VicOne

Is the Automotive Industry Prepared to Navigate API Security Risks in Software-Defined Vehicles?

Learn more about VicOne by visiting VicOne.com or scanning this QR code:

In today's automotive ecosystem, application programming interfaces (APIs) have become both ubiquitous and indispensable. Connecting various internal systems within vehicles, APIs are widely applied across multiple scenarios. These include remote vehicle activation, connection with third-party service providers for emergency assistance services, and energy management, among many other applications. Service clouds between automotive manufacturers (OEMs) and suppliers also heavily rely on APIs to facilitate rapid updating of software-defined vehicles (SDVs) to enable cloud-native technologies.

Indeed, APIs are pervasive throughout the modern automotive ecosystem, encompassing cloud-based APIs, cloud-to-vehicle APIs, mobile-to-vehicle APIs, mobile-to-cloud-to-vehicle APIs, and in-vehicle APIs. These diverse types of APIs play pivotal roles, ensuring seamless connectivity and efficient operations across the entire automotive industry.

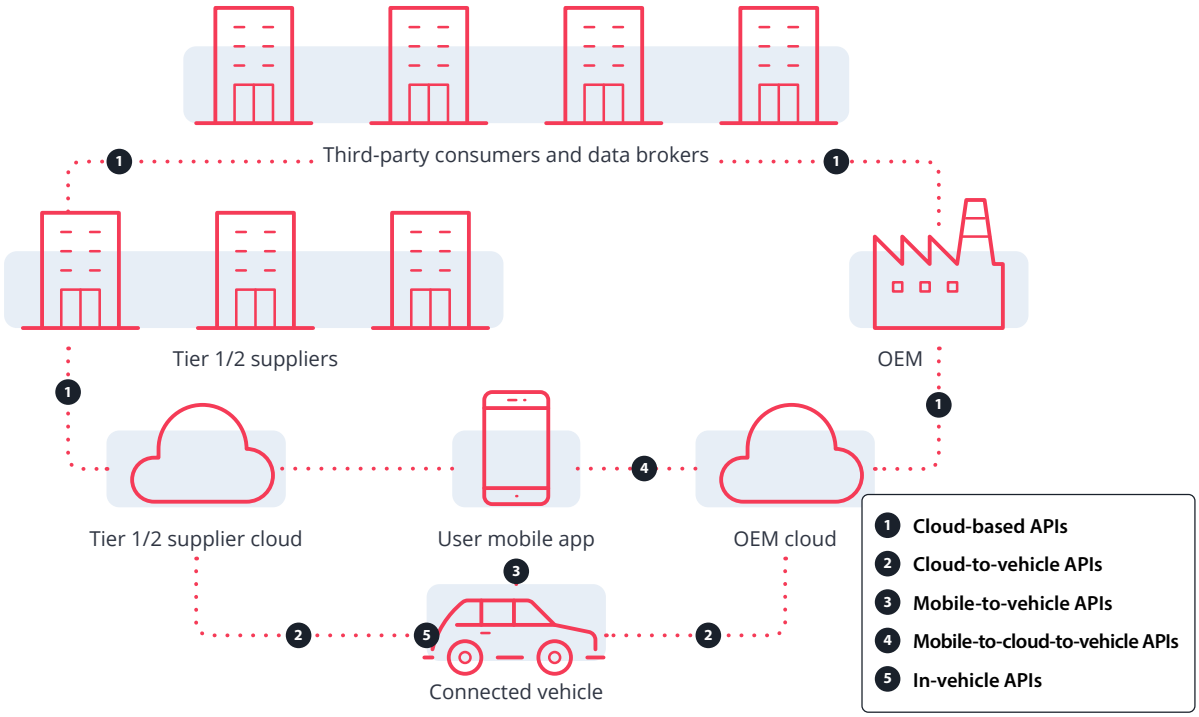

Figure 1. Interconnectivity within the automotive ecosystem made possible by APIs

The Automotive API Attack Landscape

According to our findings in the VicOne Automotive Cyberthreat Landscape Report 2023, despite the numerous benefits that APIs offered, incidents related to applications and APIs accounted for 12% of the automotive cyberattacks and security incidents from the second half of 2022 to the first half of 2023.

Our automotive threat intelligence database reveals that from 2020 to 2022, API attacks evolved from targeting individual components to adopting a comprehensive strategy encompassing the entire ecosystem. This shift in API attacks highlights a greater challenge to automotive ecosystem security, indicating that concentrating solely on protecting individual APIs is no longer adequate.

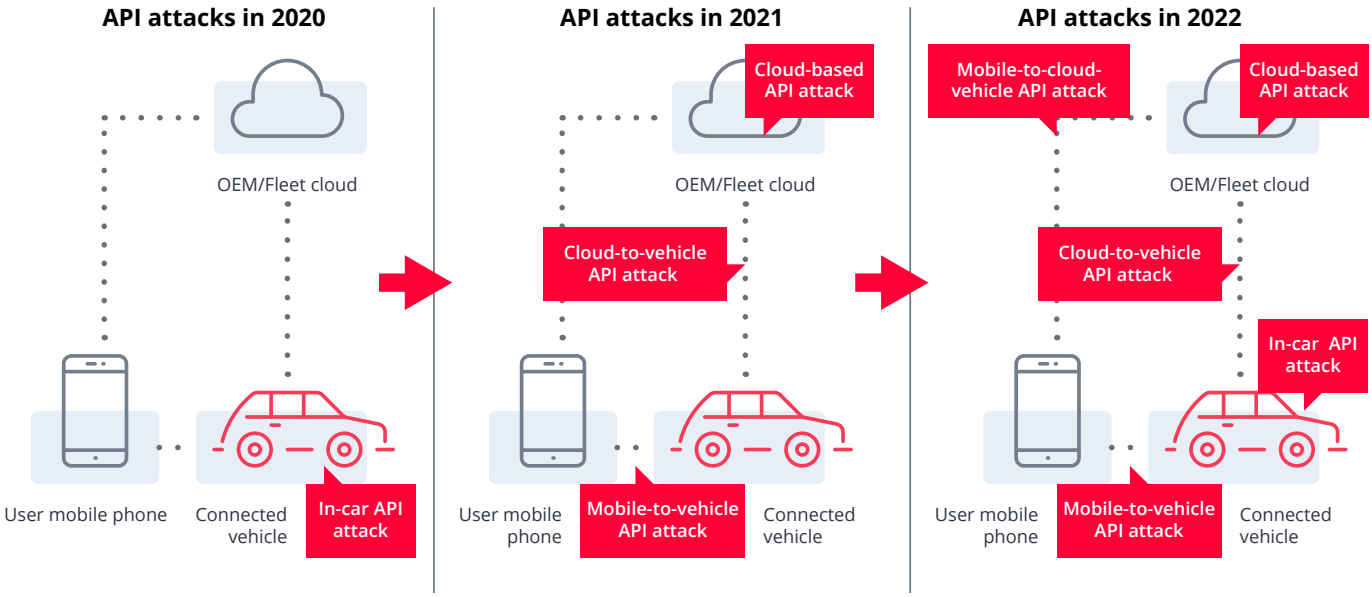

Figure 2. API attacks evolved from having single targets to having multiple targets.

Also according to our automotive threat intelligence database, in terms of categories, API attacks in the automotive industry from 2016 to 2023 primarily consisted of cloud-to-vehicle API attacks (35%) and cloud-based API attacks (30%), followed by mobile-to-vehicle API attacks and in-car API attacks (each accounting for 13%).

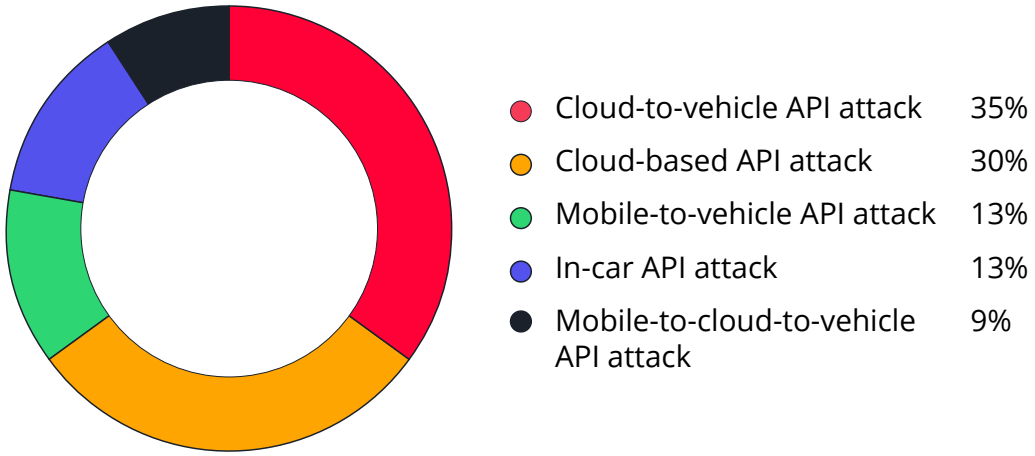

Figure 3. The distribution of API attack categories from 2016 to 2023

From these observations, we can draw three conclusions:

- Cloud-to-vehicle API attacks cover most use cases.
- Protection of web APIs is necessary but not sufficient by itself.
- Covering mobile brings additional value.

It is important to note that SDVs inherently rely heavily on APIs. Consequently, the potential attack surface expands, introducing risks due to the frequent updates of software over-the-air (SOTA) technology. If attackers breach OTA servers and inject malicious software, they could masquerade as legitimate SOTA update requests, distributing them to vehicles via unauthorized APIs. The nature of SDVs significantly boosts the attackers' chances of success. Previously, OTA updates occurred quarterly, offering only four to five chances per year. The frequency is expected to increase to potentially 12 to 14 times annually in the future. These factors underscore the critical importance of automotive API security.

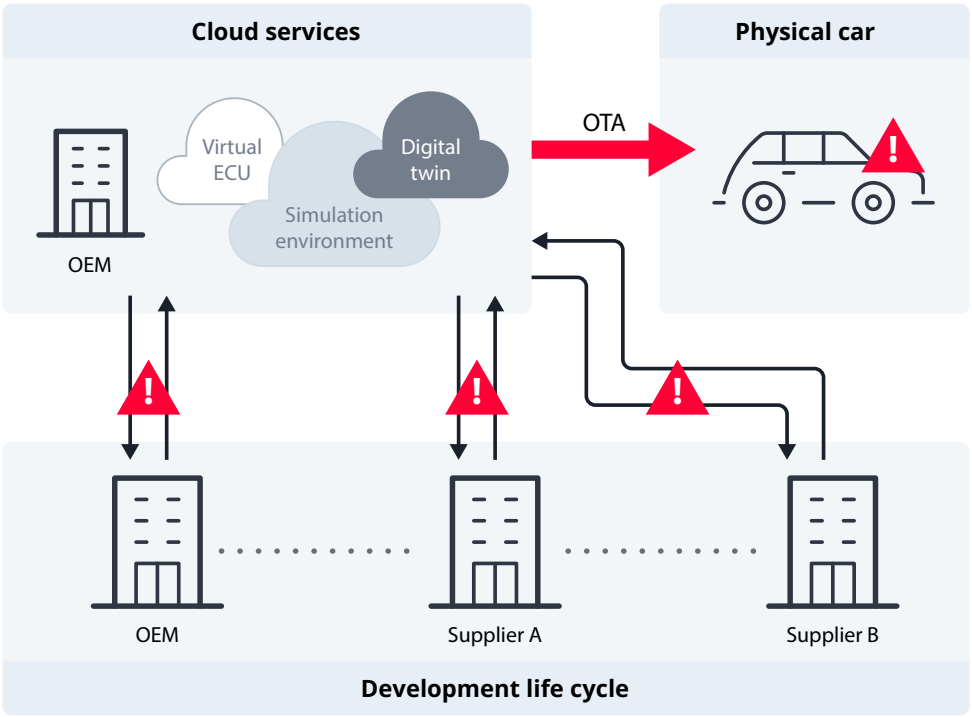

Figure 4. Risks in the SDV ecosystem

The Risks for OEMs and Fleet Managers

We now examine several reported security incidents related to APIs from the past three years, to better understand automotive API security risks.

Remote Hijack of a Vehicle: An API Attack From Halfway Across the World

According to a study by VicOne automotive security researchers, attackers can exploit compromised account credentials to execute remote attacks on vehicles, even those on the other side of the world. These credentials enable attackers to access a vehicle's APIs and perform various commands remotely. These commands include fetching the status of the vehicle's doors and remotely starting the vehicle. Attackers can obtain credentials through phishing or cyberattacks. Unfortunately, credentials are often managed as general assets despite the high financial value and privacy risks associated with vehicle fleets.

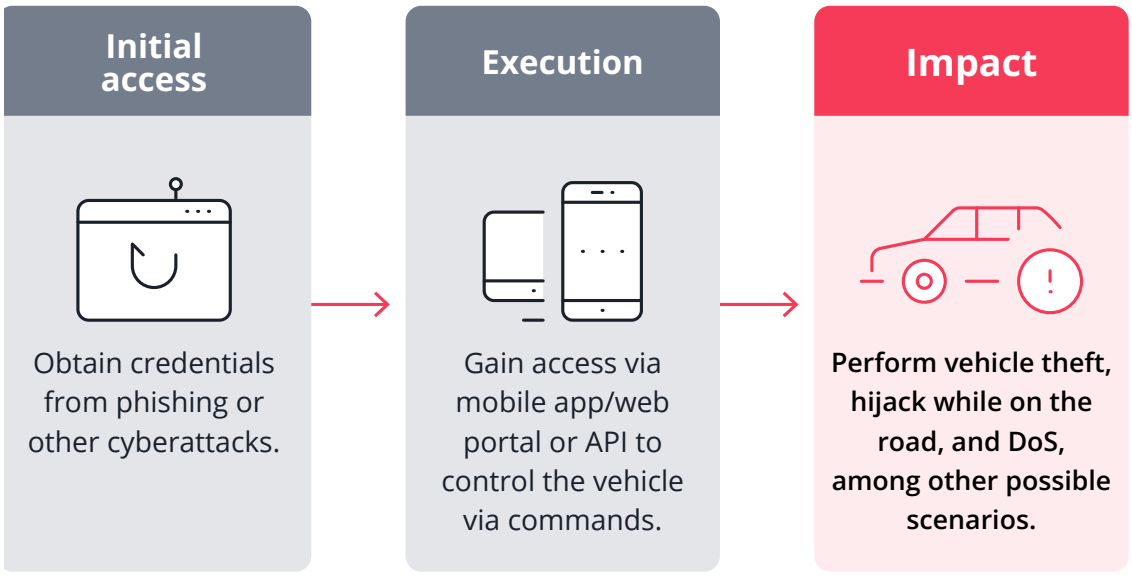

Figure 5. The attack chain for remote car hijack via API access

Remote Full Takeover of a Vehicle: Compromised Automotive Cloud Service APIs

In a blog post published in January 2023, Sam Curry, a web application security researcher, and his team demonstrated how they accessed the back-end cloud infrastructure of various OEMs by exploiting vulnerabilities in telematics systems and APIs. They uncovered a publicly accessible website for vehicle repair shops that wrote to the same database as the core employee LDAP (Lightweight Directory Access Protocol) system of a well-known automotive brand. Registering on this site granted them limited access to employee applications, which they leveraged to gain further access to sensitive internal applications, including the brand's GitHub, where they found detailed instructions for building applications to communicate with customer vehicles.

Their discoveries enabled the compilation of a list of Common Weakness Enumerations (CWEs) occurring on affected cloud service websites, revealing a gap in the automotive industry's awareness of these issues. Two main cloud-related problems were identified: authentication and authorization issues, and inadequate sanitization of input parameters. The former could lead to pre-authentication vulnerabilities and unauthorized access to personally identifiable information (PII), while the latter could expose systems to injection attacks.

These findings underscore the realization that the automotive industry faces security challenges similar to those faced by the IT industry but it lacks sufficient preparedness to address them effectively. Implementing proper input validation and sanitization, for example, is crucial to mitigating the risks, but it remains challenging without coding style guides or a CI/CD (continuous integration and continuous delivery) environment.

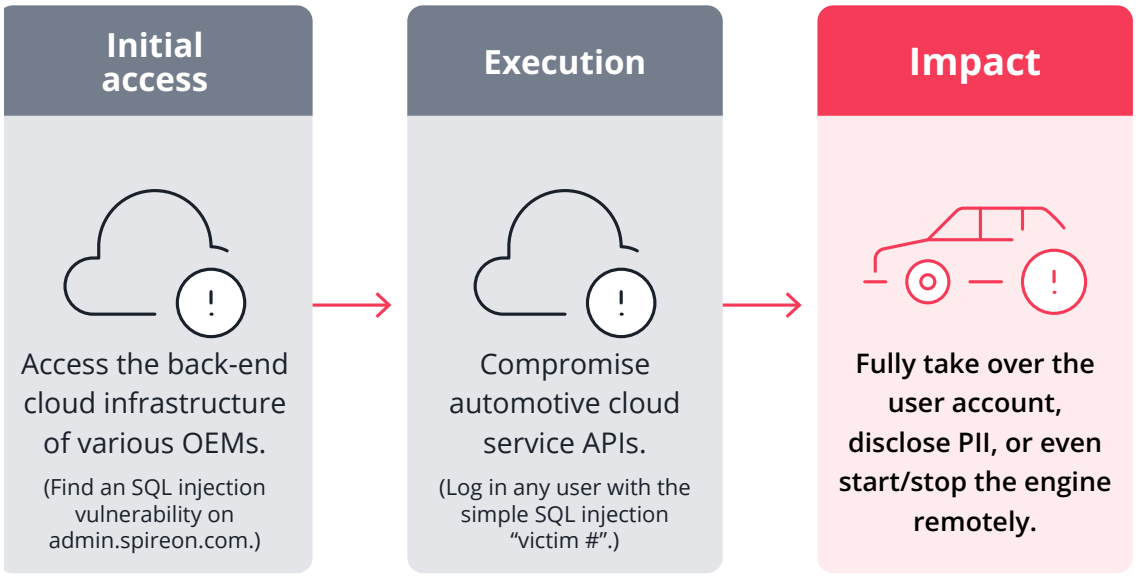

Figure 6. The attack chain for remote full takeover of a vehicle via compromised automotive cloud service APIs

Remote Full Takeover of a Fleet: Abuse of a Taxi App's API

In September 2022, hackers exploited vulnerabilities in a popular Russian taxi app's API, resulting in severe traffic congestion in Moscow. The attackers manipulated the API to send fake taxi orders to the system, overwhelming the service and causing congestion on city streets. This incident highlights the potential consequences of API security flaws and the necessity of adopting robust protective measures against such attacks. It emphasizes the importance of taking proactive security measures to safeguard critical infrastructure and mitigate the impact of cyberthreats on public safety and urban traffic.

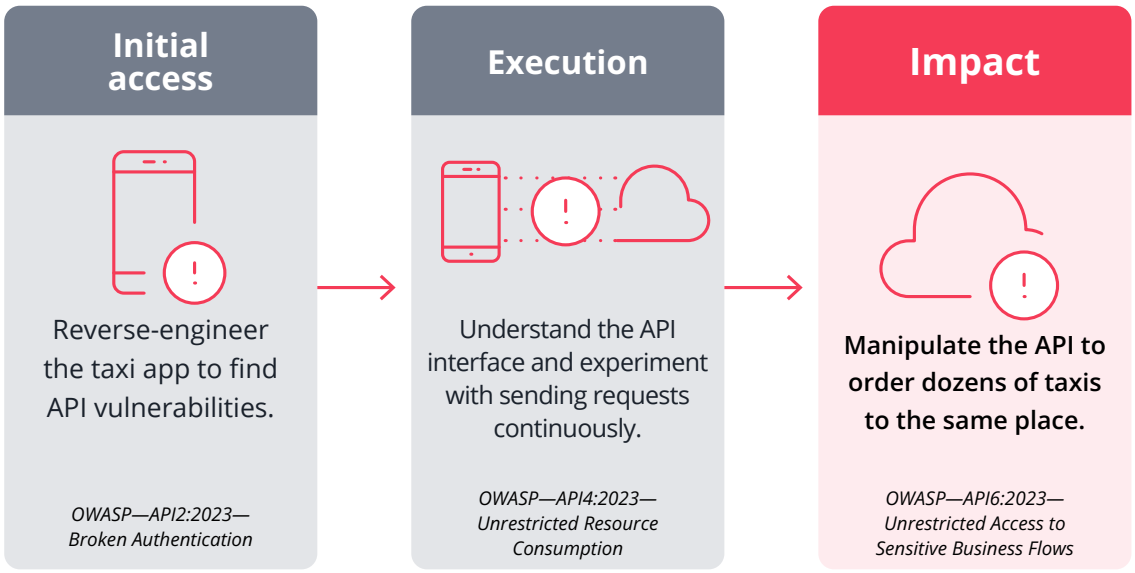

Figure 7. The attack chain for remote full takeover of a fleet via abuse of a taxi app's API

In summary, the threats and risks resulting from API vulnerabilities include:

- **OTA spoofing:** Unauthorized API calls can mimic legitimate OTA update requests.
- **Cyberattacks/Ransomware incidents:** APIs can be a gateway for attackers to infiltrate systems and deploy ransomware.
- **Vehicle entry/Immobilizer systems:** API flaws can allow unauthorized access to vehicle control systems.

Complete API and Security Risk Visibility for SDVs, From Design to On-Road, All in One Platform

To effectively mitigate API security risks in the expansive automotive ecosystem, it is essential to implement a systematic approach. Since every component represents a potential attack surface, comprehensive strategies are necessary. According to a Gartner® report, titled Innovation Insight for API Protection, "API protection products provide three main types of functionality — discovery, posture management and runtime protection."* Building upon these principles, VicOne and 42Crunch have joined forces to provide an integrated solution that enables continuous discovery, posture management, and runtime protection to address automotive supply chain API security risks across the automotive life cycle.

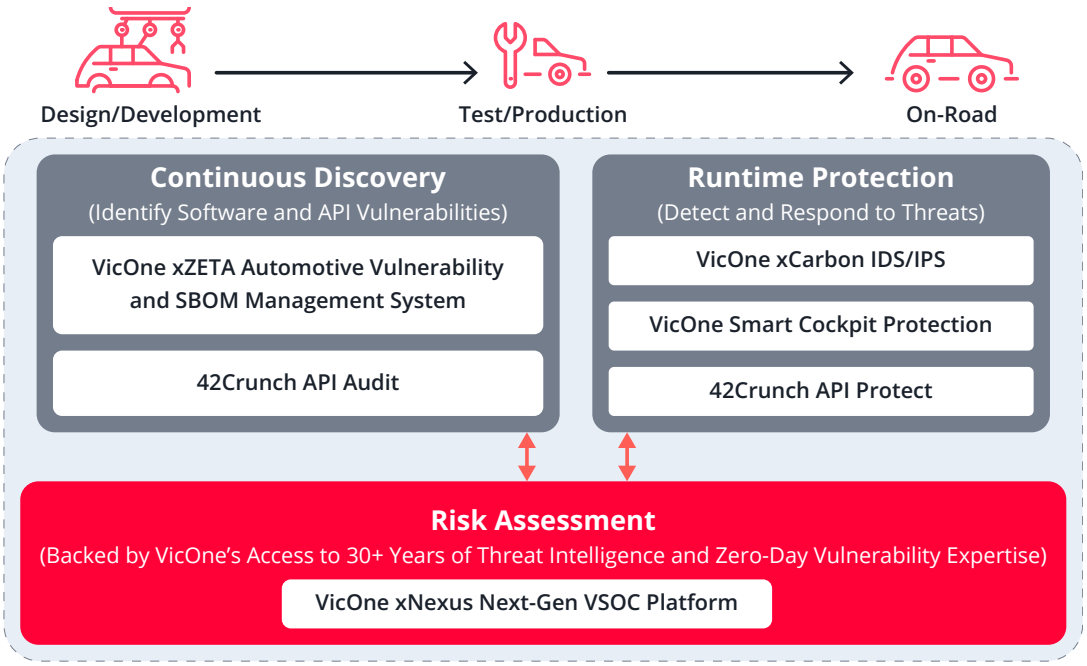

Figure 8. A comprehensive and practical solution provided by VicOne and 42Crunch throughout the automotive life cycle

In the design or testing phase, the key is the continuous identification of software and API vulnerabilities before attackers find them. With 42Crunch's API Audit, API misconfigurations and API vulnerabilities can be identified. For instance, with regard to the case involving compromised automotive cloud service APIs, SQL injection vulnerabilities can be identified during the design phase, thus eliminating the latest Open Worldwide Application Security Project (OWASP) top 10 API security vulnerabilities during development to prevent them from becoming serious threats when the system operates in the future, and empowering shift left.

With VicOne's xZETA automotive vulnerability and software bill of materials (SBOM) management system, the generation of SBOMs can be automated to enhance ongoing threat detection. Zero-day, undisclosed, and known vulnerabilities, along with malware, ransomware, and advanced persistent threats, can be uncovered within binaries and firmware. As a result, vulnerabilities in both APIs and firmware can be mitigated before becoming serious threats when the system operates in the future.

For vehicles on the road, 42Crunch's API Protect is tailored to protect each API from malicious attacks and enforce API runtime protection directly in front of APIs. On the other hand, with VicOne's xCarbon intrusion detection or prevention system (IDS/IPS) and Smart Cockpit protection solutions, anomalies like malicious CAN (controller area network) messages, denial-of-service (DoS) attacks, and abnormal API transactions can be detected. Through runtime protection, detection of and response to threats can be done in real time.

Full visibility is essential to arriving at a common understanding of both in-vehicle and back-end infrastructure issues and challenges. By bringing all vulnerabilities and security events, from the design phase to on-road runtime detection, to VicOne's xNexus next-gen vehicle security operations center (VSOC) platform, unified risk visibility can be achieved. With artificial intelligence (AI) and large language modeling (LLM), these vulnerabilities and security events can be correlated into contextualized attack paths. These contextualized attack paths, in turn, enable OEMs and suppliers to gain precise, actionable threat insights, facilitating continuous and dynamic risk assessment across the automotive supply chain.

For example, in the case of the abused taxi app API incident, with our integrated solution, broken authentication or token anomalies in APIs can be detected right from the initial access. As the attackers begin testing, we can detect unrestricted resource consumption and abnormal API transactions.

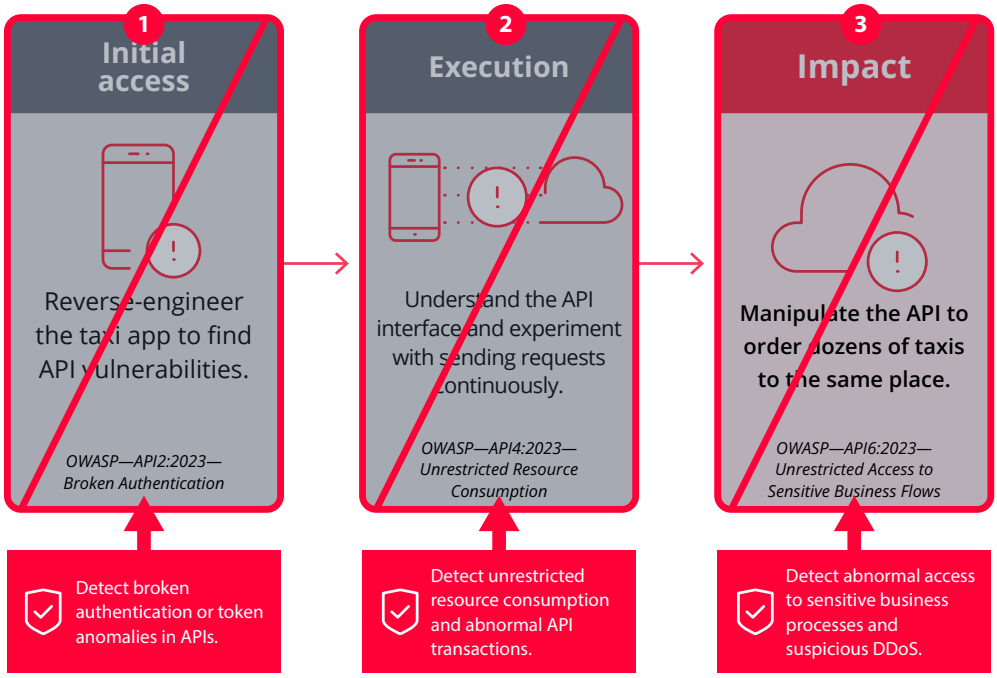

Figure 9. How our solution can help against this kind of attack

Sharper Insights, Lower Anxiety: Risk Navigation in SDVs

Our integrated solution allows OEMs and suppliers to initially assess API security issues within their ecosystem (in-vehicle, mobile, web), and OEMs to then quickly turn around to remediate these issues. It enables continuous discovery, posture management, and runtime protection to address automotive supply chain API security risks with the following benefits:

- **Enriched risk visibility for better risk prediction:** Full visibility into API security and other automotive-related risks across the full automotive ecosystem.
- **Optimized resource allocation:** Improved dynamic risk assessment through the integration of API security events along with other automotive data and security events.
- **Precise threat detection:** Quicker and more accurate detection of the latest OWASP top 10 API security vulnerabilities.
- **Contextualized risk visibility:** Actionable threat insights drawn from the correlation of security events and data across the entire ecosystem.
- **A highly integrated, future-proof solution:** Seamless phased implementation and effortless scaling from agentless to agent to support the automotive life cycle for decades without disruption.

Contact us to learn more about how we can help you navigate API security risks in SDVs.

*Gartner, Innovation Insight for API Protection, Dionisio Zumerle, Jeremy D'Hoinne, et al, 2 February 2024. (For Gartner Subscribers only) GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved.

Is the Automotive Industry Prepared to Navigate API Security Risks in Software-Defined Vehicles?

Learn more about VicOne by visiting VicOne.com or scanning this QR code: