Fatima: The importance of communication during incident response

My name is Fatima, and I'm a tech lead manager on Google's Detection and Response Team.
If there is a hacker on the network, our job is to find them.
Working in detection is really like an artist preparing for a show.
We spend all this time developing all of these signatures to detect hackers, and then one day, it's time for the show.
You get that same nervous energy and your question whether you're ready for the performance or not, but you really don't have a choice.
The hackers are going to come and you have to be ready for them.
I would say cybersecurity is very exciting.
You never know when the next vulnerability is going to be released.
You never know when the next incident is going to happen.
A great example of an incident would be the Log4j vulnerability that happened in 2021.
The entire company came together to investigate whether or not we were affected by this vulnerability.
It was my team's job to make that determination.
We ingest hundreds of millions of lines of logs per second.
After we have these logs, it requires hunting and log diving through them, creating different signatures to match against these logs.
For signs of compromise, we were able to say all clear, we are not impacted by this and we're safe.
Those are the moments. Those are the highlights.
That's where everything comes together.
Teamwork in an incident response scenario, is key.
You cannot run an incident response without a really solid team,
a team that works really well together, a team that really trust each other.
The way to maintain clear and effective communication is by communicating a lot.
During an incident it's a little bit counterintuitive, but the people who are the more senior engineers,
these people become the operational leads.
They are the people who are responsible for making sure that the communication is not breaking down within their function.
So, we shift roles from being very technical to really focusing on the communication, aggregating the data, and surfacing the data to the right people who need to know about it.
I definitely recommend cybersecurity as a career field because really the attackers, they're not going to let you get bored because they are very creative, so we have to be creative in the way

that we go out looking for them.
Being a person who likes to learn, knowing that there's always going to be a thing for me to learn and become good at, that's exciting and that keeps me motivated.

Revision #1
Created 5 September 2023 10:25:06 by naruzkurai
Updated 1 November 2023 01:10:46 by naruzkurai