PRESS RELEASE
25 April 2023
Paris

Thales seizes control of ESA demonstration satellite in first cybersecurity exercise of its kind

- For the third edition of CYSAT, the European event entirely dedicated to cybersecurity for the space industry, taking place on 26-27 April 2023 at Station F in Paris, the European Space Agency (ESA) set up a satellite test bench to simulate attempts to seize control of OPS-SAT, a nanosatellite operated by the agency for demonstration purposes.
- Thales's offensive cybersecurity team stepped up to the challenge, identifying vulnerabilities that could enable malicious actors to disrupt operation of the ESA satellite.
- The results of the ethical satellite hacking exercise, the first of its kind in the world, will be used to tighten security for the satellite and its onboard applications, helping to improve the cyber resilience of space systems, protect sensitive data and support the long-term success of space programmes.

Artist's impression of OPS-SAT. Credit: ESA – European Space Agency

The European Space Agency (ESA) challenged cybersecurity experts in the space industry ecosystem to disrupt the operation of the agency's OPS-SAT demonstration nanosatellite. Participants used a variety of ethical hacking techniques to take control of the system used to manage the payload's global positioning system, attitude control system[1] and onboard camera. Unauthorised access to these systems can cause serious damage to the satellite or lead to a loss

[1] *The attitude of a satellite refers to its orientation or position relative to a reference frame, which is usually the Earth. Specifically, it describes the satellite's three-dimensional orientation with respect to three perpendicular axes: roll, pitch, and yaw.*

of control over its mission. Thales's offensive cybersecurity team worked with the Group's Information Technology Security Evaluation Facility (ITSEF[2]) for this unique exercise, which demonstrates the need for a high level of cyber resilience in the very specific operating environment of space.

The Thales team of four cybersecurity researchers accessed the satellite's onboard system, used standard access rights to gain control of its application environment, and then exploited several vulnerabilities to introduce malicious code into the satellite's systems. This made it possible to compromise the data sent back to Earth, in particular by modifying the images captured by the satellite's camera, and to achieve other objectives such as masking selected geographic areas in the satellite imagery while concealing their activities to avoid detection by ESA. The demonstration was organised specifically for CYSAT to help assess the potential impact of a real cyberattack and the consequences for civilian systems.

Throughout the exercise, ESA had access to the satellite's systems to retain control and ensure a return to normal operation.

"Thales is grateful to ESA and the CYSAT organisers for providing this unique opportunity to demonstrate the ability of our experts to identify vulnerabilities in a satellite system. With the growing number of military as well as civil applications that are reliant on satellite systems today, the space industry needs to take cybersecurity into account at every stage in the satellite's life cycle, from initial design to systems development and maintenance. This unprecedented exercise was a chance to raise awareness of potential flaws and vulnerabilities so that they can be remediated more effectively, and to adapt current and future solutions to improve the cyber resilience of satellites and space programmes in general, including both ground segments and orbital systems." **Pierre-Yves Jolivet, VP Cyber Solutions, Thales.**

In a presentation on 27 April by Thales experts and members of the ESA team, CYSAT participants can find out more about the attack scenario used in this first demonstration of offensive cybersecurity techniques, tactics and procedures.

Thales's cybersecurity capabilities for the space industry

Drawing on more than 40 years of experience in cybersecurity and space activities, Thales applies the principles of "cybersecurity by design" to the products it develops for satellite operators and space agencies. Its joint venture with Leonardo, Thales Alenia Space, designs and delivers innovative solutions for telecommunications, navigation, Earth observation, environmental monitoring, space exploration, scientific research and orbital infrastructures. With more than 3,500 cybersecurity specialists, Thales helps to ensure the security of satellite systems for national and European space programmes – in particular Europe's Galileo satellite navigation programme – and at the international level. With its combined expertise in cutting-edge satellite systems and cybersecurity solutions relying on the latest military technologies, Thales offers governments, institutions and enterprise customers a comprehensive range of cybersecurity solutions to guarantee robust protection of all the elements of a space system. The offensive cybersecurity capabilities demonstrated by Thales at CYSAT enable customers to better anticipate and respond to current and future threats. The Group's cybersecurity solutions for the space industry encompass everything from risk and threat evaluation to data protection and network security, incident detection and response, and security maintenance throughout the system life cycle.

[2] *An Information Technology Security Evaluation Facility (ITSEF) is a trusted, independent third-party product security testing facility accredited by a national certification body (ANSSI in France).*

About Thales

Thales (Euronext Paris: HO) is a global leader in advanced technologies within three domains: Defence & Security, Aeronautics & Space, and Digital Identity & Security. It develops products and solutions that help make the world safer, greener and more inclusive.

The Group invests close to €4 billion a year in Research & Development, particularly in key areas such as quantum technologies, edge computing, 6G and cybersecurity.

Thales has 77,000 employees in 68 countries. In 2022, the Group generated sales of €17.6 billion.

These figures do not include the Transportation business, which is currently being divested.

PRESS CONTACTS

Thales Media Relations
Marion Bonnet
+33 (0)6 60 38 48 92
marion.bonnet@thalesgroup.com

More information:

Cybersecurity solutions | Thales Group

Cyberthreat Hitmap (thalesgroup.com)

Cybersecurity in space: How Thales is meeting the challenges ahead | Thales Group

Thales Alenia Space, a pivotal player in the Galileo program | Thales Group