# MACHINE LEARNING METHODS FOR OPERATIONAL MONITORING OF SECURITY EVENTS

## PECS Activity Overview

AO/1-10907/21/NL/SC

25/06/2021

New, Associate and Cooperating States (CIP-IP),

Industrial Policy and SME Division

ESA UNCLASSIFIED – For ESA Official Use Only

# DISCLAIMER

- This presentation material does not contain sufficient information to be used officially ,in any way, in the context of the expected ITT (Invitation-to-Tender ESA AO/1-10907/21/NL/SC).

- This presentation is just to help understand, in a simplified manner, some of the information associated with upcoming ESA procurements. See ESA-STAR for more details.

- Please ensure that any proposal submitted to ESA is compliant with the requirements contained in the official ITT documentation specific to the tender.

**Registration in esa-star is an essential pre-requisite to bid!**

To register in esa-star:

https://esastar-emr.sso.esa.int/

# Introduction

The **Government of the Slovak Republic** adopted on **7th October 2020** the **resolution approving** the **intention of Slovakia to continue in cooperation with ESA** after **end of PECS extension period** with focus **to become** an **Associate Member** and approved financial contribution to ESA of 4,5 million € per year during new Slovak budget period.

→ PECS

The **ESA Council** approved an 18 month extension of the current PECS agreement on the **16th of December 2020** to enable further strengthening of the Slovak Space Industry and the opportunity for advancement of products and services to higher Technical Readiness Levels (TRLs). **This is expected to offer excellent development opportunities for Slovak Space in 2021/2022**.

This top down statement of work is intended to provide Slovak entities with an opportunity to acquire practical and relevant space software development experience. The programme of work will offer Slovak entities: the opportunity to familiarize with the unique environments seen in ESA programmes, interface with ESA experts that work on these issues, and potentially help to prepare the selected Slovak company to participate in future studies or product development opportunities that may arise. Finally, the activity will offer greater familiarity with the working practices of the Agency and the use of applicable space standards (ECSS).

# MACHINE LEARNING METHODS FOR OPERATIONAL MONITORING OF SECURITY EVENTS: Objectives & Work Overview

Machine learning has rapidly emerged as a preferred technology for commercial Security Information & Event Management (SIEM) and Security Orchestration, Automation & Response (SOAR) providers in the monitoring of security events, but the algorithms involved usually require a significant amount of manual customization in order to avoid false positives or false negatives. The unique environments created by ESA programmes and missions remain largely unexplored and under analyzed. Thus, this work aims to study the optimal types and set of algorithms that could be:

- automatically trained (unsupervised);
- manually trained (supervised); or
- trained through a combination of unsupervised and supervised learning; and
- rapidly deployed and used in the most complex space infrastructure environments

# MACHINE LEARNING METHODS FOR OPERATIONAL MONITORING OF SECURITY EVENTS: Objectives & Work Overview

This activity will:

1. Study and understand the amount and types of events generated in a complex space infrastructure environment;
2. Identify and characterize a baseline set of machine learning algorithms that would address the amount and types of events identified in task 1;
3. Propose a dataset representing the theoretical magnitude and nature of the events produced by a large-scale, complex ESA programme environment;
4. Develop a real-time customizable generator capable of providing the proposed dataset;
5. Tailor and evaluate the machine learning algorithms based on the generated dataset.

- **Suggested budget ceiling / duration for all work: €170K / ~12 months**
- **Expected publication date on ESA STAR: 2 July 2021**
- **Expected deadline for proposals: 20 August 2021 @ 13:00 (CEST – Amsterdam)**
- **Start of work expected: 4Q2021**

ESA UNCLASSIFIED – For ESA Official Use Only

# MACHINE LEARNING METHODS FOR OPERATIONAL MONITORING OF SECURITY EVENTS: Work Overview & Practical Information

- **Preliminary review of requirements culminating in a Familiarisation Workshop (FW)**
  - Task 1 = Definition of the Representative Space System
- **Requirements Consolidation culminating in the Requirements Review (RR)**
  - Task 2 = Definition of the Dataset Generator
- **Design culminating in the Critical Design Review (CDR)**
  - Task 3A = Design of the Dataset Generator
  - Task 3B = Trade-offs, Definition & Justification of the ML Strategy (algorithms, methodology, tools, etc.)
  - Task 3C = Training Set(s) Identification, Analysis, and Consolidation
- **Implementation & Validation culminating in the Qualification Review (QR)**
  - Task 4A = Implementation and Validation of the Dataset Generator
  - Task 4B = Algorithms Configuration, Training & Validation
- **Demonstration & Acceptance culminating in the Final Review (FR)**
  - Task 5 = Demonstration, Acceptance & Final Reporting

# General Information

## Hints and tips: Standards

It is highly recommended to examine ECSS documentation that is available for free download from www.ECSS.nl. Registration on the website is free. Documents recommended for reading pleasure include:

- **ECSS-M-ST-10C Project Planning and Implementation**
- **ECSS-E-HB-11A, Space Engineering, Technology readiness level (TRL) guidelines**

Additional relevant references include:


1. Style Guide for Python Code, Guido van Rossum and Barry Warsaw, http://www.python.org/peps/pep-0008.html
2. Docstring Conventions, David Goodger and Guido van Rossum, http://www.python.org/peps/pep-0257.html
3. Docstring Processing System Framework, David Goodger, http://www.python.org/peps/pep-0256.html
4. Python Library Reference. https://docs.python.org/3.9/
5. International Standard ISO/IEC: Programming languages — C
6. Pinjia He, Jieming Zhu, Zibin Zheng, and Michael R Lyu. Drain: An online log parsing approach with fixed depth tree. In 2017 IEEE International Conference on Web Services (ICWS), pages 33–40. IEEE, 2017.
7. Lilian Weng. From Autoencoder to Beta-VAE. https://www.statista.com/statistics/471264/iot- number-of-connected-devices-worldwide/ , 2018.
8. Wei Xu, Ling Huang, Armando Fox, David Patterson, and Michael I Jordan. Detecting large-scale system problems by mining console logs. In Proceedings ACM SIGOPS 22nd symposium on Operating systems principles, p.117–132, 2009.

# → PECS

**Registration in esa-star is an essential pre-requisite to bid!**

To register in esa-star:

Go to https://esastar-emr.sso.esa.int/

Support information in esa-star Registration User Manual:
https://esastar-emr.sso.esa.int/Account/DownloadFile

**See also: the presentation "BRIEFING HANDBOOK BASIC OF ESA PROCUREMENT" for more support information**

ITT Expected Opening: **2 July 2021**
Expected Submission Deadline : **20 August 2021 @ 13:00 CEST**
Negotiation / contract expected: **4Q2021**