

Capgemini contacts:

Raffaella Poggio
Marketing & Communication Director
raffaella.poggio@capgemini.com
+39 347 4271901

Michela Cotich
Marketing & Communication
michela.cotich@capgemini.com
+39 347 3620244

Imageware:

Stefano Bogani
Marco Groppelli
capgemini@imageware.it
+39 02 700 251

Capgemini lancia una nuova offering per la cybersecurity nel settore automotive

Milano, 13 febbraio 2017 – [Capgemini](#), uno dei maggiori provider mondiali di servizi di consulenza, tecnologici e di outsourcing, ha annunciato oggi il lancio di una nuova proposta studiata per rafforzare la sicurezza dei veicoli connessi, degli impianti di produzione delle vetture e dei sistemi IT enterprise delle case automobilistiche. La nuova proposta combina le competenze specialistiche dei team globali automotive, cybersecurity e consulting del Gruppo, inclusa la consociata interamente controllata Sogeti, con il network di Security Operation Center (SOC). L'offerta combina una soluzione completa per aiutare produttori e fornitori di componenti a prevenire, intercettare e neutralizzare possibili minacce di cybersecurity.

Andrea Nulli, Cybersecurity Leader di Capgemini Italia, ha dichiarato: *“Chiunque lavori per un produttore automobilistico, dagli addetti agli impianti fino al CEO, si è ormai reso conto di quanto sia importante la cybersecurity. L'incapacità di prevenire un attacco può comportare richiami di massa, perdite di fatturato, sanzioni normative e persino rischi per la sicurezza dei clienti. Buona parte dell'attenzione è stata rivolta sinora alla protezione dei sistemi IT, cosa già sufficientemente difficile per sé, ma ora che le compagnie lavorano sempre più spesso con 'cose' connesse come robot di fabbrica e milioni di componenti automobilistici connessi, la complessità associata alla capacità di restare al sicuro è impressionante”.*

Il lancio avviene in un periodo nel quale il settore automotive sta affrontando delle sfide in ambito cybersecurity senza precedenti. Le automobili stanno diventando sempre più avanzate e connesse, vengono costruite con centinaia di sensori e svariati computer di bordo incaricati di controllare ogni cosa, dallo sterzo fino ai fari. Tutto questo si traduce in una moltitudine di punti di ingresso attraverso i quali gli hacker possono ottenere l'accesso e il controllo di un veicolo. E non è solamente l'automobile a essere vulnerabile: anche gli stabilimenti sono sempre più connessi e costituiscono bersagli potenziali.

“In Capgemini abbiamo una comprovata esperienza nel supportare i nostri clienti a proteggere i dispositivi connessi e l'intera infrastruttura operativa. La nuova offerta mette a disposizione tutte le competenze e la capacità che abbiamo maturato nell'area della cybersecurity per aiutare i nostri clienti del settore automotive a rendere sicuro il loro business”, afferma Andrea Nulli.

La nuova proposta di Capgemini supporta produttori e fornitori di componenti che intendono minimizzare i rischi di cybersecurity dei veicoli connessi, degli impianti di produzione e dei sistemi IT enterprise.

L'offering comprende:

- **Valutazione** della sicurezza all'interno e intorno agli impianti di produzione compresi i sottosistemi critici, e nell'autoveicolo stesso, compresa la vulnerabilità di service provider e connessioni esterne come Wi-Fi o Bluetooth. Test di penetrazione per ottenere ulteriori informazioni specialistiche sulle vulnerabilità presenti negli stabilimenti e nelle auto e valutazione del successo di una strategia e della sua implementazione.
- Definizione di una **strategia** per la protezione di ogni aspetto del veicolo, dal controllo elettronico delle unità¹, dai bus e dalla connettività esterna fino ai processi di governance che li circondano, permettendo a una compagnia automobilistica e ai propri fornitori di affrontare misure di sicurezza end-to-end.
- **Implementazione** di misure di sicurezza e azioni di rimedio. Questa fase comprende consulenza e formazione sulle best practice per lo sviluppo di software sicuri e l'implementazione operativa nel ciclo di vita dello sviluppo software.

La proposta permetterà inoltre alle aziende di accedere alla rete di SOC (Security Operations Center) mondiale di Capgemini e a SOC che si occupano nello specifico di monitorare eventi legati ai veicoli e alla loro produzione. Questi centri sono composti da team di specialisti e possono agire come team dedicati o condivisi di un OEM (Original Equipment Manufacturer) o di un fornitore di componenti. La proposta riduce significativamente la necessità per le Case automobilistiche di investire tempo, risorse e budget nello sviluppo e nel potenziamento di propri SOC interni.

La proposta per la cybersecurity automotive si affianca a una suite di servizi per il settore automobilistico erogati dagli specialisti automotive di Capgemini. Maggiori informazioni sono disponibili a questo [link](#).

Capgemini

Con oltre 180.000 dipendenti in più di 40 paesi nel mondo, Capgemini è leader mondiale nei servizi di consulenza, information technology e outsourcing. Nel 2015 il Gruppo Capgemini ha registrato ricavi per 11,9 miliardi di euro. Con i propri clienti Capgemini progetta e realizza specifiche soluzioni di business, tecnologiche e digitali, per soddisfare le loro esigenze di innovazione e competitività. L'organizzazione profondamente multiculturale contraddistingue da sempre il Gruppo Capgemini, che utilizza un approccio di lavoro unico e distintivo – la [Collaborative Business Experience™](#) – e un modello globale di produzione distribuita denominato [Rightshore®](#).

Per maggiori dettagli visita il sito www.it.capgemini.com e segui [@CapgeminiItalia](https://twitter.com/CapgeminiItalia) su Twitter.

Rightshore® è un marchio appartenente a Capgemini



¹ Sistema di comunicazione che collega unità di controllo, sensori e attuatori