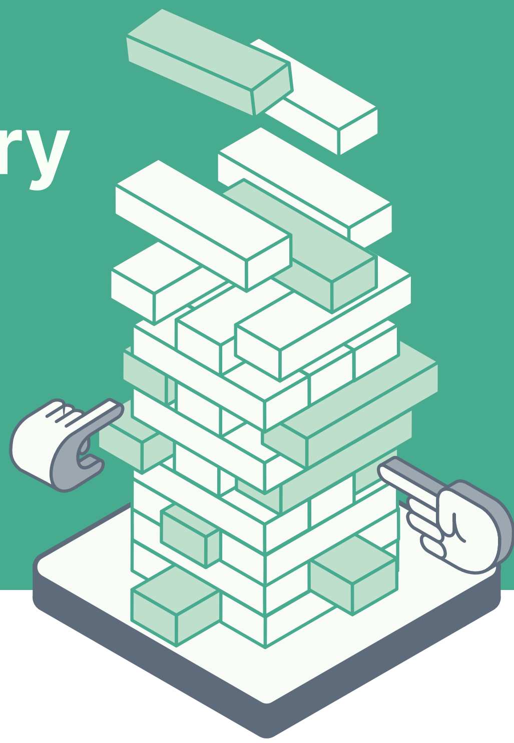
CLOUDYRION

Supply Chain Security in the Financial Industry



A FinTech company relies on in-house resources as well as external suppliers and project teams to develop digital applications for end users. To establish a compliance-compliant security-by-design approach prior to the go-live of new solutions, Cloudyrion's experts were brought on board as IT security partners.

STARTING POINT

Supply chain attacks have been a concern for cybersecurity experts for many years, as the chain reaction triggered by an attack on a single supplier can put an entire network of suppliers at risk. Malware is the predominant attack technique, used in 62 percent of attacks. According to ENISA's Threat Landscape for Supply Chain Attacks report, which analyzed 24 recent attacks, it is no longer enough for companies to have strong IT security because attackers have already shifted their attention to suppliers. This is evident in the increasing impact of these attacks: system downtime, financial losses and reputational damage.

Experts indicated that supply-chain attacks quadrupled in 2021 compared to the previous year. This trend underscores the need to act, both for companies and their decision makers. There is an urgent need to implement new safeguards to prevent potential supply chain attacks in the future and respond appropriately when needed.

Development
The increasing threat of malicious code infiltration makes it necessary to specifically secure internal code and structural dependencies – in open source as well as commercial tools. The consequences of a compromised software build and delivery pipeline included leaked trade secrets or other sensitive data and tampering with code before release. Software development managers must work with their security and risk officers to ensure the integrity of internal and external code by enforcing strict version control. Common security-effective recommendations include using artifact repositories for trusted content and managing vendor risk during the deployment lifecycle, as well as securing secrets and signing both code and container images.

Application
In this case, coordinating disparate delivery pipelines from the various teams involved in large-scale development projects of software applications and services for end customers proved to be a major challenge, time and again. In particular, the automated detection of vulnerabilities and malicious code was a difficult task because of the large number of instances involved with different levels of awareness of the issue.

Supply Chain Security
The goal: establish holistic supply chain security leaving no vulnerabilities open, from development to the end user, through which systems and processes could be compromised. The desired risk management included pipeline security, including all tests and tools used there, as well as security during the use of the application in practice (runtime). The company became aware of Cloudyrion through recommendations based on positive experiences and contacted the Düsseldorf-based IT security specialists. Above all, the security service provider impressed its prospective client with an approach that combines comprehensive consulting, technological expertise and solution-oriented, pragmatic user assistance.

CHALLENGE

The financial company needed a systematic security-by-design approach to ensure that its software, which is produced by many internal developers and suppliers, is free of vulnerabilities and malware and can be delivered to end customers. Cloudyrion was asked to optimize the entire process, from development to field deployment, from a security perspective and back it up with the governance to make the products more secure for both end customers and enterprise customers. A key target was to reach the state of so-called Minimum Valuable Security after three months.

The challenges:

- **Technological diversity, i.e., unrestricted functionality in a hybrid cloud environment**
- **Rapid software release cycles and insufficient pipeline software guardrails for application and infrastructure-as-code**
- **Regional distance between teams**
- **Compliance requirements (according to GDPR or EU-DSGVO and PCI-DSS)**
- **Insecure and highly segmented continuous integration/continuous delivery (CI/CD) tools**

SOLUTION

A detailed threat assessment was performed at the beginning. With the respective teams, Cloudyrion identified potential attack vectors as well as attackers and risk scenarios.

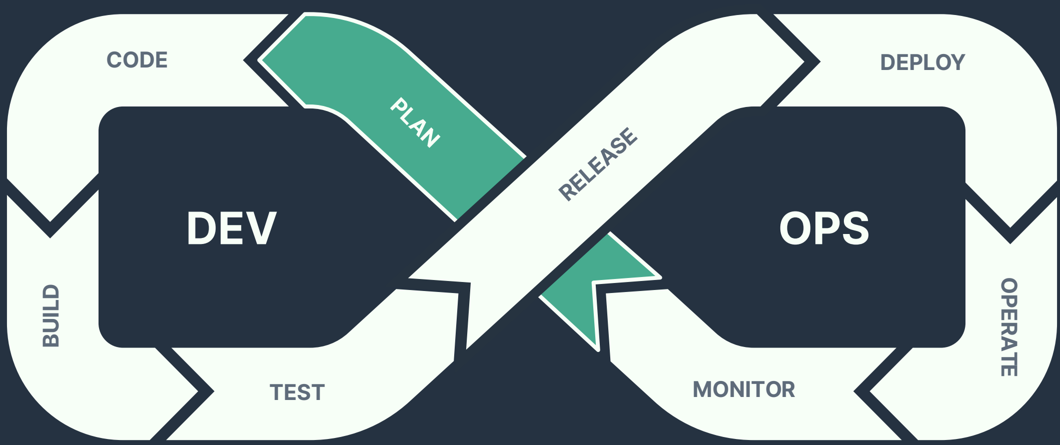
Examples from the interface between client and supplier include the complete verification of:

- **Single Sign-On integration**
- **IPS systems**
- **Web Application Firewalls**
- **Identity & User Access Management: assignment of access rights and consistent role distribution on the part of the users**
- **Provision of environments and applications for admins on the internet**
- **Certificates such as ISO, PCI-DSS, etc.**

Based on the results, the design of the security infrastructure was adapted, and the appropriate measures were implemented to effectively eliminate the identified threats. The time frame set for the project turned out to be particularly critical at an early stage. With the start of the security-by-design process, the iterative implementation of crucial project steps picked up speed, so nothing stood in the way of a secure and compliance-compliant go-live after three months. As the project progressed, the client decided to extend the process in order to continuously reduce the attack surface beyond the already-achieved minimum requirements and gradually increase security maturity more and more.

The most important to-dos for Cloudyrion at a glance:

- **Developing a joint strategy with the customer, including defining and scheduling targets**
- **Targeted support of the teams in introducing SCA, DAST or IAST into their pipeline and in the correct interpretation of the results**
- **Detailed process design for the development phase, including the definition of risk-based pipelines (guardrails)**
- **Recommending a Trusted Container Registry/Software Code Repository approach; Background: too many tools with the same functions complicated deployment. Centralization with approved tools led to standardized and controlled deployments.**
- **Hardening of the CI/CD environment with regard to security**
- **Evaluation of the security level of external software suppliers**



OUTLOOK

In accordance with needs and at the company's request, Cloudyrion continued to support users with advice after the three months following the go-live. The fact that the security consultants had previously succeeded in providing the users with the necessary know-how to confidently solve frequently occurring standard questions during the runtime paid off here. As a result, the experts were consulted primarily when unusual problems arose, such as when selecting and implementing an SCA Enterprise solution that had not previously existed. This strategic approach has proven its worth and is also recommended for any future projects outside the Supply Chain Security segment.

BENEFITS AND ASSESSMENT

„As with many of our customers, we have received particularly positive feedback about our ability to find and implement pragmatic solutions in the context of a project - and precisely because we do not go about it with the ‚security says no' attitude feared throughout the industry," explains Okay Güler, Founder & IT Security Consultant at Cloudyrion. „What is valued is our flexibility in supporting people on-site to develop an awareness around the topic of IT security and sustainably anchor it in their processes."

Key results

- **Higher security level for services for end users**
- **Acceleration of go-to-market timelines**
- **Faster deployment of version updates**
- **Exposure of strategy gaps on the enterprise side**
- **Significantly improved security awareness and know-how transfer**

Are you looking for a reliable partner who supports your team, successfully implements ambitious and security-critical IT projects, and can guarantee long term availability?
Get in touch - we would love to help.