Understanding Adversary Behavior via XAI

Leveraging Sequence Clustering To Extract Threat Intelligence

Nadeem, A.

DOI
10.4233/uuid:4a1519ba-3542-4d8f-ab91-2342e8f5bb1a

Publication date
2024

Document Version
Final published version

Citation (APA)
Nadeem, A. (2024). *Understanding Adversary Behavior via XAI: Leveraging Sequence Clustering To Extract Threat Intelligence*. [Dissertation (TU Delft), Delft University of Technology]. https://doi.org/10.4233/uuid:4a1519ba-3542-4d8f-ab91-2342e8f5bb1a

Important note
To cite this publication, please use the final published version (if applicable).
Please check the document version above.

Propositions

accompanying the dissertation

UNDERSTANDING ADVERSARY BEHAVIOR VIA XAI
LEVERAGING SEQUENCE CLUSTERING TO EXTRACT THREAT INTELLIGENCE

by

Azqa NADEEM

1. Temporal features are better at modeling attacker behavior than statistical features. *(This proposition pertains to this dissertation).*
2. For sequential data, it is easier to understand cluster separation using a combination of example-based explanations and cluster distributions compared to using standard dimensionality reduction methods. *(This proposition pertains to this dissertation).*
3. Alert-driven attack graphs empower practitioners to go beyond alert management offered by commercial tools by comparing attacker strategies and capturing increasing attacker experience. *(This proposition pertains to this dissertation).*
4. Interpretable models are less risky in terms of confusing practitioners compared to post-hoc explanations of black-box models. *(This proposition pertains to this dissertation).*
5. Academic research that assumes a gradient-based attacker model is unrealistic for industry deployment.
6. Cybersecurity should be taught as a cross-cutting concept across computer science courses.
7. For a community that opposes "security by obscurity", it is ironic that acceptance-by-obscurity is a common strategy to publish papers.
8. Individual success in academia is *not* based on meritocracy.
9. Providing expectant parents with psychological training is crucial for developing a resilient workforce of the future.
10. A cat is a far superior furry friend to humans than a dog.

These propositions are regarded as opposable and defendable, and have been approved as such by the promotors Dr.ir. S.E. Verwer and Prof.dr.ir. R.L. Lagendijk.