

Alex Withers <[alexw1@illinois.edu](mailto:alexw1@illinois.edu)>  
 Justin Azoff <[jazoff@illinois.edu](mailto:jazoff@illinois.edu)>  
 Jim Marsteller <[jam@psc.edu](mailto:jam@psc.edu)>  
 Shane Filus <[filus@psc.edu](mailto:filus@psc.edu)>  
 Linh Cao <[linhcao2@illinois.edu](mailto:linhcao2@illinois.edu)>

## SDAIA Project

The Science DMZ Actionable Intelligence Appliance (SDAIA) project addresses a critical need for security solutions for open science networks, such as the Science DMZ model, and addresses the special architecture of these networks through a virtual security appliance that benefits from shared intelligence to protect the site, and further provide intelligence to the wider community.

- Decentralized model.
- Authentication logging honeypot software.
- Scalable, near realtime dissemination of threat intelligence data.

### Components:

- Ssh-auth-logger
  - Low interaction SSH honeypot written in Go.
  - Collects: src ip, user, password, etc.
- Zyre (zeromq+p2p)
  - Very fast p2p 1:N message passing with elliptical curve encryption
- Simple Service Discovery for peer discovery and key management
- CIFv3
  - Major performance improvements, stores events.
- Apache Kafka
  - Message/event passing queue for extensibility.
- Bro IDS
  - Monitors network traffic going into honeypot.
  - Monitors and alerts on indicators seen at other sites.

### Components deployed with Ansible playbooks.

### Apache Kafka Architecture

- Producer (Ssh-auth-logger)
- Kafka Cluster
  - One Topic
  - Three brokers
  - Each broker has one leader and two replicas
- Consumer
- Zookeeper controls different nodes, Kafka topics, messages, etc.

### Future Work:

- Passing message to cifv3
- Test on real system

