How to improve resilience to cyberattacks of future hyper connected systems: feedback

Technical steering: **Nada Essaouini**, Research Engineer - cyber security analyst, IRT SystemX

Thanks to the START@SystemX Cybersecurity initiative, the startup craft ai, winner of Season 1, has been able to experience the performance of its artificial intelligence solution in the context of intrusion detection by a behavioral analysis approach. The evaluation of the predictive models generated by craft ai was based on a methodology for evaluating and comparing intrusion detection systems (IDSs) developed within the EIC project (Environment for interoperability and integration in cybersecurity). It was carried out in collaboration with Airbus CyberSecurity and Thales Services.

In the evaluation activities or comparative analysis activities of IDSs, three axes are explored: methods of generating test data, metrics and measurement methodologies. A measurement methodology is therefore to specify the properties of the IDS and to determine the test data and the metrics used to evaluate these properties.

In our experience, two properties were more particularly analysed: the precision of the attack detection and the actionability. The accuracy of attack detection is to jointly evaluate the rate of false positives (adverse event/behaviour wrongly evaluated) and the rate of true positives (adverse event/behaviour rightly evaluated). Actionability measures the relevance of reported information in IDSs alerts and their impacts on mitigation strategies to be adopted. In particular, the evaluation of the actionability presents a great challenge for the IDSs based on automatic learning unlike the IDSs with signature. Indeed, an alert issued by a signature-based IDS contains a signature ID that triggered it. Thus, evaluating the actionability of a signature-based IDS is tantamount to whether the signature that triggers the alert returns relevant information about the attack played in the test data. The more accurate the information, the more clear and effective the mitigation strategy becomes. The difficulty of evaluating IDSs is that their results are often presented in the form of scores describing the degrees of anomalies and not in the form of clear information about the nature of the attack.

In our project, the evaluation of the actionability is based on correlation mechanisms and test data describing a complete attack scenario. If the correlation, fed by the outputs of the AI, finds the attack scenario of the test, then the IDS is considered completely operable.

For experimentation, we used test data provided by Airbus CyberSecurity. This data presents a complete scenario of attacks spread over time and close to real attack techniques. An individual performs screening and targeting with the help of social networks and then usurps the identity of a referent individual. He then sends several employees an e-mail with a malicious attachment (first incongruent). The latter is activated by a careless employee. It then performs a scan of ports (second incongruent) to network devices (recognition of the target system). One of them presents a vulnerability that can then be exploited (third incongruent) by the attacker in order to compromise and/or steal sensitive information from the company present on his information system.

With respect to the correlation mechanism, Airbus CyberSecurity provided an innovative correlation process which, fed by the AI outputs, produced graphs whose relevance was quantified.

Finally, to conduct this comparative analysis, an evaluation module implemented using the predictive models of craft ai has been compared with an industrial IDS based on automatic learning. By applying the correlation tool on the outputs of the industrial IDS, the attack scenario was completely

reconstructed, the three incongruities having been clearly identified. However, no conclusive results could be obtained by combining the craft ai evaluation module with the Airbus correlation module.

At the level of the precision in the attack detection, the measurement metric used is the detection capability. The detection capacity metric measures the amount of information shared between the input data of an IDS and its outputs (i.e., mutual information). The greater the mutual information between these data, the less uncertainty there is on the IDS input data by observing the generated alerts, and therefore the greater the detection accuracy of the IDS.

Compared to the industrial IDS, craft ai has shown a higher detection capability than that of the industrial IDS which leads us to the conclusion that craft ai is more accurate in attack detection. This result is due to the fact that the craft ai models emit far less false positives than the industrial IDS on this case.

This collaboration has been beneficial in validating our methodology and our industrial partners, in particular on aspects related to the sharing of data, technologies and business knowledge of the various participants.

Here are some testimonials:

“Our collaboration with Thalès and Airbus, as well as with the IRT SystemX researchers, has enabled us to demonstrate the value of craft ai technology on the subject of cybersecurity. Through the business expertise of our partners, we were able to determine the application challenges of craft ai for intrusion detection through behavioural analysis and to frame the next steps in this fruitful collaboration”. **Caroline Chopinaud**, Chief Business Development Officer at Craft AI.

“Airbus CyberSecurity welcomes the project START@SystemX Cybersecurity, based on a quadripartite collaboration with the IRT SystemX, craft ai and Thalès. The richness of the concepts implemented and the non-uniformity and diversity of approaches adopted by the different parties have been a real source of progress, both in terms of technological advances and on how to manage and guide them”. **Jean Philippe Farr**, technical architect and Solution in cyber-security, IA, Cloud, big-data at Airbus Defence and Space CyberSecurity.

"The balance sheet of Craft Ai's participation in the cybersecurity theme of START@SystemX is positive in many respects. The continued involvement and availability of the craft ai team have allowed an understanding of our mutual interests impossible otherwise. The startup craft ai has thus demonstrated its ability to grasp the stakes of cybersecurity and its many actors, in order to identify the pros and cons of their solution. The concrete results of this phase of experimentation have shown that the operational evaluation of this type of technology implies placing itself in specific application contexts, which has been made possible thanks to the collaboration of Airbus and Thalès. The analysis of these results by the IRT SystemX confirmed the need for these AI technologies to have a number of data, sufficiently representative of the reality of a recent information system, but also of a fine knowledge of the system in order to produce workable results”. **Olivier Bettan**, Head of Cybersecurity Lab at Thales Security & Services and **Jérôme Kodjabachian**, Expert Thales, technical manager at the ThereSIS Laboratory in Palaiseau.