05/2024

BDLI Whitepaper

Education and Training Roadmap in the Field of Cyber Security

Connecting.The.Dots.

Übersicht

Contact

Sentiana Schwerin
Manager Digitalization,
Cyber Security & UAS/AAM

schwerin@bdli.de
+49 173 769 7881

German Aerospace Industries Association
(Bundesverband der Deutschen
Luft- und Raumfahrtindustrie e. V.)

ATRIUM | Friedrichstr. 60 | 10117 Berlin
Tel. +49 30 2061 40-0 | kontakt@bdli.de

www.bdli.de

Introduction

The demand for cyber security expertise in the aerospace industry is growing rapidly. In order to provide industry professionals with the relevant expertise, specific training programs need to be developed. The main issue here is to match industry needs with the current cyber security programs offered by different training organisations and academia.

Education and training for cyber security in the aerospace context is the training of specialists who comprehensively address the security of information and communication systems beyond the traditional concepts of computer security, taking into account innovative techniques for areas such as vulnerability analysis, secure hardware and software development or the generation of threat intelligence using various techniques.

The industry's need for professionals with expertise in both the cyber security and aerospace domains is expected to grow beyond the availability of this expertise. Newcomers may also be career changers who need to be trained in either cyber security or the aerospace domain.

If educational programs focusing on cyber security for aerospace exist, the industry faces a variety of sector-specific challenges, such as limited awareness, competition for talent and regulatory hurdles. Limited awareness can be identified as two separate issues, the first being that companies are not fully aware of the security requirements associated with their products. The second problem the industry suffers from is that potential cyber-capable talents are unaware that the aerospace industry needs them.

It is clear that any recruiter, applicant or newcomer needs some guidance. This industry's many particularities and needs make this document relevant to different stakeholders. This document aims to provide guidance in terms of career paths, education programs, training, and certifications on different levels for professionals in the aerospace industry. This includes experts, leaders and decision-makers.

1. Scope of This Document

This document is organised as follows:

- Identification of job profiles and their requirements
- Overview of relevant training courses
- Overview of relevant certifications
- Education and experience matrix
- Possible measures
- Events

2. Job Profiles

This section describes the different requirements and activities that potentially shape job profiles in the aerospace-cyber industry. As with any work-related activity, a workforce must be in place. Such a workforce shall comply with some personnel requirements. Aerospace companies need to employ cyber security professionals with a combination of technical skills and industry-specific knowledge. These companies may also require candidates to hold specific certifications such as CISSP (Certified Information Systems Security Professional) or CISM (Certified Information Security Manager).

Not only should this workforce exist, but they also should be trained to perform their job properly. Companies in the aerospace industry often provide cyber security training to their employees to ensure they have the necessary knowledge and skills to protect company assets. This training may include cyber security fundamentals, network security, cloud security, incident response and compliance regulations.

Furthermore, companies in the aerospace industry are subject to a wide range of compliance regulations, such as export control regulations, including ITAR (International Traffic in Arms Regulations). To comply with these regulations, cyber security professionals need to stay up-to-date with the latest requirements to ensure that their company's cyber security initiatives meet these standards.

The employee life cycle is also very relevant in this context. It consists of seven stages: attraction, recruitment, onboarding, retention, development, offboarding and happy leavers. Each stage has individual goals and objectives. By meeting these requirements, an organisation can be assured that it provides a holistic employee experience and achieves its organisational goals.

2.1 Fundamentals

Fundamentals include different fields of expertise, such as IT-related knowledge:

- IT systems and procedures
- Storing and processing data, specifically classified data
- Military and civil security
- Laws and regulations

2.2 Job-specific topics

General understanding and awareness

- Security architecture principles, e. g. defence in depth
- Security monitoring
- Terminologies of cyber security (see, e. g. NIST CSRC)

Context-specific standards and regulations

- EASA: Commission Delegated Regulation (EU) 2022/1645 of 14 July 2022 – Information Security, Commission Implementing Regulation (EU) 2023/203 of 27 October 2022 – Information Security
- EUROCAE: ED-20X standards (ED 201/202A/203A/204205)
- ICAO: SARPs – Standards and Recommended Practice

Specific technical topics

- Safety through security
- System interconnection security
- Cryptography
- Threat intelligence
- Next-generation monitoring (NGM)

Embedded security

- Security testing
- Intrusion detection
- Threat analysis/risk assessment
- Secure design principles (Zero trust, secure by design)

Organisational measures

- Electromagnetic interference
- Storage
- Maintenance, repair, overhaul
- Information security management system (ISMS)
- Site security

Job roles

- Security architect/engineer for aerospace applications
- Cloud security architect/engineer for aerospace
- SW/HW developer for aerospace
- SW integrator for aerospace
- (Cloud) security expert
- Aerospace security expert
- Penetration tester for aerospace engineering
- Aerospace certification expert for cyber security
- R&D coordinator …

3. Training Courses

3.1 Approach to training

Overall, the requirements for training and further education in the field of cyber security for aerospace reflect the need for specialised knowledge and expertise, compliance with industry-specific regulations, and collaboration across various stakeholders within and outside the organisation.

Training is necessary in the field of cyber security for aerospace for several reasons. Firstly, the cyber security landscape is constantly evolving, with new threats and vulnerabilities emerging all the time. As a result, cyber security professionals must stay up to date with the latest trends, techniques, and technologies. This requires regular training and education, which can help to enhance their knowledge and skills and enable them to respond effectively to new threats.

Whilst cyber security in aerospace targets the aerospace industry, cyber security itself is a transversal topic that requires knowledge of various fields of study covering aerospace systems. It is, therefore, vital to undergo training for the various cyber security aspects related to the mentioned aerospace systems. It would help in the long run to identify possible threat vectors for a system and proactively secure it against them.

These activities ensure compliance with the latest industry regulations and standards. The aerospace industry is highly regulated, with stringent cyber security requirements and regulations that must be met. Training helps cyber security professionals understand these regulations and standards and ensure their company complies with them.

Cyber security is not just the responsibility of the IT department – it is everyone's responsibility. It is paramount to use training as a vehicle to build a strong cyber security culture within the organisation. By providing training to all employees, organisations can raise awareness about the importance of cyber security and empower everyone to play a role in protecting the company's assets and data.

Finally, training is necessary to mitigate the risks associated with human error. Human error is one of the leading causes of cyber security incidents, such as data breaches and cyber attacks. Providing training to employees can help to reduce the likelihood of these incidents occurring by educating them on how to recognise and respond to potential threats and how to avoid common mistakes that could lead to a security breach.

Different types of training include training on the job, eLearning/online learning, and exchanging know-how with other colleagues.

In conclusion, training is essential in the field of aerospace cyber security. It helps to ensure that cyber security professionals stay up to date with the latest threats and vulnerabilities, comply with industry regulations and standards, build a strong cyber security culture within the organisation, and mitigate the risks associated with human error.

3.2 Training courses for different levels

Cyber security training courses

- Implementing and Auditing the Critical Security Controls – In-Depth (SANS)
- Defensible Security Architecture and Engineering (SANS)
- Intrusion Detection In-Depth (SANS)
- Basic IT Protection Training (BSI)
- Information security according to ISO/IEC 27000 series (TÜV)
- See under certifications also.

Aerospace-specific training courses

- Aviation Cyber Security Training (EUROCAE)
- CS-2X Certification Specification Series (EASA)
- Unmanned Aircraft Systems Airworthiness and Safety Training (EUROCAE)
- Common European (Safety) Management System Assessment Method (EASA)
- Continuing Airworthiness of Type Design (EASA)
- Electrical Wiring Interconnection Systems (EWIS) – Design Issues (EASA)
- Flight Control Functions for Unmanned Aerial Vehicles (DGLR)

One additional important field of training, in terms of project management, is an agile approach. Since technological development happens at great speed, an agile approach (e. g. SAFE, SCRUM) to the daily way of working is crucial.

4. Certifications

Cyber security certifications are important for several reasons. To begin with, they demonstrate to potential employers that an individual possesses a certain level of knowledge and expertise in cyber security.

In addition, cyber security certifications can help individuals develop their skills and knowledge in the field. Studying for a certification can involve a significant amount of learning and research, which can help individuals stay up-to-date with the latest developments and best practices in cyber security. This can not only benefit the individual but can also positively impact their organisation by improving the overall level of cyber security awareness and expertise.

Moreover, cyber security certifications can assist individuals in advancing their careers in the field. Many organisations require their employees to hold specific certifications to be considered for certain roles or to advance within the organisation. Holding a certification can also demonstrate a commitment to professional development and a willingness to go above and beyond what is required.

Lastly, cyber security certifications can help improve the overall level of cyber security in organisations and across industries. By setting a baseline of knowledge and expertise, certifications can help to ensure that cyber security professionals have the skills and knowledge necessary to protect against threats and vulnerabilities.

This is a list of the most relevant cyber security certifications:

- CC – Certified in Cybersecurity (ISC2): CC is an entry-level certification offered by ISC2. It provides a great start in the field of cyber security and builds a strong foundation for it.
- SSCP – Systems Security Certified Practitioner (ISC2): SSCP is a certification offered by ISC2 that is tailored towards helping security administrators with their day-to-day life in that role.
- CCSP – Certified Cloud Security Professional (ISC2): CCSP is another certification offered by ISC2 that is specially designed for cloud security architects. Its modules prepare you for tackling security-related topics in cloud architectures.
- Security System Management: CISM – Certified Information Security Manager (ISACA)
- CISSP – Certified Information Systems Security Professional (ISC2): CISSP is perhaps the most well-known certification from ISC2. Its modules are designed to prepare you for the leadership and operations roles in the field of cyber security.
- Advanced Certification: ISSAP – Information Systems Security Architecture Professional (ISC2): ISSAP is one of the most advanced certifications to be had from ISC2. Prerequisites include having cleared the CISSP certification and, after that, a minimum of two years of relevant work experience leading cyber security projects. This certification is a testament to your ability as a leader in cyber security.
- CompTIA: Advanced Security Practitioner (CASP)

5. Education and Experience Matrix

The education and experience matrix allows a number of careers to be compared in terms of the specific training required to match the profile of a cyber security professional in the aerospace industry.

Subject	▪ Electrical Engineering and Information Technology ▪ IT administrators	▪ Computer Science ▪ Aerospace Technology ▪ Electrical Engineering and Information Technology	▪ Computer Science ▪ Aerospace Technolo-gy ▪ Electrical Engineering and Information Technology	▪ Computer Science with a focus on Cyber Security	▪ Aerospace ▪ Electrical Engineering and Information Technology
Training	▪ Fundamentals of Aerospace Technol-ogy ▪ IT-Security basics	▪ Fundamentals of Aerospace Technolo-gy ▪ IT-Security basics	▪ SANS Training ▪ EASA / EUROCAE	▪ SANS Training ▪ EASA / EUROCAE ▪ In-depth	▪ SANS Training ▪ EASA / EUROCAE ▪ In-depth
Certifications	▪ Certification according to ISO/IEC-27000-series	▪ Certification according to ISO/IEC-27000-series	▪ CC ▪ CISM ▪ CISSP ▪ CASP ▪ CISSP-ISSAP	▪ CISM ▪ CISSP ▪ CASP ▪ CISSP-ISSAP	▪ CC ▪ CISM ▪ CISSP ▪ CASP ▪ CISSP-ISSAP

6. Conferences

6.1 Aeronautical conferences

- The Digital Avionics Systems Conference (DASC), the preeminent R&D conference in the field of digital avionics, is organised by two distinguished professional societies, the American Institute of Aeronautics and Astronautics (AIAA) and the Institute of Electrical and Electronics Engineers (IEEE).
  https://2023.dasconline.org
- The Aerospace Village is a diverse community of hackers, engineers, pilots, policy leaders and more from across both the public and private sectors
  https://www.aerospacevillage.org
- High-Level Conference on Aviation Security, AvSec – ICAO.
- Other bodies that organise regular industry gatherings are EUROCAE, EASA and ICAO. They organise several workshops and conferences throughout the year, but there are no fixed dates.

6.2 Space conferences

- CYSAT: CYSAT aims to bring together the space and IT security communities to build a European ecosystem capable of responding to current and future challenges faced by the European space industry.
- Hosted in downtown Paris, it is positioned to attract both space and cyber security players from the industry, academia, and national and European agencies.
- 3S: Security in Space Systems is being hosted by ESA for the first time in 2024 and is tailored towards securing various space system domains. It aims to bring together academia and industry to present their advancements and research on security topics for space. The topics of interest range from applied crypto for space, ground-segment security, jamming/anti-jamming, new space and mega-constellation security, optical space communications, security policies, etc.
- Munich New Space Summit: Participants at the Munich New Space Summit 2023 can expect a varied mixture of current topics and developments within the sector. Global opportunities and challenges will be addressed during interesting lectures, exciting round-table discussions and inspiring exchange sessions between scientific representatives, VIPs, SMEs and start-ups.
- In addition to the conference with high-ranking officials, decision-makers and international best practices, an exhibition area and the first Munich New Space Night will provide opportunities for exchange and networking. The summit takes place at the Ludwig Bölkow Campus in Taufkirchen, close to Munich, Germany.

- European Space Forum: Focussing on the key pillars of security and defence, sustainability, competition, innovation and connectivity, the event will provide the opportunity to come together and discuss key challenges and opportunities as Europe looks to deliver on its space ambitions and secure its position as a strong and resilient leader in the global space market.
- ESA Commercial Space Days: Commercial Space Days is a two-day conference organised in Lucerne by the Centre for Aviation and Space Competence at the University of St Gallen and the Swiss Aerospace Cluster in cooperation with ECSECO and the Swiss Space Office.
- Space Tech Expo: As the sister event to Space Tech Expo USA, the Europe edition has quickly established itself as the prominent supply-chain meeting place for the space industry and will welcome more exhibiting companies than any other space event globally in 2023. As the sector continues to grow at a fantastic pace, join us in the industry hub of Bremen in November 2023 for our largest-ever event to connect with technical and executive representatives of the European (and wider) space community.

Experience the latest technological innovations at the leading showcase for space manufacturing and testing services, components and systems engineering for spacecraft, launcher, and satellite programs at **Space Tech Expo Europe 2023**.

Space Operations Summit: This takes place every year, looking into the space operations domain and presenting the latest issues and research.

7. Conclusion

New ways of recruiting: In order to stand out and find the best profiles for the company requirements, some new innovative ideas for recruiting are:

- Social media campaigns: Leverage the power of social media platforms to promote the company's brand and job opportunities.
- Hackathons and innovation challenges: Organise hackathons or innovation challenges where candidates can showcase their skills and problem-solving abilities. This approach allows you to identify talented individuals while promoting your organisation as an innovative and dynamic workplace.
- Online talent communities: Create online communities or forums where candidates can connect with current employees, learn more about your organisation, and engage in discussions. These foster a sense of belonging and help build relationships with potential candidates.
- Podcasts or webinars: Host podcasts or webinars on topics related to your industry, featuring your organisation's thought leaders. This content can attract candidates who are interested in learning and provide insights into your company's culture and expertise.
- University collaborations: Establish partnerships with universities or educational institutions to offer specialised courses, workshops, or mentoring programs. These enable your organisation to engage with students and identify promising talent early on.

Relevant profiles to recruit include:

- Former military/air force employees
- Former pilots/employees in the aerospace industry
- Graduates with a mixed technical focus interested in the aerospace industry
- Hobby pilots with IT skills
- Security professionals from different industries, e. g. automotive

BDLI German Aerospace Industries Association

www.bdli.de