WOMEN 4CYBER
EUROPEAN CYBER SECURITY ORGANISATION
GREECE

W4C GR CYBERSECURITY WOMAN PROFILE OF THE MONTH

INTERVIEW WITH KONSTANTIA!

Name: Konstantia Barmpatsalou
Job Position: Blue Team Support Manager [Head of Detection Engineering and Threat Intelligence]
Current Employer: Obrela Security Industries
Cybersecurity areas of expertise: Detection Engineering, Threat Intelligence, DFIR
Previous career(s): SecDevOps Engineer, Cybersecurity Research Associate
Educational background: PhD in Applied Neural Networks for Mobile Forensic Data, MSc in Information Systems Security, MSc in Information Systems Management, BSc in Information and Communication Systems Engineering
Other interests/hobbies: Writing, Crafting, Running
Favourite quote: "Freedom without structure becomes chaos. Structure without care becomes rebellion." Leadership isn't about control—it's about designing systems that empower. Build trust, set clear boundaries, and lead with both precision and purpose.
Network with me: https://www.linkedin.com/in/konstantia-barmpatsalou-83ba1a25/
Are you hiring?: Yes, check out Obrela Security Industries' LinkedIn page for vacancies

Intro & Inspirational

1. Which values are guiding your life and work?

Respect, order, dedication, creativity and freedom. When someone possess the first three, then the last two can grow to their best extent.

2. What's the most important life lesson you've learned?

It may sound cliché, but nothing can be achieved without health and both physical and mental well-being. These two are the baseline and prerequisite for every other path followed.

3. How do you define success? And what's the best advice that you can give about success?

Success is highly subjective and based on each individual's own goals and aspirations. It may fluctuate overtime as well. The best advice? A successful path without hard work is just like a building without foundations. Pretty easy to collapse.

4. Do you think your job makes a difference? How?

Each job contributes with the same weight in the chain. Every position is crucial and without it, the gap left behind is unaddressed.

5. What is the best and the worst piece of advice you received? (+How did you unlearn the latter or use it to your favour?)

Best: Never give up, even when odds are not in your favor.

Worst: You have to conform to specific norms and personality traits if you want to succeed.

Unlearn? Just never conformed with it. Success while losing half of yourself is also halved.

6. Can you name a book that has influenced your journey?

I do not have a specific one, and honestly, my journey is a patchwork of "hands-on" and motivational experiences.

Cybersecurity General

7. How can someone stand out in a competitive cybersecurity job market?

Expertise and hard work. Once someone has mastered their domain in the best potential extent, then competitivity is nothing to worry about.

8. What trends in the technology & cybersecurity industry are you keeping an eye on for the future?

How deep learning models will influence different cybersecurity domains. While I find them useful and efficient, their feeding still depends and will up until a certain point depend on human expertise, and, as such, we need intelligent people in order to keep sustaining intelligent systems.

9. What is the most common mistake someone could make when applying for a role in the cybersecurity industry? What do you believe makes a successful candidate/application?

Over- or under- estimating their potential, and having only an ambition-based mentality, without doing their own reflective SWOT analysis beforehand. A successful candidate is not one who is aware about everything, but the one who is willing to learn and adapt.

10. Do you believe that there are misconceptions people make about working in the cybersecurity industry?

There are several misconceptions about working in cybersecurity. One of the most common is that it's all about hacking in the Hollywood sense — people in hoodies breaking into systems. In reality, most of the work is focused on defense: monitoring, detection engineering, threat intelligence, and aligning with business risks. People also tend to think the tools will do all the work for you, but in practice tools are only as good as the rules and the human judgment behind them. A lot of the job is about critical thinking, tuning, and collaboration across teams.

11. Which concrete recommendations would you give to women who want to change career and join cybersecurity?
Study a lot, acquire context, find the field that you are mostly interested in and assess how your skills can support it.
12. And any tips for those who are still very young and might be considering it? Can they start "preparing" somehow from early on?
If you're young and considering cybersecurity, start exploring early but don't overthink it — try out different areas, build digital literacy, and stay curious. Even simple things like CTFs, safe lab experiments, or following threat reports help you see what excites you. The mindset matters more than being technical right away
13. What skills do you think are not "most important", as this is very limiting, but skills that are key for a career in cybersecurity no matter the specific profile?
Problem-solving mentality, even for less technical roles
Analytical breakdown skills
Capability to prioritize needs and requirements
14.Do you (or did you) have a mentor or someone who guided you? What is your opinion on mentoring as well as on getting a start via an internship/traineeship? Are you planning to mentor or coach others in the future, or have you been mentoring already?
I did not have a mentor per se, but there were many people who played their part in influencing my career choices (university advisors, colleagues, industry role models). Some people though, might be more in need of a specific mentor, so I would like to coach them if it is helpful for them; even though I would still promote diversity in role models.

You & Your job

15. What was your childhood dream job (and why you liked it)?
Criminal Investigator. It is all about problem solving and profiling, multidisciplinary, requires a strong know how, but is also intuitive.
16. Did peer pressure, trends or other factors play a role in your choosing cybersecurity and particularly your specific field of work in it?
No, not really, it was the most interesting career out of the available options after graduating from Computer Engineering.
17. Did you face any challenges related to your gender, race, visual appearance, or background, or any stereotypical biases? How have you overcome these?
Even though we want to eradicate them, who hasn't? A competitive environment sometimes makes such behaviours thrive, and this is something that is not 100% controllable for the time being. The point is to keep doing what you know best, encourage diversity, focus in the result of the job done and not in one's traits, and such biases will become extinguished over time. Not by neglecting them, but by proving them wrong.
18. Do (did) you ever experience imposter syndrome and self-doubt about your career and skills?
Of course — in cybersecurity, if you've never felt imposter syndrome, you're probably an imposter. I just take it as proof I'm in the right field. Jokes aside, self-doubt is normal in a field that moves this fast. The important part is not letting it stop you — every new challenge is a chance to grow, and that's what makes the work meaningful.
19. What has been your most exciting role to date?
While each role had its perks, I think that the current one is the most exciting to date. I get to provide guidance and practice leadership in two fields that I am excited about; Detection Engineering and Threat Intelligence. Planning, designing and seeing your team grow to their best potential is the biggest reward you can get.

20. What is the best and worst experience you have had in your career?

To be honest, I do not want to specify, because they would rather be isolated comments, and far from leading anyone to an objective conclusion. Both good and bad experiences shape you into who you are today.

21. Do you enjoy your work, and why? What's your favourite and least favourite part of your job?

I really enjoy my work — cybersecurity is challenging, fast-moving, and it never feels boring. My favorite part is the problem-solving: building detections, connecting the dots in threat intelligence, and knowing that the work actually protects people and businesses. If I had to pick a least favorite part, I'd say the noise — endless false positives, vendor hype, and sometimes the bureaucracy around security can be frustrating. But in the end, even those challenges push me to refine processes and find better ways to work.

22. What role has networking played in your skill development?

It is still important but cannot act standalone. Still, it has played a significant part. Cybersecurity is too broad to learn everything on your own, so having peers to exchange ideas, share resources, or even just compare experiences has been invaluable. After all, HUMINT should never be underappreciated.

23. What's the next big milestone you're working towards (if you can and want to share)?

The next milestones are set everyday in the field of work. As such, I can't really and I don't want predefine anything but rather excel in my domain.

24. Do you have any passion or side-projects you´re focusing on?

Yes, but not cybersecurity! I am passionate about writing. I have published my first book of a dystopic sci-fi sequel, and I am preparing the second part.

Other

25. How do you handle criticism?

While not a big fan of the specific word and what it implies, I try to take criticism as an opportunity to learn. In cybersecurity, you can't know everything and mistakes do happen, so feedback is part of the process. I'm trying to focus on what I can improve — and sometimes even push back constructively if I think there's another angle.

26. How do you manage stress?

Meditation, running, humour and proactiveness.

27. Cybersecurity is considered a very demanding and "intrusive" career in someone's life (takes a lot of hours, lots of learning constantly, you are "seeing" cybersecurity triggers everywhere even outside of work). How do you balance work and personal life?

Cybersecurity can be very demanding and it has a way of following you outside of work — once you see risks, you can't unsee them. For me, balance comes from setting small boundaries, like making time to switch off from screens or focus on things completely unrelated to tech. It's not always perfect, but I've found even small routines help keep me grounded while still staying passionate about the field

28. What do you do to prevent burnout in such a demanding line of work?

Just by learning to listen to my body and brain by not pushing more from what I can sustain.

29. How do you set boundaries in the workplace?

It's about clarity and respect — I stick to my role, I'm open to collaboration, but I also make sure expectations are realistic so I can give my best.