Rook

Project Sponsors

Mat Gangwer

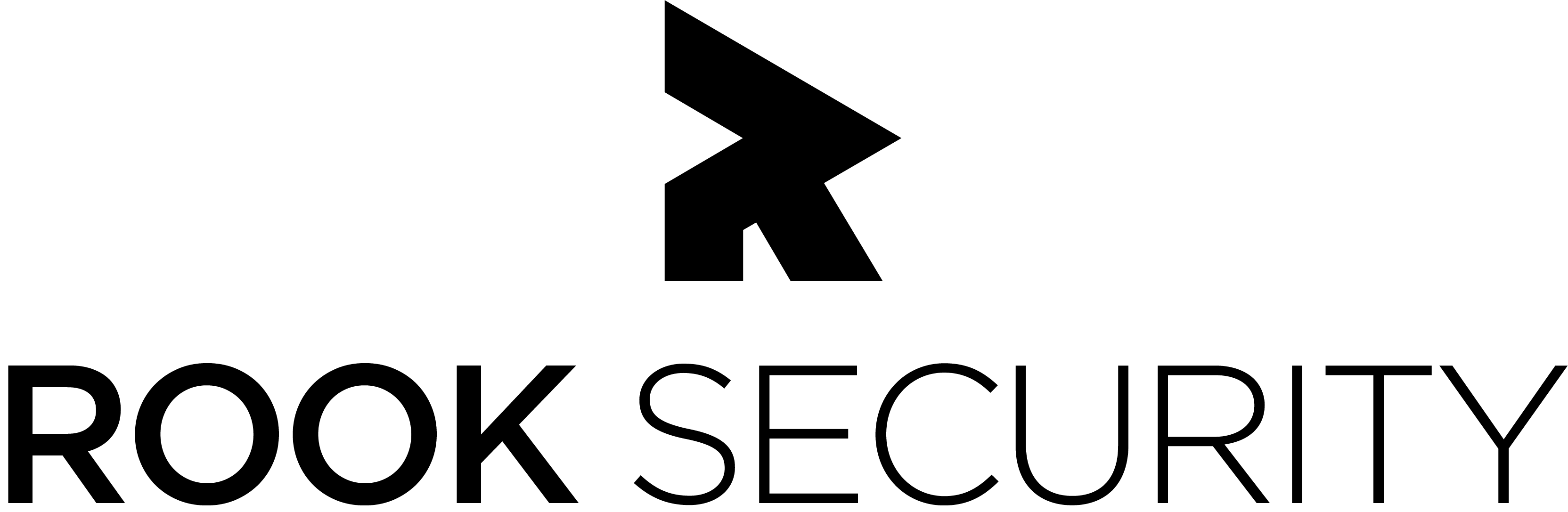
Indianapolis, Indiana

Michael Taylor

Indianapolis, Indiana

J.J. Thompson

Indianapolis, Indiana



Rook Security is a managed threat response force that is dedicated to providing global IT security solutions that anticipate, manage and eliminate threats.

Our Cloud Security Event Processing and Alerting Platform analyzes log information from a client’s computer network looking for security related events. Rook receives millions of these events that must be parsed and correlated into discrete incidents.

Our system provides a web interface that enables Rook engineers to edit existing correlation rules and to examine how these new rules perform, making it easier and more efficient to onboard new clients.

In addition, our system leverages Amazon Web Services (AWS) to create a reliable serverless architecture. Manageable from Rook’s Force web platform, our AWS system scales easily and quickly with on-demand computing to accommodate a growing base of clients and sudden surges of incoming network events.

Our Cloud Security Event Processing and Alerting Platform is identical in functionality to Rook’s previous version thereby keeping all of the same protections and making for a seamless transition for Rook’s analysts and customers alike.

The analytical Lambda functions are written in Python. The backend RESTful API leverages the Django framework with the frontend written in JavaScript using Facebook’s React/Redux libraries. The platform takes advantage of multiple Amazon Web Services including Athena, S3 and EC2.

Michigan State University

Team Members (left to right)

Jake Fenton

Kalamazoo, Michigan

Brian Jones

South Lyon, Michigan

Alexander Fall

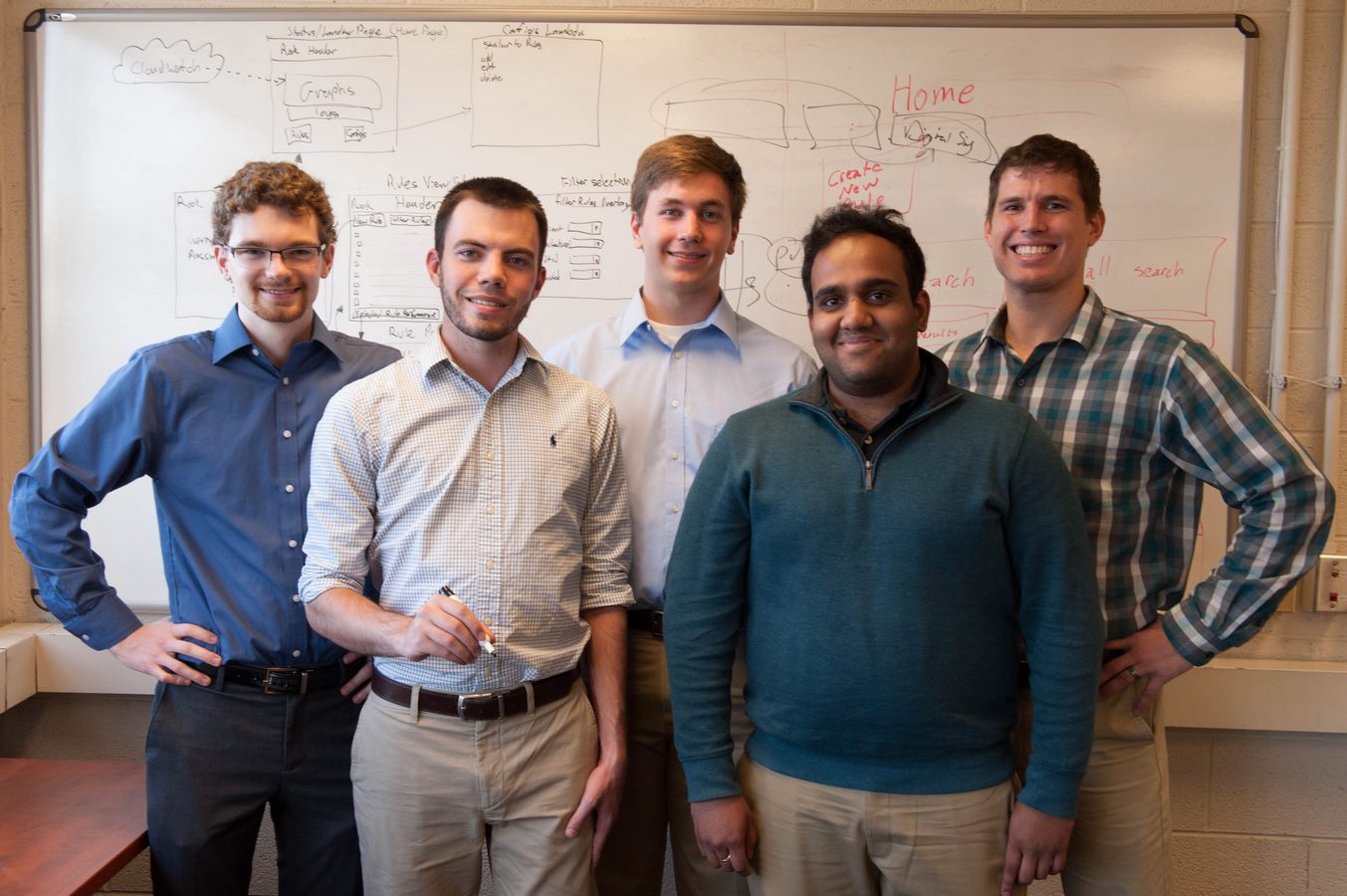
Grand Rapids, Michigan

Kaushik Sridasyam

Troy, Michigan

Bradley Baker

Carleton, Michigan



Rook Security

Cloud Security Event Processing and Alerting Platform

