Paper ID: 79410
student

56th IAA SYMPOSIUM ON SAFETY, QUALITY AND KNOWLEDGE MANAGEMENT IN SPACE ACTIVITIES (D5)
Cybersecurity in space systems, risks and countermeasures (4)

Author: Mr. Uzeyir Alirzayev
Azerbaijan State Oil and Industry University (ASOIU), Azerbaijan

Mr. Ali Rustamov
Azerbaijan State Oil and Industry University (ASOIU), Azerbaijan
Mr. Feqan Mirzeyev
Azerbaijan

SPACE-SPECIFIC SIEM SYSTEMS FOR CYBERSECURITY IN SPACE STATIONS

Abstract

Cyber threats have increased in tandem with society's growing reliance on technology and the internet. It is impossible to overstate how crucial cybersecurity is for space stations, as a successful attack could have disastrous effects on astronauts and equipment. It is crucial to create cybersecurity platforms that are tailored for space environments as a result. A Security Information and Event Management (SIEM) system is one such platform.

SIEM systems are made to quickly identify and address security threats. When a potential threat is found, they gather data from various sources, analyze it, and notify security personnel. However, creating a SIEM system for space environments has its own special difficulties. For instance, the extreme temperatures, radiation, and electromagnetic interference present in space environments can obstruct the proper operation of electronic devices.

A space-specific SIEM system must be created to address these issues. The system would collect and analyze information from various sources within the space station environment, such as network, system and security logs. Statistical, machine learning and artificial intelligence techniques what specialized against cyber threads would be used to analyze this data in order to spot potential security incidents.

The SIEM system would also be built to identify zero-day attacks, which are attacks that take advantage of flaws in software or systems that were not previously known to exist. These flaws also was knowns as backdoors or bugs. This is particularly crucial in environments like space.

The SIEM system would produce an alert to let security personnel know when a potential security incident was found. The alert will contain information about the incident, such as the type of threat, the location of affected files or software, and the danger level of the incident. The threat would then be contained and its effects would be reduced through the use of an incident response procedure. This would cause working in tandem with other security programs, such as firewalls and intrusion detection systems, to take steps to lessen the threat. Also AI will learn methods against these attacks time by time.

In conclusion, a SIEM system designed specifically for the difficulties of space environments might give space station operators a strong tool for spotting and responding to security threats. The significance of cybersecurity in space stations cannot be overstated as space exploration grows, and the creation of specialized SIEM systems is crucial to ensuring the security and success of space missions.