# Effective and Economical Protection for High-Performance Research and Education Networks

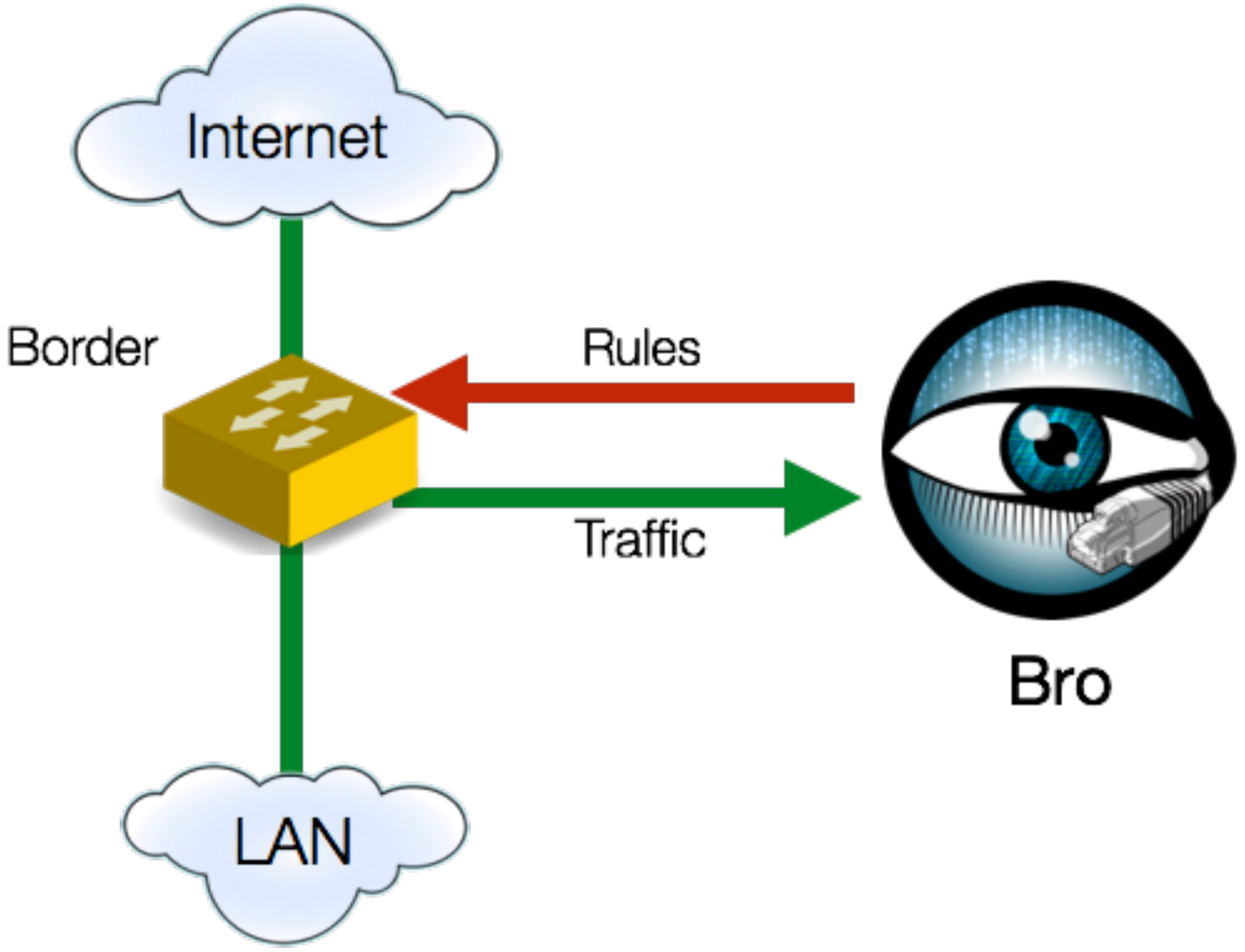
Johanna Amann

johanna@icir.org

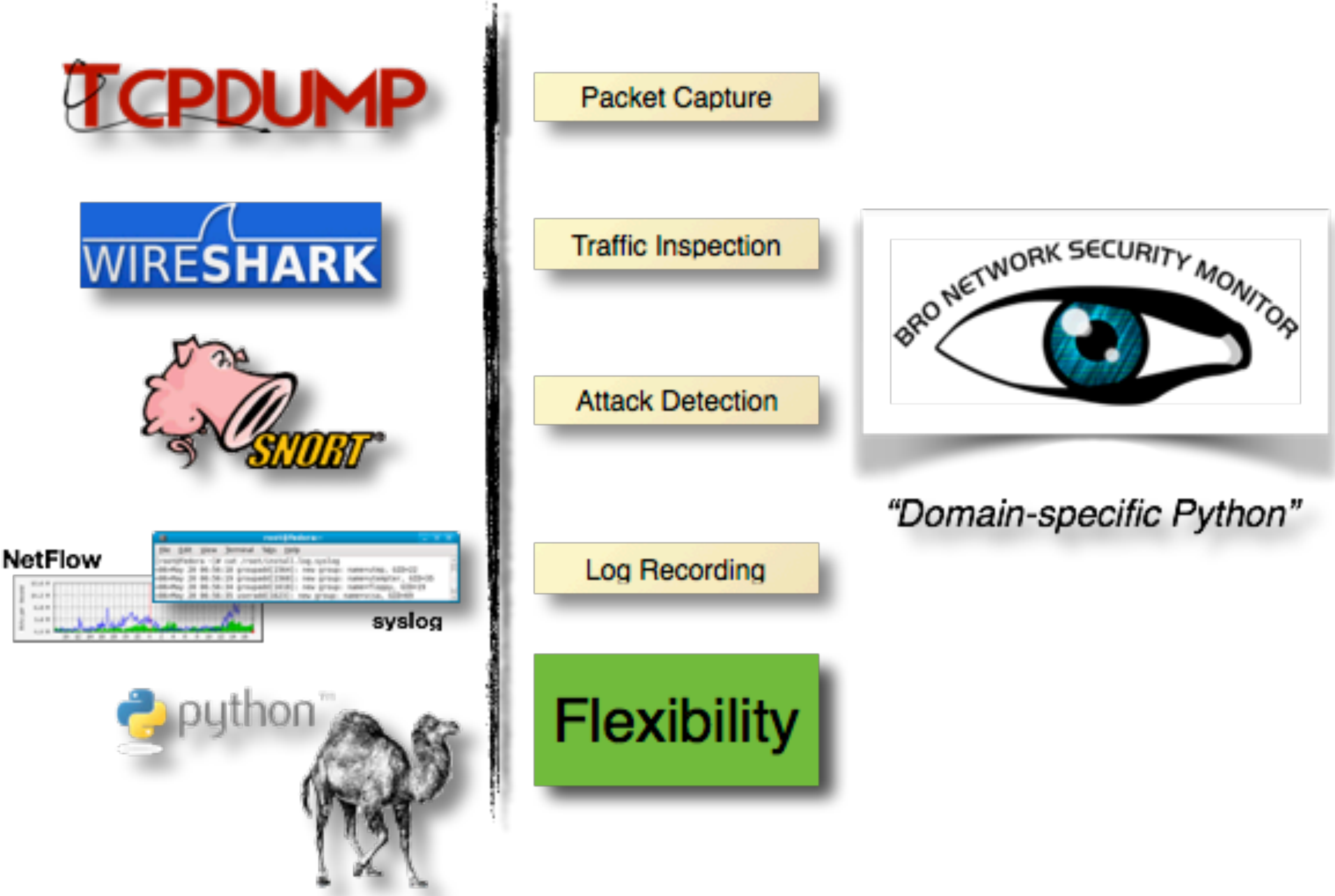
ICSI

INTERNATIONAL COMPUTER SCIENCE INSTITUTE

# Typical Network Monitoring Setup



# What is Bro?



Packet Capture

Traffic Inspection

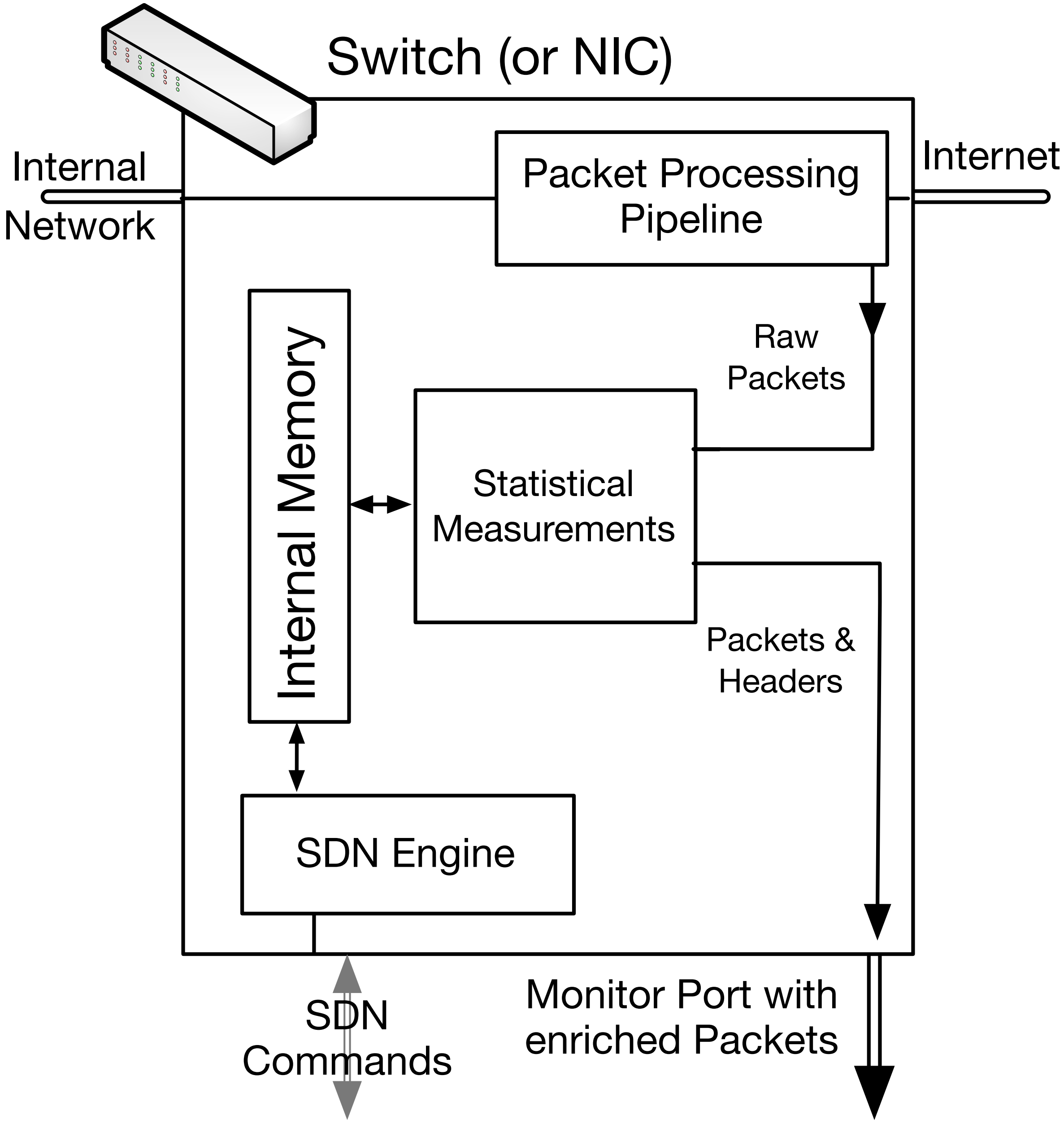
Attack Detection

Log Recording

Flexibility

*"Domain-specific Python"*

# Hard/Software Co-Design for Network Monitoring



# Domain-Specific Security Monitoring

- Domain-specific protocols
- User authentication
- Network activity profiling
- Security policy enforcement
- DOS Protection