UNSUPERVISED GRAPH-BASED ANOMALY DETECTION IN ENTERPRISE FIREWALL TRAFFIC

VYTAUTAS MAGNUS UNIVERSITY
Faculty of Informatics

AUTHORS:
Deividas Valiuška deividas.valiuska@vdu.lt
Nerijus Šakinis nerijus.sakinis@vdu.lt
Eimantas Zaranka eimantas.zaranka@vdu.lt
Justinas Juozas Dainauskas justinas.dainauskas@vdu.lt
Rimantė Povilavičienė rimante.povilaviciene@vdu.lt
Tomas Krilavičius tomas.krilavicius@vdu.lt

MOTIVATION & CONTEXT

Enterprise networks generate vast volumes of firewall traffic logs, allowing malicious or unusual behaviour to become invisible

→ Data annotation is impossible due to massive amount of data

→ Network anomalies detection is a critical task for network security, but supervised approaches are impractical due to an absence of labeled data

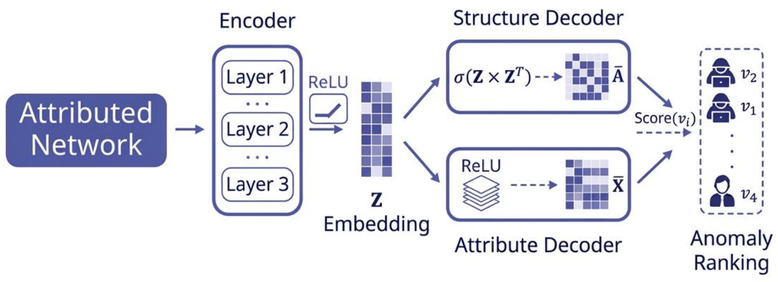
OBJECTIVES

1. Apply **unsupervised graph-based** anomaly detection methods to real enterprise firewall traffic logs
2. Apply **Log2Vec** method to real Sysmon user activity logs
3. Evaluate results within a given 2-week time window with a help of experts

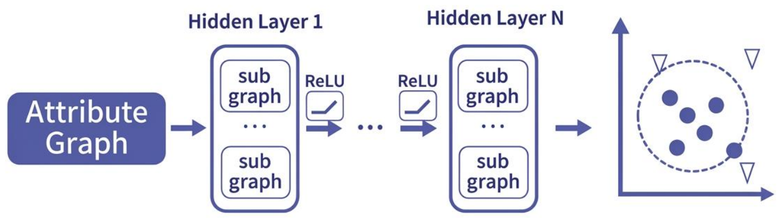
TO-DOs:

- [ ] Complete the expert evaluation for Anomal-E results.
- [ ] The firewall-based methods detected complementary parts of the known attack; we expect to develop an ensemble to give a more complete view of anomalous events.

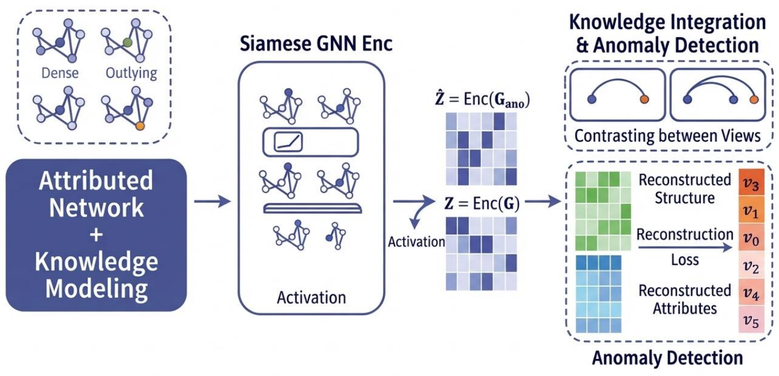
DOMINANT



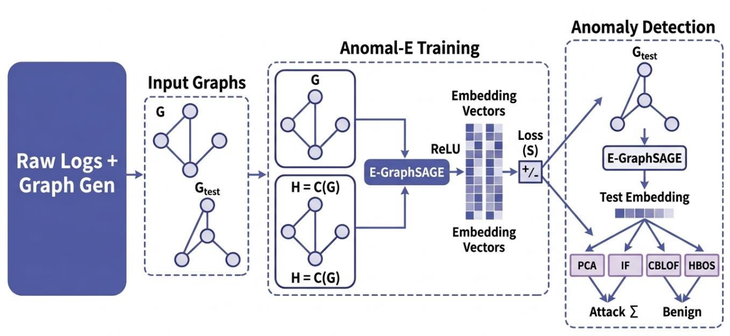
OCGNN



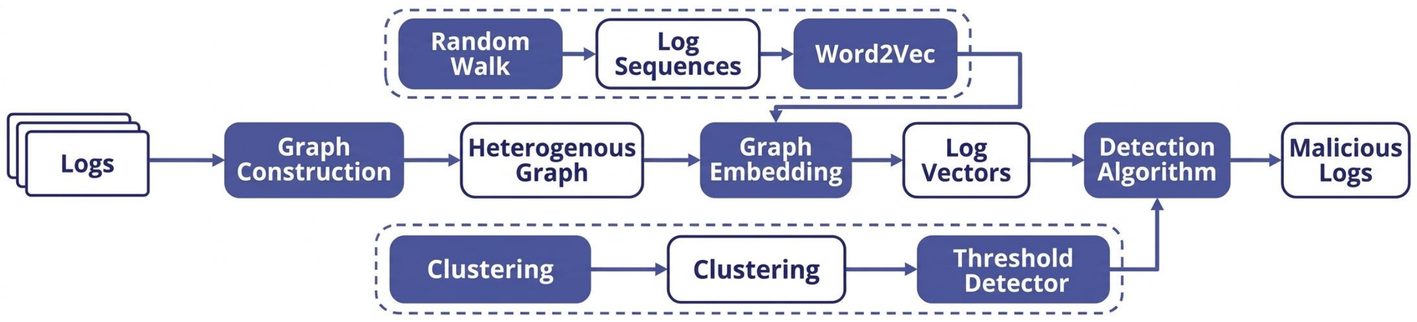
CONAD



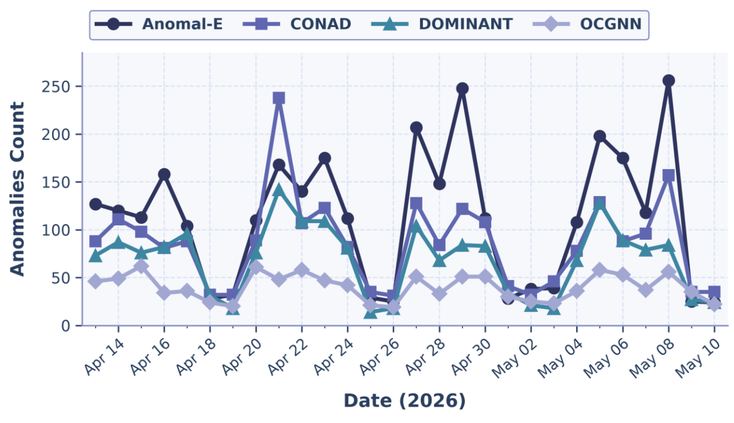
ANOMAL-E



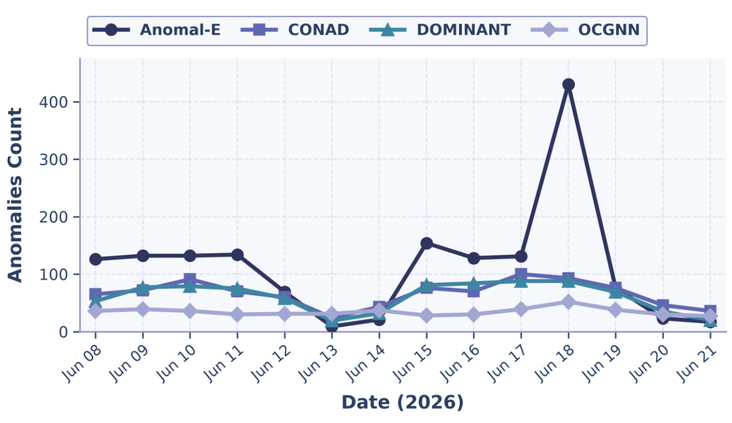
LOG2VEC



FIRST TEST PERIOD
April 13 – May 10, 2026



SECOND TEST PERIOD
June 8–21, 2026



Conclusion #1

Log2Vec revealed no real intrusions, although 3 hosts appeared anomalous and required deeper inspection.

Conclusion #2

Experts reviewed the 10 most anomalous hosts from Log2Vec and the 4 most anomalous hosts from each of DOMINANT, CONAD and OCGNN.

Conclusion #3

DOMINANT and CONAD flagged the internal attacker host of a previously known attack but missed the attacked host and additionally flagged one non-malicious host whose behaviour experts judged genuinely anomalous.

Conclusion #4

OCGNN flagged the attacked host but missed the attacker host.

CARD
CENTRE FOR APPLIED RESEARCH AND DEVELOPMENT