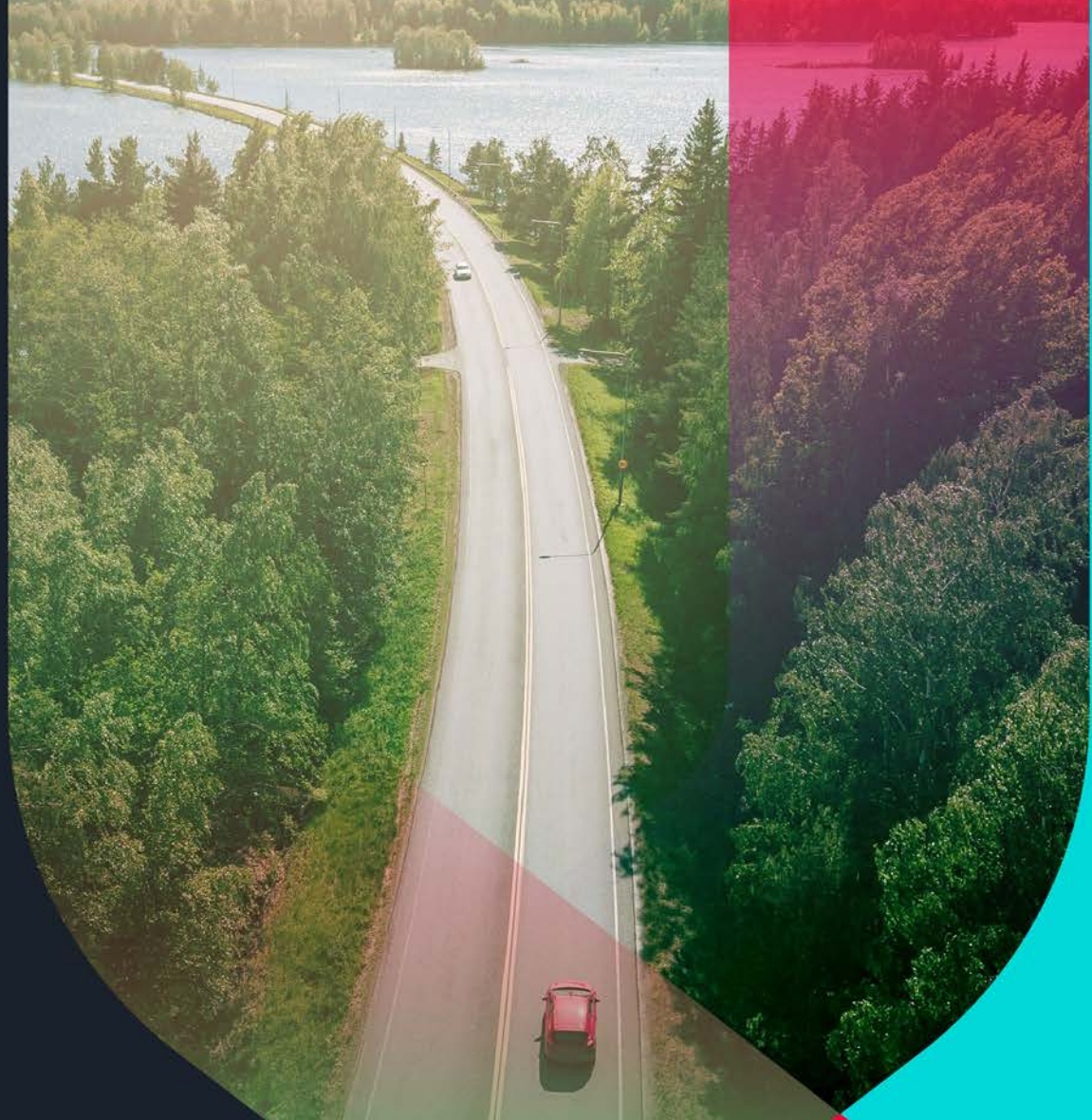
VicOne

VinCSS
Cyber Security Services



Spurring a Green Mobility Era

Elevating EV Software Supply Chain Security With a Superior Vulnerability and SBOM Management System

Driving Green Mobility

In line with the global push for net-zero emissions, countries are actively working to reduce vehicular particulate emissions. Both traditional automotive manufacturers (OEMs) and emerging electric vehicle (EV) makers, such as those in Vietnam and China, are accelerating their transition to support net-zero goals. Gartner predicts that by 2030, more than half of all vehicle models in the market will be EVs.

As EVs gain popularity, cybersecurity experts raise concerns about increasing threats. The connectivity and computing capabilities in EVs make them attractive targets for attackers. Attackers can spread malicious software or exploit Bluetooth vulnerabilities to remotely hijack EVs. Such are situations that EV makers aim to prevent, and companies like VinCSS play an essential role in helping EV makers secure the EV revolution.

VinCSS — a subsidiary of Vingroup, Vietnam's leading enterprise — specializes in cybersecurity services. Drawing on its distinctive proficiency in automotive cybersecurity, VinCSS offers comprehensive services tailored for EV makers. The company is dedicated to supporting global EV makers in enhancing their cybersecurity capabilities, and it has already demonstrated success by supporting a Vietnamese EV maker.

"At every step of the vehicle's development, our team actively participates, striving to integrate security seamlessly into the entire process," said Tin T. Nguyen, Director of the Automotive Cybersecurity Division of VinCSS. "We meticulously handle every aspect, from component design to EV ecosystem integration, even in the future EOL activities, recognizing our pivotal role in upholding customer trust in EV vehicles."

ABOUT VINCSS

Founded: **2018**

Headquarters: **Ho Chi Minh City, Vietnam**

Industry: **Computer and network security**

Employees: **100+**

www.vincss.net

Uncovering EV Software Risks: Time-Consuming

VinCSS understands the dynamic nature of cyberthreats, emphasizing the need for continuous attention. As indicated in VicOne's automotive cyberthreat landscape report for 2023, there has been an average of 300 automotive-related CVEs reported each year since 2019. This underscores the increasing number of vulnerabilities in the automotive industry that could be exploited.

In the past, VinCSS relied on Tier 1/Tier 2 suppliers, but this often led to situations where, when VinCSS asked suppliers about their cybersecurity measures, the typical response was, "Well, what do you mean by that?" This prompted VinCSS to explore solutions that could provide vulnerability insights to aid suppliers in understanding and addressing issues, fostering a collective effort to build secure products with consistent standards and knowledge.

Before more efficient methods were available, VinCSS heavily depended on manual efforts for vulnerability collection, assessment, and management. This approach not only was time-consuming but also carried the risk of human errors from a managerial perspective. Consequently, a significant amount of manpower was dedicated to researching software bills of materials (SBOMs) and existing vulnerability information.

Nguyen explained: "Evaluating just one electronic control unit (ECU) could potentially take weeks to months for my team. However, with around 100 ECUs to monitor, we urgently need a more automated and comprehensive process to ensure accuracy, precision, and thoroughness. This way, we can provide more actionable insights to suppliers, collaborating to deliver a 'trusted' product to our customers."

Actionable Intelligence That Fuels Supply Chain Security

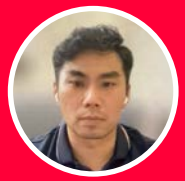
To tackle its challenges, VinCSS carefully assessed various vendors and ultimately opted for VicOne's xZETA, a superior vulnerability and SBOM management system. xZETA not only excels in identifying potential vulnerabilities within the automotive supply chain but also provides actionable insights, empowering VinCSS and its suppliers to take prompt action.

Nguyen highlighted: "What I value about xZETA is not only its ability to identify vulnerabilities but also its provision of concrete remediation recommendations. For instance, when xZETA detects potential vulnerabilities, it offers a detailed breakdown of the necessary steps and clickable links to relevant resources. It clearly outlines the 'next steps,' guiding me on how to address these issues."

This lays the groundwork for VinCSS to build a strong connection with suppliers, recognizing that cybersecurity is a collective effort requiring mutual learning and growth to effectively protect EVs. Nguyen added, "Sharing actionable insights generated by xZETA with suppliers not only allows us to provide clear guidance but also revolutionizes our interactions with our suppliers."

In the past, constrained by insufficient information, OEMs had to compel suppliers to find solutions, lacking motivation and often failing to prompt immediate action. Now, armed with comprehensive information from xZETA, suppliers can make informed judgments and act promptly.

> "xZETA provides us with the necessary coverage of vulnerabilities coupled with resources in remediation, and data in overall risk to our vehicle infrastructure. ... With automation, it **minimizes the monthslong manual efforts** previously required by my team."



TIN T. NGUYEN
Director
Automotive Cybersecurity Division
VinCSS

Nguyen elaborated: “I believe this is where the true value of xZETA lies. xZETA provides us with the necessary coverage of vulnerabilities coupled with resources in remediation, and data on overall risk to our vehicle infrastructure. It not only spots potential threats but also empowers me to furnish suppliers with more thorough information, assisting them in meeting OEM standards. With automation, it minimizes the monthslong manual efforts previously required by my team.”

From a managerial standpoint, xZETA’s user-friendly interface allows VinCSS to seamlessly navigate between overviews and in-depth insights. Nguyen explained: “Whether I need a holistic view or detailed specifics, I can easily switch between them. The intuitive interface design is incredibly user-friendly for our technical team, saving us a considerable amount of learning time.”

In addition, VinCSS acknowledges that vulnerabilities go beyond well-known CVEs, encompassing zero-day vulnerabilities as well. Nguyen provided his perspective, stating: “The fear of zero-day vulnerabilities is justified because, beforehand, we are unaware of their existence and may lack mitigation strategies. Hence, early detection of these vulnerabilities is crucial for risk prevention.” Consequently, xZETA not only covers information about known vulnerabilities but also identifies zero-day vulnerabilities, undisclosed vulnerabilities, advanced persistent threats (APTs), and ransomware. With the support of the Zero Day Initiative (ZDI), the leading vulnerability disclosure program since 2007, xZETA ensures the best detection coverage. This capability enables VinCSS to gain a comprehensive, automated understanding of potential software vulnerability threats within its components, ensuring timely threat awareness.

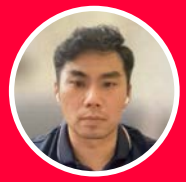
Driving Trust, Securing Future Green Mobility

With VicOne's xZETA, VinCSS is now able to have greater, more insightful, and automated awareness of what possible threats exist within its components, ensuring it is up to date on threats. Nguyen shared, "We utilize the xZETA system to demonstrate our effective vulnerability management capabilities to auditors, which helps us meet the requirements of UN R155."

Nguyen added: "xZETA gives us greater confidence in our ability to mitigate security risks that were previously out of our control: SBOM risks due to vulnerabilities in Tier 1 and 2 supplier components. It provides us with deeper reach in being an initiative-driven organization, being more proactive rather than reactive."

Looking forward, VinCSS faces the challenge of securing the entire EV ecosystem. With the expanding EV market, the risk of exploitation grows. Partnering with VicOne strategically positions VinCSS to address this challenge.

> We utilize the xZETA system to demonstrate our effective vulnerability management capabilities to auditors, which **helps us meet the requirements of UN R155**.



TIN T. NGUYEN
Director
Automotive Cybersecurity Division
VinCSS

Learn more and request a demo at **VicOne.com**.