NORTHWAVE
CYBER SECURITY

# Gold Teaming.
# The perfect combination of testing and training.

In this expert Interview, we are meeting with two of our seasoned cyber security professionals; Eva Maas and Jaimy Thepass.

Eva is the Operational Lead of Northwave's Cyber Resilience Team and Jaimy runs our international group of Ethical Hackers. Together they help our clients with building and maintaining cyber resilience based on realistic attack simulations we call Gold Teaming.

## What is the main and common concern with the clients that you work with?

**Eva:** "All of the clients we work with are concerned that a crisis will impact their company's trustworthiness and continuity. I don't think that there are many companies in the world that don't worry about their digital resilience. Lately, we also see more worry about the personal liability of board members. They specifically want to understand how they can best take their responsibility."

## Many companies are struggling to find a pragmatic approach to Cyber Security. How are you helping them?

**Jaimy:** "Well for starters, we do that by making it simple. Forget abstract, theoretical risk projections on a PowerPoint slide. We deliver a realistic experience to the organisation. Managing cyber security is not trivial and, in all honesty, our industry is not always making it easier either. Eva and I, we have a motto: "Whether you are sure or unsure about your security, put it to the test." By doing what we do, we give our clients a two-edged sword. On the one hand, it shows them where they can still improve their preventive approach, while at the same time, they are instantly getting better in dealing with the eventuality of a breach.

We talk with them about a relatively new phenomenon called Gold Teaming, where an organisation is using the outcomes of a realistic cyberattack simulation in a crisis management exercise. This is the most realistic way to not only test security but immediately improve your response to a crisis, for everybody in your company, and not restricted to board level.

### The Gold Teaming approach sounds like something for really mature organisations, or is it useful to any company?

**Jaimy:** "We see that it makes sense for every organisation, regardless of their maturity to embrace the practical side of this. There is one certainty; almost every organisation will face a serious cyber crisis sooner or later. There is no point in just relying on prevention. Even if you have a clear roadmap to improve your protection, this in most cases will take time. In the meantime, you better be smart and get ready for a crisis!". "A full-blown Gold Teaming based on an Advanced Red Team would not be a logical first step for an organisation that is really immature on cyber security. This is why we work with a pallet of tests and exercises to bring clients to the next level step by step. It makes sense to start small when you are really just getting started. The investment in a Gold Teaming is substantial. However, the business case is there as incidents show us time and time again that a good response makes a huge difference in the speed of recovery and the subsequent impact on the business. A professional response limits the damage to your reputation and potential issues with authorities."

**Eva adds:** "It's smart to separate between testing and training at first. Testing is really done on measures that exist. Training can and should be done regardless of the actual posture. Small training sessions can already have a big impact on the ability to respond, when you know what you are doing. We take a lot of the exercises straight from our Incident Response practice. We have helped hundreds of companies recover from attacks and those cases we turn into training scenarios."

### Your teams work very closely together in these Gold Teaming engagements. What is the added value of this tight cooperation for your clients?

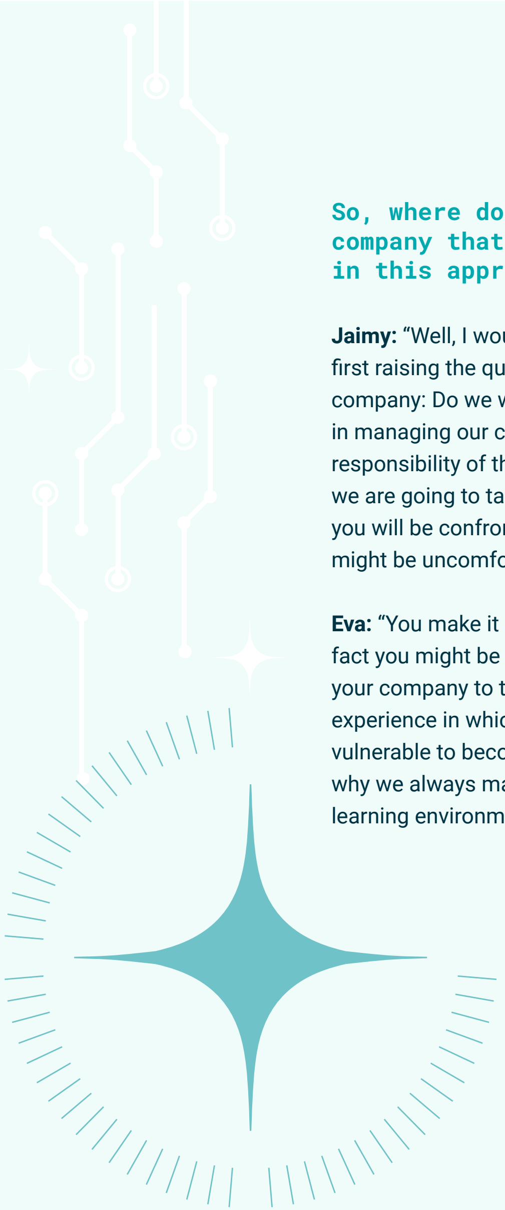
**Jaimy:** "Well of course my team starts the whole process and that predominantly has a technical focus. We take the latest cyber threat intelligence that is relevant within the business context of the client, and we create a realistic cyberattack based on that. This means that we behave like the attacker would behave and we use the tools and tricks that they use. Doing this will put stress on the actual preventive measures, but also on the quality of the monitoring, detection, and response capabilities. But if the customer asks us a specific scope or way of attacking, because they see this as their biggest threat, we adjust this. Think of APT simulation, an add-on like physical entrance, insider threat or social engineering."

**Eva adds:** "What we see is that usually, the tech teams with our client have some idea about where they are good and maybe are weak. Often, they have been trying to address that, but not always get the attention of the board for the investments needed to improve the security posture. By evolving a technical test into a crisis management exercise, we often create a reality check with that level of the organisation."

**Jaimy:** “What we see in real incidents is that the tech teams that must deal with the actual technical problems are finding it difficult to communicate in the best way with their colleagues in the boardroom, who need to manage the business impact of the crisis. We often see the techies struggle to explain what is going on in terms that the business leaders understand. Vice versa, we see board members dive into the details and become sidetracked in discussions about stuff they know nothing about. In the meantime, they forget to manage the business fallout of the crisis.”

### The new buzzword is cyber resilience. We hear everybody talking about this. What is it actually and what is your view on how to achieve resilience?

**Eva:** “Resilience is about being able to bounce back when an incident happens. For me, this is mostly about enabling the people responsible for dealing with incidents and crises. The resilience of a company surely also depends on the array of measures that we help them take across their organisation. Their technical measures to protect and recover their IT, their business continuity management, their information security management system, their supplier management, etc. But for me, in essence, Cyber Resilience is about confidence. It is very rewarding to see how these exercises instigate confidence within the team members that we train. Confidence that will prove to be of golden value when there is a real crisis to deal with”.



### So, where does a company that is interested in this approach start?

**Jaimy:** “Well, I would argue it starts with first raising the question in the board of that company: Do we want to get actively involved in managing our cyber risk and take our responsibility of this topic seriously? Because we are going to take you on a journey where you will be confronted with things that you might be uncomfortable with.”

**Eva:** “You make it sound a bit daunting, but in fact you might be right. Taking yourself and your company to the test will be a learning experience in which you need to be a little vulnerable to become more resilient. This is why we always make sure to create a safe learning environment.”

### With a rise in regulations, like NIS2, organisations need to prove continuous control over their cyber security. How does your approach fit into this?

**Eva:** “The signature of Northwave is that we always take a holistic perspective on cyber security, and we always work from the basis of ongoing security management. These Gold Teaming exercises as a tool can be part of testing the effectiveness of the measures that you take, as NIS2 says. The way we construct them is very much based on the actual risk of the client. Our Red Team testing is driven by the latest relevant Cyber Threat Intelligence. But more then only being a “check in the box” I believe that the learning experience of testing and exercising is that you get to see in practice where you are with regard to your cyber security maturity: that gives a really good basis to focus your efforts where really needed.”

**Jaimy:** “In all honesty I find all this commotion about NIS2 almost a little bit annoying. In fact, there have been other regulations like the GDPR that impose similar requirements on many companies. I just hope that we can steer away from this focus on compliance. There is a changing threat landscape where numerous actors, often state-sponsored, are taking their business of cybercrime and cyber espionage very seriously and investing almost endless amounts of money in them. That should be our first concern.”

### Eva Maas

Eva Maas studied International Relations and completed a Master in International Law. Eva started her career at the Department of Defense, where she worked in international legal affairs. She entered the world of cybercrime in 2015, when she joined the Ministry of Justice as a Policy Officer Cybercrime. She served with the Dutch National Bank for close to five years in the Threat Intelligence Unit, establishing the TIBER (Threat Intelligence Based Ethical Red Team) program. Before joining Northwave in 2024, she was executing the Cyber Resilience Program for the Dutch water management sector.

### Jaimy Thepass

Jaimy Thepass joined the Dutch Army, straight out of Highschool, where she specialised in electronic warfare. She was deployed to Mali as part of the United Nations stabilisation mission. During her service, Jaimy completed a Bachelor in Business, IT and Management, and worked in several different units within the Army. In the last years of her career, she worked at the Cyber Warfare and Training Centre of the Dutch Cyber Command. Having walked through the gate as a nineteen-year-old private, she left the service as a first lieutenant, to join Northwave in 2022. She is currently in charge of our Red Team; Northwave's group of expert ethical hackers and completing an Executive MBA at the Free University in Amsterdam.

**Would you like us to assist you on your journey towards cyber resilience and NIS2 readiness? You can reach us at:**

NORTHWAVE
CYBER SECURITY

E: info@northwave-cybersecurity.com
T: +31 (0) 30 303 1240
W: northwave-cybersecurity.com