

#### AWS Certified Security – Specialty An overview

Simon Whittaker

Cyber Security Director - Vertical Structure Ltd

#### Prepare, Protect, Persist ®



#### Prepare

• We help you and your partners to understand how to identify and resolve potential security issues at the earliest stages with hands on 'hack yourself first', threat modelling and GDPR compliance workshops as well as security training for non-technical colleagues.

#### Protect

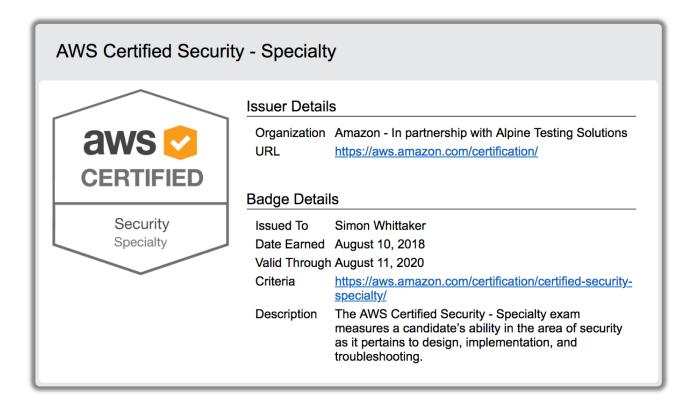
• Using automated and manual penetration testing techniques, we provide a comprehensive security report for your Web and mobile applications, including API testing, and networks. The report highlights potential issues and their resolutions.

#### Persist

• We ensure that your organisation benefits from continual improvements in security levels through information assurance processes, auditing and certification including ISO27001:2013 and Cyber Essentials.

#### The certification









#### McAfee says cloud security not as bad as we feared... it's much worse

Quick takeaway: most everyone sucks at laaS



The average business has around 14 improperly configured laaS instances running at any given time and roughly one in every 20 AWS S3

https://www.theregister.co.uk/2018/10/30/mcafee\_cloud\_security\_terrible

## Lies, damn lies and statistics



- 14 improperly configured IaaS instances running at any given time
- Roughly one in every 20 AWS S3 buckets are left wide open to the public internet
- The average business uses around 1,900 cloud instances, but most of the companies they surveyed only thought they used around 30

#### We're doing it wrong





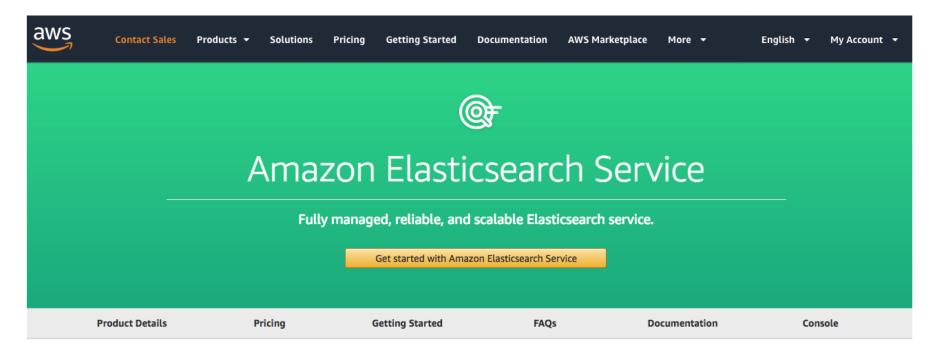
Elasticsearch is a search engine based on Lucene. It provides a distributed, multitenant-capable full-text search engine with an HTTP web interface and schema-free JSON documents.

https://en.wikipedia.org/wiki/Elasticsearch



#### Elasticsearch in AWS





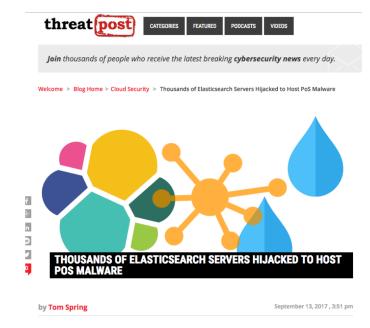
Amazon Elasticsearch Service makes it easy to deploy, secure, operate, and scale Elasticsearch for log analytics, full text search, application monitoring, and more. Amazon Elasticsearch Service is a fully managed service that delivers Elasticsearch's easy-to-use APIs and real-time analytics capabilities alongside the availability, scalability, and security that production workloads require. The service offers built-in integrations with Kibana, Logstash, and AWS services including Amazon Virtual Private Cloud (VPC), AWS Key Management Service (KMS), Amazon Kinesis Data Firehose, AWS Lambda, Amazon Cognito and Amazon CloudWatch so that you can go from raw data to actionable insights quickly and securely.

#### **Access Restrictions**



- Resource based
  - Assigned access to a account, user or role to a domain in AWS
- Identity based
  - Assigned access to a account, user or role to a domain in AWS
  - Tend to be more generic
- IP based
  - Anyone from the right IP can access anything





Thousands of insecure Elasticsearch servers are hosting point-of-sale malware, according to an analysis by Kromtech Security Center. In total, researchers found 15,000 insecure Elasticsearch servers with 27 percent (4,000) hosting the PoS malware strains Alina and JackPoS.

"The absence of authentication on some Elasticsearch servers allowed attackers to take full administrative control on the exposed instance," wrote Bob Diachenko, Kromtech's chief communication officer on Tuesday in a blog post outlining the research.

## Methodology



- Shodan for understanding initial numbers
- Basic interrogation of top 1000 instances in export to understand:
  - Cluster Name
  - Health
  - Number of documents
  - Size of data
  - Index Names
  - Key names within index
- Regex to understand key name and rate "interesting-ness"

# Some figures



TOTAL RESULTS

44,313

#### TOP COUNTRIES

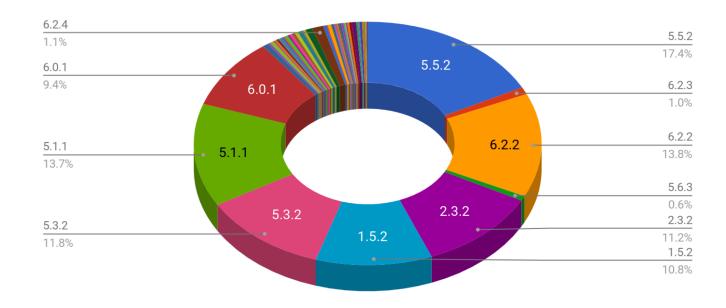


TOP SERVICES	
НТТР	23,857
ElasticSearch	20,242
HTTP (8080)	116
Qconn	13
5601	11
TOP ORGANIZATIONS	
Amazon.com	21,285
Hangzhou Alibaba Advertising Co.,Ltd.	2,519
Amazon	1,663
Amazon Data Services Ireland Limited	902
Microsoft Azure	851
TOP OPERATING SYSTEMS	
Linux 3.x	9
Windows 7 or 8	6
TOP VERSIONS	
6.2.2	4,961
5.5.2	4,770
5.1.1	3,645
5.3.2	3,302
1.5.2	2,591

#### Versions of Elasticsearch



#### Elasticsearch versions discovered





Version	End of Life?	Currently maintained?
5.5.2	2019-01-06	No
6.2.2	2019-08-06	Yes
2.3.2	2017-09-30	No
1.5.2	2016-09-23	No
5.3.2	2018-09-28	No
5.1.1	2018-06-08	No
6.0.1		Yes  The Ltd where applicable and the structure of the st

## AWS Usage



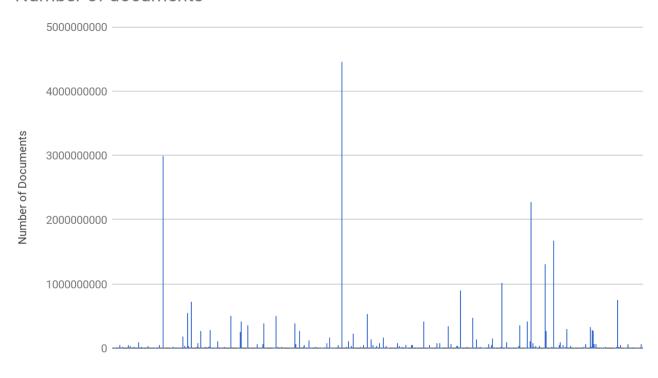


<sup>©</sup> Vertical Structure Ltd where applicable simon.whittaker@verticalstructure.com

#### **Amount of Documents**



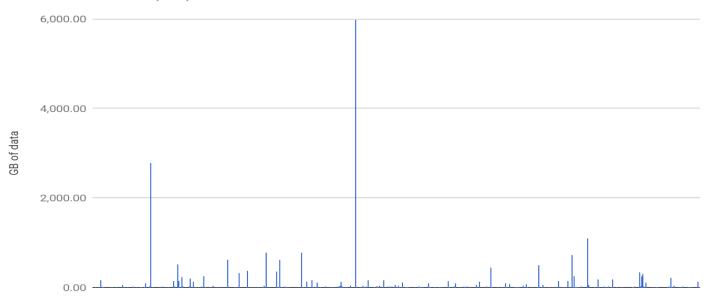
#### Number of documents



#### Amount of Data



#### Amount of Data(GB)

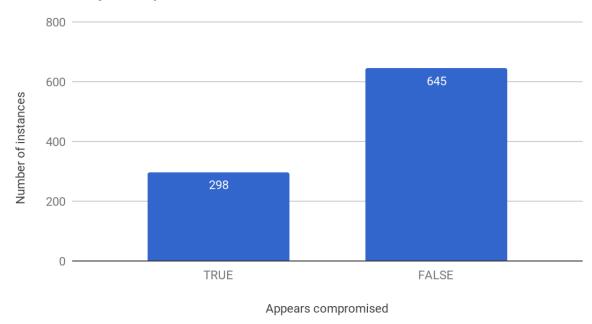


Total Data is 24,510.49 GB

#### **Potentially Compromised Hosts**



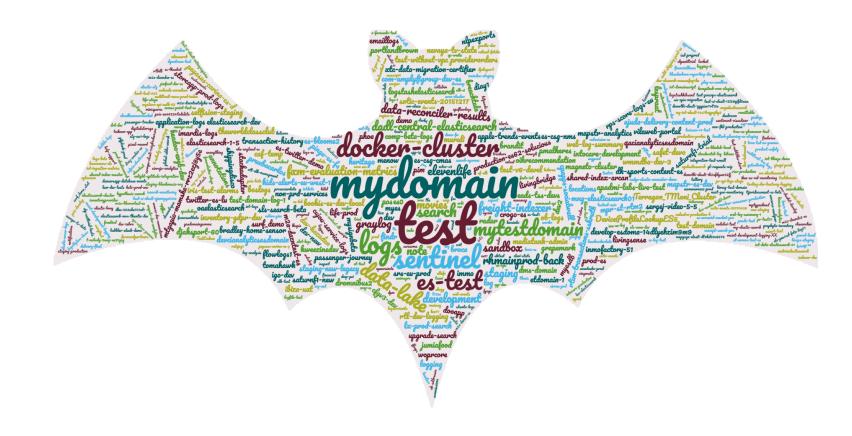




Basic:(command.php|hedwig.cgi|login.action|ge tcfg.php|wpadmin|jackposv2|jacpos|pleasereadthis|readme

#### Who doesn't love a wordcloud?





## **Interesting Clusters**



```
"_index":"payments-local",
"_type":"pin",
" id":"255190",
" score":1.0,
"_source": - {
   "uid":"4190486",
   "nid":"40798476",
   "type": "pin",
   "reference id":"1524476991",
   "message_id":null,
   "transaction_id":"3300900068121214",
   "datetime": null,
   "amount": "200",
   "status": "success",
   "payment type": "online",
   "payment_method":"card",
   "name": "<NAME REMOVED>",
   "phone": "97470330372",
   "email": "<EMAIL REMOVED>",
   "billing_address":"<ADDRESS REMOVED>",
   "membership_option":"200 QAR for 1 week",
   "membership role": null,
   "membership_other_roles":null,
   "expire after":"+1 week",
   "start_date":"",
   "expire_date":"",
   "comments":"",
   "source": "web",
   "chargebee_id":"",
   "related_id":null,
   "username":"<USERNAME REMOVED>",
   "product plan": "200 QAR for 1 week",
   "product": "pin",
   "product_type": "pin",
   "category": null,
   "sub_category": null,
   "@timestamp":"2018-04-23T12:50:17",
   "request uri": "/qpay/response?
   status=success&referenceId=1524476991&transactionId=<ID
   REMOVED>&datetime=2018-04-23%2012:49:57.0&amount=200.000&",
   "referer_uri":"https://demopaymentapi.qpayi.com/datacash/clien
   t/response?dts_reference=3300900068121214&pm=1",
   "ip":"127.0.0.1",
   "user agent": "Mozilla/5.0 (X11; Ubuntu; Linux x86 64; rv:59.0)
   Gecko/20100101 Firefox/59.0"
```

## Interesting clusters pt 2



```
"_index" : "vod_asset_purchases",
"_type" : "vod_asset_purchase",
"_id" : "15857",
"_source" : ⊡{
   "created_at" : "2017-01-12T08:46:38.000Z",
   "charae" : "0.0".
   "site_id" : 73,
   "room_id" : 1823,
   "guest_id" : 59177,
   "company_id" : 48,
    "guest" : ⊡{
       "id" : 59177,
       "name" : "to Room 2",
       "pms_uid" : null,
       "vip" : null,
       "title" : null,
       "first_name" : null,
       "last_name" : null
    "vod_asset" : ⊡{
       "id" : 142,
       "name" : "We're the Millers",
       "description" : "David\r\n Clark  is a small-time pot dealer whose clientele includes chefs\r
       \n and soccer moms, but no kids\u2014after all, he has his scruples. So what could go\r\n wrong? Pl
       enty. Preferring to keep a low profile for obvious reasons, he\r\n learns the hard way that no good
       deed goes unpunished when he tries to help\r\n out some local teens and winds up getting jumped by
       a trio of gutter punks. ",
       "year" : 2013,
       "hd" : false.
       "cover" : "/media/W1siZiIsIjIwMTYvMTIvMDgvMTMvMTYvMjQvYTU3MzhlZDAtOTcxMy00NzYwLTk4ZGEtMGNmNzVhYTkyY
       jkzL1dlX3JlX3RoZV9NaWxsZXJzLmpwZyJdLFsicCIsInRodW1iIiwiMTIweDE4MCMiXV0/9203b6b413ea605f",
       "rating" : "15",
       "new_release" : false
       "pre_release" : false
```

```
"created_at" : "2017-01-12T06:17:30.000Z",
"charge" : "0.0",
"site_id" : 169,
"room_id" : 4788.
"guest_id" : 128632,
"company_id" : 89,
"quest" : ⊡{
   "id" : 128632,
   "name" : " to
                       Hotel Soho",
   "pms_uid" : "",
   "vip" : null,
   "title" : null,
   "first_name" : null.
   "last_name" : null
"vod_asset" : ⊡{
   "id" : 73,
   "description" : "Forget\rn going against the game show clock, these
                       all in the name of fun!"
   "year" : null,
   "hd" : true,
   "cover" : "/media/W1siZiIsIjIwMTYvMTIvMDgvMTMvMTYvMDcvMjk3YjljNGEtYWIZNy00Yzk4LWI1NmEtZmMyMTIyYzZhY
   WU4L05vbl9TdG9wX1RlZW5fUG91bmRpbmdfRnJvbnRDb3Zlci5qcGciXSxbInAiLCJ0aHVtYiIsIjEyMHgx0DAjIl1d/7fe5071
   6723c6dfe",
   "rating" : "R18",
   "new_release" : false,
   "pre_release" : false
"room" : ⊡{
   "id" : 4788,
   "name" : "405"
},
"site" : ⊡{
   "id" : 169,
   "name" : "
```

## Interesting clusters pt 3



#### Store receipts

```
..........
.....¥Ï.ý%¢.[Ö.í#Ú3..â#À¥Ä&Ë=æ.ìJ
U.ÿ¤.×.£9Tm}.²T..Ä,Rq.d{.î.ºIÖ.å´.qÏ?[F.ÆÄ.,.@X¢.>!xÕÛ·Ð...L[*h7.Âò½.ÄÒi.JXR«.āíÝ....5-
ÂÌ.Ê.H.+XxTkè.16.J..GT67.,2..}_x.JáÀ.àQx»..cô+.Áý>oÊÁō<@.R.À%
v.Þþ.þÿÂkō[^¬sQI.V.ÌC.Ì...Ð .¶\±iii...h&&9...s°
]ÅsÐßv;Ø-Ù..ãì.Ïâ.ĐÓú&U.ïâ.I#.....
£..×0..60?..+.....3010/..+....0..#http://ocsp.apple.com/ocsp03-wwdr040...U......
¤.üÄv·. .ôMõ.6]í+..0...U....ÿ..0.0...U.#..0....'.
                                                        ©¶.`.ìëºÖGYÅRT£.0....U. ....0...0..
*.H.÷cd...0.p0.A..+......0.¶...3Reliance on this certificate by any party assumes acceptance of
the then applicable standard terms and conditions of use, certificate policy and certification
practice statements.06..+......*http://www.apple.com/certificateauthority/0...U....ÿ......0..
*.H.÷cd.....0
        *.H.÷
. . . . . . . . . .
|.Ó.=ā[+.nB.lóè.C0._à\Ñ.¾½.½.ü%.Û..Ã.Yßāâ×...¬
Û¶, þü5. | Ë..k...äw¹±g.´.^¦..vøZ .çc..süèí£.®.øeH\ à(:À.7-¹ .9.s¹È.ýòÞ..**n+.ü \Ùë}'¦3øõ.à&DÛ±Lgün
OÉâ."Ò.6$.kQ¢Z.ueÑ..bāÁ ō.Φïhù..ÉÁ.3ø..dQX`À| .uÊi¹[*Ö.hn.BōL$7..ì;.z.C6£mčH`..6.+lp.μ.Ú-
#Đ.ü i.....{9GE0a/Ç."0.."0..
 .....⊅¾Ä9m .0
```

```
0..í. *.H.+
... ..⊅0..Ú...1.0
               ..+.....0.... *.H.÷
.... 11..w0
......P2500.......1.1.30..........g3.O.jÜ.VwríÑÏÅØ0.......ProductionSandbox0.......£4¢
.¹£..OlÃë<=.¹5Ð.0......2018-05-23T16:53:31Z0.......2013-08-
01T07:00:00Z0!......com.play
                           War0V.....N6./.*Qku
                                             ¿&6MZÑæ..hìl.ì..
<f}.if.E.q.ÖÀa¦ð
..ìÅ.K.sâG..¦Ö...À.F_kÏ£O\.....T.Ú:*.ÿÿ¤ùÇüã.X...ilðø.ͽ.Ä.á¯+vâ<½ªIUù.Ô]§"ñÝ+BV.Ûî9...ù.
£.>ºÝ..?¶C`0Ú.f..-....
.....0.....kill.event.40....$......10000004012686580.............10000004012686580........
.....2018-05-23T16:53:30Z0....a......2018-05-23T16:53:30Z ..e0..|0..d ......ëw.ç. .0
.....0..1.0 ..U....US1.0...U.
```

# Interesting clusters pt 4 - a lot of logs



```
"_index" : " fill-schedules-dataset",
"_type" : "stagingRecord",
"_id" : "_SOURCE_1412985322822",
"_score" : 1,
"_source" : ⊡{
   "id" : "_SOURCE_1412985322822",
   "domainKey": "1412985322822",
   "source": "_SOURCE",
   "payload" : "V2VsbCBkb25lIGZvciBjb3B5aW5nIHRoaXMgYW5kIGRlY29kaW5nIGl0IGJ1dCB1bmZvcnR1bmF0ZWx5IHRoZSBkY
   XRhIGhhcyBiZWVuIHJlbW92ZWQgYnkgU2ltb24gVw==",
   "updatedTime" : 1520014665574,
   "compressed" : true
               base64 -D -i testingb64.txt |
               gunzip
```

# Interesting clusters pt 4 - a lot of logs



```
id: "1412985322822",
name: "HM __223320X Calendar",
timeZone: "Europe/Berlin",
version: 1,
active: "N",
deleted: false,
attributes: [
       name: "SD_MARKETPLACE_ID",
       value: "A
        name: "SD_OWNER"
       name: "SD_FMID",
        value: "/ Z6GLS"
        name: "SD_COUNTRY"
        name: "SD_SHIP_OPTION"
        name: "SD_PRODUCT_SELECTION"
       name: "SD_USE_CASE"
        name: "SD_DELIVERY_SPEEDS",
        value: "[{\"charge\":{\"ic\":{\"v\":0,\"ltu\":\"EUR\"},\"sc\":{\"v\":0,\"ltu\":\"EUR\"}},\"lt\":{\
        name: "SD_JURISDICTION"
        name: "SD REGION"
        name: "SD_PRIME_BENEFIT"
```

# Interesting clusters pt 4 - a lot of logs



```
"_index" : "dev. .....api-sandbox.co.uk",
"_type" : "/var/log/nginx_access_json",
"_id" : "34026272625880389028810097554658157382791273612723814401".
"_score" : 1,
"_source" : ⊡{
   "@id": "34026272625880389028810097554658157382791273612723814401",
   "@timestamp" : "2018-05-08T14:47:14.475Z",
   "@message" : "{ remote_addr:\"10
                                           31\", remote_user:\"-\", time_iso
   8601:\"2018-05-08T14:47:14+00:00\", request:\"POST /
   unt-requests HTTP/1.1\", status:\"201\", body_bytes_sent:\"466\", http_ref
   erer:\"-\", http_user_agent:\"Apache-HttpClient/4.5.2 (Java/1.8.0_131)\",
   http_x_forwarded_for:\"-\", server_name:\"dev. .api-sandbox.co.uk\", pr
   oxy_protocol_addr:\"1
                                  7\", request_time:\"1.877\", ssl_client_s_
   dn:\"CN=BoR0bPpgZQu1VejJUlZV9,OU=oUPke3kdcSslKSL9MH,O=
                                       9\", request_id:\"332
   d, C=GB\", hostname:\"07
   c7686c166c16e\", request_method:\"POST\", request_uri:\"/ /v1.
   1/account-requests\", server_protocol:\"HTTP/1.1\" }",
   "@client_dn" : "CN=BoR0bPpgZQu1VejJUlZV9,0U=oUPke3kdcSslKSL9MH,0=
              , C=GB",
   "@brand_name" : "dev. .api-sandbox.co.uk",
   "@request_endpoint" : "/ /v1.1/account-requests",
   "@request_method" : "POST",
   "@response_time" : 1.877,
   "@response_status" : "201",
   "@owner": "625789635960",
   "@log_group" : "/var/log/nginx_access_json";
   "@log_stream" : "i-0781e347a4e3020d9"
```

### Interesting clusters pt 5



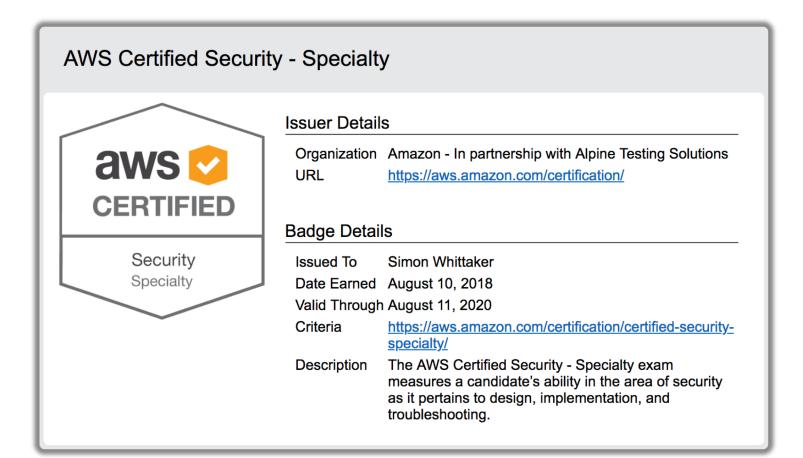
- Major brand names
- Broadcaster
- Online services
- Games providers
- Interesting index names
  - Inventory-gdpr-dev
  - kicsps-staging
  - Storeapp-prod-logs
  - Gisapi-prod



## We're doing it wrong

#### AWS answer





## What do you have to demonstrate?



- An understanding of specialized data classifications and AWS data protection mechanisms.
- An understanding of data encryption methods and AWS mechanisms to implement them.
- An understanding of secure Internet protocols and AWS mechanisms to implement them.
- A working knowledge of AWS security services and features of services to provide a secure production environment.
- Competency gained from two or more years of production deployment experience using AWS security services and features.
- Ability to make tradeoff decisions with regard to cost, security, and deployment complexity given a set of application requirements.
- An understanding of security operations and risk.

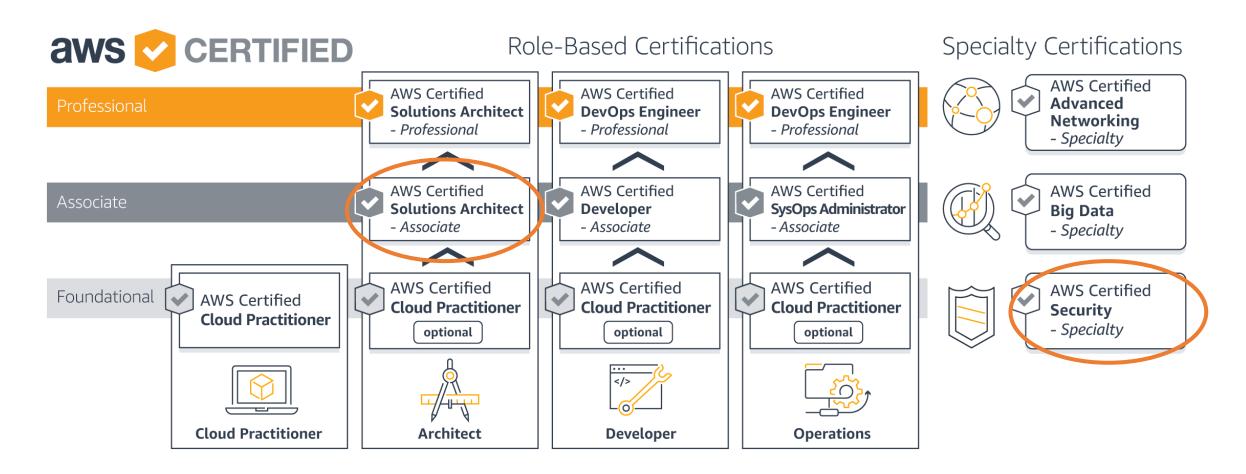
## Recommended knowledge



- A minimum of five years of IT security experience designing and implementing security solutions.
- At least two years of hands-on experience securing AWS workloads.
- Security controls for workloads on AWS.

## Certification roadmap









- Format: Multiple choice, multiple answer
- Length: 170 minutes, 65 questions
- Registration Fee: 300 USD

#### Content



Domain	% of Examination
Domain 1: Incident Response	12%
Domain 2: Logging and Monitoring	20%
Domain 3: Infrastructure Security	26%
Domain 4: Identity and Access Management	20%
Domain 5: Data Protection	22%
TOTAL	100%

## Domain 1 - Incident Response



- 1.1 Given an AWS abuse notice, evaluate the suspected compromised instance or exposed access keys.
- 1.2 Verify that the Incident Response plan includes relevant AWS services.
- 1.3 Evaluate the configuration of automated alerting, and execute possible remediation of security-related incidents and emerging issues.





- 2.1 Design and implement security monitoring and alerting.
- 2.2 Troubleshoot security monitoring and alerting.
- 2.3 Design and implement a logging solution.
- 2.4 Troubleshoot logging solutions.





- 3.1 Design edge security on AWS.
- 3.2 Design and implement a secure network infrastructure.
- 3.3 Troubleshoot a secure network infrastructure.
- 3.4 Design and implement host-based security.

#### Domain 4 – Identity and Access Management



- 4.1 Design and implement a scalable authorization and authentication system to access AWS resources.
- 4.2 Troubleshoot an authorization and authentication system to access AWS resources.





- 5.1 Design and implement key management and use.
- 5.2 Troubleshoot key management.
- 5.3 Design and implement a data encryption solution for data at rest and data in transit.

## The big stuff – from my experience



## AWS Key Management Service (KMS)

Easily create and control the keys used to encrypt your data

## The big stuff – from my experience



## **AWS Certificate Manager**

Easily provision, manage, and deploy public and private SSL/TLS certificates for use with AWS services and your internal connected resources

## The big stuff – from my experience



### Amazon CloudWatch

Complete Visibility of Your Cloud Resources and Applications

#### AWS CloudTrail

Track user activity and API usage



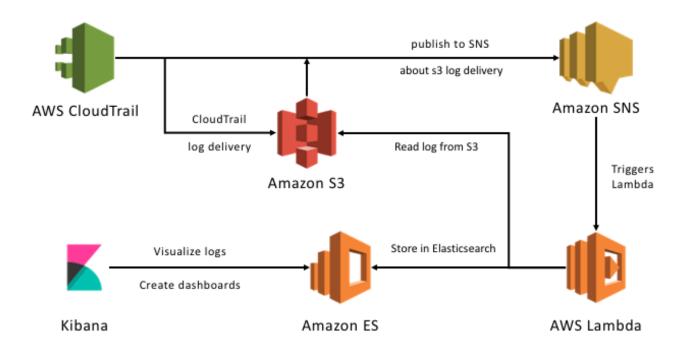


- Really important but a bit of a snoozefest
- FIPS and EAL compliance are possible with CloudHSM
- Logging





#### CloudTrail log analytics using Elasticsearch



https://allthingscloud.io/serverless-app-aws-cloudtrail-log-analytics-using-amazon-elasticsearch-service-f4612b2103c1

## Things I wasn't asked much about (but you may be...)



- Hypervisor security
- NAT instances vs gateways
- VPC endpoints
- API gateway

### API gateway

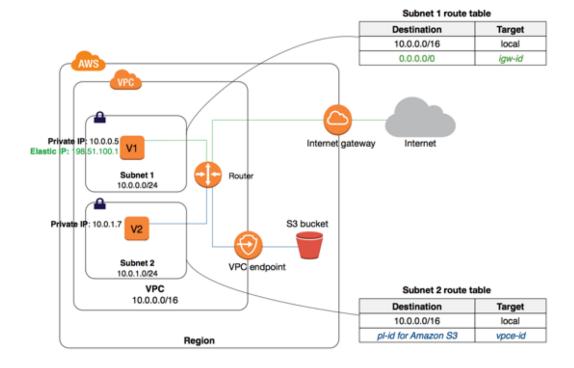


- If a caller submits 10,000 requests in a one second period evenly (for example, 10 requests every millisecond), API Gateway processes all requests without dropping any.
- If the caller sends 10,000 requests in the first millisecond, API Gateway serves 5,000 of those requests and throttles the rest in the one-second period.
- If the caller submits 5,000 requests in the first millisecond and then evenly spreads another 5,000 requests through the remaining 999 milliseconds (for example, about 5 requests every millisecond), API Gateway processes all 10,000 requests in the one-second period without returning 429 Too Many Requests error responses.

### Hide the instances



- NAT gateway + Endpoint Gateways = hidden instances
- Get containers and services out of the public network







- Use CIS images if you would like a level of security pre-rolled
- Questions about Amazon services vs self-rolled
- Encrypting root EBS volumes

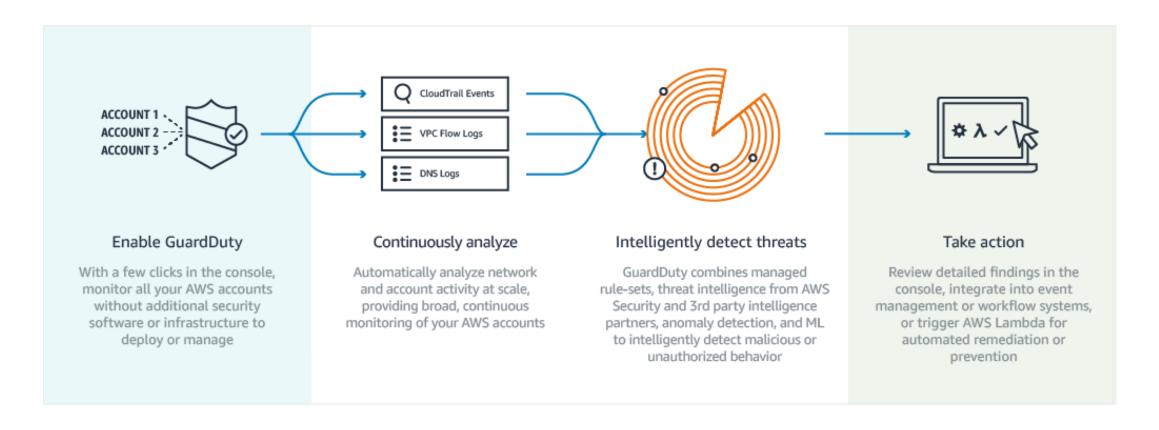


## Tools

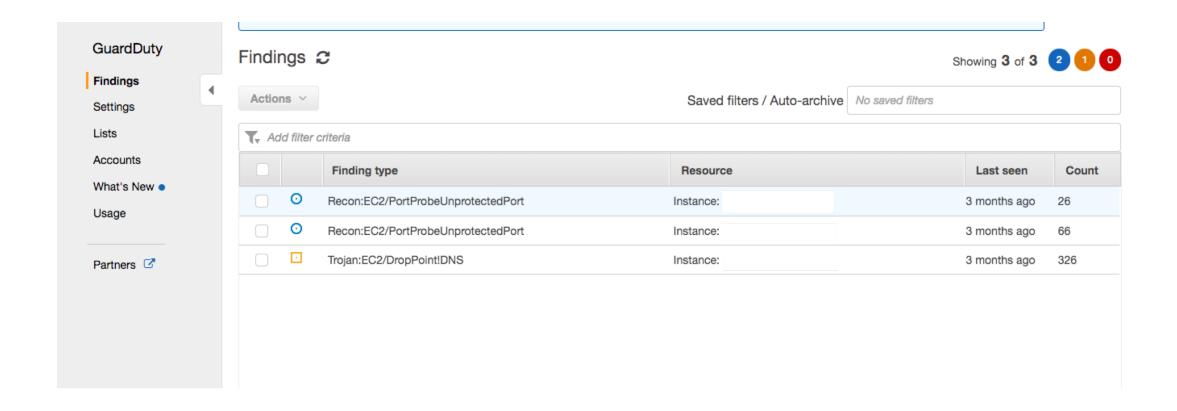
Useful tools

## Guardduty – Intelligent threat detection and continuous monitoring



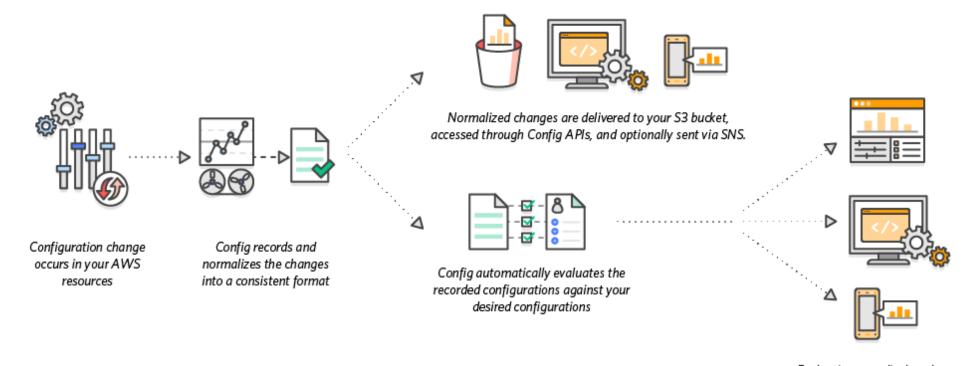






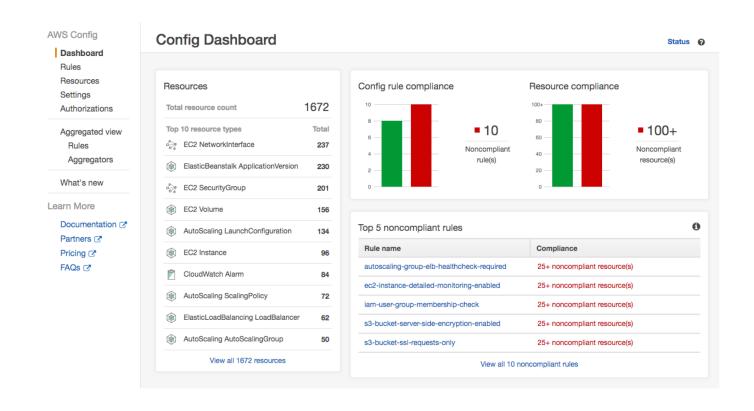
## Config - Record and evaluate configurations of your AWS resources





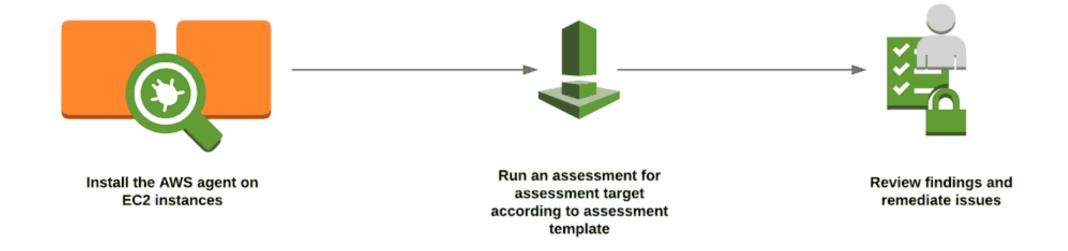
Evaluations are displayed on a dashboard, accessed through Config APIs, and optionally sent via SNS





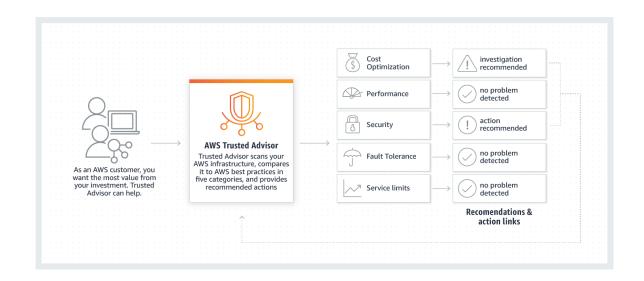
## Inspector - Automated security assessment service



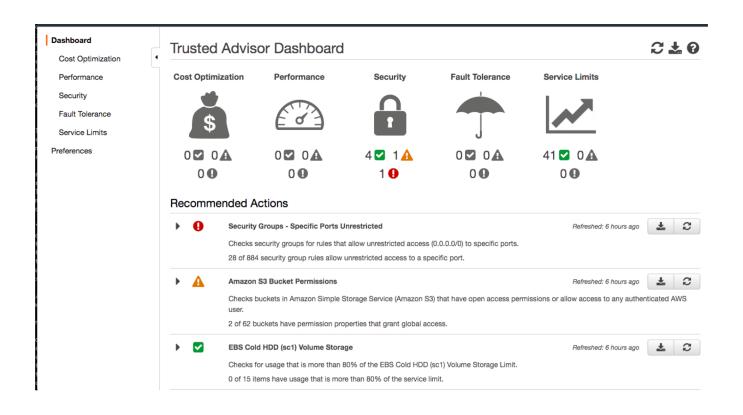


# Trusted advisor – A service to help you reduce cost, increase performance, and improve security



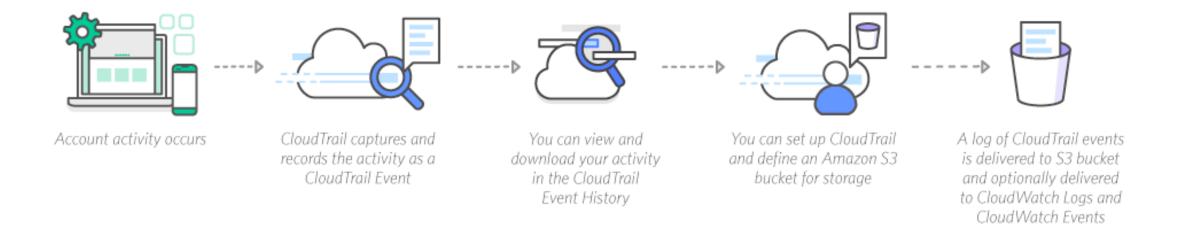




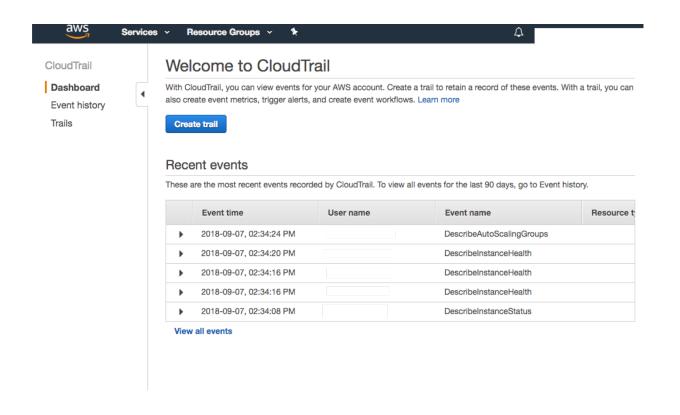


## Cloudtrail - Track user activity and API usage



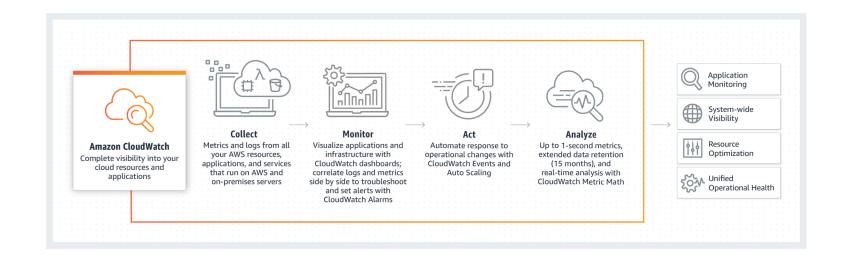






## Cloudwatch - Complete Visibility of Your Cloud Resources and Applications





### Cloudwatch



CloudWatch Dashboards Alarms ALARM 34	Amazon CloudWatch la	raph options: Vertical annota aunches vertical annotations. Add v may also format your text with Mark	vertical annotations to mark the beg	ginning and end of an o	perational e
INSUFFICIENT OK Billing Events Rules	currently have 10,922 CloudWater	perational and performance metrics the metrics available in the US East get started graphing data and creates.	(N. Virginia) region.	d applications. You	Add Gettir Monit
Event Buses Logs Metrics Favorites		Q. Search Metrics X			Forur Repo
		NetworkOut < 2,000,000 for 1 data  2,500,000 2,000,000 1,500,000 1,500,000 1,000,000 1,100,0	NetworkOut < 2,000,000 for 1 data  2,500,000 2,000,000 1,000,000 1,000,000 9/07 9/07 9/07 11:00 12:00 13:00	NetworkOut < 2,000.00  2,500,000 2,500,000 1,500,000 1,500,000 0/07 9/07 11:00 12:00	9/07
	Service Health	С	! =		
	Current Status	Details			
	Amazon CloudWatch Service	Service is operating normally			
		View complete service health details			





#### **AWS Shield**

#### Standard Protection



Available to all customers at no additional cost

#### Advanced Protection



Paid service that provides additional, comprehensive protections from large and sophisticated attacks



#### **AWS Shield**

As an AWS customer, you automatically have basic DDoS protection with the AWS Shield Standard plan, at no additional cost beyond what you already pay for AWS WAF and your other AWS services. For an additional cost, you can get advanced DDoS protection by activating the AWS Shield Advanced plan. The following table shows a comparison of the two plans.

Features	AWS Shield Standard	AWS Shield Advanced
Active monitoring		
Network flow monitoring	~	<b>~</b>
Automated application (layer 7) traffic monitoring		<b>✓</b>
DDoS mitigations		
Helps protect from common DDoS attacks, such as SYN floods and UDP reflection attacks	<b>~</b>	~
Access to additional DDoS mitigation capacity		<b>~</b>
Visibility and reporting		
Layer 3/4 attack notification and attack forensic reports	-	<b>~</b>
Layer 3/4/7 attack historical report		<b>~</b>
DDoS response team support		
Incident management during high severity events		<b>~</b>
Custom mitigations during attacks	-	<b>~</b>
Post-attack analysis	-	<b>~</b>







### AWS Systems Manager



## **AWS Systems Manager**

Gain operational insights and take action on AWS resources

#### In conclusion



- Know and use the tools
- It is not practical, there are no simulations
- Certificates and keys are "key"
- Learning the types of questions will help you
  - ACloudGuru
  - Whizlabs



## Fancy trying your hand?

https://vsltd.co/devopsbelfastnov18