



SECURITY INFORMATION AND EVENT MANAGEMENT FOR
AIRBUS DEFENCE AND SPACE

**recognize security
incidents and take
countermeasures**

ConSecur

[security and consulting]

Project outline

Airbus Defence and Space has been contracted by the European Space Agency to implement a Security Information Event Management System (SIEM) for the operation of the international Space Station. The aim is to monitor the IT infrastructure of the Columbus module of the International Space Station. The aim is to monitor the IT infrastructure of the Columbus module of the International Space Station (ISS) and the associated ground segment, which is accessed by various national space agencies, user operational support centres and European partners throughout Europe.

The responsible programme of Airbus Defence and Space has entrusted Confiseur GmbH with the conceptual design and implementation of such a SIEM system for the ISS programme.

„A major strength of ConSecur is the set-up and operation of SIEM systems.“

**MARKUS BRACHMANN,
AIRBUS DEFENCE AND SPACE**

„For this project, we were looking for a partner who aligns its project management with our structure within the European Space Agency.“

Initial situation

Airbus Defence and Space operates the IT infrastructure of the Columbus module on the International Space Station (ISS) as well as parts of the ground segment for the European Space Agency (ESA) together with the German Aerospace Center (DLR) and other European partners. The project partners want to bring the communication of this IT infrastructure, which consists of an onboard and a flight segment, to new level of security. The planned active security monitoring will be an interplay of machine and human security: security incidents in the IT infrastructure will be identified as such by the SIEM and the countermeasures will initiated by the analyst team.

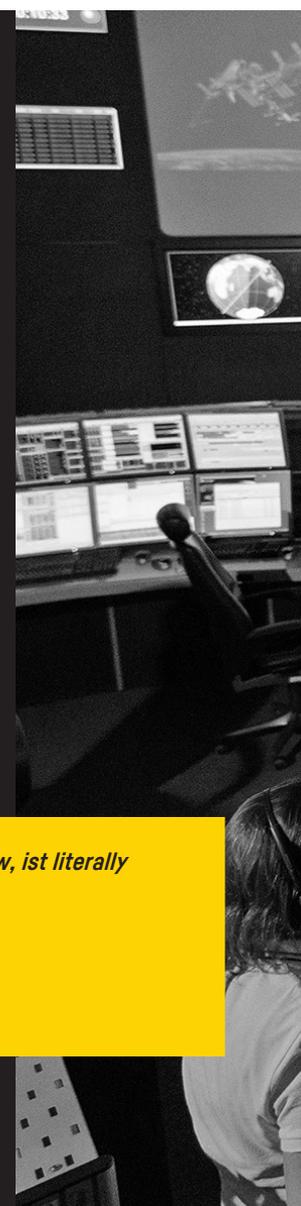
Airbus Defence and Space decided for ConSecur as an external partner for setting up and operating the planned SIEM, which is based on IBM QRadar, after a selection process based on conviction.

"For this project we were looking for a partner who understands our requirements and who aligns its project management with our structure within the European Space Agency," according to Markus Brachmann. Beyond the conceptual and technical challenges, Markus Brachmann considers the permanent dialogue with all European partners involved in project processing as well as short communication channels in project implementation to be a critical core task.

Markus Brachmann wanted this flexibility for this project.

"What we don't want for this project is a solution that, in our view, is literally dumped over the fence after the contract has been completed."

**Markus Brachmann,
AIRBUS DEFENCE AND SPACE**



Project implementation

In the initiating kick-off workshop at the airbus site in Bremen, ConSecur and Airbus Defence and Space visualised the project sequence and defined specific time periods for all actions.

At the official start of the project, Airbus Defence and Space and ConSecur invited all European partners to Oberpfaffenhofen in order to present the project objective and process at a table in order to create a common knowledge base and to solicit the support of the internal national administrators.

„For us it has been clear that we will only be successful if we resolve possible uncertainties in this sensitive security area in advance and consistently respect national interests and harmonise them for the success of the project,“ Markus Brachmann said looking back.

**CHRISTOPH KRONABEL,
CONSECUR PROJECT MANAGER**



Distinguish authorised access from anomalies

The planned SIEM should be able to automatically distinguish from anomalies automatically. This automation is based on a set of rules in which all legitimate accesses are defined from the various log sources of the European partners are stored and at the same time predefined patterns for anomalies.

Markus Brachmann describes the connection of these log sources as a "high coordination task" and the first milestone on the way to efficient security monitoring."

Together with Markus Brachmann, the ConSecur

project manager Christoph Kronabel has defined rules for anomalies that can hide unauthorised access or attacks on the IT infrastructure.

These patterns include, for example, out-of-office hours or access from countries with which individual European partners do not maintain relations. Events such as these will automatically trigger a chain of alarm reactions in the operational SIEM, alerting security analysts, who will initiate appropriate countermeasures to prevent the tried system access.



Conclusion

During the implementation, it has been possible to successfully integrate all external partners into the regulations. ESA allows various European universities secure access to the network of the international space station for teaching and research purposes.

After successful project implementation, Airbus Defence and Space and ConSecur are working on the next expansion stage. The aim is to transfer the implemented SIEM into operational use, which analysts from the ConSecur Cyber Defense Center in Meppen and Bochum will ensure.



Columbus Modul

The European Space Agency (ESA) is involved in the International Space Station (ISS) with the Columbus module. The Columbus Module is a laboratory-module for scientific and medical experiments to investigate various questions such as the behavior of biological reactions or the organism during prolonged weightlessness. How does the organism behave during prolonged weightlessness?

Airbus Defence and Space / ESA

Airbus Defence and Space is part of the Airbus Group and Europe's leading defence and space company. Together with the DLR, Airbus Defence and Space operates parts of the IT infrastructure of the Columbus module on the International Space Station (ISS) for the European Space Agency (ESA). The IT infrastructure consists of a ground segment and a flight segment.

Internet connection to the International Space Station (ISS)

Airbus Space and Defence is part of the Airbus Group and Europe's leading defence and space company. Together with DLR, Airbus Defence and Space operates parts of the IT infrastructure of the Columbus module on the International Space Station (ISS) for the European Space Agency (ESA). The IT infrastructure consists of a ground segment and a flight segment.

IBM QRadar

IBM® QRadar® Security Information and Event Management (SIEM) helps security teams accurately detect and prioritise security threats. The solution provides intelligent insights enabling teams to respond quickly to reduce the impact of security incidents. QRadar consolidates log events and network flow data from thousands of devices, endpoints and applications across the network, correlates all of this associated data and aggregates events into single alerts to accelerate security incident analysis and remediation.

ConSecur

ConSecur GmbH develops custom-fit IT security concepts and solutions for the detection, defence and analysis of cyberattacks. Buzzwords such as artificial intelligence, Industry 4.0 and the Internet of Things (IoT) become added value for our customers. We combine the personal proximity of a medium-sized company with the range of services of a corporate group. The core competence of the ConSecur GmbH is Information Security Event Management (ISMS) and Security Information Event Management (SIEM). In the ConSecur Cyber Defense Centers (CDC) in Meppen and Bochum, our security knowledge is available to our customers. We support our customers in setting up a Cyber Defense Center (CDC) on site or provide our qualified IT security analysts.

ConSecur

[security and consulting]

ConSecur GmbH
Nödiker Straße 118
49716 Meppen

TEL.: +49 5931 9224-0
info@ConSecur.de

www.ConSecur.de