Monday, October 19	
12:15 – 1:00 pm	*Keynote* Emily Fox
Tuesday, October 20	
6:00 – 8:00 pm	**Afternoon Workshop – Shaun McCullough**
Wednesday, October 21	
5:30 – 5:50 pm	**Attacking AWS: the full cyber kill chain** **Pawel Rzepa**, Senior Security Specialist, SecuRing While it is quite common practice to do periodic security assessments of local network, it is really rare to find a company who puts the same effort for testing the security in their cloud. According to Gartner report: through 2022, at least 95% of cloud security failures will be the customer's fault. This is why we have to understand what new threats and risks appeared with the cloud and how should we change our attitude to testing cloud security. The goal of my presentation is to show how security assessment of cloud infrastructure is different from testing environments in classic architecture. I'll demonstrate a hypothetical attack on a company which is fully deployed in the AWS environment. I'm going to show whole kill chain starting from presenting cloud-applicable reconnaissance techniques. Then I'll attack the Jenkins server hosted on EC2 instance to access its metadata and steal the access keys. Using the assigned role, I'll access another AWS service to escalate privileges to administrator and then present how to hide fingerprints in CloudTrail service. Finally, I'll demonstrate various techniques of silent exfiltrating data from AWS environment, setting up persistent access and describe other potential, cloud-specific threats, e.g. cryptojacking. The presentation shows practical aspects of attacking cloud services and each step of the kill chain will be presented in a form of live demo. On the examples of presented attacks, I'll show how to use AWS exploitation framework Pacu and other handy scripts.

6:00 – 6:20 pm	**Integrating Policy as code into your CI/CD pipeline** **Barak Schoster**, Co-founder & CTO, Bridgecrew With the growth of cloud and API-driven infrastructure, came infrastructure as code. This movement shifted the management of configuration to a larger and more explicit part of software development. In this talk, we'll cover the possible issues on cloud infrastructure configurations and some practical ways to identify them in your CI/CD pipeline demonstrating using https://github.com/bridgecrewio/terragoat and https://github.com/bridgecrewio/checkov
6:30 – 6:50 pm	**Serverless is the New Black: Common threat vectors, detections, and defenses** **Travis Altman**, Cyber Security Leader, OWASP Industry trends show that serverless architectures are gaining in popularity. Organizations are always on the hunt to save money and leveraging runtime environments instead of virtual servers helps reduce that cost. What happens when organizations change their architecture to this new paradigm? What risks are they introducing and what can they do to protect against these risks? This talk will perform a deep dive into how attackers are taking advantage of serverless applications and systems. It will go into the various tactics and techniques that have been seen in the wild where threat actors are leveraging common weaknesses within serverless systems to gain a larger foothold within the environment. This talk will focus on AWS serverless architecture but the core concepts will apply across multiple cloud provider solutions.
Thursday, October 22	
5:30 – 5:50 pm	**Securing Serverless with Terrascan** **Cesar Rodriguez,** Head of Developer Advocacy, Accuric As development teams move to serverless architectures, how does this change the way security is handled vs traditional infrastructure? In this talk we'll walk through how security controls can be embedded into serverless architectures and how Terrascan, an open source static code analyzer for Infrastructure as Code, can help find security issues in your serverless infrastructure before it's deployed.
6:00 – 6:20 pm	**What I have learned writing Prowler** **Toni de la Fuente**, Senior Security Consultant, AWS

	Prowler is an AWS security assessment Open Source tool that helps cloud security auditors to know the security status of their resources in the AWS cloud. I want to share all what I have learned during the last 3 years, not only in terms of Open Source and such but also around use cases, community, AWS security, AWS services APIs, AWS command line interface and security in general. What mistakes I've made and what would be different if I start it again. This talk will help attendees to make better decisions and fail earlier if they start the journey of building their own security tools.
6:30 – 6:50 pm	**Architecting for Threat Hunting** **Shaun McCullough**, Developer Improve your Threat Hunting success through architecture and operations. This talk will highlight architecture design patterns, DevSecOps pipelines, and the Cloud's automatable infrastructure to mitigate the threat and make attacker behaviors stand out.