Problem:
Millions of endpoints feed our cloud systems with a huge amount of data related to malware detections, ransomware detections, suspicious activities and other relevant security events, every day.
We process this data efficiently and we index it to allow company’s IT departments to search, analyze (and respond) to cyber threats targeting their businesses, in an effortless and elegant manner, using our API.

Goal:
Be part of the Cloud services team and help to improve our backend applications and our API offering.
Design and implement new components to extend our cloud-based services.

Tasks:
- Design, implement and test production-ready backend components
- Improve and optimize our systems
- Collaborate with Dev, Quality Assurance, Test Automation, Site Reliability Engineering departments throughout all the software development lifecycle to transform a set of requirements into a running application used by millions.

Technologies used:
- Java, Golang, Node.js
- SQL, noSQL (DynamoDB, mongoDB), Redis
- Kafka, SQS, Pub/Sub

Requirements for the intern:
- Be able to think at scale. The system you’ll build will be under heavy load once deployed
- Experience with monitoring applications (APM, metrics)
- Experience with Java, Golang or Node.js
- Experience with GIT
- Experienced in server-side development
- Experience with asynchronous processing, data streaming, distributed environments, microservices architecture (if you don’t have, it is enough to be willing to learn!)
- Algorithms (complexity analysis) and data structures knowledge is required

Comments: We are looking for people who like complex challenges and solving them in elegant ways. Experience is helpful, but not critical. As an intern, your attitude and willingness to learn are what matter the most.
You will be assigned to a project that matches your skills and you will work in a team throughout the SDLC.