WOMEN 4CYBER
EUROPEAN CYBER SECURITY ORGANISATION
GREECE

W4C GR CYBERSECURITY WOMAN PROFILE OF THE MONTH

INTERVIEW WITH ASIMINA!

Name: Asimina Basdani
Job Position: Chief Information Security Officer (CISO)
Current Employer: I.DI.K.A. SINGLE MEMBER S.A.
Cybersecurity areas of expertise: Cybersecurity Strategy, Lead Incident Response, Risk Management
Previous career: Informatics Lecturer
Educational background: MSc in Intelligent Systems & Computer Architecture, MSc Informatics & Management, BSc Industrial Informatics
Other interests/hobbies (if you want to share): Reading, Volleyball, Tennis
Favourite quote: “It’s not what happens to you, but how you react to it that matters.”
Network with me: https://gr.linkedin.com/in/asimina-basdani

Intro & Inspirational

1. Which values are guiding your life and work?

The values that guide my life and work are integrity, passion, and authenticity. I believe in approaching everything I do with purpose and commitment, striving each day to grow personally and professionally, while ensuring that my work creates genuine value and a meaningful impact.

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

Nothing truly meaningful is built without patience and consistency. Growth is the result of small, steady steps, even when the outcome is not immediately visible. I have also learned to view mistakes as valuable lessons rather than failures.

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

For me, success means living and working in alignment with your values, continuously growing, while maintaining your balance. The best advice I can give is, don't compare your journey to others. Invest in your own progress with consistency, authenticity, and perseverance.

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

Yes, absolutely. By strengthening cybersecurity frameworks and resilience, my team and I contribute to protecting critical infrastructure, ensuring data integrity, and supporting the continuity of digital services that healthcare professionals, social security officials, and citizens rely on every day.

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?)

The best advice I received was, "Make the impossible possible".

The worst advice was, "Always play it safe". I unlearned this by realizing that meaningful growth comes from taking calculated risks..

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

One book that has influenced me greatly is "The Alchemist" by Paulo Coelho, for its message about pursuing your dreams and learning from every step of the journey.

Cybersecurity General

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

To stand out in a highly competitive cybersecurity job market, it is essential to combine strong cybersecurity and technical knowledge with professional experience. At the same time, a commitment to lifelong learning and staying up to date with technological developments are key factors for long-term success in the field.

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

One of the key trends I am keeping an eye on is quantum cryptography and the broader impact of quantum computing on cybersecurity. As quantum technologies evolve, they are expected to challenge many of today's cryptographic standards. This is driving the need for quantum-resistant cryptography and long-term security planning, so organizations can protect sensitive data against future threats.

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?

One of the most common mistakes is submitting a generic application that does not clearly align with the specific role. Cybersecurity is a broad field, and employers look for candidates who understand the requirements of the position and can demonstrate relevant skills or experience. A successful application clearly connects technical knowledge with practical experience, shows curiosity and willingness to learn, and demonstrates an understanding of how cybersecurity supports business objectives, not just technology.

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

A common misconception about working in cybersecurity is that it is limited to technical tasks such as monitoring systems or responding to cyberattacks. In reality, it is a multidisciplinary field that includes risk management, strategy, governance, collaboration across teams, and building a strong security culture to proactively protect information and ensure organizational resilience.

11. Which concrete recommendations would you give to women who want to change career and join cybersecurity?

The advice I would give to women who want to change career and join cybersecurity is not to be discouraged at the beginning. At first, everything may seem overwhelming and difficult to understand, but this is completely normal. With time, hands-on experience, and continuous learning, concepts become clearer and confidence grows. I would also encourage women to ask questions, seek support from colleagues or mentors, and trust in their ability to succeed. Cybersecurity is a field that values curiosity, persistence, and collaboration, not perfection from day one.

12. And any tips for those who are still very young and might be considering it? Can they start "preparing" somehow from early on?

There are many tips I could give to young people who are considering a career in cybersecurity. One of the most important is to develop hobbies related to technology, such as robotics, or programming, as these help build problem-solving skills and a logical way of thinking. They can also start learning basic concepts around computers, networks, and security through online platforms and hands-on experimentation. Just as importantly, developing curiosity, critical thinking, and an ethical mindset from an early age can lay a strong foundation for a future career in cybersecurity. Preparation does not have to be formal at the beginning, passion and consistency make a real difference over time.

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?

I don't believe there is a single "most important" skill in cybersecurity, as that can be limiting. While programming skills can be useful depending on the role, they are not essential for every cybersecurity profile. Across the field, key skills include strong communication, analytical thinking, and effective problem-solving. Being able to analyze situations, understand risk, and clearly communicate findings to both technical and non-technical stakeholders is critical in almost every cybersecurity role.

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?

Throughout my career, I have been fortunate to learn from many colleagues I have collaborated and communicated with, each of whom acted as a mentor in different ways. Every interaction offered an opportunity to gain new perspectives, knowledge, and practical insights. I consider myself especially lucky in my career, and particularly at I.DI.K.A., where I have the opportunity to work with highly skilled professionals who possess strong technical expertise in cybersecurity and a collaborative mindset.

I strongly believe in the value of mentoring, as well as in internships and traineeships, as they provide an excellent starting point for gaining real-world experience and guidance. Learning from others has played a key role in my professional development, and I would be more than happy to mentor or support others in the future, contributing back to the cybersecurity community.

You & Your job

15. What was your childhood dream job (and why you liked it)?

My childhood dream was to pursue a career in technology. I was drawn to the rapid pace of technological innovation and its ability to positively impact society. Technology has the potential to improve communication, simplify everyday work, and create new opportunities across critical sectors such as healthcare and medicine. From an early age, I was motivated by the idea of contributing to solutions that make people's lives easier and more efficient through technology.

16. Did peer pressure, trends or other factors play a role in your choosing cybersecurity and particularly your specific field of work in it?

My decision to pursue a career in cybersecurity was partly influenced by global trends, as it has become one of the most dynamic and critical fields worldwide. However, the defining factor was my professional experience at I.DI.K.A. Working initially as a Network Security Engineer and later assuming the role of CISO allowed me to fully understand the vital role of cybersecurity in protecting national critical infrastructures. This experience strengthened my commitment to the field and motivated me to continuously deepen my expertise and advance professionally in cybersecurity.

17. Did you face any challenges related to your gender, race, visual appearance, or background, or any stereotypical biases? How have you overcome these?

Cybersecurity is a traditionally male-dominated field and women often face initial skepticism. I experienced this early in my career, but I overcame it through continuous learning, professionalism and proven results. Today, the environment is gradually improving with organizations, such as Women4Cyber Greece, actively supporting and empowering women, helping to create a more equitable cybersecurity community.

18. Do (did) you ever experience imposter syndrome and self-doubt about your career and skills?

Yes, absolutely. I have experienced this on several occasions, particularly during periods of intense pressure, tight deadlines, and increased responsibilities. However, I strongly believe that continuous education and hands-on experience are keys to overcoming these feelings. As you grow professionally and see the impact of your work, your confidence naturally increases.

19. What has been your most exciting role to date?
The most exciting role I have held to date is that of CISO. It is a highly dynamic position with multidimensional challenges, requiring a constant balance between cybersecurity strategy, governance, regulatory compliance, and operational security. From defining the organization's overall cybersecurity strategy to leading the response and investigation of security incidents, every day is different and demands quick decision-making, accountability, and strong teamwork.
20. What is the best and worst experience you have had in your career?
In cybersecurity, it is difficult to clearly separate experiences into "best" and "worst." Every day brings new challenges. Often, the most demanding situations become the most valuable experiences. Handling a serious security incident, while highly stressful, is also a unique opportunity to improve processes, strengthen teams, and enhance organizational resilience. In this field, even the most difficult experiences are ultimately transformed into valuable knowledge and professional growth.
21. Do you enjoy your work, and why? What's your favourite and least favourite part of your job?
I truly enjoy my work! My favourite part of the role is staying up to date with technology developments and designing strategies. The least enjoyable aspect is when there is a lack of effective communication, which can sometimes delay decision-making and the resolution of security issues.
22. What role has networking played in your skill development?
Networking has played a crucial role in my professional development and skill enhancement. Through networking, I am able to exchange experiences, discuss real-world incidents, and view challenges from different perspectives.
23. What's the next big milestone you're working towards?
At this stage, I'm not able to share details about my next milestone.
24. Do you have any passion or side-projects you´re focusing on?
One of my side projects is scientific research in cybersecurity, focused on developing and testing AI models, aiming to enhance security and strengthen organizational resilience.

Other

25. How do you handle criticism?
I welcome constructive criticism aimed at professional growth. When feedback is clear and respectful, I see it as a valuable opportunity to improve myself.
26. How do you manage stress?
I manage stress primarily through organization and prioritization. In my work, pressure is often unavoidable, especially during critical situations, but having clear processes and a well-prepared team helps me stay focused and in control.
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?
I consciously try to separate my personal time from cybersecurity activities. Outside of work, I focus on different interests that help me disconnect from constant learning, analysis, and planning. This balance allows me to recharge mentally and return to work with renewed focus and energy.
28. What do you do to prevent burnout in such a demanding line of work?
To prevent burnout in such a demanding field, I take breaks when needed and engage in physical activities.
29. How do you set boundaries in the workplace?
I believe the key to setting boundaries is clear communication and realistic expectations within the team.