Managing AWS Logs with Elastic Stack

Description: Learn how to send AWS logs to an off-site (meaning not at AWS) Logstash (ELK) stack. We use this setup in my company for reviewing security logs in our multiple AWS environments. Although AWS offers an elasticsearch as a service inside AWS for our security operations center we need both our cloud and on-premise (company data centers) security log events all in one place.

Course Outline:

- Introduction into AWS logging options
- Real cost of “free tiers” in AWS
- Setup of student’s AWS accounts
- Enabling CloudTrail
- Setup of IAM service account for Logstash
- Spinning up “outside AWS” VM for ELK install
- Installing ELK
- Review of S3 buck in AWS
- Configure Logstash to consume AWS logs
- Setup the Kibana interface
- Generate security events in AWS
- View the log events in Kibana
- Useful security event filters
- AWS native logging & alerting alternatives
- Review CloudWatch (and pricing)
- Review SNS alerting
- Alternative open source tool: SecurityMonkey
- Limits of SecurityMonkey
- Tools to auto-rotate API keys located outside AWS

Required materials:

- Students must bring a laptop
  - Wifi capability
  - Students should bring an ethernet cable as a backup
  - VMWare Player/Workstation or VirtualBox or equivalent software for running a Linux virtual machine
  - Students should bring the necessary Linux distro VM already installed (probably CentOS 7 64-bit minimal for headless server)
  - The VM needs to be able to install an ELK v5 stack
  - Alternative: Students can (at their own cost) run the VM in AWS as an EC2 instance
- Students will be provided with an Amazon gift code to pay for necessary AWS costs.