STINGAR

THREAT INTELLIGENCE FOR HIGHER EDUCATION

ResearchSOC

STINGAR, or Shared Threat Intelligence for Network Gatekeeping with Automated Response, is a solution developed by Duke University to identify and defend against attacks targeting your network.

Download

STINGAR's Community Honey Network (CHN) software.

Join the mailing list

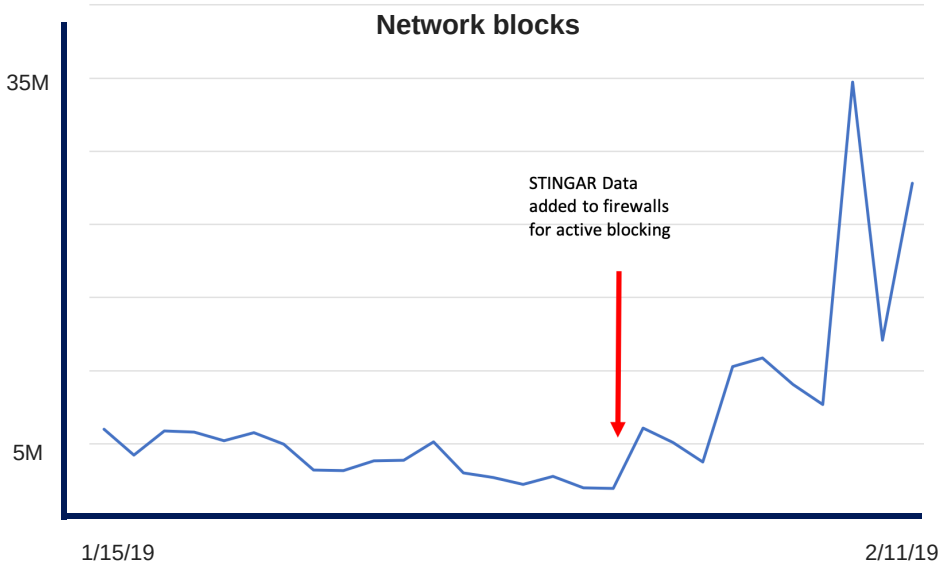
Visit https://researchsoc.iu.edu/contact/index.html to be added to the ResearchSOC mailing list.

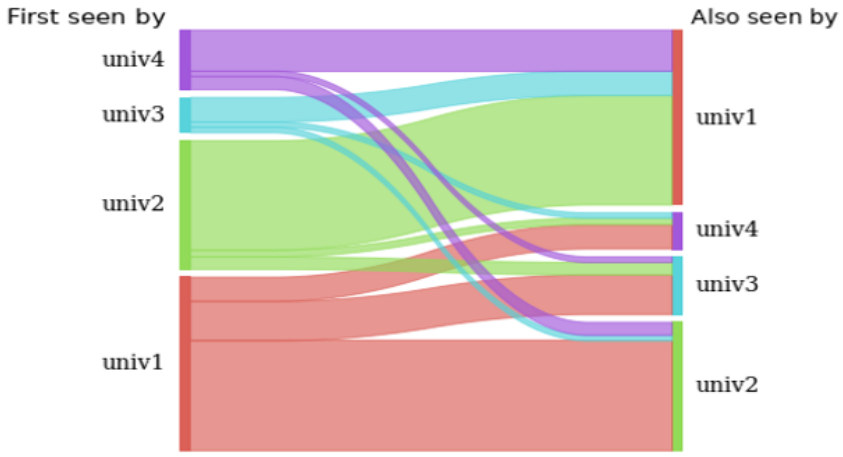
Visit website

Find a quick start guide, configuration documentation. and deploying to cloud providers.

With flexibility in mind, STINGAR:

- Makes use of network sensors (honeypots).
- Identifies attackers.
- Blocks via existing network security appliances
- Shares threat intelligence with trusted groups.





Using STINGAR, four participating universities are able to share information about attacks seen on their network with the other participants. When attacks are first seen at one university, the other 3 universities benefit from receiving the information to proactively block later attacks.

Visit researchsoc.iu.edu