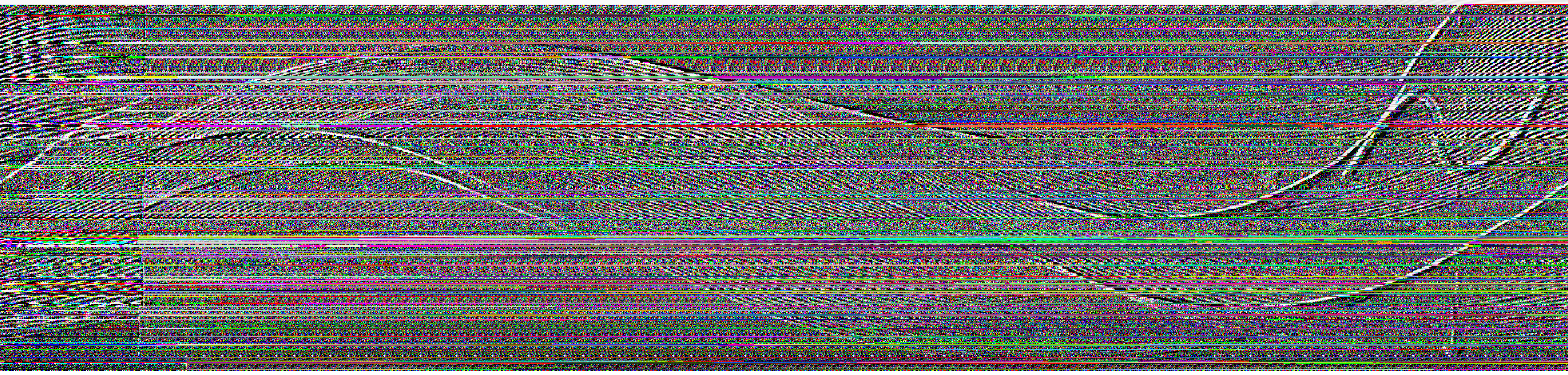

ndaal - Mamoona Aslam

Mamoona Aslam's resume content:

Chapter 1

Introduction

1.1 Availability

07.2024

1.2 Focus Areas

- Cloud Computing such as AWS, Azure
- Python Development
- Web Technologies
- IT Security
- **Automation/Orchestration**
  - Infrastructure as a Code (Ansible, Terraform, Pulumi)
  - Documentation as a Code (Sphinx)
  - Compliance as a Code (Prevent, Detect and Remediate)
  - Continuous Integration (CI)
  - Continuous Delivery (CD)
  - CasC (Configuration as Code)
  - JCasC (Jenkins Configuration as Code)
- Blockchain, Hyperledger
- Machine Learning / Data Science
- Internet of Things
- Container (e.g.; Docker, Podman)
- DevSecOps
- Site Reliability Engineering (SRE)
- Platform Engineering (PE)
- Hashicorp Secret Vault
- **BaFin**
  - BAIT (based on KWG (Kreditwesengesetz))
  - KAIT (based on KAGB (Kapitalanlagegesetzbuch))
  - VAIT (based on VAG (Versicherungsaufsichtsgesetz))

    - ZAIT (Zahlungsdiensteaufsichtliche Anforderungen an die IT von Zahlungs- und E-Geld-Instituten)

- Digital Operational Resilience Act (DORA) - Regulation (EU) 2022/2554
- European Cyber Resilience Act (CRA)
- NIS 2 Directive, European Union as Directive (EU) 2022/2555
- Critical Entities Resilience Directive (CER), European Union as Directive (EU) 2022/2557

1.3 Languages

- English (Fluent)
- English (Working Proficiency)
- German (C1)
- Urdu (native)

1.4 Locations

- Germany
- Europe (EU)

1.5 Experience

- more than 5 years

1.6 Sectors

- Automotive
- Consulting
- Finance
- Industry
- Information Technology
- Trade
- Transportation
- Healthcare

Chapter 2

Overview

2.1 Operating Systems

- Apple
  - Apple iOS
  - Apple macOS (previously Mac OS X and later OS X)
- Linux
  - Debian
  - Ubuntu
  - Red Hat RHEL/CentOS
- Windows

2.2 Automation - Orchestration

- Automation/Orchestration
- Infrastructure as a Code (e.g. Ansible, Terraform, Pulumi)
- Documentation as a Code (e.g. Sphinx)
- Compliance as a Code (e.g. Prevent, Detect and Remediate)
- Continuous Integration (CI)
- Continuous Delivery (CD)
- CasC (Configuration as a Code)
- JCasC (Jenkins Configuration as a Code)
- Threat Modeling as a Code
- reStructuredText
- Markdown
- Sphinx-doc
- Python
- bash
- Terraform
- OpenTofu (an Open Source Fork of HashiCorp Terraform)
- Ansible
- Pulumi
- Microsoft PowerShell
- Jenkins
- Git
- GitLab
- GitHub
- Azure DevOps

2.3 Programming Languages, Scripting Languages

Please have also a quick look on the section Automation and Orchestration. We want to prevent double entries.

- Python
- Javascript
- Typescript
- Shell-Scripts (bash)
- Solidity
- Ruby

2.4 Databases

- PostgreSQL
- Elasticsearch
- MongoDB
- MySQL (also MariaDB)
- HeidiSQL
- InfluxDB

2.5 Network

- Ethernet
- TCP/IP

2.6 Tools

- Amazon AWS
- Microsoft Azure
- CI/CD Pipelines
- Docker-Swarm
- Ansible
- Terraform
- Pulumi
- Elasticsearch, Logstash, Kibana, Beats (ELK)
- Linux KVM
- VMware
- Wireshark
- GitHub
- GitLab
- Microsoft Office
- Libre Office
- Sphinx-doc

2.7 Processes

- Agile
- Scrum
- PDCA iterative management of projects
- Waterfall Model
- GitOps
- DevOps
- DevSecOps
- Site Reliability Engineering (SRE)
- Platform Engineering (PE)
- Threat Modeling

2.8 Machine Learning

- **Analysis and Modeling:**
  - Regression
  - Clustering
  - Decision Trees
  - SVMs
  - Hypothesis Testing
  - Time-Series Forecasting
  - Data Visualization
  - Dimension Reduction
  - Ensemble Learning

  - Boosting
  - Stacking
  - Hyper-parameter tuning
  - Feature Scaling
  - Dimensionality Reduction
  - Anomaly Detection
  - Text Mining
  - NLP (Natural Language Processing)
  - Computer Vision
  - CNNs (Convolution Neural Networks), etc.
- **Data Science Tools:**
  - Pandas,
  - Numpy,
  - Scikit-Learn,
  - Tensorflow,
  - Keras,
  - Pytorch,
  - XGBoost,
  - LightGBM,
  - Scikit-Optimize,
  - Matplotlib,
  - Seaborn,
  - Plotly,
  - Cufflinks,
  - PySpark,
  - Sqlalchemy,
  - wxPython,
  - Tkinter, etc.

2.9 Other Skills

- Infrastructure as a Service (IaaS),
- Platform as a Service (PaaS),
- Software as a Service (SaaS),
- Atlassian Confluence,
- Atlassian JIRA,
- Azure,
- Azure cli,
- Continuous Integration (CI),
- Continuous Delivery (CD),
- Cyber Security,
- Splunk,
- Elasticsearch, Logstash, Kibana, Beats (ELK),
- Docker,
- Podman,
- IoT (Internet of things),
- Blockchain,
- Hyperledger,
- Microservices,
- Monitoring,
- OAUTH2,
- Ethereum,
- Quroum,
- Representational State Transfer (RESTful) with HATEOAS (Hypermedia as the Engine of Application State),
- Vagrant,
- Django,
- Nodejs,
- Flask,
- AWS,
- AWS cli,
- AWS services like WAF
- Ansible molecule,
- Python pytest,
- Bastion Hosts,
- DNS,
- CoreDNS,
- Route53 (DNS),
- Privileged Access Management (PAM),
- Hashicorp Secret Vault,
- OpenBao (an Open Source Fork of HashiCorp Secret Vault),
- eperi Gateway,

Chapter 3

Projects

Content

3.1 2023 - 2024

3.1.1 KELAG, Austria, Klagenfurt

```
Time:      11.2023 - 04.2024

Activity: Cloud Computing, Automation, Security

Tasks:     • Configured Elasticsearch, Logstash, and Kibana for seamless
```

(continues on next page)

(continued from previous page)

```
            log processing from Winlogbeat.
          • Orchestrated end-to-end log management, implementing
            real-time log shipping from Windows endpoints to ELK Stack
            (Elasticsearch, Logstash, Kibana).
          • Addressed delays in log shipping post system events (e.g.,
            power interruptions, network handover etc) and attacks
            by fine-tuning Winlogbeat configurations.
          • Developed Kibana dashboards for visualizing log trends
            and set up alerts for proactive responses to critical events.
          • Overcame challenges in detecting system failures
            by exploring continuous log streaming.
          • Proof of Concept for Cribl Log Aggegation
```

3.1.2 ESWE Stadtwerke, Germany, Wiesbaden

```
Time:     09.2023 - 05.2024

Activity: Cloud Computing, Automation, Security

Tasks:    • Automation for Hashicorp Secret Vault with Ansible
          • Resilient Hashicorp Secret Vault implementation
          • Automation Linux Hardening with Ansible
          • Automation Windows Hardening with Ansible
          • Documentation as a Code
          • Molecule testing within container (Docker, Podman)
          • Active Directory hardening
          • Automation of a secure DNS infrastructure with CoreDNS
          • Automated control of the hardening with the following tools:
            - PingCastle,
            - Rusthound,
            - Bloodhound,
            - Microsoft ARI,
            - Scoutsuite,
            - Monkey365,
            - Prowler,
            - Scuba gear,
          • Automating of Tier 0 hardened Active Directory environments
```

3.2 2023

3.2.1 OYAK Bank, Germany, Frankfurt

```
Time:     09.2023 - 10.2023

Activity: Cloud Computing, Automation

Tasks:    • Automation for Azure Log Management with templates
          • Automation for Azure Hardening with templates
```

3.2.2 MKS Instruments, USA, worldwide

```
Time:     02.2023 - 04.2023

Activity: Incident Response Team Ransomware

Tasks:    • Recreating VMware ESXi and Hyper-V landscape as part of the
            incident response team after a successful ransomware attack
            https://www.csoonline.com/article/3687098/mks-instruments-falls-victim-to-
↪ransomware-attack.html
          • Automating CIS hardened Windows 10 and Windows 11 analyst VMs
            on AWS with Pulumi, Terraform, Ansible and PowerShell
```

3.3 2022

3.3.1 H&M, Sweden, Stockholm

```
Time:     08.2022 - 10.2022

Activity: Cloud Computing, Automation, Azure

Tasks:    • Automation of a Compliance Check for Azure
            - create automated compliance check (Function as a App)
            - create a report with findings
            - create a Dashboard
            - using diverse Azure APIs
            - Main tools were Python, RESTFul, Ansible, Terraform, Azure-cli
          • Molecule testing within container (Docker, Podman)
          • Documentation as a Code
```

3.3.2 SABIC, Gelsenkirchen Germany

```
Time:     01.2022 - 03.2022

Activity: Automation with Ansible and Terraform

Tasks:    • Setup Linux Debian Test Environment with Ansible
          • Setup Linux Windows Test Environment with Terraform in AWS
          • Linux Hardening with Bash, Ansible
          • Windows Hardening with Ansible Powershell
```

3.4 2021 - till now

3.4.1 ndaal Gesellschaft für Sicherheit in der Informationstechnik, Cologne, Germany

```
Time:     07.2021 - present

Activity: Machine Learning

Tasks:    • Documentation automation & optimization
          • Machine Learning
          • Python Development
          • Hardening of Windows Systems especially Windows 2016, 2019 and 2022
          • Automation for Telegraf, InfluxDB, Grafana
          • Automation with Ansible [1], Terraform and Pulumi
          • Automation for Hashicorp Secret Vault with Ansible
          • Resilient Hashicorp Secret Vault implementation
          • Creating automated tests with Ansible molecule and Python pytest
```

3.5 2020

3.5.1 AKKA TECHNOLOGIES - Köln, Germany

```
Time:     11.2019 - 09.2020

Activity: Blockchain, VANET (Vehicular adhoc network),
          Automation, IT Security, Web Technologies

Tasks:    • Solved main issues in VANET by utilizing Blockchain technology, to benefit␣
↪from its
            built-in integrity and trust.
          • Developed a customized blockchain to store and transact Vehicle Sensor Data␣
↪in
            Python using Flask.
          • Imported Real world maps (OpenStreetMap), extracting street and roadside
            components and Simulating Traffic according to these parameters in SUMO.
          • Generated Vehicle Data from the simulation, filtered and parsed from XML to␣
↪JSON
            via RESTAPI endpoints into Blockchain application.
          • Automated security key / certificate generation and Securing communication␣
↪(Curve
            for ZMQ, SSL/TLS for HTTP traffic).
          • Containerized all applications in Docker, and created Docker-Compose␣
↪playbooks for
            deployment locally or in AWS Cloud.
          • Created a metrics endpoint and used it to generate visualization.
```

3.6 2019

3.6.1 FRAUNHOFER (FIT) - Sankt Augustin, Germany

```
Time:     11.2019 - 09.2020

Activity: Blockchain, Quality Compliance,
          Automation, IT Security, Web Technologies, Industry 4.0

Tasks:    • Setup Quorum blockchain implementations on vagrant, docker and Amazon EC2
          • Tested out Quorum transaction and consensus algorithms.
          • IoT Arduino Programming and Data acquisition of IoT sensor data through MQTT.
          • Wrote Smart contract on Ethereum blockchain in Solidity.
          • Created Web templates with JavaScript / HTML for User Interface.
          • Developed Core application in Python using Flask that interacts via REST API␣
↪for
            deploying smart contracts in Blockchain.
          • Parsed JSON Data from Blockchains and generated compliance certificates.
```

3.7 2018

3.7.1 TH KOELN - Cologne, Germany

```
Time:     04.2018 - 07.2018

Activity: Blockchain, VOIP, SIP Server, Automation


Tasks:    • Blockchain technology was used to create a shared ledger between Asterisk SIP
            servers that contain user information.
          • Blockchain web (Flask) application was created to allow users to signup &␣
↪login, view
            the blockchain, make transactions and mine new blocks, using REST API.
          • SIP registration/calling/answering functions were scripted using PJSIP␣
↪library and
            calls were initiated via Android SIP client.
```

3.8 2017-2018

3.8.1 TH KOELN - Cologne, Germany

```
Time:     11.2017 - 02.2018

Activity: DASH, Video streaming, Traffic Shaping


Tasks:    • Setup HTTP video Streaming using NGINX server and DASH.JS framework.
```

(continues on next page)

(continued from previous page)

```
          • MPEG-DASH conversion and MPD generation with FFMPEG and MP4BOX.
          • Traffic Shaping at bridge gateway using Linux networking tools such as iperf,
            Wondershaper etc.
          • Video streaming metrics via DASH.JS and packet analysis with Wireshark.
```

Chapter 4

Publications

Content

4.1 2023

4.1.1 2023, October eleventh

```
Integrating Data-Privacy Through Pipelines at data2day conference

All data stored on a filesystem has some metadata. Sometimes more and
other times less. This can be a huge privacy breach, since the metadata
can contain sensible data that can be used to identify persons, locations,
or other interesting information.

To not leak any hidden sensitive information, it is crucial to ensure
that all data that is stored and processed is clean. This task is
predestined to automate.

This talk will focus on how to remove all the metadata and automate this
procedure through data processing pipelines that can be used in an MLOps
as well as the classical DevSecOps cycle. [1]_
```

4.2 2021

4.2.1 2021, December fourteenth

```
Research Paper log4j Vulnerability [2]_
```

4.2.2 2021, November 21th

```
Ansible Role InfluxDB 2.0 with encryption on Linux Debian [3]_
```

Chapter 5

Education

Content

5.1 2023

```
- Certified LPIC-1, v5, Linux Professional Institute,
  Linux Hotel

- Information Security Threat Modeling (STRIDE)
```

5.2 2022

```
- Hashicorp Vault training with certification Vault Associate (002)
```

5.3 2017-2020

```
- Master of Science in Communication Systems and Networks
  Technische Hochschule Köln, Köln (Germany)
```

5.4 2010-2014

```
- Bachelor of Engineering in Electronic Engineering
  NED University of Engineering & Technology, Karachi (Pakistan)
```

Contact

ndaal Gesellschaft für Sicherheit in der Informationstechnik mbH & Co KG

Headquarter: Adolf-Grimme-Allee 3, D 50829 Köln, Deutschland.

Office: Christophstr. 15-17, D 50670 Köln, Deutschland.

[redacted]