Supply chain security risks of software driven products

Supply Chain Security:

New standards and best practices to mitigate supply chain security risks of software driven products.

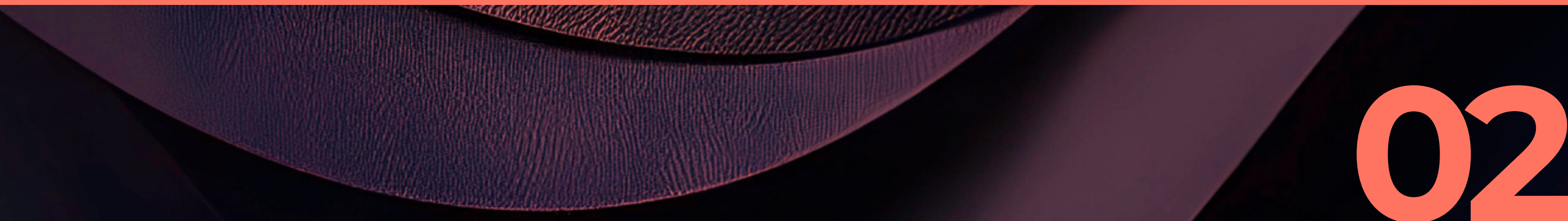
Table of Contents

1. Management Summary

Complex supply chains are a major attack surface for products and software enabled enterprises. Managing associated risks has been a major challenge for product integrators. Established security controls focus on availability of supply but lack effectiveness to prohibit proliferation of vulnerabilities throughout the value chain. With ever increasing software focus new measures must be taken to ensure cybersecurity of products and the enterprise IT landscape.

Authorities and standardization bodies are defining and publishing new regulations and standards to address the software supply chain – e.g., ISO 21434, Supply Chain Act, NIS 2 regulation, NIST CSF 2.0. While the NIS 2 regulation came into force in Europe at the end of last year, in the USA the issue is being driven forward primarily by the National Institute of Standards and Technology (NIST). These obligations from a regulatory perspective have a fundamental impact on each individual company.

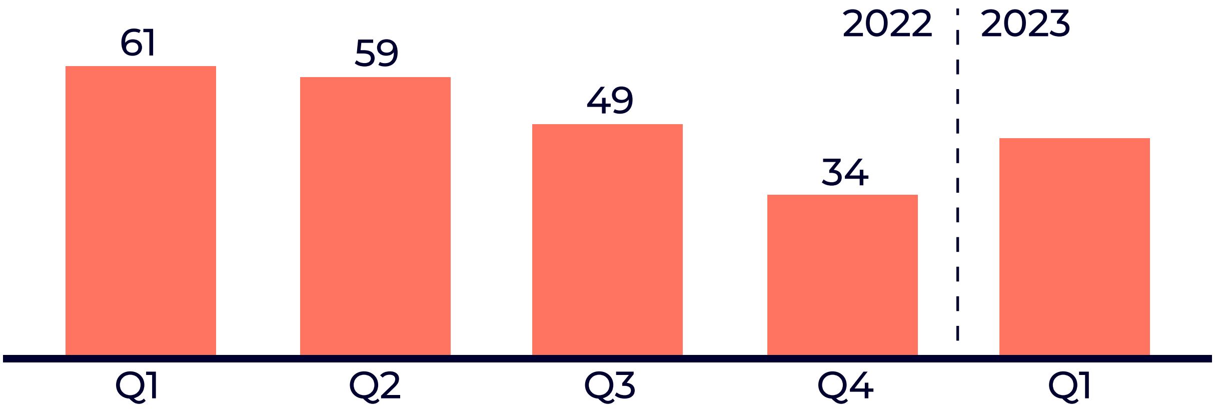
Based on emerging guidelines and from practical project experience, we present best practices for security controls to mitigate vulnerability propagation in the supply chain of software enabled products and the ecosystem. Additionally, we will address possible prevention assessments, potential defence & protection measures - both on company and product level - as well as defined processes after the incident.



2. Security attacks on the automotive supply chain are steadily increasing

With technology increasingly integrated into vehicles, securing vehicle software, electronic control units (ECUs), and communication networks against cyberattacks is imperative.

Global supply chain complexity exposes automotive companies to vulnerabilities, necessitating robust cybersecurity measures, including regular assessments and incident response plans. This requires a proactive approach, as existing security controls, focused on supply chain availability, often fail to address vulnerabilities, particularly in software supply chains, posing risks such as counterfeit parts. The number of attacks on automotive companies was analysed using media sources and presented in tabular form in Figure 1.



Statista/P3 Group

Figure 1: NUMBER OF ATTACKS on automotive suppliers remain on a high and rising level with peaks

Regulatory efforts like UN-R 155 and GBT (China) provide a general cybersecurity baseline but lack specificity for automotive supply chains. New regulations and standards, such as ISO 21434, aim to address this gap. We aim to outline best practices for security controls within software-enabled product supply chains, drawing on emerging guidelines and project experiences. This includes prevention assessments, defence mechanisms, and post-incident procedures to enhance supply chain integrity and resilience in software-driven enterprises. Given the dynamic nature of supply chain security, staying abreast of evolving trends and practices is crucial for effective mitigation of current challenges.

3. Supply Chain Resilience vs. Supply Chain Compromise

Supply Chain Resilience and Supply Chain Compromise are pivotal aspects of managing and securing supply chains. Supply Chain Resilience involves readiness for and recovery from disruptions, while Supply Chain Compromise addresses security threats that can compromise operations. Both are essential for modern supply chains, though they focus on different management and security dimensions.

Supply Chain Resilience denotes a supply chain's ability to endure and bounce back from disruptions like natural disasters or cyberattacks. Its aim is to minimize disruption impact and ensure continuous service. Strategies include diversifying suppliers, redundancy in processes, and robust contingency plans.

Supply Chain Compromise entails infiltration by malicious actors, aiming to access or manipulate components or processes. Its goal is to prevent unauthorized access, manipulation, or theft of sensitive data or products. Compromise can occur through cyberattacks, malware insertion, or tampering with physical goods.

4. Supply Chain Resilience

Supply chain resilience against cyber threats refers to the capacity of a supply chain to withstand, adapt to, and recover from cybersecurity incidents and disruptions while maintaining the continuity of operations. Ensuring supply chain resilience against cyber threats is crucial in today's interconnected and digital-driven business environment.

Supply Chain Resilience - Outcomes

Suppliers are frequent targets of cyberattacks, posing direct risks to downstream organizations. Malware and ransomware can disrupt operations, leading to downtime, delayed deliveries, and financial losses. Stolen data, like customer information or proprietary designs, may be used fraudulently or sold on the dark web.

Third-party vendors can serve as entry points for cyberattacks, while insiders may leak sensitive information or engage in sabotage. Nation-state actors may conduct cyber espionage, targeting supply chains for competitive advantage or infrastructure disruption.

Supply chain management software vulnerabilities can be exploited for order manipulation or unauthorized data access. Internet of Things (IoT) devices in supply chains, such as sensors, are also susceptible to cyberattacks.

To bolster supply chain resilience against cyber risks, proactive measures like risk assessments, robust cybersecurity, employee training, and collaboration with suppliers are crucial. The aim is to identify vulnerabilities, mitigate risks, and respond effectively to cyber incidents, safeguarding the supply chain's integrity.

Supply Chain Resilience - Norms & Regulations

Several norms and regulations existed around the world to address and promote supply chain resilience. These regulations varied by region and industry but shared the common goal to increase the Supply Chain Resilience.

1. ISO 22301:2019 (Business continuity management systems) outlines the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining, and continually improving a business continuity management system (BCMS).
2. EU Directive on Security of Network and Information Systems (NIS Directive) (2.0): The NIS Directive imposes security and reporting obligations on operators of essential services and digital service providers.
3. NIST Cybersecurity Framework (2.0) developed by the National Institute of Standards and Technology (NIST), this framework offers guidelines and best practices for organizations to manage and reduce cybersecurity risks.
4. C-TPAT (Customs-Trade Partnership Against Terrorism) is a voluntary program led by U.S. Customs and Border Protection (CBP) that encourages businesses to enhance the security of their international supply chains.

Many countries have established supply chain security programs specific to certain industries or commodities. Certain industries, such as pharmaceuticals and aerospace, have specific regulations related to supply chain resilience and security. These regulations often focus on quality control, traceability, and risk management within the supply chain. Additionally, regional variations exist, and new regulations are continuously being introduced in response to emerging threats and challenges. Organizations should stay informed about relevant regulations in their specific industry and geographic region and adapt their supply chain management practices accordingly to ensure compliance and enhance resilience.

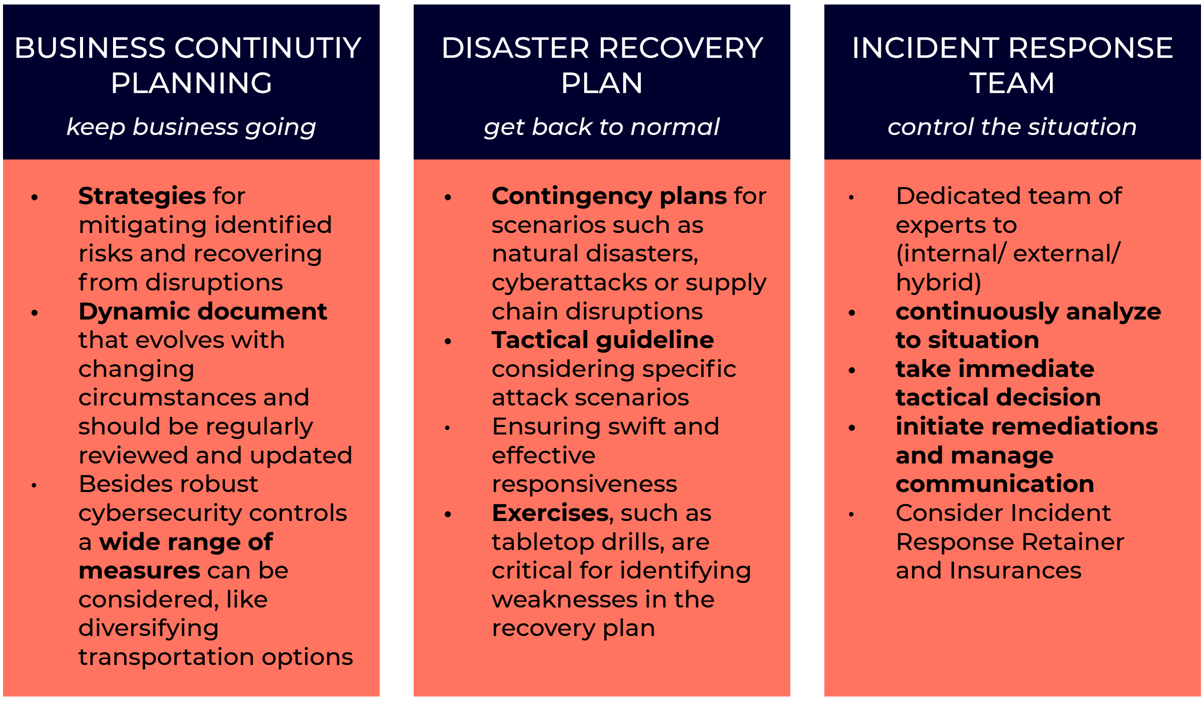
5. Security Controls to foster Supply Chain Resilience and Business Continuity Management

Business continuity management (BCM) is a critical framework that plays a critical role in ensuring the seamless and uninterrupted operation of the automotive supply chain. In this complex and interdependent industry, many factors, including natural disasters, cyber threats, logistical challenges, and geopolitical issues, pose significant risks. Therefore, a comprehensive approach to BCM is essential for automotive business continuity management (BCM) is pivotal for ensuring uninterrupted operations in the automotive supply chain, given its intricate nature and susceptibility to diverse risks like natural disasters, cyber threats, and logistical challenges. A tailored approach to BCM, aligned with organizational circumstances and risk profiles, is imperative. Regular reviews and updates of continuity plans are essential to adapt to evolving threats.

A fundamental aspect of BCM in this context is rigorous risk assessment, encompassing the identification of threats and vulnerabilities throughout the supply chain. Supplier and vendor evaluation, along with the adoption of multiple sourcing strategies for critical components, enhance supply chain resilience. Real-time visibility solutions aid in monitoring shipments and inventory, facilitating prompt response to disruptions.

A robust business continuity plan (BCP), continuously updated and tested, forms the crux of BCM. Containing strategies for risk mitigation and recovery, it addresses scenarios like natural disasters and cyberattacks. Measures such as maintaining adequate inventory, diversifying transportation options, and implementing cybersecurity controls are vital for resilience. Employee training, physical security measures, and effective collaboration with stakeholders further bolster preparedness.

Exploring insurance policies covering supply chain disruptions adds an additional layer of financial protection. Ensuring business continuity in the automotive supply chain is indispensable for meeting customer demand and sustaining industry success, necessitating a multifaceted approach encompassing physical, operational, and cybersecurity measures.



BUSINESS CONTINUTIY PLANNING

keep business going

- **Strategies** for mitigating identified risks and recovering from disruptions
- **Dynamic document** that evolves with changing circumstances and should be regularly reviewed and updated
- Besides robust cybersecurity controls a **wide range of measures** can be considered, like diversifying transportation options

DISASTER RECOVERY PLAN

get back to normal

- **Contingency plans** for scenarios such as natural disasters, cyberattacks or supply chain disruptions
- **Tactical guideline** considering specific attack scenarios
- Ensuring swift and effective responsiveness
- **Exercises**, such as tabletop drills, are critical for identifying weaknesses in the recovery plan

INCIDENT RESPONSE TEAM

control the situation

- Dedicated team of experts to (internal/ external/ hybrid)
- **continuously analyze to situation**
- **take immediate tactical decision**
- **initiate remediations and manage communication**
- Consider Incident Response Retainer and Insurances

Figure 2: The Elements of Business Continuity Management (BCM)

6. Supply Chain Compromise

The integration of digital technologies in vehicles has heightened cybersecurity threats in the automotive industry. This complexity in supply chains leads to unique security challenges at each tier. Security compromises within the supply chain jeopardize component integrity, vehicle safety, and data privacy. To address these risks, manufacturers and suppliers must implement rigorous security measures such as authentication, encryption, and monitoring. Compliance with industry standards and regulations also plays a crucial role in ensuring security and integrity.

Supply Chain Compromise - Outcomes

As vehicles increasingly rely on software and connectivity, security breaches in the automotive supply chain pose multifaceted risks beyond data exposure, impacting vehicle safety and functionality. This underscores the critical importance of robust cybersecurity practices within the industry.

Counterfeit automotive parts infiltrating the supply chain present a significant hazard, compromising product quality and safety, often resulting in recalls and reputational damage. Electronic Control Units (ECUs) are susceptible to malware attacks if supply chains are compromised, potentially leading to performance issues, safety hazards, or unauthorized vehicle control.

Supply chain breaches may also involve fraudulent safety testing and certification processes, allowing substandard components to enter vehicles, endangering occupants. Compromised Vehicle-to-Infrastructure (V2I) communication systems could impede critical traffic and safety information transmission.

In the connected car era, the collection and transmission of driver and vehicle data raise privacy concerns. Breaches in supply chain security may grant unauthorized access to sensitive information, as seen with vulnerable key fobs susceptible to manipulation for unauthorized vehicle access.

To address these risks, automotive stakeholders must implement robust supply chain security measures such as authentication, encryption, and monitoring. Compliance with regulatory standards is essential for ensuring industry-wide security requirements are met.

7. What resources are needed?

There are various norms and regulations aimed at addressing supply chain compromise. These regulations focused on ensuring the integrity and security of supply chain components.

1. EU Cybersecurity Act and NIS Directive (EU): These regulations set cybersecurity standards for critical infrastructure and digital service providers in the EU, addressing supply chain security and incident reporting.
2. NIST Special Publication 800-171 (US): Provides guidelines for safeguarding Controlled Unclassified Information (CUI) in non-federal systems, emphasizing measures to prevent supply chain compromise.

Countries have established industry-specific supply chain security programs and customs regulations to ensure the integrity of supply chain processes and combat illicit trade. Sectors like healthcare and finance adhere to specific regulations emphasizing data protection and cybersecurity practices. Staying updated on relevant regulations is essential to avoid legal consequences and reputational damage. Continuous improvement of supply chain security practices is vital to mitigate risks.

Two main approaches—white box and black box—are used to assess supply chain security. The white box approach involves examining internal workings, while the black box approach evaluates systems with unknown architecture.

8. Software Bill of Material (SBOM) – White Box Approach

Software Bill of Materials (SBOMs) are structured lists detailing the components and software dependencies of a given software application or system. They play a crucial role in tracking and managing software components within projects or products.

Various industries and regulatory bodies mandate organizations to maintain accurate records of software components, aligning with licensing agreements, open-source software usage, and legal requirements. In supply chain security, SBOMs aid in comprehending software composition and identifying security risks linked to third-party providers or dependencies.

SBOMs facilitate risk evaluation of software components, enabling organizations to gauge the impact of vulnerabilities in third-party libraries or components on overall software security and stability. Through comprehensive documentation of software components and versions, organizations can promptly identify known security flaws and undertake appropriate risk mitigation measures.

A typical SBOM includes information such as:

- The names of software components and libraries
- Version numbers of each component
- Licensing information (e.g., open-source licenses)
- Dependencies between components
- Vendor or supplier information
- Security-related data, including known vulnerabilities

Automated tools are commonly utilized to generate and manage SBOMs, particularly for intricate software systems with numerous dependencies. The industry is increasingly acknowledging the significance of SBOMs in software security and supply chain management, with emerging initiatives and standards advocating for their adoption.

The following Figure 2 shows the method for identifying compromised software components.

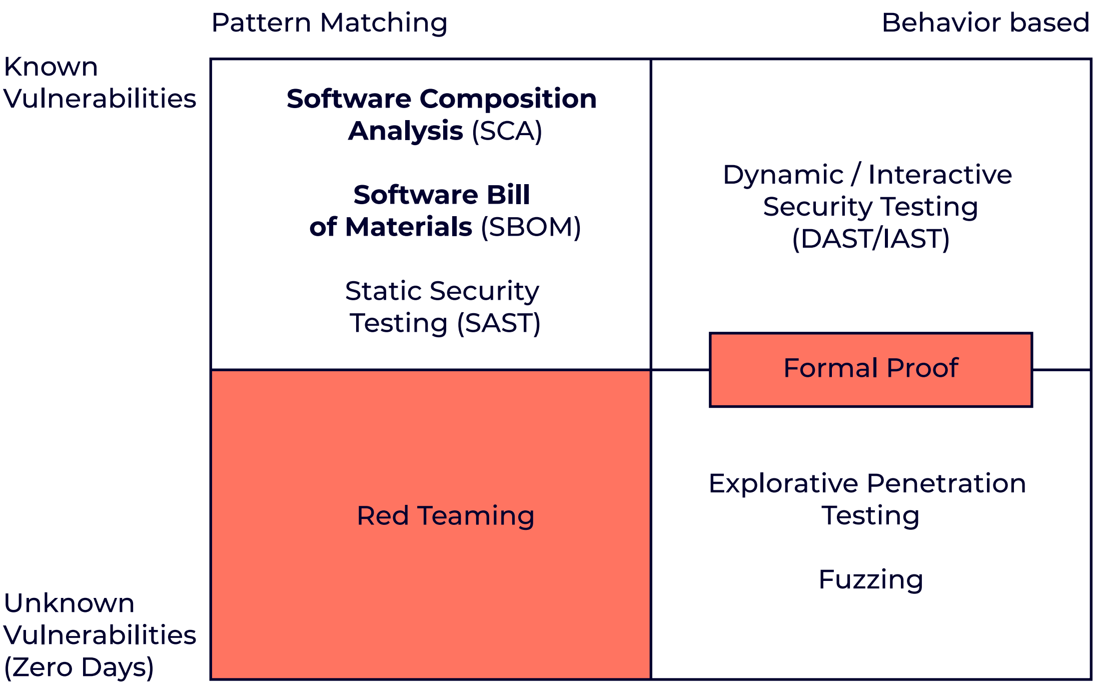

Pattern Matching
Behavior based
Known Vulnerabilities
Unknown Vulnerabilities (Zero Days)
Software Composition Analysis (SCA)
Software Bill of Materials (SBOM)
Static Security Testing (SAST)
Dynamic / Interactive Security Testing (DAST/IAST)
Formal Proof
Red Teaming
Explorative Penetration Testing
Fuzzing

Figure 3: METHODOLOGIES to identify compromised software components

9. Software Composition Analysis (SCA) – Black Box Approach

Software Composition Analysis (SCA) is a security practice that focuses on identifying and managing the open-source and third-party components used in software applications. It involves analysing and monitoring the software dependencies within an application to:

Identify Components: Discover all third-party libraries, frameworks, and open-source software components relied upon by a software application.
Assess Vulnerabilities: Evaluate these components for known security flaws, providing information on any vulnerabilities present in the software's dependencies.

License Compliance: Verify compliance with open-source software licenses, ensuring adherence to licensing requirements for third-party components.
Risk Management: With insights into vulnerabilities and licensing issues, SCA aids organizations in evaluating and mitigating risks within the software supply chain.

Remediation: Offer recommendations for addressing issues, such as upgrading to patched library versions or selecting alternative components with fewer vulnerabilities or more compatible licenses.

Software Composition Analysis is crucial in contemporary software development and cybersecurity, given the prevalent use of open-source components and libraries. It enables organizations to uphold software security and compliance while harnessing the advantages of third-party software components.

10. Best Practices

Mitigating supply chain security issues is crucial to safeguarding the integrity and reliability of your supply chain operations.

Table 1: Best practices fostering supply chain resilience and mitigation supply chain compromise

No.	Security Control	Description
1	Risk Assessment	Conduct comprehensive risk assessments to identify vulnerabilities, threats, and potential weaknesses in your supply chain. Consider both physical and cybersecurity risks.
2	Security Standards and Certifications	Encourage suppliers to adhere to recognized security standards and certifications, such as ISO 27001 for information security management.
3	Incident Response Plan	Review robustness of incident response plans from suppliers that outline steps to take in the event of a security breach or compromise within the supply chain.
4	Supply Chain Resilience	Develop and maintain supply chain resilience plans to address disruptions and recover quickly from adverse events.
5	Regulatory Compliance	Stay informed about relevant regulations and standards related to supply chain security and ensure compliance with them.
6	Cybersecurity Insurance	Enforce cybersecurity insurance to foster financial resilience in a supply chain security breach.

11. Summary

Automotive supply chain security is increasingly vital in today's tech-driven industry. With software integration, cybersecurity is paramount to safeguard vehicle safety and data integrity against threats like counterfeit parts and cyberattacks. Regulatory standards like ISO 21434 and the Supply Chain Act aim to address these challenges.

To enhance resilience, organizations conduct thorough risk assessments, implement robust cybersecurity measures, and collaborate closely with stakeholders. Emerging practices like Software Bill of Materials (SBOM) and Software Composition Analysis (SCA) help manage software-related risks. Effective security measures include encryption, access control, continuous monitoring, and comprehensive employee training. Compliance with regulations like GDPR and CCPA is essential, alongside regular audits, contingency plans, and transparent communication with supply chain partners.

By implementing the presented best practices and staying proactive, organizations can enhance their supply chain security and reduce the risk of security issues and disruptions. Organizations should regularly review and update their security practices to address emerging threats.

Supply chain security is an ongoing, adaptive process, requiring constant vigilance and adaptation to emerging threats and regulations.

12. P3 Group

Contact for questions and remarks

Tobias Löhr

Associate Partner
Cybersecurity & SW Compliance

tobias.loehr@p3-group.com

Benedikt Bauer

Senior IT & Security Consultant

benedikt.bauer@p3-group.com

Introduction of P3 Group

P3 is an independent and international consulting company that offers consulting and engineering services, as well as software development for numerous customers. Since its founding in 1996 in Aachen, Germany, P3 always found new branches and has over 1900 employees in 26 locations in close vicinity of its customers.

Vision - We advise our clients strategically in the areas of technology strategy, business process optimization and organizational development. P3 develops new business models, opens future revenue sources for the clients and accompanies them in building up competencies.

Perspective - We carry out complex projects and optimize business processes in customer organizations and their global supplier network. P3 supports and empowers customer organizations to create robust structures to operate sustainably and grow in the future.

Insight - We develop & test innovative IT solutions for specific business requirements. From individual solutions to cloud-based IoT services. P3 delivers end-to-end solutions in security consulting and ensures a seamless service and product rollout.

Automotive Cybersecurity Services of P3 Group

P3 is an END-TO-END SECURITY SERVICE PROVIDER advising on GOVERNANCE, RISK & COMPLIANCE and providing MANAGED SECURITY SERVICES.

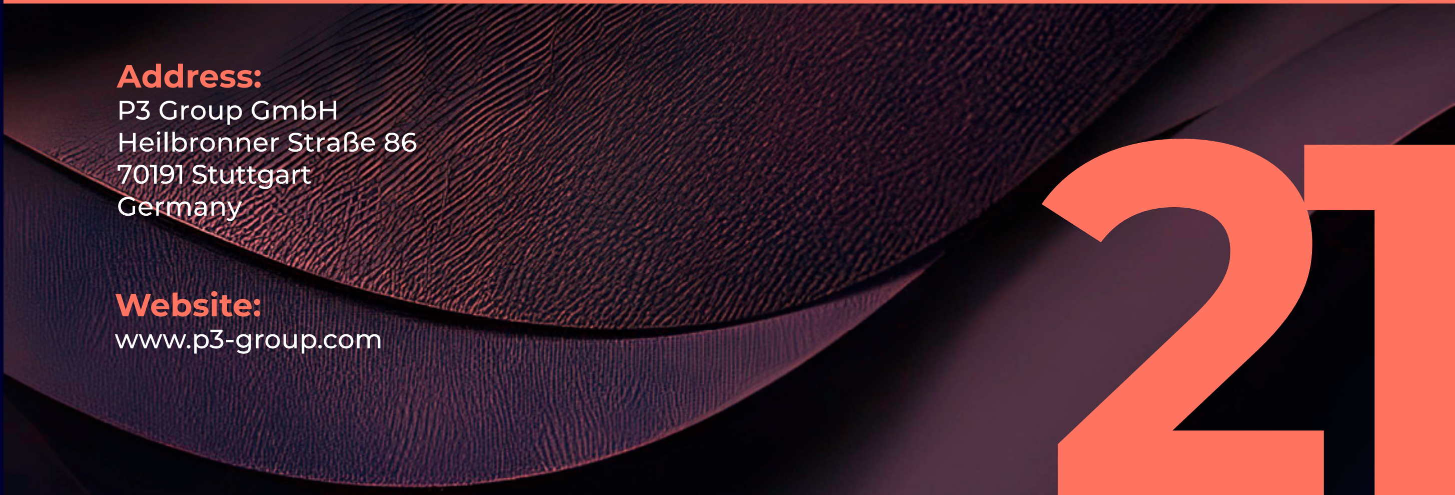
We help automotive companies to conceptualize and implement effective security management systems and are proficient in handling complex product and project environments. Our best practices help to achieve compliance with global standards and regulations on security, privacy, and data governance. We support our customers in security certification and authority communication.

Our enabling services ensure successful change of global organizations with large-scale training & awareness programs and End-to-End security toolchains.

Managed Security Services cover the full security cycle including predict, prevent, detect, respond. Our services are provided from our near shoring locations in Mexico, Romania, Thailand with an onsite point of contact. Our onsite customer interface ensures efficient service execution considering customer specific needs. Our team earned various security certifications - technical, governance and industry specific - and is proficient in a wide range of security tools.

Disclaimer

This document and all information contained herein are the sole property of P3. No intellectual property rights are granted by the delivery of this document or the disclosure of its content. This documentshall not be reproduced or disclosed to a third party without the express written consent of P3. This document and its contentshall not be used for any purpose other than that for which it is supplied.



Address:
P3 Group GmbH
Heilbronner Straße 86
70191 Stuttgart
Germany

Website:
www.p3-group.com