

### 1. Background

#### Alert Fatigue

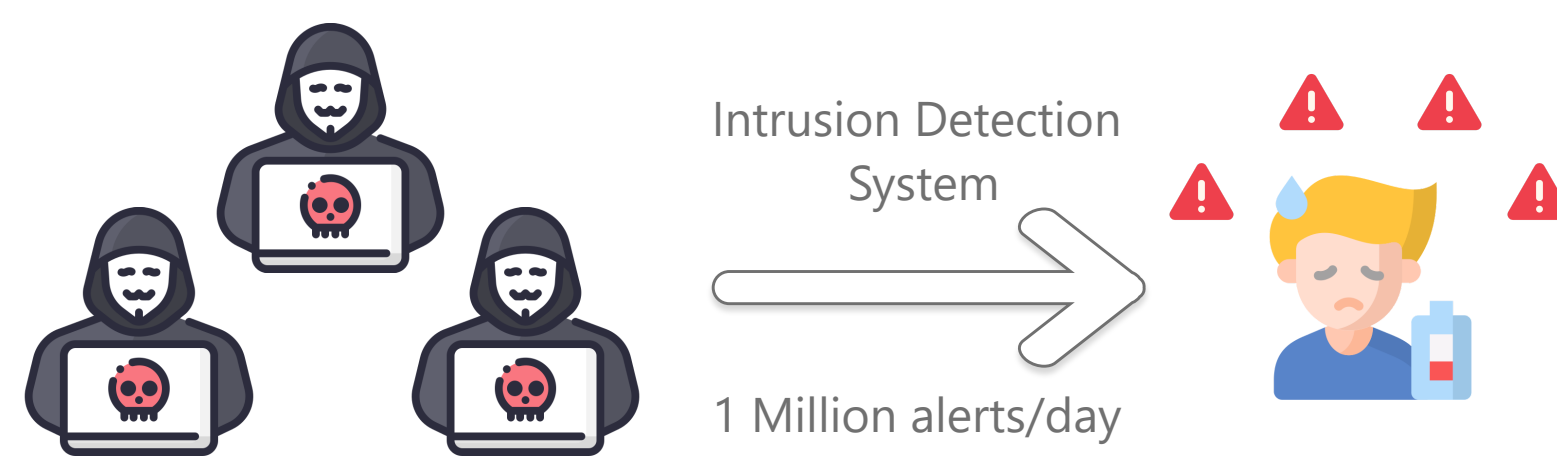


Figure 1: Intrusion alerts leading to alert fatigue.

#### SAGE Compresses alerts into attack graphs (AGs) [1]

Large quantity/size of AGs → need interactive dashboard [2]



Figure 2: From alerts to AG interactive exploration.

#### Prioritising Attack Stages

**Issue:** current metric not granular and ignores paths  
**Proposed Solution:** PICA (Paths, Integrity, Confidentiality, Availability)



Figure 3: The CIA triad.

### 2. Problem Definition

#### Baseline

$$Urgency(AS) = Prevalence(AS) \cdot Severity(AS)$$

#### PICA

Node urgency is the normalised in-degree  $\times$  weighted CIA average  
 AS urgency is the average of the top X% urgent nodes

### 3. Methodology

1. How does PICA affect the (number of) urgent attack stages?
2. How are PICA's urgent nodes positioned in the attack graphs?
3. What are the effects of changing the weights in PICA?

### 4. Results

Attack Stage Urgency for baseline and PICA (15%) (CPTC-2017)

Attack Stage	Baseline	PICA (15%)
DATA_EXFILTRATION	1.000	0.722
DATA_DELIVERY	0.701	0.308
NETWORK_DOS	0.442	0.848
ACCT_MANIP	0.163	0.367
ARBITRARY_CODE_EXE	0.143	0.649
BRUTE_FORCE_CREDS	0.129	0.111
COMMAND_AND_CONTROL	0.102	0.390
REMOTE_SERVICE_EXP	0.075	0.266
SERVICE_DISC	0.058	0.335
VULN_DISC	0.041	0.662
USER_PRIV_ESC	0.034	0.127
INFO_DISC	0.027	0.367
ROOT_PRIV_ESC	0.027	0.114
HOST_DISC	0.024	0.386
SURFING	0.020	0.304
DATA_MANIPULATION	0.020	0.038
PRIV_ESC	0.007	0.017
PUBLIC_APP_EXP	0.000	0.051
DEFENSE_EVASION	0.000	0.000

Figure 4: Urgency scores for baseline and PICA (15%) on CPTC-2017.

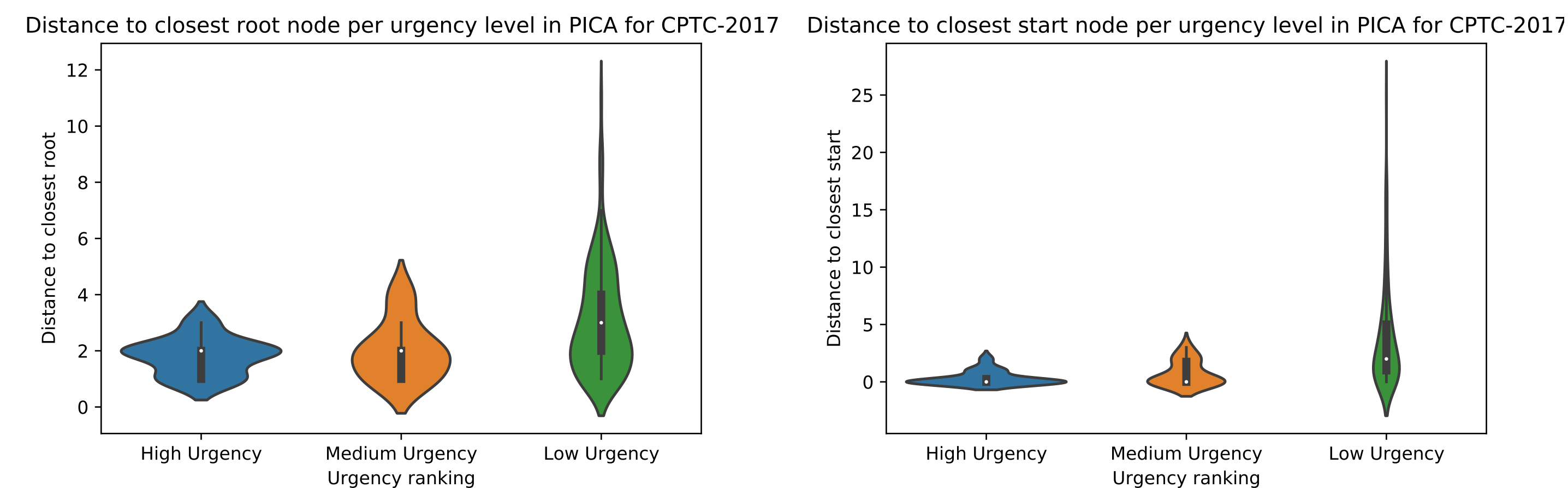


Figure 5: Distance to root node (left) and starting node (right) for nodes in different urgency levels in PICA (15%) for CPTC-2017.

Attack Stage Urgency for PICA (15%) with varying weights (CPTC-2017)

Attack Stage	[1, 1, 1]	[2, 1, 1]	[1, 2, 1]	[1, 1, 2]	[2, 2, 1]	[2, 1, 2]	[1, 2, 2]
NETWORK_DOS	0.848	0.554	0.687	0.849	0.570	0.848	0.848
DATA_EXFILTRATION	0.722	0.804	0.584	0.423	0.803	0.722	0.435
VULN_DISC	0.662	0.568	0.705	0.419	0.705	0.546	0.546
ARBITRARY_CODE_EXE	0.649	0.571	0.709	0.383	0.719	0.521	0.521
COMMAND_AND_CONTROL	0.390	0.344	0.426	0.229	0.433	0.313	0.313
HOST_DISC	0.386	0.365	0.353	0.256	0.399	0.358	0.289
ACCT_MANIP	0.367	0.296	0.367	0.266	0.355	0.319	0.319
INFO_DISC	0.367	0.347	0.335	0.243	0.379	0.341	0.275
SERVICE_DISC	0.335	0.317	0.306	0.222	0.346	0.311	0.251
DATA_DELIVERY	0.308	0.200	0.428	0.180	0.344	0.184	0.309
SURFING	0.304	0.245	0.304	0.220	0.293	0.264	0.264
REMOTE_SERVICE_EXP	0.266	0.235	0.291	0.156	0.296	0.213	0.213
USER_PRIV_ESC	0.127	0.112	0.101	0.101	0.112	0.127	0.101
ROOT_PRIV_ESC	0.114	0.092	0.114	0.083	0.110	0.099	0.099
BRUTE_FORCE_CREDS	0.111	0.099	0.089	0.089	0.099	0.112	0.089
PUBLIC_APP_EXP	0.051	0.041	0.051	0.037	0.049	0.044	0.044
DATA_MANIPULATION	0.038	0.023	0.057	0.021	0.044	0.020	0.040
PRIV_ESC	0.017	0.020	0.013	0.009	0.020	0.018	0.009
DEFENSE_EVASION	0.000	0.000	0.000	0.000	0.000	0.000	0.000

Figure 6: Urgency scores PICA (15%) with varying weights for the CIA triad on CPTC-2017.

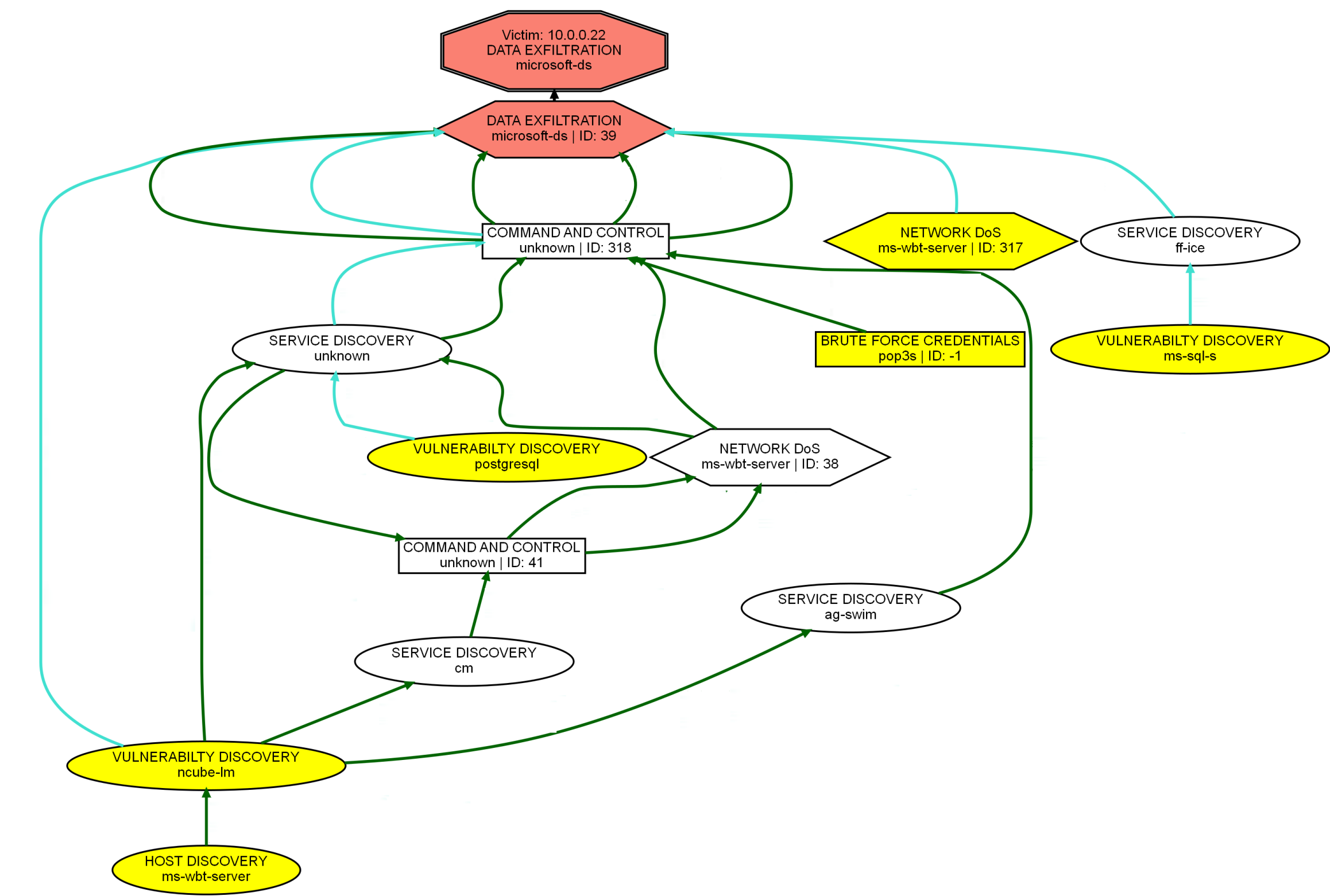


Figure 7: Example attack graph

### 5. Limitations

- Detection of many low-in-degree nodes
- Treats nodes as sequential
- Merging of low-severity nodes with (possibly) different context

### 6. Future Work

- Weighted node count, e.g. paths, objective distance
- Not merging low-severity nodes with (possibly) different contexts
- Different normalisation techniques
- Information loss in sub-graphs objectives

### 7. Conclusion

- PICA with 15% average a good balance between few urgent discovery attacks and retaining highly-urgent attacks
- PICA is more evenly balanced over the urgency levels, while baseline is more skewed
- Discovery attacks increase in urgency
- Objectives are often starting nodes
- Weights only have the desired impact on (close to) high-urgency attack stages

### Contact

Student  
 Senne Van den Broeck  
 S.M.Z.VandenBroeck@student.tudelft.nl  
 Responsible Professor: Sico Verwer  
 Supervisor: Azqa Nadeem

### References

[1] Azqa Nadeem, Sico Verwer, and Shanchieh Jay Yang. "SAGE: Intrusion Alert-driven Attack Graph Extractor". In: *Symposium on Visualization for Cyber Security (VizSec)*. IEEE, 2021.  
 [2] Azqa Nadeem, Sonia Leal Diaz, and Sico Verwer. "Critical Path Exploration Dashboard for Alert-driven Attack Graphs". In: [https://vizsec.org/files/2022/vizsec\\_p4\\_abstract.pdf](https://vizsec.org/files/2022/vizsec_p4_abstract.pdf) (2022).