Thomas Boeglin

Cybersecurity Specialist

Personal Website
https://www.boeglin.xyz

Linkedin
thomas-boeglin

GitHub
thomasboegl1

Personal Informations

Email
**********@gmail.com

Phone
(+33) * ** ** ** **

Address
**********, France

Languages

French
C2 - Native

(Swiss) German
C1 - Fluent

English
C1 - Fluent (2019 TOEIC: 960pts)

Other

Birthday
** ***. **** (**)

Work permit
G - French nationality

Driving liscence
Cat B. (and personal car)

References

On demand

Hobbies

- Video Games
- Fitness
- Running & Hiking
- Home automation

Personal projects

soc-threat-report-tool - web app for SOC teams to generate monthly security reports with PDF export capabilities.

usbrubberducky-payloads - payload that captures screenshots from a Windows machine every 10 seconds and uploads them to a specified server using the Powershell.

More on GitHub.

About me

Currently part of the Cyber Defense Center at Baloise Group, I focus on protecting the organization against evolving cyber threats while continually building my expertise in the fast-changing IT landscape.

With a strong background in networks and telecommunications, I graduated top of my class from the M.Sc.Eng program at IMT Mines Alès, specializing in cybersecurity thanks to my apprenticeships. I bring hands-on experience across both IT and OT environments, and work closely with cross-functional teams to drive security initiatives.

I'm comfortable in agile environments, experienced in small-project management, and quick to adapt. I enjoy solving complex problems, designing practical solutions, and turning ideas into secure, working systems that benefits the business.

Experience

09/2022 - **Present** Basel, CH

Baloise Group

Cybersecurity Analyst

Subject Matter Expert (SME):
Incident Response
Threat Intelligence

Part of a 8-person, group wide, cyber defense team in the financial sector. Focus on incident response, security monitoring, vulnerability management and threat intelligence

- Co-developed the long-term cyber defense strategy and evaluated solutions to strengthen detection and response capabilities
- Built the internal Threat Intelligence service, enhancing C-level awareness.
- Investigated, contained, and eradicated security incidents, including on-call incident response coverage.
- Represented the team in front of C-level stakeholders, delivering strategic reporting.
- Delivered live-hacking awareness sessions to 100+ users (webinars and in-person)
- Automated key defensive workflows and developed Power BI dashboards for security reporting and KPI tracking

09/2019 - 09/2022 Mulhouse, FR

Eiffage Énergie Systèmes

Cybersecurity Engineer

Apprenticeship contract Cybersecurity team of 15 people. Specialized in aeronautics, space, national defense, transportation and energy sectors.

- Integrated security solutions into industrial systems
- Configured, implemented, and secured Linux servers (CentOS 7)
- Analyzed and provided security recommendations for Microsoft Active Directory environments
- Drafted technical documentation (security plans, test cases, user manuals)
- Evaluated and secured third-party equipment

09/2017 - 09/2019 Mulhouse, FR

Eiffage Énergie Systèmes

Network Technician

Apprenticeship contract in the Network infrastructure team for multiple clients. Worked on infrastructure projects for a range of clients, from SMEs to large industrial sites.

- Configured and installed Cisco network devices
- Performed LAN and Wi-Fi audits to assess and improve network performance
- Set up firewalls and OT (Operational Technology) end devices
- Diagnosed and resolved network issues across diverse environments

Education

IMT Mines Alès
École Mines-Télécom

IMT Mines Alès
Valedictorian - 2022

Master of Science in Engineering

(M.Sc.Eng) Computer Science and Network Engineering

Université de Haute-Alsace
2019

Associate degree

Networks & Telecommunications

Skills

Technical skills

- Incident handling
- **SIEM, SOAR**
- **EDR, NDR**
- Log analysis
- Power BI
- **Defender XDR**
- DevOps
- **Scripting**
- Linux
- Windows
- Cisco devices
- **Azure**
- **Docker**
- Terraform
- Awareness
- Automations

Soft skills

- **Creative**
- Initiative
- **Communication**
- Live Hacking
- Teamwork
- Adaptability
- **Problem-solving**
- Analytical thinking
- **Solution oriented**
- Time management

Certifications

Microsoft

Associate
SC-200 - Security Operations Analyst

Fundamentals
AZ-900 - Azure
SC-900 - Security

ISC2

C.C. - Certified in Cybersecurity

GitLab

GitLab Certified Associate

Stormshield

CSNA - Stormshield Network Administrator