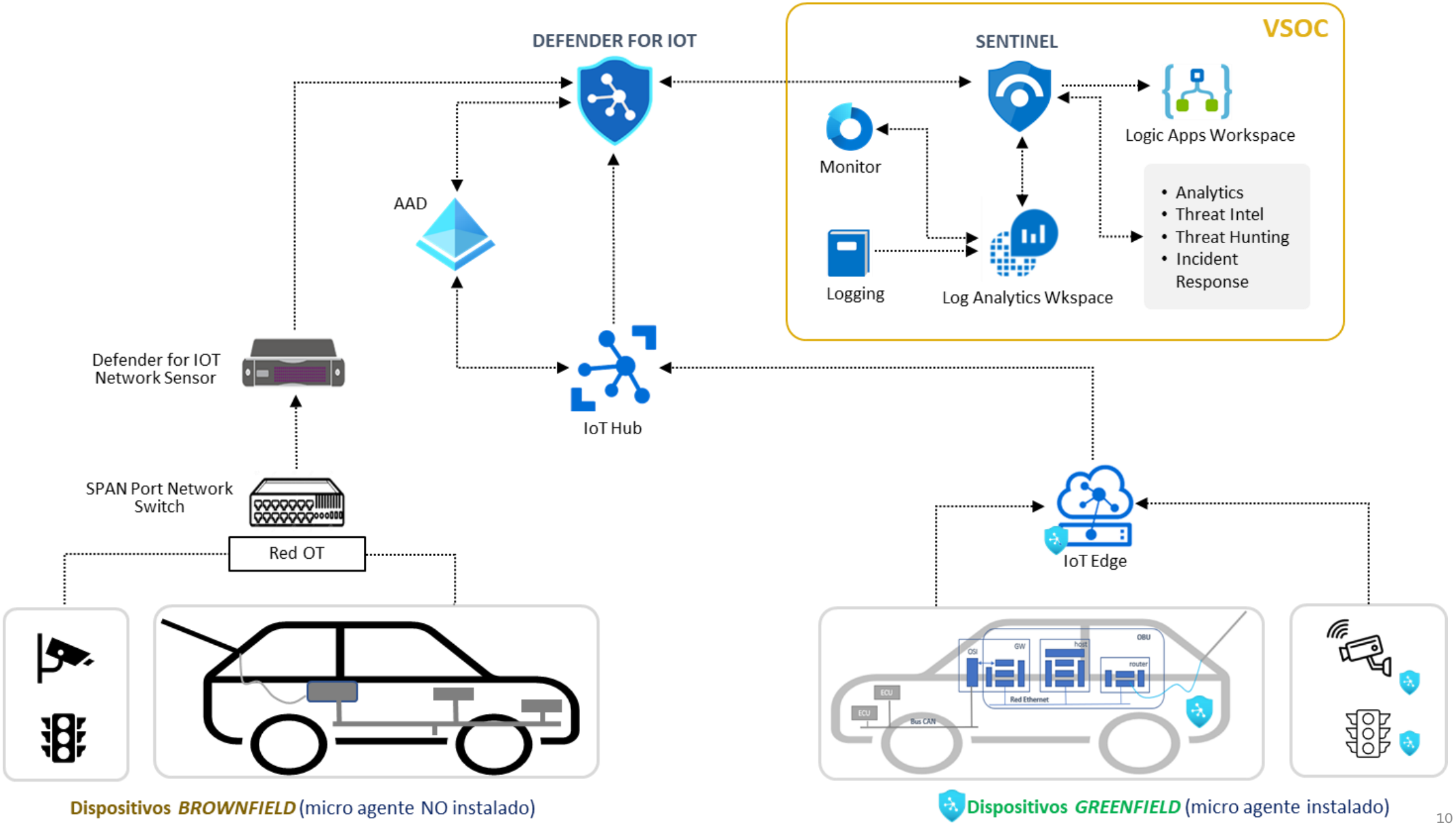
"La ciberseguridad es una lucha sin fin, en la que sólo es cuestión de tiempo que una vulnerabilidad llegue a ser explotada."

Anatomía del vehículo conectado

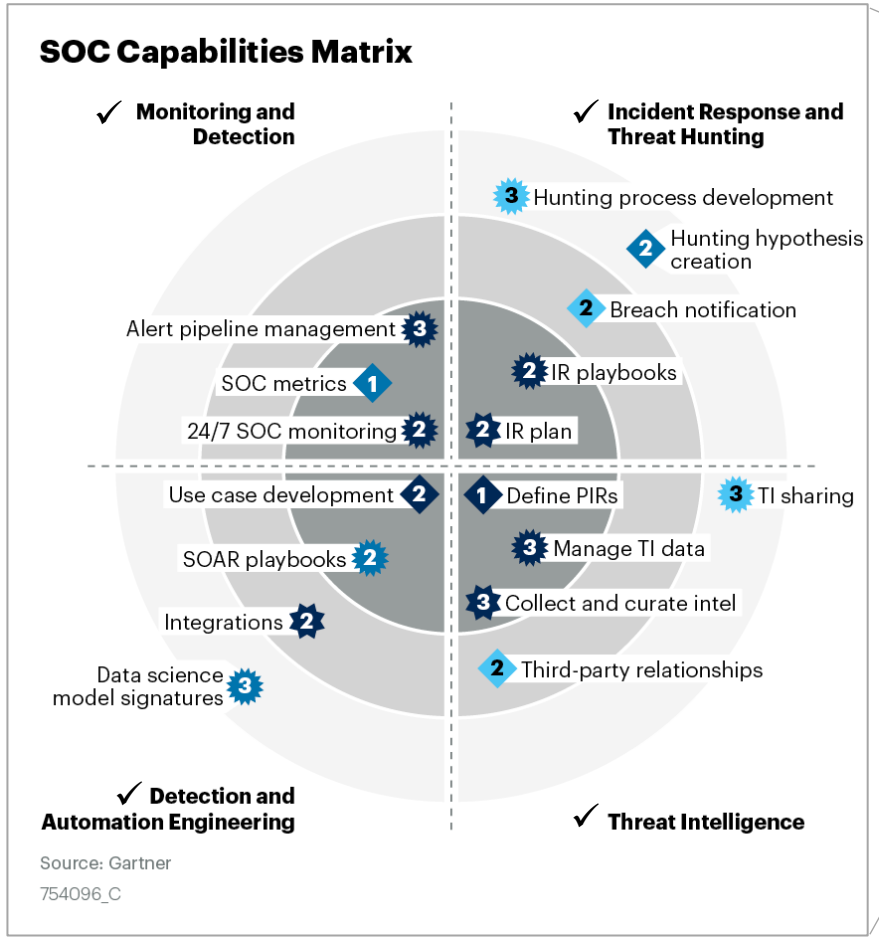




Ecosistema de la solución



Solución VSOC



VSOC

Sentinel

- ✓ Monitorización
- ✓ Threat Hunting
- ✓ Threat Intelligence
- ✓ Reglas automáticas

Logic Apps Workspace

Logging

Log Analytics Workspace

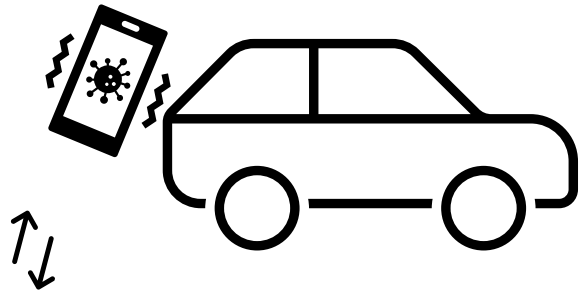
Monitor

Eventos de seguridad

Caso de uso - Contexto

Escenario: Presencia de mensajes maliciosos en la red interna del vehículo

1

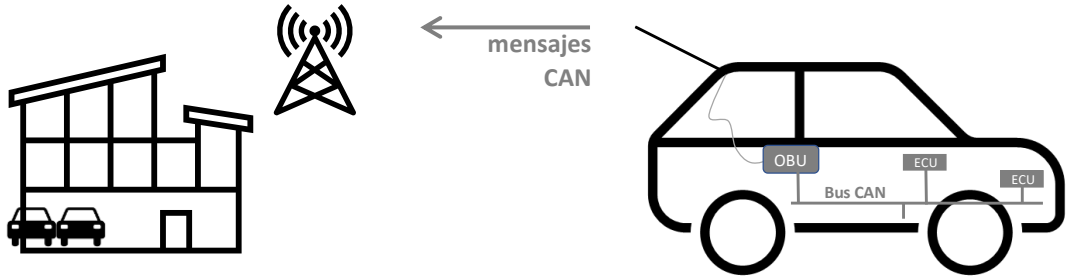


La víctima ha instalado en su smartphone una **aplicación de diagnósticos** sin advertir que es falsa **(maliciosa)**. El smartphone infectado se empareja por Bluetooth al conector OBD-II de su vehículo a través de un adaptador ELM327.

2

La aplicación se conecta por Internet a un servicio web malicioso desde el que el atacante puede **obtener información del vehículo** y controlar su comportamiento mediante el **envío de comandos** AT.

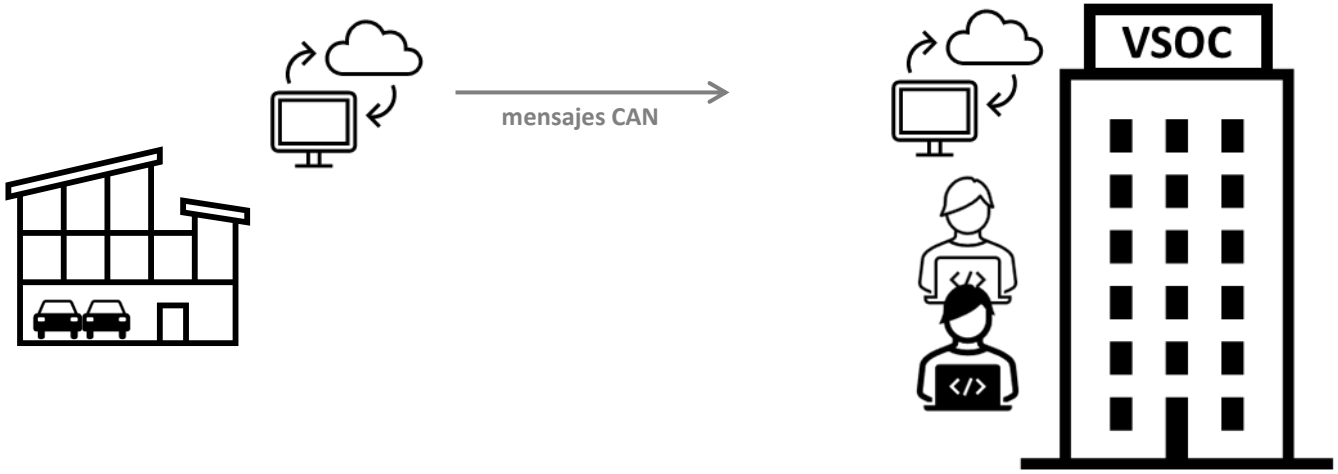
3



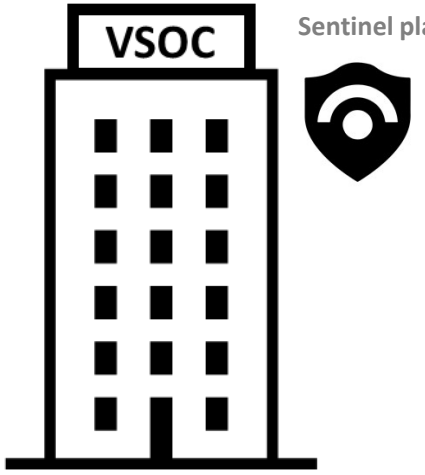
El automóvil incorpora una tarjeta eSIM para conexión telefónica con el concesionario, y le **envía muestras de los mensajes** de diagnóstico que circulan por el bus CAN.

Caso de uso - Solución

1 El concesionario transforma y reenvía en tiempo real al VSOC los mensajes de de la flota.

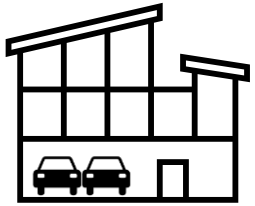


2 El VSOC dispondrá de un automatismo para este caso de uso, y actuará en función del nivel de severidad del incidente.



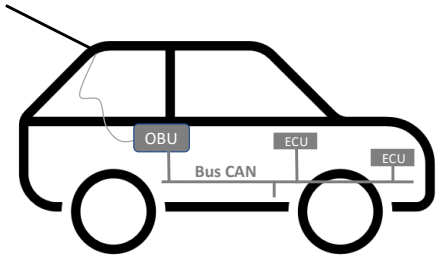
Sentinel playbook

(a) Alerta – ID desconocido



Si el mensaje presenta un ID de ECU no conocido, envía una alerta por email al concesionario para que lo verifique

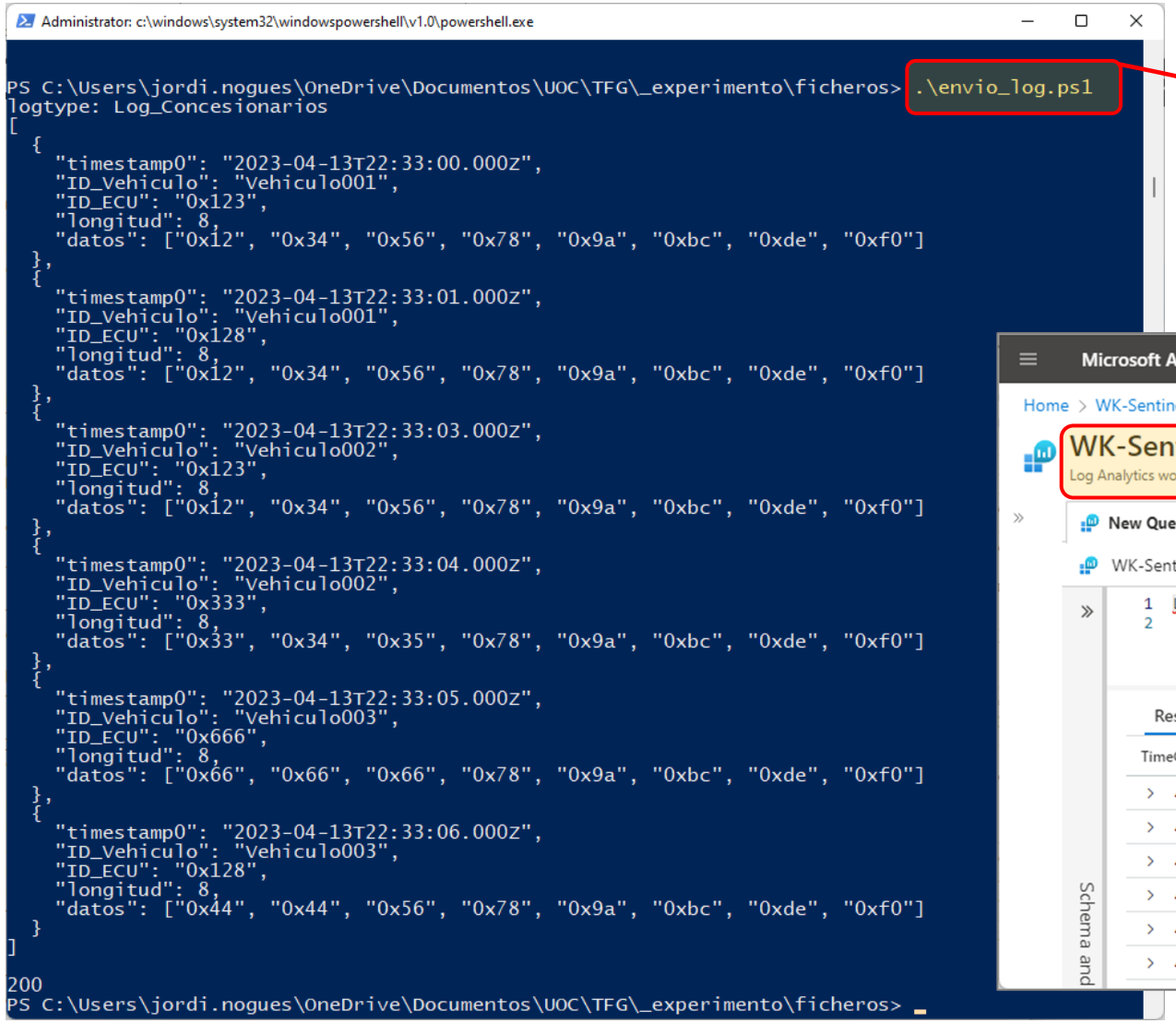
(b) Incidente confirmado



Si el mensaje presenta un ID que está reportado como malicioso, se enviará una llamada de emergencia directamente al propio vehículo para advertirle que se ha producido un incidente de seguridad y debe dejar de circular urgentemente

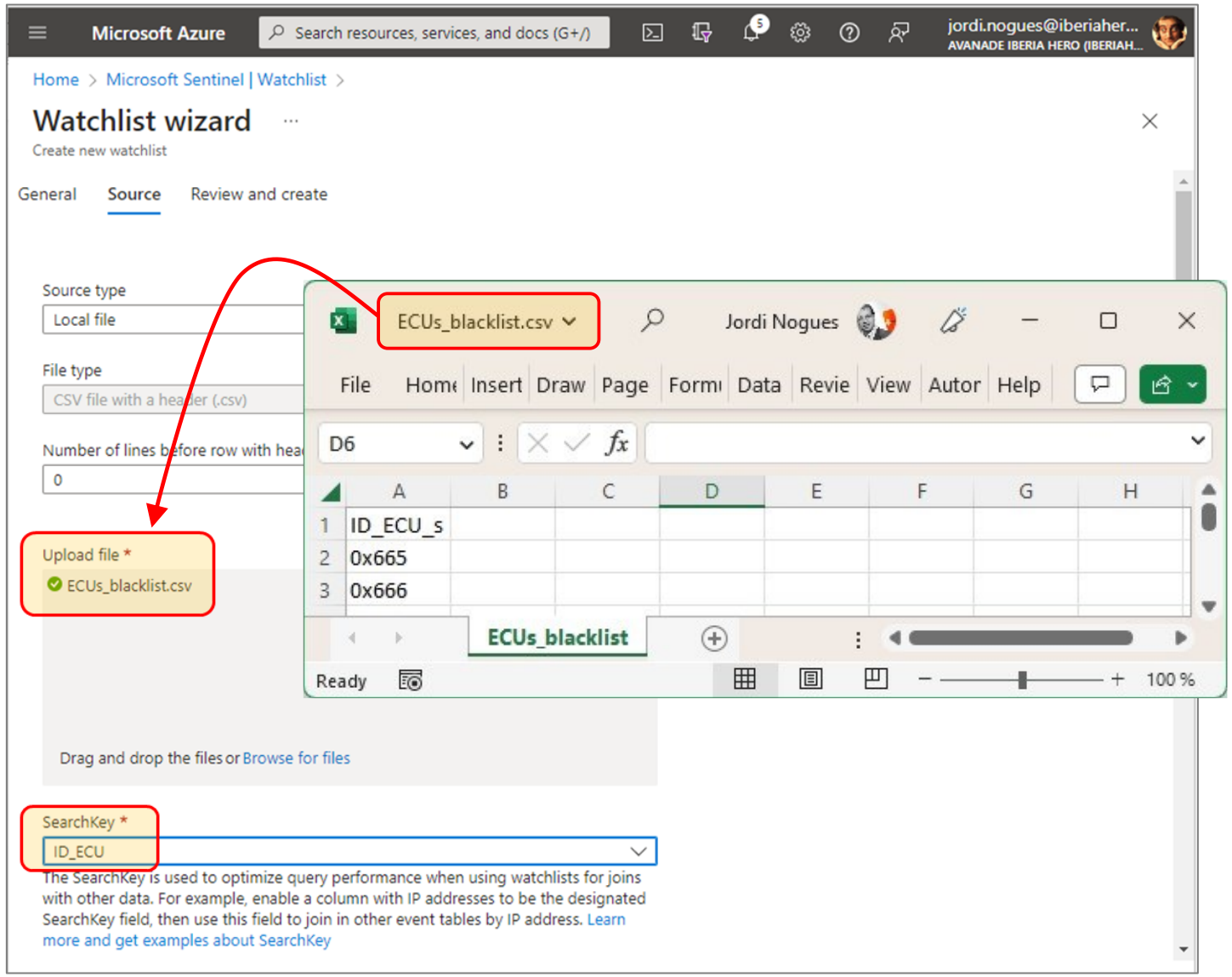
Experimento (1/4)

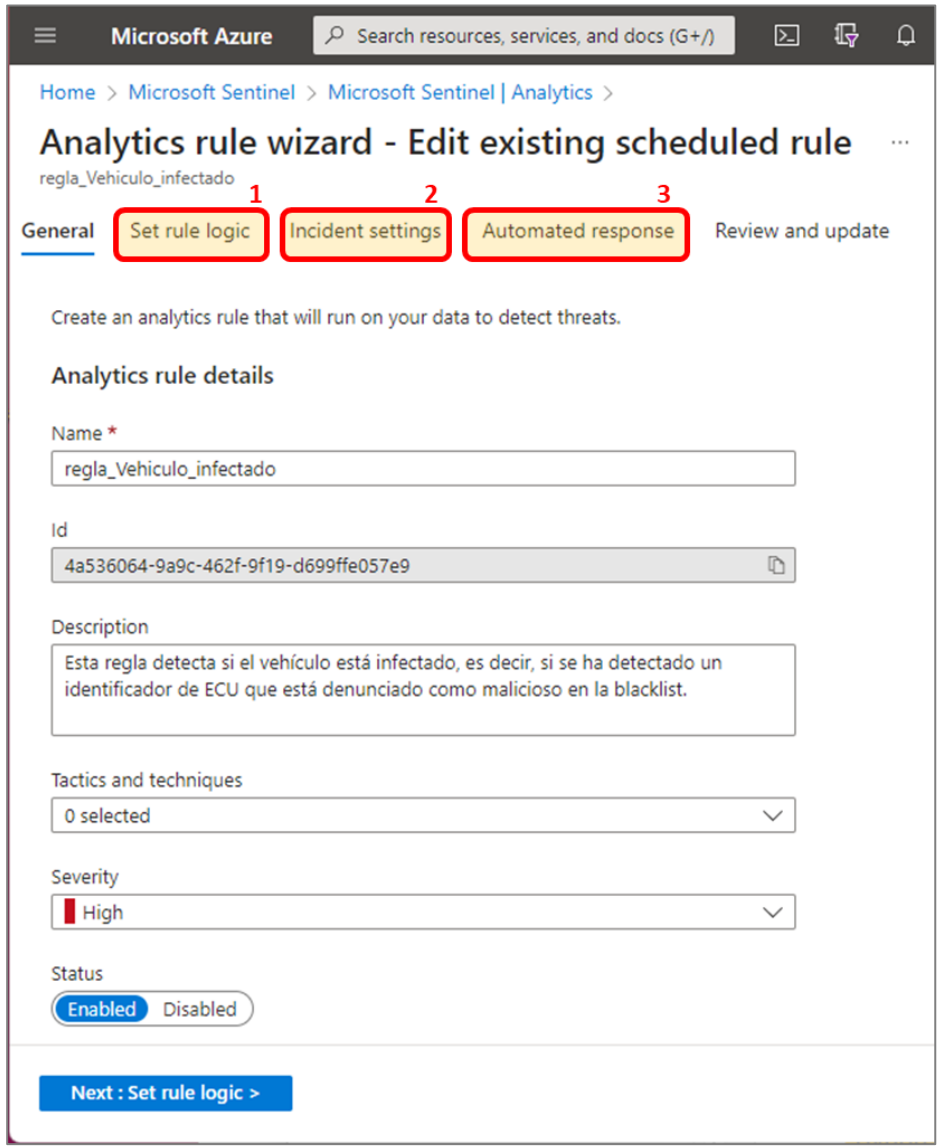
Envío de los mensajes CAN desde el concesionario al VSOC



Experimento (2/4)

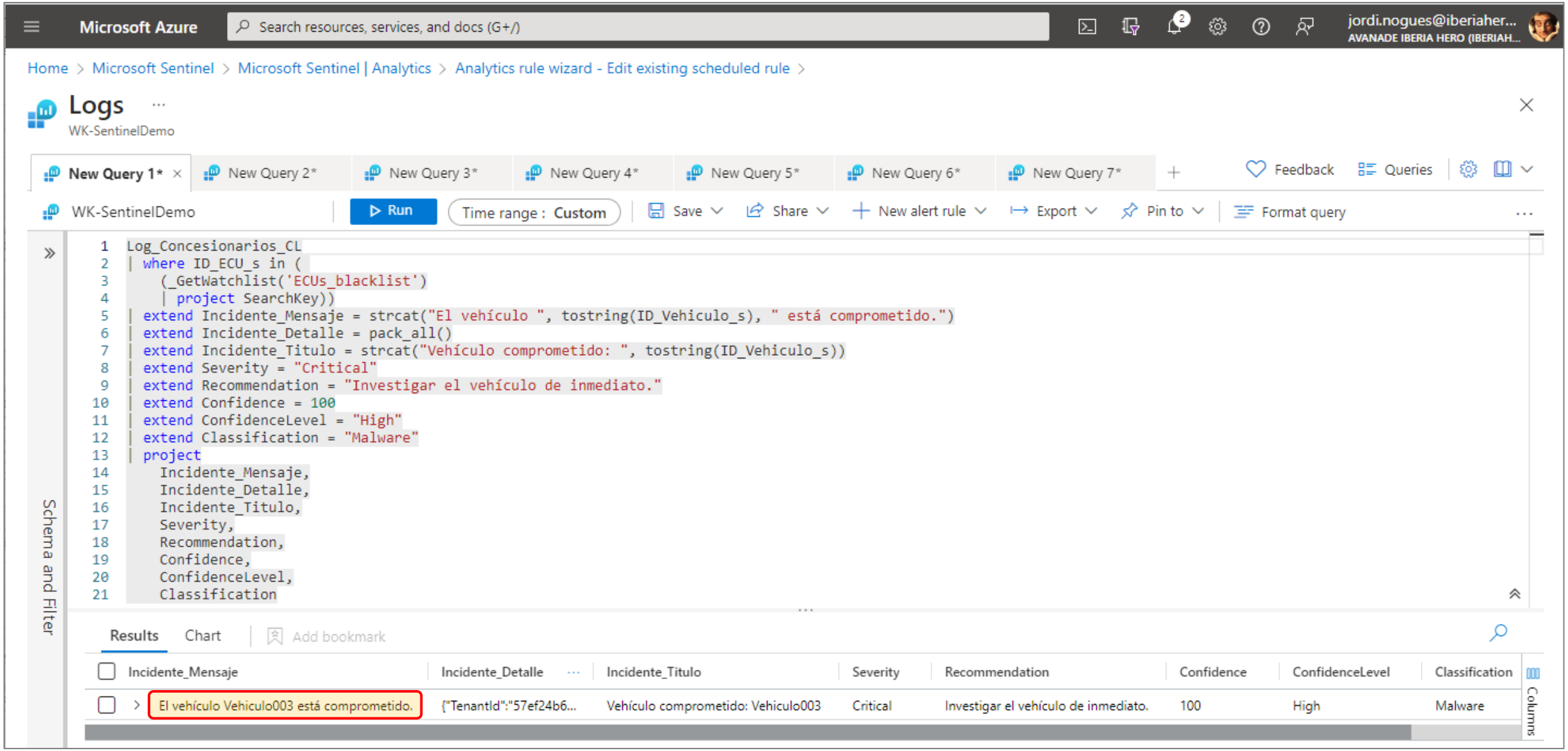
Definición de la *blacklist*, y creación de la regla





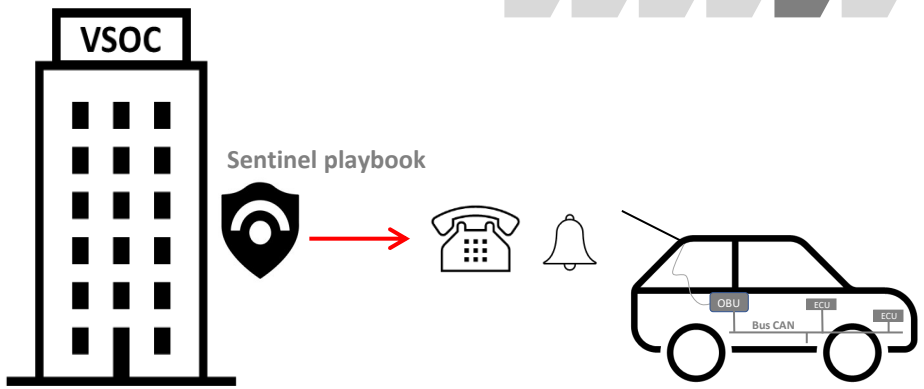
Experimento (3/4)

Detección del incidente



Experimento (4/4)

Respuesta automática (playbook)



Microsoft Azure | Search resources, services, and docs (G+/) | jordi.nogues@iberiaher... AVANADE IBERIA HERO (IBERIAH...

Home > LlamarVehiculoJN >

Logic Apps Designer

Save | Discard | Run Trigger | Designer | Code view | Parameters | Templates | Connectors | Help | Info

Microsoft Sentinel incident

HTTP

* Method: POST

* URI: https://api.twilio.com/2010-04-01/Accounts/{AccountSID}/Calls.json

Headers

Authorization	'Basic ' + base64('SK9e85ca36b97da26748 d03f8656b5b96:Cdj8LbYG16gOptIPO9FvA 46DeCDkH8Z')
Content-Type	application/x-www-form-urlencoded
Enter key	Enter value

Queries

Enter key	Enter value

Body

'From=' + encodeUriComponent('+16205220849') + '&To=' + encodeUriComponent('+346 + '&Url=' + encodeUriComponent('https://www.learningcontainer.com/wp-

Microsoft Azure | Search resources, services, and docs (G+/) | jordi.nogues@iberiaher... AVANADE IBERIA HERO (IBERIAH...

Home > Logic apps >

LlamarVehiculoJN

Logic app

Run Trigger | Refresh | Edit | Delete | Disable | Update Schema | Clone | Open in mobile | Export

Introducing the new portable Logic Apps runtime that supports local development and debugging. Click to learn more. →

Essentials — JSON View

Resource group (move): RG-SECURITY-TEAM
Location: West Europe
Subscription (move): SA-MAPS-Iberia Lab
Subscription ID: db600528-5207-4293-91a2-a8144db2dbdf
Definition: 1 trigger, 1 action
Status: Enabled
Runs last 24 hours: 0 successful, 10 failed
Integration Account: -- --

Get started | Runs history | Trigger history | Metrics

All | Start time earlier than | Pick a date | Pick a time

Specify the run identifier to open monitor view directly

Status	Start time	Identifier	Duration	Static Results
Succeeded	4/18/2023, 10:21 PM	08585197576178950960018825897CU...	498 Milliseconds	

Conclusiones

En cada etapa de este proyecto se han generado reflexiones de diversa índole:

Etapa	Conclusiones
Estado del arte de las comunicaciones V2X	• La continua evolución del 3GPP en su hoja de ruta habilita de forma sistemática nuevos escenarios de uso y de negocio, lo que a su vez origina **nuevas superficies de ataque**.
Análisis del marco regulatorio	• 60 países –incluyendo España- han adoptado la reglamentación de las Naciones Unidas UNECE WP.29, la cual impone unos requisitos de seguridad para la industria automotriz que serán de obligado cumplimiento a partir de **julio de 2024**. Entre ellos, la **implantación de un Centro de Operaciones de Seguridad Vehicular** (VSOC).
Arquitectura de la solución	• Según el último Magic Quadrant de Gartner, la tecnología líder para la implantación de un SOC es **Microsoft Sentinel**, por sus capacidades SIEM y SOAR. • En la **seguridad IoT**, se pueden aplicar soluciones análogas a las de las redes de ordenadores, pero se requieren estrategias específicas en varios aspectos, principalmente en los procesos de recolección de los registros de actividad y en los de detección de amenazas.

Próximos pasos

Aunque se han logrado los objetivos establecidos, la contribución de este proyecto como guía para la implementación de un Centro de Operaciones de Seguridad en el ámbito del vehículo conectado solamente representa un primer paso dentro de un proceso mucho más amplio y complejo.

Se ha desarrollado un caso de uso relativamente sencillo, basado en la identificación de códigos de dispositivo (ECUs) reportados como maliciosos en una "blacklist", para gestionarlos de forma análoga a los IoCs (Indicadores de Compromiso) que típicamente proporcionan las fuentes de *Threat Intelligence* con direcciones IP o hashes de archivos identificados como maliciosos, pero existen muchos más casos de uso a explorar, como aquellos basados en mecanismos de inteligencia artificial, por ejemplo:

- Recepción de códigos no habituales
- Contenido atípico en los mensajes
- Frecuencia de envíos atípica

En resumen, se ha aplicado un enfoque de "producto mínimo viable" para ilustrar adecuadamente los beneficios potenciales de la solución y su lógica de funcionamiento, pero limitado por los plazos que exige un Trabajo de Final de Grado. Por lo tanto, este proyecto está abierto a una posible continuidad, quizás en un futuro Trabajo de Fin de Máster.


Gracias!