

MDR, OT and Automotive Security trends

Bartosz Czyzewski, Eviden

Mindshare 2023
September 19th/20th

A front-facing view of a classic Ferrari sports car, likely a 250 GT, featuring a prominent chrome grille with the Ferrari logo, round headlights, and a steering wheel visible through the windshield. The car is set against a light background with a dark grey geometric shape in the upper right corner.

Automotive security

In a past it was...



..just a production line of the car in time-laps

From manual craftwork to semi-automation

1950



1970



..just a production line of the car in time-lapse
From automation to full digitalization

1990



2020



The mobility use cases



Vehicle
2 Grid



Vehicle 2
Infrastructure



Vehicle 2
Vehicle



Vehicle 2
Network



Vehicle 2
Cloud



Vehicle 2
Device



Vehicle 2
Pedestrians

Software
Development
Life Cycle

MDR

Intrusion Prevention
& Detection Systems

FOTA
update

Vulnerabilities

Events

Security
incidents

PKI



Phishing

MFA

Physical
Security

Proxy

API Security

Encryption

Firewalls

Cloud Security

Vehicle security ecosystem is very complex

The next target for cybercriminals - Connected cars

How I got access to 25+ Tesla's around the world. By accident. And curiosity.

David Colombo

Presented by David Colombo

2nd June 2022 - 13:30 PT

Google Offices



INNOVATION

The Connected Car Is The Next Attack Vector



Nic Surpatanu Brand Contributor

Tanium BRANDVOICE | Paid Program

Sep 7, 2022, 09:21am EDT

IOT SECURITY

16 Car Makers and Their Vehicles Hacked via Telematics, APIs, Infrastructure

A group of seven security researchers have discovered numerous vulnerabilities in vehicles from 16 car makers, including bugs that allowed them to control car functions and start or stop the engine.



By Ionut Arghire
January 5, 2023



Millions of cars' anti-theft systems vulnerable to hacking

By E&T editorial staff

Published Friday, March 6, 2020

The next target for cybercriminals - Connected cars

How I got access to 25+ Tesla's around the world. By accident. And curiosity.

David Colombo

Presented by David Colombo

2nd June 2022 - 13:30 PT

Google Office



INNOVATION

The Connected Car Is The Next Attack Vector

TANIUM

Nic Surpatanu Brand Contributor

Tanium BRANDVOICE | Paid Program

Sep 7, 2022, 09:21am EDT

IOT SECURITY

16 Car Makers and Their Vehicles Hacked via Telematics, APIs, Infrastructure

A group of seven security researchers have discovered numerous vulnerabilities in vehicles from 16 car makers, including bugs that allowed them to control car functions and start or stop the engine.



By Neil Arghve
January 5, 2023



Millions of cars' anti-theft systems vulnerable to hacking

By E&T editorial staff

Published Friday, March 6, 2020

Most common incidents:

Data/Privacy Breach – 31%

Service/Business... – 23%

Car Theft/Break-ins – 22%

Control of Car... – 13%

Car System... – 3%

Location Tracking – 3%

Fraud – 3%

Policy Violation – 1%

Malware – 1%

Ransomware – 0,1%


Car system... – 0,1%

Source: Upstream

MDR for Automotive

Key Features

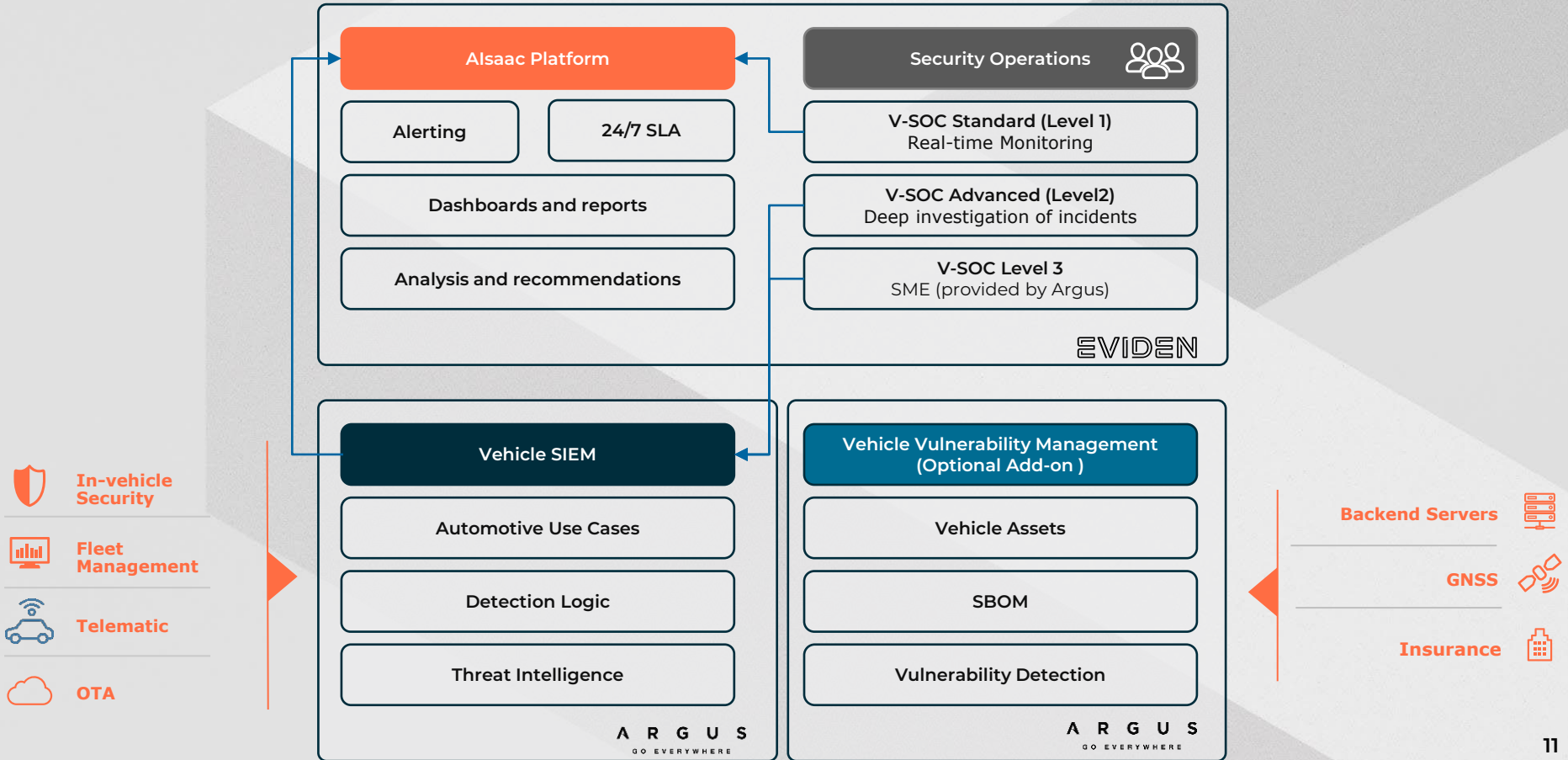
- Continuous **monitoring** for suspicious behaviors by the V-SOC
- Automotive cyber security experts to **investigate** and analyze incidents
- Reduced **response time** to minimize the impact of security incidents
- Relevant reporting to help meeting cybersecurity **regulations**
- Advanced detection of cyber threats based on **top security technology** for Automotive
- Reduce the **risk of fraud** in connected vehicles



End-to-end service for
automotive cyber security
and compliance

MDR for Automotive – Overview

Incident Management and Response

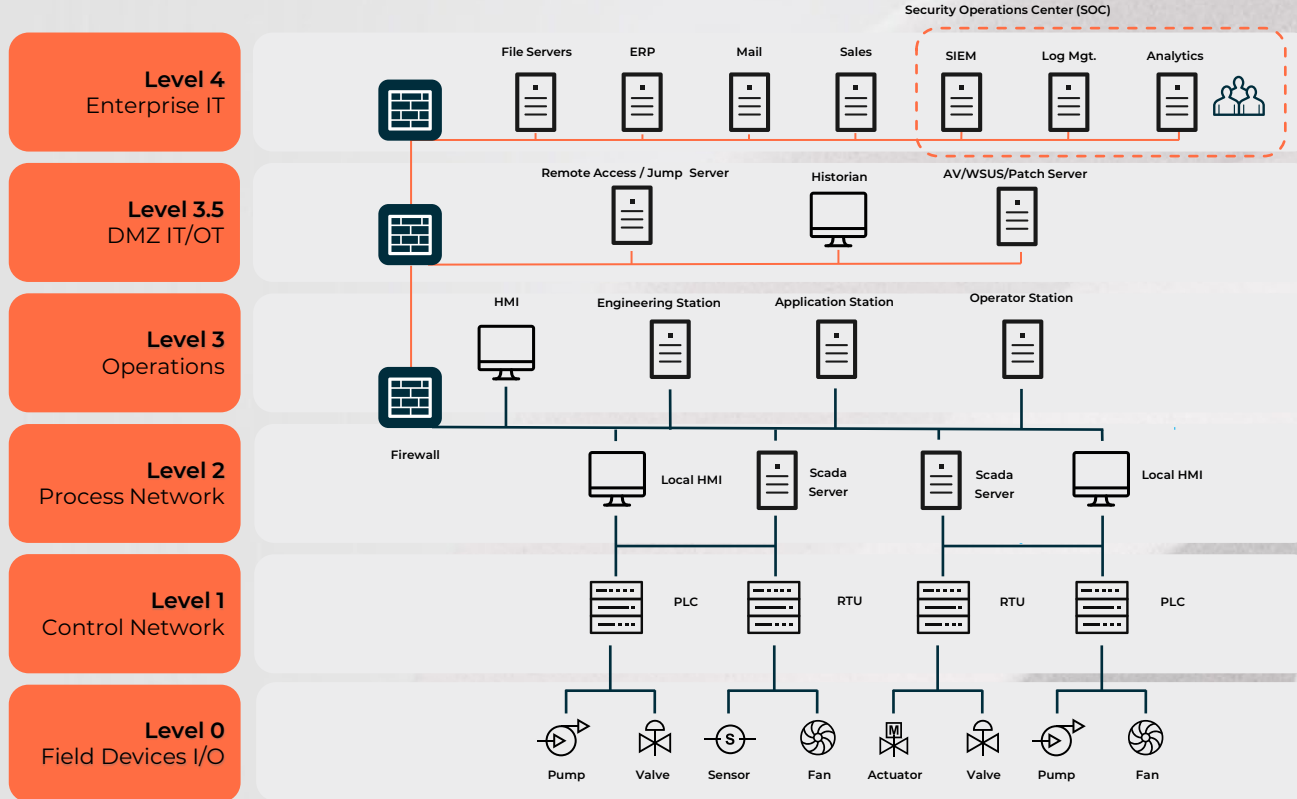


Industrial Security



Purdue Model

ICS Network Segmentation



MODERN Purdue Model



Colonial Pipeline Attack

One of the largest publicly disclosed attack against critical infrastructure

Target

Colonial Pipeline



Targeted systems

Computer systems including billing and accounting



Consequences

The pipeline was shut down for 6 days causing gas shortage and affecting consumers and the airline on the East Coast.



Date

May 2021

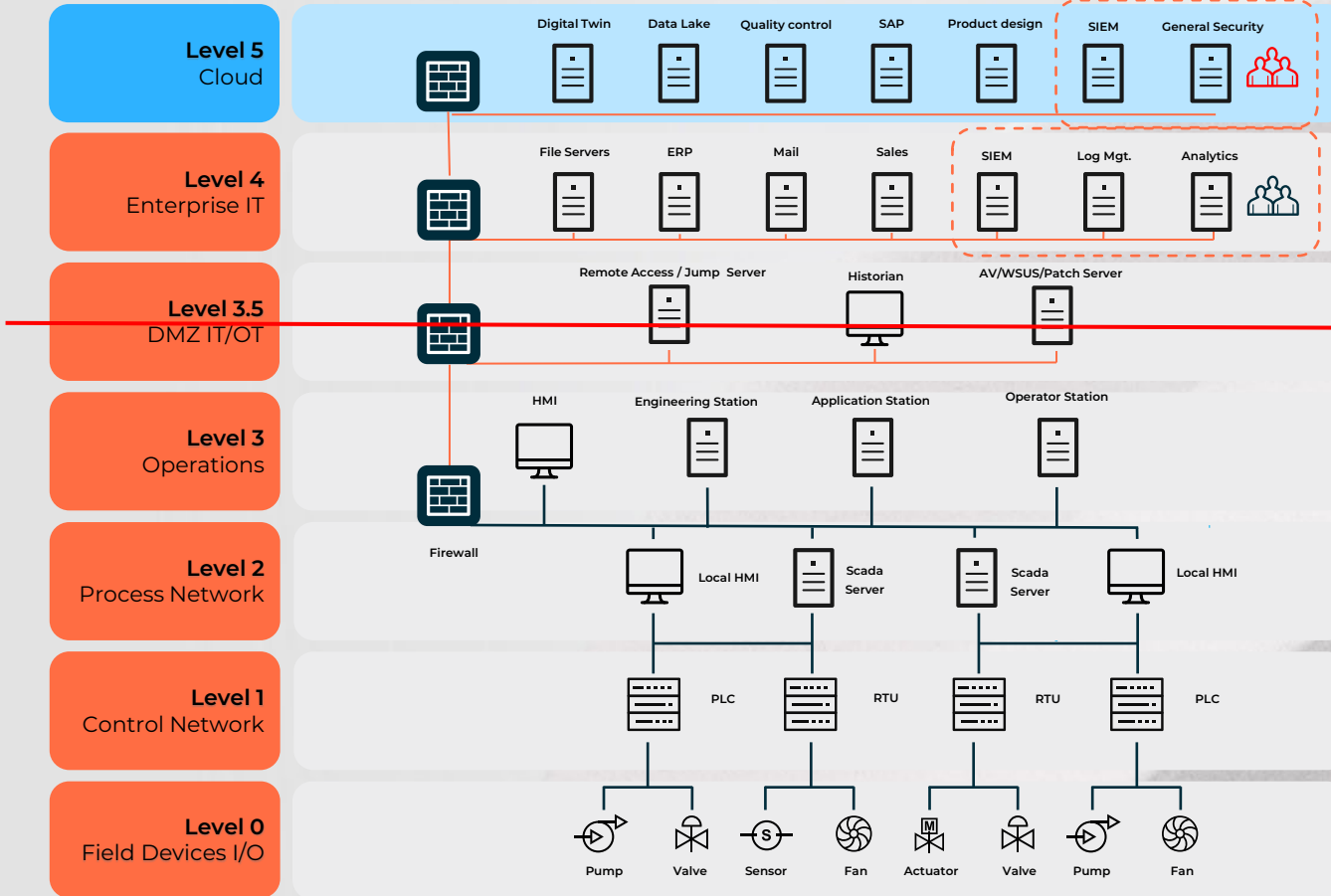


Method

A hacker group breached the Colonial Pipeline network and stole 100 gigabytes of data



MODERN Purdue Model



IT Standard tools

OT Dedicated tools & technics



A top-down view of a car body on an assembly line. The car is positioned in the center, with several yellow robotic arms surrounding it. The background is a grey, perforated metal surface. The text "Forward thinking" is overlaid in orange.

Forward thinking

Future threats – Foresight 2030

Based on recent ENISA Threat Report

HUMAN ERROR AND EXPLOITED LEGACY SYSTEMS WITHIN CYBERPHYSICAL ECOSYSTEMS

TARGETED ATTACKS (E.G. RANSOMWARE) ENHANCED BY SMART DEVICE DATA

LACK OF ANALYSIS AND CONTROL OF SPACE BASED INFRASTRUCTURE AND OBJECTS

RISE OF ADVANCED HYBRID THREATS

SKILL SHORTAGES

[Foresight 2030 Threats – ENISA \(europa.eu\)](https://www.europa.eu)

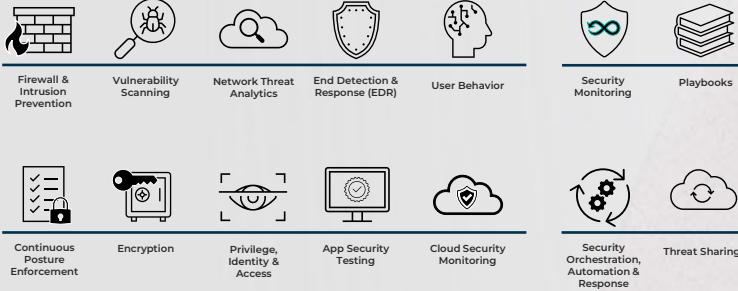
MDR/SOC IT/OT/IoT/IIoT Capabilities

MDR/SOC IT/OT/IoT/IIoT

MDR for IT/OT/IoT/IIoT based on AlsaaC

SOC for IT/OT/IoT/IIoT based on SIEM & SOAR

MDR / SOC for IT/OT/IoT/IIoT based on Cybersecurity Solutions



OT Network Segmentation



OT & IoT Network Security and Asset Visibility



Secure Remote Access



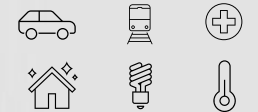
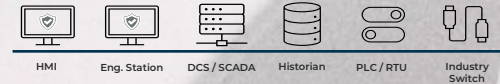
OT & IoT Endpoint Security



OT, IoT Compliance & Risk Management Platform



Other Industry-specific vendors



Questions

