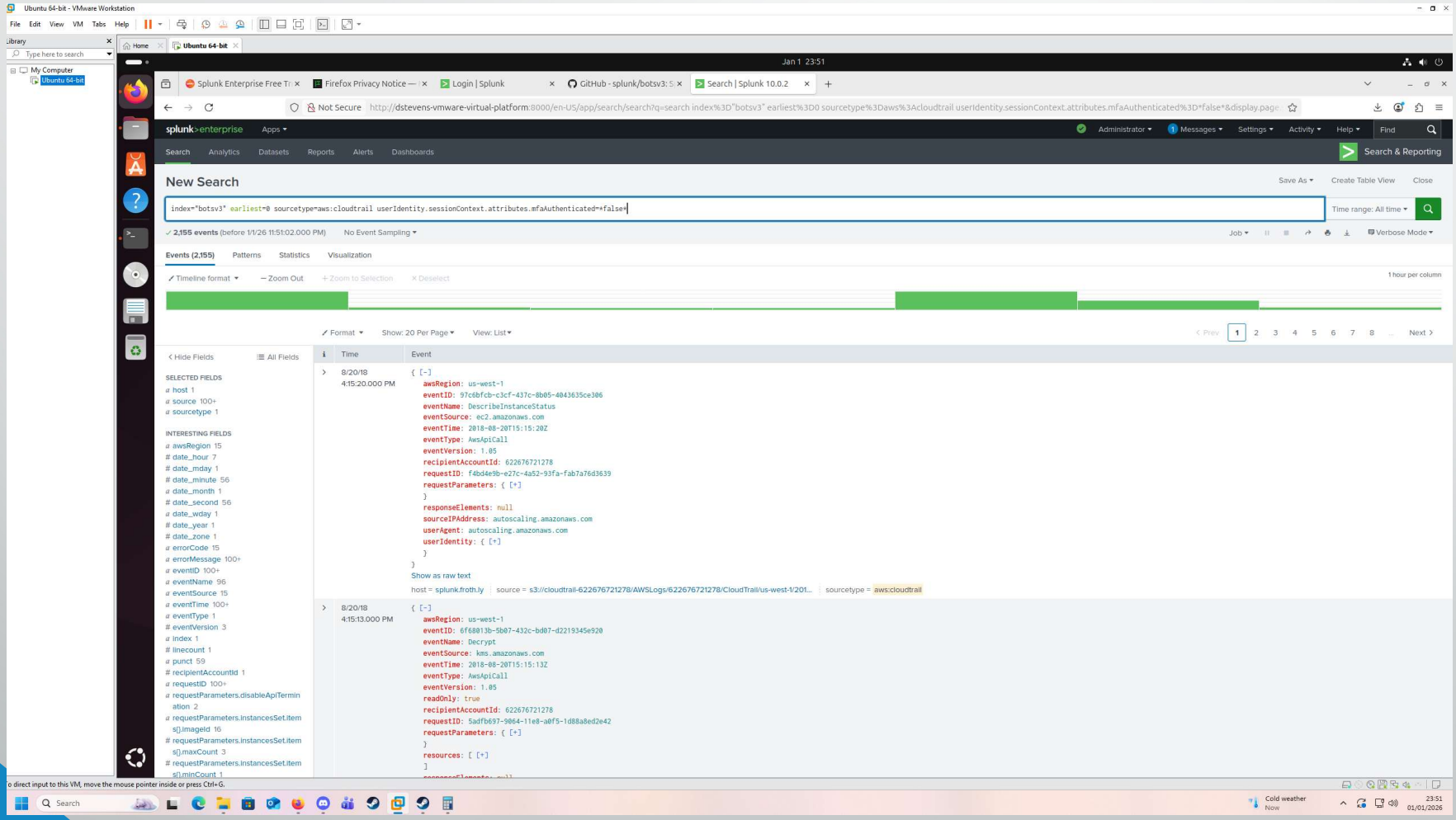
Botsv3 Dataset exercise

D. Stevens

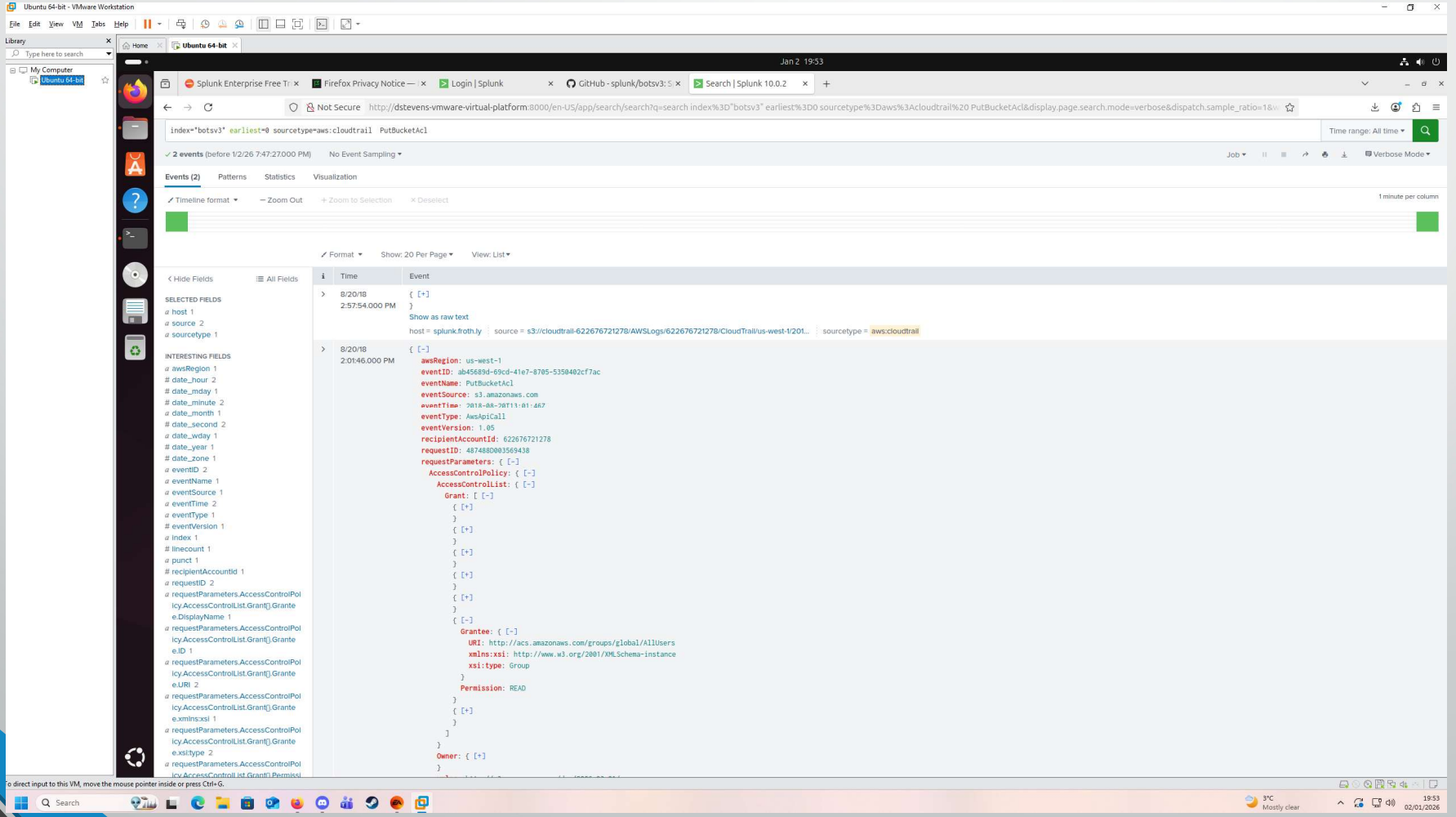
Key findings

- 4 IAM users using the service
- API calls made without MFA
- S3 Bucket made public by user bstoll
- During public access, a file called “OPEN_BUCKET_PLEASE_FIX.txt” was uploaded

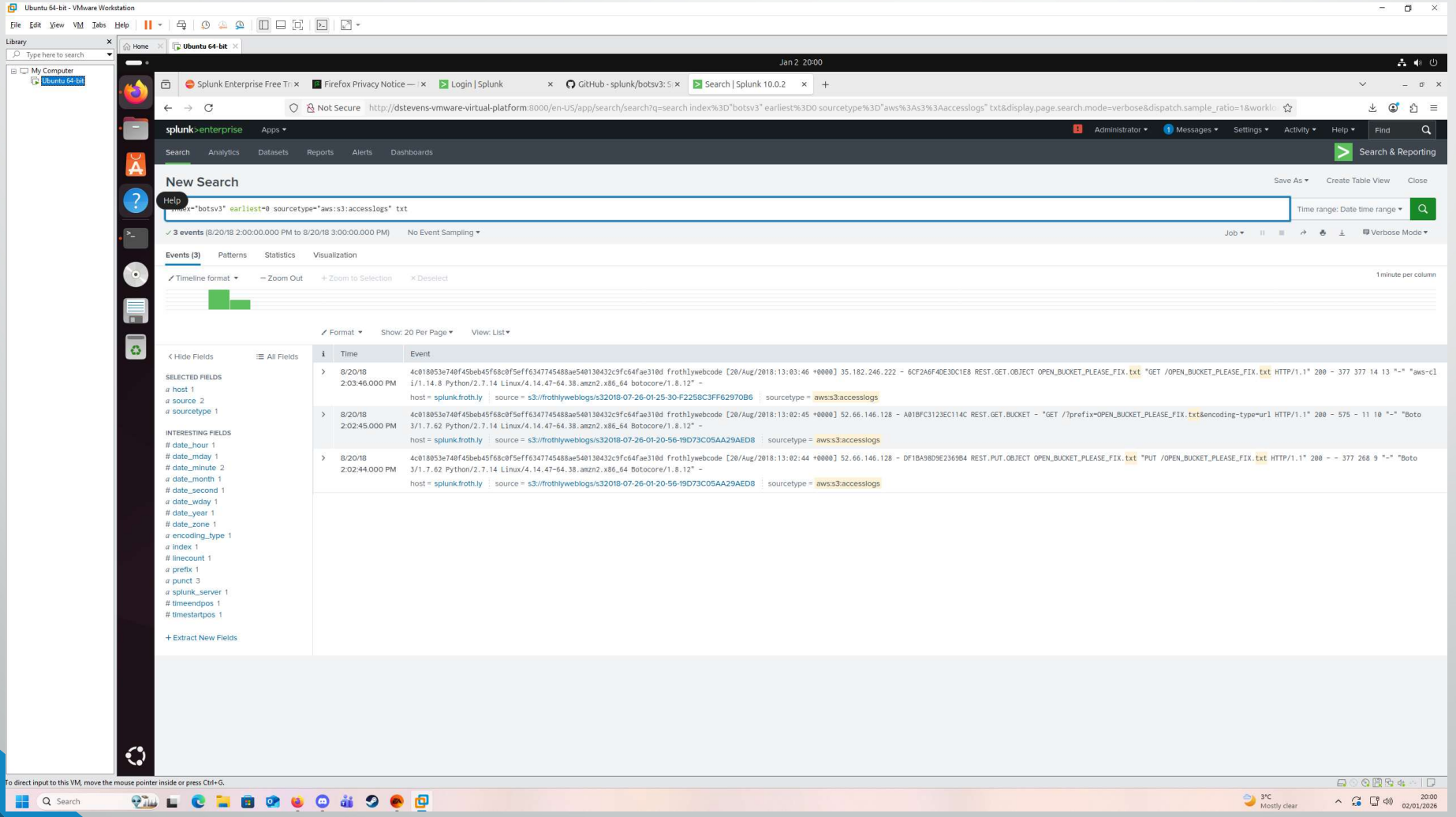
Key Queries: No MFA authentication



Key Queries: PutBucketAcl



Key Queries: Files uploaded



Reflection on SOC operations and incident response lessons

- Comprehensive and rigorous event logging aids massively in investigation
- SIEM tools like Splunk greatly hastens investigation and response to threats and allows easy following problem to the source
- The act of responding to a breach can give ideas for prevention strategies not necessarily relevant to the breach.