CyberSmart-Analytics

Avionics Cyber Threats Analysis Services

PROTECT YOUR PLATFORM

Astronautics is providing cyber protection solutions for avionics and military systems, in a group of solutions called CyberSmart.

CyberSmart-Analytics is a service to identify and map all relevant threats to a specific platform.

CyberSmart-Analytics:

❖ **In-depth analysis** of the relevant threats vector, performed by a team of Astronautics' cyber & avionics specialists, teaming together to analyze the relevant platform

❖ **Vulnerability Assessment-** As part of the analysis, the team will generate a full list of platform vulnerability to cyber threats, along with an analysis of each threat implementation feasibility and difficulty to implement, along with the potential damage of the identified threat.

Possible military & avionics Attacks - Hackers may attack today military and airborne platforms in various possible methods, such as:

- ✓ Compromised software loaded into the system
- ✓ Compromised software and/or data loaded via data-link
- ✓ Compromised equipment, infected during maintenance
- ✓ Physically installed "Cyber-Bomb" in an operational system

CyberSmart-Analytics shall evaluate all possible threats to the platform, presenting a full-analysis of threats vectors. Each threats shall be analyzed for the level of system damage potential, along with the possibility to implement & difficulty of such implementation. The provided analysis could be a basis for any cyber-protection implementation required.

Astronautics C.A.Ltd.
A Subsidiary of the Astronautics Corporation of America

16 Martin Gehl St. , P.O.B. 3351
Petah Tikva 4951207, ISRAEL
Tel. (972-3) 9251555 , Fax. (972-3) 9251550
Email: astro@astro.co.il

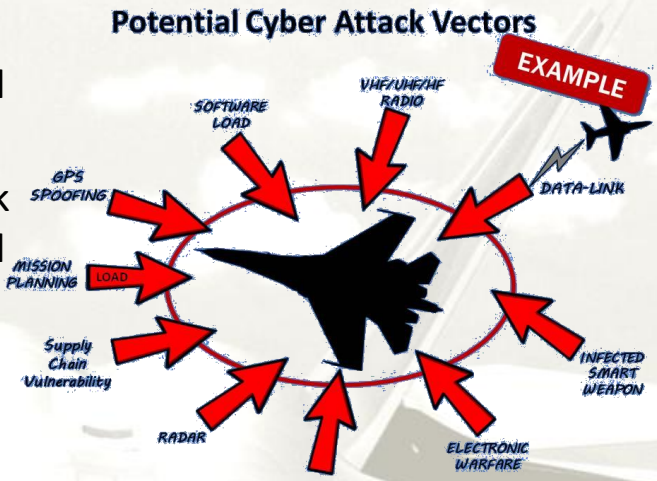
CyberSmart-Analytics

Avionics Cyber Threats Analysis Services

PROTECT YOUR PLATFORM

Threats Analysis Consists of:

- Analyzing the system to determine all potential Threat Vectors
- Capturing the information in an Attack Vector Matrix, for further analysis and to focus on practical solutions
  - Identify threats that are most likely to happen
  - Focus on the threats that may cause significant damage to the system



Threats Analysis shall begin with an interaction with the customer, to capture the specific system architecture and study all relevant interface. At this stage it is expected to receive relevant information from the customer, and perform a Q&A session with the customer to capture all specific system's information required for the analysis.

In the second step of the **Threats Analysis** **Astronautics'** cyber/avionics team shall generate threats vector table, listing all possible **attack vectors**, to the lowest level of details, along with the identification of each threat (spoofing, fishing, Denial Of Service attack etc.), and the assessment of:

- Attack implementation difficulty
- Potential Damage of such attack to the system functionality (Attack severity).

The product of **CyberSmart-Analytics** is an analysis document, that will capture all the above, including a list of recommendation for possible actions to protect the system against all high priority threats that "scored" the maximum score of a combined high-level of a threat to the system, along with a reasonable possibility to implement. This combination indicates that the identified threats have the potential to be the **most vulnerable** areas in the system for **possible compromising by hackers** and should be actively protected.

Astronautics C.A.Ltd.
A Subsidiary of the Astronautics Corporation of America

16 Martin Gehl St. , P.O.B. 3351
Petah Tikva 4951207, ISRAEL
Tel. (972-3) 9251555 , Fax. (972-3) 9251550
Email: astro@astro.co.il