Information Security Assurance for IoT

Securing an innovative Internet-of-Things data platform to go-live with confidence.

planit. an NRI company

www.planit.com

Key outcomes

- Implemented strategic security measures to secure the data platform in the short and long run.
- Strengthened security stance before placing data platform on the market and offering access to customers.
- Improved customer confidence from better ability to maintain contractual and regulatory compliance requirements.
- Improved readiness to recognise a cyberattack and take prompt action to eliminate possible negative impacts.

Delivered

- Security Testing
- Penetration Testing

The challenge

This agricultural technology (AgTech) company is revolutionising the livestock industry with its proprietary smart ear tag and information platform.

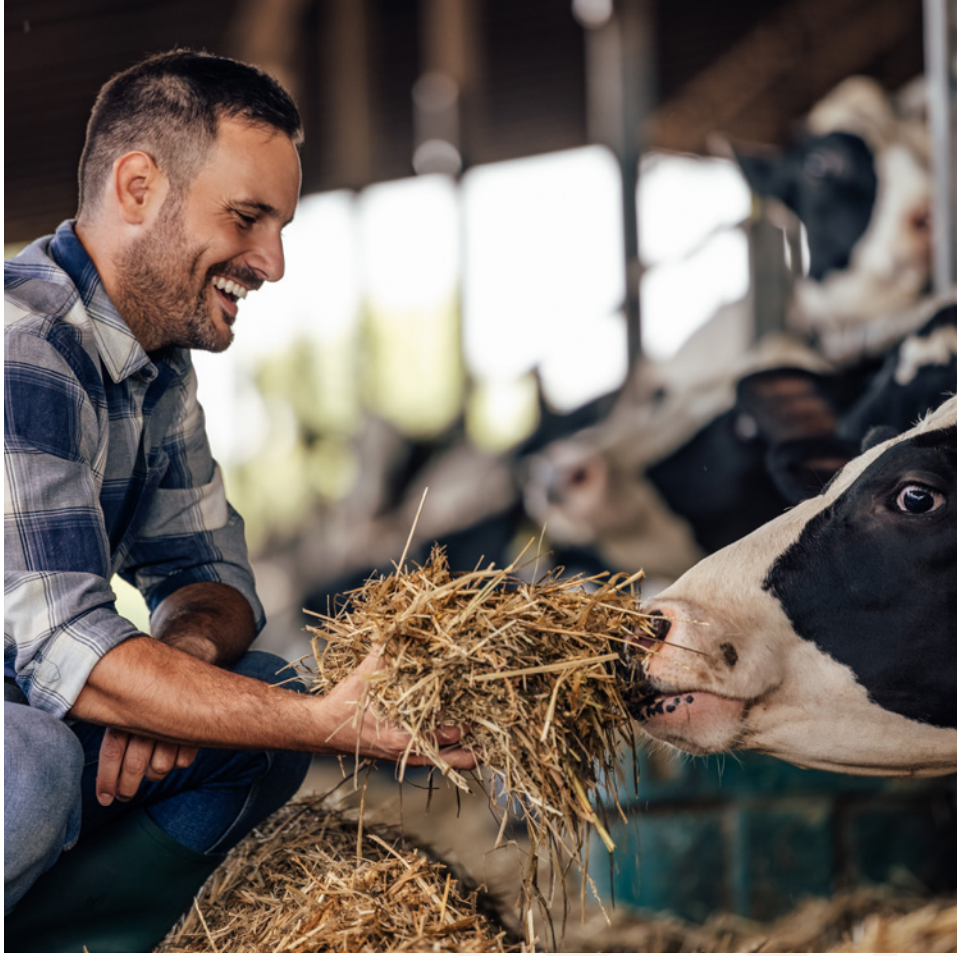
The ear tag incorporates a GPS tracking system, RFID, accelerometer, ambient temperature, geofencing capability, Bluetooth, and satellite connectivity. These functions are then used to collect various types of information about the animal, while on-tag analytics monitor whether behaviour is following normal patterns.

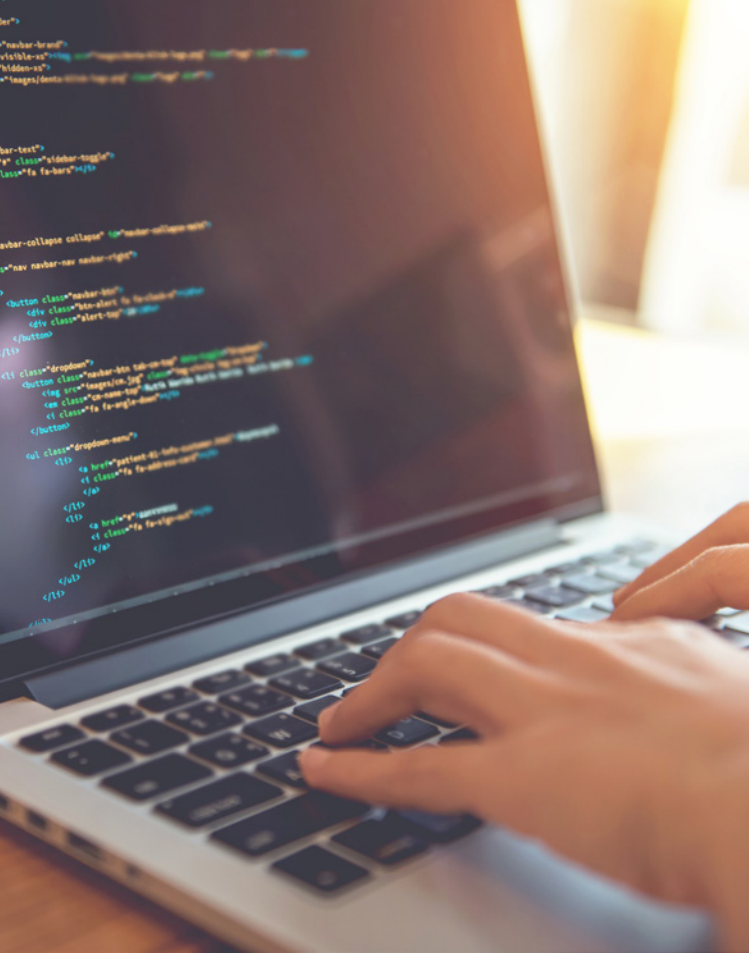
The tag consistently collects and transmits this data every five minutes to low earth orbit satellites. It is then sent to the central data platform where it is combined for further data analytics.

Data and insights are transmitted to partner software platform(s), with access controlled and changed over time as the livestock moves through the supply chain. The information provided allows farmers to optimise their operational management, improve detection of stolen livestock, and gain increased insights into animal welfare and health.

The data platform consists of a large database of sensitive information, making it an appealing target for intruders. In recognition of this risk, the company required a high level of protection for their Cloud-based application to ensure robust data security for their customers.

The company's leadership team recognised that they needed adequate security measures to confidently protect their valuable assets from unauthorised access. The team also identified that they did not have the expertise in-house to complete a security assessment, and therefore required a partner to evaluate the security levels of their solution, identify possible vulnerabilities, and help eliminate any revealed security issues.





The solution

The company engaged Planit through the recommendation of one of their existing software partners. We carried out an external penetration test against their solution and provided a report detailing any vulnerabilities discovered, potential impact, and recommendations to remediate the risks identified.

Planit's security engagement model provides a tailored security assurance solution. It began with a discovery phase, where a preliminary review of the solution was completed.

The review enables identification of the areas of the solution to be targeted (a.k.a. the attack surface), the risk appetite, the attacker profile, and the appropriate assessment services. The results of this activity are captured as the scope and schedule, with the scope detailing the attack surface to be covered, and the schedule aligned to the project timeframe.

A basic threat model was defined, and an objective was established - to reveal if attackers could access the sensitive data stored in the data platform. The attacker profile was a proficient hacker who had Internet access exclusively.

For the reconnaissance phase of the penetration test, the web application was mapped out to determine all functionality present, roles available, and what functionality was present for each role in the system. The functionality was then investigated in further detail to determine which API calls were made on each page and for each action a user could do.

Based on the results of the reconnaissance, the security team identified potential weaknesses and entry points through the identification of common vulnerabilities, such as command/code injection, missing authorisations, sensitive data exposure, and outdated libraries that contain known vulnerabilities. The security team also investigated business logic holes that sometime become a blind spot to the development team and functional testers.

Our comprehensive report outlined the entire penetration testing process to clearly show what areas of the data platform were tested.

If a vulnerability is positively identified, the report outlines what risks it poses for the system and business, and how the security team attempted to exploit it through weaponisation of proof-of-concept code, reverse engineering, and many other innovative ways and techniques of breaking in.

Our initial assessment identified that automated security scanning would not provide sufficient penetration to identify complex issues.

Therefore, it was recommended most of it was done manually. This has the added benefit of closely simulating an actual attacker who is not a bot, but has expert technical computing skills, access to tools, and an intention to steal.

Outcome

Our penetration test process identified several vulnerabilities which were captured in an interim report that contained recommendations to mitigate the associated risks. Our security team also presented the findings and recommendations of the report to the company.

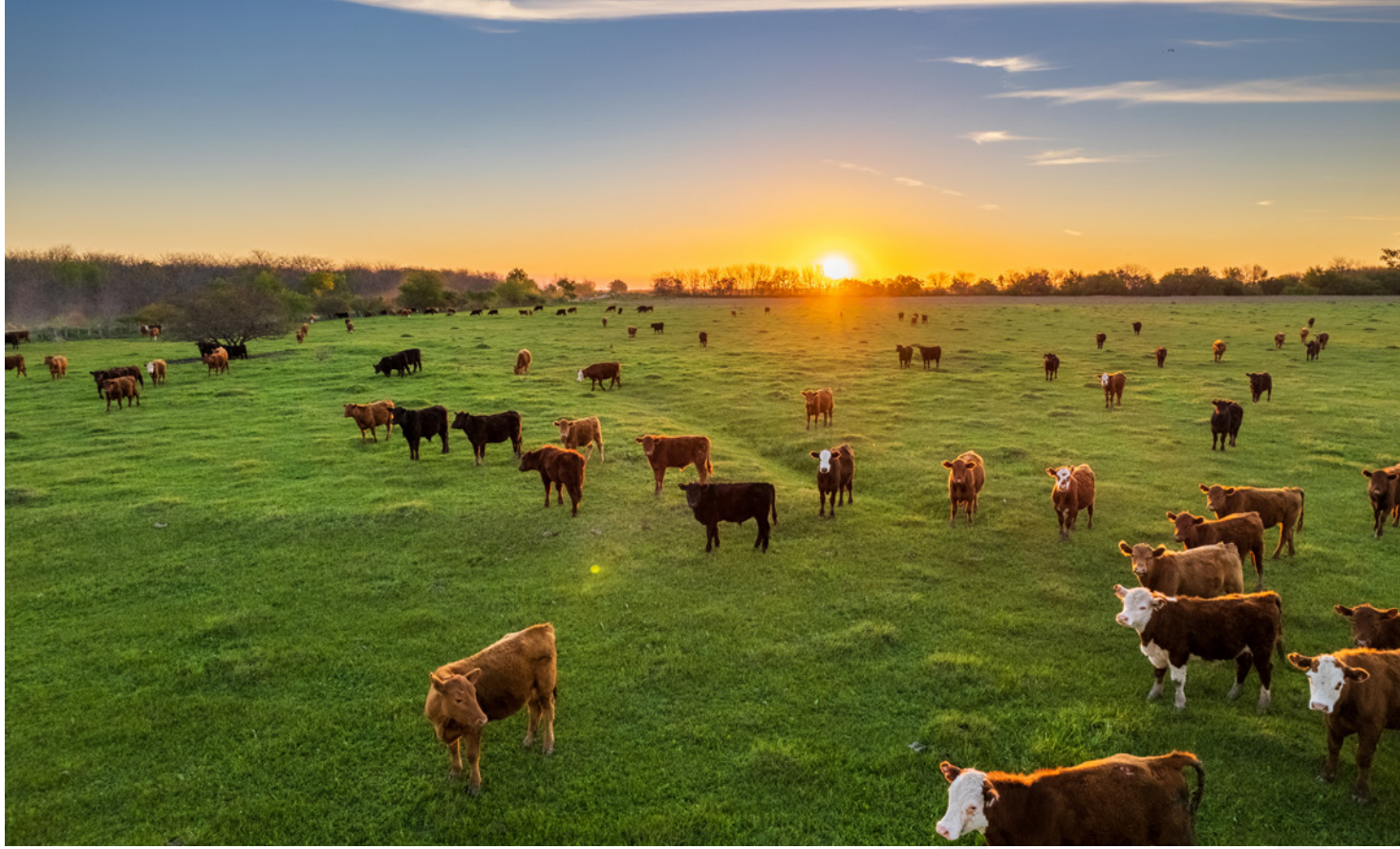
Following our report and presentation, the company leveraged the results of the penetration test to prioritise and systematically implement the recommendations. This enabled them to strengthen the security of their data platform before placing it on the market and offering access to their customers.

In addition to revealing technical issues, the penetration test enabled the company to evaluate their readiness to recognise an attack and take appropriate action to eliminate any potential impact. It also demonstrated the value of including penetration testing in the requirements for the next phase of the data platform's development.

Following confirmation by the company's development team that our recommendations were implemented, we tested the changes to confirm that they had been made correctly and caused no subsequent issues. Since the penetration testing and re-testing was done in a staged development environment, the company's development team experienced no disruption to the data platform.

By testing the data platform against best practice standards and protocols for security, our penetration testing provided the company with the necessary confidence to go-live on schedule. The improved security posture also improved their ability to maintain contractual and regulatory compliance requirements, which boosted customer confidence and the company's competitiveness within the AgTech sector.

All our penetration testing for various clients has been delivered on time and on budget. This company is our latest customer to realise these same benefits.



About Planit

We can help you protect your valuable assets and brand reputation. Following an international best practice methodical approach, we provide you with in-depth reports into weaknesses that attackers could exploit in your specific systems. We can then work with you to close these loopholes.

Find out how Planit's three-pronged approach to security testing can help you protect your systems by addressing development, use, and infrastructure.

planit an NRI company

www.planit.com