Arastoo Zibaeirad

Skype: aras2zibaeirad
Email · LinkedIn · Website · GitHub

Research Interests

My research focuses on developing software and strategies in Incident Response Planning, mainly focused on security event correlation, log analysis, malware detection, and automated anomaly detection with machine learning, in specific Cyber Threat Intelligence and User and Entity Behavior Analytics.

I love researching at the intersection of software engineering, cybersecurity, and artificial intelligence.

Research Interests Keywords: Software Development, Machine Learning, Deep Learning, Threat Intelligence, Anomaly Detection, Reverse Engineering, Malware Analysis, Cloud Security, Network/Security Architecture, Network Complexity, Query Languages and Optimization, NoSQL databases, Indexing and Query Processing, Inverted Indexing, Text Analysis and Classification, SDN, Innovative Technologies

Education

- **Bachelor of Science in Electrical Engineering** **(11/2014-04/2019)**
  Iran University of Science and Technology (IUST), Tehran, Iran
  Thesis Title: Online Full-Duplex Temperature Monitor and Control

Honors and Awards

- **Huawei ICT Skill Competition Iran 2017 (1st prize)**
  Huawei company annually holds this competition over the world. It was about Network Routing, switching, and Security. I won the 1st prize awards among over 2000 participants in Iran.
- **Grants from Huawei University (2018)**
  Participated in a professional Computer Network class. (Fast Track)

Teaching Experience

- **Teaching Assistant for Linear Algebra** **(11/2018-02/2019)**
  Dr. Saeed Ebadollahi, Iran University of Science and Technology, Dept. of Electrical Engineering
  Developed assignments, marked assignments and exams.

Skills

- **Scripting**: Python, MATLAB
- **Databases**: SQL (MySQL), NoSQL (Elasticsearch, MongoDB)
- **Query Languages**: SQL, EQL (Event Query Language), KQL (Kibana Query Language), DSL (Domain Specific Language)
- **Others:** Linux, GIT, Docker

Professional Experience

- **Researcher and Developer at Andisheh Negar Pars(01/2021-Present)**

Mainly involved in developing and supporting security software related to Cyber Threat Intelligence, Incident Response, and Threat Hunting. Massive knowledge of SIEM, Elasticsearch Security technologies. Able to troubleshoot and optimize python software and new software designs. Successfully maintains professionalism and personal commitment with excellent communication and people skills with the ability to train and motivate a team.

- Develop an open-source application for correlating events, alerting incidents to Elasticsearch, and finally planning strategies in Incident Response and management (named Elastalert, written by Yelp).
- Customizing the open-source detection rules (written by Elastic) that are compatible with the MITRE ATT&CK framework to detect incidents.
- Research on open source/commercial security solutions: ELK (Elasticsearch, Logstash, Kibana) | Elastalert | MISP | Sagan | UEBA (User and Entity Behavior Analytics)
- Parsing log patterns with Logstash and integrated them with SIEM correlation.
- Tunning Elasticsearch and Logstash performance and configuration.
- Design, configure and manage the ELK cluster for centralized logging and search functionalities for the App and created watches to check for the health and availability of the nodes.
- Identify and remedy any indexing issues.
- Written watcher alerts based on required scenarios.
- Customize mapping for indexing documents in Elasticsearch
- Worked on Docker-Compose to create Docker containers for testing applications in the QA environment.
- Configured and Managed 18 nodes with docker-compose in Elasticsearch: 3 Master Nodes, 9 Data Nodes (Hot, Warm, Cold), 3 Coordinating Nodes, 3 Ingest Nodes.
- Worked with Docker Container, attaching to a running container, managing containers, and directory structures and removing Docker images.
- Apply software design and development practices in an agile scrum environment

Memberships

- **Member of EESA (Electrical Engineering Scientific Association)**
  EESA holds seminars, camps, extra curriculum classes, and so forth for students.

Courses and Certifications

- HCNA (*Huawei Certified Network Associate*)
- CCNA (*local certificate*)
- HCNP (*training course, it was held at Huawei University and Huawei HQ in Shenzhen, China.*)
- HCIE *(Self-study + Practical Experience, Fail in the exam, No certificate)*
- CEH (Certified Ethical Hacker) *(Self-study + Practical Experience, No certificate)*
- CompTIA Network+ *(local certificate)*
- CompTIA Security+ *(local certificate)*
- Linux LPIC-1 *(local certificate)*
- Incident Response and Planning *(3 months training course, Tehran)*

References

- Dr. Saeed Ebadollahi
  Electrical Engineering Department, Iran University of Science and Technology
  s_ebadollahi@iust.ac.ir

- Dr. Alireza Mohammad Shahri (retired)
  Electrical Engineering Department, Iran University of Science and Technology
  shahri@iust.ac.ir