

Answers to the 200-level Questions

Question 1: Which IAM users used AWS services?

Answer: bstoll,btun,splunk_access,web_admin

Search used: `index=botsv3 sourcetype=aws:cloudtrail | stats count by userIdentity.userName | sort userIdentity.userName`

The screenshot shows the Splunk Enterprise search interface. At the top, it displays "splunk>enterprise" and "應用套件 ▾". Below the header is a navigation bar with tabs: 搜尋 (selected), 分析, 資料集, 報告, 較示, and 儀表板. A green horizontal bar highlights the "搜尋" tab. The main area is titled "新搜尋" (New Search). In the search bar, the query `index=botsv3 sourcetype=aws:cloudtrail earliest=0` is entered.

```
> 18/08/20      { [-]
  23:15:04.000
    awsRegion: us-west-1
    eventID: 51b2664e-dd61-4db3-ab77-31b...
    eventName: DescribeSecurityGroups
    eventSource: ec2.amazonaws.com
    eventTime: 2018-08-20T15:15:04Z
    eventType: AwsApiCall
    eventVersion: 1.05
    recipientAccountId: 622676721278
    requestID: 11a2f0a0-78b1-4968-8887-4...
    requestParameters: { [+]
    }
    responseElements: null
    sourceIPAddress: 107.77.212.175
    userAgent: signin.amazonaws.com
    userIdentity: { [-]
      accessKeyId: ASIAZB6TMXZ7FYCAEHN...
      accountId: 622676721278
      arn: arn:aws:iam::622676721278:use...
      invokedBy: signin.amazonaws.com
      principalId: AIDAJUFKXZ44LV4EN4MG...
      sessionContext: { [+]
      }
      type: IAMUser
      userName: bstoll
    }
  }
```

Pay attention to userName

The screenshot shows the Splunk Enterprise search interface. The search bar contains the query: `index=botsv3 sourcetype=aws:cloudtrail | stats count by userIdentity.userName | sort userIdentity.userName`. Below the search bar, it says "✓ 6,571 個事件 (10/01/01 0:00:00.000 至 20/01/01 0:00:00.000)" and "無事件取樣". The "統計資料 (4)" tab is selected. At the bottom, there is a list of user identities: bstoll, btun, splunk_access, and web_admin.

Why it matters: In a real company, SOC must watch who is using cloud accounts. Strange users or too many actions can be signs of hacking.

Question 2: Which field shows if someone did NOT use MFA?

Answer: `userIdentity.sessionContext.attributes.mfaAuthenticated`

The screenshot shows the Splunk Enterprise search interface. The search bar contains the query: `index=botsv3 sourcetype=aws:cloudtrail earliest=0`.

```
> 18/08/20      { [-]
23:15:20.000    awsRegion: us-west-1
                  eventID: 97c6bfcb-c3cf-437c-8b05-4043635ce306
                  eventName: DescribeInstanceStatus
                  eventSource: ec2.amazonaws.com
                  eventTime: 2018-08-20T15:15:20Z
                  eventType: AwsApiCall
                  eventVersion: 1.05
                  recipientAccountId: 622676721278
                  requestID: f4bd4e9b-e27c-4a52-93fa-fab7a76d3639
                  requestParameters: { [+]
}
                  responseElements: null
                  sourceIPAddress: autoscaling.amazonaws.com
                  userAgent: autoscaling.amazonaws.com
                  userIdentity: { [-]
                      accountId: 622676721278
                      arn: arn:aws:sts::622676721278:assumed-role/AWS
                      invokedBy: autoscaling.amazonaws.com
                      principalId: AROAIOHK7E4SHKYSVYLM:AutoScaling
                      sessionContext: { [-]
                          attributes: { [-]
                              creationDate: 2018-08-20T15:09:21Z
                              mfaAuthenticated: false
}
                          sessionIssuer: { [+]
}
}
                      type: AssumedRole
}
}
```

Pay attention at mfaAuthenticated

splunk>enterprise 應用套件 ▾

搜尋 分析 資料集 報告 警示 儀表板

新搜尋

```
index=botsv3 sourcetype=aws:cloudtrail earliest=0  
| table userIdentity.sessionContext.attributes.mfaAuthenticated
```

✓ 6,571 個事件 (10/01/01 0:00:00.000 至 20/01/01 0:00:00.000) 無事件取樣 ▾

事件 樣式 統計資料 (6,571) 視覺化

顯示: 20 每頁 ▾ 格式 ▾ 預覽: 開

userIdentity.sessionContext.attributes.mfaAuthenticated ▾

userIdentity.sessionContext.attributes.mfaAuthenticated
false

MfaAuthentication: false

Why it matters: Without MFA, stolen passwords are very dangerous. SOC should make an alert for any important action done without MFA.

Question 3: What CPU model is on the web servers?

Answer: E5-2676

The screenshot shows a Splunk search interface with the following search bar query: `index=botsv3 sourcetype=hardware earliest=0`. Below the search bar, it says "3 個事件 (26/02/12 19:00:11.000 之前)" and "無事件取樣". The main area displays a table with three columns: "事件 (3)", "樣式", "統計資料", and "視覺化". Under "時間表格式", there are buttons for "縮小" and "取消選擇". The table header includes "時間" and "事件". The table body shows the following data:

	時間	事件
	18/08/20 22:26:25.000	KEY VALUE CPU_TYPE Intel(R) Xeon(R) CPU E5-2676 v3 @ 2.40GHz CPU_CACHE 30720 KB CPU_COUNT 2 HARD_DRIVES xvda 8 GB; 顯示全部 9 行
		host = gacrux.i-09cbc261e84259b54 source = hardware sourcetype = hardware

Why it matters: Knowing normal hardware helps SOC notice strange things, for example if CPU usage suddenly goes very high because of malware.

Question 4: What is the Event ID that made the S3 bucket public?

Answer: ab45689d-69cd-41e7-8705-5350402cf7ac

The screenshot shows a new search interface in Splunk with the following search bar query: `index=botsv3 sourcetype=aws:cloudtrail eventName=PutBucketAcl earliest=0`. The interface includes a navigation bar with tabs: 搜尋, 分析, 資料集, 報告, 警示, 儀表板. Below the search bar, it says "新搜尋".

```

{ [-]
  Grantee: { [-]
    URI: http://acs.amazonaws.com/groups/global/AllUsers
    xmlns:xsi: http://www.w3.org/2001/XMLSchema-instance
    xsi:type: Group
  }
  Permission: READ
}
{ [-]
  Grantee: { [-]
    URI: http://acs.amazonaws.com/groups/global/AllUsers
    xmlns:xsi: http://www.w3.org/2001/XMLSchema-instance
    xsi:type: Group
  }
  Permission: WRITE
}
]
}

```

Pay attention at /AllUsers

Why it matters: This ID proves exactly when and how the security mistake happened.

Question 5: What is Bud's username?

Answer: bstoll

_time	eventID	userIdentity.userName	requestParameters.bucketName
2018/08/20 21:57:54	9a33d8df-1e16-4d58-b36d-8e80ce68f8a3	bstoll	frothlywebcode
2018/08/20 21:01:46	ab45689d-69cd-41e7-8705-5350402cf7ac	bstoll	frothlywebcode

Why it matters: We can see it was probably an accident by an employee, not an outside hacker.

Question 6: What is the name of the public S3 bucket?

Answer: frothlywebcode

The screenshot shows a Splunk search interface with the following details:

- Search Query:** index=botsv3 sourcetype=aws:cloudtrail eventName=PutBucketAcl earliest=0
- Results:** 2 個事件 (26/02/10 22:41:52.000 之前) 無事件取樣 ▾
- Event Details:**

_time	eventID	userIdentity.userName	requestParameters.bucketName
2018/02/20 21:57:54	9a33d8df-1e16-4d58-b36d-8e80ce68f8a3	bstoll	frothlywebcode
2018/02/20 21:01:46	ab45689d-69cd-41e7-8705-5350402cf7ac	bstoll	frothlywebcode

```
        }
        {
        [-]
        Grantee: [-]
            URI: http://acs.amazonaws.com/groups/global/AllUsers
            xmlns:xsi: http://www.w3.org/2001/XMLSchema-instance
            xsi:type: Group
        }
        Permission: WRITE
    }
]
}
Owner: [-]
    DisplayName: bstoll
    ID: 4c018053e740f45beb45f68c0f5eff6347745488ae540130432c9fc
}
xmlns: http://s3.amazonaws.com/doc/2006-03-01/
}
acl: [-]
]
bucketName: frothlywebcode
}
```

Pay attention at bucketName

Why it matters: Knowing the exact bucket name helps understand how much data was at risk.

Question 7: What text file was uploaded when the bucket was public?

Answer: OPEN_BUCKET_PLEASE_FIX.txt

The screenshot shows a Splunk search interface with the following details:

- Search Bar:** Index=botssv1 sourcetype=s3.accesslogs "frothlywebcode" "PUT" "200" *.txt | sort -time
- Results:** 1 個事件 (18/08/20 21:02:44.000 至 18/08/20 21:02:44.001)
- Event Details:**
 - 時間: 18/08/20 21:02:44.000
 - 事件: 4c918853e740f45beb45f68c0f5eff6347745488ae540130432c9fc64fae310d frothlywebcode [28/Aug/2018:13:02:44 +0000] 52.66.146.128 - DF1BA98D9E2369B4 REST.PUT.0B
JECT OPEN_BUCKET_PLEASE_FIX.txt "PUT /OPEN_BUCKET_PLEASE_FIX.txt HTTP/1.1" 200 - - 377 268 9 "-" *Bot03/1.7.62 Python/2.7.14 Linux/4.14.47-64.38.amzn2.x8
6.64 Botcore/1.8.12" -
host = spunk.froth.ly source = s3://frothlyweblogs/s32018-07-26-01-20-56-19073C05AA29AEDB sourcetype = aws.s3.accesslogs

Why it matters: This shows attackers (or curious people) could download secret files very easily after the mistake.

Question 8: Which computer has a different Windows version?

Answer: bstoll-l.froth.ly

index=botsv3 sourcetype=winhostmon "operatingsystem" earliest=0		
✓ 204 個事件 (26/02/12 19:21:23.000 之前) 無事件取樣 ▾		
事件 (204) 樣式 統計資料 視覺化		
時間表格式 ▾	-縮小	+縮放至選取範圍 × 取消選擇
格式 ▾ 顯示: 20 每頁 ▾ 檢視: 清單 ▾		
◀ 隱藏欄位	所有欄位	i 時間 事件
所選欄位		> 18/08/20 Type=OperatingSystem 23:17:23.000 OS="Microsoft Windows 10 Pro" Architecture="64-bit" Version="10.0.17134" BuildNumber="17134" 顯示全部 22 行 host = FYODOR-L source = operatingsystem sourcetype = WinHostMon
a host 8		
a source 1		
a sourcetype 1		
關注欄位		> 18/08/20 Type=OperatingSystem 23:16:28.000 OS="Microsoft Windows 10 Pro" Architecture="64-bit" Version="10.0.17134" BuildNumber="17134" 顯示全部 22 行 host = JWORTOS-L source = operatingsystem sourcetype = WinHostMon
a Architecture 1		
# BuildNumber 1		
a BuildType 1		
# CodeSet 1		
a ComputerName 8		
# CountryCode 1		
# FreePhysicalMemoryKB 100+		
# FreeVirtualMemoryKB 100+		
a index 1		
a InstallDate 5		
a LastBootUpTime 38		
# linecount 1		
# Locale 1		
a OS 2		
a punct 1		
a SerialNumber 2		
a splunk_server 1		
		> 18/08/20 Type=OperatingSystem 23:14:22.000 OS="Microsoft Windows 10 Enterprise" Architecture="64-bit" Version="10.0.17134" BuildNumber="17134" 顯示全部 22 行 host = BSTOLL-L source = operatingsystem sourcetype = WinHostMon

Pay attention at OS=" Microsoft Windows 10 Enterprise"

Other hosts using Microsoft Windows 10 Pro, but host: BSTOLL-L is uniquely using Microsoft Windows 10 Enterprise version.

splunk>enterprise 應用套件 ▾

Administrator 1 訊息 ▾

搜尋 分析 資料集 報告 警示 儀表板

新搜尋

```
index=botsv3 BSTOLL-L OR bstoll-l earliest=0
| search sourcetype IN ("WinEventLog:Security", "xmlwineventlog:microsoft-windows-sysmon/Operational", "wineventlog")
| table _time host ComputerName
| search ComputerName=*.froth.ly
```

✓ 23,812 個事件 (26/02/10 23:20:00.000 之前) 無事件取樣 ▾

工作

事件 (23,812) 樣式 統計資料 (23,812) 視覺化

顯示 20 每頁 ▾ ✓ 格式 ▾ 預覽:開 1 2

_time	host	ComputerName
2018/08/20 23:17:58	BSTOLL-L	BSTOLL-L.froth.ly
2018/08/20 23:17:29	BSTOLL-L	BSTOLL-L.froth.ly
2018/08/20 23:17:29	BSTOLL-L	BSTOLL-L.froth.ly
2018/08/20 23:17:28	BSTOLL-L	BSTOLL-L.froth.ly
2018/08/20 23:17:22	BSTOLL-L	BSTOLL-L.froth.ly
2018/08/20 23:16:47	BSTOLL-L	BSTOLL-L.froth.ly

Why it matters: Different versions can be a sign of compromise, or just bad management — SOC should check both.