ISSA
Information Systems Security Association
of Orange County

PRESENTATION	*Automating Security Operations and Alerting in the Cloud using Serverless Technologies*
ABSTRACT	*Full visibility into key operations within the cloud is a must for security. Cloud providers offer a variety of virtual resources for tenants to consume. The majority of these resources provide logging and monitoring capabilities to not only offer a peek into the operational aspect of these services but also provide information about on-going attacks. For example, AWS Virtual Private Cloud (VPC) provides flow Logs that captures information about the IP traffic going to and from network interfaces within the VPC. Using these logs, the tenant can detect various network-level attacks on the cloud infrastructure and workload executing within it. Analyzing these logs to identify attack patterns is like finding a needle in the haystack.* *Further, collecting and storing logs into SIEM and reviewing it daily, weekly, or monthly not only delays attack detection significantly but also require a lot of human resources to analyze billions of records. A real-time or near real-time solution that scans logs continuously and alerts on any on-going attacks drastically reduces the effort from security analysts. In this presentation, I will discuss how to automate log analysis and alerting in the cloud using serverless technologies. Attendees will walk away with an understanding of how various serverless technologies can help design data analytics pipeline and use slack and other messaging systems to respond to generated alerts in real-time.*
ORIGINAL BROADCAST	September 17, 2020 @ 8:20 AM PST
SPEAKER	Abhinav Srivastava, VP and Head of Information Security & Infrastructure at Frame.io
BIO	*Abhinav Srivastava is a VP and the Head of Information Security & Infrastructure at Frame.io, where he manages security, infrastructure, and IT departments. At Frame, he is building the security and infrastructure programs from the ground up — making sure that Frame.io is secure and compliant, and its services are available and reliable. Before joining Frame.io, Abhinav spent six years in AT&T Shannon Labs as a Principal Researcher working on systems, cloud, IoT, and network security projects. He authored 30+ research papers in peer-reviewed conferences and journals and held multiple patents. Abhinav earned a Ph.D. degree in Computer Science from Georgia Tech.*
LINK TO RECORDING	https://issaoc.sharepoint.com/:v:/g/EZ_GsPMVQmFDvJ2NN121wdMBAsRCPxZv_TNIadPiYYlGwg