



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 search interface within a VMware Workstation environment. The search query is: `index="botsv3" earliest=0 sourcetype=aws:cloudtrail userIdentity.sessionContext.attributes.mfaAuthenticated=false`. The results show two events from AWS CloudTrail logs.

Event 1:

- Time: 8/20/18 4:15:20.000 PM
- awsRegion: us-west-1
- eventId: 97c0fcb-c1cf-437c-8685-4843635ce386
- eventName: DescribeInstanceStatus
- eventSource: ec2.amazonaws.com
- eventTime: 2018-08-20T15:15:20Z
- eventType: AwsApiCall
- eventVersion: 1.05
- recipientAccountId: 622676721278
- requestId: f4b0ee9b-e27c-4a52-93fa-fab7a76d9639
- requestParameters: { [] }
- responseElements: null
- sourceIPAddress: autoscaling.amazonaws.com
- userAgent: autoscaling.amazonaws.com
- userIdentity: { [] }

Event 2:

- Time: 8/20/18 4:15:13.000 PM
- awsRegion: us-west-1
- eventId: 8f688138-3847-432c-bd87-d2219345e928
- eventName: Decrypt
- eventSource: kms.amazonaws.com
- eventTime: 2018-08-20T15:15:13Z
- eventType: AwsApiCall
- eventVersion: 1.05
- readOnly: true
- recipientAccountId: 622676721278
- requestId: 5a0f857-9864-11e8-a0f5-1d88a8ed2e42
- requestParameters: { [] }
- resources: [[]]
- responseElements: null

Key Queries: PutBucketAcl

The screenshot displays a Splunk search interface within a VMware Workstation environment. The search bar contains the query: `Index="botsv3" earliest=0 sourcetype=aws:cloudtrail PutBucketAcl`. The search results show two events. The first event is a raw text log entry from `splunk:trfthly`. The second event is a structured JSON log entry from `aws:cloudtrail` detailing a `PutBucketAcl` operation.

Event 1 (Raw Text):

```
{
  "Time": "8/20/18 2:57:54.000 PM",
  "Event": "Show as raw text"
}
```

Event 2 (Structured JSON):

```
{
  "Time": "8/20/18 2:01:46.000 PM",
  "Event": {
    "awsRegion": "us-west-1",
    "eventID": "ab45689d-69cd-41e7-8705-5358402cf7ac",
    "eventName": "PutBucketAcl",
    "eventSource": "s3.amazonaws.com",
    "eventTime": "2018-08-20T11:01:46Z",
    "eventType": "AwsApiCall",
    "eventVersion": "1.05",
    "recipientAccountId": "622676721278",
    "requestID": "4874880003569438",
    "requestParameters": {
      "AccessControlPolicy": {
        "AccessControlList": {
          "Grant": [
            {
              "Grantee": {
                "URI": "http://acs.amazonaws.com/groups/global/AllUsers",
                "xmlns:xsi": "http://www.w3.org/2001/XMLSchema-instance",
                "xsi:type": "Group"
              },
              "Permission": "READ"
            }
          ]
        },
        "Owner": {
          "xsi:type": "Group"
        }
      }
    }
  }
}
```

The interface also shows a sidebar with field lists and a bottom status bar indicating the system temperature and time.

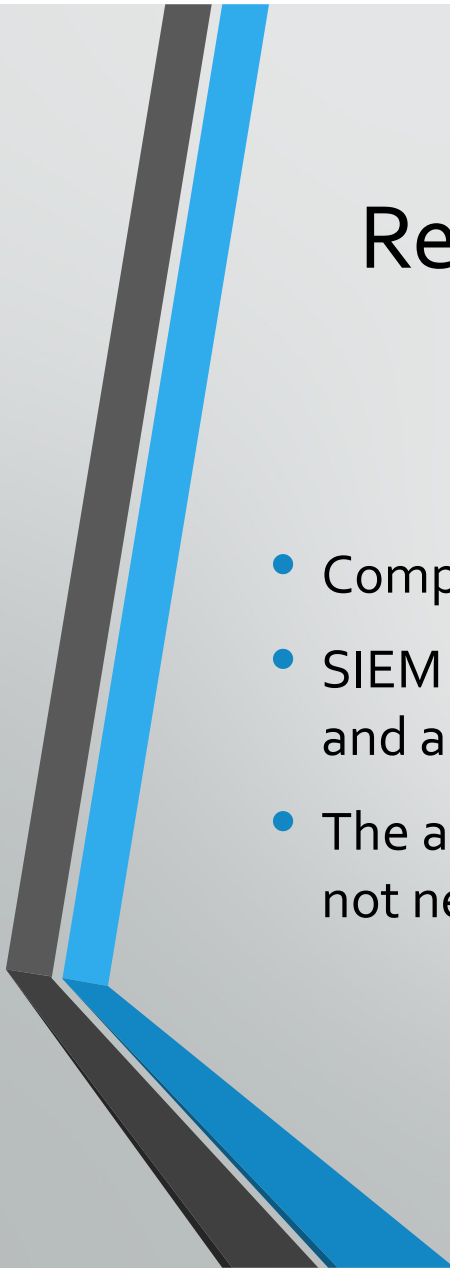
Key Queries: Files uploaded

The screenshot displays a Splunk Enterprise search interface within a VMware Workstation environment. The search query is `index="botsv3" earliest=0 sourcetype="aws:s3:accesslogs" txt`. The results show three events from 8/20/18, detailing file uploads to an S3 bucket. The left sidebar lists selected fields and interesting fields. The bottom status bar indicates the system is at 3°C and 20:00 on 02/01/2026.

Search Query: `index="botsv3" earliest=0 sourcetype="aws:s3:accesslogs" txt`

Results: 3 events (8/20/18 2:00:00.000 PM to 8/20/18 3:00:00.000 PM)

Time	Event
8/20/18 2:03:46.000 PM	4c018053e740f45beb45f68c9f5eff6347745488ae540130432c9fc64fae310d frothywebcode [20/Aug/2018:13:03:46 +0000] 35.182.246.222 - 6CF2A6F4DE30C1E8 REST.GET.OBJECT OPEN_BUCKET_PLEASE_FIX.txt "GET /OPEN_BUCKET_PLEASE_FIX.txt HTTP/1.1" 200 - 377 377 14 13 "-" "aws-c1i/1.14.8 Python/2.7.14 Linux/4.14.47-64.38.amzn2.x86_64 boto/1.8.12" - host = splunk.frothy source = s3://frothyweblogs/s32018-07-26-01-25-30-F2258C3FF62970B6 sourcetype = aws:s3:accesslogs
8/20/18 2:02:45.000 PM	4c018053e740f45beb45f68c9f5eff6347745488ae540130432c9fc64fae310d frothywebcode [20/Aug/2018:13:02:45 +0000] 52.66.146.128 - A01BF3C123EC114C REST.GET.BUCKET - "GET /?prefix=OPEN_BUCKET_PLEASE_FIX.txt&encoding-type=url HTTP/1.1" 200 - 575 - 11 10 "-" "Boto/3.1.7.62 Python/2.7.14 Linux/4.14.47-64.38.amzn2.x86_64 Boto/1.8.12" - host = splunk.frothy source = s3://frothyweblogs/s32018-07-26-01-20-56-19D73C05AA29AED8 sourcetype = aws:s3:accesslogs
8/20/18 2:02:44.000 PM	4c018053e740f45beb45f68c9f5eff6347745488ae540130432c9fc64fae310d frothywebcode [20/Aug/2018:13:02:44 +0000] 52.66.146.128 - DF1BA98D9E2369B4 REST.PUT.OBJECT OPEN_BUCKET_PLEASE_FIX.txt "PUT /OPEN_BUCKET_PLEASE_FIX.txt HTTP/1.1" 200 - - 377 268 9 "-" "Boto/3.1.7.62 Python/2.7.14 Linux/4.14.47-64.38.amzn2.x86_64 Boto/1.8.12" - host = splunk.frothy source = s3://frothyweblogs/s32018-07-26-01-20-56-19D73C05AA29AED8 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.