

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

The screenshot shows a Splunk Enterprise Free Edition interface running on an Ubuntu 64-bit VM. The search bar contains the query: `index=botsv3 earliest=0 sourcetypeaws:cloudtrail userIdentity.sessionContext.attributes.mfaAuthenticated=false`. The results show 2,155 events from January 1, 2018, at 15:20:00 PM. The event details are displayed in a table format, showing fields like awsRegion, eventID, eventName, eventSource, eventTime, eventType, eventVersion, recipientAccountId, requestId, requestParameters, responseElements, sourceIPAddress, userAgent, and userIdentity. Two specific events are expanded:

```
awsRegion: us-west-1
eventID: 97c6fcfc-c1cf-437c-8b85-4043635ce306
eventName: DescribeInstanceStatus
eventSource: ec2.amazonaws.com
eventTime: 2018-08-20T15:15:20Z
eventType: AwsApiCall
eventVersion: 1.0
recipientAccountId: 622676721278
requestID: fbd4de9b-e27c-4a52-93fa-fab7a76d3639
requestParameters: [{}]
responseElements: null
sourceIPAddress: autoscaling.amazonaws.com
userAgent: autoscaling.amazonaws.com
userIdentity: { [1] }
```

```
awsRegion: us-west-1
eventID: 6f68013b-5b07-432c-bd07-d2219345e920
eventName: Decrypt
eventSource: kms.amazonaws.com
eventTime: 2018-08-20T15:15:13Z
eventType: AwsApiCall
eventVersion: 1.0S
readonly: true
recipientAccountId: 622676721278
requestID: 5adfb697-9064-11e8-af05-1d88a8ed2e42
requestParameters: [{}]
resources: [{}]
```

Key Queries: PutBucketAcl

The screenshot shows a VMware workstation window running an Ubuntu 64-bit VM. Inside the VM, a Firefox browser is open to a Splunk search interface. The search query is:

```
index="botsv3" earliest=0 sourcetype=aws:cloudtrail PutBucketAcl
```

The search results show two events from Jan 2, 2018:

- Event 1:** Occurred at 2:57:54.000 PM. The event ID is ab45689d-8cd-41e7-8705-535b0402cf7ac. It was triggered by a PutBucketAcl API call from the source `s3.amazonaws.com` at event time 2018-01-02T14:57:54Z. The event type is AwsApiCall, version 1.05. The request ID is 4874880803569438. The request parameters include:
 - AccessControlPolicy: []
 - AccessControlList: []
 - Grant: []
 - Grantee: []
 - URI: http://acs.amazonaws.com/groups/global/allUsers
 - xmns xsi: http://www.w3.org/2001/XMLSchema-instance
 - xs:type: Group
 - Permission: READ
- Event 2:** Occurred at 2:01:46.000 PM. The event ID is ab45689d-8cd-41e7-8705-535b0402cf7ac. It was triggered by a PutBucketAcl API call from the source `s3.amazonaws.com` at event time 2018-01-02T14:01:46Z. The event type is AwsApiCall, version 1.05. The request ID is 4874880803569438. The request parameters include:
 - AccessControlPolicy: []
 - AccessControlList: []
 - Grant: []
 - Grantee: []
 - URI: http://acs.amazonaws.com/groups/global/allUsers
 - xmns xsi: http://www.w3.org/2001/XMLSchema-instance
 - xs:type: Group
 - Permission: READ

Key Queries: Files uploaded

The screenshot shows a Splunk search interface running on an Ubuntu 64-bit VM. The search bar contains the query: `index="botsv3" earliest=0 sourcetype="aws:s3:accesslogs" txt`. The results table displays four log entries from August 20, 2018, at various times between 2:03:46 PM and 2:04:44 PM. Each entry includes fields like host, source, and event, indicating REST API calls to AWS S3 buckets.

Time	Event
2018-08-20T14:03:46.000Z	host = splunk.frothly source = s3://frothlyweblogs/s32018-07-26-01-25-30-F225C3FF62970B6 sourcetype = aws:s3:accesslogs
2018-08-20T14:02:45.000Z	host = splunk.frothly source = s3://frothlyweblogs/s32018-07-26-01-20-56-19D73C05AA29AEDB sourcetype = aws:s3:accesslogs
2018-08-20T14:02:44.000Z	host = splunk.frothly source = s3://frothlyweblogs/s32018-07-26-01-20-56-19D73C05AA29AEDB sourcetype = aws:s3:accesslogs

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.