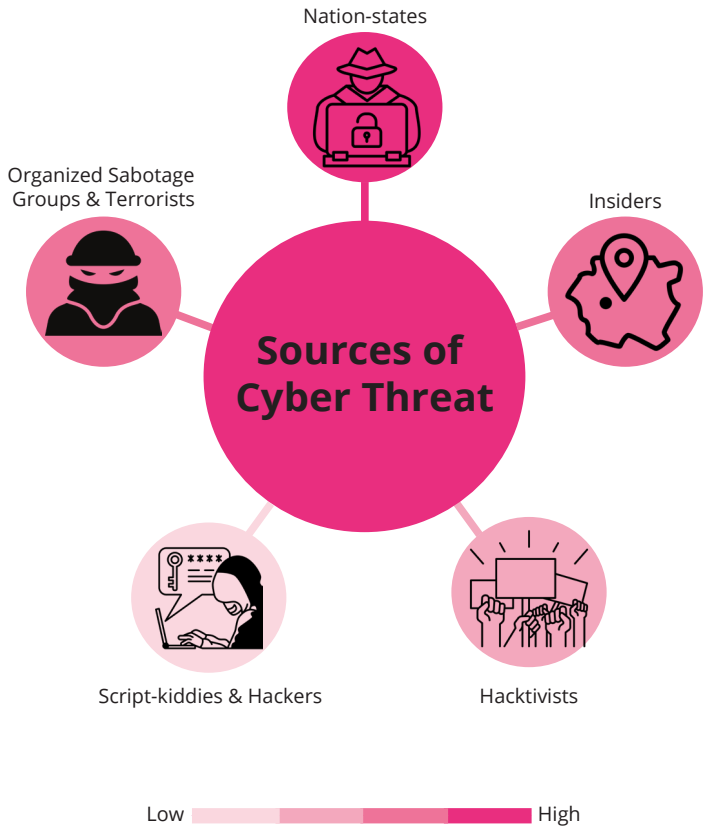
Machine Learning-based Intrusion Detection Systems

Deployment Guidelines for Industry

Industrial Control Systems (ICS) are increasingly becoming the subject of high profile cyber attacks. The motivations for these attacks can range from financial, socio-political, military advantage, and corporate advantage, amongst others.



Categories of cyber threat sources based on level of sophistication

In the coming decade, due to increasing sophistication of attackers and their attack methods, it is critical that security measures also advance. Machine Learning is one such promising technology.

This guideline is intended for:

- Operators and managers of ICS
- Those making decisions related to designing, installing, purchasing, or maintaining the performance of Intrusion Detection Systems (IDS)
- ICS suppliers, component designers, etc. during the design/architecture definition processes
- Decision-makers at the boardroom level when taking high level decisions about the preparedness of their ICS facilities

This guideline provides guidance on:

- The types of Maching Learning-based anomaly detection tools available
- Aspects to consider while selecting one/discussing one
- How to define well-rounded performance
- Options for deploying and maintaining them when they are in use
- Limitations

Machine Learning-based Intrusion Detection Systems

Deployment Guidelines for Industry

Key Recommendations

Dataset:

To maximise protection, identify the critical assets and processes with regard to safety and security to allow data capture at suitable points around the system. Anomaly detectors with a wide enough focus will also be able to capture this context-based anomaly.

Model Selection:

Semi-supervised and unsupervised detectors should be your first choice due to their ability to detect zero-day attacks. If hand-labelling is feasible to some extent, semi-supervised learning would be the best option. However, in a novelty detection form, this approach would first require an anomaly-free dataset for the model to learn normal behaviour.

Interpretability/Usability:

A cyber defence system is inherently socio technical. Thus, use performance metrics that account for anomaly detection false positive rates to minimize unnecessary operator distractions, and interpretability augmentation methods such as data visualisation and independent explainability tools to provide the operator insights regarding "where", "when" and "why" some data was classified as anomalous. These would increase tool trustworthiness and allow the operators to make better decisions regarding corrective actions/ countermeasures.

Maintenance:

Post-deployment, to keep up with process changes and to ensure that the system remains performant, it is essential that you perform periodic and rigorous re-assessment with baselines, and model updating (with documentation). If feasible, collect fresh data from the field to perform online training with the goal of making the system robust to operational drift.

Full report: petras-iot.org/update/guideline-for-industry-machine-learning-based-intrusion-detection-systems

Information on the ELLIOTT research project: petras-iot.org/project/early-anomaly-detection-for-securing-iot-in-industrial-automation-elliott/