

IISAS Cloud infrastructure

Viet Tran

Institute of Informatics, Slovak Academy of Sciences (IISAS)

IISAS-FedCloud site

- Among the first cloud sites in EGI Federated Cloud
- The first site with GPU support in FedCloud
- Powerful NVIDIA-A100 GPUs coming soon



Security monitoring at IISAS-FedCloud

- 2012-2022: OSSEC-HID IDS + network monitoring
- 2018-now: Zeek network IDS + abnormal detection

OSSEC configuration at IISAS

- OSSEC is a multiplatform, open source and free Host Intrusion Detection System
- Ossec-agent installed on every worker nodes for collecting data
- Iptables+ulog for network logging
- Customized rules for alerting
- Web-based GUI for monitoring changes and alerts

Advantages: powerful monitoring, GUI

Disadvantages: too static rules

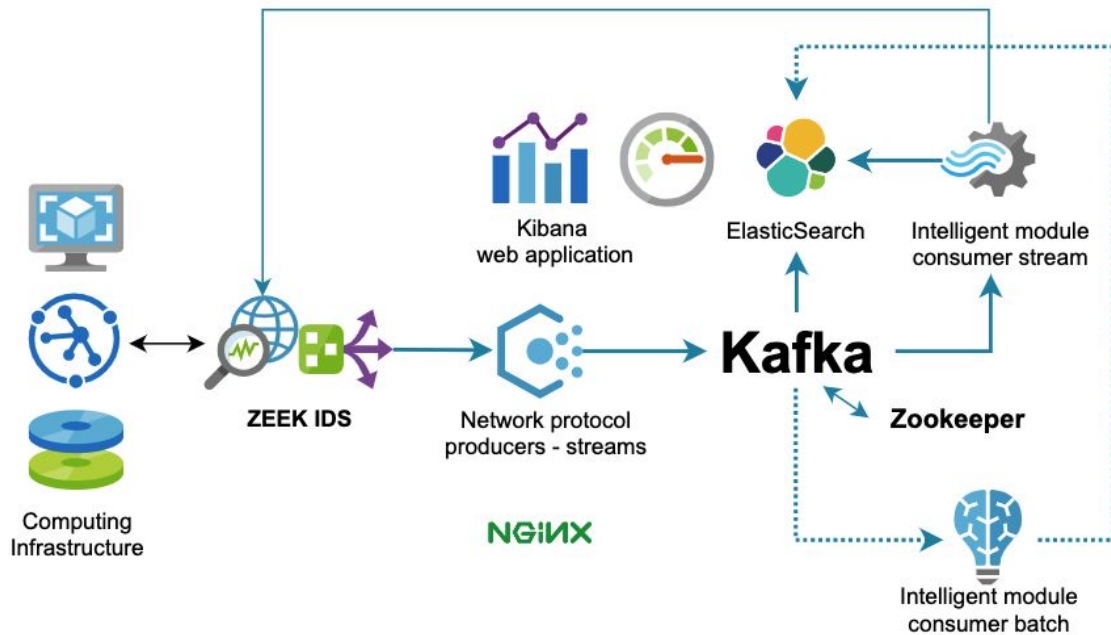
Zeek + abnormal detection

- Deployed as part of DEEP-HybridDataCloud project
- Zeek IDS for network monitoring
- Deep learning for abnormal detection

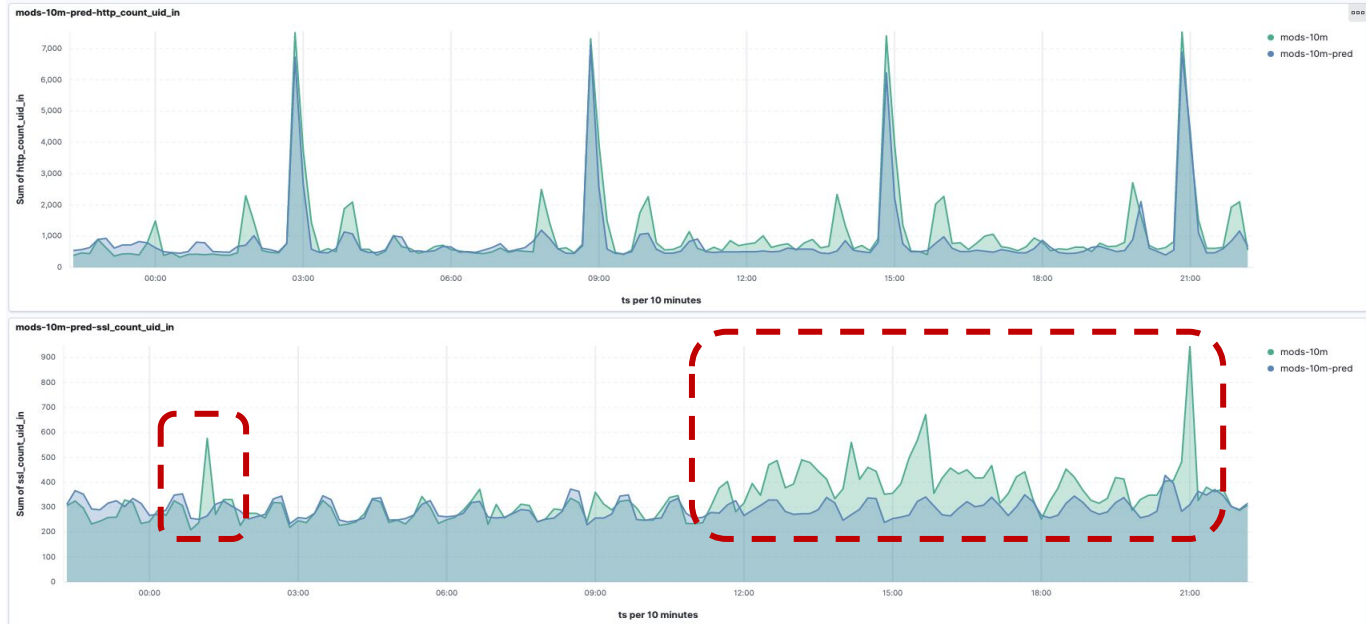
Advantages: powerful network monitoring

Disadvantages: Abnormal detections are still experimental

Zeek configuration at IISAS



Realtime monitoring and prediction



Thank you for your attention
