At Microsoft, you’ll have access to vast amounts of threat-related data from hundreds of millions of endpoints and other sources. You will have the opportunity to collaborate with partners across Microsoft who have decades of security and ML expertise. We also offer many company-sponsored classes and conferences that focus on data science, ML, and engineering excellence. Microsoft provides phenomenal community, tools, and technologists to grow your expertise in this field. Best of all, on the MDE team, you'll be able to apply that expertise to protecting people. Responsibilities Code in C# near-production level cybersecurity detector logic Monitor and analyze protection big data to uncover protection gaps Build a holistic understanding of our products, features, customers, data infrastructure, and business goals Understand business performance as well as answer questions to drive product actions Code end-to-end rule-based, automation, statistical, or machine learning pipelines for turning raw data into protection value for customers Define and implement measures and dashboards that accurately quantify the value of improvements Provide technical leadership to our team by reviewing problem sets, proposing solutions, and reviewing experiments and data Qualifications Applicants early in career or without industry experience are welcome to apply. Required Qualifications: Bachelor’s or master’s degree or higher or equivalent experience in Data Science, Statistics, Applied Mathematics, Computer Science, Engineering, or another data-focused field Strong coding skills in C# or Java Knowledgeable in machine learning and statistical concepts Knowledgeable in data technology such as SQL, Spark, or similar Experience with ML frameworks, such as PyTorch, Tensorflow, scikit-learn, or similar Preferred Qualifications: Experience in cybersecurity a bonus Ability to meet Microsoft, customer and/or government security screening requirements are required for this role.