Cybersecurity projects 2025-2026

Project selection and submission instructions

Project selection

By October 31, you must indicate your preferences for three projects in order of interest and list the members of your group (max. 4 people) on the form.
The project is assigned to the group that selects it first, so First Come First Served.

N.B. Even those who have already submitted their project and indicated the group by email must fill out the form.

Project submission

For those taking the exam in **December**, the project must be submitted at least **48 hours before the exam date**. For example, if you have the exam on 16 December, you must turn it in by 23:59 on 13 December.
For **other exam date**s, the project must be submitted at least **one week before**.

The submission must be made using the dedicated form, and it should include:

- Code (it must be well documented with a README)
- Report
- Presentation

1. An Adaptive IDS Based on CIL for Continuously Evolving Threats

isabella.marasco4@unibo.it

Artificial Intelligence-based Intrusion Detection Systems (IDS) represent the state-of-the-art for identifying cyber threats. However, their real-world efficacy is limited by an inherently static operational paradigm: models are trained offline on a dataset that captures the threat landscape at a specific moment in time and are then deployed into production.
This approach fails in a real-world context, which is by nature dynamic. The threat landscape is subject to constant evolution (concept drift) and, most importantly, the continuous emergence of new attack types (0-day threats). A static model cannot recognize these new threats and quickly becomes obsolete, requiring costly and time-consuming complete retraining cycles.
The objective of this project is to overcome the limitations of static IDS by designing and implementing an adaptive Intrusion Detection System based on Class-Incremental Learning (CIL). CIL, a scenario of Continual Learning (CL), allows a model to be sequentially updated from new data streams and, crucially, to increase the number of classes (attack types) it can identify over time. A central challenge in this scenario is

catastrophic forgetting, the tendency of the model to drastically degrade performance on previously learned classes after being trained on new ones.

Goals:

- Realize an IDS CIL scenario based using PyTorch.
- Integrate these three strategies for mitigating catastrophic forgetting: iCarl, Dark Experience, and ER.
- Evaluate how the size of the incremental task (i.e., the number of new attack classes introduced in each phase) affects performance. Different scenarios will be compared (e.g., 10 total attacks introduced as 1+1+1... vs. 5+5 vs. 2+3+5) to understand the system's sensitivity to the frequency and size of updates, the benign traffic is always present.
- Few-Shot Scenario Evaluation (Optional): extend the analysis to investigate how the system performs when new attack classes are introduced with a very limited number of samples (few-shot learning), a realistic scenario for emerging threats.

Evaluation Metrics:

- Accuracy and average accuracy
- Forgetting**:** measures the average performance degradation on classes learned in previous tasks after training on new tasks

Datasets:

- CICIDS-2017
- UNSW-NB15

Other references:

- A Comprehensive Survey of Continual Learning: Theory, Method and Application
- Class-Incremental Learning: A Survey