IMF 2018

Streamline AWS Security Incidents

Asif Matadar
@d1r4c

#whoami

- **Director of Endpoint Detection & Response (EDR), EMEA at Tanium**

- **Seasoned Incident Response professional with over 7 years' experience leading high-profile cases around the world, such as advanced targeted attacks, nation-state attacks, and data breaches, to name a few**

- **Public speaker at industry recognised conferences around the world:**
  - OSDFCon 2017
  - BSidesNOLA 2017
  - BSidesMCR 2015

- **Research focus on memory analysis and automation, *nix based forensics, cloud forensics, and triage analysis**

Streamline AWS Security Incidents

- **As Amazon AWS becomes more prevalent within organisations, there has been a significant rise in AWS compromises**

- **Due to how quick AWS deployments can be:**
  - Virtual machines can be spun-up in quick succession
  - Fast deployment of AWS S3 buckets
  - False sense of security in relation to AWS which is resulting in the increase of breaches

- **This talk will detail the challenges of undergoing AWS incidents and how DFIR professionals can streamline the process during an Incident Response engagement and uncover vital artefacts along with components that are usually overlooked**

Challenges with AWS environments

- **There are challenges with AWS environments during Incident Response engagements, such as:**
  - Lack of inventory:
    - Virtual machines
    - AWS S3 Buckets
    - Firewalls
    - AWS Network Appliances
  - Lack of visibility:
    - Delays triage analysis for Investigators
    - Opportunities to take advantage of Threat Hunting are not taken
  - Regional environments – Europe, US, etc
  - Large organisations have many AWS accounts to administer

Artefacts to keep in mind

- Due to the lack of documentation on AWS, it makes it difficult for IR teams to investigate an AWS intrusion with due diligence

- Many components within AWS so even the most experienced IR teams can find it difficult

- There are many artefacts on AWS environment to keep in mind which I will discuss in detail

CloudFront

- CloudFront is a web service that speeds up distribution of your static and dynamic web content, such as .html, .css, .js, and image files, to your users

- Content Delivery Network (CDN) provided by Amazon Web Services (AWS)

- CloudFront users create "distributions" that serve content from specific sources

CloudFront

- Create an Amazon S3 bucket for your Amazon CloudFront access logs to be delivered to and stored in

- Configure Amazon S3 event notification on the CloudFront access logs bucket, which contains the raw logs, to trigger the Lambda pre-processing function

- CloudFront Logs are useful during the analysis process whilst an incident is underway or post-breach

CloudFront

- **There are 2 types of logs:**
- **Web Distribution Logs**
  - Are used to serve static and dynamic content:
    - Provides information about a specific user request
    - Fields that are worth keeping a close eye on during analysis include:
      - date, time, sc-bytes, c-ip, cs-method, sc-status, cs(User-Agent), x-host-header, and cs-bytes

CloudFront

- **RTMP Distribution Logs**
  - RTMP (Real-Time Messaging Protocol) Distribution Logs corresponds to each record in an RTMP access log which represents a playback event, for example connect, play, pause, stop, and disconnect
  - Fields to keep in mind whilst undergoing analysis are:
    - date, time, c-ip, x-event, sc-bytes, cs-uri-query, x-page-url, and c-user-agent

CloudTrail

- CloudTrail provides event history of your AWS account activity, such as actions taken place through the AWS Management Console, AWS SDKs, command line tools, and other AWS services

- CloudTrail allows one to have visibility of user and resource activity by recording AWS Management Console events and API calls

- Login attempts with actions taken can be determined along with firewall changes

- 7 days worth of logs:
  - Log retention is recommended

CloudTrail Extract

- "awsRegion": "eu-west-1",
- "eventName": "AuthorizeSecurityGroupIngress",
- "eventSource": "ec2.amazonaws.com",
- "eventTime": "2018-03-30T11:32:01Z",
- "eventType": "AwsApiCall",
- "groupId": "sg-902asdlkj",
- "sourceIPAddress": "123.11.9.89",
- "accessKeyId": "PQWE23412834SDKFJ",
- "accountId": "123097803810",
- "arn": "arn:aws:iam::123097803810:user/user-account@example.com",
- "userName": "user-account@example.com"

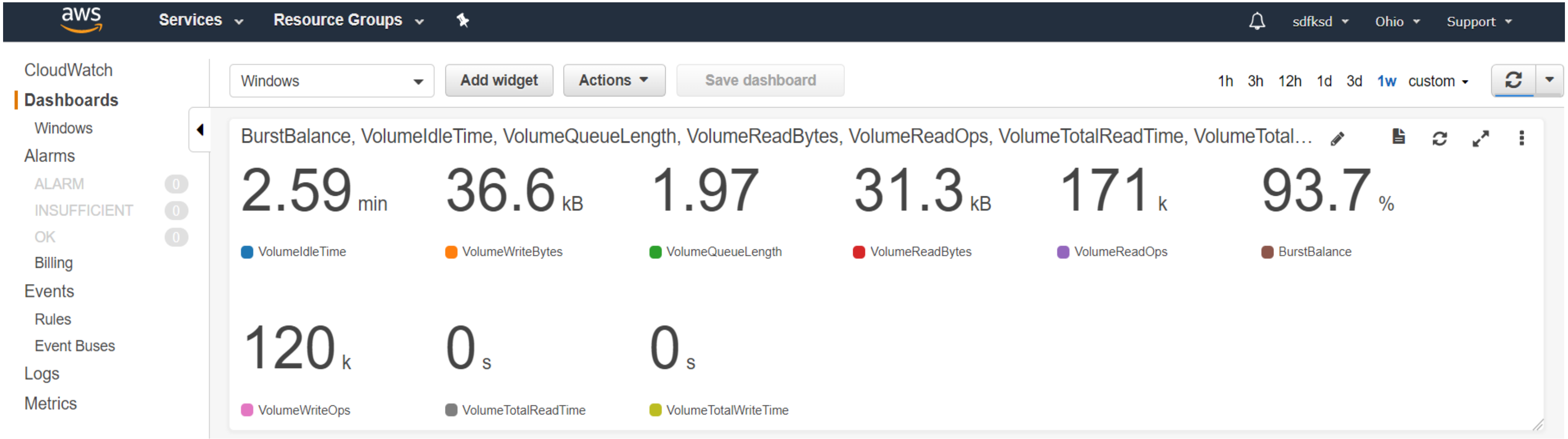
CloudWatch

- **CloudWatch Logs can be used to collect, monitor and set alarms based on events**

- **CloudWatch Logs can be monitored in real-time**

- **CloudWatch Archive Logs can be retained for analysis:**
  - Useful for post-breach incidents

CloudWatch Extract



BurstBalance, VolumeIdleTime, VolumeQueueLength, VolumeReadBytes, VolumeReadOps, VolumeTotalReadTime, VolumeTotal…

2.59 min
■ VolumeIdleTime

36.6 kB
■ VolumeWriteBytes

1.97
■ VolumeQueueLength

31.3 kB
■ VolumeReadBytes

171 k
■ VolumeReadOps

93.7 %
■ BurstBalance

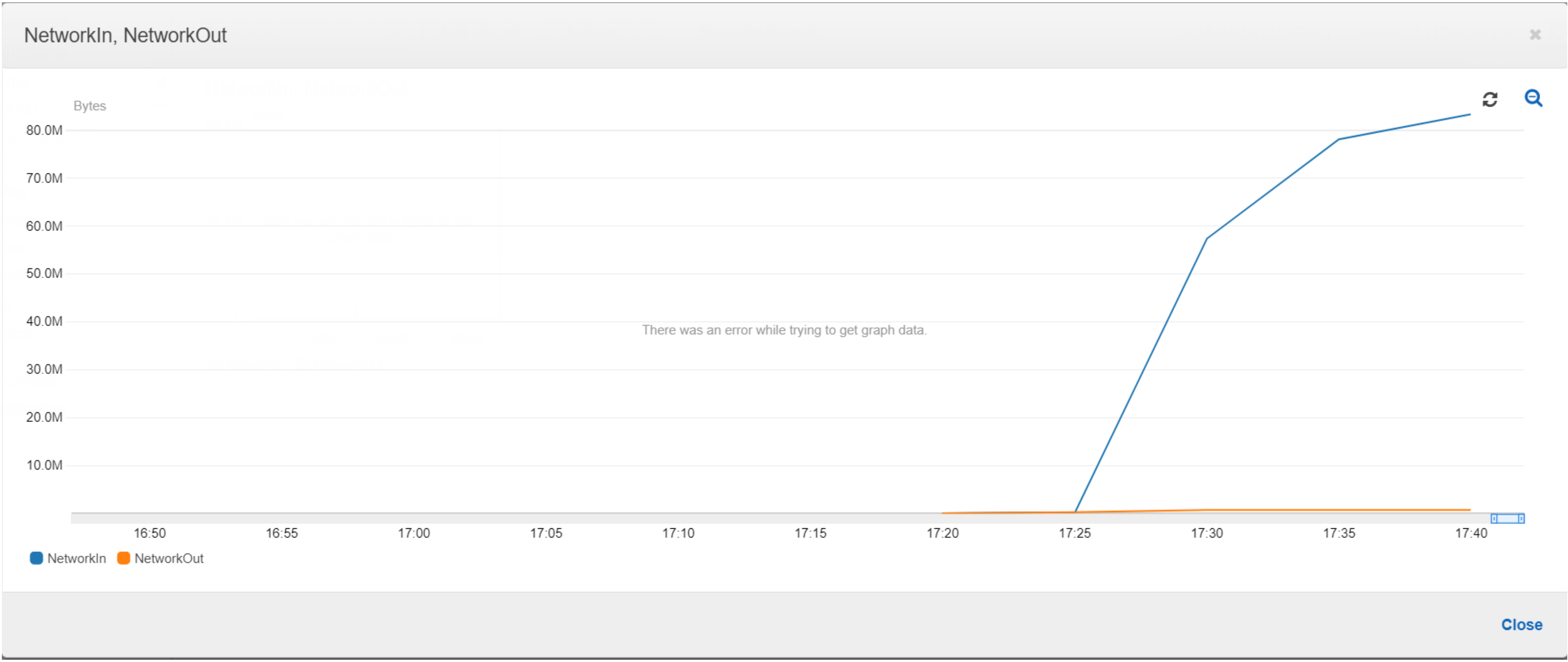
120 k
■ VolumeWriteOps

0 s
■ VolumeTotalReadTime

0 s
■ VolumeTotalWriteTime

CloudWatch Extract

- Exfiltration alarms can be set



NetworkIn, NetworkOut

There was an error while trying to get graph data.

VPC Flow Logs

- Enables you to capture information about the IP traffic going to and from network interfaces in your VPC

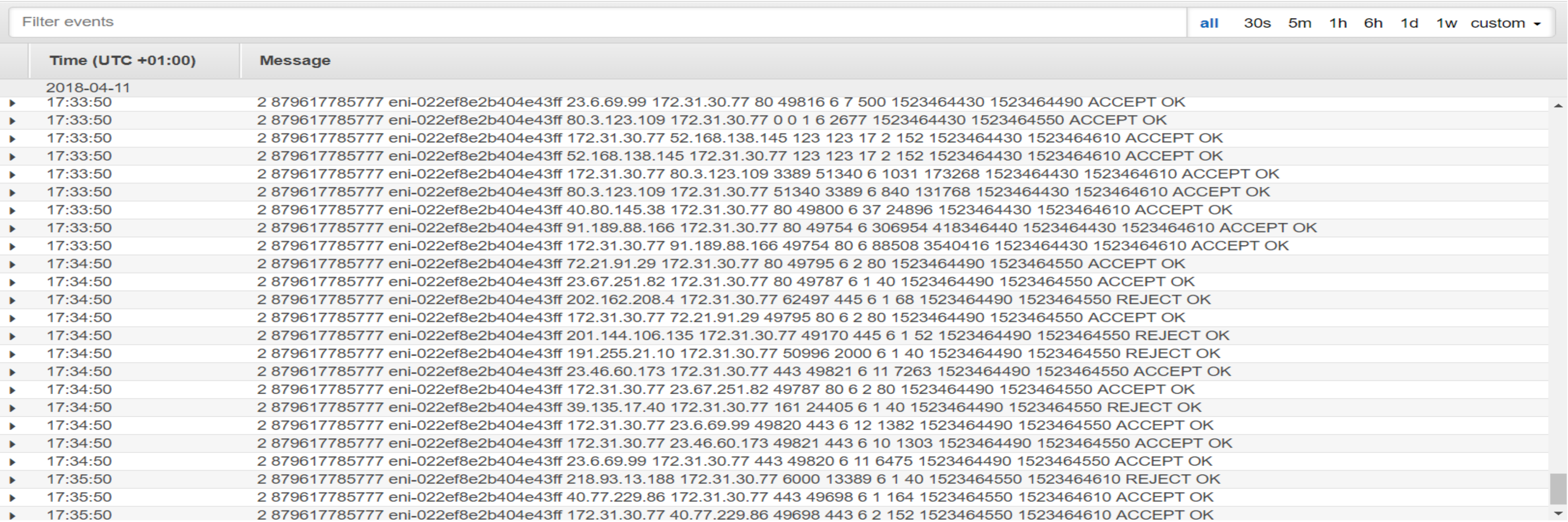
- Useful when troubleshooting network traffic

- VPC Flow Logs can be viewed through CloudWatch

- Can be useful during an incident or post-breach to determine network perimeter activity for signs of intrusions:
  - Lateral Movement
  - Command and Control
  - Exfiltration

VPC Flow Logs Extract

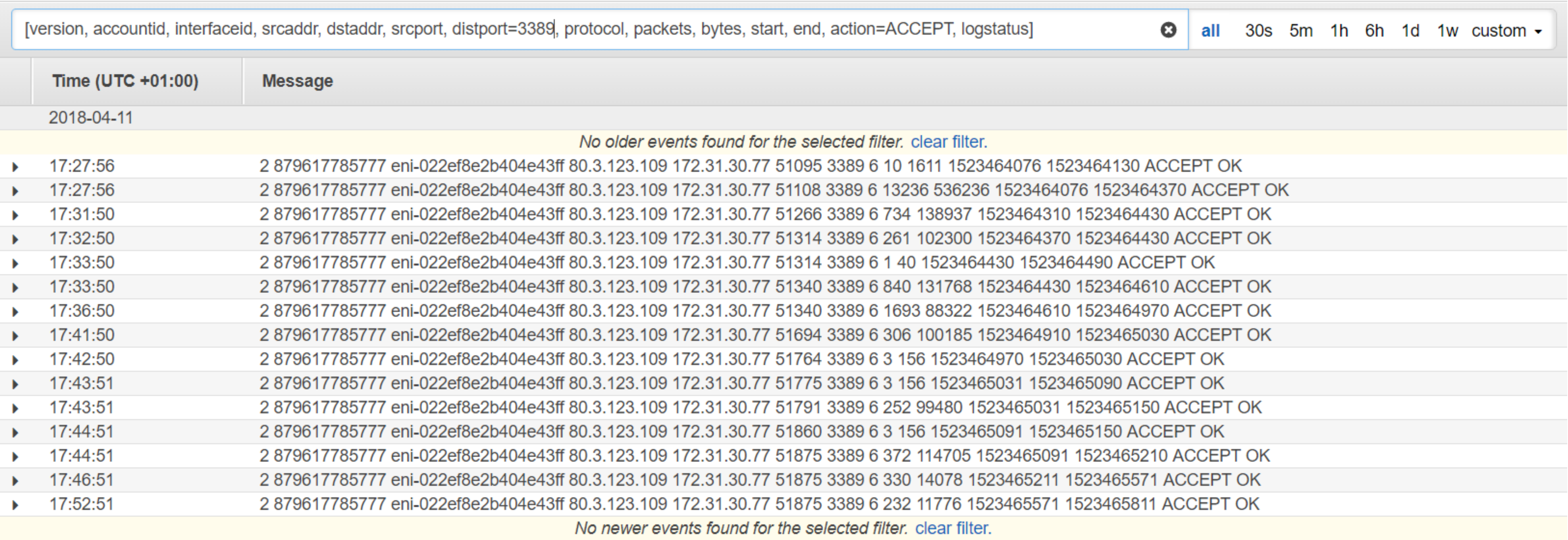
- Events can be filtered



```
Time (UTC +01:00)   Message
2018-04-11
17:33:50   2 879617785777 eni-022ef8e2b404e43ff 23.6.69.99 172.31.30.77 80 49816 6 7 500 1523464430 1523464490 ACCEPT OK
17:33:50   2 879617785777 eni-022ef8e2b404e43ff 80.3.123.109 172.31.30.77 0 0 1 6 2677 1523464430 1523464550 ACCEPT OK
17:33:50   2 879617785777 eni-022ef8e2b404e43ff 172.31.30.77 52.168.138.145 123 123 17 2 152 1523464430 1523464610 ACCEPT OK
17:33:50   2 879617785777 eni-022ef8e2b404e43ff 52.168.138.145 172.31.30.77 123 123 17 2 152 1523464430 1523464610 ACCEPT OK
17:33:50   2 879617785777 eni-022ef8e2b404e43ff 172.31.30.77 80.3.123.109 3389 51340 6 1031 173268 1523464430 1523464610 ACCEPT OK
17:33:50   2 879617785777 eni-022ef8e2b404e43ff 80.3.123.109 172.31.30.77 51340 3389 6 840 131768 1523464430 1523464610 ACCEPT OK
17:33:50   2 879617785777 eni-022ef8e2b404e43ff 40.80.145.38 172.31.30.77 80 49800 6 37 24896 1523464430 1523464610 ACCEPT OK
17:33:50   2 879617785777 eni-022ef8e2b404e43ff 91.189.88.166 172.31.30.77 80 49754 6 306954 418346440 1523464430 1523464610 ACCEPT OK
17:33:50   2 879617785777 eni-022ef8e2b404e43ff 172.31.30.77 91.189.88.166 49754 80 6 88508 3540416 1523464430 1523464610 ACCEPT OK
17:34:50   2 879617785777 eni-022ef8e2b404e43ff 72.21.91.29 172.31.30.77 80 49795 6 2 80 1523464490 1523464550 ACCEPT OK
17:34:50   2 879617785777 eni-022ef8e2b404e43ff 23.67.251.82 172.31.30.77 80 49787 6 1 40 1523464490 1523464550 ACCEPT OK
17:34:50   2 879617785777 eni-022ef8e2b404e43ff 202.162.208.4 172.31.30.77 62497 445 6 1 68 1523464490 1523464550 REJECT OK
17:34:50   2 879617785777 eni-022ef8e2b404e43ff 172.31.30.77 72.21.91.29 49795 80 6 2 80 1523464490 1523464550 ACCEPT OK
17:34:50   2 879617785777 eni-022ef8e2b404e43ff 201.144.106.135 172.31.30.77 49170 445 6 1 52 1523464490 1523464550 REJECT OK
17:34:50   2 879617785777 eni-022ef8e2b404e43ff 191.255.21.10 172.31.30.77 50996 2000 6 1 40 1523464490 1523464550 REJECT OK
17:34:50   2 879617785777 eni-022ef8e2b404e43ff 23.46.60.173 172.31.30.77 443 49821 6 11 7263 1523464490 1523464550 ACCEPT OK
17:34:50   2 879617785777 eni-022ef8e2b404e43ff 172.31.30.77 23.67.251.82 49787 80 6 2 80 1523464490 1523464550 ACCEPT OK
17:34:50   2 879617785777 eni-022ef8e2b404e43ff 39.135.17.40 172.31.30.77 161 24405 6 1 40 1523464490 1523464550 REJECT OK
17:34:50   2 879617785777 eni-022ef8e2b404e43ff 172.31.30.77 23.6.69.99 49820 443 6 12 1382 1523464490 1523464550 ACCEPT OK
17:34:50   2 879617785777 eni-022ef8e2b404e43ff 172.31.30.77 23.46.60.173 49821 443 6 10 1303 1523464490 1523464550 ACCEPT OK
17:34:50   2 879617785777 eni-022ef8e2b404e43ff 23.6.69.99 172.31.30.77 443 49820 6 11 6475 1523464490 1523464550 ACCEPT OK
17:35:50   2 879617785777 eni-022ef8e2b404e43ff 218.93.13.188 172.31.30.77 6000 13389 6 1 40 1523464550 1523464610 REJECT OK
17:35:50   2 879617785777 eni-022ef8e2b404e43ff 40.77.229.86 172.31.30.77 443 49698 6 1 164 1523464550 1523464610 ACCEPT OK
17:35:50   2 879617785777 eni-022ef8e2b404e43ff 172.31.30.77 40.77.229.86 49698 443 6 2 152 1523464550 1523464610 ACCEPT OK
```

VPC Flow Logs Extract

- You can narrow the search criteria to a specific port, as such:



[version, accountid, interfaceid, srcaddr, dstaddr, srcport, distport=3389, protocol, packets, bytes, start, end, action=ACCEPT, logstatus]

```
Time (UTC +01:00)   Message
2018-04-11
                    No older events found for the selected filter. clear filter.
17:27:56            2 879617785777 eni-022ef8e2b404e43ff 80.3.123.109 172.31.30.77 51095 3389 6 10 1611 1523464076 1523464130 ACCEPT OK
17:27:56            2 879617785777 eni-022ef8e2b404e43ff 80.3.123.109 172.31.30.77 51108 3389 6 13236 536236 1523464076 1523464370 ACCEPT OK
17:31:50            2 879617785777 eni-022ef8e2b404e43ff 80.3.123.109 172.31.30.77 51266 3389 6 734 138937 1523464310 1523464430 ACCEPT OK
17:32:50            2 879617785777 eni-022ef8e2b404e43ff 80.3.123.109 172.31.30.77 51314 3389 6 261 102300 1523464370 1523464430 ACCEPT OK
17:33:50            2 879617785777 eni-022ef8e2b404e43ff 80.3.123.109 172.31.30.77 51314 3389 6 1 40 1523464430 1523464490 ACCEPT OK
17:33:50            2 879617785777 eni-022ef8e2b404e43ff 80.3.123.109 172.31.30.77 51340 3389 6 840 131768 1523464430 1523464610 ACCEPT OK
17:36:50            2 879617785777 eni-022ef8e2b404e43ff 80.3.123.109 172.31.30.77 51340 3389 6 1693 88322 1523464610 1523464970 ACCEPT OK
17:41:50            2 879617785777 eni-022ef8e2b404e43ff 80.3.123.109 172.31.30.77 51694 3389 6 306 100185 1523464910 1523465030 ACCEPT OK
17:42:50            2 879617785777 eni-022ef8e2b404e43ff 80.3.123.109 172.31.30.77 51764 3389 6 3 156 1523464970 1523465030 ACCEPT OK
17:43:51            2 879617785777 eni-022ef8e2b404e43ff 80.3.123.109 172.31.30.77 51775 3389 6 3 156 1523465031 1523465090 ACCEPT OK
17:43:51            2 879617785777 eni-022ef8e2b404e43ff 80.3.123.109 172.31.30.77 51791 3389 6 252 99480 1523465031 1523465150 ACCEPT OK
17:44:51            2 879617785777 eni-022ef8e2b404e43ff 80.3.123.109 172.31.30.77 51860 3389 6 3 156 1523465091 1523465150 ACCEPT OK
17:44:51            2 879617785777 eni-022ef8e2b404e43ff 80.3.123.109 172.31.30.77 51875 3389 6 372 114705 1523465091 1523465210 ACCEPT OK
17:46:51            2 879617785777 eni-022ef8e2b404e43ff 80.3.123.109 172.31.30.77 51875 3389 6 330 14078 1523465211 1523465571 ACCEPT OK
17:52:51            2 879617785777 eni-022ef8e2b404e43ff 80.3.123.109 172.31.30.77 51875 3389 6 232 11776 1523465571 1523465811 ACCEPT OK
                    No newer events found for the selected filter. clear filter.
```

[version, accountid, interfaceid, srcaddr, dstaddr, srcport, distport=3389, protocol, packets, bytes, start, end, action=ACCEPT, logstatus]

VPC Flow Logs

- **It is more efficient to download the logs offline and feed into an SIEM solution during an incident or post-breach**

- **Stacking technique can be used:**
  - Ports:
    - SSH, HTTP, HTTPS, MS-SQL, MySQL, NETBIOS, SMB, …
  - Destination and Source IP addresses
  - Known Bad IP addresses
  - Byte size for inbound and outbound connections

- **Grouping**

Config

- **Config Logs provide valuable information, such as:**
  - AWS resource inventory
  - Configuration history
  - Configuration change notifications
  - Resource configuration

Elastic Load Balancing

- **Elastic Load Balancing provides access logs that capture detailed information about requests sent to your load balancer, such as:**

  - Client IP address
  - Source IP address
  - Server responses
  - Latencies
  - Application errors
  - High volume applications can be monitored for performance
  - Trend analysis for different applications and systems can be made

Redshift

- **Redshift Logs allows one to monitor database security:**
  - Authentication:
    - Connections
    - Disconnections
  - User activity:
    - Queries are logged before they are run on the database
  - User:
    - Changes made to the database user definitions

Redshift

- **Attacker activity can be determined:**
  - Queries made on databases
- **Compromised accounts can be identified:**
  - Successful and failed connections
- **Advanced targeted attacks will focus on important databases**

Web Application Firewall

- Web Application Firewall Logs allows one to monitor HTTP and HTTPS requests

- Allow and block requests on the WAF

- Custom rules on the WAF can block common attack patterns:
  - SQL injection
  - Remote code execution
  - Cross-site scripting

Web Application Firewall

- **Can be instrumental during an incident or post-breach:**
  - HTTP GET requests
  - HTTP POST requests
  - Allowed requests
  - Brute-force requests
  - Frequency Analysis on specific web applications:
    - HTTP Status codes:
      - 200
      - 3**
      - 4**
      - 5**

Server Access Logging (S3 Logs)

- **S3 Logs allows one to track requests for access to your bucket**

- **Each access log provides details on the following:**
  - Requester
  - Bucket name
  - Request time
  - Request action
  - Response status
  - Error codes

Server Access Logging (S3 Logs)

- **Can be useful for Investigators to identify signs of intrusions:**
  - Bucket owner that was requested
  - Date and time of the request
  - Remote IP address that made the request
  - HTTP Methods:
    - GET
    - POST
  - Number of response bytes sent
  - HTTP User Agent headers

API Gateway

- **Amazon API Gateway is an AWS service that enables developers to create, publish, maintain, monitor, and secure APIs at any scale**

- **API Gateway lets you create, configure, and host a RESTful API to enable applications to access the AWS Cloud**

- **There are two kinds of developers who use API Gateway:**

  1) app developers

  2) API developers

API Gateway

- **API Gateway Logs are beneficial for Investigators:**
  - API calls
  - Tracks execution
  - Latency
  - API Gateway to CloudWatch - This is a two step process:

    1) Create an IAM role that allows API Gateway to write logs in CloudWatch

    2) Turn on logging for our API project

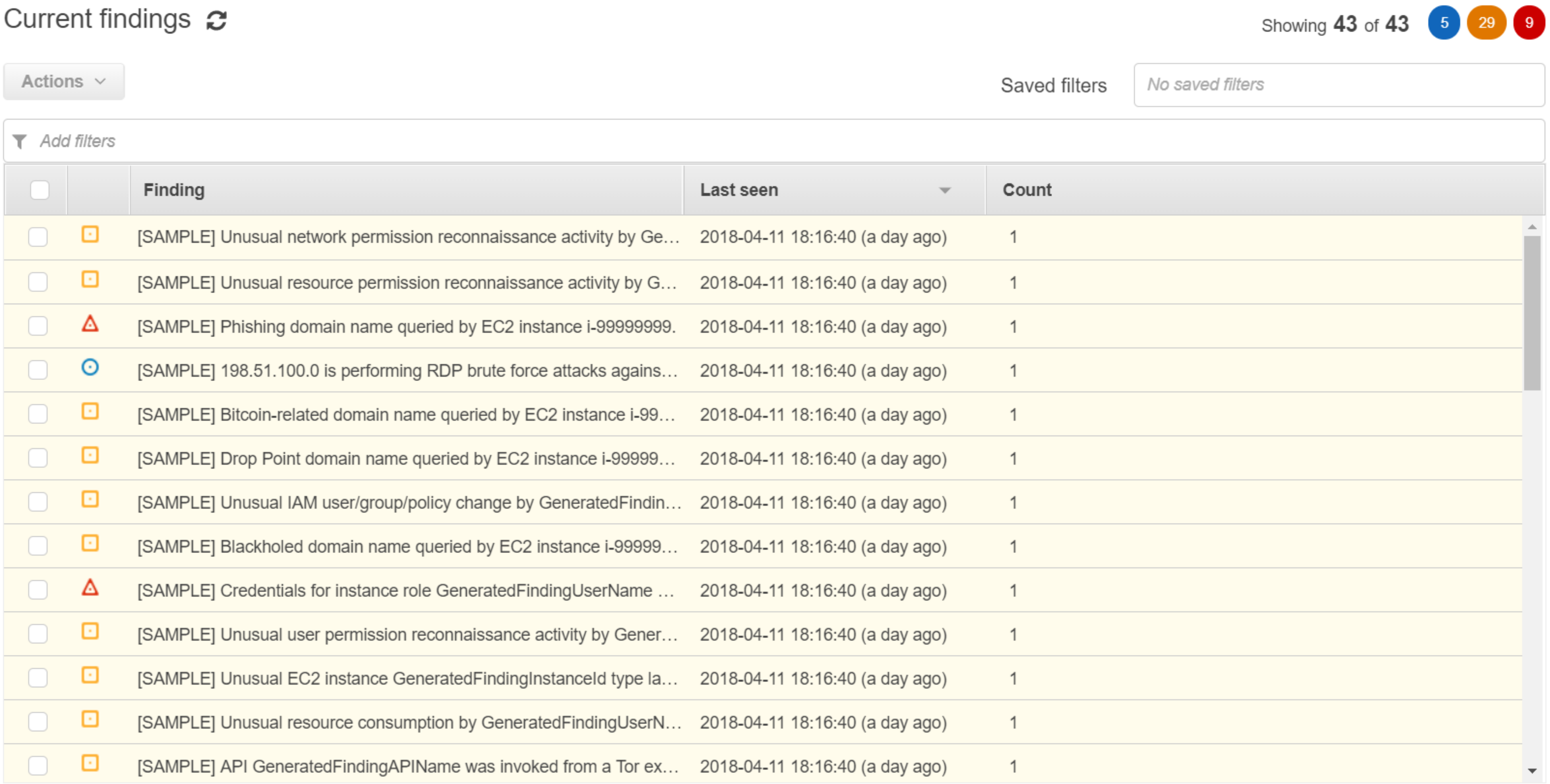
GuardDuty

- Amazon GuardDuty is a managed threat detection service that continuously monitors for malicious or unauthorised behaviour to help you protect your AWS accounts and workloads

- Monitors activity such as unusual API calls or potentially unauthorised deployments that indicate a possible account compromise

- GuardDuty also detects potentially compromised instances or reconnaissance by attackers

GuardDuty



Current findings

Showing **43** of **43** 5 29 9

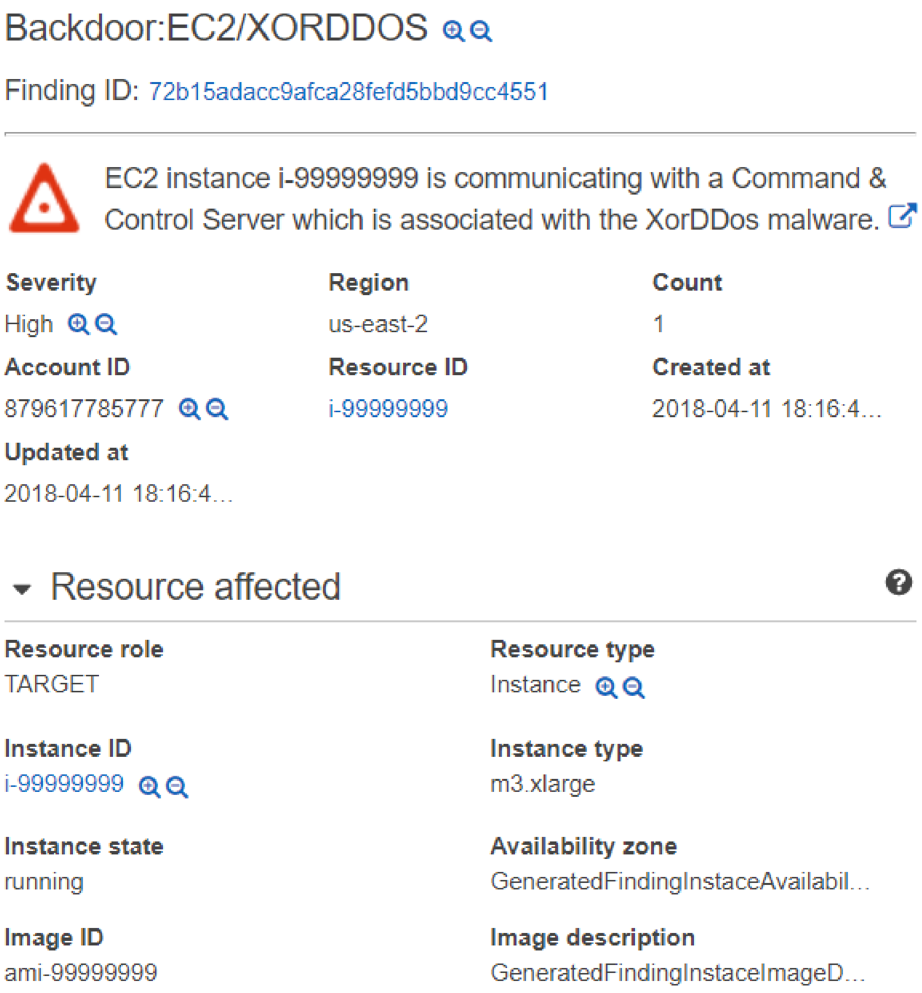
Actions

Saved filters No saved filters

Add filters

□		Finding	Last seen	Count
□	⊡	[SAMPLE] Unusual network permission reconnaissance activity by Ge…	2018-04-11 18:16:40 (a day ago)	1
□	⊡	[SAMPLE] Unusual resource permission reconnaissance activity by G…	2018-04-11 18:16:40 (a day ago)	1
□	△	[SAMPLE] Phishing domain name queried by EC2 instance i-99999999.	2018-04-11 18:16:40 (a day ago)	1
□	⊙	[SAMPLE] 198.51.100.0 is performing RDP brute force attacks agains…	2018-04-11 18:16:40 (a day ago)	1
□	⊡	[SAMPLE] Bitcoin-related domain name queried by EC2 instance i-99…	2018-04-11 18:16:40 (a day ago)	1
□	⊡	[SAMPLE] Drop Point domain name queried by EC2 instance i-99999…	2018-04-11 18:16:40 (a day ago)	1
□	⊡	[SAMPLE] Unusual IAM user/group/policy change by GeneratedFindin…	2018-04-11 18:16:40 (a day ago)	1
□	⊡	[SAMPLE] Blackholed domain name queried by EC2 instance i-99999…	2018-04-11 18:16:40 (a day ago)	1
□	△	[SAMPLE] Credentials for instance role GeneratedFindingUserName …	2018-04-11 18:16:40 (a day ago)	1
□	⊡	[SAMPLE] Unusual user permission reconnaissance activity by Gener…	2018-04-11 18:16:40 (a day ago)	1
□	⊡	[SAMPLE] Unusual EC2 instance GeneratedFindingInstanceId type la…	2018-04-11 18:16:40 (a day ago)	1
□	⊡	[SAMPLE] Unusual resource consumption by GeneratedFindingUserN…	2018-04-11 18:16:40 (a day ago)	1
□	⊡	[SAMPLE] API GeneratedFindingAPIName was invoked from a Tor ex…	2018-04-11 18:16:40 (a day ago)	1

GuardDuty



Backdoor:EC2/XORDDOS

Finding ID: 72b15adacc9afca28fefd5bbd9cc4551

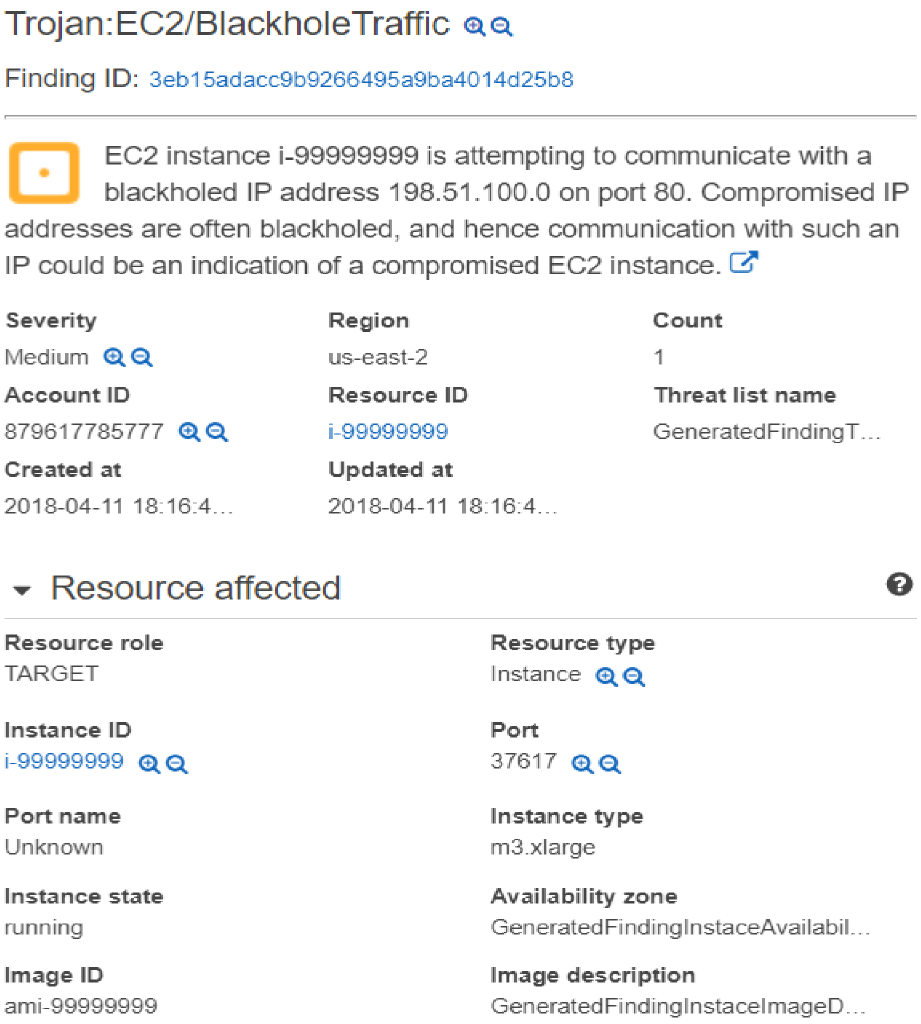
EC2 instance i-99999999 is communicating with a Command & Control Server which is associated with the XorDDos malware.

Severity	**Region**	**Count**
High	us-east-2	1
Account ID	**Resource ID**	**Created at**
879617785777	i-99999999	2018-04-11 18:16:4…
Updated at		
2018-04-11 18:16:4…		

Resource affected

Resource role TARGET	**Resource type** Instance
Instance ID i-99999999	**Instance type** m3.xlarge
Instance state running	**Availability zone** GeneratedFindingInstaceAvailabil…
Image ID ami-99999999	**Image description** GeneratedFindingInstaceImageD…

GuardDuty



Trojan:EC2/BlackholeTraffic

Finding ID: 3eb15adacc9b9266495a9ba4014d25b8

EC2 instance i-99999999 is attempting to communicate with a blackholed IP address 198.51.100.0 on port 80. Compromised IP addresses are often blackholed, and hence communication with such an IP could be an indication of a compromised EC2 instance.

Severity	**Region**	**Count**
Medium	us-east-2	1
Account ID	**Resource ID**	**Threat list name**
879617785777	i-99999999	GeneratedFindingT…
Created at	**Updated at**	
2018-04-11 18:16:4…	2018-04-11 18:16:4…	

Resource affected

Resource role	**Resource type**
TARGET	Instance
Instance ID	**Port**
i-99999999	37617
Port name	**Instance type**
Unknown	m3.xlarge
Instance state	**Availability zone**
running	GeneratedFindingInstaceAvailabil…
Image ID	**Image description**
ami-99999999	GeneratedFindingInstaceImageD…

GuardDuty

- **Create filters for certain parameters, such as:**
  - Severity events
  - Blocked events
  - Remote / Local ports
  - Protocols
  - Connection direction:
    - Inbound
    - Outbound

GuardDuty

- **You can export the events in JSON format for offline or import into an SIEM for further analysis**

- **Events can be archived**

- **Centralised Threat Detection across all of your AWS accounts**

- **Threat Detection:**
    - Collects, analyses, and correlates events from CloudTrail, VPC Flow Logs, and DNS Logs across all of your associated AWS accounts

AWS Forensic environment

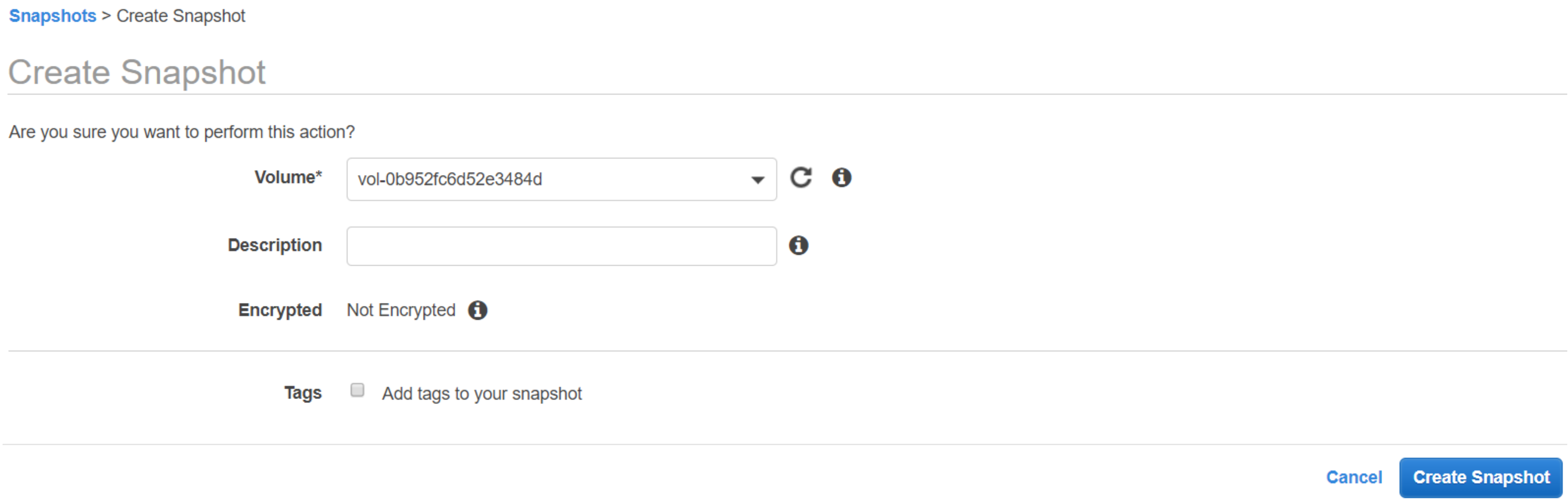
- **One can create an AWS Forensic environment with an AWS authorised account:**
  - Internal teams
  - Consultancy
- **Virtual machine snapshots can be shared with other AWS accounts**
- **Disk Forensic acquisition of those snapshots can be acquired too**
- **Memory acquisition of the snapshot is also possible and highly recommended**

AWS Forensic environment

- **If the client permits, analysis can be done on AWS rather than downloading Images:**
  - Snapshot needs to be shared with an AWS account
  - Volume of the snapshot can be created
  - Attach the Volume to the Analysis Virtual Machine
  - Image the Volume
  - Detach the Volume

AWS Forensic environment

- Create a Snapshot of the Virtual Machine snapshot



Snapshots > Create Snapshot

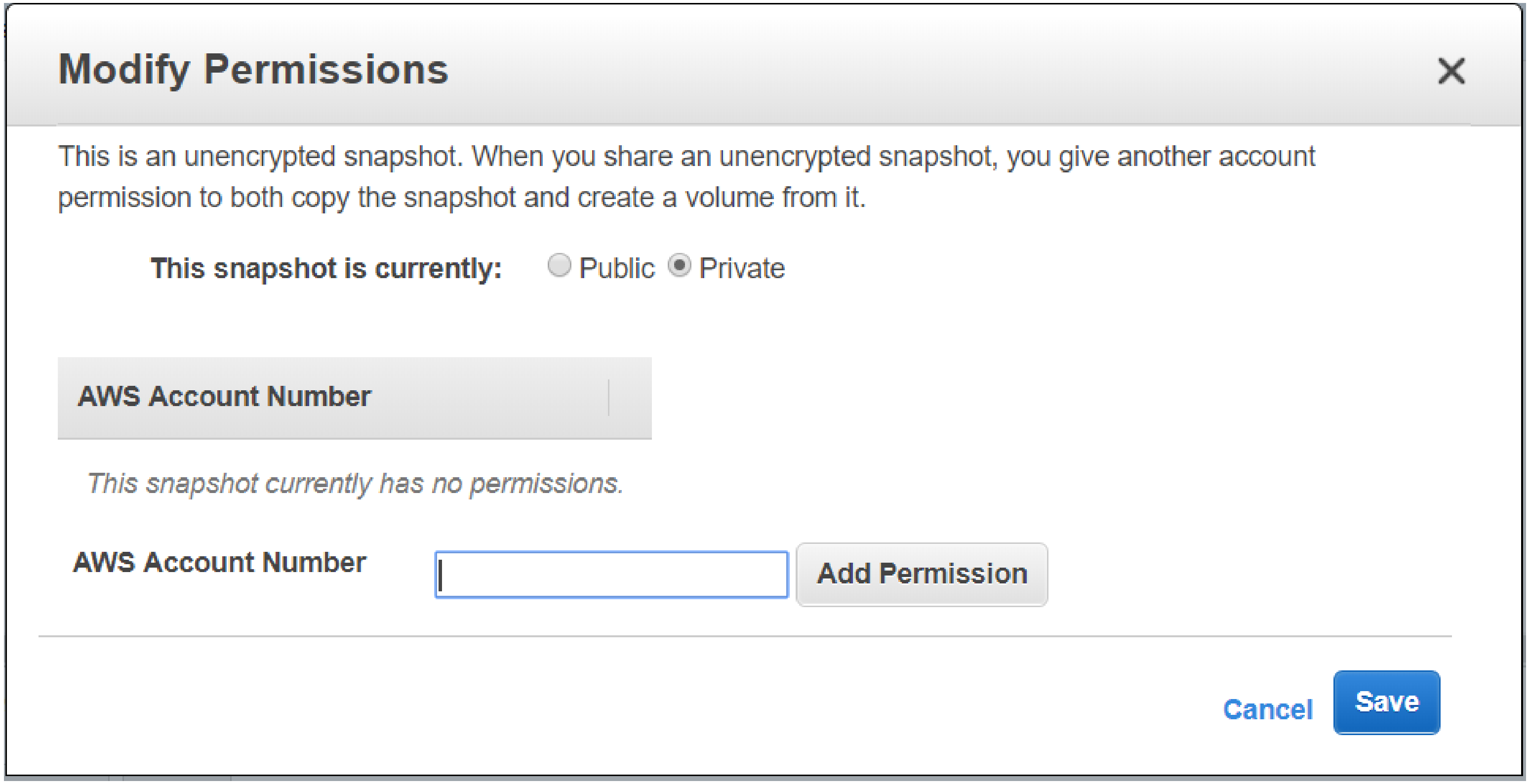
Create Snapshot

Are you sure you want to perform this action?

Volume*	vol-0b952fc6d52e3484d
Description	
Encrypted	Not Encrypted
Tags	□ Add tags to your snapshot

AWS Forensic environment

- EBS snapshot will be created with permissions to share with another AWS account



Modify Permissions

This is an unencrypted snapshot. When you share an unencrypted snapshot, you give another account permission to both copy the snapshot and create a volume from it.

This snapshot is currently: ○ Public ● Private

AWS Account Number

This snapshot currently has no permissions.

AWS Account Number

AWS Threat Hunting

- **To help with AWS Threat Hunting, an excellent project called tf-aws has been developed by Apollo Clark:**
  - https://github.com/apolloclark/tf-aws

- **Terraform stack to deploy ELK Threat Hunting on Amazon AWS**

- **End-to-end encrypted, auto-scaling, AWS Multi-tier LAMP webstack, with ELK metrics and log monitoring, integrating osquery, and multiple AWS security features**

- **It enables groups to deploy a fully secured web stack, and perform threat hunting. It is deployed with:**
  - Packer - AMI builder
  - Ansible - service configuration
  - Serverspec - service verification
  - Terraform - cloud resource builder

AWS Threat Hunting

- **Components for tf-aws include:**
  - Ubuntu 16.04
  - osquery 2.11.0 (Dec 18, 2017) - endpoint visibility
  - Filebeat - log file collector
  - Metricbeat - metric collector
  - Packetbeat - network analytics collector
  - Heartbeat - uptime monitor
  - Elasticsearch - document-store database
  - Logstash - log file processor
  - Kibana - metric and log dashboards
  - ModSecurity - Apache firewall
  - McAfee MySQL Audit Plugin - MySQL security logging

Conclusion

- AWS environment can provide great visibility during an incident or post-breach

- Knowledge of AWS environment is essential to ensure comprehensive analysis during an incident or post-breach

- Vital artefacts mentioned can aid Investigators during the analysis process

- Threat Hunting on AWS is possible for continuous monitoring purposes

???