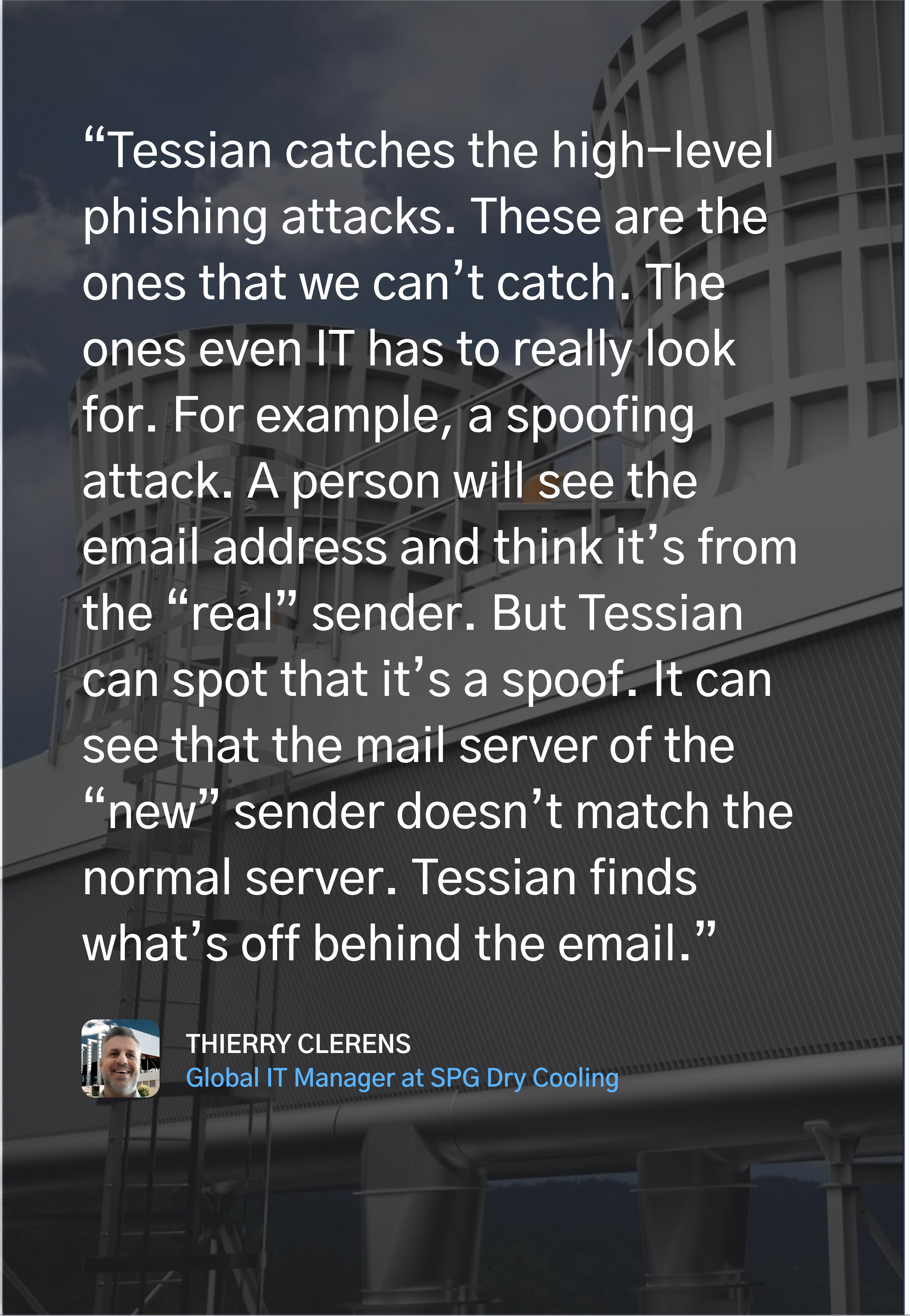
How Tessian is Preventing Advanced Impersonation Attacks in Manufacturing

ABOUT SPG DRY COOLING

SPG Cooling is an innovative, global leading manufacturer of air–cooled condensers that has been providing exceptional quality equipment to coal, oil, and gas industrial plants for over a century. They employee a global workforce and have over 1,000 customer references. We talked to Thierry Clerens, Global IT Manager at SPG Dry Cooling, to learn more about the problems Tessian helps solve and why he chose Tessian Defender over other solutions.

KEY FACTS

- 368 User Deployment
- Tessian Defender Deployed



> "Tessian catches the high-level phishing attacks. These are the ones that we can't catch. The ones even IT has to really look for. For example, a spoofing attack. A person will see the email address and think it's from the "real" sender. But Tessian can spot that it's a spoof. It can see that the mail server of the "new" sender doesn't match the normal server. Tessian finds what's off behind the email."

THIERRY CLERENS
Global IT Manager at SPG Dry Cooling

PROBLEM

The most advanced threats can slip past other controls

Phishing is a big problem across *all* industries. But, because email attacks are becoming more and more sophisticated and hackers continue using tactics like domain impersonation and email spoofing, Thierry knew he needed to implement a new solution that could stop the advanced phishing emails that might slip past his O365 controls and trained employees.

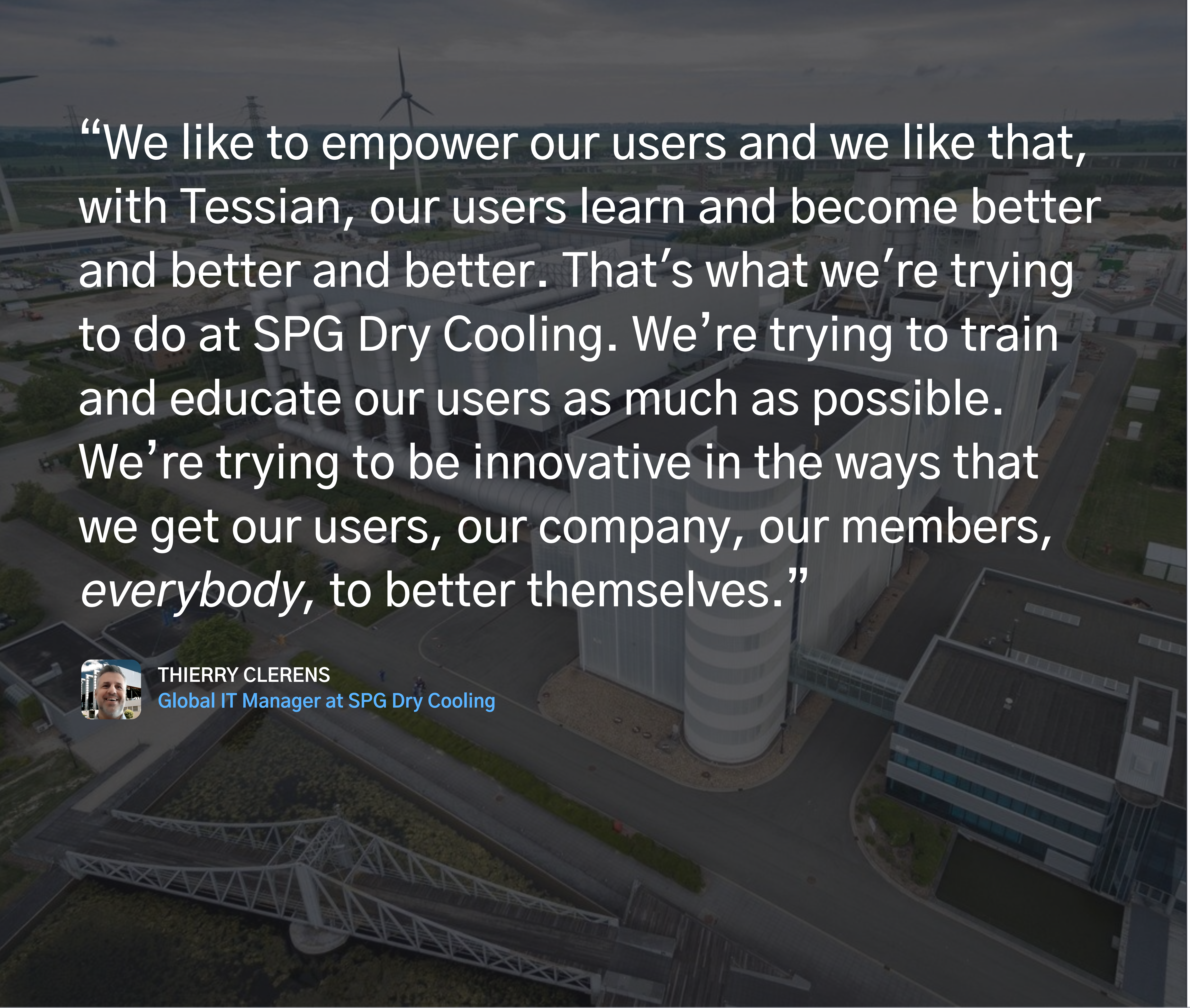
He cited one specific incident where a hacker impersonated a company in SPG Cooling's supply chain and attempted to initiate a wire transfer. How? A tiny, difficult-to-spot change in the domain name.

"They created a fake domain with exactly the same name as the real user. But the top-level domain .tr was missing at the end. So it was just .com. No user – not even IT! – is looking at the domain name that closely. They tried to get us to deliver money to another account," Thierry explained.

While the attack wasn't successful (SPG Dry Cooling has strong policies and procedures in place to confirm the legitimacy of requests like this) he wanted to level-up his email security and help users spot these advanced impersonation attacks. So, he invested in Tessian.

Tessian Defender analyzes up to 12 months of historical email data to learn what "normal" looks like. It then uses natural language processing, behavioral analysis, and communication analysis to determine if a particular email is suspicious or not **in real-time.**

To learn more, read the data sheet.



> “We like to empower our users and we like that, with Tessian, our users learn and become better and better and better. That’s what we’re trying to do at SPG Dry Cooling. We’re trying to train and educate our users as much as possible. We’re trying to be innovative in the ways that we get our users, our company, our members, *everybody*, to better themselves.”

THIERRY CLERENS
Global IT Manager at SPG Dry Cooling

PROBLEM

You can’t train employees to spot *all* phishing attacks.

Tessian also helps employees get better at spotting malicious emails with in-the-moment warnings (written in plain English) that reinforce training by explaining exactly why an email is being flagged.

This feature is especially important to Thierry, who values phishing awareness training but understands it has to be ongoing. In evaluating solutions, he wanted something that would protect his people, while also empowering them to make smarter security decisions.

He found that in Tessian, explaining that “the most interesting feature for me is the user education. You have to train your users. You *have* to help them get better at spotting threats by helping them understand the threats. Tessian does that.”

PROBLEM

It’s nearly impossible for IT teams to manually investigate all potential threats

Before Tessian, Thierry and his team had to manually investigate all emails that employees flagged as suspicious. With limited time and resources – and given the fact that “some are really good and are even hard for IT people to find” – it was nearly impossible for them to keep up.

“The limitation of manually looking at all these emails was that it really hangs on the person. And humans can make mistakes.”

Thierry explained that Tessian extends the capabilities of his team. How?

1. It automatically detects and prevents threats.
2. Domains can be added to the denylist in a single click, before they even land in employee’s mailboxes.
3. Tessian dashboards make it easy for IT to see trends and create targeted security campaigns to help educate users.

Tessian was also easy to deploy.

> “As a part of our proof of concept, Tessian started ingesting historical data about employee’s IP addresses, what emails they normally send, who they normally communicate with. We saw how it was helping in just a few weeks. After that, we connected Tessian to Office 365. It took just 15 minutes.”

THIERRY CLERENS
Global IT Manager at SPG Dry Cooling

Learn more about Tessian's intelligent approach to email security.

Powered by machine learning, Tessian's Cloud Email Security technology understands human behavior and relationships.

GUARDIAN

Automatically detects and prevents misdirected emails.

ENFORCER

Automatically detects and prevents data exfiltration attempts.

DEFENDER

Automatically detects and prevents spear phishing attacks

Importantly, Tessian's technology automatically updates its understanding of human behavior and evolving relationships through continuous analysis and learning of an organization's email network. That means **it gets smarter over time to keep you protected, wherever and however your work.**

Interested in learning more about how Tessian can help secure your email?

REQUEST A DEMO →

CUSTOMER STORIES →

TESSIAN

TESSIAN.COM/CUSTOMERS →