



# Elizabeth Ijeoma Ojeme

---

**Nationality:** Austrian | **Gender:** Female | **Phone number:**

(+43) 6603763238 (Home) | **Email address:** [ojeme.elizabeth@gmail.com](mailto:ojeme.elizabeth@gmail.com) |

**Address:** Lore-Kutschera-Weg 20/5/8, 1120, Wien, Austria (Home)

## ● ABOUT ME

---

Passionate about Audit, ISO27001, Change and Information Security Risk Management, Threat and Vulnerability Management, Security monitoring etc.

## ● WORK EXPERIENCE

---

01/05/2023 – CURRENT Vienna, Austria

**INFORMATION SECURITY OFFICER (ISO) SOZIALVERSICHERUNGS-CHIPKARTEN BETRIEBS- UND ERRICHTUNGSGES.M.B.H. - SVC**

---

- Carrying out risk analyses for new software that the services want to procure and for requested new functions and plug-ins for software that are already in the production environment.
- Processing tickets for security incidents and problem management. Conduct lessons learned sessions after each security incident.
- Technical support for all CRISAM related activities except server and application upgrade support.
- Project manager for the implementation of the SIEM solution. Handling all topics, from requirements gathering, impact assessment, design, deployment to go-live phase.
- Project manager for the implementation of Email Security Gateway & EDR. Handling of all topics, from requirements gathering, impact assessment, design, deployment to the go-live phase.
- Define and design the security incident management optimization process, the Information Security Incident Response Management document, which includes the security incident response process/plan, lifecycle, playbook, severity, incident categorization and recommended actions.
- Ensure that SVC domains that are due to expire soon are reviewed and renewed.
- Deploy a sandbox solution to support the proper investigation and analysis of email security incidents.
- Support the execution of internal pen tests, including the evaluation of the pen test report for found and known security vulnerabilities and the coordination with the responsible services for remediation measures and the cross-checking of their effectiveness.
- Provide the necessary support in accordance with ISO 27001 and in preparation for ISO 270001 certification, including assessing identified gaps and ensuring implementation and verification of corrective actions.
- Collaborate with respective departmental team leaders to establish an effective information security audit program.
- Ensure that the organization IT systems are compliant with the changing laws and regulations.
- Develop and implement internal audit plans that are aligned with the organizational objectives and security requirements. Schedule and conduct IS internal audits, as well as analyze and interpret IS audit
- Review and interpret cybersecurity / information security policies and controls and make changes wherever needed.
- Develop and create security awareness trainings and send it out to all employees.

01/06/2021 – 30/04/2023 Vienna, Austria

**SECURITY ENGINEER ANOVIS IT- SERVICES AND TRADING GMBH**

---

- Responsible for email security gateway, web application firewall, vulnerability management, deception technology and CloudGen Firewall.
- Implemented security project (deployment, analysis, configuration, roll-out and management of the security tool)
- Upgraded Proofpoint protection server to latest release, as well as relevant patches, MLX and Spam engines.
- Added new Proofpoint agent to the master for better performance of email processing
- Analysed email security incidents, mitigated threat, extracted malicious emails from user mailboxes
- Created policy routes, email protection security rules and implemented exemptions for trusted host/IP/URL

- Performed sandboxing of URLs and Attachment and compared with the verdict of the protection server before releasing quarantined messages to the end users
- Vendor management (discussed open cases, new features with Proofpoint, agreed on solutions)
- Added and removed senders from organizational safe and block list
- Performed DKIM Key rotation (Generated new DKIM keys, provided to customer to update their DNS and tested to ensure email authentication continues to function)
- Adding a new inbound domains, mTLS domains
- Defined project timelines in alignment with customer. Gathered OS and HW requirement, installed and configured vulnerability management system (Nessus) and necessary packages
- Created and scheduled scans for different locations and generated high level report for the customer to mitigate vulnerability in their infrastructure.
- Conducted investigation to ensure the firewall isn't blocking Nessus scan requests, thereby impacting the scan results.
- Upgraded the Nessus Instance to latest release.
- Added and removed services on Web application firewall and defined security policies based on customers requirement.
- Imported new certificates and assigning to the WAF services
- Configuring cookie and pattern exemptions, added specific HTTP methods that are required for specific security policies
- Created URL and Header allow/deny/ rules as recommended by the vendor to block newly detected vulnerabilities
- Creating json key profiles to allow certain key in request that triggers json violations.
- IP reputation (Blocking request from certain countries or geographical locations on the web application firewall)
- Migrating customer on-premise web application firewall to web application firewall as a services and ensuring necessary security configurations are in place and enabled.
- Actively investigated, analysed web application firewall incident tickets and implemented change request
- Prevention of attacks exploiting web application's known vulnerabilities such OWASP top 10 using or Baracuda WAF tools to filter, inspect and block HTTP traffic to and from a web service.
- Created new VLAN on the firewall, configured network box and server Ips.
- Created global, local firewall objects and firewall ruleset. Carried out live troubleshooting session to identify and fix problems

01/12/2020 – 31/05/2021 Vienna, Austria

**SENIOR NETWORK MANAGEMENT SYSTEM ENGINEER** KAPSCH CONVERGED SERVICES GMBH  
(FORMER LIBERTY GLOBAL)

---

06/02/2012 – 30/11/2020 Vienna, Austria

**NETWORK MANAGEMENT SYSTEM ENGINEER** LIBERTY GLOBAL

---

- Lead expert for the monitoring tool ServAssure Performance Management (SAPM) und AlarmCentral that monitors over 16 Million customer devices in 10 European countries.
- Administrator for host and service check monitoring with Nagios and host and trap integration using Spectrum umbrella system.
- Incident and problem ticket handling, fixing with agrees SLA. Change request implementation.
- Project implementation from assessment phase to implementation and go-live phase
- Ensure that the central design, build and integration principles are properly followed and that all applications in scope are deployed, optimized and maintained in a fully functional and scalable way.
- Responsible for supporting the strategic delivery and operations of the Service Monitoring and Assurance solutions to enable centralized monitoring capabilities for Liberty Globals 10 European country networks, systems and services.
- Point-of contact for other Corporate groups and countries on all Assurance/Monitoring related topics
- Hands-on resolution management of operational issues with the help of outsourced partners, respectively vendors
- Ensure that SAPM, Alarmcentral, Nagios und Spectrum, Transmode Systems are stable and available to users. Minimize downtime, quick recovery from outages, carry out root cause analyses and write a report to the impacted country management.
- Overseeing the technical design of the SAPM/AlarmCentral environment ensuring proper scaling and service availability
- Governance of engineering and implementation tasks required for these systems. Performance analyses, tuning and capacity planning.

- Migrated SAPM application for all 10 Liberty countries from Solaris to Linux. Installed patches, perform application upgrade and fine tune monitoring after upgrade. Ensuring all requirements are met prior to upgrade and monitoring systems is adjusted after the upgrade.
- Implemented Spectrum trap/MIB Integration for several technologies MIBs for fault detection and alarming.
- Built, installed, and monitored over 500 Star nodes/Server for SAPM application in 10 European countries.
- Starnodes and CMTs Provisioning and configuration using appropriate community strings..
- Conducted trainings for ServAssure Advanced Performance Management users
- Vendor management, alignment on opened cases and agree on a solution for further improvement and implementation.
- Server and application hardening
- Installed Splunk forwarder on SAPM system for logs forwarding, dashboard and report creation.
- Security events log onboarding, parsing, searching, analyses for dashboard creation using different use cases.
- Integrated SAPM Systems with LDAP for user and group management and set permissions for users.
- For data privacy purpose: Implemented DOCSIS network topology data visibility restriction for AT-Wierer, AT-Kurthaler und AT-Rolland, so that they do not see nor access Liberty Global data.
- Using Tcpdump and Wireshark to capture packets and conduct analyses

## ● EDUCATION AND TRAINING

04/09/2018 – 18/11/2021 Innsbruck, Austria

**BACHELOR OF ARTS IN BUSINESS ADMINISTRATION** Internationale Hochschule Management Center Innsbruck (MCI)

**Address** Universitätstrasse 15, 6020, Innsbruck, Austria

05/09/2005 – 14/11/2008 Ibadan, Nigeria

**NATION DIPLOMA (ND) IN COMPUTER SCIENCE** The Polytechnic of Ibadan (Fachhochschule)

**Address** Sango eleyele road, Ibadan, Nigeria

07/09/1998 – 28/06/2004 Ibadan, Nigeria

**SENIOR SECONDARY SCHOOL (GYMNASIUM)** Orogun Grammar School

**Address** Ojo-road Ibadan, Nigeria, Ibadan, Nigeria

03/09/1990 – 30/06/1998 Ibadan, Nigeria

**PRIMARY SCHOOL COMPLETION** Command Children School

**Address** Letmauck Cantonement Mokola , Ibadan, Nigeria

## ● LANGUAGE SKILLS

Mother tongue(s): **ENGLISH AND KWALE**

Other language(s):

	UNDERSTANDING		SPEAKING		WRITING
	Listening	Reading	Spoken production	Spoken interaction	
<b>GERMAN</b>	B2	B2	B2	B2	B2
<b>YORUBA</b>	C1	C1	C1	C1	C1

*Levels: A1 and A2: Basic user; B1 and B2: Independent user; C1 and C2: Proficient user*

## ● DIGITAL SKILLS

Security Incident Handling & Response | risk analysis | Vulnerability Management | Network security | Malware Analysis | Good knowledge of Windows and Linux O.S

## ● ADDITIONAL INFORMATION

---

### BARRACUDA EMAIL PROTECTION CERTIFICATION

16/01/2023 – 16/01/2025

**Barracuda Cloud to Cloud Backup Certified Product Specialist**

---

20/12/2022 – 20/12/2024

**Barracuda Web Security Gateway - Foundation**

---

22/11/2022 – 22/11/2024

**Barracuda Essentials Troubleshooting**

---

20/09/2022 – 20/09/2024

**Barracuda Cloud-to-Cloud Backup - Foundation**

---

19/09/2022 – 19/09/2024

**Barracuda Email Protection - Cloud Archiving Service – Foundation**

---

15/09/2022 – 15/09/2024

**Barracuda Email Protection - Email Gateway Defense - Foundation**

---

### ACHIEVEMENTS

10/10/2018 – 10/10/2018

**Extraordinary performance bonus in the course of the cable route project (Awarded by Liberty Global)**

---

### BARRACUDA MESSAGE ARCHIVER CERTIFICATION

12/01/2023 – 12/01/2025

**Barracuda Message Archiver Certified Product Specialist**

---

14/07/2022 – 14/07/2024

**Barracuda Message Archiver – Foundation**

---

### BARRACUDA WEB APPLICATION AS A SERVICE & ON-PREM CERTIFICATION

20/11/2022 – 20/11/2024

**Barracuda WAF-as-a-Service Certified Product Specialist**

---

06/11/2022 – 06/11/2024

**Barracuda WAF-as-a-Service – Advanced**

---

24/10/2022 – 24/10/2024

**Barracuda WAF-as-a-Service – Foundation**

---

06/09/2022 – 06/09/2025

**Airlock WAF Allrounder Secure Access Hub & Connaisseur Gateway**

---

23/06/2021 – 23/06/2023

**Barracuda Web Application Firewall – Foundation**

---

### PROOFPOINT PROTECTION SERVER & THREAT RESPONSE CERTIFICATION

02/08/2022 – 02/08/2024

**Protection Server - Level 3 - certification**

---

13/05/2022 – 13/05/2024

**Protection Server - Level 2 - certification**

---

01/12/2021

**Protection Server Security – Level 1**

---

30/11/2021

**Protection Server Configuration – Level 1**

---

03/03/2022

**Threat Response Auto-Pull (TRAP) Integration and Incident Response – Level 1**

---

23/02/2023

**Threat Response Auto-Pull (TRAP) Administration – Level 1**

---

23/02/2022

**Threat Response Dashboard – Level 1**

---

23/02/2022

**Targeted Attack Protection (TAP) Threat Reporting – Level 1**

---

23/02/2022

**TAP SaaS Defense – Level 1**

---

11/02/2022

**Targeted Attack Protection (TAP) Threat Analysis – Level 1**

---

22/01/2022

**Targeted Attack Protection (TAP) Foundations – Level 1**

---

20/05/2022

**Email Fraud Defense (EFD) Foundations – Level 1**

---

04/03/2022

**Closed-Loop Email Analysis and Response (CLEAR) – Level 1 and Level 2**

---

## **VULNERABILITY MANAGEMENT CERTIFICATION**

01/10/2021

**Nessus Foundation**

---

## **BARRACUDA CLOUDGEN FIREWALL CERTIFICATION**

25/08/2021 – 25/08/2023

**Barracuda CloudGen Firewall – Large Scale Management**

---

09/06/2021 – 09/06/2023

**Barracuda CloudGen Firewall – Foundation**

---

## **PERFORMANCE & FAULT MANAGEMENT CERTIFICATE**

05/12/2016

**Ca Spectrum R10 Optimization And Customization 300 – Broadcom Inc.**

---

12/08/2015 – 14/08/2015

**Unix/Linux Advanced Administration Course**

---

18/11/2013 – 19/11/2013

**Unix/Linux 1 Fundamentals**

---

31/05/2012

**Arris Servassure Advanced Performance Management Administrator (SAPM) – Arris Group B.V.**

---

25/05/2012

**Ca Spectrum R9.1 Foundation 200 Administrator – Broadcom Inc.**

---

26/11/2008 – 26/11/2011

**Cisco Certified Network Professional**

---