

The Careers, Lessons, and Stories Shaping Cyber Threat Intelligence

Sixteen conversations on finding their way into cyber threat intelligence, the work that keeps them there, and the people who helped along the way.

Contents

Introduction	3	CHAPTER 6	The Moment that Changed Everything	35
CHAPTER 1		CHAPTER 7		
Curiosity Is the Only Prerequisite	5	Busting the Myths	40	
CHAPTER 2				
Someone Took a Chance on Me	11	What People Get Wrong	46	
Beyond CTI	17	CHAPTER 8	Why We Stay	47
CHAPTER 3		CHAPTER 9		
Earning the Room	18	Lifting As We Climb	52	
CHAPTER 4				
The Human in the Loop	23	Conclusion	57	
Using AI in CTI	28	Contributors	58	
CHAPTER 5				
Staying Sharp	29	Resources	59	
Breaking into CTI	34			

INTRODUCTION

There are many ways to get into cyber threat intelligence.

For some of the women in this eBook, it was an obvious career choice. For others, it wasn't even on the radar. They came into Cyber Threat Intelligence (CTI) following very different paths: from intelligence, the military, political science, marketing, game development, engineering, recruitment, theatre, and ten years at home raising children.

Between them, they've built threat intelligence functions from scratch, tracked a Russian influence operation across a decade of Olympic Games, and shown that attackers can be spotted months before they build their infrastructure.

There isn't a single way into CTI, and there isn't a single kind of person who belongs here.

There are at least sixteen ways it can happen.

Our conversations with these sixteen professionals went well beyond career paths. We talked about building trust, keeping up with a field where uncertainty is certain, where AI fits into the work, the investigations they still think about years later, and some of the misconceptions that come with working in cybersecurity.

We also heard a lot about **community** and **camaraderie**.

Managers who hired for potential. Mentors who made time. Friends who made introductions or simply gave someone the confidence to try.

That **generosity** runs through many of these stories. The women featured here have benefited from it, and they're passing it on.

For women considering a career in CTI, their stories show just how many ways there are to get started, build experience, and find where they fit.

We hope you'll enjoy getting to know each of these Women in CTI.

WHAT WE CONTRIBUTE TO THE BROADER CTI COMMUNITY IS THE BIGGER PURPOSE.

Einat Argon and I co-founded Women in CTI from something simple. In the intelligence-sharing Slack channels we were part of, very few women were contributing. We knew women were doing incredible work in this field, but their knowledge wasn't showing up where intelligence was being exchanged.

Intelligence only becomes valuable when it is shared and acted upon. If voices are missing from that exchange, **all of us are working with an incomplete picture.**

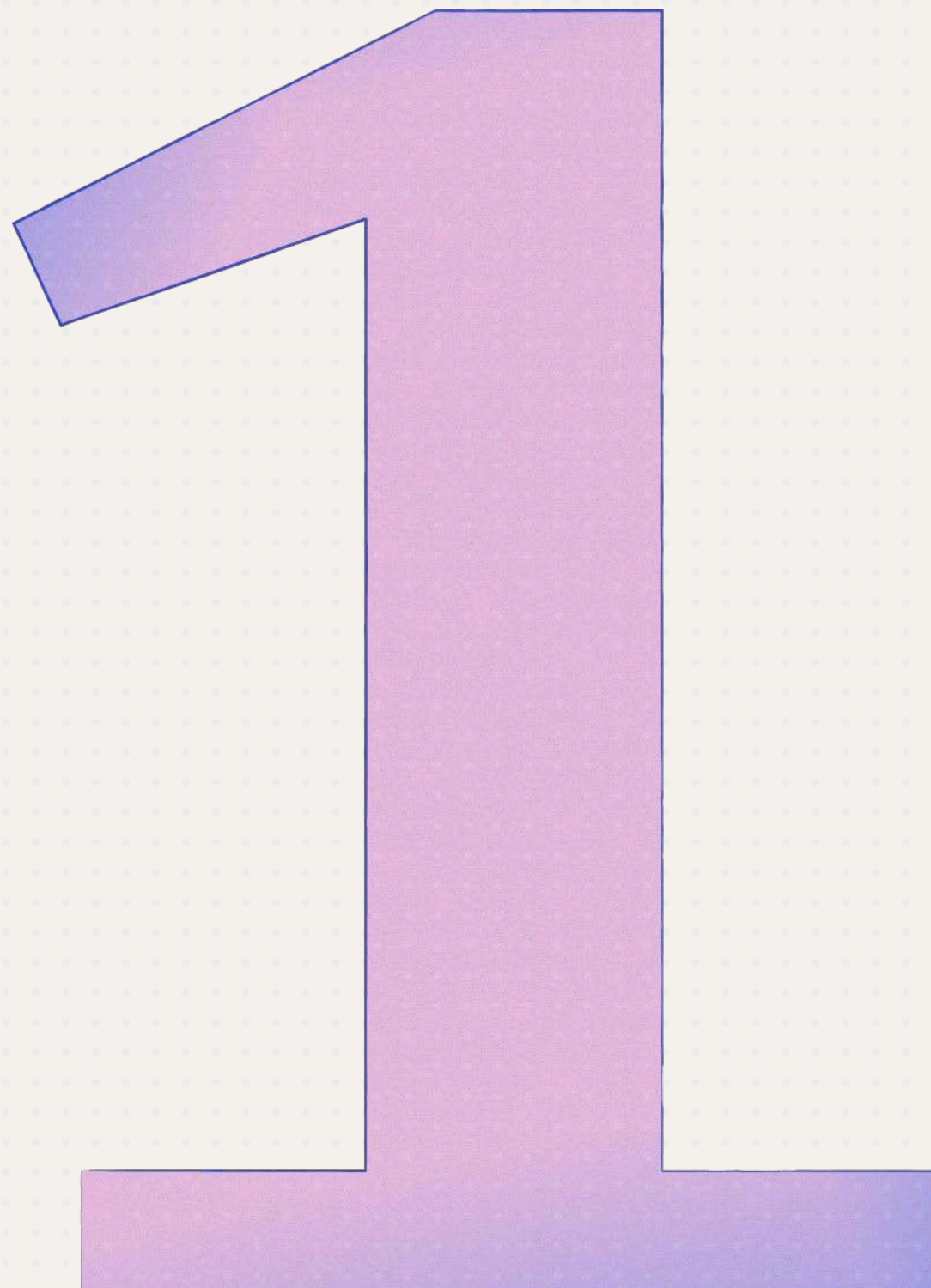
So Women in CTI is about building a real community where women feel comfortable contributing, asking questions, and taking up space, and where **the next woman entering this field doesn't have to figure everything out alone.**

We haven't done it alone either. Lara Meadows of Dataminr has been an enabling partner from the beginning and we're grateful for it.

Being women may be what connects us. **What we contribute to the broader CTI community is the bigger purpose.**

Mary D'Angelo

CO-FOUNDER, WOMEN IN CTI
– SENIOR SOLUTIONS LEAD, FILIGRAN



Curiosity Is The Only Prerequisite

Ask people working in cyber threat intelligence how they got there, and you won't hear the same story twice. Some started in computer science. Others came from marketing, counterterrorism, consulting, or the military.

What these stories share is curiosity, a willingness to learn, and the confidence to take an opportunity without knowing everything first. For anyone considering CTI, there are plenty of ways in.

I found my way into CTI by being curious, wanting to connect the dots, and understanding the bigger picture.

Amanda Capobianco

FROM INTERN TO CTI TEAM LEAD

“A lot of my confidence came from people trusting me with difficult problems before I felt completely ready.”

I studied computer science and software engineering, but I didn't feel like I fit the stereotype of the typical hacker in a hoodie.

During my final year, I got an internship with Richemont, where I was exposed to **incident response, forensic investigations, and threat hunting**. There wasn't a CTI function at the time, so **I started asking questions**. Why was this happening? What were the motives? **What patterns could we track to get ahead of an adversary?**

That curiosity led me toward threat intelligence. My internship became a full-time role, and I was eventually **given the freedom to build a CTI operation. Today, I manage that team.**

A lot of my confidence came from people **trusting me with difficult problems before I felt completely ready**. Meeting women across the CTI community also helped me see that **there wasn't one type of person who belonged here**.

You don't have to fit a certain mold to be a leader in this field.

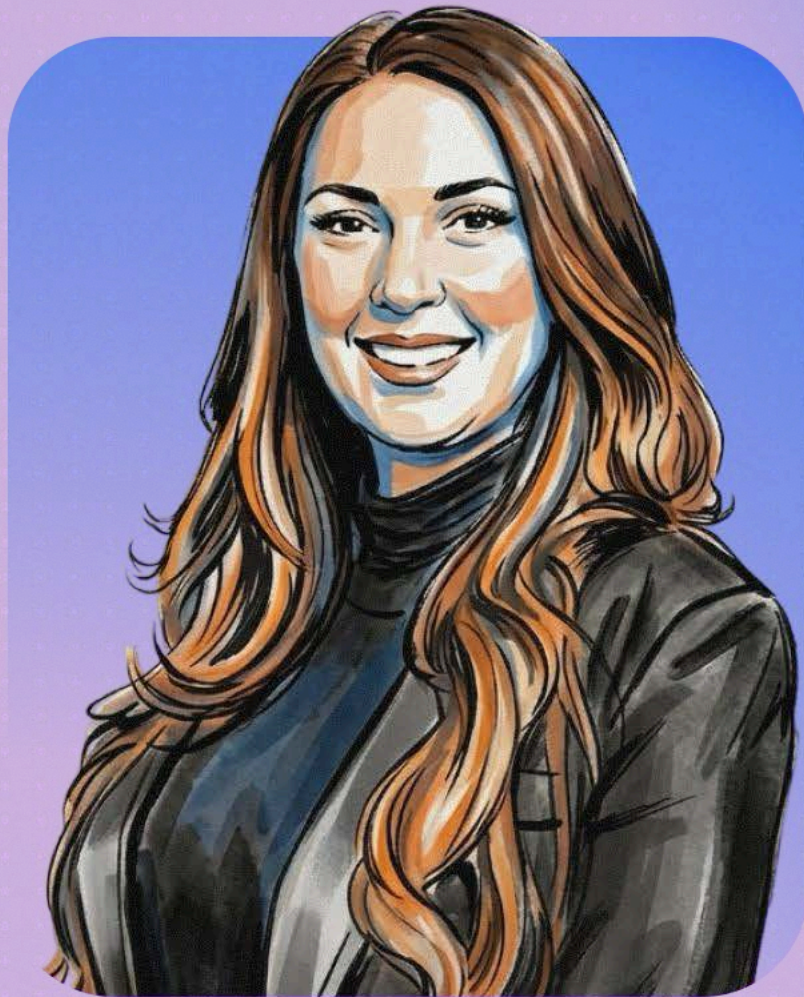


**Amanda
Capobianco**

CTI MANAGER, RICHEMONT

Route to CTI: A computer science and software engineering degree, followed by a final-year internship that led to building the CTI function.





Maril Vernon

FIELD CISO, HORIZON3

Route to CTI: A marketing career, re-enlisting in the Air National Guard, a cyber unit, then talking her way into penetration testing.



TALKING MY WAY IN, EARNING MY WAY UP

“Start trying, start failing, start learning. If you're failing, you're learning.”

I came into **cybersecurity completely cold at 30**. I'd already had a career in marketing, and before that, **I'd been everything from a barista and wedding planner to an IT recruiter**.

I knew cyber would be difficult to break into, so I **re-enlisted in the military and joined the Nevada Air National Guard** to get experience in a cyber unit. About a year later, **I landed my first private-sector cyber role in GRC**.

A few months later, a penetration testing job opened. **I didn't have the technical skills yet, but I knew the company, its people, its tools, and what the team was trying to achieve**.

I told my boss, “We both know I'm not the candidate today that you wish you had.

Give me a shot, and I promise a year from now you'll have the pen tester that you wish you had today.”

I got the job by talking my way in. From there, I moved through pentesting, red teaming, application security, and consulting before eventually coming **back to my GRC roots as a field CISO**.

My advice now is simple: **start trying, start failing, start learning. If you're failing, you're learning.**

I changed careers at 30. My mother started at 63 and now works as an incident response analyst for the federal government. Whether cyber is your first career or your third, **it's never too late to start.**

THE LONG WAY BACK TO INTELLIGENCE

“Each job taught me important things about being an intelligence professional.”

My journey didn't go in a straight line. I started in **counterterrorism**, and my first opportunity came at 18 through a Colonel who was willing to talk to me even though he didn't have any internships, and certainly not one for kids fresh out of high school. **A 30-minute conversation about geopolitics and the Army ran for two and a half hours.**

At the end, he walked me down the hall, leaned into the Head of Research's office, and said, **“You're getting an intern.”** That became **my first real job and my start into the counterterrorism and intelligence space.**

From there, I moved into **business strategy and consulting**, including a stint at a 20-person wine importer in California. At a company that small, **I did a bit of everything: IT and security, HR, customer service, shipping, and data analysis.**

I eventually went to graduate school to focus on **cybersecurity** and joined a cybersecurity startup. In 2019, I started at **CISA**, where I spent almost seven years. At CISA, I worked on **cyber defense for Operation Warp Speed**, launched **CISA's post-quantum cryptography work**, became **the agency's first chief of operations**, and **directed threat hunting operations.**

Today, **I lead threat intelligence at CoreWeave**, leading a team that looks at **multi-domain threats** that could affect our people, technology, facilities, suppliers, or ability to operate.

Looking at these pieces individually, things can seem disconnected, but **each job taught me important things about being an intelligence professional and how to best serve our customers.**



Natasha Eastman

HEAD OF THREAT
INTELLIGENCE, COREWEAVE

Route to CTI: Counterterrorism at 18, consulting, a California wine importer, grad school, then almost seven years at CISA.



HOWEVER YOU GET THERE, BRING YOUR CURIOSITY

There are plenty of routes into CTI, including some that only make sense in hindsight. Previous careers, unexpected opportunities, and skills picked up elsewhere can all become part of the work.

If you're considering CTI, your background doesn't necessarily have to resemble any of theirs. Curiosity, problem-solving, learning, and a desire to understand why something happened can all give you somewhere to start.



Someone Took a Chance on Me

Few people build a career entirely on their own. At some point, somebody has to give you the opportunity to do something you haven't done before, or encourage you to keep going when you're not sure you belong.

For each of these women, somebody saw what they could become before they could see it themselves. Each now does the same for the people coming up behind her.

**Great leaders
don't just hire
experience, they
recognize potential.**

Saba Bagheri

POTENTIAL BEFORE PROOF

“Sometimes all it takes is one person saying, “I think you can do this,” before you start believing it yourself.”

I didn't plan to end up in Cyber Threat Intelligence. I worked across different areas of cyber, and CTI was an opportunity that came along rather than something I deliberately targeted.

The biggest opportunity came when I was working in government. I hadn't spent years in CTI, but instead of looking for someone who had already built a threat intelligence function, **my manager trusted me to build one from scratch.**

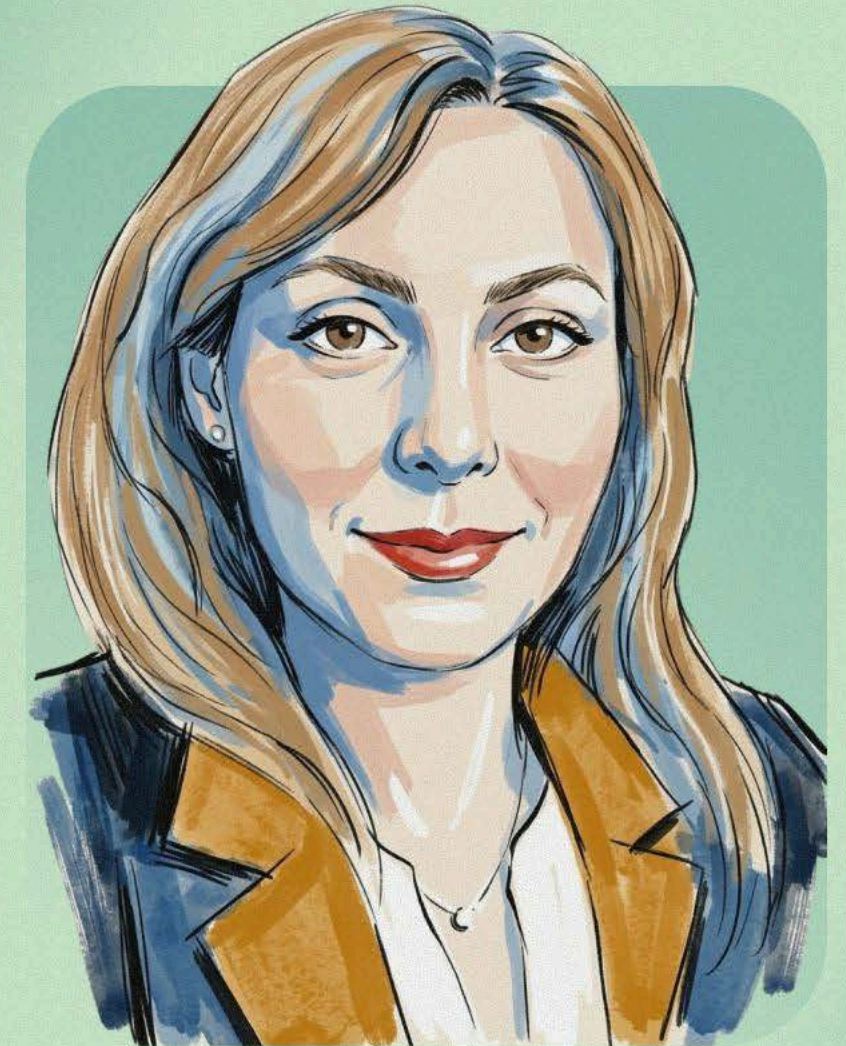
It wasn't just a promotion. I had to **define the strategy, establish processes, build relationships with stakeholders, and demonstrate why threat intelligence mattered.**

Looking back, that experience taught me far more than I would have learned by inheriting a mature team. It also taught me something important about leadership: **great leaders don't just hire experience. They recognize potential.**

CTI brought together everything I enjoyed most: understanding how attackers think, analyzing information, and helping organizations make better decisions. You don't need to know everything about every threat actor to do that. Nobody can. **Curiosity, critical thinking, and communication matter just as much.**

Someone gave me an opportunity before I had the experience on paper. Now I try to do the same for others, **especially women who might not yet see themselves as leaders.**

Sometimes all it takes is one person saying, “I think you can do this,” before you start believing it yourself.



**Saba Bagheri,
PhD**

CYBER THREAT INTELLIGENCE
MANAGER, BUPA APAC

Route to CTI: Cybersecurity roles across government, then a manager who trusted her to build a threat intelligence function from scratch.





Rebecca Taylor

RESEARCHER,
SOPHOS X-OPS
COUNTER THREAT UNIT

Route to CTI: An English and creative writing degree, then a personal assistant role.



SOMEONE WHO SAW ME

“Don't let a lack of technical qualifications convince you that you don't belong.”

I was headhunted into Secureworks (since acquired by Sophos) as a personal assistant, making tea, booking meeting rooms, and doing expenses. Within two weeks, I saw **the depth of opportunity in cybersecurity**. If I worked hard and remained curious, **I could be somebody in this industry**.

I worked my way up to our **first Incident Command team**, sitting alongside major ransomware incidents. It was a real challenge and in many ways exhausting. I wasn't sure if I was the right fit or that I could keep up with the pace.

That's when Barry Hensley, whom we called the Colonel, stepped in. Barry was C-suite, but **hierarchy didn't matter to him**. He listened, made sure I was looking after 'me', and **helped me progress into the Counter Threat Unit**.

He just saw me. He knew if given a chance, I would work my magic and **be a real asset in CTI**.

Today, I have a series of personas which I use to monitor and collect across underground forums. I focus on **access brokers, data leaks, and emerging threats like new ransomware groups**. It is a long way from booking meeting rooms and getting the coffee in.

When I mentor now, I ask people to make two lists: **a joys list and a non-negotiables list**. This field can be really hard and so if you're going to work in it, you should **find the parts of it that fit you and that make you happy**.

Don't let a lack of technical qualifications convince you that you don't belong. Lived experience matters. Passion matters. Sometimes you need somebody else to see what you could bring before you see it yourself.

THEY SEE WHO YOU ARE

“Find the thing that speaks to you. Follow the thread.”

I never thought I would wind up here.

Truly. **Not in my wildest dreams.**

I spent ten years out of the workforce raising my children. When I came back, I started from the ground up at a tiny managed services company in a basement, doing whatever needed doing.

Then I came across an article about Stuxnet. I have a degree in political science, and suddenly I could see technology and geopolitics colliding. **It was an aha moment: now I know what I want to do. This actually exists.**

I started devouring everything I could find about information security, asking questions, and going down a thousand rabbit holes. Eventually, people in the community started inviting me to things.

There I was, **a self-described middle-aged housewife at a hacker conference in Indianapolis, and I was welcomed as I was.**

Then Stephanie Carruthers encouraged me to submit a talk to the Proving Ground at BSides Las Vegas. I remember getting the acceptance email on a Friday night and falling off the couch.

I think I yelled, **“I'm going to Vegas.”**

I didn't have much money. I went with a box of cereal bars, volunteered so I could get meals, and stayed with a friend. The event stipend was enough to buy a DEF CON pass. **I arrived feeling like Alice in Wonderland.**

People kept helping me take the next step. Virginie Robbins and Sarah Clarke got me to my first ShmooCon. Later, my friend told me, **“Send me your resume, damn it.”** That helped me make the move to KPMG. **He saw something in me that I didn't believe in yet.**

I have a wall of conference lanyards behind me now, most of them speaker badges. That's why **I pay it forward.** I mentor people, encourage them to submit the talk, and remind them **they don't need the perfect background.**

Find the thing that speaks to you. Follow the thread. And when somebody sees something in you that you haven't learned to see in yourself yet, listen to them.



Cheryl Biswas

CYBERSECURITY RESEARCHER, FREELANCE

Route to CTI: political science, a small managed services provider, and teaching herself security after reading about Stuxnet.



PASSING IT ON

A chance can look like a new role, a conversation, an introduction, a conference ticket, or somebody insisting that you send the résumé.

Those moments matter because somebody saw potential before there was proof. And once you've experienced that kind of belief, you remember what it can do.

BEYOND CTI

Away from work, these women find very different ways to switch off, recharge, and pursue the things they love.



SPEED PUZZLING

Maril Vernon

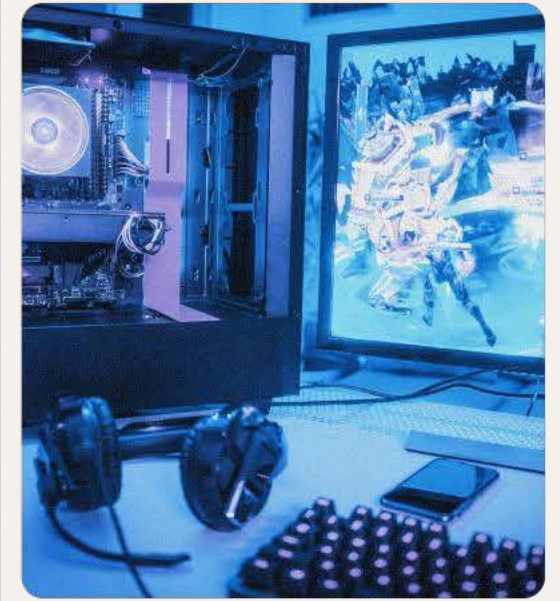
I compete in speed puzzling and deliberately pick harder and harder puzzles. One almost completely black puzzle took me about 25 hours.



BASS GUITAR

Angélique Jard

A bad day is a day when everything you do doesn't work. On those days, it's good to just disconnect and accept it will be better soon. I'm a musician, so I can just take the guitar.



GAMES AND ART

Jasmina Zito

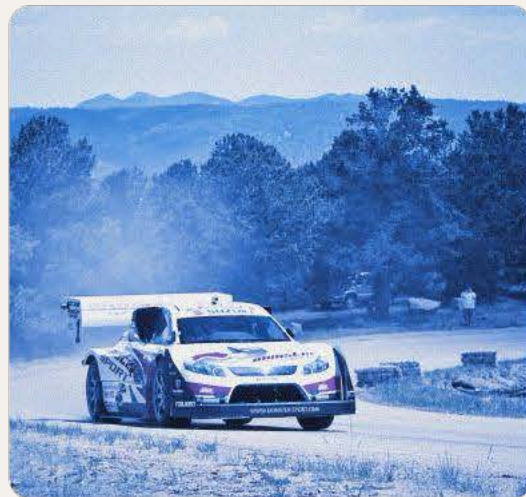
Video games are a big one for me, along with drawing, painting, music, or whatever happens to be my current obsession. When 5 p.m. hits, I switch off from threat intelligence.



ROAD CYCLING

Einat Argon

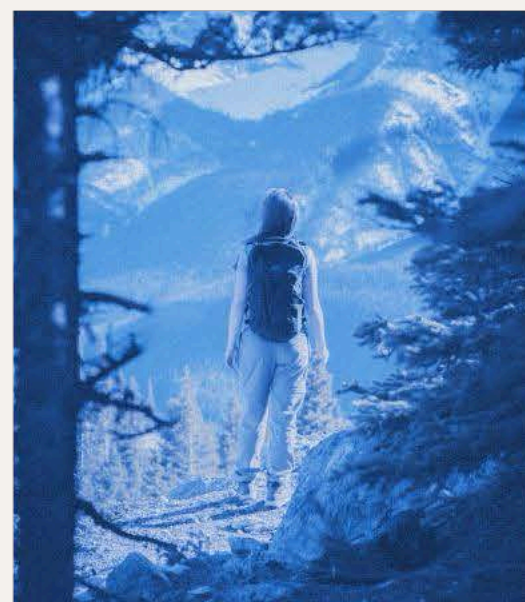
I raced semi-professionally for seven years, mostly in Europe. Cycling taught me a lot about what it means to keep going when things get hard.



HILL CLIMB MOTORSPORT

Sophia McCall

My dad was a rally driver, so motorsport has always been a big passion. Now I do competitive hill climbing around the UK. It keeps me completely in the zone, switched off from work.



HIKING

Nitsan Daniel

I love hiking with my family, especially in northern Israel. When the view opens up around you, something changes. Even your breathing tempo changes.



COOKING AND PAINTING

Amanda Capobianco

After a technical, stressful day, cooking, painting and art take the edge off and bring me back down to earth.



SCUBA DIVING

Natasha Eastman

I picked the most nerdy version of scuba diving, building my rebreather and testing oxygen cells. Underwater photography, sharks, wrecks. It literally puts me in another world.



Earning the Room

Knowing your subject is only part of working in threat intelligence. The intelligence still has to reach someone who trusts it enough to act.

That trust can take time to earn. These next stories reveal how credibility came from listening first, delivering what people need, and proving the value of their work over time.

**People respect
honesty far more
than false certainty.**

Saba Bagheri

DON'T GIVE AN ANSWER FOR EVERYTHING

“Earning credibility also means being comfortable with what you don't know.”

I came into cybersecurity through customer success, but before that, I spent seven years racing as a semi-professional cyclist across Europe.

When I decided I needed a different challenge, I looked at what I had already done and which of those skills could transfer into technology. Cycling had taught me a lot about **preparation and adapting when things don't go as planned**. You can ride the same course many times in the sun, then turn up on race day and find it completely wet and raining. You prepare as much as you can, then deal with what is in front of you.

I see a lot of women trying to move into technology who start with what they haven't done and what they don't have. I look at it differently. **What have I done already that can translate into results or show somebody that they can trust me to execute?**

When I started looking at technology, **customer success was where my existing skills fitted best**.

My leading mentors, Effie Mansdorf and Kate Neal, told me that if I was curious and had the ability to learn, **cybersecurity was absolutely achievable**.

I later took a security analyst course because I wanted to **understand the technical side rather than be intimidated by it**. I wanted the vocabulary and a better understanding of what analysts do every day.

That **willingness to keep learning** is something else I took from cycling. Most of your time as an athlete is spent training rather than racing. Cybersecurity can feel much the same. You don't know what you're going to wake up to. **You prepare, keep learning, and get comfortable dealing with something you didn't expect**.

Earning credibility also means **being comfortable with what you don't know**. You don't need to give an answer to everything. If you don't know, you should be able to **say so with confidence, find the answer, and come back**.



Einat Argon

MANAGER, CUSTOMER SUCCESS, FILIGRAN

Route to CTI: hotel customer journey work and a CRM rollout after racing, then a customer success course that led to a cybersecurity startup.





Karla Reffold

CHIEF INSIGHTS OFFICER, SUREFIRE CYBER

Route to CTI: founding a recruitment company that pivoted to become the biggest cyber-specific recruiter, then moving into intelligence.



EARNING TRUST WHEN THE STAKES ARE HIGH

“Trust has come by listening to what they want and then delivering on that.”

The first thing I tell people is that **I manage ransomware negotiations**. My team **communicates with threat actors and helps our clients manage the negotiation process**. It's a different area of threat intelligence and an interesting one.

My path here is an unusual one. I founded a recruitment company, and very early on, a partner told us, “You should check out this cyber thing. I think it's going to be big.” We pivoted and became the first and ultimately **the biggest cyber-specific recruitment company in the UK**.

After I sold it, I went on to run a **cyber threat intelligence product company**. That's where I got **my first real experience of threat intelligence**.

Today, **we turn what we learn during incidents into insights our partners can act on**. Every client wants something slightly different, so trust

starts with listening to what they care about and **making the intelligence actionable for them**.

Some of the most important relationships were within the company itself. My team had to **build credibility with the incident response team and forensic investigators** so they could see what my team was capable of. **Trust has come by listening to what they want and then delivering on that**.

Being part of incident response has also changed how I see the value of the work we do. **We see people on one of the worst days of their lives**.

Still, **there are limits to what intelligence can tell you**. Threat actors aren't sitting on the dark web saying, “Hey, I'm going to go attack Karla tomorrow.” You see indicators, and **somebody has to translate what they mean so you can act**. You could call that predictive, but I don't think it makes you an oracle.

TRUST IS EARNED IN THE FOLLOW- THROUGH

Credibility grows through small moments: admitting when you don't know, coming back when you said you would, and delivering intelligence people can use.

That trust can take months to build, particularly when colleagues are still learning what intelligence can contribute. Knowing your subject matters. So does becoming someone people trust when it matters.



The Human in the Loop

AI can take work off an analyst's plate, but deciding what to hand over is becoming a skill in itself.

Our next two experts both use AI in their work, without dismissing what it can do. But both draw a line around the work that still needs human expertise, whether that's checking that something exists in the first place or working through the evidence to decide what it means.

**You can go very fast
alone, but you can go
very fast into a wall.**

Angélique Jard

A GOOD ASSISTANT, IF YOU KNOW THE WORK

“The best work I've done has always been with other people, people who challenge your ideas and see the problem differently.”

I've been a software developer for 20 years, so I've already seen the job change many times. AI is another change I have to keep up with.

I'm a practical person. When something new comes up, I read about it, try it in different ways, and form my own opinion. With AI, I also watch the people using it most, ask them questions, and then tell myself: **go and try it. You will learn.**

There are parts of software development where AI is very useful. I call it the **“copy-paste and replace” work**, doing something similar to what you've done before, but not exactly the same. **AI handles that very quickly. It's useful for documentation too.**

Sometimes it feels like software development 20 years ago, when you had to wait for the computer to compile the program. Now you ask AI to do something, go and grab a coffee, and wait for the result.

The problem comes when people **assume the result must be right.**

We now receive bug and security reports created with AI. Because **AI can hallucinate, somebody still has to reproduce the steps.** Sometimes you spend an hour investigating only to discover **the problem was invented.**

It's the same with AI-generated code.

More people can produce code now **without understanding what they're doing. Somebody still has to review it, and that comes back to the experts.**

The best work I've done has always been with other people, **people who challenge your ideas and see the problem differently.**

AI can help us move faster too. **We still need people to make sure we're moving in the right direction.**



Angélique Jard

PRINCIPAL SOFTWARE
ENGINEER, OPENCTI, FILIGRAN

Route to CTI: twenty years as a software developer, drawn to Filigran by the open source side of OpenCTI rather than by security itself.





Jasmina Zito

HEAD OF THREAT INTELLIGENCE
AND RED TEAM, CANVA

Route to CTI: digital art and games development, then a mentorship pairing that pushed her toward a cybersecurity grad program.



DON'T OUTSOURCE THE CRAFT

“I would rather use AI to speed up the repeatable work and protect the parts where we add the most value.”

I was a massive AI hater at first. I don't think it was ready when everybody started going nuts about it.

What changed my mind was realizing that people were using AI for things I would previously have written a Python script to automate. Thinking about it that way, I could see where it fitted into my work.

If something is repeatable, AI can be useful. I can give it a workflow: get this context, search this system, pull this information together, and synthesize it.

Where I don't trust it is reasoning and conclusions. Sometimes it hits the mark, and sometimes it doesn't.

I'm wary of using AI to write threat intelligence reports because **writing is part of the analysis.** When you make sense of the information yourself, you also interrogate the sources.

Why did this person say this? Where did they get it from? If AI does that part for you, **you risk losing a key part of the craft.**

Even reviewing an AI first draft isn't necessarily the answer. I've seen people experience **review fatigue.** Your attention drops, and you're no longer doing the hard work of synthesizing the information yourself.

So I would rather **use AI to speed up the repeatable work and protect the parts where we add the most value.**

People at work joke about my “Red Pen of Doom” because I'm meticulous about the language we use. **What you say, what you imply, and what you leave out can all change the meaning.**

Words matter. AI can give us more ways to produce them. **We still have to decide whether they're the right ones.**

DECIDING WHAT NOT TO AUTOMATE

AI can take on more of the repetitive work, speed up research, and help analysts process information faster.

But tomorrow's CTI leaders will still need to know how to question what they are given, follow the evidence, and make the call themselves. Those are skills worth holding on to.

USING AI IN CTI

Where AI earns its place, and where it wastes your afternoon.



Karla Reffold

AI can use a lot of words that sound right until you stop and go, "Hang on, what does that actually mean?"



Alex Keedy

AI is that buzzword that often gets overused and overvalued. There is a lot it cannot do, yet some stakeholders believe it can substitute a real-life human. It is headed in the direction of augmenting analysts, triaging alerts, pulling out relevant metadata, and synthesizing data.



Nitsan Daniel

Suddenly, you see back-end engineers who said they'd never do any UI building the whole thing. Research that took weeks, you can now do on top of our data.



Natasha Eastman

We have agents that perform quality control on our data in OpenCTI, agents that conduct hunts, and AI that helps our interns build dashboards. AI is only as good as the data you push at it.



Jane Ginn

LLMs and agents have significantly improved my ability to find and use resources that, before, were beyond my reach. The noise comes from influencers pushing AI-generated content to build their reputation.



Rachel Mansson

AI will probably help us go faster, but we'll still need to do the analysis and context-building, because the point of threat intel is actionable insight with business context.



Mariana Mazi

I want AI to be something I can bounce ideas off, not something I follow blindly. You need training on how to use it. It's like riding a liter bike. You start on the bicycle, then 125, then 250, then 500, and then the liter bike is no problem.



Cheryl Biswas

We have to be sharing information because of where AI is now and where it's going. We need to collaborate like we never have before.



Staying Sharp

Threat intelligence never reaches a point where you know enough. New vulnerabilities appear, techniques change, and the volume of information keeps growing.

Keeping up can mean getting hands-on with something new to understand how it works. It can also mean knowing what deserves your attention when there is more information than anyone can reasonably follow.

There will always be another alert, another vulnerability, or another piece of news that sounds urgent. My first question is: what information is relevant right now?

Rachel Mansson

TRAIN BEFORE THE RACE

“Staying current comes down to studying. Reading, reading, reading, and then trying things for myself.”

The first thing I do when I wake up, before I even get out of bed, is open the news and see what happened while I was sleeping.

Any breach, any takedown, any new threat.

The algorithms know me too well by now.

When I get to work, I check again, partly because I was only just opening my eyes the first time and might have missed something.

Reading isn't enough for me. If I see a new exploit or CVE, one of my tasks that day might be to **build a VM and try it myself**. I don't want to be working out how a vulnerability works in the middle of an assessment.

I think of it as training. If you're going to run a marathon, **you train before the race**. I also go into TryHackMe or Hack The Box and look at **new rooms, new data, new skills to acquire**.

I've always liked breaking things. My father used to ask what I was going to do with my life if I kept messing with things like that.

I worked in Level 1 IT support while studying, dealing with technical problems and, most of the time, human problems. By the end of my bachelor's degree, I knew **the answer was cybersecurity**.

I was around 40 when I was finally given my chance to put what I'd learned into practice by my current boss and mentor, Dr. Konstantinos Votis. I've been **making up for lost time ever since**.

That curiosity also affects how I use AI. If it gives me a Python script for an assessment, I don't just run it and move on. **I study the code. I change things. I want to know why it works.**

For me, staying current comes down to studying. **Reading, reading, reading, and then trying things for myself.**



Mariana Mazi

SENIOR CYBERSECURITY ENGINEER
AND PENETRATION TESTER, CERTH/ITI

Route to CTI: level one IT support during her studies, a master's at Aristotle University, and a professor who kept believing in her.





Rachel Mansson

ASSOCIATE DIRECTOR, CYBER SECURITY
THREAT INTELLIGENCE, DEAKIN UNIVERSITY

Route to CTI: an unexpected move from science into IT project management, then eight years in cyber that led to a new chapter in threat intelligence.



CALM IS CONTAGIOUS

“I’ve stacked skills as I’ve gone. I’m still adding to that stack now.”

There is so much to learn and not enough time in the day. I’ve got three boys, and the pace of life is fast even before you add cybersecurity. A motto I have running through my head: **calm is contagious**.

I carry that into **threat intelligence, vulnerability management, and operations**. There will always be another alert that sounds urgent. My first question is: **what information is relevant right now?**

I’m a **lifelong learner**. I’m always reading and trying to make time for podcasts. At the moment, I’m reading **The Checklist Manifesto**, and it has made me think a lot about **playbooks and checklists and what they mean for threat intelligence**.

When something happens, I don’t want the team panicking because of the hype around a piece of news. What exactly is this alert? What do our playbooks tell us to do? **Have we got the basics covered?**

I’m relatively new to threat intelligence specifically, and I’m helping build a dedicated CTI

team at **Deakin University**. I’ve been working in **cybersecurity for the past eight years**, across various cyber domains.

I started my career in science before moving into IT project management while I was pregnant with my first son. That move set me on the path to cybersecurity.

I’ve **stacked skills** as I’ve gone. The **organization and analysis from the lab, the communication and engagement from awareness work, and the delivery and project skills** I’ve developed along the way all help me in threat intelligence. I’m still adding to that stack now.

There is no way I can read or know everything, and I don’t think you need to. **My team helps, and so do my peers**. I’m lucky to work in a **collaborative team and sector** where people are generous with their knowledge and are always willing to learn from each other.

For me, **staying sharp means continuing to learn, staying curious, and having enough structure around the work to focus on what matters most right now**.

KEEPING PACE

There will always be another vulnerability, technique, tool, or piece of intelligence demanding attention. Nobody gets to the end of the reading list.

Staying sharp means learning to live with that: keep studying, test things for yourself, and know what can wait. You don't have to know everything, but you do have to keep learning.

BREAKING INTO CTI

We asked about breaking in, what to study, what they'd tell somebody considering CTI, and what they'd leave out.



Maril Vernon

Go out there and start trying, start failing, start learning. I learned way more when things went wrong and I had to debug them than when things magically went right.



Cheryl Biswas

If I wrote a talk and it got accepted, that covered the cost of my admission. If you don't want to give a talk, volunteer. Volunteers are golden.



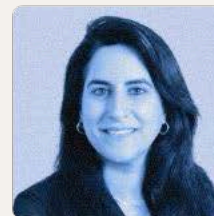
Amanda Capobianco

Everyone harps on the technical side. But curiosity, listening, and problem solving are what set you apart from everyone who has all the technical qualifications.



Jane Ginn

Don't take intellectual shortcuts. AI can't replace doing the work. Study the threat actors, understand the patterns, and build that knowledge for yourself. That's how you develop the judgment you'll need.



Nitsan Daniel

This isn't a job you do in isolation. The best ideas come from having somebody challenge your assumptions. I can't imagine not wanting to spend the day with my team.



Alex Keedy

I like to do a bit of cross-training and ask my employers for training assistance, such as paid courses and certifications. When you are interested in the subject matter, it doesn't really feel like work.



The Moment that Changed Everything

Sometimes a single investigation changes how you understand the work, revealing a connection you hadn't appreciated or proving that something you thought possible works in practice.

The evidence may stretch further back than expected, or make more sense against events far beyond the network. Either way, the investigation gets bigger than it was before.

**It was not a woman
who helped me the
most. It was the actor
Robert Redford.**

Jane Ginn

LEARNING THROUGH CHANGE

“It has always been hard for me to upskill while working, so I have routinely taken time off to do it.”

It was actor **Robert Redford**. He founded an institute that funded my graduate work as one of 19 fellows in the 1980s. After the fellowship, I moved to Washington, D.C., to a company with **Department of Energy contracts**.

Through DOE, I had early exposure to **ARPAnet**, the precursor of the internet, and it convinced me to **retool and pivot to operational IT**. Ten years later, I pivoted again into **cybersecurity and CTI**.

It has always been hard for me to **upskill while working**, so I have routinely taken time off to do it. I took a sabbatical to earn my **second master’s degree in information assurance**. When **quantum computing** arrived as the next big challenge, I enrolled in **MIT’s xPRO program**.

However, **one experience changed the way I saw CTI itself**.

As co-founder of the **Sports-ISA0**, I ran pop-up

SOC operations for major sporting events, including several **Olympics and World Cups**.

During the **2016 Summer Olympics in Rio**, I began observing the **[Redacted Russian influence operation]**, and I kept watching over the next ten years as its activity evolved.

My career has taught me to look at **geopolitics, threat actor motivations, and public policy** alongside the technical picture. Watching that **influence operation brought those strands together**. Understanding an actor can mean looking at the **political forces around its actions**.

That connection matters more as CTI expands into **information operations and disinformation**. **Rio changed how I saw the field** and what **threat intelligence can contribute to understanding events beyond the network**.



Jane Ginn

CYBER THREAT ANALYST AND CO-FOUNDER,
CYBER THREAT INTELLIGENCE NETWORK

Route to CTI: theatre training and a geography degree, then engineering consulting through the 1990s and a master's in information assurance.





Nitsan Daniel

CTO AND COFOUNDER, VISIONHEIGHT

Route to CTI: an intelligence unit in the army, then co-founding a cybersecurity startup as its CTO.



MONTHS BEFORE THEY BUILT IT

“Prediction can sound like magic or like something based on a heuristic.”

I've spent my entire career working with large amounts of data and trying to **find insights that wouldn't be visible otherwise**. But there was one investigation where I saw what that could mean for **threat intelligence in a new way**.

We heard about an **attack on the Polish energy sector**. I think Google published information about it and asked whether anyone had more, so I started researching it using our data.

It was **the first time I had been able to do a complete investigation end to end using our data together with AI**.

Within an hour, I was already confident we had something. Over the next few hours and then days, I built out the investigation.

We could see the attackers during the attack, but we could also go much further back.

Our data showed them months earlier, building their infrastructure and preparing for what they were going to do. Then we could follow them through the attack and see where they moved afterward.

For me, that was significant. **Threat intelligence is often thought of as something based on the past**. You investigate what happened and use that information to **help protect against the next attack**. Prediction can sound like magic or like something based on a heuristic.

This investigation showed me a different possibility. The signs were there months before the attack happened. With the right data, we could find them.

SEEING THE RIGHT SIGNALS

Some investigations permanently change what you know to look for. A wider context can reveal forces beyond the network. A longer timeline can show signs of an attack months before it happens.

Experiences like these stay with you. They change the questions you ask, the signals you pay attention to, and what you believe threat intelligence can help uncover.



Busting the Myths

Cyber threat intelligence attracts its share of assumptions. Some come from films and television. Others come from a narrow idea of who works in cybersecurity, what they look like, and what skills they need.

The reality is usually less glamorous, more demanding, and far more varied. The work can mean tracking criminals through underground forums, helping other security teams understand where to focus, or spending hours researching a way into a system that somebody assumes can be hacked in seconds.

**I'm not a spy, I'm
too tired to be one.**

Rebecca Taylor

A NICE TO HAVE, NOT A NEED TO HAVE

“CTI is proactive intelligence, and you don't always see the ROI of preventing an attack.”

I knew I wanted to do something **security-related after 9/11**. During my master's in security and international relations, an opening came up at the **Kentucky Office of Homeland Security**, where I was **first exposed to cybersecurity**. I just sort of fell into it.

My first real position involved **identifying and tracking threats and profiling actors**. **I knew I had found my calling ever since**.

I'll never forget one of my favorite bosses and mentors, Joseph Harris **at Intel 471**. He gave me **the autonomy to make decisions on projects I'd never worked on** and buildouts I'd never managed, when I didn't have the explicit skills on my resume. I would like to think **the team I built made him proud**.

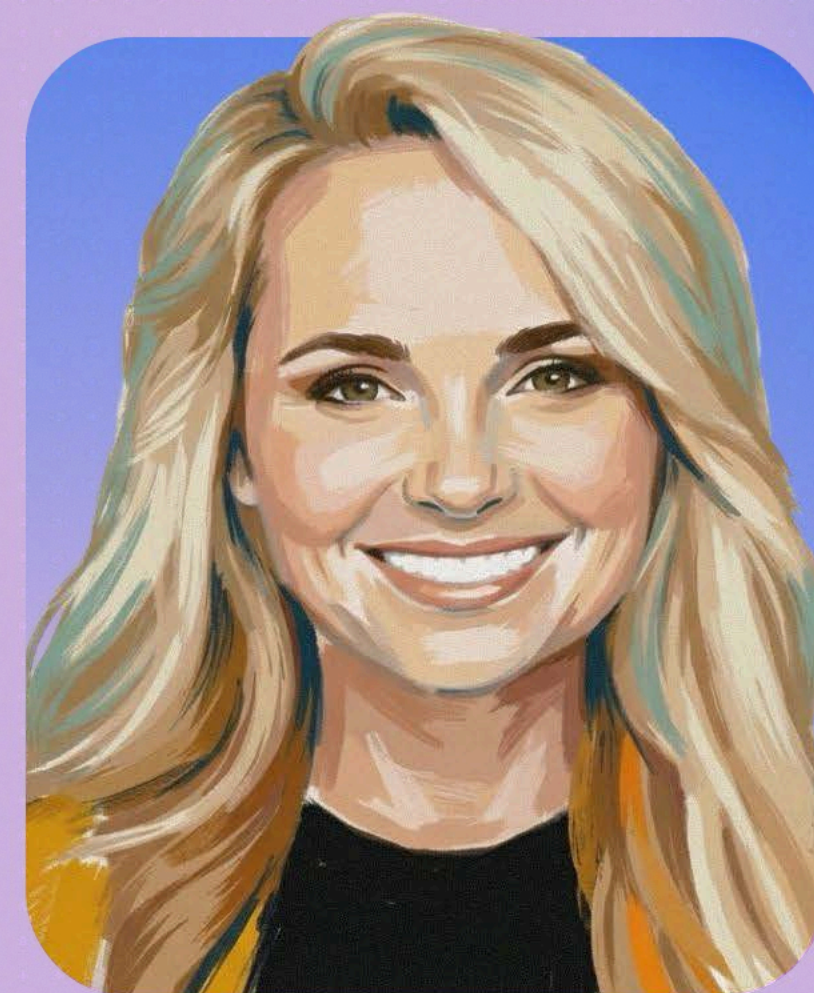
Today, I work in **dark web intelligence, profiling actors, tracking their campaigns, and notifying law enforcement**. I sometimes describe it as **Hollywood spy work, but on the internet**.

The misconception that costs organizations is the one inside them: that **threat intelligence is a “nice to have” rather than a “need to have.”**

Because **CTI is proactive**, you don't always see **the ROI of the attack that was prevented**.

But I know the work makes a difference, whether it's **identifying violent chatter online** or helping **thwart a multimillion-dollar ransomware incident**.

CTI is proactive intelligence, and you don't always see **the ROI of preventing an attack but you'll sure wish you had prior**.



Alex Keedy

SENIOR STRATEGIC
ADVISOR, FLASHPOINT

Route to CTI: a master's in security and international relations, a post at the Kentucky Office of Homeland Security, then Booz Allen.





Rebecca Taylor

RESEARCHER,
SOPHOS X-OPS
COUNTER THREAT UNIT

Route to CTI: an English and creative writing degree, then a personal assistant role.



NO, I'M NOT A SPY

“People assume I'm out there crimefighting in dark sunglasses and a Macintosh jacket.”

People often ask if this is really what I do.

I'm not a spy, I'm too tired to be one!

There can be a lot of hype around threat intelligence, particularly when you tell people you have **personas across underground forums and engage with cybercriminals.**

People assume I'm out there crimefighting in dark sunglasses and a Macintosh jacket.

It does make me smile, but that excitement can take away from **the seriousness of what we see.**

Two weeks into my **Human Intelligence role**, we found **an 80-page guide**

explaining how to **find a child to extort.**

I knew these things happened, but I had never imagined somebody would **write a manual explaining how to do it.**

Seeing things like that **changes you.** It makes **the threat so real, almost personal.** People think I'm being difficult when I don't want photographs of my children posted online.

But I know where **apparently harmless information can end up** and I know **the reality of online harms.**

WE BOTH HAVE BRAINS

“People ask how a woman ends up doing this kind of work. We both have brains.”

When I tell people **I work in cybersecurity**, I tend to hear the same things.

The first is that I'm the person in the black hoodie from the movies who can click a few keys and break into anything. I wish it were that easy.

Breaking into something means doing your homework. You study the system, do the reconnaissance, understand the architecture, gather information, and find your way in.

The second is: “Can you hack my ex?” No. Apart from being illegal, **I believe in privacy.**

And again, it isn't something you do with a couple of keystrokes.

Then there is the reaction I still get because I'm a woman. People ask how a woman ends up doing this kind of work.

We both have brains. Men and women can acquire the same knowledge.

What matters is having **the training and, most of all, the patience to do the job.**



Mariana Mazi

SENIOR CYBERSECURITY
ENGINEER AND PENETRATION
TESTER, CERTH/ITI

Route to CTI: level one IT support during her studies, a master's at Aristotle University, and a professor who kept believing in her.

BEYOND THE STEREOTYPES

CTI has accumulated plenty of mythology: spies, black hoodies, effortless hacks, and a certain idea of the person behind the keyboard.

Despite the stereotypes, there is no particular look, background, or path into cybersecurity. What matters is the willingness to learn, the patience to keep digging, and the judgment to know what matters.

WHAT PEOPLE GET WRONG

The myths that make them laugh, and
the ones that make their job harder.



Jasmina Zito

The biggest misconception is that threat intelligence recommendations are a mandate. I always say "I'm not your mom, I don't tell you what to do." We curate and contextualize information to help teams make decisions. They need to own those decisions.



Rachel Mansson

The misconception for threat intel is that you have to be technical to step into the role. It brings a bit of imposter syndrome. Everything you do in threat intelligence is communication with stakeholders.



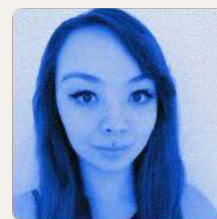
Karla Reffold

People have a pretty good understanding of threat intelligence itself. The misconception is how easy it is. Reading some cybersecurity blogs and keeping up with what's going on isn't intelligence.



Einat Argon

Analysts will say, "We ingested millions of indicators." That's not enough. I've seen a customer go from two days to half an hour to brief stakeholders on a zero day. That's the impact management wants to see.



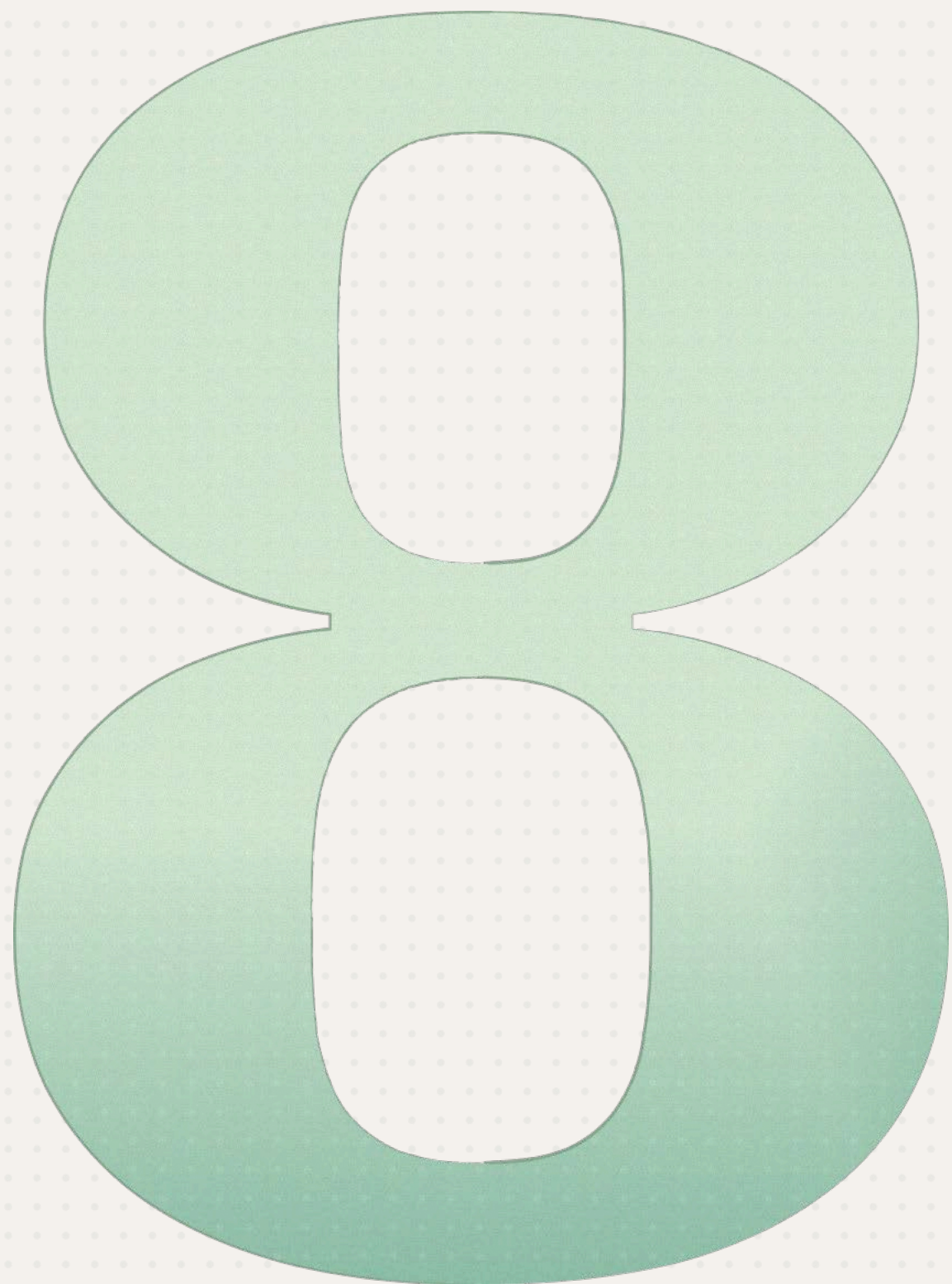
Sophia McCall

A lot of people think CTI is quite theoretical, that we just ponder the what-ifs. Modeling what a threat actor might do is part of it, but the work is data-driven, built on incident data, CVEs, and compromise metrics.



Mariana Mazi

That a well-built system can't be broken into. A human built it, so a human can break it. I once found a bug that let me impersonate anyone in the organization. That was the moment it stopped being a game, and I understood the power in my hands.



Why We Stay

The threats never stop, the technology never stands still, and much of the best work happens without an obvious moment of success.

So what keeps people coming back?
Sometimes it is a problem that looks different every day, or knowing the work may have stopped a bad day from ever happening.

**What keeps me going
is understanding
the threat actor
and getting
inside their mind.**

Sophia McCall

I LIKE HARD DAYS

“Your hard days and your good days come from the people you work with.”

I like hard days. Life isn't fun without a little bit of challenge.

It helps to **keep perspective on what a hard day really is.** If you're a small business owner who has just been told to pay a million dollars or lose your systems, that's a hard day. Mine don't compare.

In most jobs, **your hard days and your good days come from the people you work with.** If you can master how you approach that and **give people some grace, days are not hard.**

My team helps too. I'm probably **more motivated to help other people succeed and get promoted than anything else.** Having a team is very motivating for me.

And **I enjoy the work itself.** We're always trying to **stay one step ahead of the adversary,** and **as long as we have data and technology, this work will be needed.**

I always think **people should follow the path they enjoy.** I hate hearing people talk about their job as something they have to do. For me, **this is exciting and fun, and work is a core part of my life.**



Karla Reffold

CHIEF INSIGHTS OFFICER, SUREFIRE CYBER

Route to CTI: founding a recruitment company that pivoted to become the biggest cyber-specific recruiter, then moving into intelligence.





Saba Bagheri, PhD

CYBER THREAT INTELLIGENCE
MANAGER, BUPA APAC

Route to CTI: Cybersecurity roles across government, then a manager who trusted her to build a threat intelligence function from scratch.



THE SUCCESSES YOU NEVER SEE

“Cybersecurity is not a field where you immediately see the outcome of your work.”

When people ask what I do, I tell them, **“I spend my days thinking about how cybercriminals operate, so my organization doesn't have to learn about them the hard way.”** It usually gets a laugh, but that is a big part of what keeps me in this work.

Cybersecurity is not a field where you immediately see the outcome of your work. **Some of our greatest successes are the things that never happen. The incident that was avoided, the vulnerability that was prioritized in time, the risk that was reduced before it became a crisis.**

That can be challenging. You're fighting an invisible battle, and there are moments when you ask yourself if you're making enough of a difference.

What brings me back is remembering that **our role is to bring clarity into uncertainty, helping teams focus their limited resources on the risks that matter most.**

We are not just studying threats. We are helping people prepare for something they may never see coming.

COMING BACK TOMORROW

There may never be a final piece of the puzzle, and nobody gets to see a list of every incident that didn't happen because someone acted in time.

But there will always be another threat to understand tomorrow, and another chance to help someone make the right call. That is enough reason to come back and keep looking.



Lifting As We Climb

Every career here has been shaped by someone who offered encouragement, shared knowledge, or simply believed in someone before they believed in themselves.

The women we spoke to are determined to do the same for the next generation. This could mean mentoring someone who is making a career change, introducing them to the right people, or giving someone a platform when their work deserves more attention.

A lot of women come with what they didn't do and what they don't have. I always look at what they have done already.

Einat Argon

A NICE FULL CIRCLE

“Go to the conferences and meetups. Make connections.”

It started at university with **Cybersecurity Challenge UK**, with CTFs, hackathons, boot camps, and careers fairs. I worked my way up to the grand final masterclass and eventually **represented Team UK at the European Cybersecurity Challenge**.

I was part of Team UK from 2017 to 2019. When the program went on hiatus, I was heartbroken. **That community had played such a pivotal part in my career**, particularly in that period when you leave academia and are trying to find your feet.

Then last year, I came back to Team UK as a coach. This year, **I run the program as director of the UK Cyber Team**, the nonprofit that manages the UK's representation at the European Cybersecurity Challenge.

It's kind of a nice full circle. Now I help other people find their way in. One friend is in his 40s and has worked in carpentry all his life. He wants to move into cybersecurity, and my advice comes from my own experience: **put yourself out there, build relationships, and find your village**.

Without the community, I 100% hands down wouldn't be where I am in my career today. Now I get to help somebody else find their way into it.

That's why I tell people coming into cybersecurity to put themselves out there. **Go to the conferences and meetups. Make connections. Find your village and find your support.**



Sophia McCall

CTI SPECIALIST

Route to CTI: Capture the Flag competitions at the university, a graduate program doing penetration testing, and then threat intelligence.





Einat Argon

MANAGER, CUSTOMER SUCCESS, FILIGRAN

Route to CTI: hotel customer journey work and a CRM rollout after racing, then a customer success course that led to a cybersecurity startup.



GIVE THEM THE STAGE

“I want to create more opportunities for other women to be heard and recognized.”

From the early days and still today, I’ve had a **mentor in the cybersecurity industry**: Effie Mansdorf, Director of Customer Success at CrowdStrike. I absolutely follow what she does, and I speak with her quite often about challenges in customer success or new trends in cybersecurity.

Very specific to customer success, I have another person from those early days, Kate Neal, who's the Director of Customer Success at Gainsight.

Having those people to learn from has been important to me. I still look for new people who can give me a different perspective or teach me something I don't know. But I'd say a lot of the people who inspire and keep me going are **women who are customers**.

This is how the whole **Women in CTI initiative** started. I’d often be in meetings with groups of 10 or 12 customers, with maybe one or two women in the room, and they wouldn’t get much of a chance to speak.

I knew they had something to contribute. **I wanted to give them the stage.**

So together with Mary D’Angelo, we co-founded **Women in CTI**. The idea was that even if they didn’t have **the opportunity to shine** within their own company, they could do it through us. I started writing articles with them, publishing them on the Filigran blog, and making sure **their names and their work were highlighted**.

For me, **it comes back to people**. I've had people I could turn to throughout my own career, and now I want to create **more opportunities for other women to be heard and recognized for what they know**.

FIND YOUR VILLAGE, THEN GROW IT

Very few of these careers were built alone. People opened doors, made introductions, and created space for someone else to be heard.

Somebody's encouragement probably plays a part in your story too. When it's your turn, be that person for someone else.

SPENDING TIME WITH THESE SIXTEEN WOMEN LEAVES YOU EXCITED ABOUT THE FUTURE OF CTI.

There's so much energy in the way they talk about their work and the people they're bringing along with them.

They went back to study, took sabbaticals, tested exploits in virtual machines at night, took certifications on personal time, changed careers completely, and made the case for functions their organizations didn't yet know they needed. Often, they had no idea exactly where it would lead.

Other people played a part too. They offered advice, took chances, made introductions, and gave encouragement at the right moment. Now, many of these women are doing the same for others.

That deserves to be celebrated as loudly as the technical work.

Perhaps that's where the next story begins: with someone reading this applying for the role they've been talking themselves out of, sending the message, asking for the introduction, submitting the talk, or simply deciding to start.

Small decisions have a funny way of becoming careers.

Thank you to the sixteen women who trusted us with their stories. We're very glad we got to share them.

NOW WE'D LOVE TO HEAR YOURS.

CONTINUE THE CONVERSATION

Join 6,500+ women in CTI
in the Filigran community on Slack.

community.filigran.io

Contributors

Einat Argon		Manager, Customer Success, Filigran
Saba Bagheri, PhD		Cyber Threat Intelligence Manager, Bupa APAC
Cheryl Biswas		Cybersecurity Researcher, Freelance
Amanda Capobianco		CTI Manager, Richemont
Nitsan Daniel		CTO and Cofounder, VisionHeight
Natasha Eastman		Head of Threat Intelligence, CoreWeave
Jane Ginn		Cyber Threat Analyst and Co-founder, Cyber Threat Intelligence Network
Angélique Jard		Principal Software Engineer, OpenCTI, Filigran
Alex Keedy		Senior Strategic Advisor, Flashpoint
Rachel Mansson		Associate Director, Cyber Security Threat Intelligence, Deakin University
Mariana Mazi		Senior Cybersecurity Engineer and Penetration Tester, CERTH/ITI
Sophia McCall		CTI Specialist
Karla Reffold		Chief Insights Officer, Surefire Cyber
Rebecca Taylor		Researcher, Sophos X-Ops Counter Threat Unit
Maril Vernon		Field CISO, Horizon3
Jasmina Zito		Head of Threat Intelligence and Red Team, Canva

Organizations, communities, and platforms our contributors named, and what you'll find at each.

COMMUNITIES

Women in CTI

A place for women in threat intelligence to be heard on their own terms. Members publish and speak with their names on the work.

filigran.io/women-in-cti

Filigran Community on Slack

Open workspace for OpenCTI and OpenAEV users. 6,500+ members.

community.filigran.io

The Diana Initiative

Annual Las Vegas conference supporting people underrepresented in information security.

dianainitiative.org

CyNam, Cyber Cheltenham

Free events connecting Cheltenham's cyber professionals, students, and businesses.

cynam.org

Women4Cyber Foundation

A non-profit organization aimed at promoting, encouraging, and supporting the participation of women in the field of cybersecurity.

women4cyber.eu

HANDS-ON PRACTICE

TryHackMe

Browser-based labs that teach offensive and defensive skills, from complete beginner up.

tryhackme.com

Hack The Box

Labs and Capture the Flag challenges against realistic targets once the basics are in place.

hackthebox.com

TRAINING AND READING

Filigran Academy

Official training and certification for OpenCTI and OpenAEV.

academy.filigran.io

The Checklist Manifesto, 2009

Atul Gawande's book on the power of checklists.

EVENTS

BSides Las Vegas

Community-run security conference. Its Proving Ground track pairs first-time speakers with mentors to get them on stage.

bsideslv.org

ShmooCon, 2005 to 2025

Washington DC hacker convention built on original security research. Closed after its final event in January 2025.

shmoocon.org

Which events and resources do you find useful as a practitioner?

Let's continue the conversation on the [#women-in-cti](#) channel in [Slack](#)!

WOMEN // CTI supported by  Filigran