SANS | GIAC CERTIFICATIONS

CASE STUDY

Closing The Gap:

How Early, Targeted Training Reshaped One Cybersecurity Engineer's Career

With Marta Xavier, Cyber Security Analyst

She had learned the theory at university. Her first job showed her exactly what that theory had not prepared her for. For one young cybersecurity engineer, structured, hands-on training closed the gap, fast.

Marta Xavier was two months into her first job when the gap hit her. She had a master's degree in cybersecurity, but the work in front of her looked nothing like her studies. University had given her theory and controlled problem sets. Her job gave her live incidents: compromised systems, intrusions in progress, and organisations in crisis. The analytical foundation was there. The operational knowledge was not.

> *"In university it was all Linux-based. But when you come into the real world, virtually every company's infrastructure runs on Windows."*

The incidents that mattered most all pointed to the same blind spot. "*In university it was all Linux-based*," she says. "*But when you come into the real world, virtually every company's infrastructure runs on Windows.*" She had been trained for one environment and was now working in another. Her employer made it clear from day one, that the fastest way to bridge that gap was through structured, practical training.

Her employer recommended SANS, starting with FOR508: Advanced Incident Response, Threat Hunting and Digital Forensics. Within a week of completing the course, incidents that had previously been out of reach were within her grasp. She knew which forensic artefacts to collect from a compromised system, how to analyse them, and how to translate her findings into guidance the affected organisation could act on.

A New Course for Every Challenge

Stronger investigations brought a new challenge. As Marta moved into larger and more complex cases, expanding from individual machines to entire organisational infrastructures, the organisations she helped began asking a harder question once the forensic report had been delivered: what's next? "*An intrusion is never the result of a single mistake*," Marta says. "*It is misconfigurations and bad practices across the entire infrastructure, and those organisations needed concrete guidance on how to rebuild, right down to specific network configurations and architectural decisions.*"

That led her to SEC530, Defensible Security Architecture and Engineering, a course covering infrastructure security from the ground up, from the configuration of switches and routers through to architectural decisions at the application layer. Where FOR508 had taught her to investigate, SEC530 taught her to advise. "*You can go really deep into this layered approach*," Marta says. "*For every layer of an infrastructure, you can give concrete security measures and configurations, and then move up to the next.*" It became her favourite course, and the most content-rich training she had undertaken.

The next challenge was one of scale. The sheer volume of threat intelligence crossing her desk, from paid and free feeds, incident reports, and information-sharing platforms such as MISP, each with its own structure and taxonomy, was becoming an operational problem in its own right. "*We had all this data from completely different sources, and we had to find a way to standardise it and generate actionable intelligence,*" Marta says. "*That is what led me to SEC595, Applied Data Science and Machine Learning for Cybersecurity Professionals.*"

Gotta Catch 'Em All

Marta had taken three courses, each in direct response to a problem she had encountered in her work. Her wishlist for what comes next is, she laughs, considerably longer. "*It's a bit like Pokémon,*" she says. "*I want to collect them all.*" She has spent two years building her knowledge of defensive security, but one question keeps pulling at her. "*I know the blue team side, the defensive architecture side*," she says. "*But how does an attacker actually think? I have not explored that enough yet, and I think understanding that will make me a much better defender.*" That is what makes SEC599, which focuses on purple team tactics and adversary emulation, the logical next step.

Marta also has her eye on SANS's applied knowledge certifications, a more advanced track where candidates must use tools in realistic laboratory environments rather than simply answer questions about them. She has not attempted one yet, but the appeal is obvious. "*You have to apply all the tools, hands-on*," she says. "*That is my next challenge.*"

> *"If I hadn't done the certifications, the knowledge would have been good, but it would not have stuck the same way. I forced myself to go through every page of the material, to study every evening after work."*

Certification as Knowledge Proof

Each of Marta's SANS courses gave her the opportunity to earn a GIAC certification through a separate, rigorous exam that tests whether she had genuinely mastered the material. For Marta, preparing for those exams turned knowledge into lasting capability. "*If I hadn't done the certifications, the knowledge would have been good, but it would not have stuck the same way,*" she says. "*I forced myself to go through every page of the material, to study every evening after work. That is what allowed me to truly internalise it.*"

The certifications also carry weight in her day-to-day work. Marta regularly advises professionals with decades more experience than she has, often in high-pressure incidents when systems have already been severely compromised. "*Even though I am young, my certifications demonstrate that I have the expertise to back up what I am saying,*" Marta says. "*When you are advising experienced professionals under pressure, that credibility matters.*"

> *"We are all young, super open-minded, but through SANS we have built up knowledge that you would normally only accumulate after ten years in the field."*

Dedication Goes Both Ways

"*None of us would be where we are without our employer investing in us,*" Marta says. "*They encourage us to develop, they give us the opportunities, and we give that dedication back. It goes both ways.*" She is not just talking about herself. Her wider team is young, she explains, and that is part of what makes it work. "*We are all young, super open-minded, but through SANS we have built up knowledge that you would normally only accumulate after ten years in the field,*" she says. "*We have the experience, but we still have the fresh perspective and motivation of people who just came out of college. It is really the best of both worlds.*"

> *"I want to keep contributing to my organisation's mission, to see the impact of our work and to keep growing, both professionally and personally."*

For Marta, that combination is what keeps her exactly where she wants to be. "*I want to keep contributing to my organisation's mission, to see the impact of our work and to keep growing, both professionally and personally,*" she says. "*Opportunities like SANS are what allow me to do that better every day. This is the right place for me.*"

Marta's SANS Training Path

FOR508: Advanced Incident Response, Threat Hunting, and Digital Forensics | GCFA

SEC530: Defensible Security Architecture and Engineering | GDSA

SEC595: Applied Data Science and AI/Machine Learning for Cybersecurity Professionals | GMLE

SEC599: Defeating Advanced Adversaries - Purple Team Tactics & Kill Chain Defenses | GDAT

SANS | GIAC CERTIFICATIONS