DETECTING SOPHISTICATED THREAT ACTORS IN AWS

Alfie Champion

Nick Jones

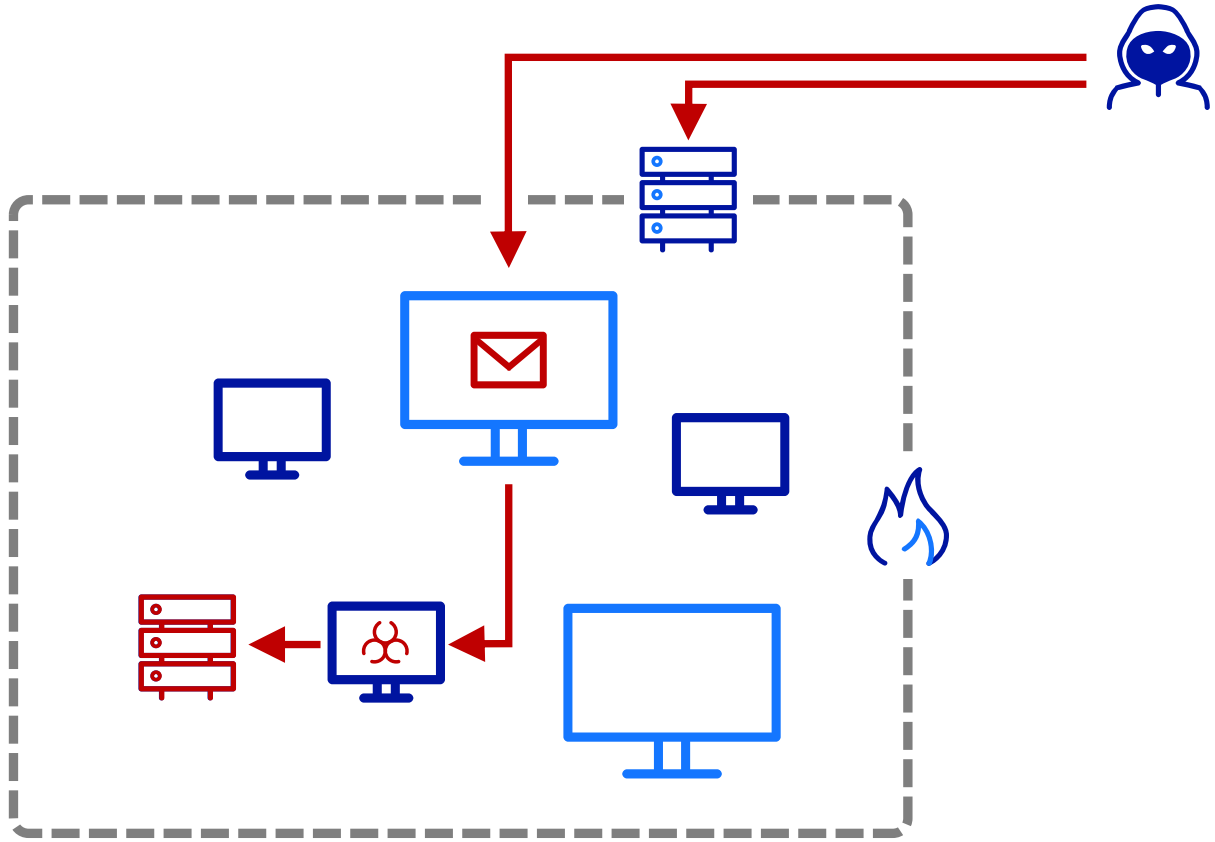
F-Secure

AGENDA

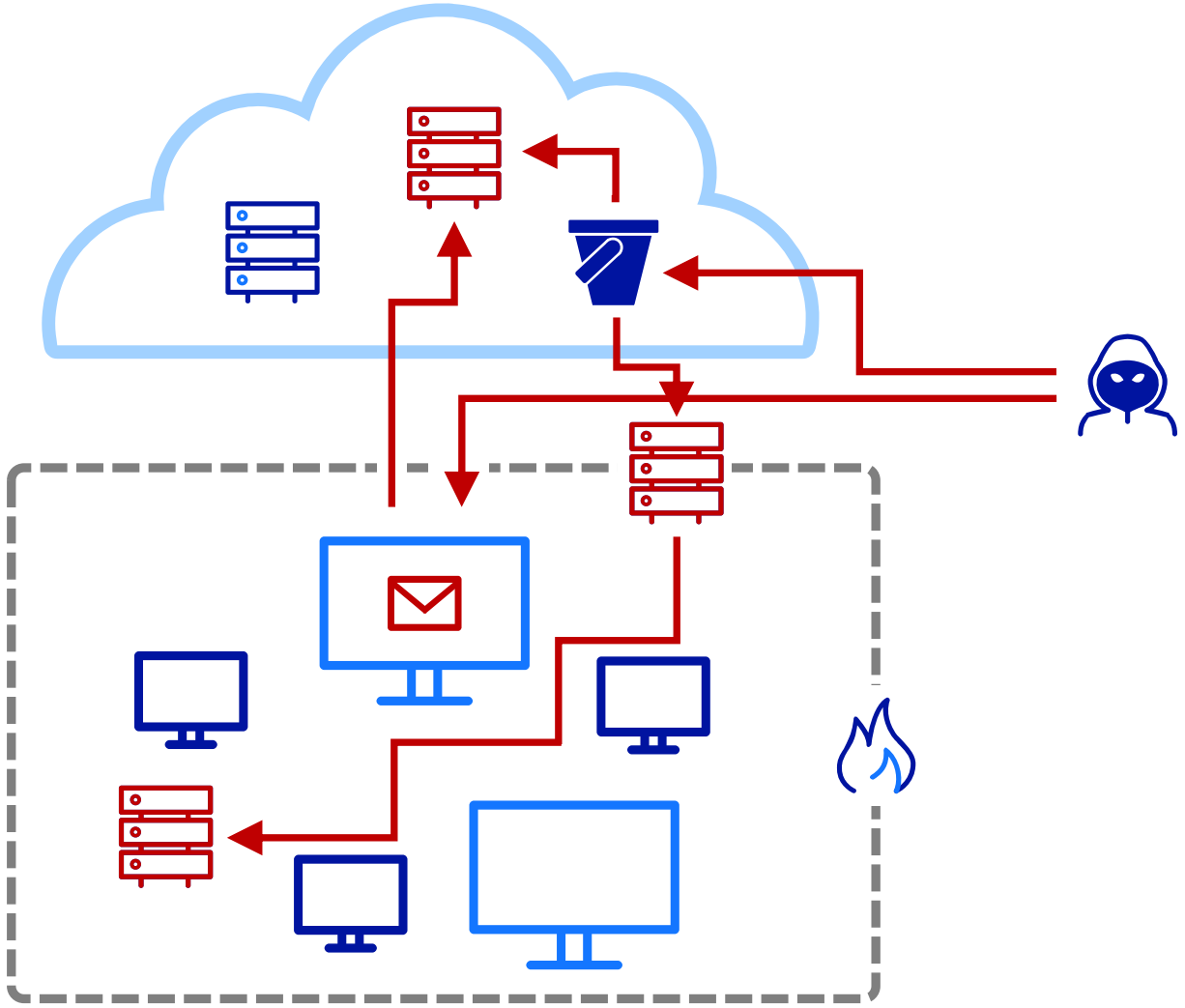
RIP PERIMETER

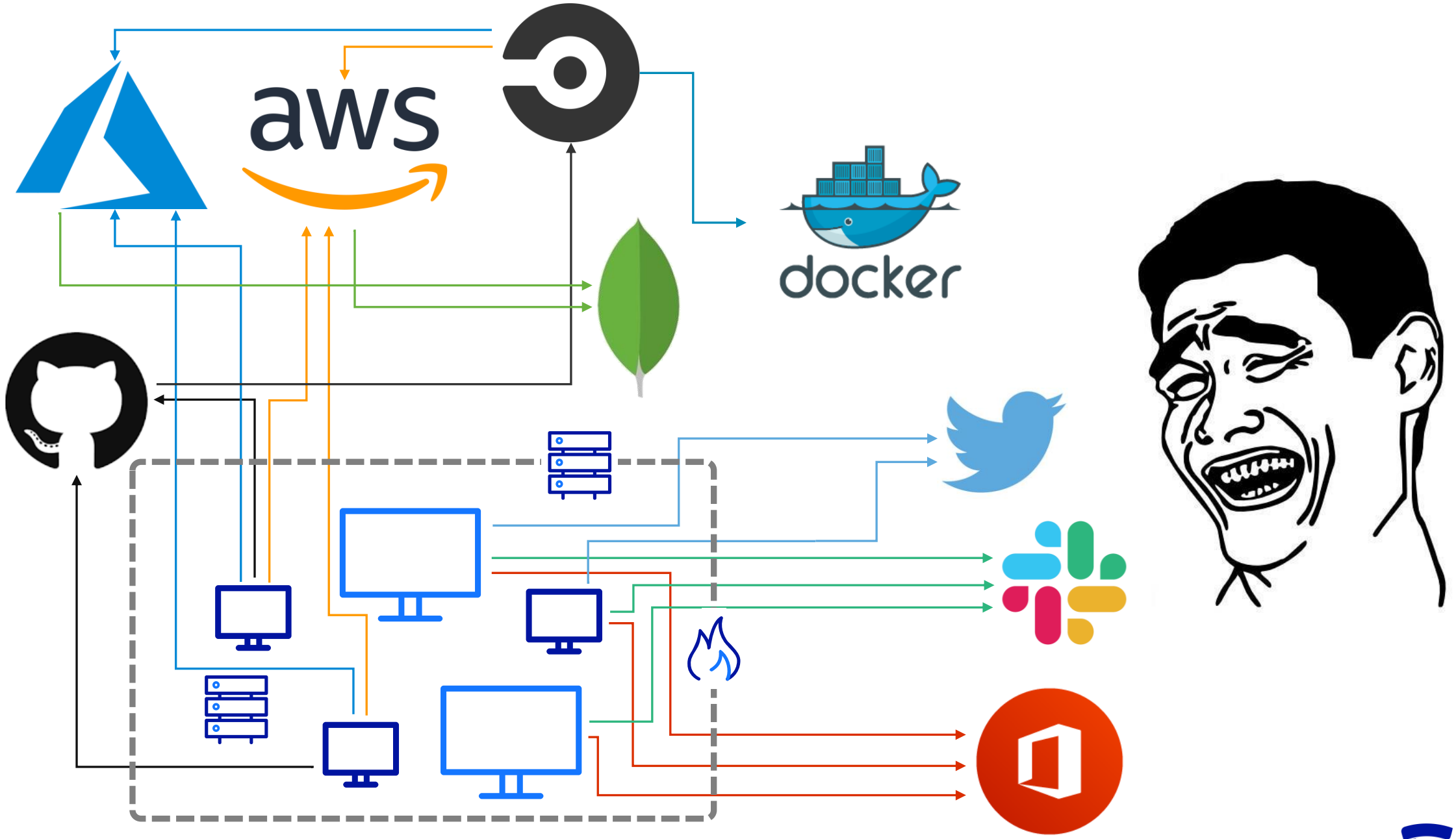
F-Secure

CLASSIC ORGANISATION



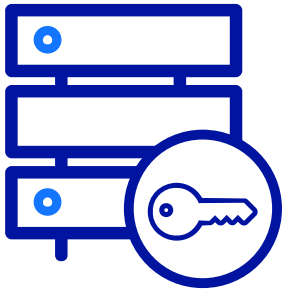
MODERN ORGANISATION



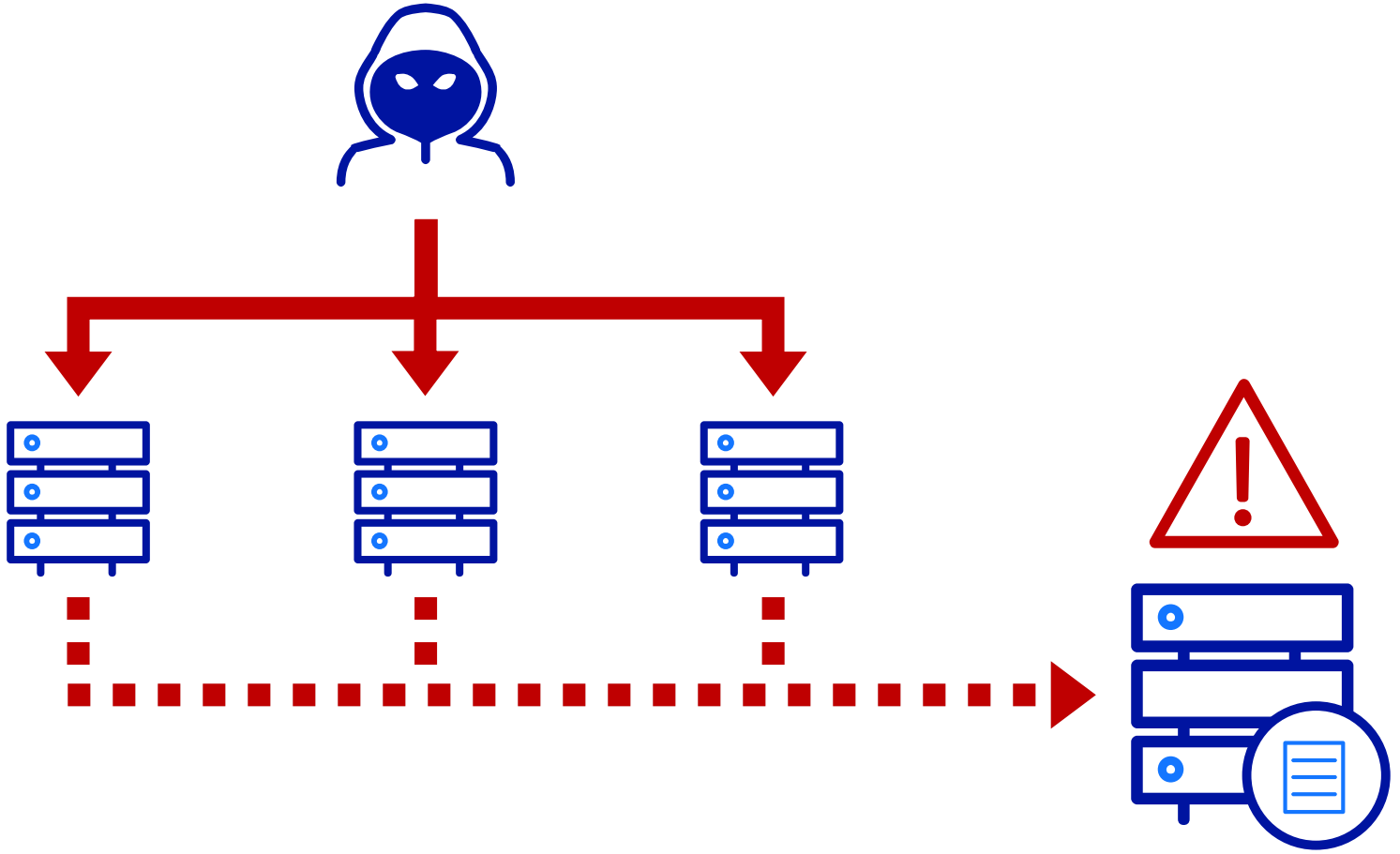


MODERN ATTACKS

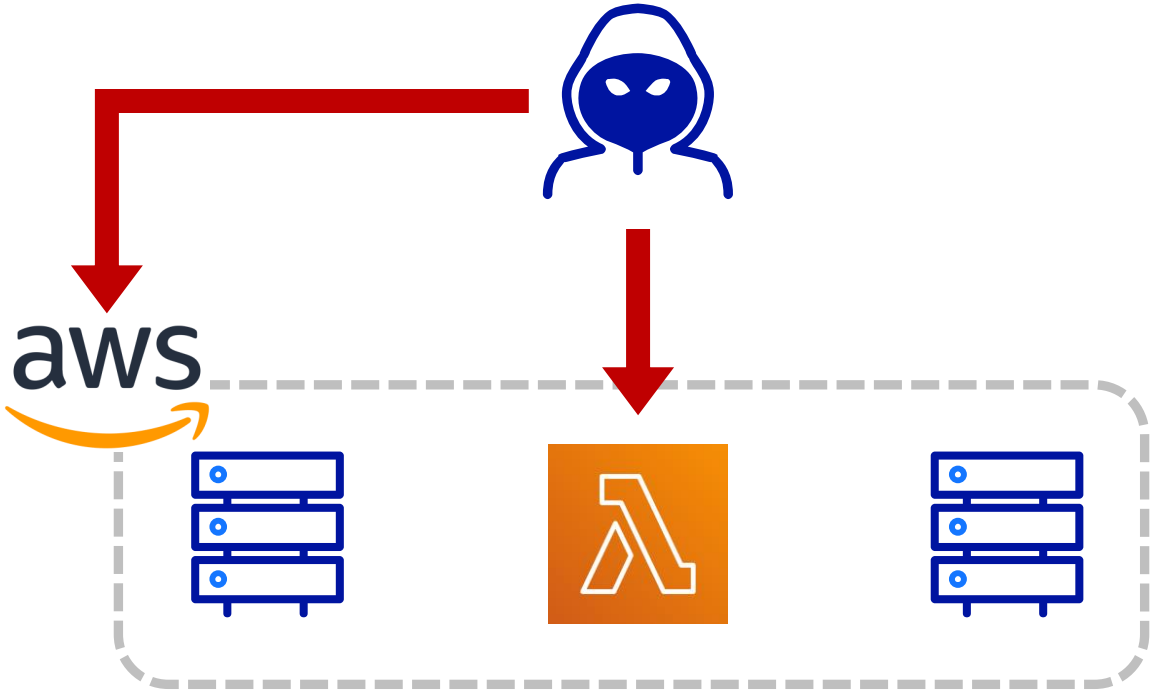
INITIAL VECTORS



ATTACK SURFACE



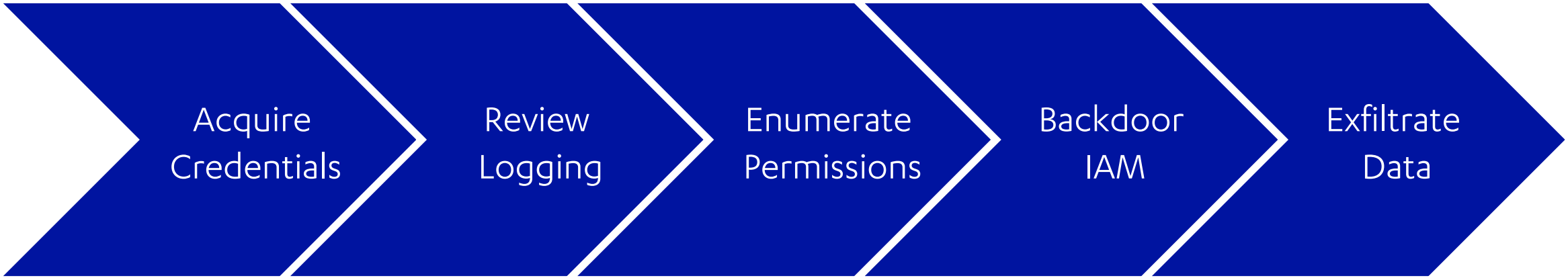
ATTACK SURFACE



ATTACKER OBJECTIVES

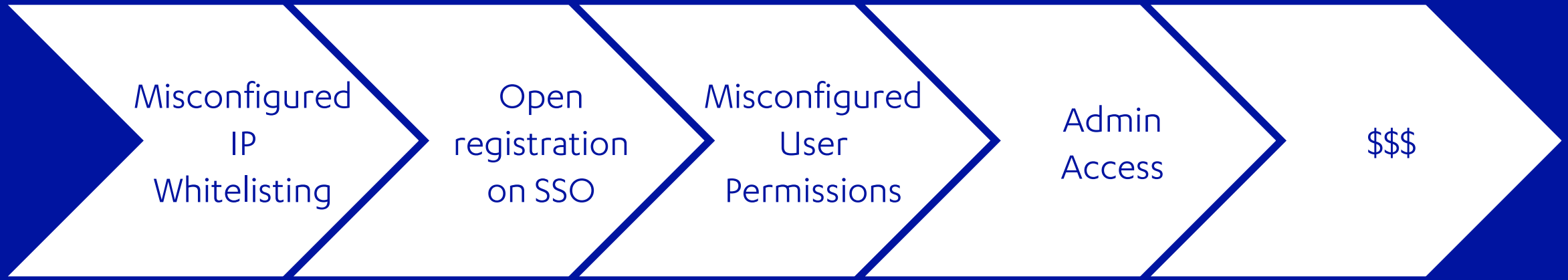
ATTACK PATHS

ATTACK PATHS



F-Secure

WAR STORIES #1

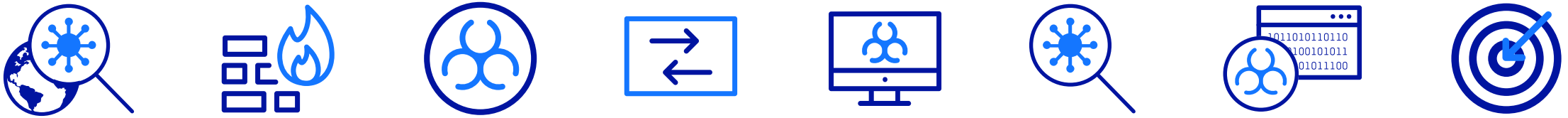


WAR STORIES #2

CAPITAL ONE BREACH

EC2 Instance Metadata

Sync 700+ S3 Buckets



Recon | Delivery | Exploit | C2 | Persistence | Int. Recon | Lat. Mov. | Objective

Misconfigured Firewall

List Buckets

EC2 Instance Metadata

Exploit

```
ec2-user@ip-192-168-221-53:~$ curl http://169.254.169.254/latest/meta-data/
ami-id
ami-launch-index
ami-manifest-path
block-device-mapping/
events/
hostname
identity-credentials/
instance-action
instance-id
instance-type
local-hostname
local-ipv4
```

Int. Recon

List Buckets

```
alfie@mwr-alfie:~$ aws s3 ls
2019-09-05 15:10:33 firehose-bucket-logs-12345
2019-02-09 23:41:07 remote-state-cloud-detection
2019-09-05 14:47:39 tf-bucket-logs-12345
```

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:GetObject",
                "s3:ListBucket",
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

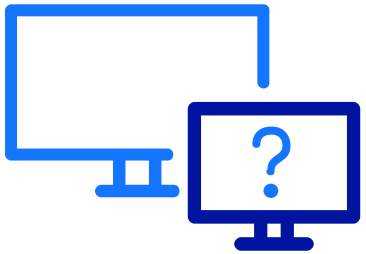
Sync 700+
S3 Buckets

Objective

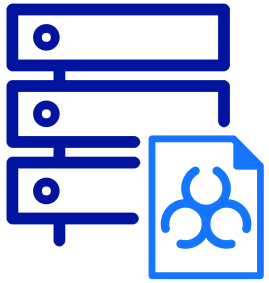
```
alfie@mwr-alfie:/tmp$ aws s3 sync s3://tf-bucket-logs-12345 test-data/
download: s3://tf-bucket-logs-12345/AWSLogs/299338442723/CloudTrail/ap-northeast-1/2019/09/05/299338442723_Cl
oudTrail_ap-northeast-1_20190905T1700Z_I8N1FnYiHf32mt4E.json.gz to test-data/AWSLogs/299338442723/CloudTrail/
ap-northeast-1/2019/09/05/299338442723_CloudTrail_ap-northeast-1_20190905T1700Z_I8N1FnYiHf32mt4E.json.gz
download: s3://tf-bucket-logs-12345/AWSLogs/299338442723/CloudTrail/ap-northeast-1/2019/09/05/299338442723_Cl
oudTrail_ap-northeast-1_20190905T1705Z_HOl5Npr4Sj6PrQRG.json.gz to test-data/AWSLogs/299338442723/CloudTrail/
ap-northeast-1/2019/09/05/299338442723_CloudTrail_ap-northeast-1_20190905T1705Z_HOl5Npr4Sj6PrQRG.json.gz
download: s3://tf-bucket-logs-12345/AWSLogs/299338442723/CloudTrail/ap-northeast-1/2019/09/05/299338442723_Cl
oudTrail_ap-northeast-1_20190905T1355Z_R8EFIHTEXRQQNkU1.json.gz to test-data/AWSLogs/299338442723/CloudTrail/
ap-northeast-1/2019/09/05/299338442723_CloudTrail_ap-northeast-1_20190905T1355Z_R8EFIHTEXRQQNkU1.json.gz
download: s3://tf-bucket-logs-12345/AWSLogs/299338442723/CloudTrail/ap-northeast-2/2019/09/05/299338442723_Cl
oudTrail_ap-northeast-2_20190905T1350Z_6LIKPUq0C4K4yvhQ.json.gz to test-data/AWSLogs/299338442723/CloudTrail/
ap-northeast-2/2019/09/05/299338442723_CloudTrail_ap-northeast-2_20190905T1350Z_6LIKPUq0C4K4yvhQ.json.gz
```

CLOUD ATTACK DETECTION CHALLENGES

ON-PREMISE

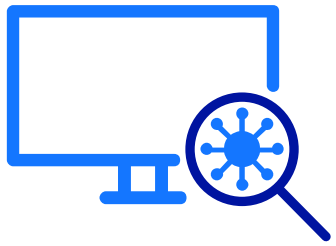


Asset Management



Log Storage

Tooling Deployment



Technologies

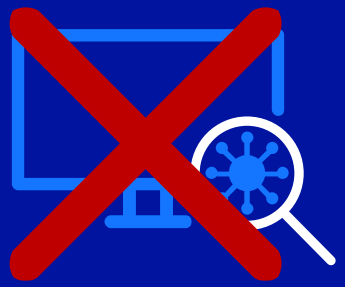
F-Secure

CLOUD

Asset Management

Log Storage

Tooling Deployment

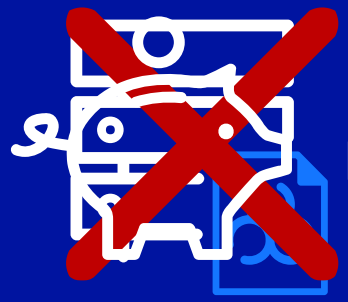


Technologies

F-Secure

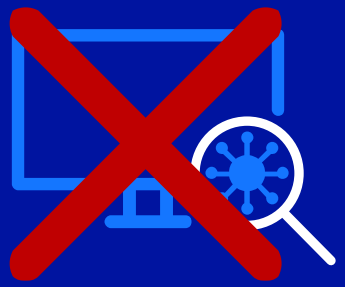
CLOUD

Asset
Shadow IT
Management



Log Storage

Tooling
Deployment



Technologies

F-Secure

WHAT ARE PROVIDERS DOING ABOUT IT?

AWS SERVICES

Amazon Macie

Amazon Elasticsearch Service

Amazon CloudWatch

AWS CloudTrail

AWS Control Tower

AWS Config

Amazon GuardDuty

Amazon Inspector

AWS SERVICES

Amazon Macie

Amazon Elasticsearch Service

Amazon CloudWatch

AWS CloudTrail

AWS Control Tower

AWS Config

Amazon GuardDuty

Amazon Inspector

F-Secure

AWS SERVICES

Amazon Macie

Amazon Elasticsearch Service

Amazon CloudWatch

AWS CloudTrail

AWS Control Tower

AWS Config

+

Lambda

Amazon GuardDuty

+

Lambda

Amazon Inspector

F-Secure

AWS SERVICES

Amazon Macie

Amazon Elasticsearch Service

Amazon CloudWatch

AWS CloudTrail

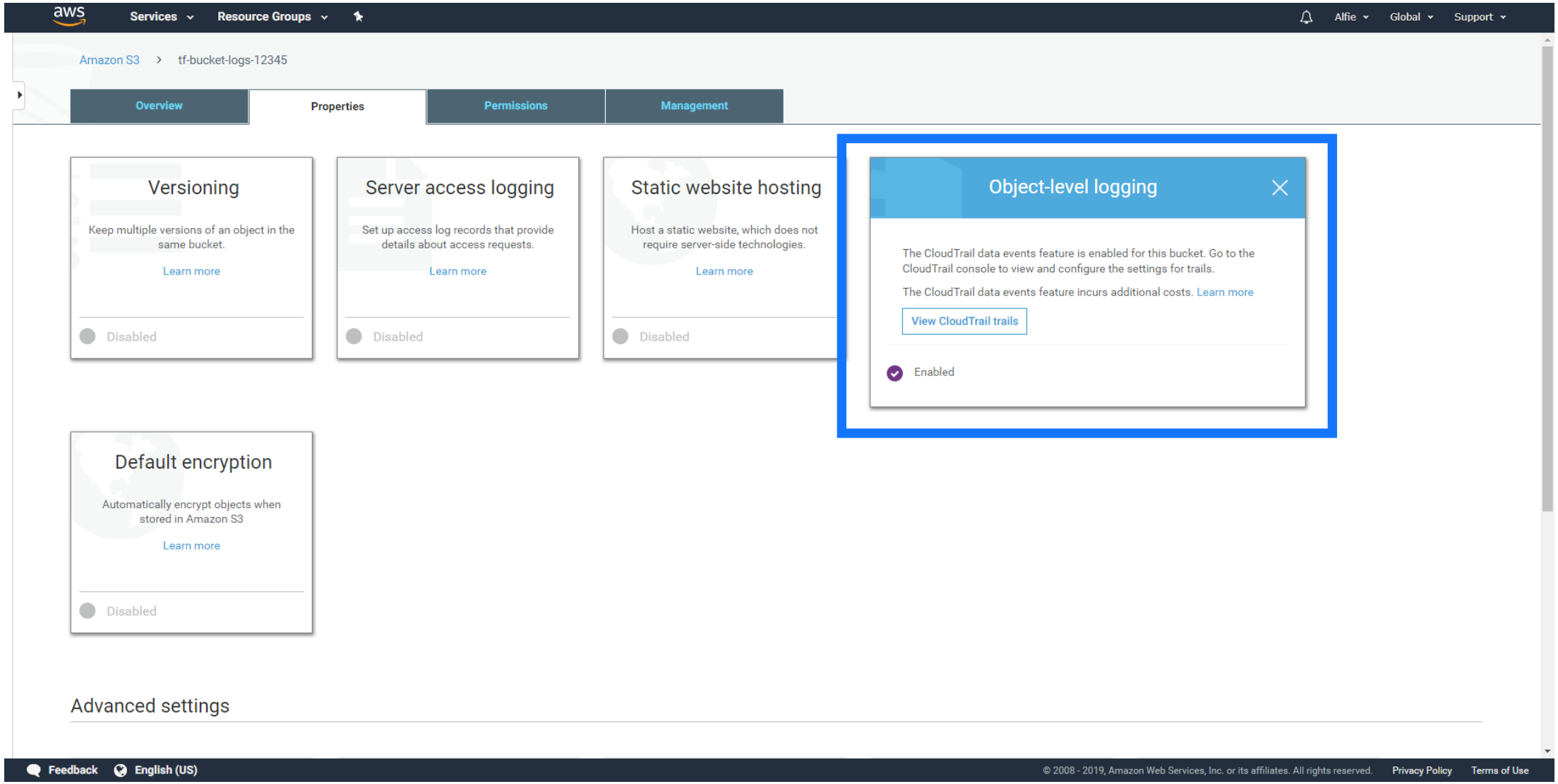
AWS Control Tower

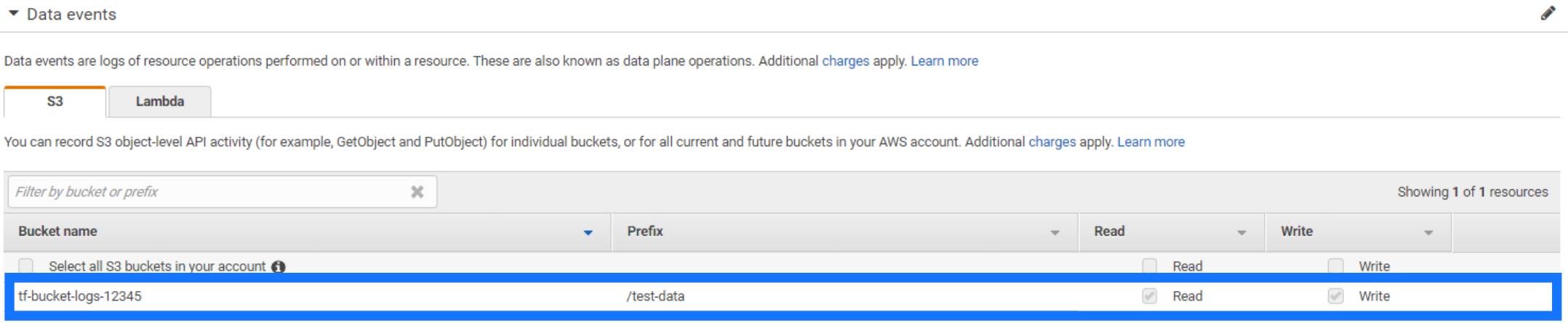
AWS Config

Amazon GuardDuty

Amazon Inspector

F-Secure


aws
Services
Resource Groups
Alfie
Global
Support
Amazon S3
tf-bucket-logs-12345
Overview
Properties
Permissions
Management
Versioning
Keep multiple versions of an object in the same bucket.
Learn more
Disabled
Server access logging
Set up access log records that provide details about access requests.
Learn more
Disabled
Static website hosting
Host a static website, which does not require server-side technologies.
Learn more
Disabled
Object-level logging
The CloudTrail data events feature is enabled for this bucket. Go to the CloudTrail console to view and configure the settings for trails.
The CloudTrail data events feature incurs additional costs. Learn more
View CloudTrail trails
Enabled
Default encryption
Automatically encrypt objects when stored in Amazon S3
Learn more
Disabled
Advanced settings
Feedback
English (US)
© 2008 - 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use



▸	September 5th 2019, 18:21:03.276	s3.amazonaws.com	GetObject	tf-bucket-logs-12345	test-data/dataAug-16-2019.json
▸	September 5th 2019, 18:21:03.276	s3.amazonaws.com	GetObject	tf-bucket-logs-12345	test-data/dataSep-5-2019.json
▸	September 5th 2019, 18:21:03.276	s3.amazonaws.com	GetObject	tf-bucket-logs-12345	test-data/dataJuly-27-2019.json

WHAT DOES BAD LOOK LIKE?

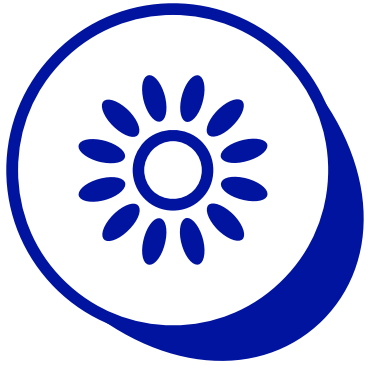
PRIOR RESEARCH

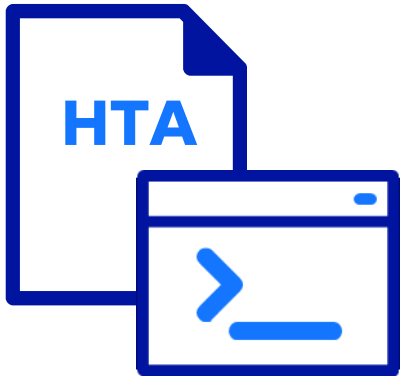
ON-PREMISE EQUIVALENTS

ATT&CK Matrix for Enterprise

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collecti	trol	Exfiltration	Impact
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript			Automated Exfiltration	Data Destruction
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Softw			Compressed	Data Encrypted for Impact
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery	Distributed Com Object Mo			crypted	Defacement
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	Domain Trust Discovery	Exploitation Servi			ize Limits	Disk Content Wipe
Replication Through Removable Media	Control Panel Items	AppInit DLLs	Application Shimming	Clear Command History	Credentials in Files	File and Directory Discovery	Logon S			lternative	Disk Structure Wipe
Spearphishing Attachment	Dynamic Data Exchange	Application Shimming	Bypass User Account Control	CMSTP	Credentials in Registry	Network Service Scanning	Pass the			Command Channel	Endpoint Denial of Service
Spearphishing Link	Execution through API	Authentication Package	DLL Search Order Hijacking	Code Signing	Exploitation for Credential Access	Network Share Discovery	Pass the Tic			Over Other k Medium	Firmware Corruption
Spearphishing via Service	Execution through Module Load	BITS Jobs	Dylib Hijacking	Compile After Delivery	Forced Authentication	Network Sniffing	Remote Desktop Protocol			on Over Physical Medium	Inhibit System Recovery
Supply Chain Compromise	Exploitation for Client Execution	Bootkit	Exploitation for Privilege Escalation	Compiled HTML File	Hooking	Password Policy Discovery	Remote File Copy	E		Scheduled Transfer	Network Denial of Service
Trusted Relationship	Graphical User Interface	Browser Extensions	Extra Window Memory Injection	Component Firmware	Input Capture	Peripheral Device Discovery	Remote Services	Input Capture	Fallback Channels		Resource Hijacking
Valid Accounts	InstallUtil	Change Default File Association	File System Permissions Weakness	Component Object Model Hijacking	Input Prompt	Permission Groups Discovery	Replication Through Removable Media	Man in the Browser	Multi-hop Proxy		Runtime Data Manipulation

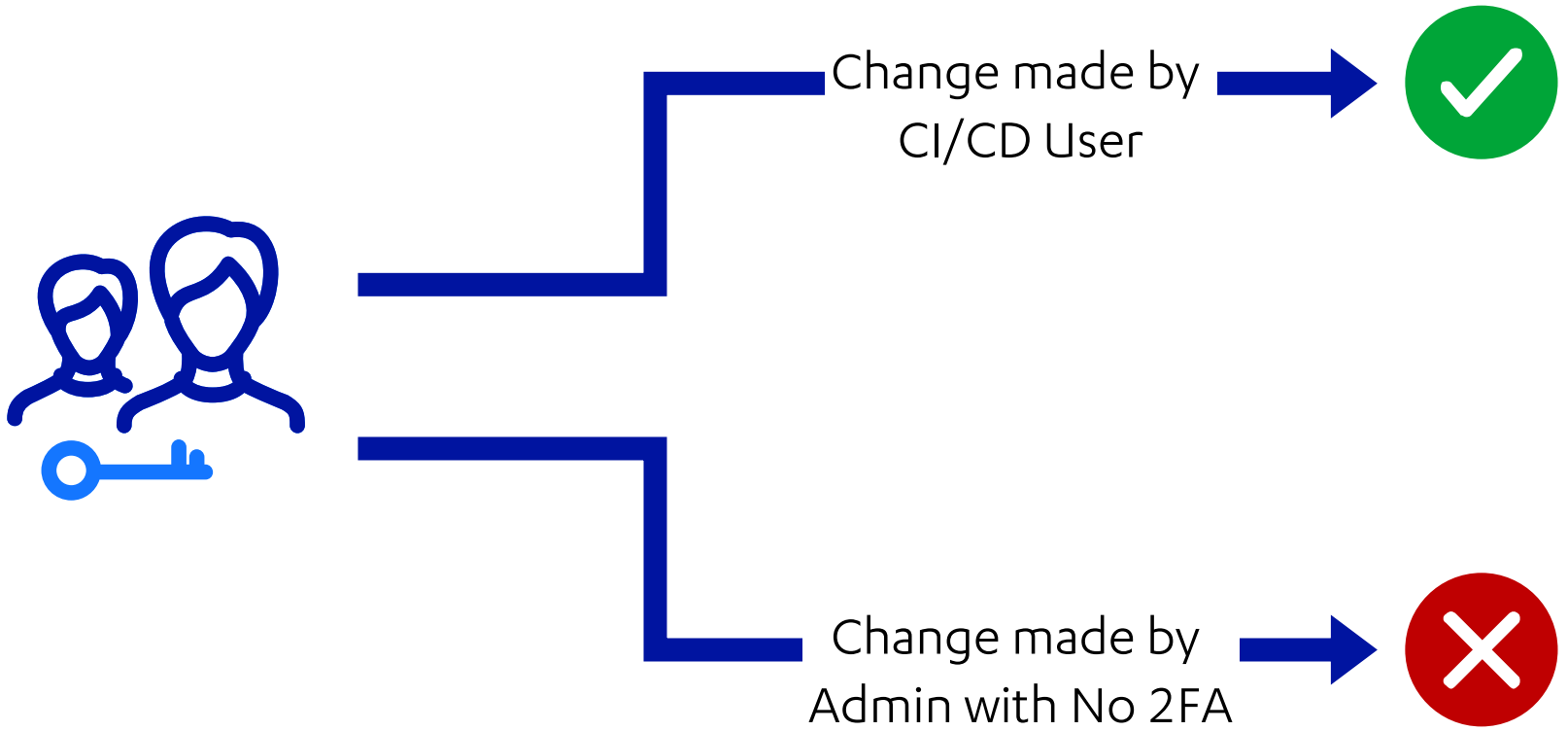
MINDSET SHIFT

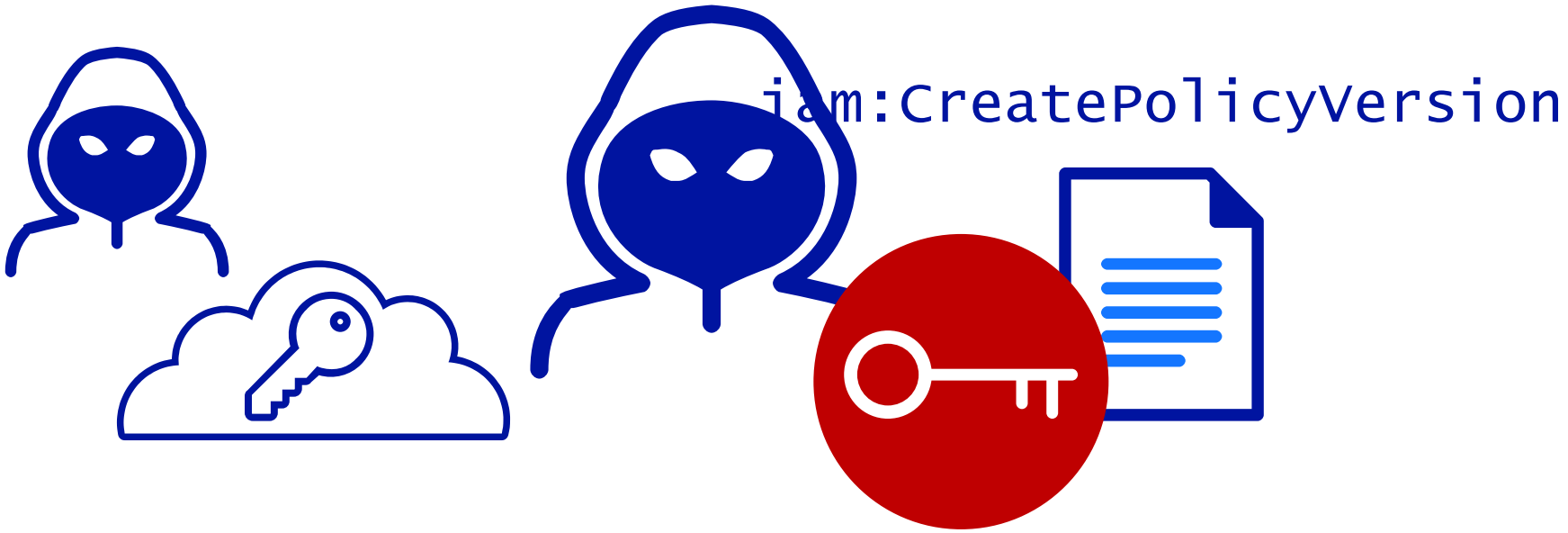




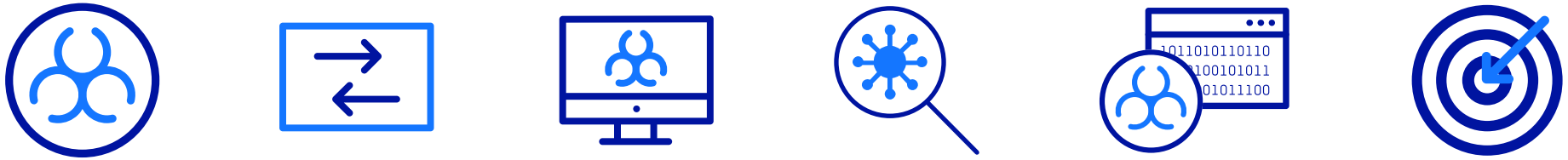
UNCERTAINTY OF MALICIOUS INTENT

CONTEXT IS KEY





CODIFY ATTACKS



DETECTION FIDELITY

F-Secure

LEONIDAS

Leonidas 1.0

[Base URL: /dev]
https://nb2dfjx41h.execute-api.us-east-1.amazonaws.com/dev/swagger.json

An API for executing attacker actions within AWS

enumeration Enumeration

GET **/enumeration/enumerate_cloudtrails_for_all_regions** An adversary may attempt to enumerate the configured trails, to identify what actions will be logged and where they will be logged to

GET **/enumeration/enumerate_cloudtrails_for_current_region** An adversary may attempt to enumerate the configured trails, to identify what actions will be logged and where they will be logged to

defense_evasion Defense Evasion

GET **/defense_evasion/add_new_guardduty_ip_set** An adversary may attempt to add a new GuardDuty IP whitelist in order to whitelist systems they control and reduce the chance of malicious activity being detected

GET **/defense_evasion/update_guardduty_ip_set** An adversary may attempt to alter a configured GuardDuty IP whitelist in order to whitelist systems they control and reduce the chance of malicious activity being detected

Parameters Cancel

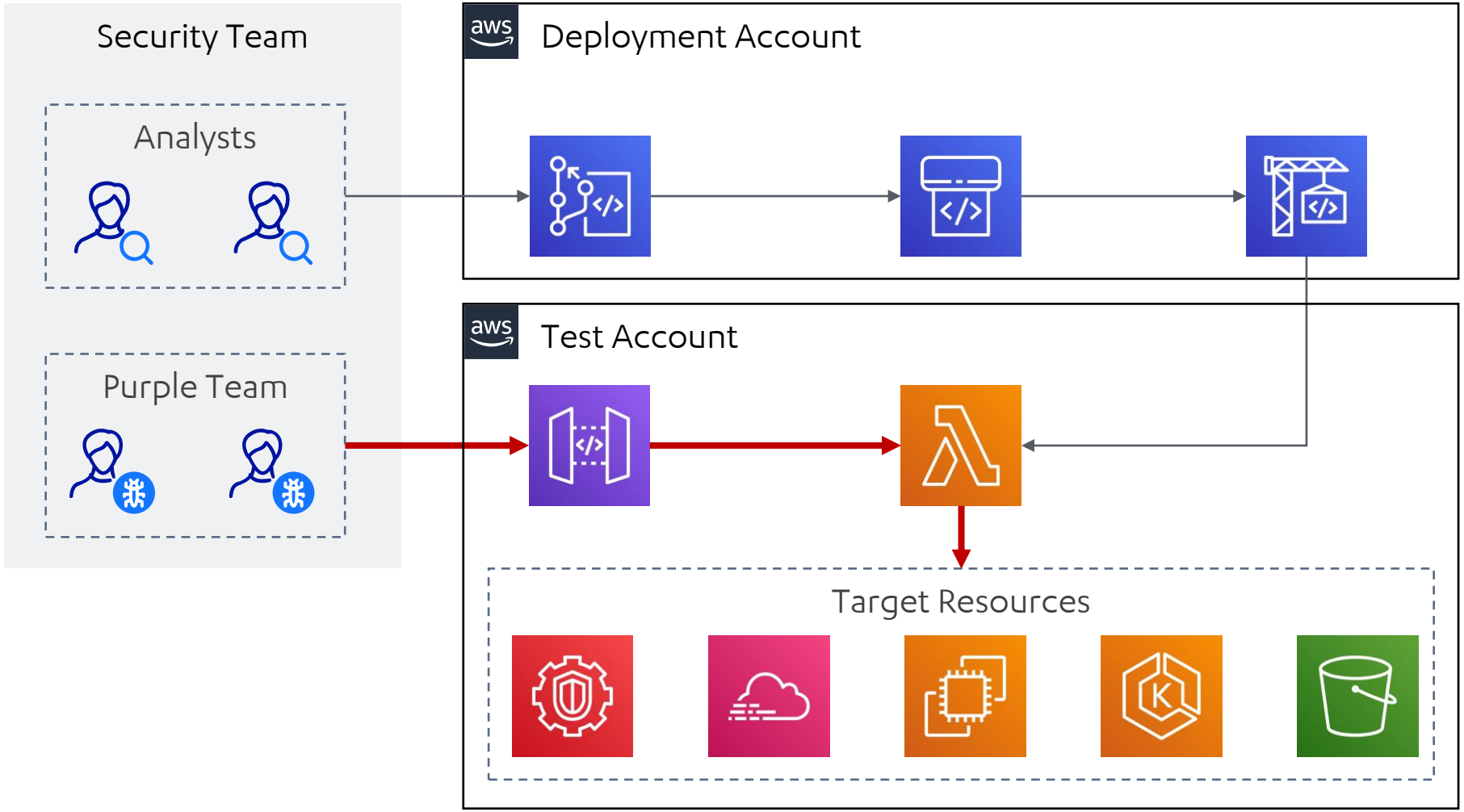
Name	Description
detectorid **string** *(query)*	ID of the guardduty detector associated with the IP set list detectorid - ID of the guardduty detector assc
ipsetid **string** *(query)*	ID of the IP set to be updated ipsetid - ID of the IP set to be updated
location **string** *(query)*	Location of the IP whitelist location - Location of the IP whitelist

F-Secure

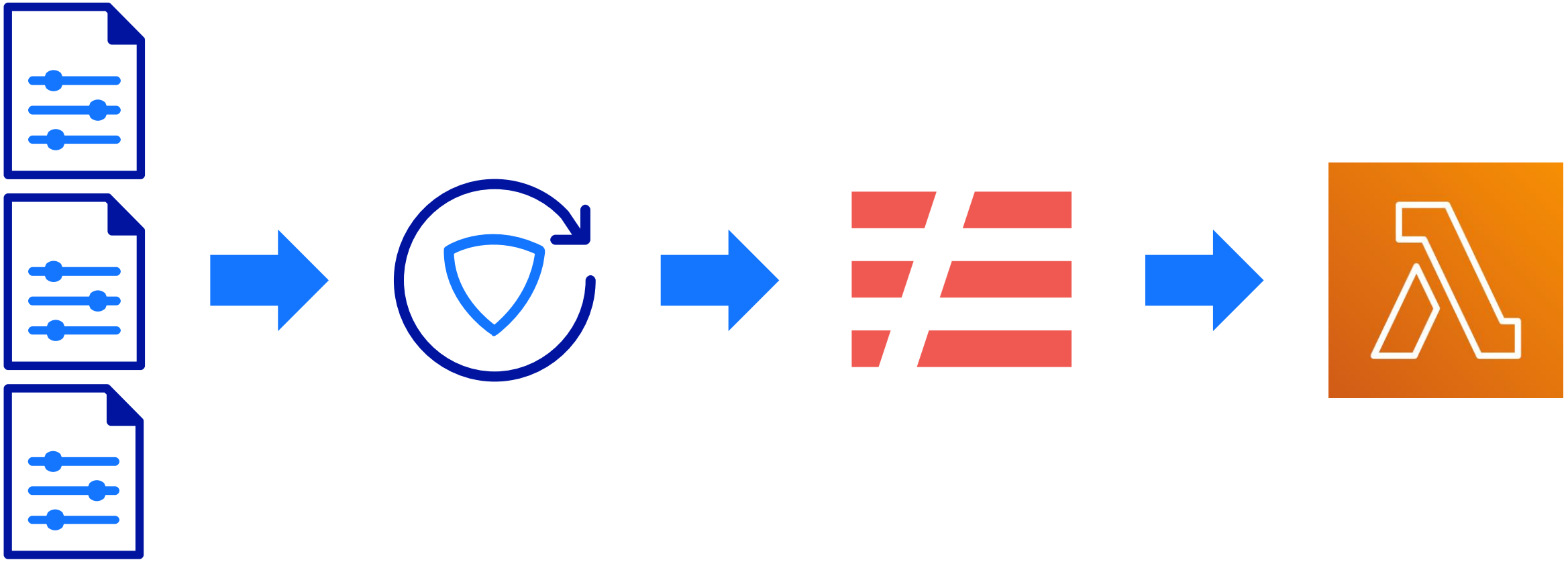
LEONIDAS

```
nick@DESKTOP-RG0SK17:~$ curl -s -X GET "https://n[redacted]h.execute-api.us-east-1.amazonaws.com/dev/enumeration/enumerate_cloudtrails_for_current_region"
 -H "accept: application/json" -H "x-api-key: Kba[redacted]cx" | jq .
{
  "trailList": [
    {
      "Name": "leonidas-target-trail",
      "S3BucketName": "leonidas-target-bucket",
      "S3KeyPrefix": "prefix",
      "IncludeGlobalServiceEvents": true,
      "IsMultiRegionTrail": true,
      "HomeRegion": "us-east-1",
      "TrailARN": "arn:aws:cloudtrail:us-east-1:573816966241:trail/leonidas-target-trail",
      "LogFileValidationEnabled": true,
      "HasCustomEventSelectors": false,
      "IsOrganizationTrail": false
    }
  ],
  "ResponseMetadata": {
    "RequestId": "397f3c4b-f6f3-43e6-8c5b-de6b4c01bf8e",
    "HTTPStatusCode": 200,
    "HTTPHeaders": {
      "x-amzn-requestid": "397f3c4b-f6f3-43e6-8c5b-de6b4c01bf8e",
      "content-type": "application/x-amz-json-1.1",
      "content-length": "371",
      "date": "Tue, 01 Oct 2019 14:53:44 GMT"
    },
    "RetryAttempts": 0
  }
}
nick@DESKTOP-RG0SK17:~$
```

LEONIDAS

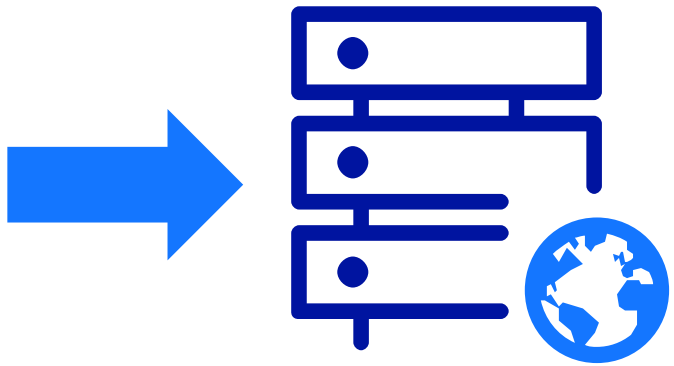


BUILD PROCESS



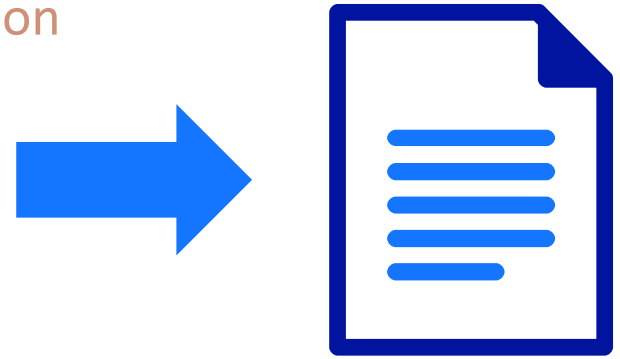
CODE GENERATION

```
- name: Enumerate Cloudtrails for Current Region
  permissions:
  - cloudtrail:DescribeTrails
  input_arguments:
  executors:
    python:
      code: |
        client = boto3.client('cloudtrail')
        response = client.describe_trails()
        return response
```



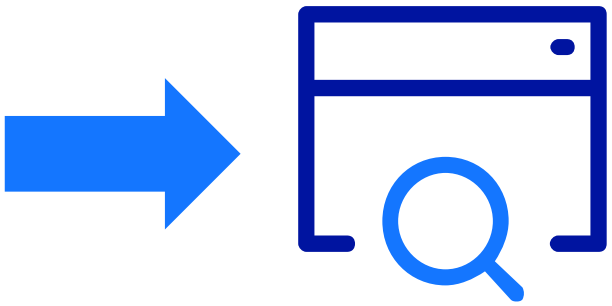
CODE GENERATION

```
- name: Enumerate Cloudtrails for Current Region
  permissions:
  - cloudtrail:DescribeTrails
  input_arguments:
  executors:
    python:
      code: |
        client = boto3.client('cloudtrail')
        response = client.describe_trails()
        return response
```



CODE GENERATION

```
- name: Enumerate Cloudtrails for Current Region
  detection:
    sources:
    - name: "cloudtrail"
      attributes:
        eventName: "DescribeTrails"
        eventSource: "*.cloudtrail.amazonaws.com"
```



DOCUMENTATION GENERATION

T1501 - Add an API key to an existing user

Add API key to existing user

An adversary may attempt to maintain access by creating an API key attached to an existing privileged user

Required Permissions

- iam:CreateAccessKey

Required Parameters

user - str

IAM user to generate the API key for

Attacker Action

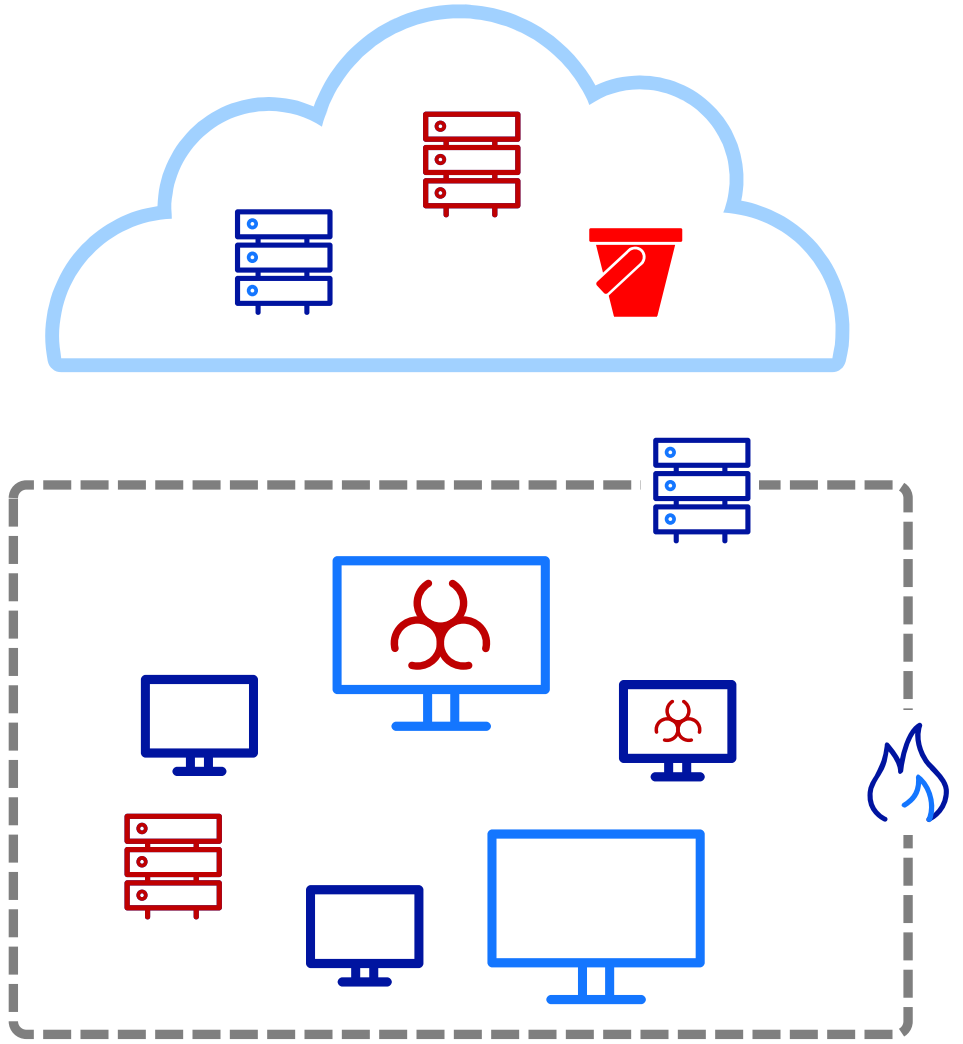
```
aws iam create-access-key --user-name [user]
```

Detection Case

When logs are ingested into ELK, the following Lucene query can be used to identify relevant events.

```
eventName:CreateAccessKey AND eventSource:iam.amazonaws.com
```

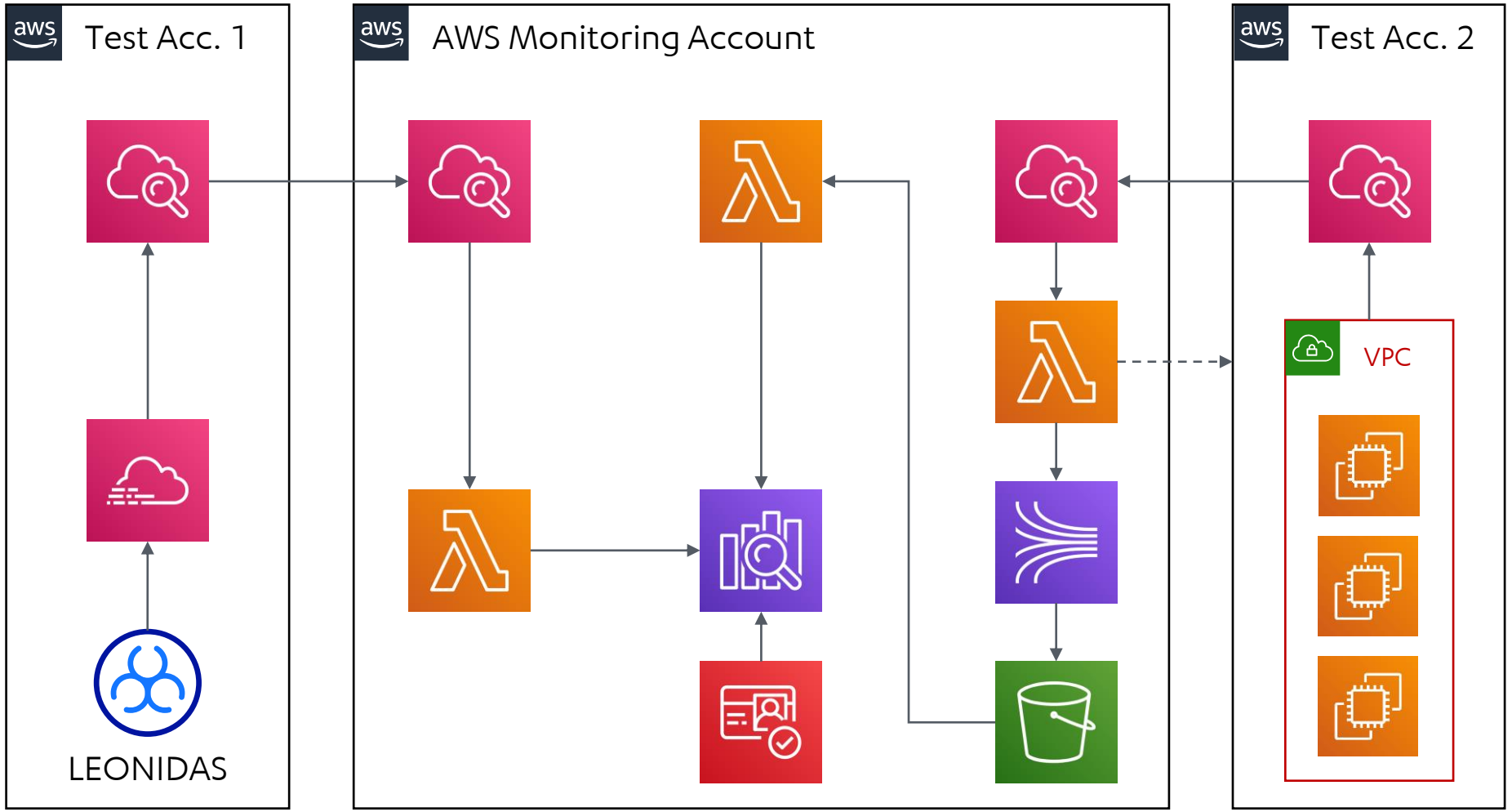
CONTINUOUS TESTING

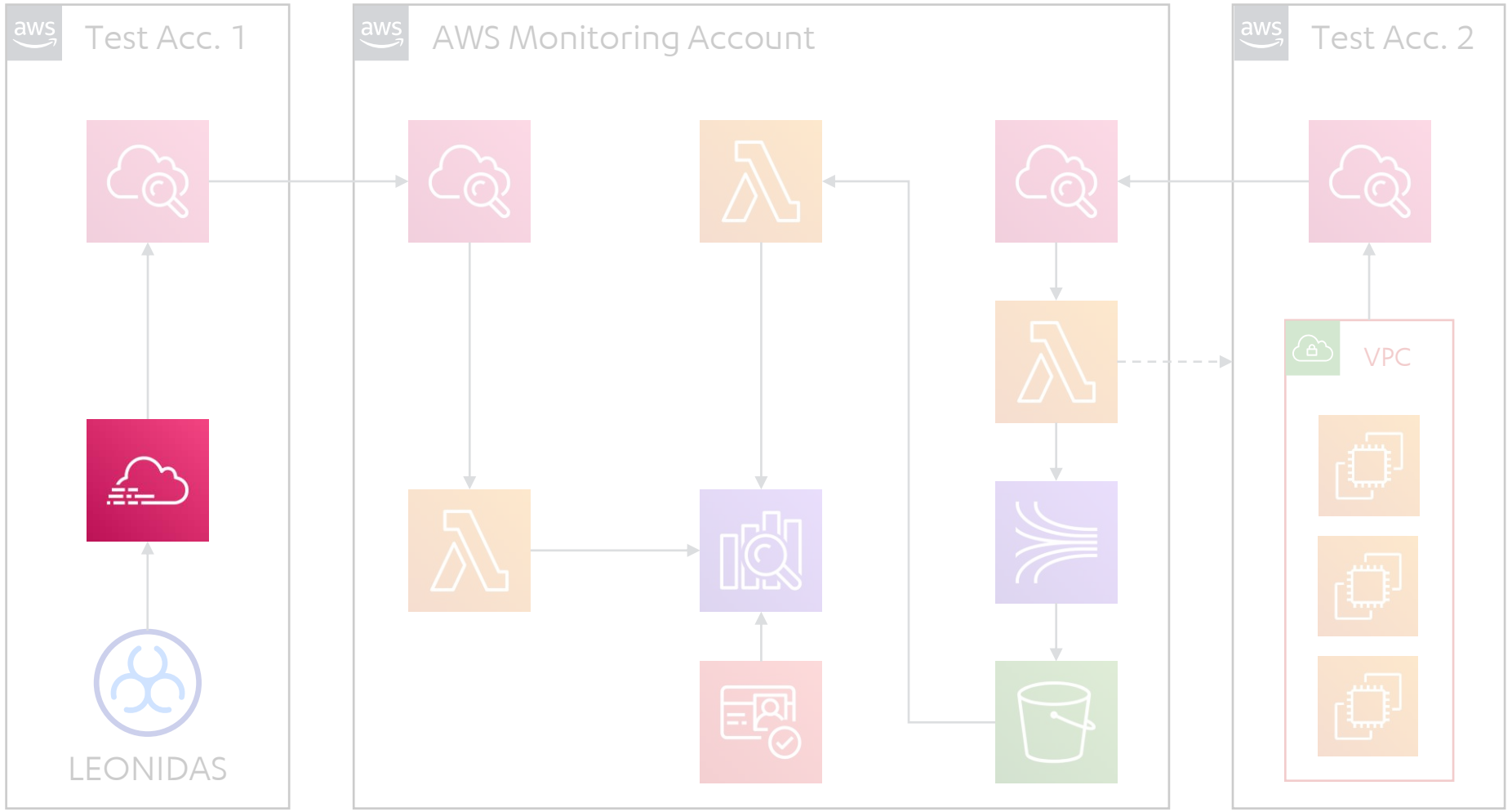


F-Secure

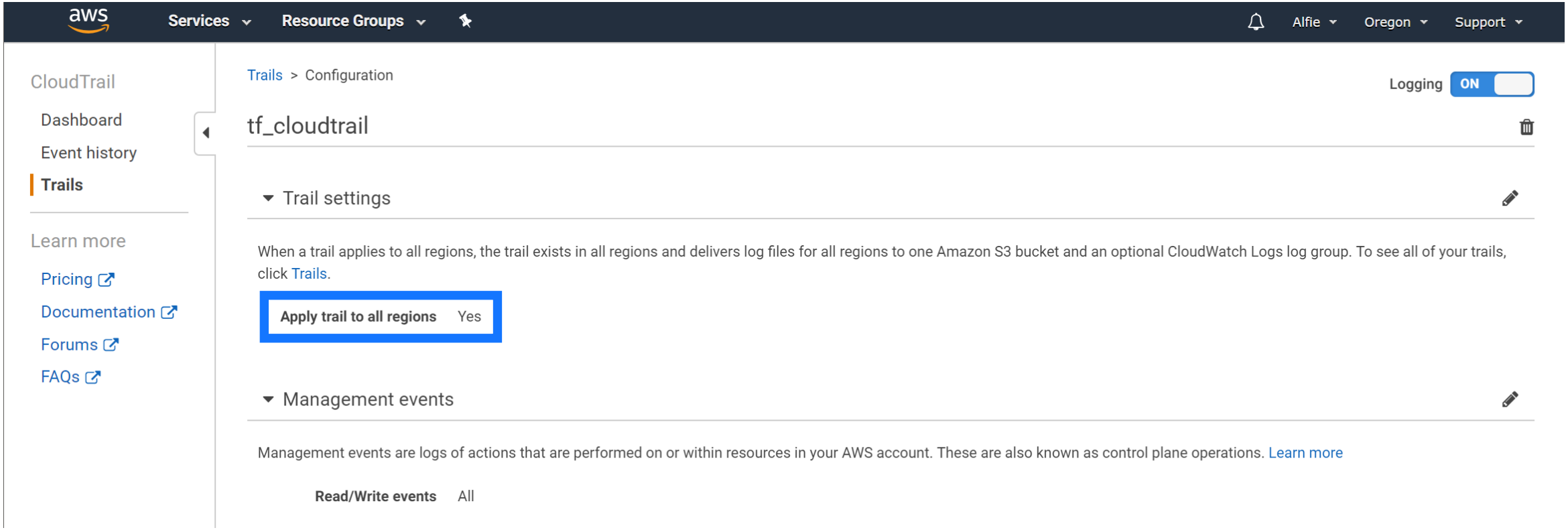
TERRASIEM

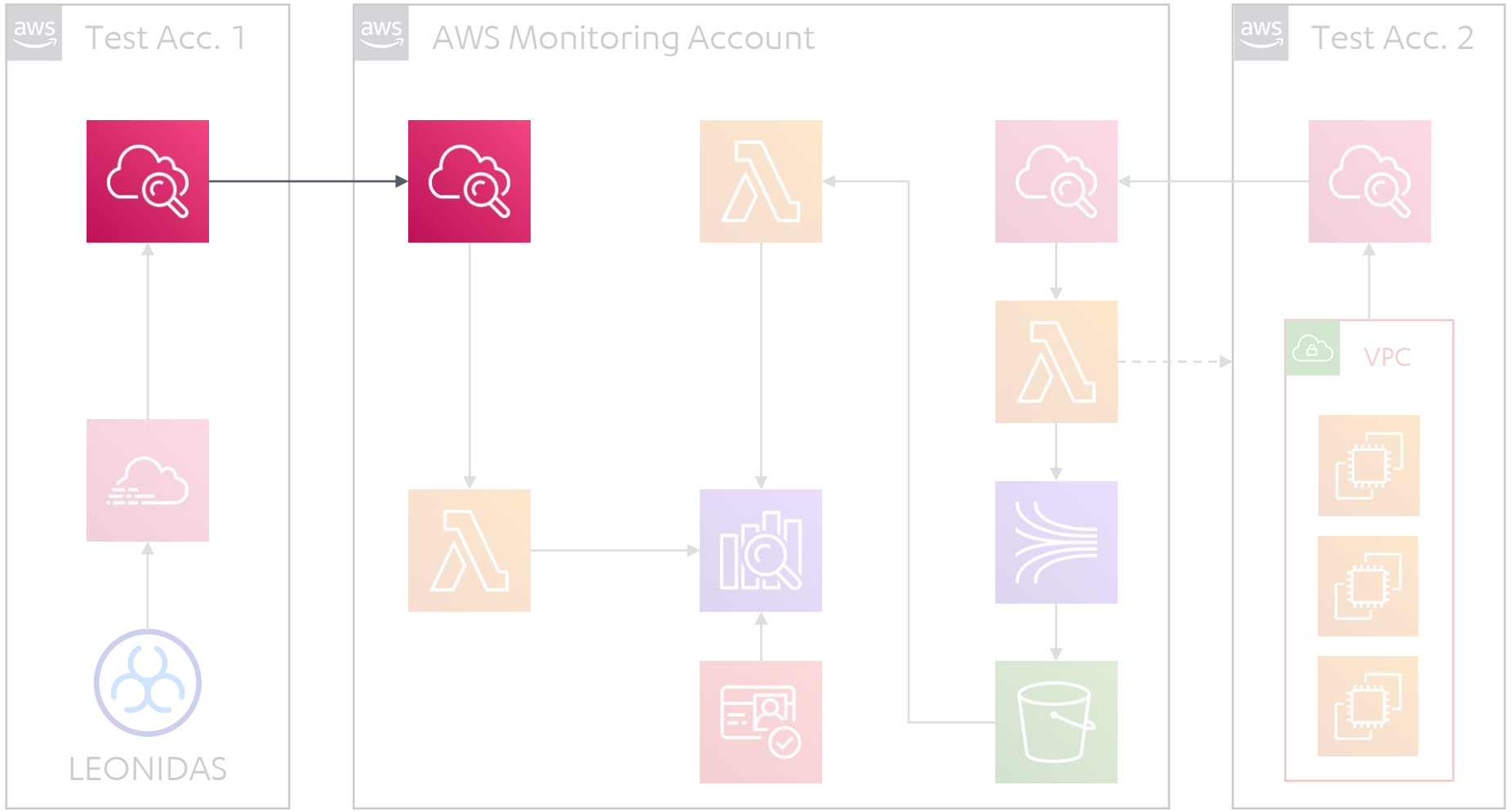
TERRASIEM



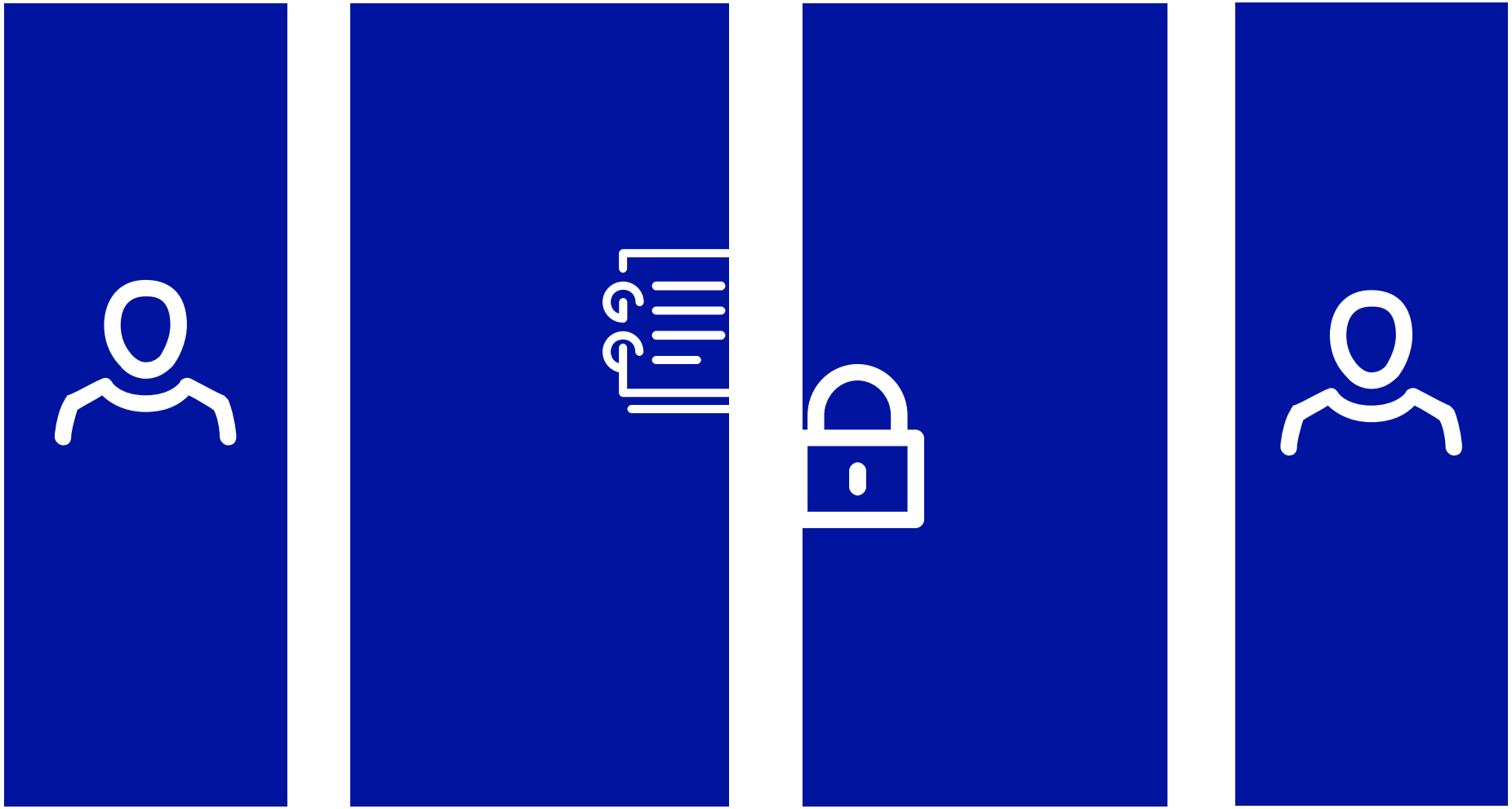


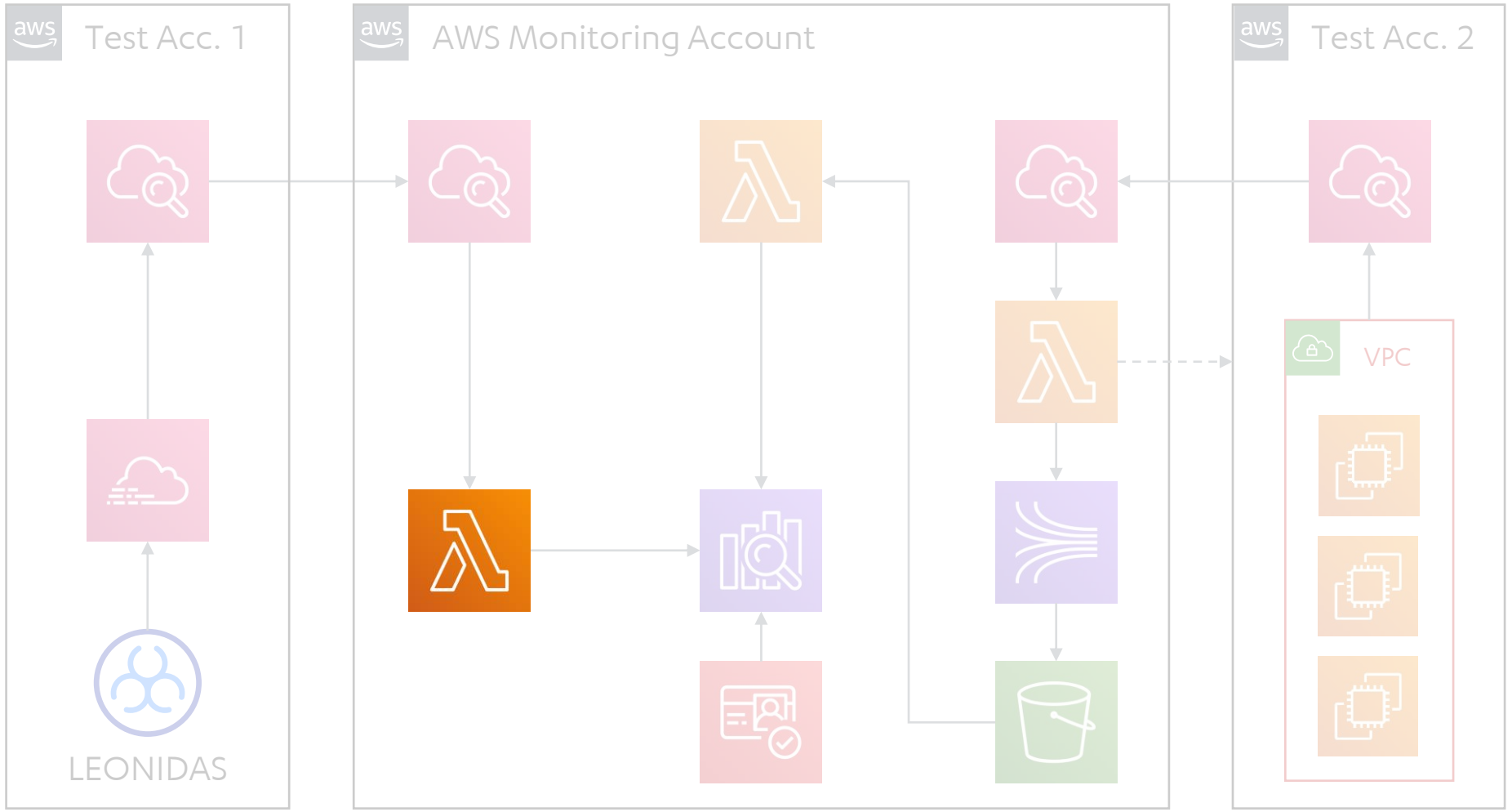
CROSS-REGION CLOUDTRAIL





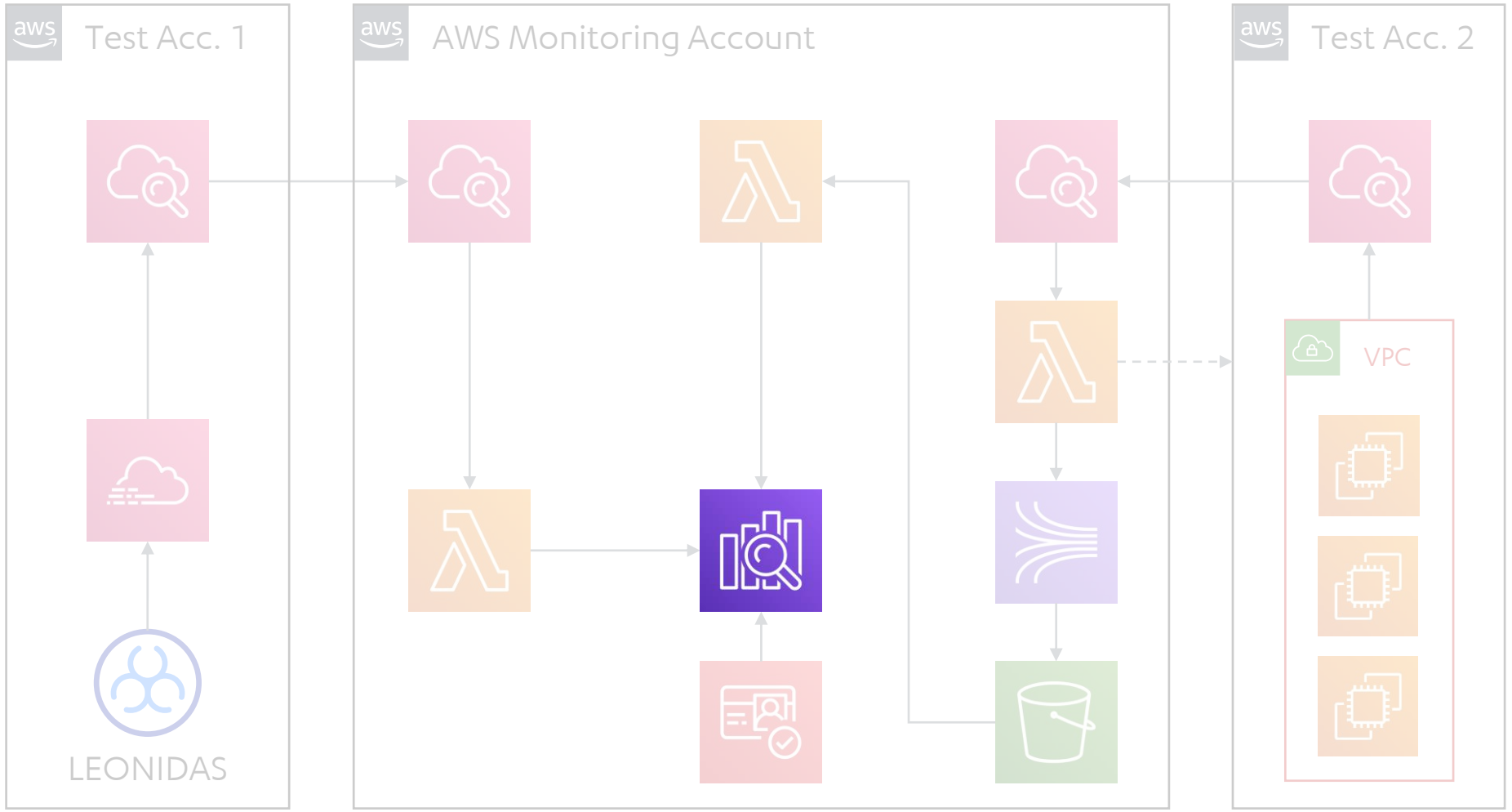
REDUCING BLAST RADIUS





GEO IP ENRICHMENT

```
jsonSubString = extractJson(message);
if (jsonSubString !== null) {

    var source = JSON.parse(jsonSubString);
    if (source['sourceIPAddress']) {
        var geoInfo = geoip.lookup(source['sourceIPAddress']);

        if (geoInfo) {
            source['geoip'] = geoInfo;
            if (geoInfo['ll']) {
                source['geoip']['ll'].reverse(); // Does not conform to GeoJSON format!
            }
        }
    }
    return source;
}
```

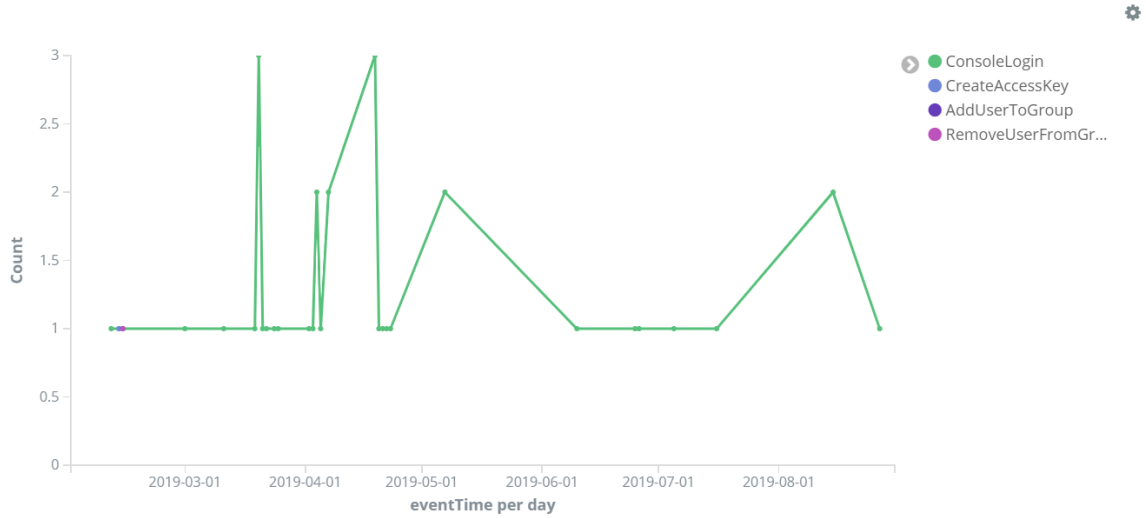


IAM Key Events

0
New Users Created

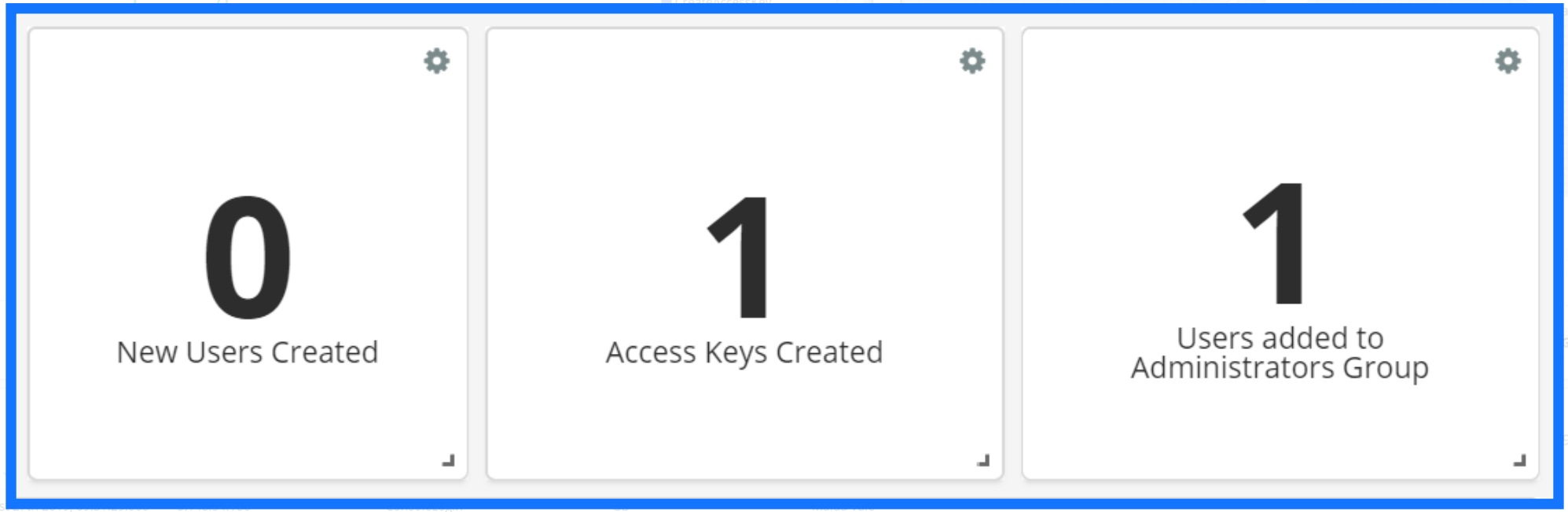
1
Access Keys Created

1
Users added to Administrators Group



1–39 of 39

Time	sourceIPAddress	eventName	geoip.country	geoip.city	requestParameters.userName	requestParameters.groupName
August 27th 2019, 09:31:29.000	5.148.34.186	ConsoleLogin	GB	Maida Vale	-	-
August 15th 2019, 01:11:50.000	109.231.195.254	ConsoleLogin	GB	Crowborough	-	-
August 15th 2019, 01:11:34.000	109.231.195.254	ConsoleLogin	GB	Crowborough	-	-
July 16th 2019, 21:39:28.000	85.255.237.65	ConsoleLogin	GB		-	-
July 5th 2019, 10:42:50.000	5.148.34.186	ConsoleLogin	GB	Maida Vale	-	-
June 26th 2019, 13:59:45.000	109.231.195.254	ConsoleLogin	GB	Crowborough	-	-
June 25th 2019, 18:22:22.000	109.231.195.254	ConsoleLogin	GB	Crowborough	-	-
June 10th 2019, 19:45:12.000	109.231.195.254	ConsoleLogin	GB	Crowborough	-	-
May 7th 2019, 13:38:42.000	5.148.34.186	ConsoleLogin	GB	Maida Vale	-	-


0
New Users Created
1
Access Keys Created
1
Users added to Administrators Group

IAM Key Events

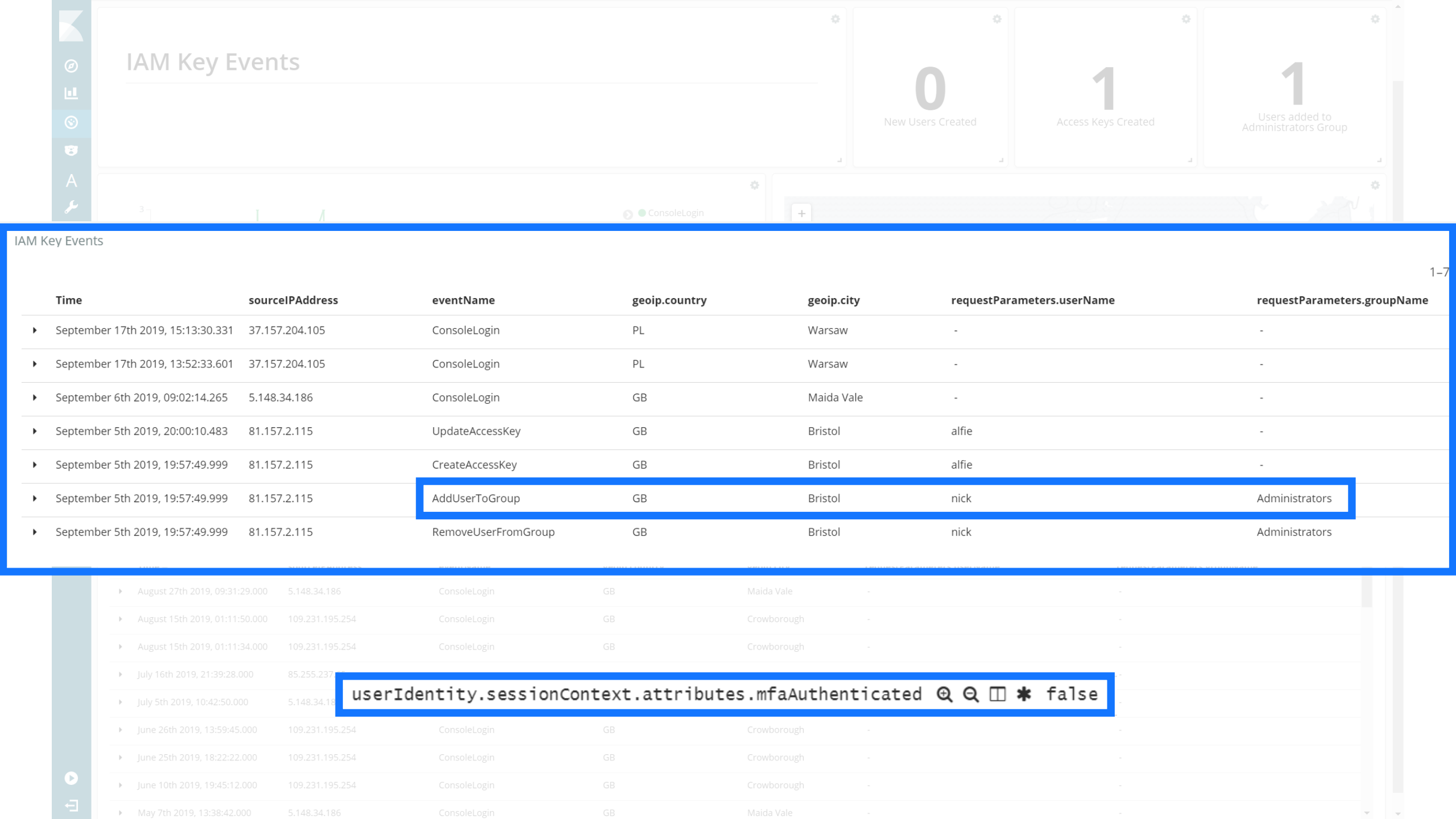
0
New Users Created

1
Access Keys Created

1
Users added to Administrators Group

1–39 of 39

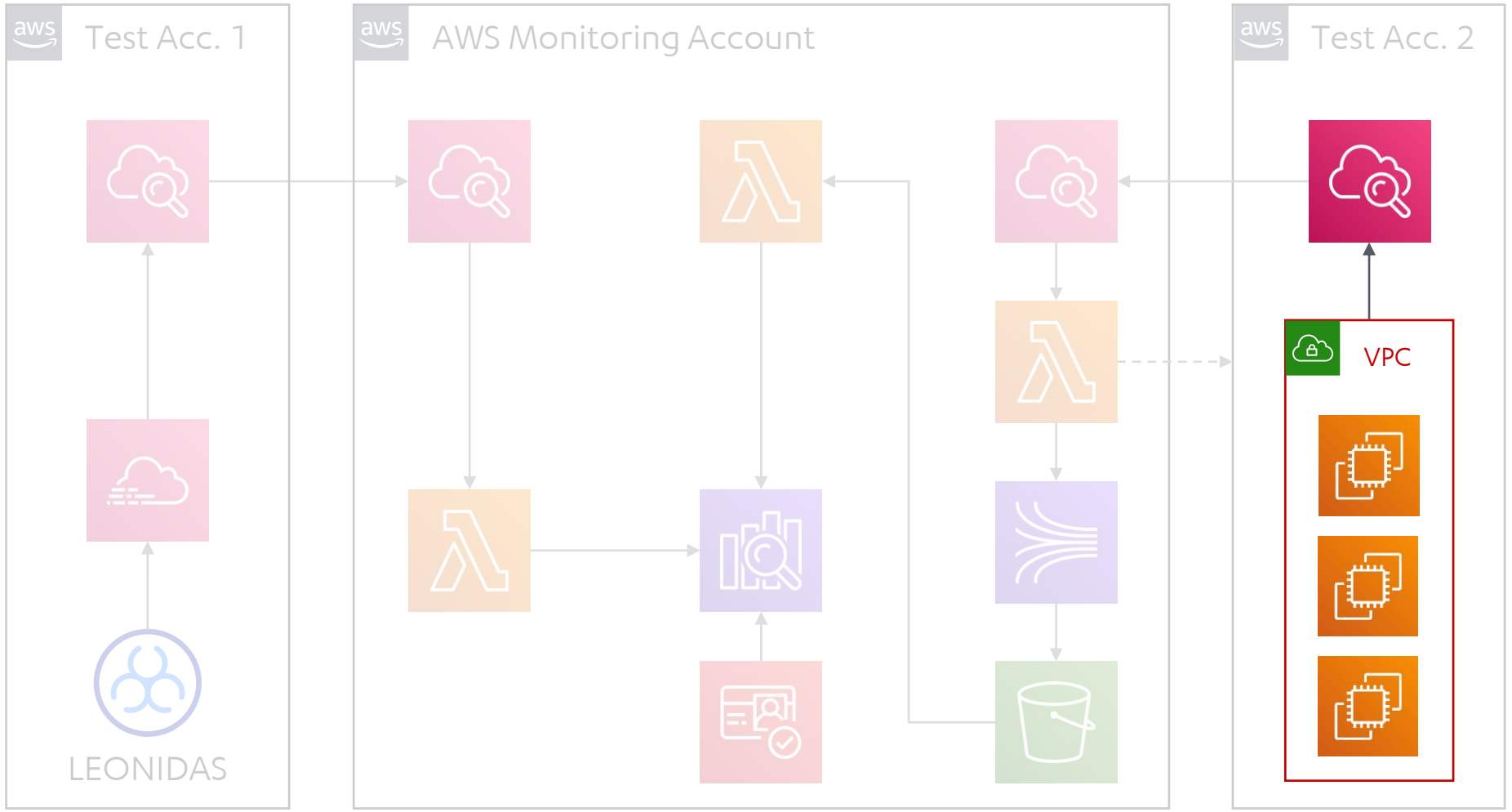
Time	sourceIPAddress	eventName	awsRegion	userAgent	requestParameters.groupName
August 27th 2019, 09:31:29.000	5.148.34.186				-
August 15th 2019, 01:11:50.000	109.231.195.254	ConsoleLogin	GB	Crowborough	-
August 15th 2019, 01:11:34.000	109.231.195.254	ConsoleLogin	GB	Crowborough	-
July 16th 2019, 21:39:28.000	85.255.237.65	ConsoleLogin	GB		-
July 5th 2019, 10:42:50.000	5.148.34.186	ConsoleLogin	GB	Maida Vale	-
June 26th 2019, 13:59:45.000	109.231.195.254	ConsoleLogin	GB	Crowborough	-
June 25th 2019, 18:22:22.000	109.231.195.254	ConsoleLogin	GB	Crowborough	-
June 10th 2019, 19:45:12.000	109.231.195.254	ConsoleLogin	GB	Crowborough	-
May 7th 2019, 13:38:42.000	5.148.34.186	ConsoleLogin	GB	Maida Vale	-



IAM Key Events

1–7

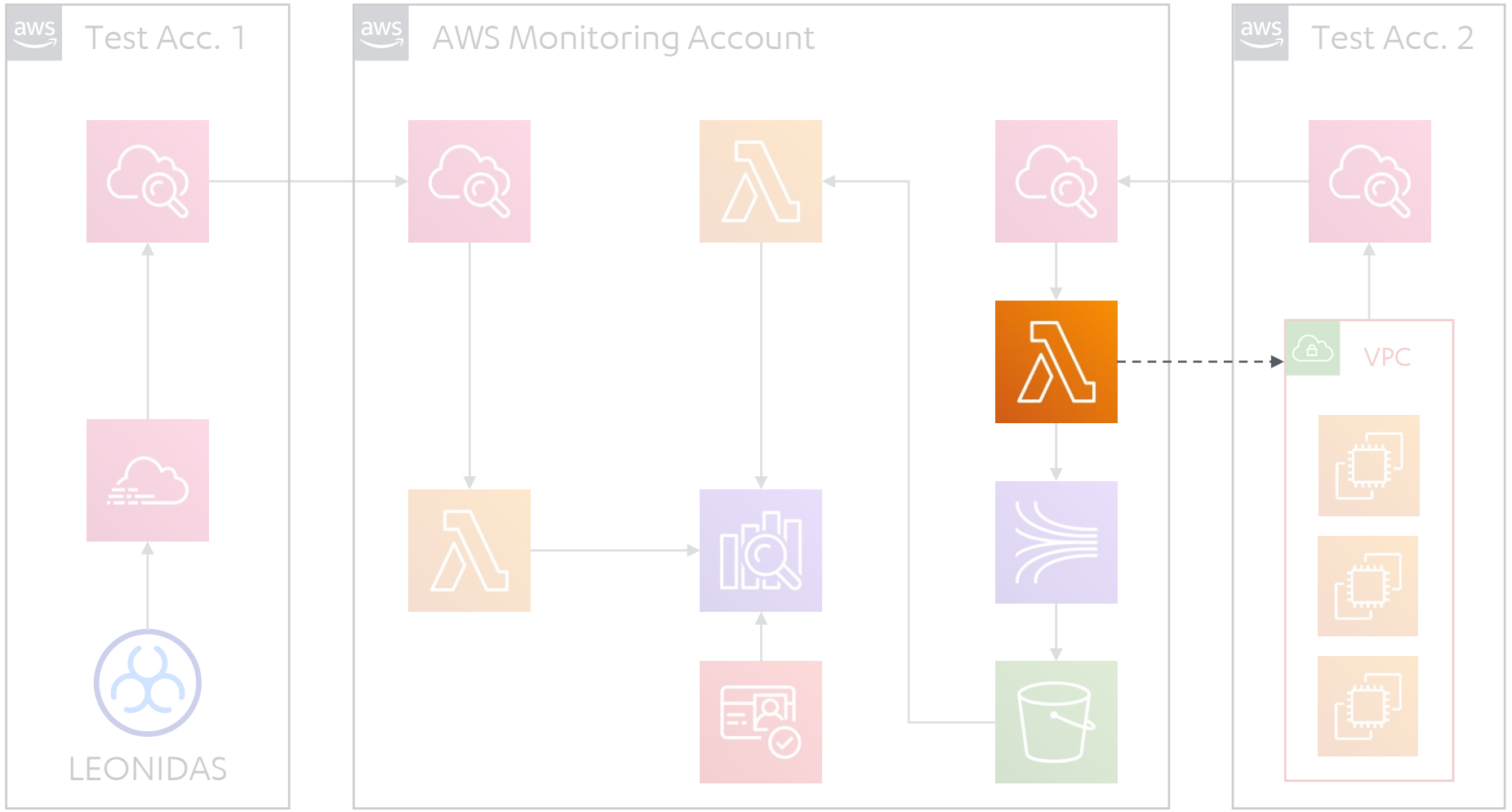
Time	sourceIPAddress	eventName	geoip.country	geoip.city	requestParameters.userName	requestParameters.groupName
September 17th 2019, 15:13:30.331	37.157.204.105	ConsoleLogin	PL	Warsaw	-	-
September 17th 2019, 13:52:33.601	37.157.204.105	ConsoleLogin	PL	Warsaw	-	-
September 6th 2019, 09:02:14.265	5.148.34.186	ConsoleLogin	GB	Maida Vale	-	-
September 5th 2019, 20:00:10.483	81.157.2.115	UpdateAccessKey	GB	Bristol	alfie	-
September 5th 2019, 19:57:49.999	81.157.2.115	CreateAccessKey	GB	Bristol	alfie	-
September 5th 2019, 19:57:49.999	81.157.2.115	AddUserToGroup	GB	Bristol	nick	Administrators
September 5th 2019, 19:57:49.999	81.157.2.115	RemoveUserFromGroup	GB	Bristol	nick	Administrators



VPC FLOW LOGS

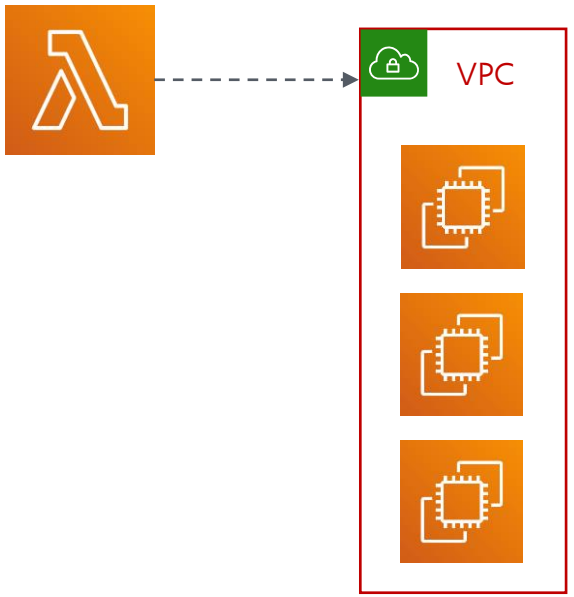
Filter events

Message
2019-09-05 14:51:22
2 870081948864 eni-0f61bb7c7df6cf46a 91.189.92.20 192.168.221.53 443 35480 6 7 4615 1567695082 1567695112 ACCEPT OK
2 870081948864 eni-0f61bb7c7df6cf46a 91.189.92.19 192.168.221.53 443 36816 6 341 497461 1567695082 1567695112 ACCEPT OK
2 870081948864 eni-0f61bb7c7df6cf46a 195.170.224.235 192.168.221.53 58636 80 6 3 140 1567695082 1567695112 ACCEPT OK
2 870081948864 eni-0f61bb7c7df6cf46a 91.189.95.15 192.168.221.53 80 52684 6 7 4967 1567695082 1567695112 ACCEPT OK
2 870081948864 eni-0f61bb7c7df6cf46a 192.168.221.53 195.170.224.235 80 58164 6 1 40 1567695082 1567695112 ACCEPT OK
2 870081948864 eni-0f61bb7c7df6cf46a 192.168.221.53 195.170.224.235 80 58636 6 1 40 1567695082 1567695112 ACCEPT OK
2 870081948864 eni-0f61bb7c7df6cf46a 192.168.221.53 18.130.123.69 22 57000 6 209 20293 1567695082 1567695112 ACCEPT OK
2 870081948864 eni-0f61bb7c7df6cf46a 192.168.221.53 185.5.16.119 80 12629 6 1 40 1567695082 1567695112 ACCEPT OK
2 870081948864 eni-0f61bb7c7df6cf46a 192.168.221.53 91.189.92.19 36816 443 6 40 2750 1567695082 1567695112 ACCEPT OK
2 870081948864 eni-0f61bb7c7df6cf46a 18.130.123.69 192.168.221.53 57000 22 6 233 174665 1567695082 1567695112 ACCEPT OK
2 870081948864 eni-0f61bb7c7df6cf46a 91.189.94.4 192.168.221.53 123 37970 17 1 76 1567695082 1567695112 ACCEPT OK
2 870081948864 eni-0f61bb7c7df6cf46a 192.168.221.53 91.189.95.15 52684 80 6 6 503 1567695082 1567695112 ACCEPT OK

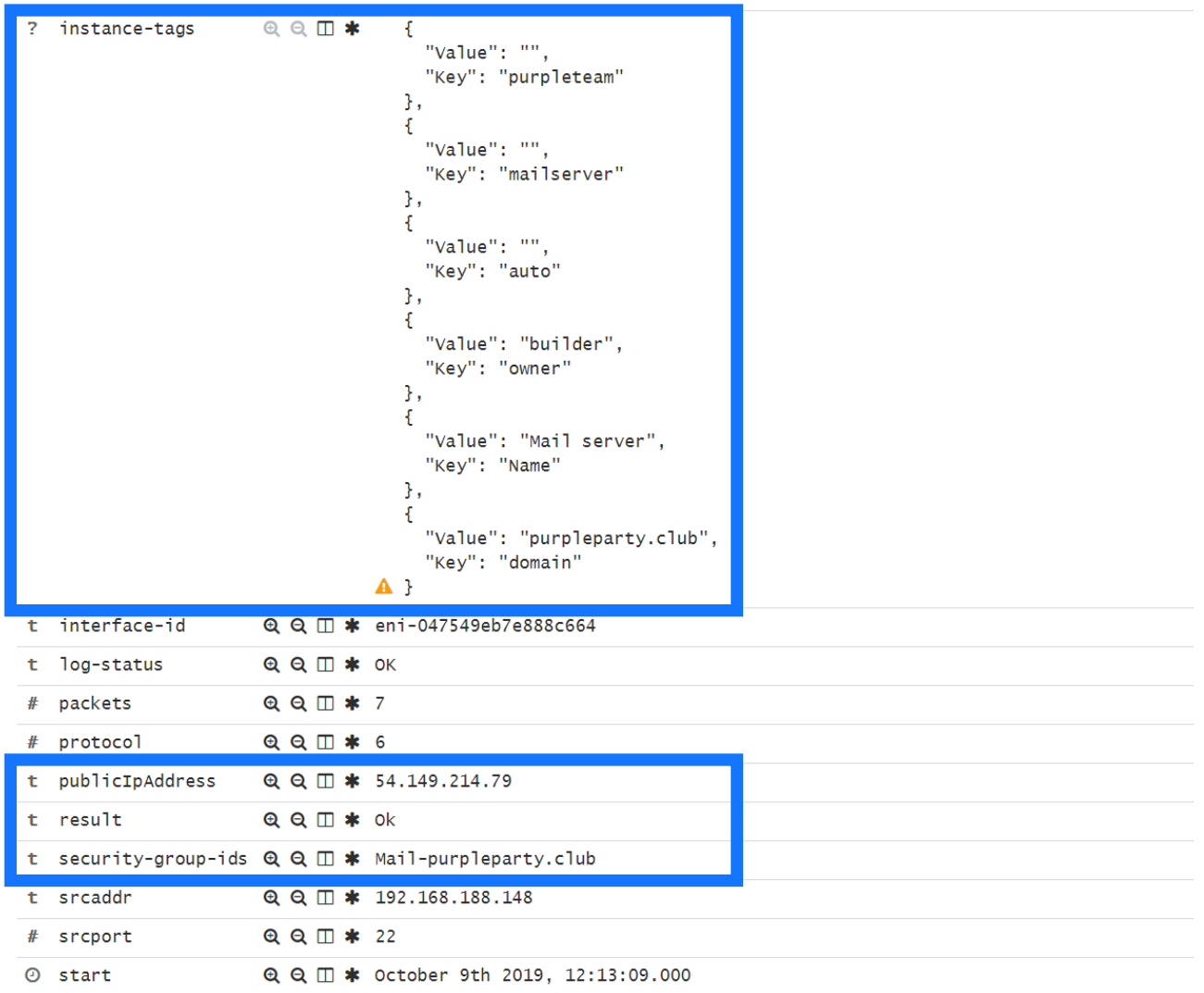


CROSS-ACCOUNT LOG ENRICHMENT

```
function decorateRecords (records, mapping) {
  console.log(`Decorating ${records.length} records`);

  for(let record of records) {
    let eniData = find(mapping, { 'interfaceId': record['interface-id'] });

    if (eniData) {
      record['security-group-ids'] = eniData.securityGroupIds;

      if (isRfc1918Address(record['destaddr']) && isRfc1918Address(record['srcaddr'])){
          record['direction'] = 'internal'
      } else if (record['destaddr'] == eniData.ipAddress) {
          record['direction'] = 'inbound';
      }
      else {
          record['direction'] = 'outbound';
      }

      record['publicIpAddress'] = eniData.publicIpAddress;
      record['instance-tags'] = eniData.instanceTags;
      record['instance-id'] = eniData.instanceId
    } else {
      console.log(`No ENI data found for interface ${record['interface-id']}`);
    }
    console.log(`${JSON.stringify(record)}`);
  }


  console.log(`Finished with ${records.length} records`);
  return Promise.resolve(records);
}
```



CROSS-ACCOUNT LOG ENRICHMENT



?	instance-tags	{ "Value": "", "Key": "purpleteam" }, { "Value": "", "Key": "mailserver" }, { "Value": "", "Key": "auto" }, { "Value": "builder", "Key": "owner" }, { "Value": "Mail server", "Key": "Name" }, { "Value": "purpleparty.club", "Key": "domain" }
t	interface-id	eni-047549eb7e888c664
t	log-status	OK
#	packets	7
#	protocol	6
t	publicIpAddress	54.149.214.79
t	result	Ok
t	security-group-ids	Mail-purpleparty.club
t	srcaddr	192.168.188.148
#	srcport	22
	start	October 9th 2019, 12:13:09.000

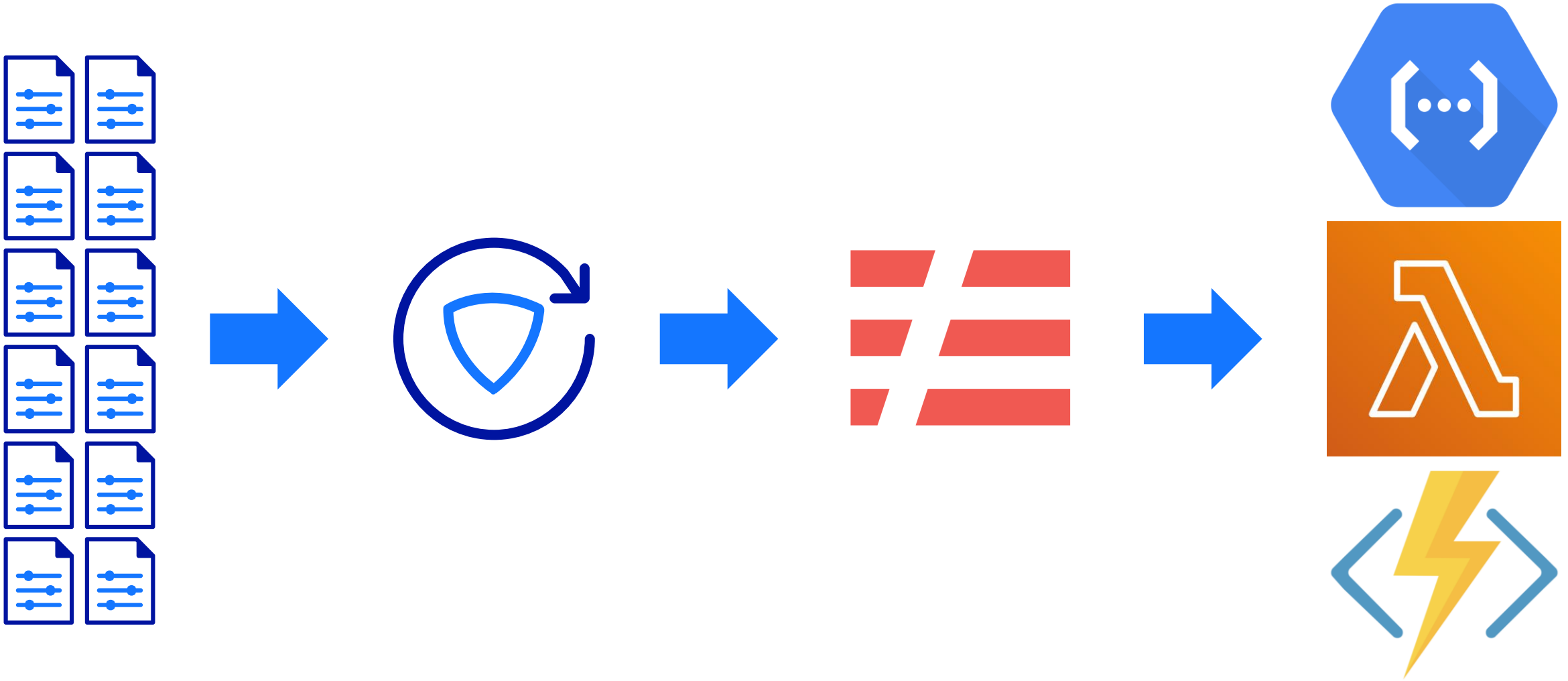
F-Secure

CROSS-ACCOUNT LOG ENRICHMENT

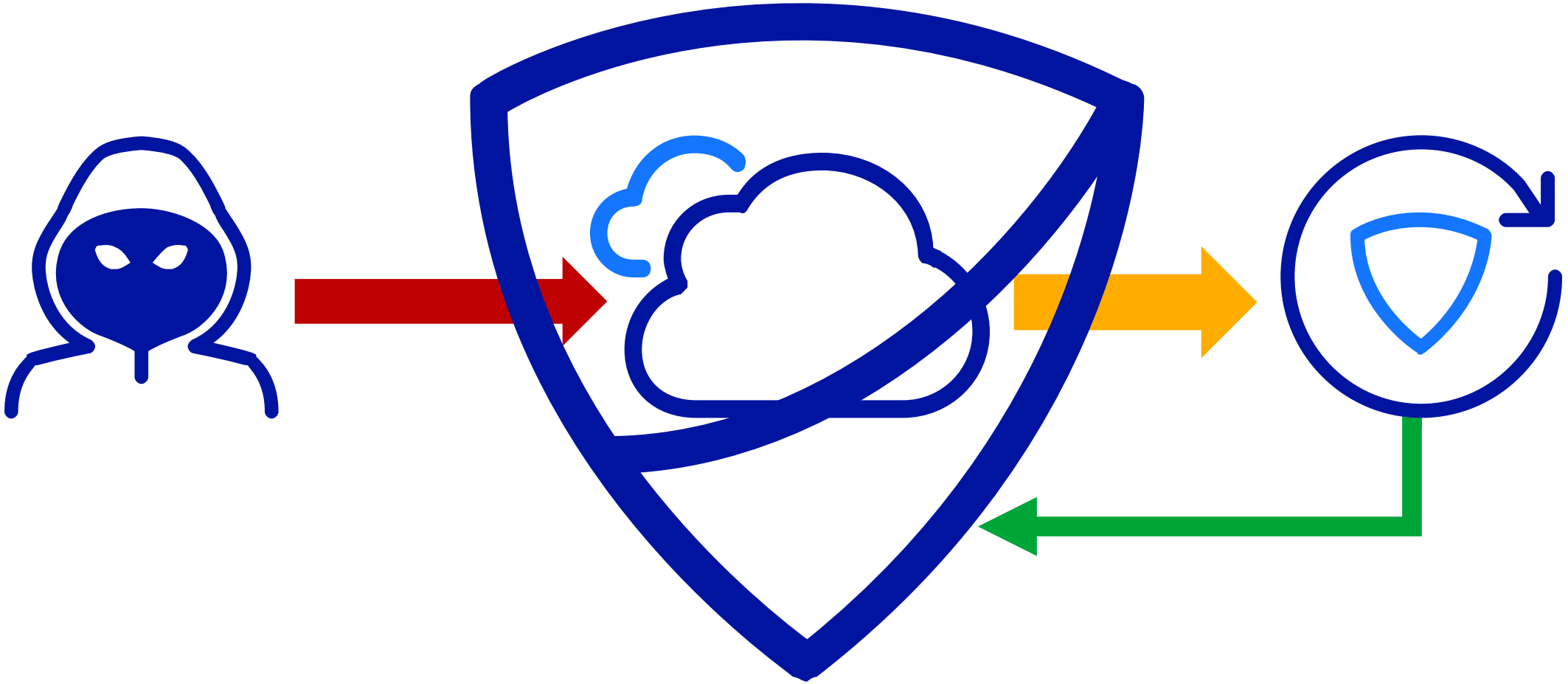
Time	srcaddr	srcport	destaddr	dstport	direction
September 5th 2019, 16:26:53.000	192.168.221.53	33,408	192.168.92.66	110	internal
September 5th 2019, 16:26:53.000	192.168.221.53	36,216	192.168.92.66	1,723	internal
September 5th 2019, 16:26:53.000	192.168.221.53	32,978	192.168.92.66	995	internal
September 5th 2019, 16:26:53.000	192.168.221.53	39,424	192.168.92.66	80	internal
September 5th 2019, 16:26:53.000	192.168.221.53	39,408	192.168.92.66	25	internal
September 5th 2019, 16:26:53.000	192.168.221.53	56,846	192.168.92.66	3,306	internal
September 5th 2019, 16:26:53.000	192.168.221.53	57,420	192.168.92.66	23	internal
September 5th 2019, 16:26:53.000	192.168.221.53	55,450	192.168.92.66	993	internal
September 5th 2019, 16:26:53.000	192.168.221.53	36,232	192.168.92.66	1,723	internal
September 5th 2019, 16:26:53.000	192.168.221.53	57,436	192.168.92.66	23	internal
September 5th 2019, 16:26:53.000	192.168.221.53	55,080	192.168.92.66	111	internal
September 5th 2019, 16:26:53.000	192.168.221.53	57,156	192.168.92.66	53	internal
September 5th 2019, 16:26:53.000	192.168.221.53	48,626	192.168.92.66	21	internal
September 5th 2019, 16:26:13.000	192.168.221.53	48,544	192.168.92.66	22	internal
September 5th 2019, 16:26:13.000	192.168.221.53	39,424	192.168.92.66	80	internal

WHERE NEXT?

EXPAND LEONIDAS

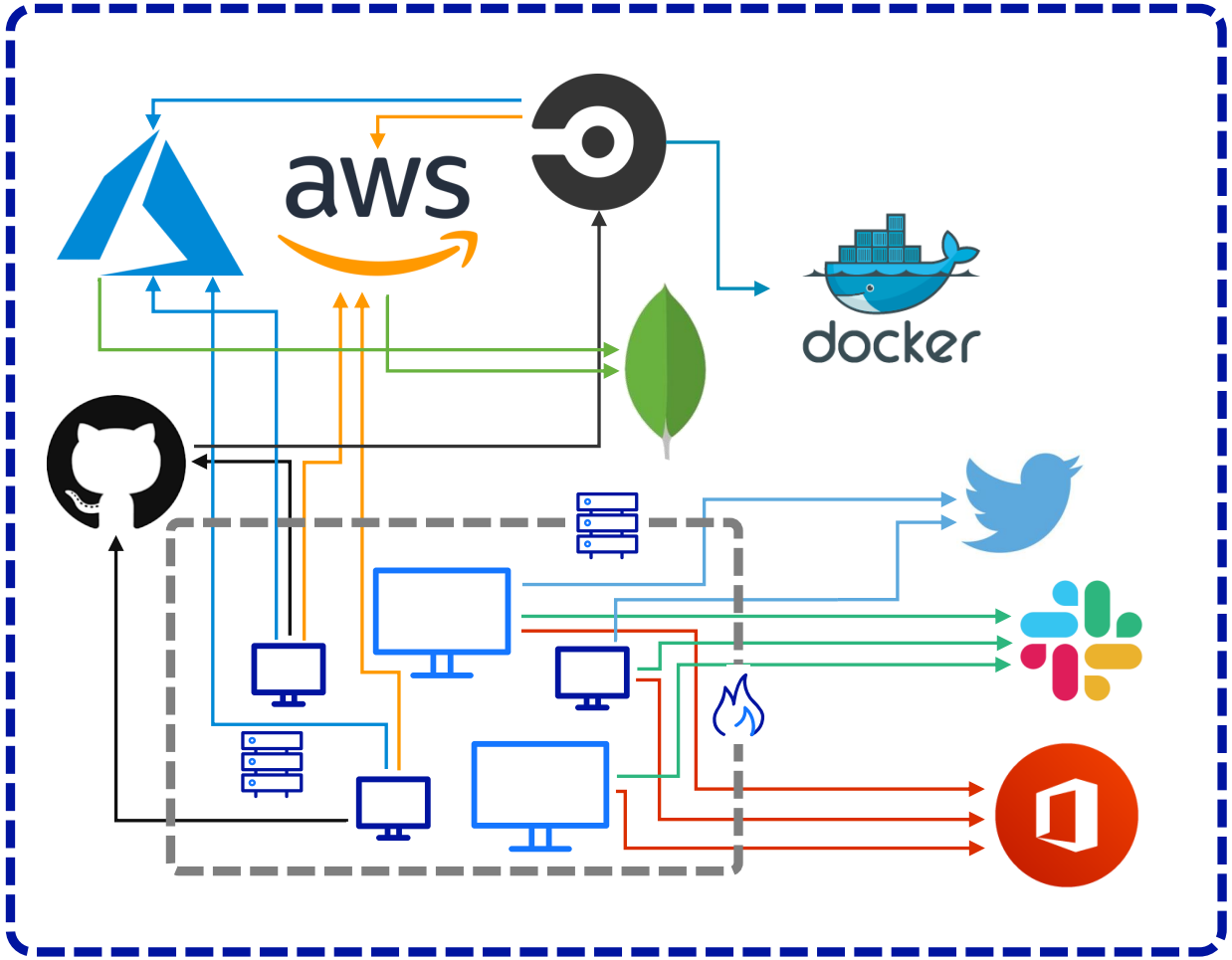


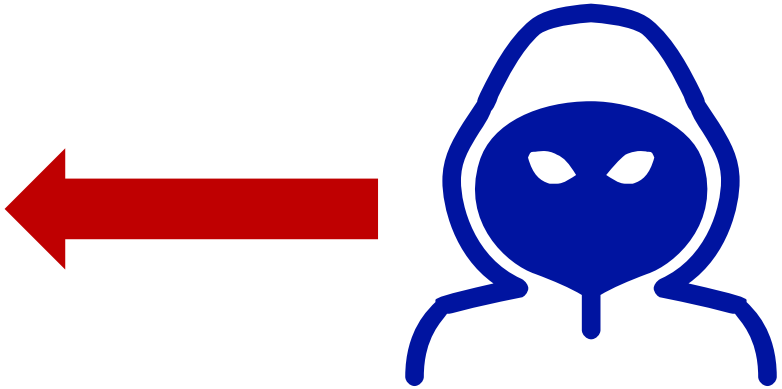
AUTOMATED RESPONSE



CONCLUSIONS

CONCLUSIONS





CONCLUSIONS