xNIDS: Explaining Deep Learning-based Network Intrusion Detection Systems for Active Intrusion Responses

Feng Wei, *University at Buffalo;* Hongda Li, *Palo Alto Networks;*
Ziming Zhao and Hongxin Hu, *University at Buffalo*

https://www.usenix.org/conference/usenixsecurity23/presentation/wei-feng

This artifact appendix is included in the Artifact Appendices to the Proceedings of the 32nd USENIX Security Symposium and appends to the paper of the same name that appears in the Proceedings of the 32nd USENIX Security Symposium.

August 9–11, 2023 • Anaheim, CA, USA

978-1-939133-37-3

Open access to the Artifact Appendices to the Proceedings of the 32nd USENIX Security Symposium is sponsored by USENIX.

USENIX'23 Artifact Appendix
xNIDS: Explaining Deep Learning-based Network Intrusion Detection Systems for Active Intrusion Responses

Feng Wei
University at Buffalo

Hongda Li
Palo Alto Networks

Ziming Zhao
University at Buffalo

Hongxin Hu
University at Buffalo

A Artifact Appendix

A.1 Abstract

We present xNIDS, a novel framework that facilitates active intrusion responses by explaining DL-NIDS. Our artifact includes the proposed explanation method dedicated to explaining DL-NIDS.

A.2 Description & Requirements

A.2.1 Security, privacy, and ethical concerns

This artifact can be used by users anywhere, but it should be utilized strictly for research purposes and in adherence to good ethical practices.

A.2.2 How to access

This artifact is publicly available at https://github.com/CactiLab/code-xNIDS/releases/tag/v2023.1.0.

A.2.3 Hardware dependencies

The demo code is hardware-independent and can be optimized for execution on Google Colab.

A.2.4 Software dependencies

To run the code, the following software packages are required: Python, TensorFlow, Keras, NumPy, pandas, scikit-learn, Matplotlib, psutil, and asgl.

A.2.5 Benchmarks

The benchmark datasets utilized in this artifact are the NSL-KDD and Kitsune datasets.

A.3 Set-up

A.3.1 Installation

To access the code, kindly download it from the following link https://github.com/CactiLab/code-xNIDS/tree/main.

A.3.2 Basic Test

The demo code is written in Jupyter Notebook and can be executed on Google Colab.

A.4 Version

Based on the LaTeX template for Artifact Evaluation V20220926. Submission, reviewing and badging methodology followed for the evaluation of this artifact can be found at https://secartifacts.github.io/usenixsec2023/.