WOMEN 4CYBER
EUROPEAN CYBER SECURITY ORGANISATION
GREECE

# W4C GR CYBERSECURITY WOMAN PROFILE OF THE MONTH

**INTERVIEW WITH KATERINA!**

**Name: Katerina Tasiopoulou**
**Job Position:** CEO
**Current Employer:** ThreatScene
**Educational background:** BSc in Computer Science, MBA in Senior Leadership

# Intro & Inspirational

***1.Which values are guiding your life and work?***

I have always believed that integrity, resilience, and responsibility should be at the core of everything we do. In cybersecurity, trust is not a slogan but a daily commitment. Leading ThreatScene, I feel a deep responsibility to our clients, to our people, and to the broader ecosystem we serve.

Another value that guides me is resilience. Cybersecurity is a field where challenges are constant, and what truly matters is how quickly you can adapt, recover, and help others do the same. This applies both at a professional and a personal level.

Finally, I place great importance on empowerment. Building ThreatScene has taught me that real impact comes when you create an environment where teams feel supported, respected, and free to innovate. I want to empower not only my colleagues but also the next generation of women in cybersecurity to believe that they can shape this field with confidence.

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

The most important lesson I have learned is that fairness should always come first. Whether in leadership, decision-making, or daily life, choosing what is fair creates trust, builds credibility, and sets the foundation for long-term success. Even in moments when it might seem easier to compromise or take a shortcut, I have seen that fairness always wins in the end.

In my role as a CEO, this principle is non-negotiable. Respecting people, valuing their contributions, and making balanced decisions not only strengthens the organisation but also ensures that everyone feels they are part of something just and meaningful. Cybersecurity is a high-pressure environment, but fairness is what keeps both teams and partnerships resilient.

***3.Do you think your job makes a difference? How?***

*I truly believe my job makes a difference. Cybersecurity is no longer a technical afterthought but a cornerstone of a country's progress and resilience. Every time our team prevents an incident from escalating or helps an organisation recover from disruption, we are not just protecting systems — we are safeguarding jobs, continuity, and trust. That impact is very real.*

*At the same time, being the first woman leading a cybersecurity company in Greece carries its own responsibility. Representation matters. I want my journey to show other women that they can take leadership roles in this field and redefine what the industry looks like. If my work helps open that door wider, then I know it is making a difference not only for businesses but also for the next generation of women in cybersecurity.*

# Cybersecurity General

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

*Two areas stand out to me: the evolution of artificial intelligence and the enforcement of new regulations such as NIS2. AI is transforming cybersecurity on both sides of the spectrum. It empowers defenders with faster detection, analysis, and response, but it also equips attackers with new tools for automation, deepfakes, and large-scale social engineering. The challenge is to stay ahead of that curve while using AI responsibly.*

*At the same time, frameworks like NIS2 and DORA are reshaping how organisations must approach security. Compliance is no longer a box-ticking exercise — it is directly tied to resilience, accountability, and leadership responsibility.*

*Finally, I believe the maritime and critical infrastructure sectors deserve particular attention. The increasing connectivity of ships, ports, and energy systems makes them highly attractive targets. The future of cybersecurity will be measured not only by how well we defend corporate networks but also by how we protect the backbone of our economies and societies.*

***5.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 I see is that candidates often play it too safe. They present themselves in a very standard way, repeating what they think an employer wants to hear instead of showing how they think differently. Cybersecurity is a field that thrives on creativity and problem-solving. Attackers are always innovating, so defenders need to think out of the box as well.*

*A successful candidate is not necessarily the one who has memorised every framework or earned the longest list of certifications, but the one who demonstrates curiosity, adaptability, and the ability to approach problems from unexpected angles. I value people who show initiative, bring original perspectives, and are willing to keep learning. That mindset is what makes a real difference in this industry.*

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

*Absolutely. One of the biggest misconceptions is that cybersecurity is purely a technical profession. While technical expertise is important, the reality is that our field is much broader. Cybersecurity requires strategy, communication, risk management, governance, legal understanding, and above all, teamwork.*

*Many successful professionals in this industry come from diverse backgrounds — law, business, marketing, psychology, even the maritime sector. What matters most is the ability to understand risk, think critically, and connect the dots between technology and people. By seeing cybersecurity only as a technical path, we lose talented individuals who could bring valuable skills and perspectives to the table.*

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

*Young people today are in a very fortunate position because they can start their cybersecurity journey much earlier than previous generations. If you begin exploring the field at a young age, you gain years of practice and experience that can later set you apart in your career. I have seen many professionals distinguish themselves in their companies simply because they started early and built a strong foundation.*

*The best way to prepare is to combine curiosity with structure. Explore freely, experiment with tools, join communities, but also invest in recognised certifications. Even entry-level certifications provide credibility and give you a framework to build on. By the time you enter the job market, you will not only have knowledge but also the confidence that you belong in this industry.*

***8.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?***

*In cybersecurity, there is no single “most important” skill, but there are a few that I believe are fundamental across every role. The first is curiosity — the willingness to ask questions, dig deeper, and not accept things at face value. This mindset often reveals vulnerabilities or solutions that others might overlook.*

*Second, adaptability is essential. The threat landscape changes constantly, so the ability to learn quickly, adjust, and apply new knowledge is what keeps a professional relevant.*

*Finally, communication is often underestimated but absolutely critical. Whether you are a technical analyst, a consultant, or a leader, you need to explain risks and solutions in a way that others can understand and act upon. Cybersecurity is not only about technology — it is about people, processes, and trust. The ability to bridge those areas through clear communication is what makes a professional truly effective.*

# You & Your job

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

*Since I was very young, I dreamed of becoming a CEO. One of my first memories was learning to say the words "chief executive officer" and proudly telling everyone that I would become one — even though I had no idea what it actually meant. And once I discovered what it meant, I wanted it even more.*

*The idea of leading, creating, and building something meaningful has always fascinated me. I was drawn to the thought of turning ideas into reality, inspiring people, and shaping a vision that could make an impact. Looking back now, it feels like that childhood ambition quietly guided every step of my journey — and today, it has become both my career and my purpose.*

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

*Yes, especially in the early years of my career, I was often the only woman in the room. In many meetings or industry events, the default expectation was that cybersecurity was a men's domain, and I had to face the stereotypes that came with that.*

*The way I chose to overcome this was through knowledge. I made sure that whenever I spoke, I spoke with depth and confidence. Preparation, expertise, and the ability to bring clear insights into the discussion gradually changed perceptions. Over time, people stopped seeing me as "the only woman in the room" and started recognising me for my contribution and leadership.*

*While it was not always easy, I believe these experiences strengthened me. They also remind me why representation is so important — so that future women in cybersecurity don't have to prove themselves twice before being taken seriously.*

***11.What has been your most exciting role to date?***

*Without question, my current role as CEO of ThreatScene has been the most exciting and fulfilling chapter of my career. Leading a company is not only about strategy and business growth — it is about shaping a vision, building teams, and setting a culture that can truly make an impact.*

*What excites me most is seeing how our work directly strengthens organisations and, in some cases, even entire sectors. From incident response that saves companies from major disruption to pioneering frameworks that raise the standard of maritime cybersecurity, every day brings the opportunity to contribute to something larger than myself.*

*At the same time, being a CEO gives me the privilege to mentor, to empower others, and to demonstrate that women can lead at the highest levels of this industry. It is both a professional challenge and a personal mission, and that combination makes it incredibly rewarding.*

***12.What role has networking played in your skill development?***

*Networking has been absolutely crucial in my journey. I see it as building an extended team of people that you can turn to for help, insights, feedback, or simply a fresh perspective. No one in cybersecurity can know everything — the field is too broad and too fast-moving. Having a strong network means you never face challenges alone.*

*Through networking, I have gained knowledge, discovered opportunities, and learned from the experiences of others. It has also allowed me to share my own lessons and support people who are earlier in their careers. In many ways, networking is not just about professional growth — it is about creating a community that makes all of us stronger.*

***13.What's the next big milestone you're working towards?***

*My next big milestone is to establish our two elite units — Unit 13 and Unit 31 — as the leading offensive and defensive cybersecurity teams in Greece, and to expand their presence across Europe and the Middle East. They represent the heart of ThreatScene's expertise, and my goal is to ensure they set the standard for precision, resilience, and excellence well beyond our borders.*

*At the same time, I am deeply committed to advancing cybersecurity in the maritime sector. With our Marine Cybersecurity Framework, we have already taken steps to raise the level of protection for shipping companies, ports, and critical maritime operations. My vision is for ThreatScene to become the top firm in maritime cybersecurity, shaping a safer future for an industry that is vital not only to Greece but to the global economy.*

**14.Do you have any passion or side-projects you´re focusing on?**
Outside of cybersecurity, one of my passions is music. I am currently working towards a diploma in Byzantine music, which has been a personal dream of mine for many years. For me, music is not only a creative outlet but also a source of balance and reflection.

Studying Byzantine music requires patience, discipline, and attention to detail — qualities that I also find invaluable in my professional life. It reminds me that growth can happen in many different areas, and that pursuing a passion outside of work can enrich both your personal and professional journey.

## Other

**15.How do you manage stress?**
For me, managing stress is about maintaining mental balance. Cybersecurity is a demanding field where unexpected challenges can arise at any moment, so staying centred is essential. I try to approach each situation calmly, focusing on clarity and perspective rather than letting pressure take over.

I also believe in small but consistent habits that support balance — taking breaks when needed, setting boundaries to protect focus, and keeping time for personal interests outside of work. These practices help me reset and ensure that I can lead with a clear mind, even in high-pressure environments.

**16.What do you do to prevent burnout in such a demanding line of work?**
Preventing burnout, for me, begins with work-life balance. I make it a priority to arrange free time outside of work and protect it as much as possible. It’s not always easy, but I’ve learned that dedicating time to myself is just as important as dedicating time to the company.

Another important practice is scheduling. I organise my daily tasks carefully — not only work responsibilities, but also time for hobbies or activities I enjoy. By putting them on my calendar, I ensure they are not overlooked, and I give myself the chance to recharge.

Finally, there are moments when the best thing you can do is to make a hard stop. Disconnecting completely, even briefly, allows me to clear my mind from constant demands and return with renewed energy and perspective. In a field as consuming as cybersecurity, this discipline is essential.