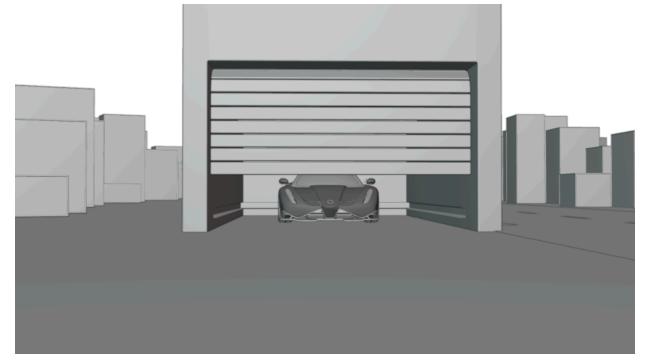
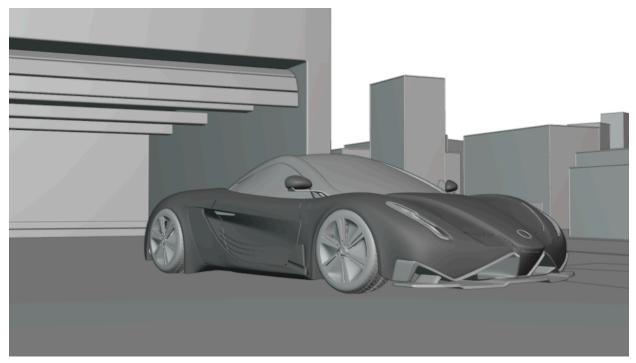
CARALERT storyboard

Introduction-Security

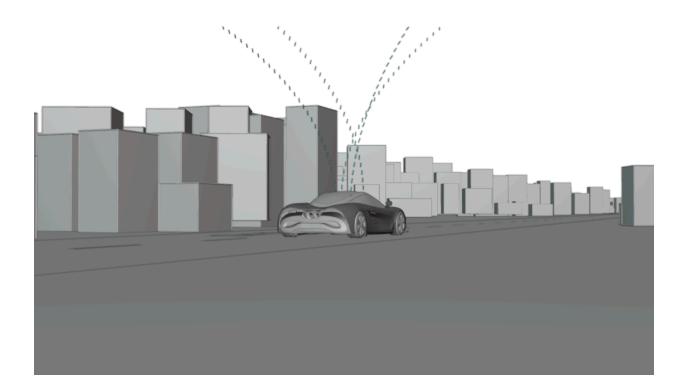
[Music starts playing, garage door opens, our car is revealed]



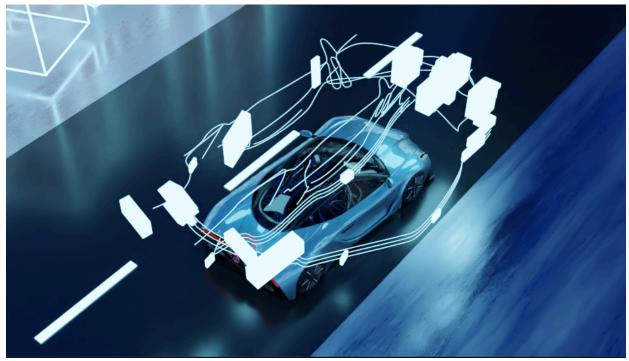
Narration: Today's cars are essentially computers on wheels



[As the car drives out of the garage in a futuristic city, communication signals of different sorts interact with the vehicle]



With up to 150 ECUs,



[a complex network of ECU's is showen and they fly into the car]



hundreds of millions of lines of code,

[code is presented in several dynamic windows, different programming languages, one by one the flow into the car as well]



[Code is compiled and enters the car]



and many interfaces-



vehicles are becoming prime targets for cyberattacks.

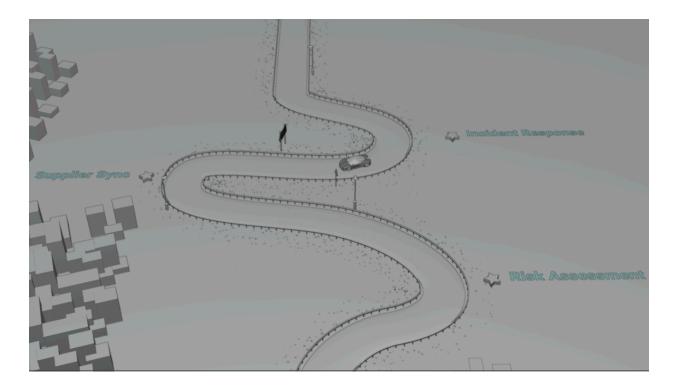


Introduction-Regulation

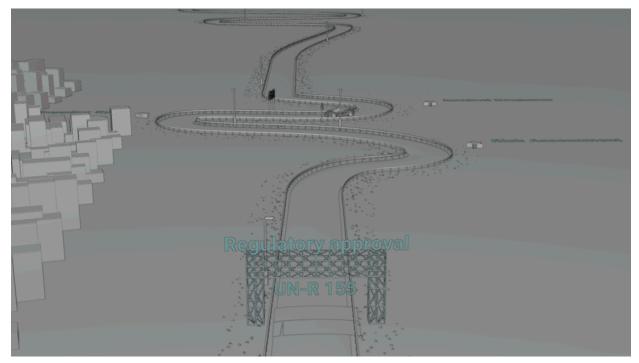
Navigating the regulatory challenge of UN-R155,



automotive manufacturers face the complex task of managing countless components



and software from diverse suppliers



Note:Finish line should be clear that continues after the finish line, camera panning , sign says production

Solution- CarAlert

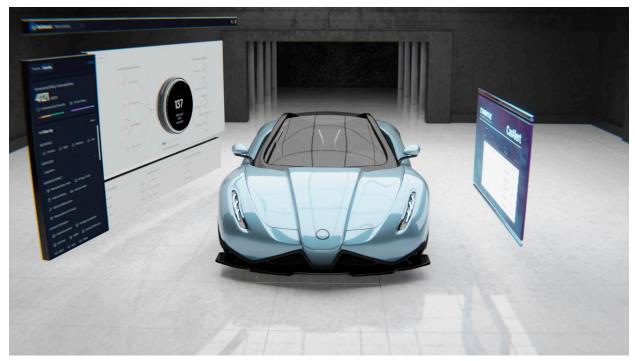


Car Alert by CYMOTIVE is engineered to help manufacturers and suppliers

[Cloth reveal of the software] note- faster reveal needed

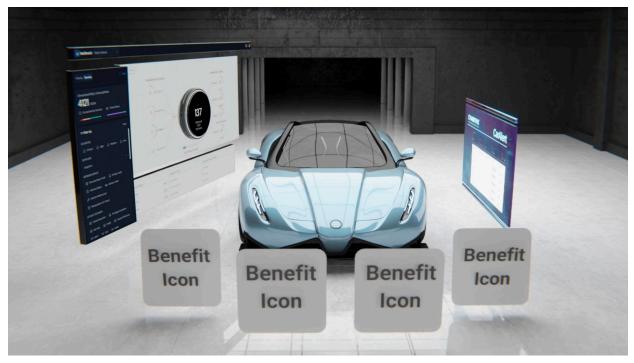


[the car enters the service zone]



[we can show multiple dashboards and informative screens]

enhance vehicle security at every level, reduce development time, gain trust with customers, and protect cars from digital threats.



[The icons appear one by one in sync with the narration]

Car Alert begins with Asset Identification including management of assets, bill of materials, vehicles, and ECUs.

TECHNOLOGIES	CarAlert
Asset Identific	
	Maddle in Andrew Brief (March) (March
	Op Roc (1) Op Ro (1) Op R

[The software performs a 'CT scan' on the car, ECU's are visually listed on the left with titles and visual representations]

Note: 1st line in the table, full names:

Initial Access Execution Persistence Privilege Escalation Defense Evasion Credential Access Discovery Lateral Movement Collection Command and Control Exfiltration Impact Proper content for the asset:

A 14 (m)	199 m - (11)	Q	22 PF (10)	F or (m)	E es (0)	A0 85 (10)	ALC 1 1 1 1 1 1	M 0.1(7)		(TP) = + (m)	(4)
1A (2)	🖹 Exe (1)	2" Per (7)	Aga PE (10)	⊕ DE (12)	@ CA (6)	88 Dis (15)	≒ LM (4)	\$\$ Col (7)	5 CAC (1)	图 Exf (0)	() Imp (4)
pply Chain Com	Software Deploym_	Boot or Logon Aut	Abuse Elevation C	Abuse Elevation C	Man-in-the-Middle	Account Discovery	Remote Services	Man-in-the-Middle	Ingress Tool Transf		Account Acces
Valid Accounts		Boot or Logon Initi	Access Token Man	Access Token Man	Brute Force	Browser Bookmark_	Software Deploym	Audio Capture			Endpoint Denia
		Create or Modify S_	Boot or Logon Aut	Hijack Execution FL.	Credentials from P_	File and Directory _	Taint shared conte	Automated Collec			Firmware Corru
		Event Triggered Ex	Boot or Logon Initi	Impair Defenses	Network Sniffing	Network Service S_	Use Alternate Aut	Man in the Browser			Network Denial
		Hijack Execution FL	Create or Modify S	Indicator Removal	Steal or Forge Ker	Network Share Dis_		Clipboard Data			
		Server Software C	Escape to Host	Masquerading	Unsecured Creden	Network Sniffing		Email Collection			
		Valid Accounts	Event Triggered Ex	Modify Registry		Peripheral Device		Screen Capture			
			Hijack Execution FL.	Process Injection		Permission Group					
			Process Injection	Rootkit		Process Discovery					



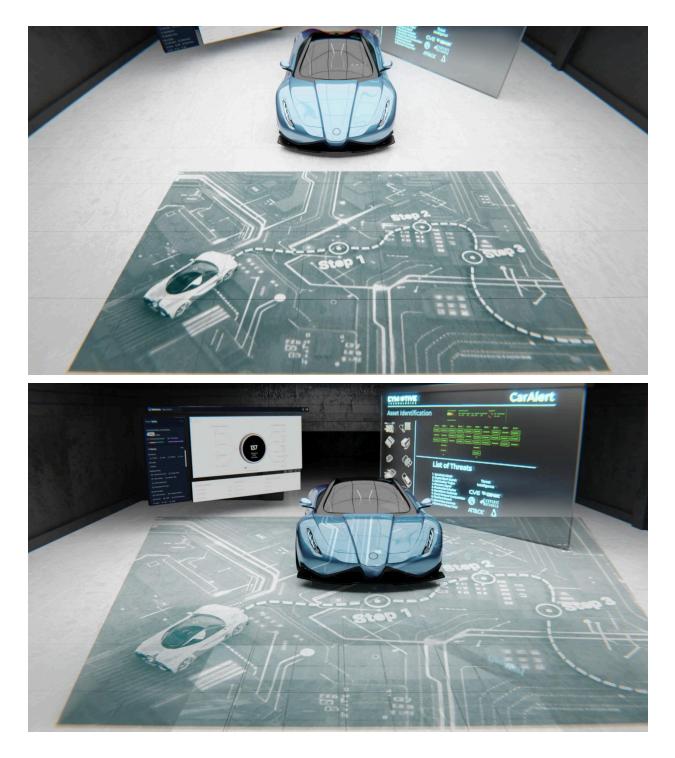
[As profiling takes place, assets are colored by their threat level- red/orange/green. Some of the issues are resolved and turn green, some of the red turns into orange]

Automatically mapping all the vulnerabilities, exploits and threats to the ECUs and vehicles CarAlert prioritizes them according to their potential impact and damage,

	CarAlert
et Identification	HOT Nome (Mar) Nom (Mar) Nome (Mar) Nom
	Image: Second
	Nuelosh- Nuelosh- 15
1. A A A A A A A A A A A A A A A A A A A	List of Threats 1. SyncJack Attack 2. CryptoHijack Exploit 2. CryptoHijack Exploit 3. SyncJack Attack 2. CryptoHijack Exploit 3. SyncJack Attack 4. SyncJack Attack 5. SyncJack At
	 S. Gatecons Signal A. Phantom Signal S. ShadowBot Infusion S. NanoWorm Outbreak NanoWorm Outbreak R. FleetFeet Breach S. Echo Pulse Anomaly J. Cuantum Decay Fault

[Threat icons appear, and a list of threats is assembled] note-replace the icons (threat intelligence) with more threats (a long list is provided in the end of the document)

and recommends the best path for risk minimization.



[Hologram screen shows a navigation-style interface with a clear path to fix vulnerabilities]

At any time, you can track the process and focus only on the critical risks,



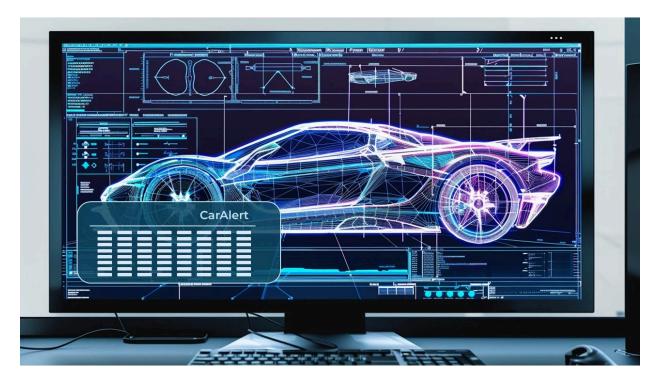
[a fresh angle and a new screen with the tickets interface, fully animated]

Closing Remarks

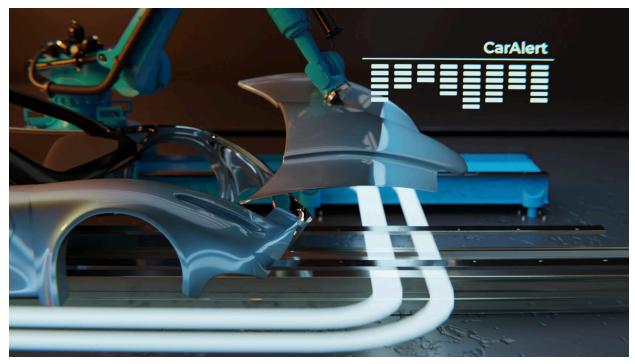
From design and development through post-production,



[Car schematics on a screen in contemporary office, CarAlert 'CT Scan' is performed on the schematics]



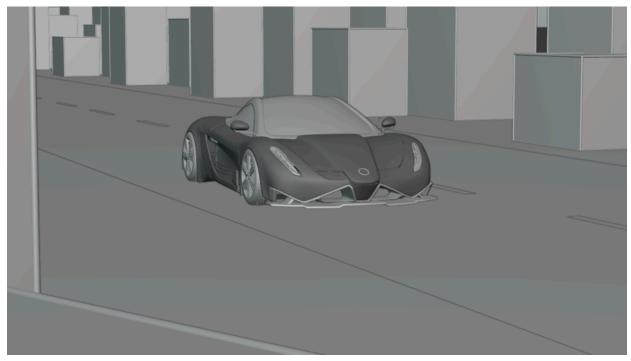
[The CarAlert visual cue provides a quick report screen]



[The car is 'scanned' again by CarAlert while in production]



Car Alert's automated full lifecycle coverage continuously monitors and safeguards your vehicle long after it leaves the production line.



[The car is driving the same city as the introduction shot, visual representation of over the air scan and update]





CYMOTIVE.COM

Full list of threats: (techniques)

Supply Chain Compromise Valid Accounts Software Deployment Tools Boot or Logon Autostart Execution Boot or Logon Initialization Scripts Create or Modify System Process Event Triggered Execution:.bash_profile and .bashrc Hijack Execution Flow Server Software Component Valid Accounts Abuse Elevation Control Mechanism Access Token Manipulation Boot or Logon Autostart Execution Boot or Logon Initialization Scripts Create or Modify System Process Escape to Host Event Triggered Execution:.bash_profile and .bashrc Hijack Execution Flow **Process Injection** Valid Accounts Abuse Elevation Control Mechanism Access Token Manipulation Hijack Execution Flow Impair Defenses Indicator Removal on Host Masquerading Modify Registry **Process Injection** Rootkit Subvert Trust Controls Use Alternate Authentication Material Valid Accounts Man-in-the-Middle Brute Force Credentials from Password Stores Network Sniffing Steal or Forge Kerberos Tickets **Unsecured Credentials** Account Discovery Browser Bookmark Discovery File and Directory Discovery Network Service Scanning

Network Share Discovery Network Sniffing Peripheral Device Discovery Permission Groups Discovery Process Discovery Remote System Discovery System Information Discovery System Network Configuration Discovery System Owner/User Discovery System Service Discovery System Time Discovery **Remote Services** Software Deployment Tools Taint shared content Use Alternate Authentication Material Man-in-the-Middle Audio Capture Automated Collection Man in the Browser Clipboard Data Email Collection Screen Capture Ingress Tool Transfer Account Access Removal Endpoint Denial of Service Firmware Corruption Network Denial of Service