PROBLEM TITLE
Sensor Ingest and Analytics Platform

CHALLENGE
Cyber defense operators need a way to verify the cause of a malfunction in real time in order to save time and Cyber Watch Operations Center resources.

BACKGROUND
The Cyber Watch Operations Center (CWOC) and Network Operations Center (NOC) are tasked with protecting North American Aerospace Defense Command (NORAD) and U.S. Northern Command's (USNORTHCOM) internal and secure sensor data from unwanted infiltration or external attacks. If a malicious actor gets past the perimeter lines of defense the intruder could cause an anomaly, malfunction, or crash affecting North American defense operations.

When a system malfunctions, cyber defense operators troubleshoot to determine if the malfunction is benign or malignant. In order to verify the cause of the malfunction, the operators assess system operations prior to the disruption, as well as the time the system was compromised. This includes an assessment of data confidentiality, integrity and accessibility. Troubleshooting is a resource-intensive process, where multiple cyber analysts must spend hours looking through NORAD's and USNORTHCOM's entire networks attempting to identify any possible anomalies.

OPERATIONAL CONSTRAINTS
- Preference given to a cloud-based solution that can improve trust-based relationships and support micro-segmentations of applications, sensors, services and data.
- Preference given to a cloud-based solution that can enable relatively quick, reliable and secure expansion of sensor inputs using industry-standard, open source data interfaces.

Do not exceed one page