

# Eduardo Milhomem - <https://eduardomilhomem.tech>



## Summary

Dynamic and dedicated IT System Security Engineer with 10+ years of comprehensive experience in IT Systems Engineering and Security Operations. Recent hands-on experience as an IT Security Analyst in a SOC environment, where I specialised in monitoring, detecting, and mitigating complex security threats. Proven expertise in securing diverse IT infrastructures. Adept at aligning security strategies with business goals, ensuring robust protection of critical assets. Solid soft skills and ability to collaborate across international teams.

## Professional Experience

**Worldsec Technologies LLP**  
Karnataka, India

10/2023 – 06/2024

### IT Security Analyst - Remote Internship

- Continuously monitor security information, event management systems (Splunk and ArcSight), and other security tools to detect potential security incidents.
- Review and analyse security logs, alerts, and reports from various network devices, applications, and systems.
- Prioritise incidents based on their impact and urgency.
- Escalate confirmed security incidents to L2 or L3 analysts for further investigation and remediation.
- Identify and document false positives, tuning the detection systems to reduce unnecessary alerts.
- Conduct fundamental threat analysis and research on emerging security threats and vulnerabilities.
- Provide on-call support during off-hours to monitor and respond to security incidents.


**Woodman Asset Management AG**  
Zug, Switzerland


03/2019 – 09/2023


### Senior IT System Engineer


- Administrate the Microsoft 365 platform, Azure (Identity-Entra ID), and Exchange Online, and manage SharePoint, Security and Teams Portals, as well as hands-on ArcSight and Splunk.
- Manage server and IT infrastructure issues, including troubleshooting LAN, WAN, DNS, VPN, endpoint, Wireless access points, Photocopier printers, IP telephones, mobile phones, website hosting, MPLS connection, networking, and application program issues.
- Create and maintain IT documentation, security policies and configuration standards, including a Business Continuity Plan.
- Manage and collaborate with third-party IT contractors (Bloomberg, Abacus, Lucanet, WIZE, Expersoft, Docuware, Pythagoras, Adobe Professional, Docusign, and IP telephone providers to ensure that stakeholders have a stable, efficient and secure IT environment.
- Train users on cybersecurity IT awareness and advise them about risks and procedures to enhance cyber resilience.
- Applied encryption to all devices, including desktops and laptops, and implemented e-mail server point-to-point security hardening.
- Experience implementing authentication services and working with AD, MFA and IAM management.
- Support network infrastructure components, including firewalls, gateway routers and switches.

## Personal Details


 Holzmoosrütistrasse 1B  
CH - 8820 Wädenswil


 [eduardo@eduardomilhomem.tech](mailto:eduardo@eduardomilhomem.tech)

 +41 79 961 62 27

 Married, 2 Children

 <https://www.linkedin.com/in/edmil>

 Nationality: British and Brazilian

 Residence Status:  
C Permit – Since 2006

## Languages

- Portuguese Mother Tongue
- English Fluent
- French Fluent
- German B2 Level
- Spanish Intermediate

## Hobbies

I enjoy sports, cooking, reading, and spending time with my family and friends.

## **Tool Competencies**

---

- Expert in Microsoft 365, AD, Azure Entry ID, Office 365, Server 2016, Macs, Linux, Outlook, Project, To Do, SharePoint, OneNote, Relational Database, Bloomberg
- Administrator
- IOS & Android
- SIEM – ArcSight and Splunk

**\*\* See more technical skills below**

## **Business Competencies**

---

- Several years of experience in Microsoft and Mac platforms environments.
- Extensive know-how in Finance business operation processes.
- Anticipate future technology trends and their impact on the business.
- Develop and implement long-term technology roadmaps.
- Align IT initiatives with business goals and objectives.

## **Methodological Competencies**

---

- Project & Program Management
- Data Analysis
- Problem-Solving
- Process improvement (ITIL, SCRUM)

## **IT Specialist**

- Administrating Windows Server 2008 and Exchange 2010, Windows 7/10, Office 2010/2013/16, Office365, Cloud Platform, Virtual Citrix Server support, Macs and Network Infrastructure Management.
- Support the entire network infrastructure architecture, such as firewalls, routers, and switches.
- Lead IT Project management in Zurich, UK, US and Singapore.
- Set up new desktops, laptops, mobile phones, Citrix, and hard and soft IP telephones and tablets.
- Provide service for product teams to identify applicable Cyber cybersecurity standards and laws.
- Providing responsive support to all end-user questions and best IT security practices.
- Working directly with external providers to resolve server & infrastructure problems, including LAN, WAN, WIFI DHCP, TCP/IP, IMAP, POP, SMTP, FIREWALL, AV, patch cabling and fault finding.
- Manage and support AV for Conference meeting rooms – Zoom, Sky4B, and Webex.
- Manage peripheral IT equipment, including printers, IP telephones, and mobile phones.

**Zürich International School**  
Wädenswil, Switzerland

08/2008 – 06/2014

## **IT Technician**

- Manage Active Directory and support stakeholders.
- Create computer images for PC and Mac Win7/8 and deploy them.
- Manage Servers and support clients (Win/Mac).
- Managing MDM for 700 iPads, iMacs, and iPhones.
- Responsible for Annual Budget, IT suppliers and IT projects.

**Baker McKenzie – US Legal Tax Team**  
Zurich, Switzerland

05/2007 – 08/2008

## **IT Support / Legal Assistant**

- Microsoft Office IT support.
- Troubleshoot Servers, workstations, and IT equipment.
- Conflict checks, collaborating with the tax team to onboard new clients.
- Business Application Trainer (CMIS) for Legal Assistants.

**Stimulating World Research**  
London, UK

06/2001 – 03/2006

## **IT Manager / Helpdesk Support**

**Environmental Investigation Agency**  
London, UK

09/2000 – 03/2001

## **IT Consultant**

## **Academic Qualifications**

---

<b>Arden University, Coventry, UK</b> MSc IT Security Management	2017 - 2022
<b>Teesside University, New Castle, UK</b> BSc Business Computing	2011 - 2013
<b>University of Westminster, London, UK</b> HNC Information System, Computing	1996 - 1998
<b>Hammersmith and West London College</b> BTEC in Computer Studies	1994 – 1996



## Further Education



## Personal Competencies

- Technical Knowledge
- Collaborative Teamwork
- Attention to details
- Learning agility
- Solid soft skills
- Time management
- Customer service

### Legend →

- Very good knowledge** ●●●●
- Good Knowledge** ●●●○
- User knowledge** ●●○○
- Knowledge applied some time ago** ●○○○

Splunk Enterprise and Security Administrator Training Certificate	2024
Certified CrowdStrike – Falcon EDR/XDR	2023
Certified SOC Expert	2023
Certified SOC Analyst Foundation	2023
Azure - Understanding the Big Picture	2023
Python for Absolute Beginners	2023
Introduction to FortiGate	2023
Certified Chief Information Security Officer	2022
Introduction to JavaScript	2019
Security+ Certification	2018
Communicating With Impact	2018
Cyber Security Course: Anonymous Browsing	2017
Learn Ethical Hacking From Scratch Online	2017
How To Defeat Advanced Malware	2014
ITIL Foundation	2014
How To Protect Your Website From Bot Attacks	2014
Advanced Threat Detection in ICS – SCADA Environments	2014
Network+ Certified Professional - CompTIA	2005
A+ Certified Professional – CompTIA	2005

## Technical Skills

### System Administration

- Microsoft 365 Azure, AD, Entra ID, Security, Exchange Online, SharePoint, Sophos Endpoint, Defender, Teams, Security Portal. ●●●●
- Desktop & Workstation Management: Setup, reimaging, MDM for mobile devices (phones, iPads) ●●●●
- Software Management: Expersoft, Wise, Abacus, SAP B1, Sage, Lucanet, Pythagoras, Docuware, INSA ●●●●
- IT Technician Skills: Hardware repair, software installation, user support ●●●●
- Video Conferencing: Room setup, maintenance, troubleshooting ●●●●

### Security & Compliance

- SIEM: ArcSight, Splunk Enterprise (Administration, Log Analysis, Incident Response) ●●●●
- Bloomberg Administrator and client support ●●●●
- Vulnerability Management: Refinitiv World-Check ●●●●
- Data Security: Compliance with relevant regulations (GDPR) ●●●○

### Project Management

- Acquisition, Data Migration, Office Relocation: Planning, execution, risk management ●●●●
- Agile/Waterfall Methodologies: User stories, sprints, change control, communication ●●●●
- Project Management Tools: JIRA, Trello, MS Project, To Do ●●●●

### Infrastructure & Automation

- Virtualisation: VMware and Virtual Box ●●●○
- Scripting: Python, PowerShell for automation ●●●○