AWS Certified Security – Specialty
An overview

Simon Whittaker

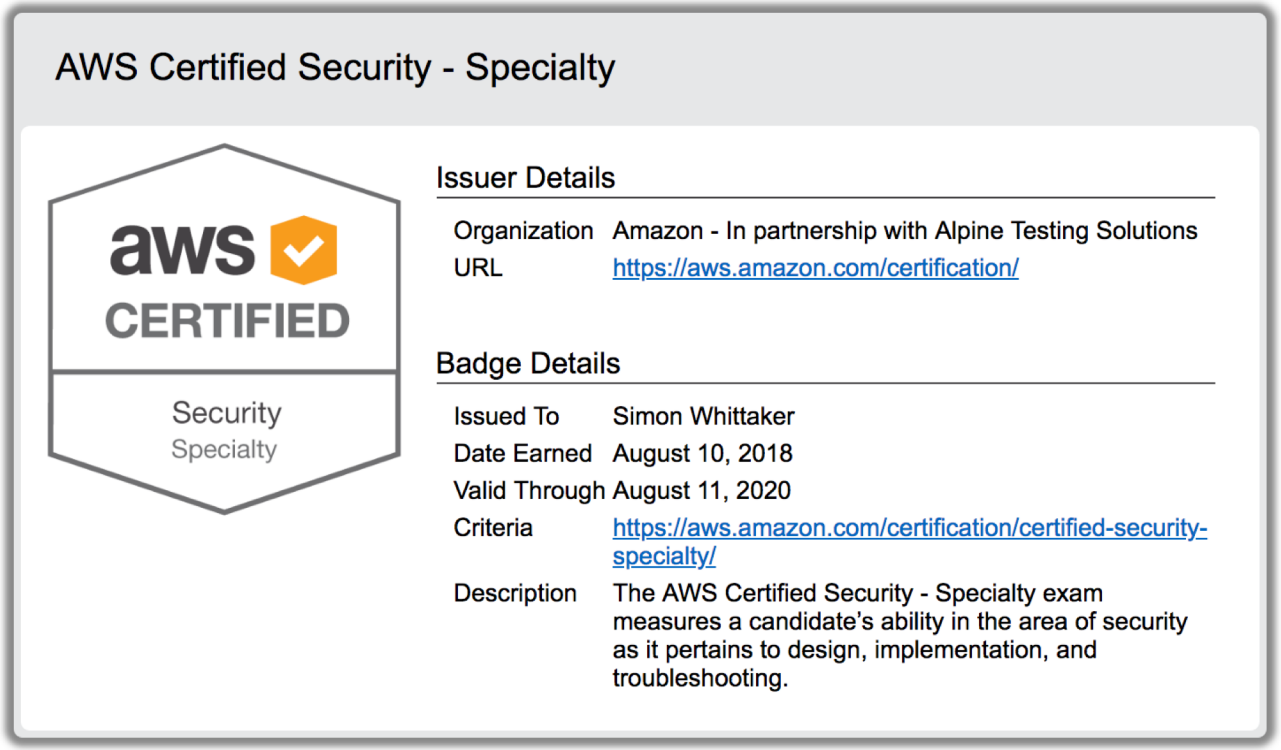
Cyber Security Director - Vertical Structure Ltd

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.

simon.whittaker@verticalstructure.com

The certification



We're doing it wrong

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

Quick takeaway: most everyone sucks at IaaS

By Shaun Nichols in San Francisco 30 Oct 2018 at 00:39 33 SHARE ▼

https://www.theregister.co.uk/2018/10/30/mcafee_cloud_security_terrible

simon.whittaker@verticalstructure.com

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

https://www.theregister.co.uk/2018/10/30/mcafee_cloud_security_terrible

simon.whittaker@verticalstructure.com

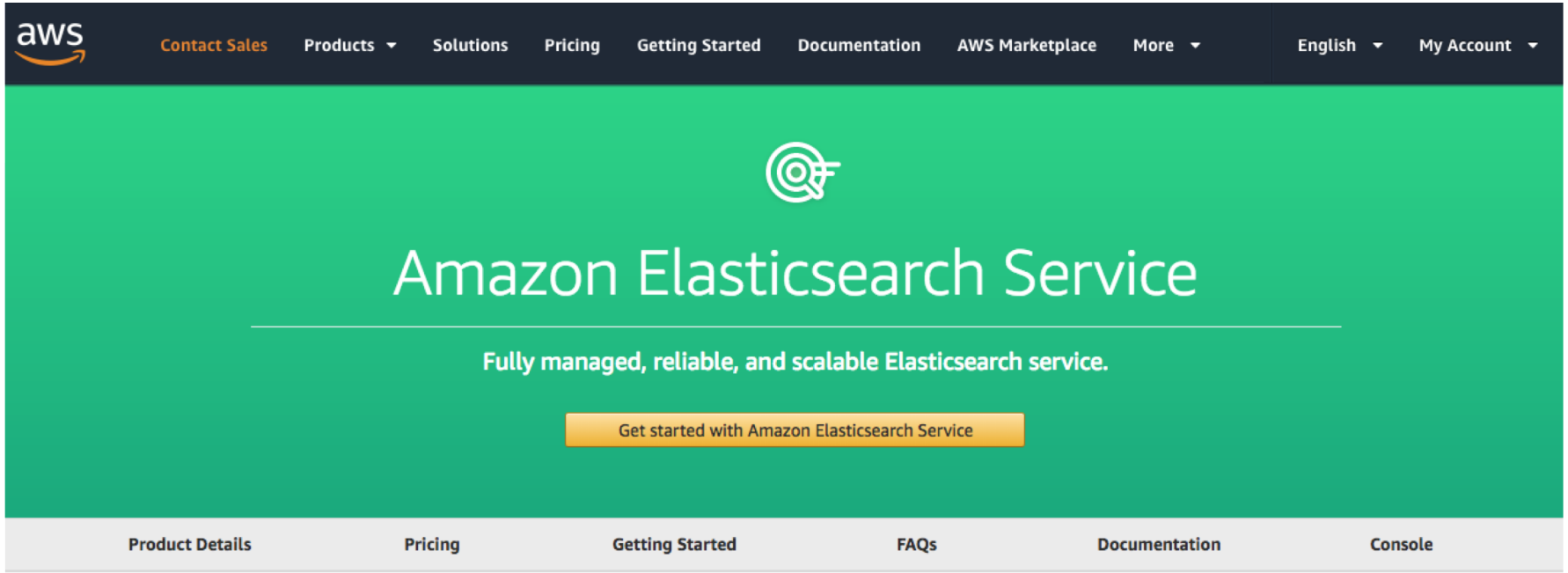
Example

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

simon.whittaker@verticalstructure.com

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.

simon.whittaker@verticalstructure.com

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

simon.whittaker@verticalstructure.com

threatpost | CATEGORIES | FEATURED | PODCASTS | VIDEOS

*Join thousands of people who receive the latest breaking **cybersecurity news** every day.*

Welcome > Blog Home > Cloud Security > Thousands of Elasticsearch Servers Hijacked to Host PoS Malware

by Tom Spring

September 13, 2017 , 3:51 pm

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”

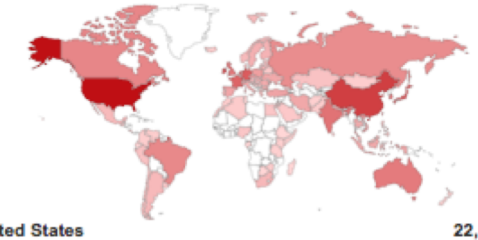
simon.whittaker@verticalstructure.com

Some figures

TOTAL RESULTS

44,313

TOP COUNTRIES



United States	22,056
China	5,486
Ireland	3,258
Germany	2,139
Singapore	1,617

TOP SERVICES

HTTP	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

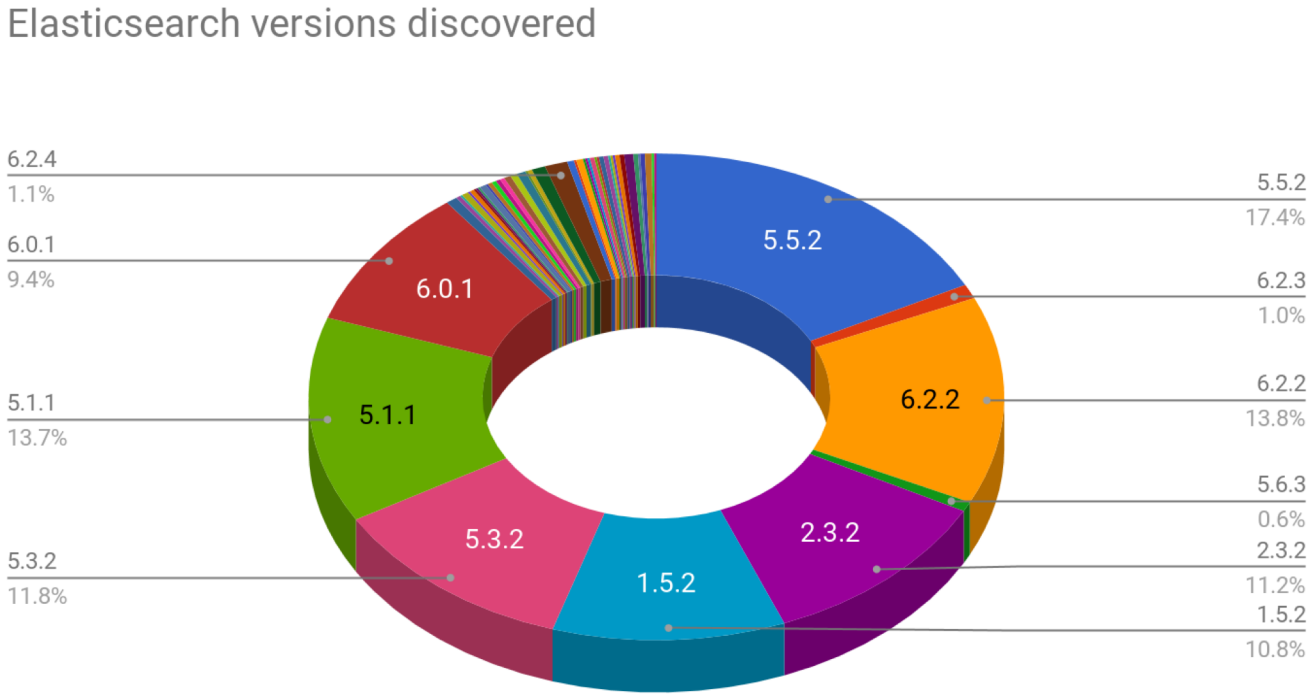
Linux 3.x	9
Windows 7 or 8	6

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

simon.whittaker@verticalstructure.com

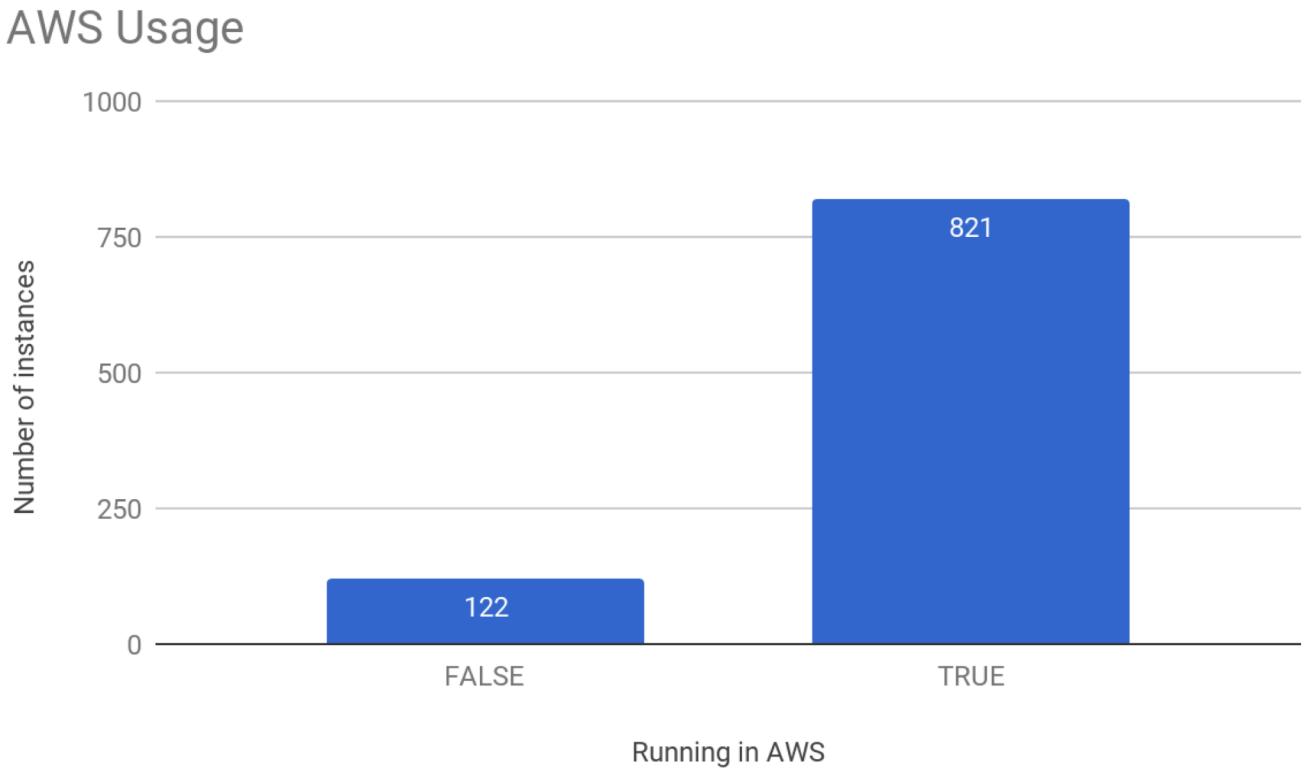
Versions of Elasticsearch



simon.whittaker@verticalstructure.com

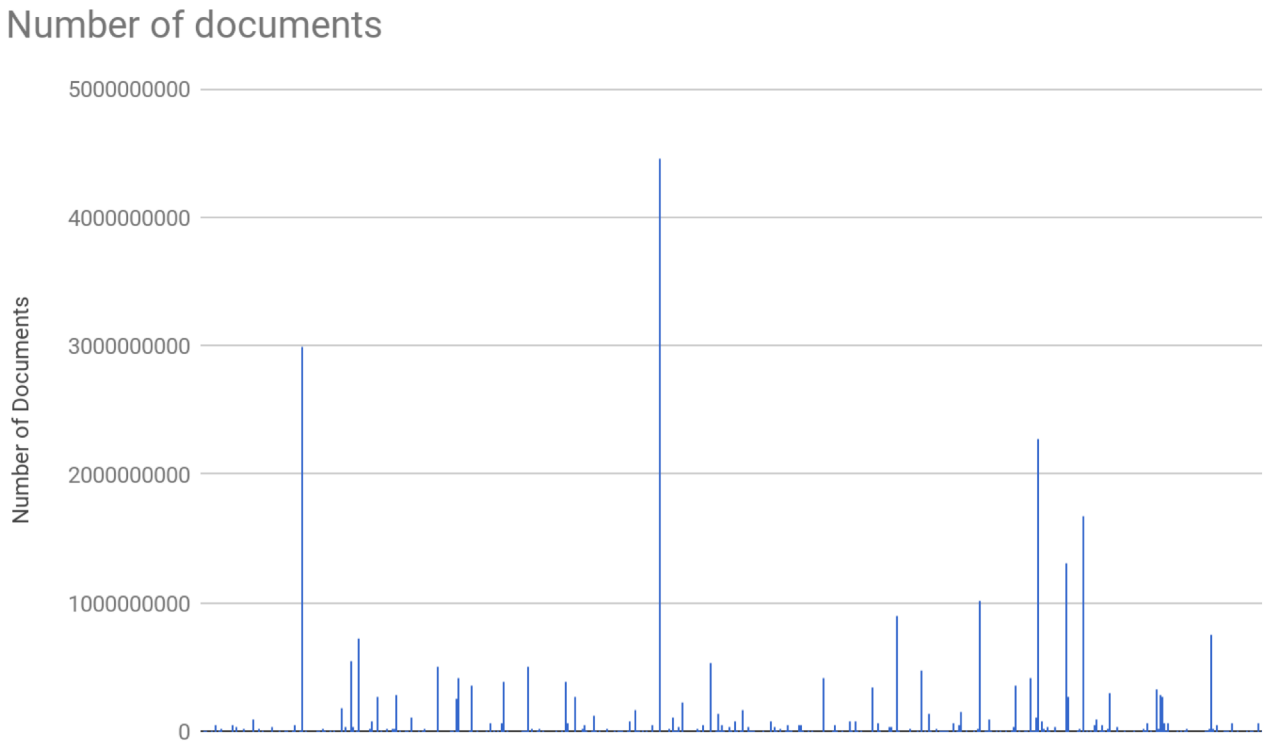
Version	End of Life?	Currently maintained?
5.5.2	2019-01-06	No
6.2.2	2019-08-06	Yes
2.3.2	2017-09-30	No
1.5.2	2016-09-23	No
5.3.2	2018-09-28	No
5.1.1	2018-06-08	No
6.0.1	2019-05-14	Yes

AWS Usage



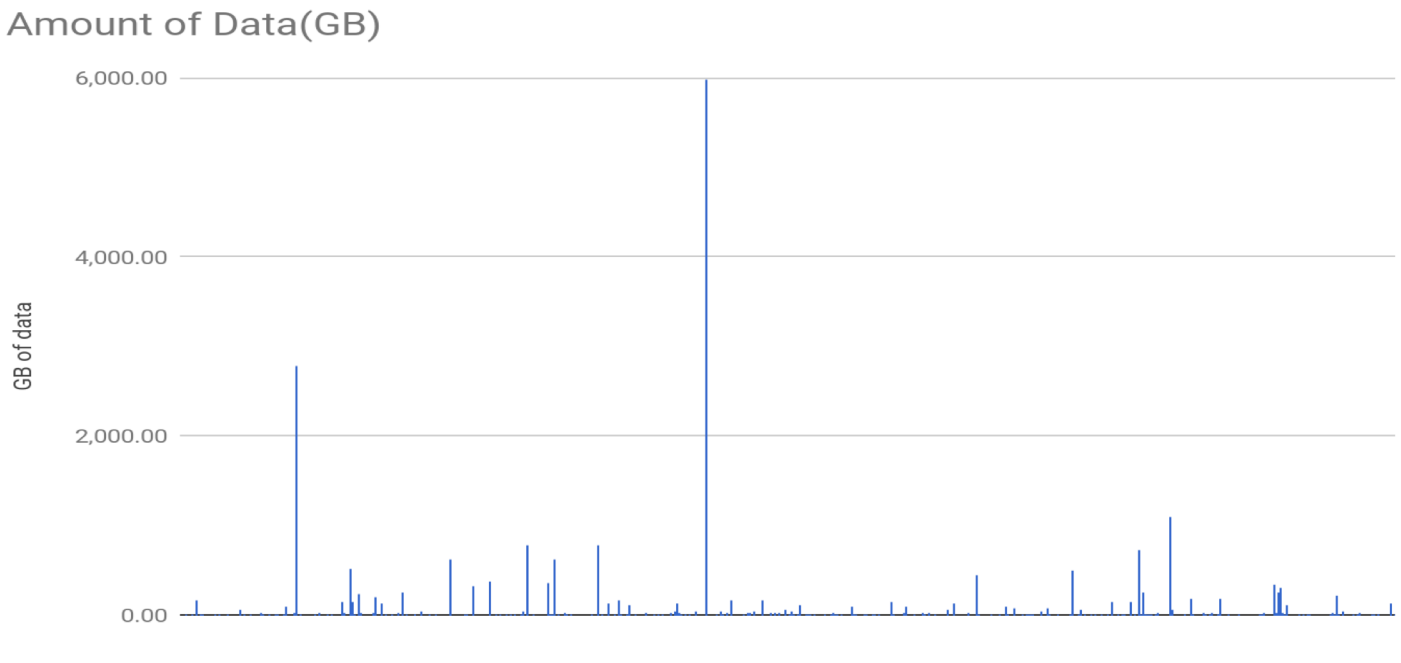
simon.whittaker@verticalstructure.com

Amount of Documents



simon.whittaker@verticalstructure.com

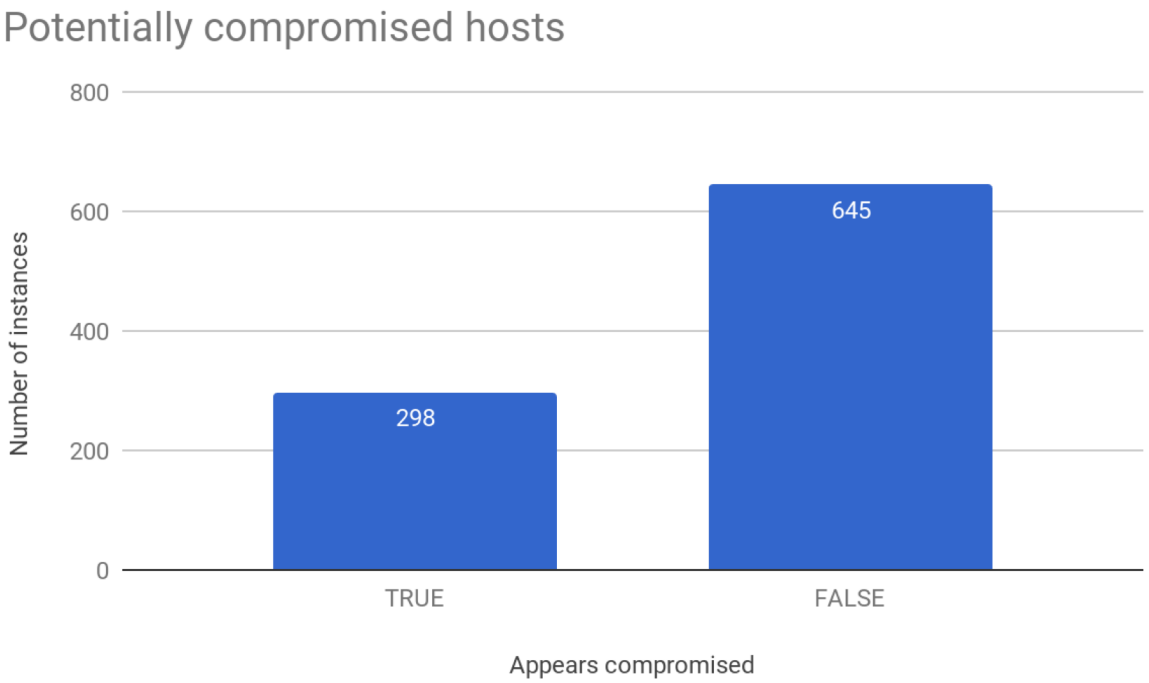
Amount of Data



Total Data is 24,510.49 GB

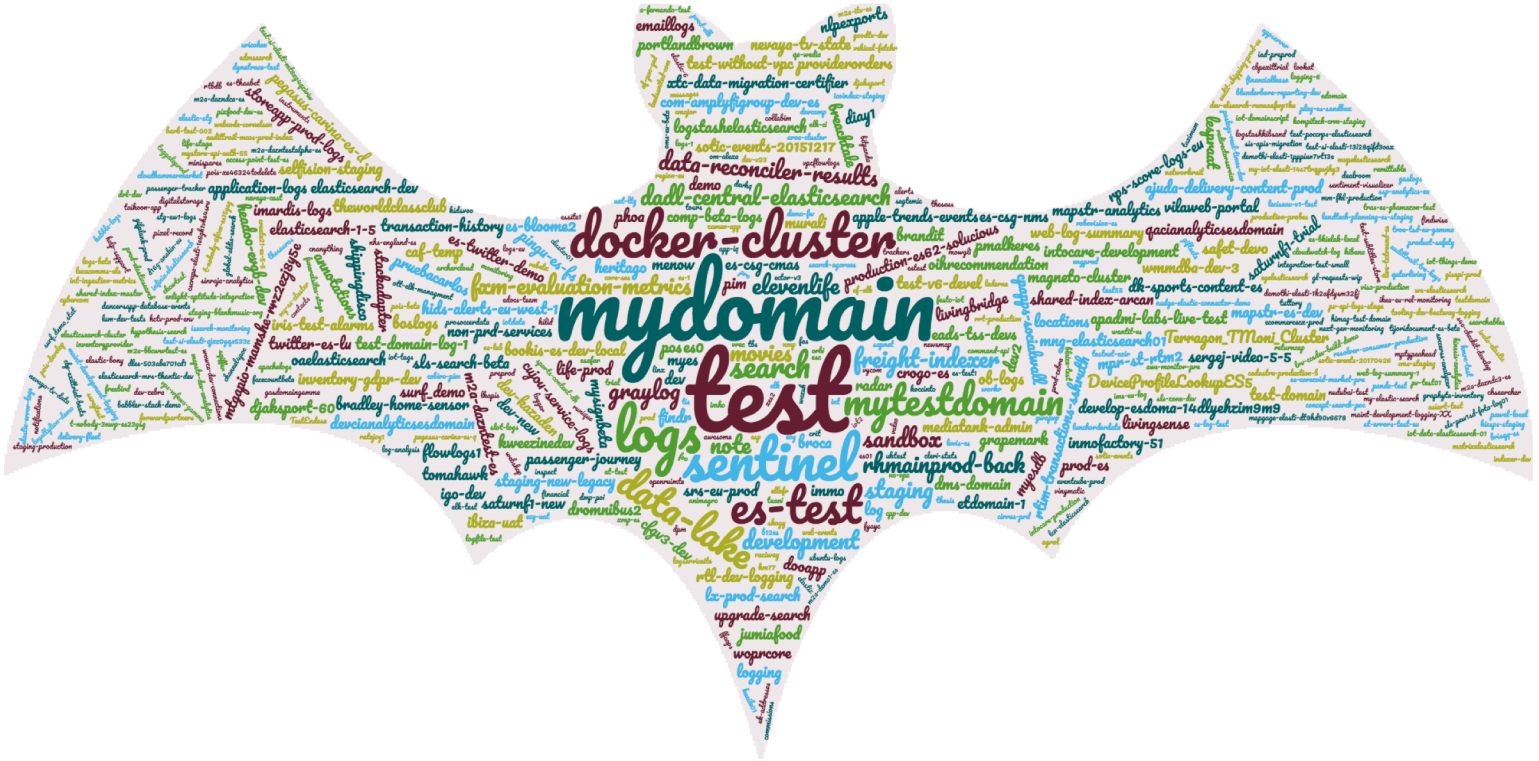
simon.whittaker@verticalstructure.com

Potentially Compromised Hosts



Basic:(command.php|hedwig.cgi|login.action|getcfg.php|wp-admin|jackposv2|jacpos|pleasereadthis|readme)

Who doesn't love a wordcloud?

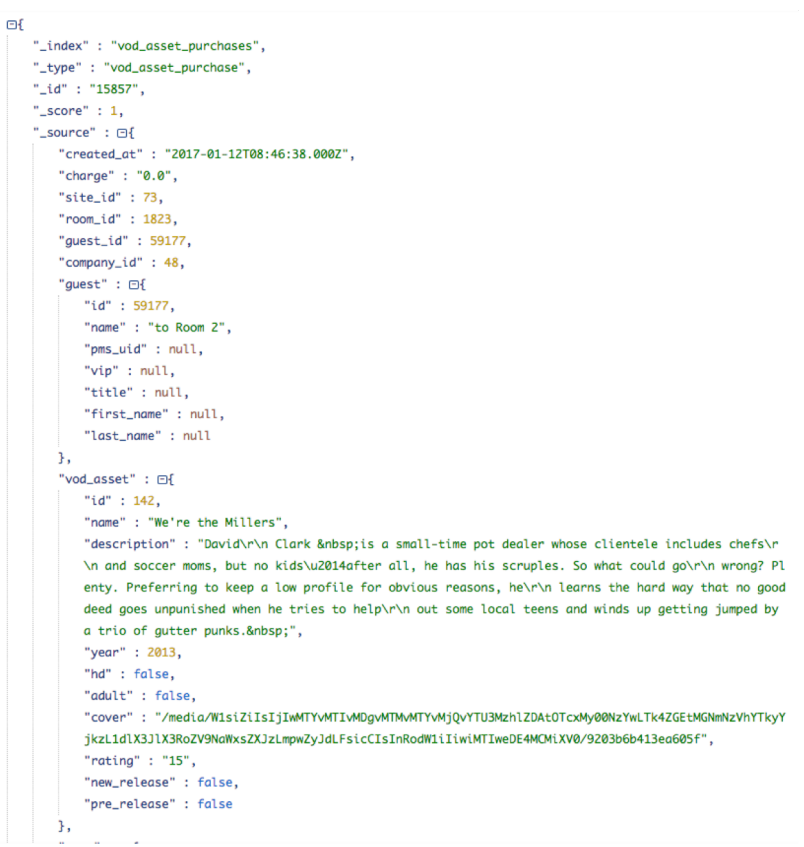


simon.whittaker@verticalstructure.com

Interesting Clusters

simon.whittaker@verticalstructure.com

Interesting clusters pt 2



simon.whittaker@verticalstructure.com

Interesting clusters pt 3

Store receipts

simon.whittaker@verticalstructure.com

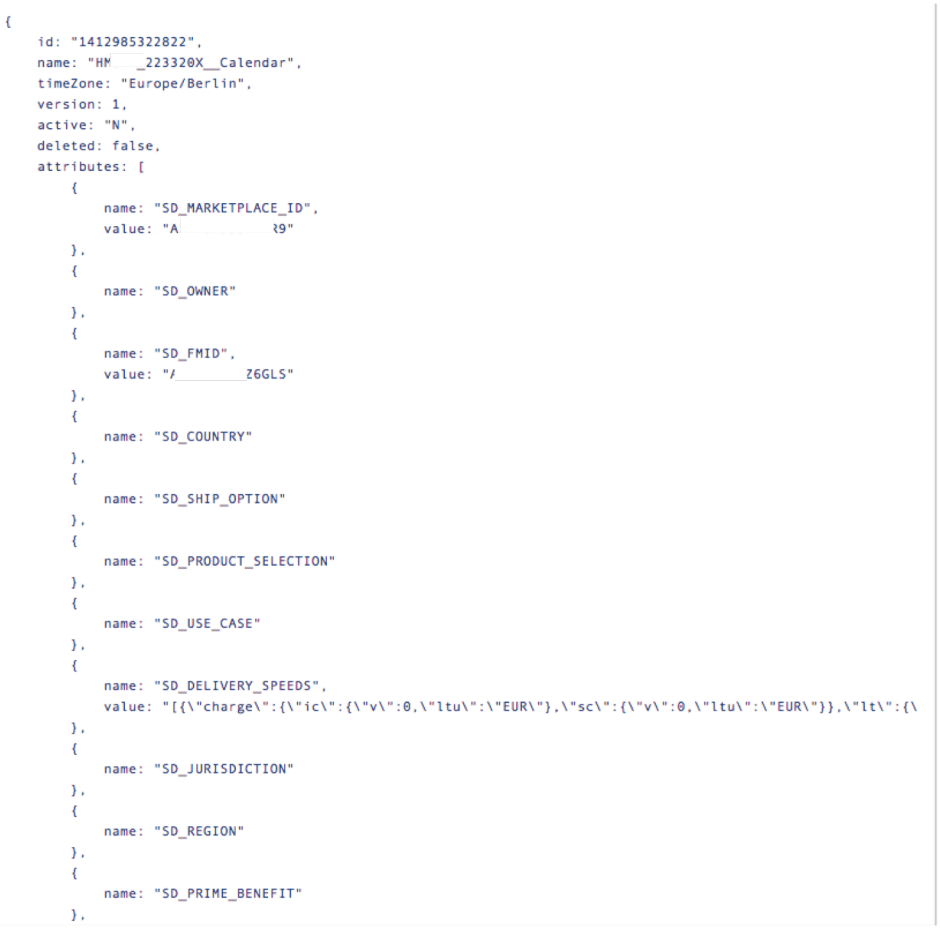
Interesting clusters pt 4 - a lot of logs


```
{
   "_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
```


simon.whittaker@verticalstructure.com

Interesting clusters pt 4 - a lot of logs



simon.whittaker@verticalstructure.com

Interesting clusters pt 4 - a lot of logs

simon.whittaker@verticalstructure.com

Interesting clusters pt 5

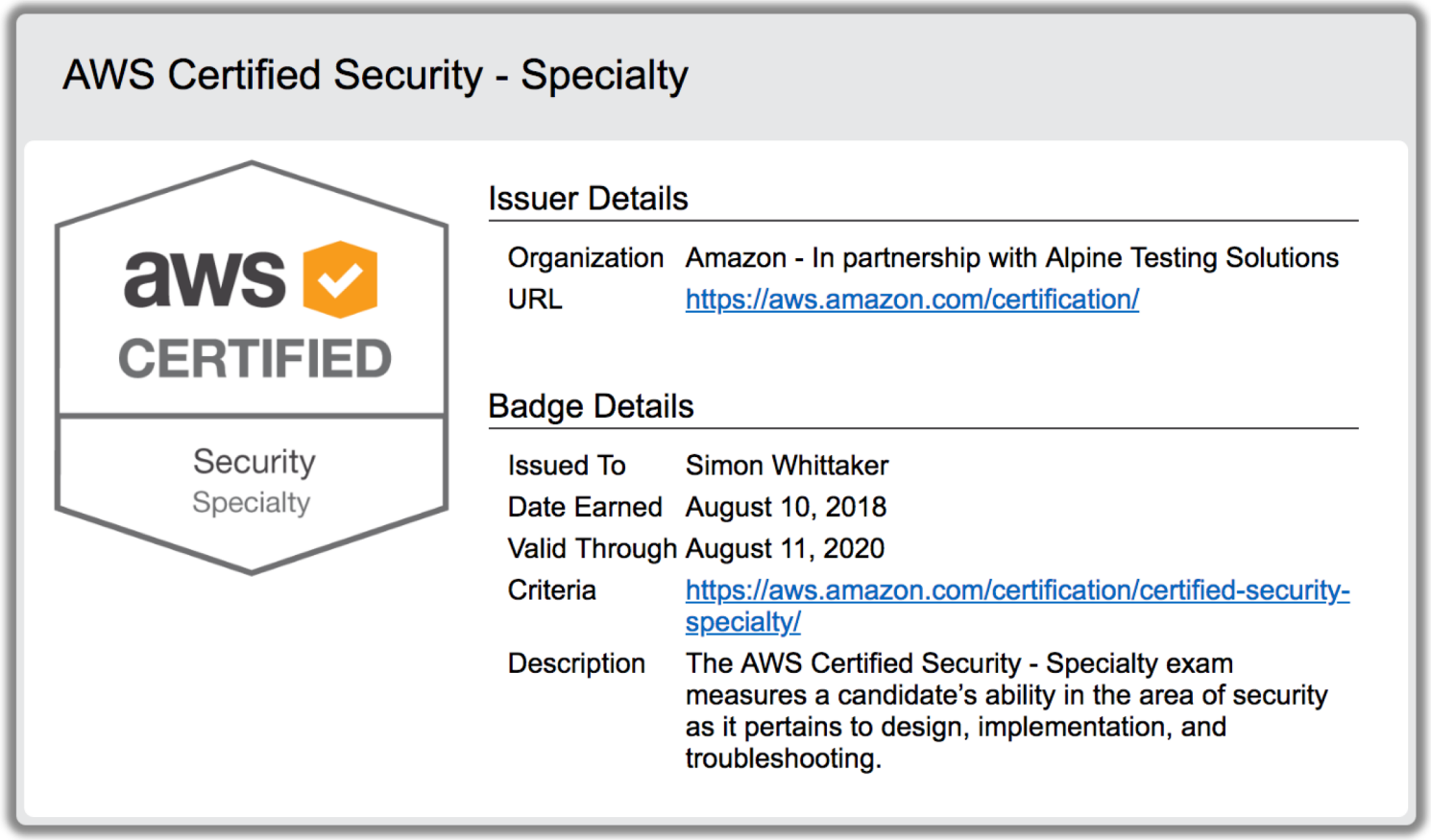
- Major brand names
- Broadcaster
- Online services
- Games providers
- Interesting index names
  - Inventory-gdpr-dev
  - kicsps-staging
  - Storeapp-prod-logs
  - Gisapi-prod

simon.whittaker@verticalstructure.com

We’re doing it wrong

simon.whittaker@verticalstructure.com

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.

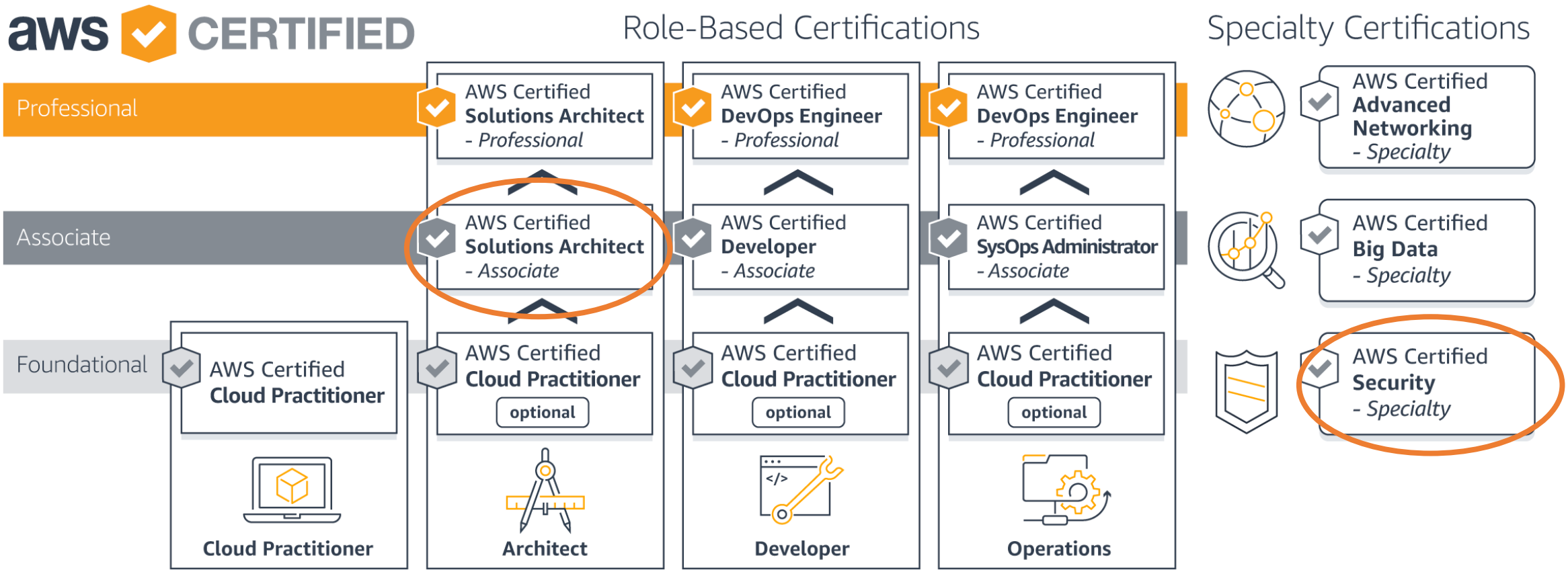
simon.whittaker@verticalstructure.com

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.

simon.whittaker@verticalstructure.com

Certification roadmap



simon.whittaker@verticalstructure.com

Exam format

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

simon.whittaker@verticalstructure.com

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%**

simon.whittaker@verticalstructure.com

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.

simon.whittaker@verticalstructure.com

Domain 2 – Logging and Monitoring

- 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.

simon.whittaker@verticalstructure.com

Domain 3 – Infrastructure Security

- 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.

simon.whittaker@verticalstructure.com

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.

simon.whittaker@verticalstructure.com

Domain 5 – Data Protection

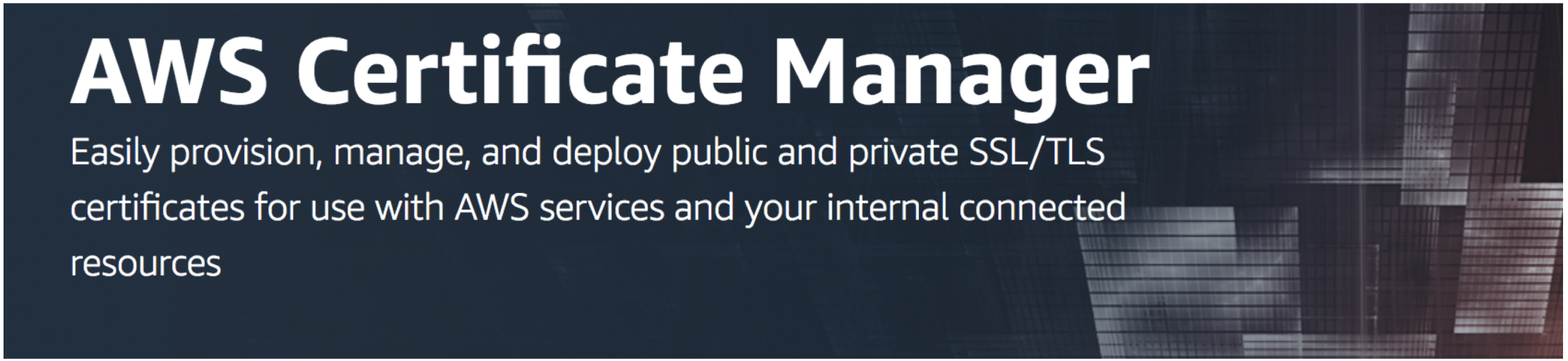
- 5.1 Design and implement key management and use.
- 5.2 Troubleshoot key management.
- 5.3 Design and implement a data encryption solution for data at rest and data in transit.

simon.whittaker@verticalstructure.com

The big stuff – from my experience

simon.whittaker@verticalstructure.com

The big stuff – from my experience



simon.whittaker@verticalstructure.com

The big stuff – from my experience

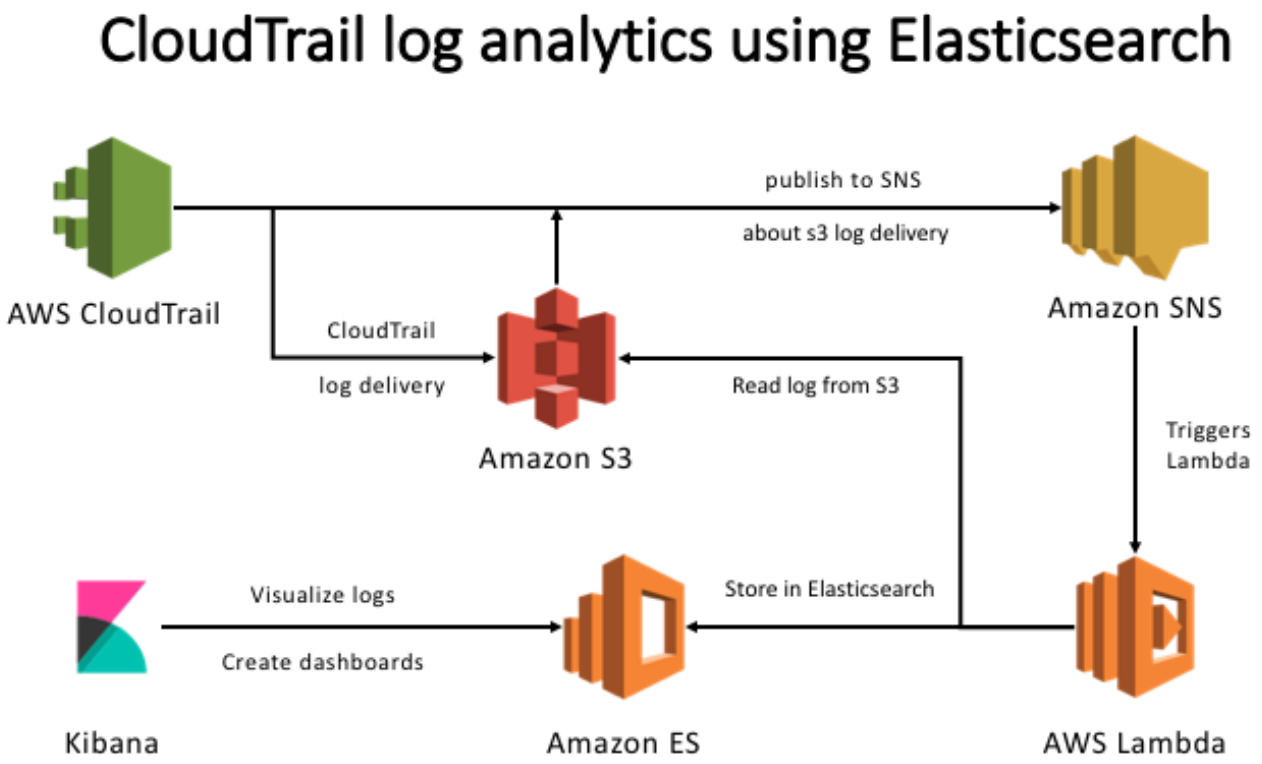
Simon.whittaker@verticalstructure.com

Regulatory requirements

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

simon.whittaker@verticalstructure.com

Logging Suggestions



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

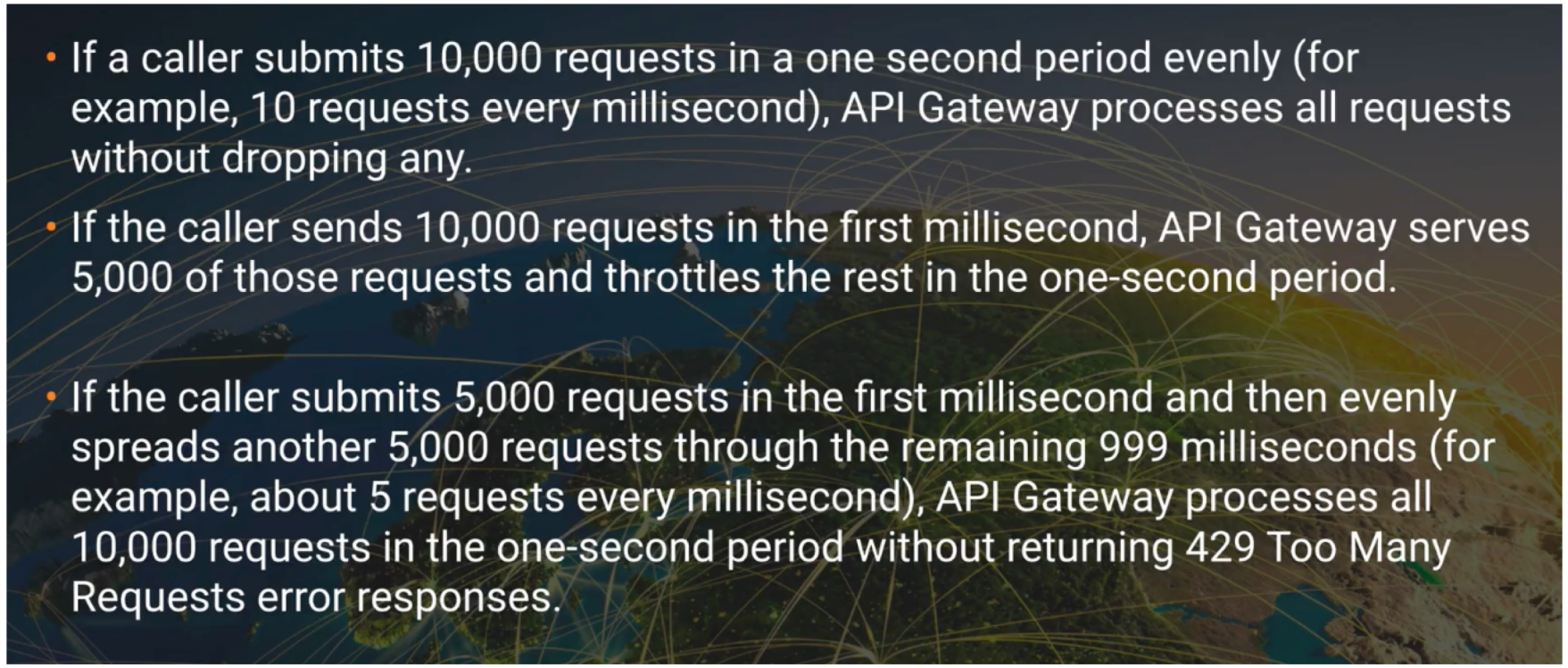
simon.whittaker@verticalstructure.com

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

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

simon.whittaker@verticalstructure.com

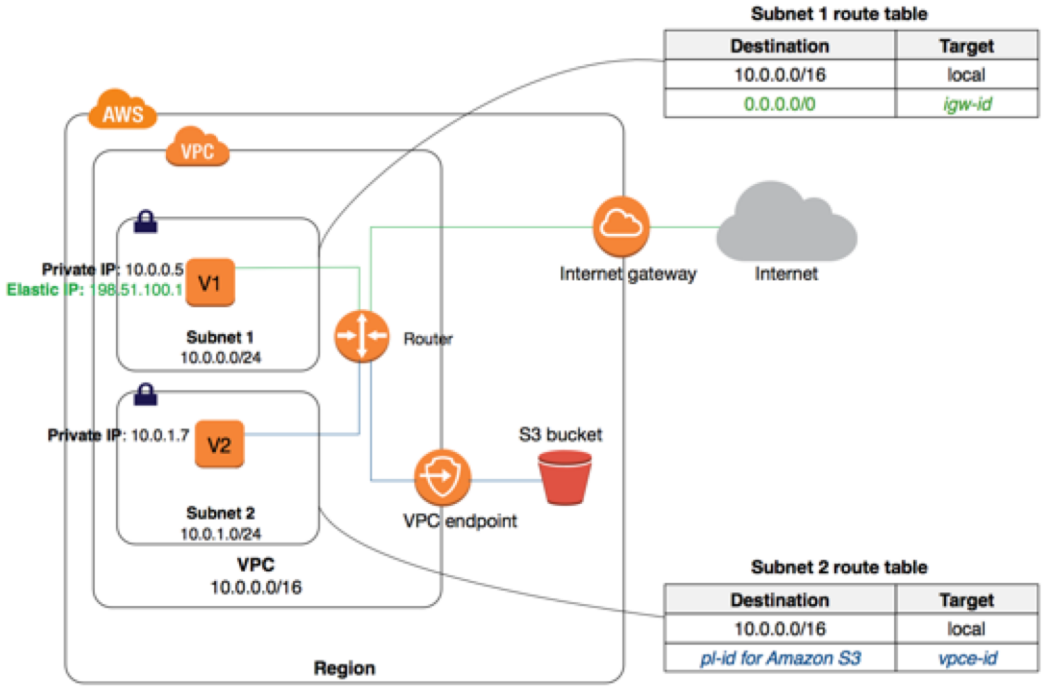
API gateway



simon.whittaker@verticalstructure.com

Hide the instances

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



simon.whittaker@verticalstructure.com

Other useful items to help prepare

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

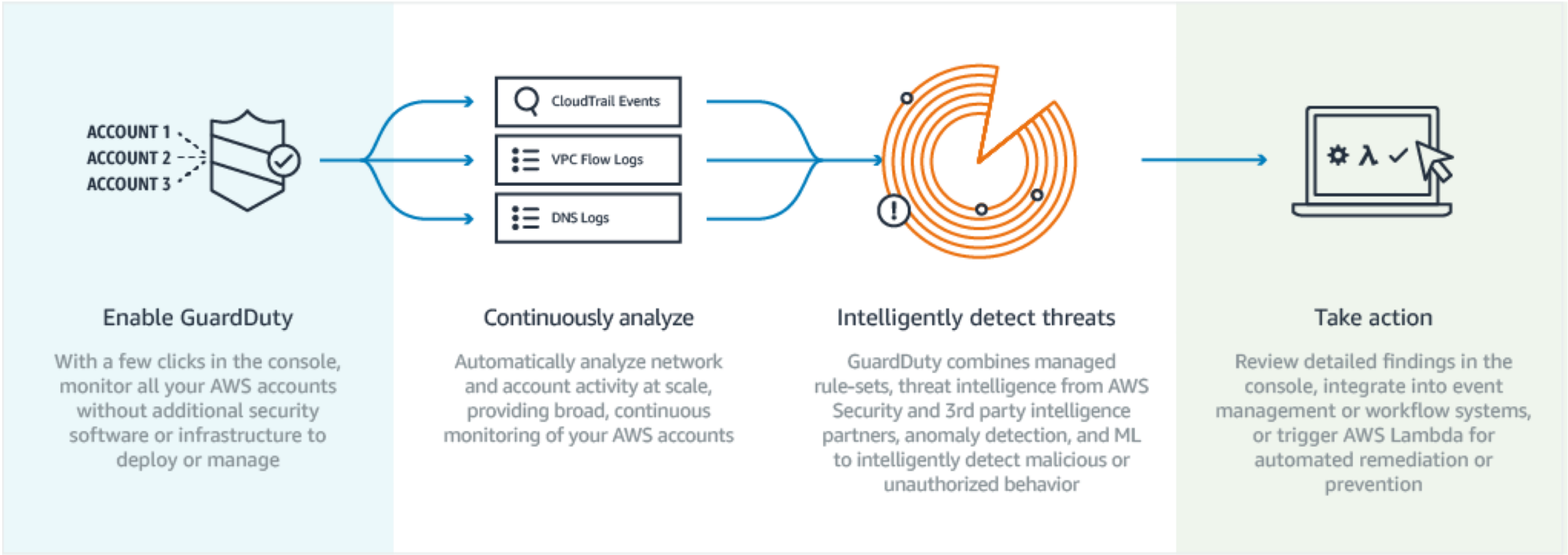
simon.whittaker@verticalstructure.com

Tools

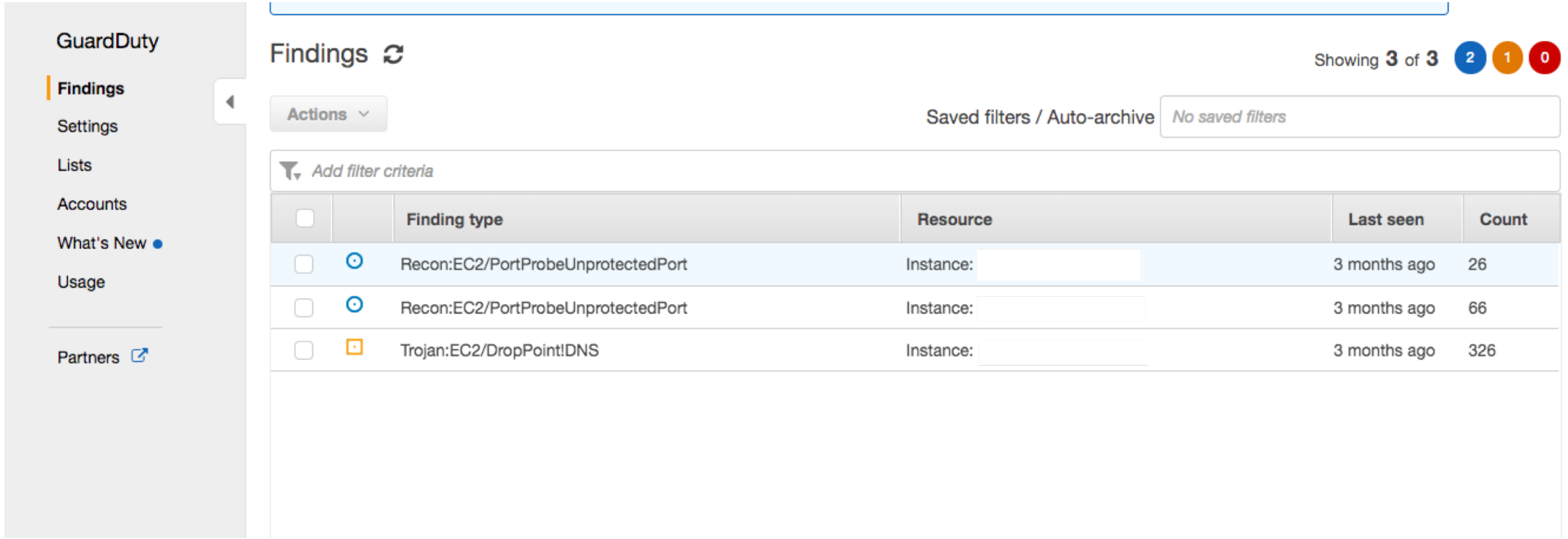
Useful tools

Simon.whittaker@verticalstructure.com

Guardduty – Intelligent threat detection and continuous monitoring

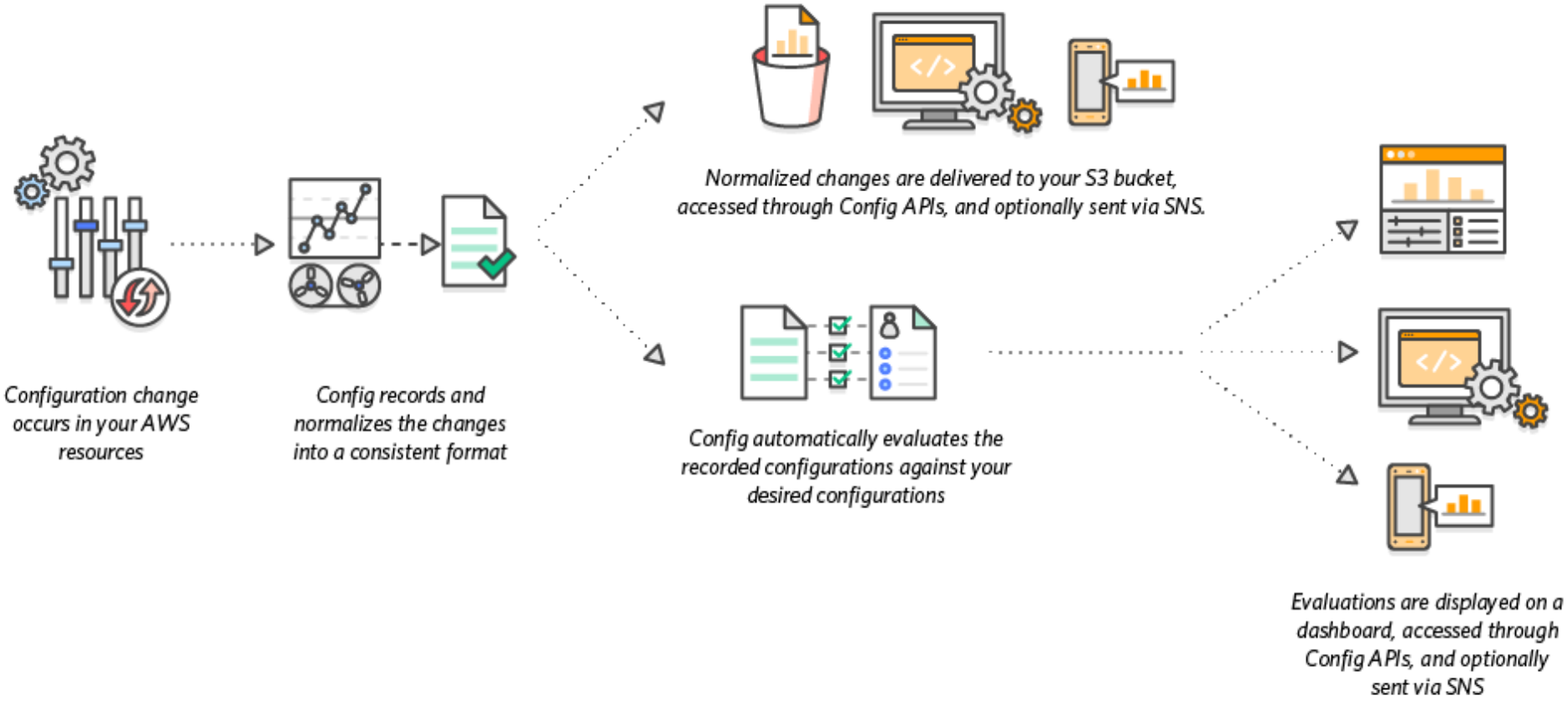


simon.whittaker@verticalstructure.com

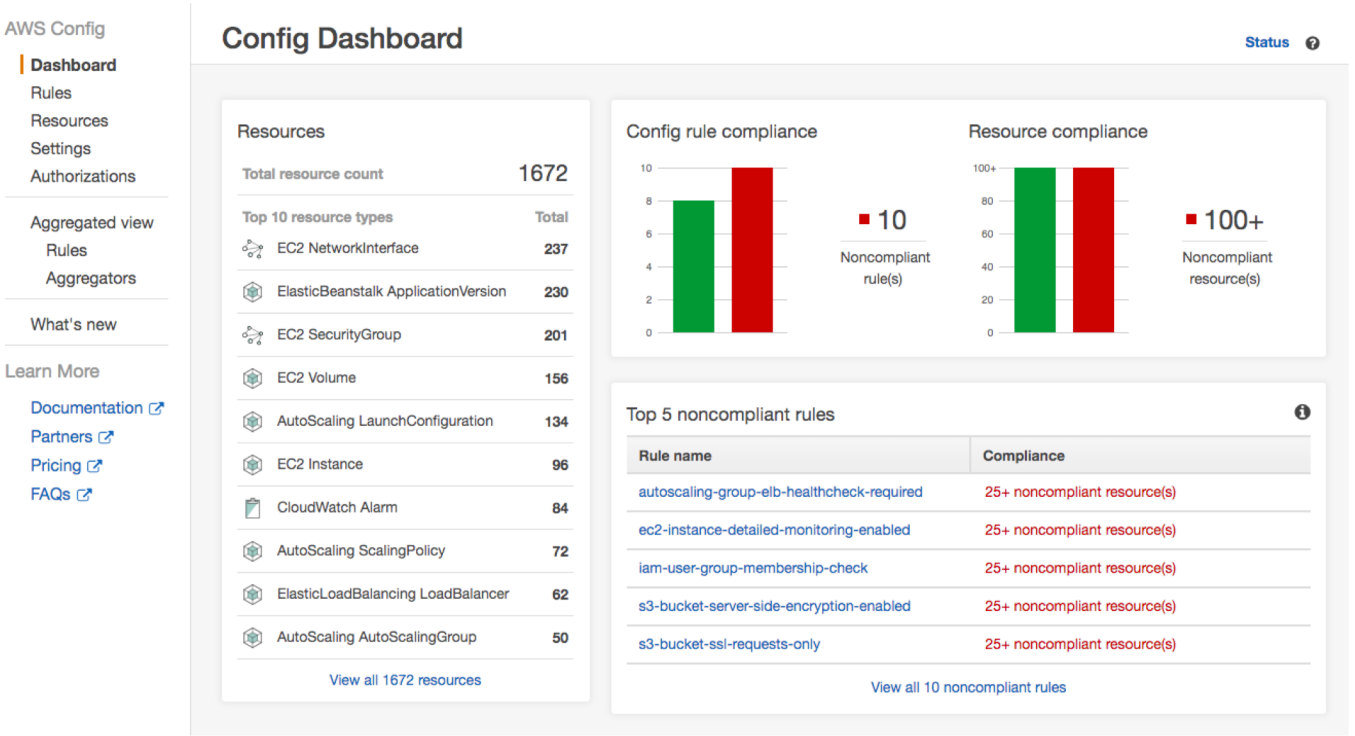


simon.whittaker@verticalstructure.com

Config - Record and evaluate configurations of your AWS resources



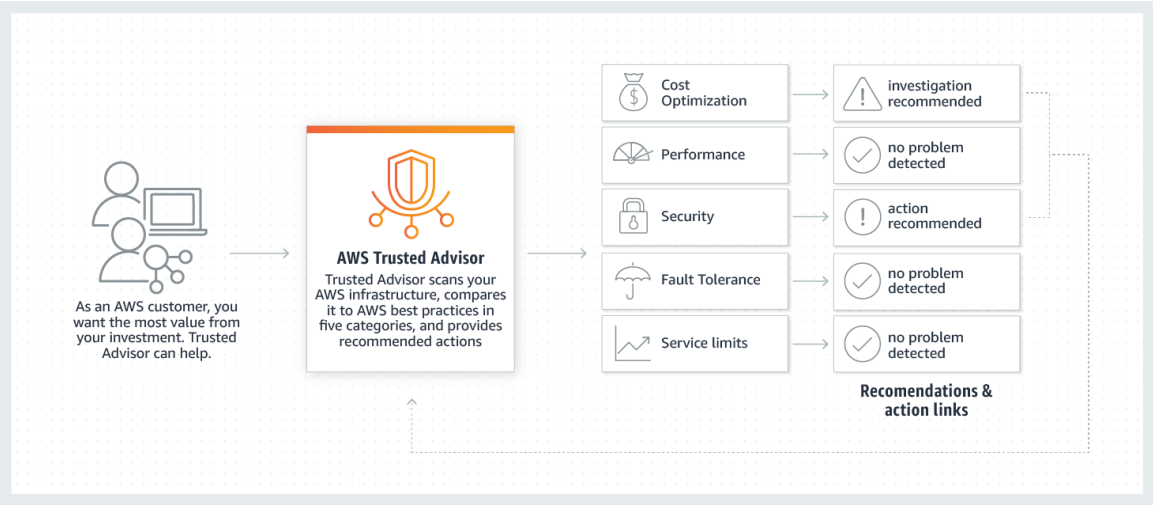
simon.whittaker@verticalstructure.com



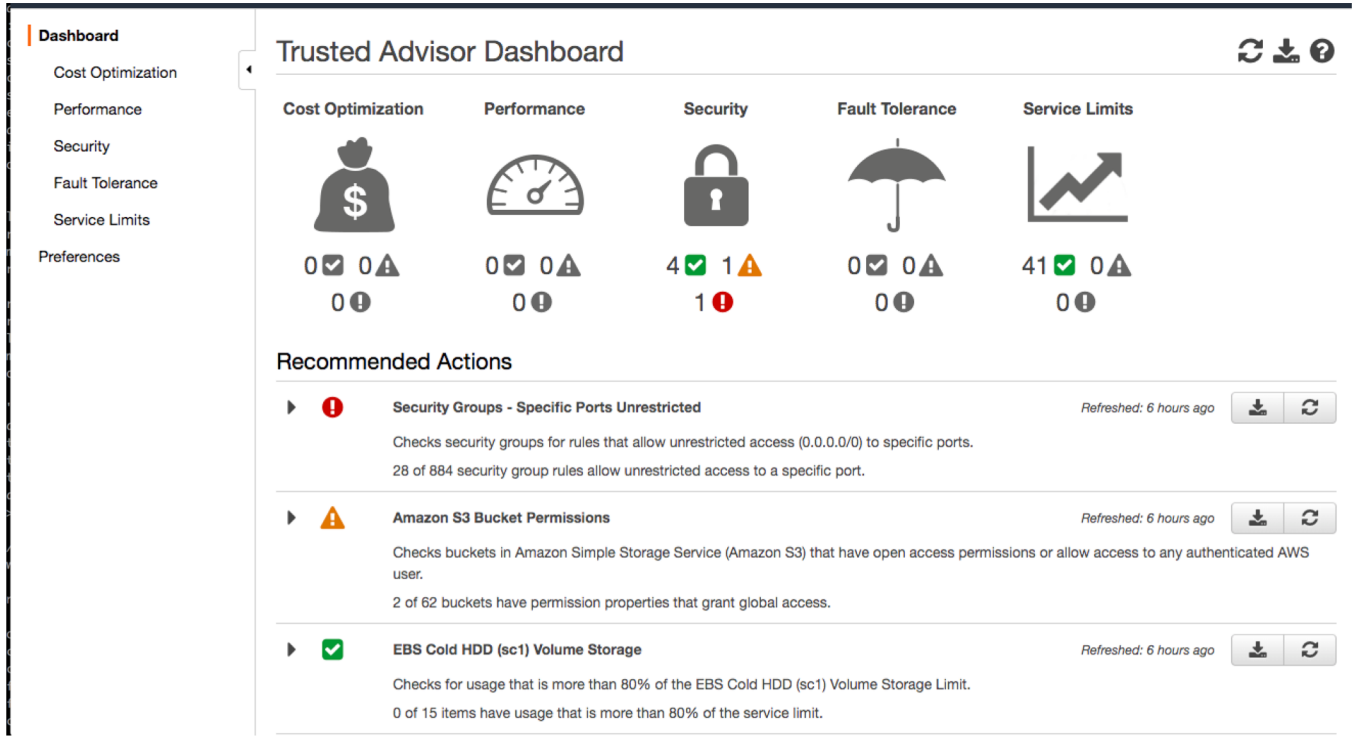
Inspector - Automated security assessment service

simon.whittaker@verticalstructure.com

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

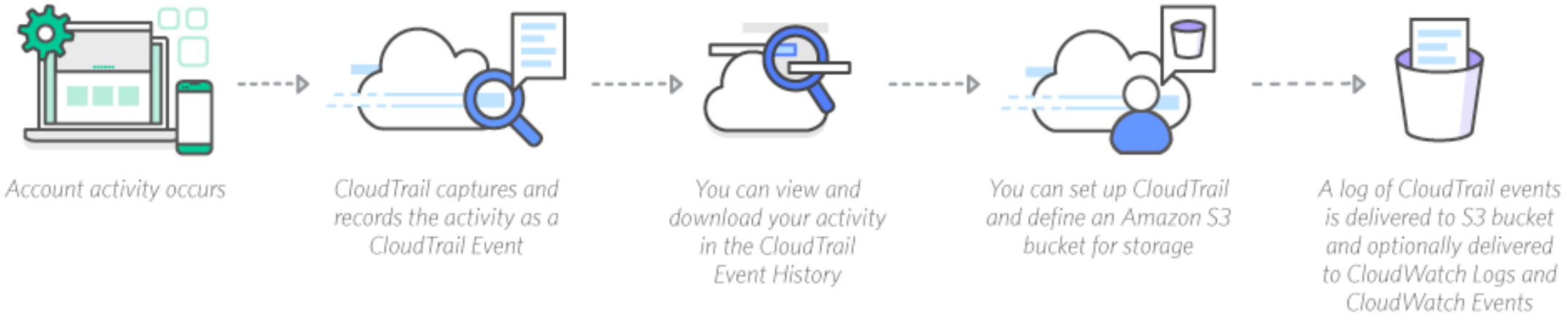


simon.whittaker@verticalstructure.com

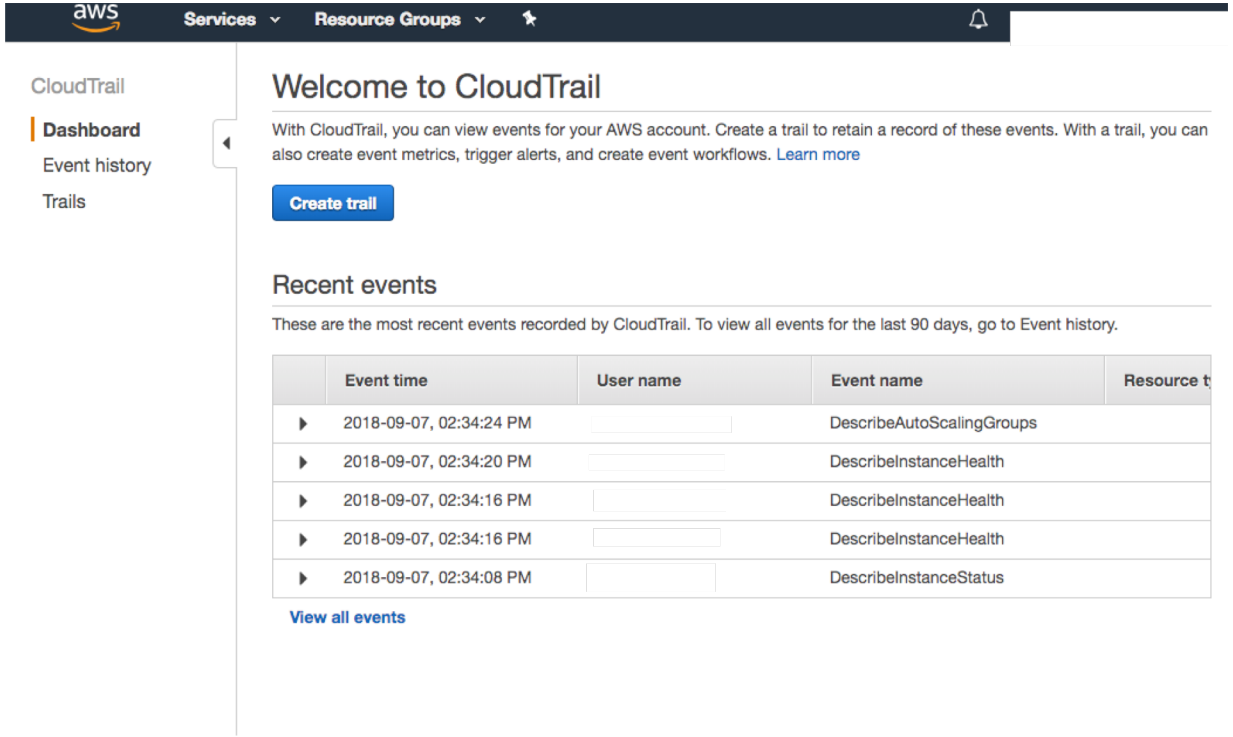


simon.whittaker@verticalstructure.com

Cloudtrail - Track user activity and API usage

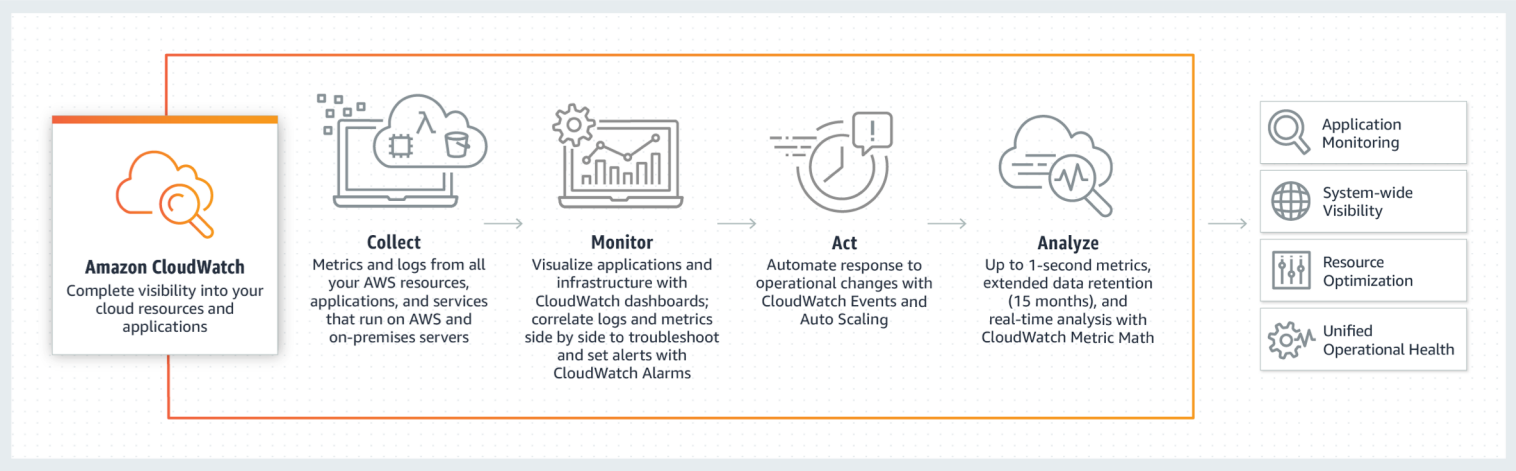


simon.whittaker@verticalstructure.com



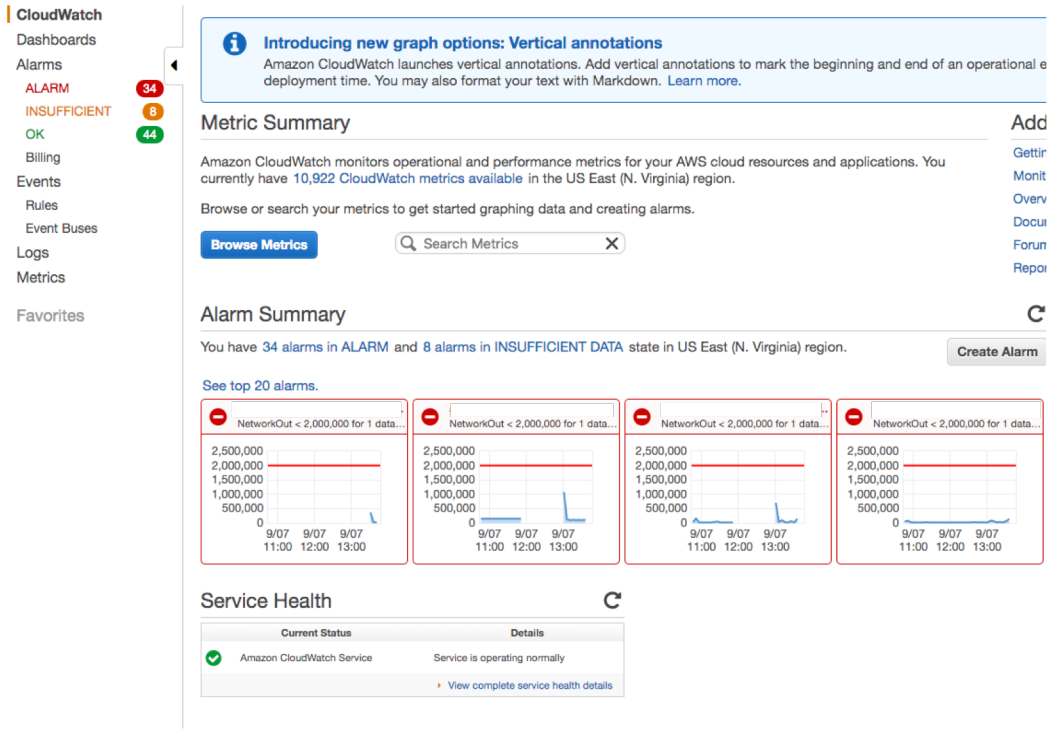
simon.whittaker@verticalstructure.com

Cloudwatch - Complete Visibility of Your Cloud Resources and Applications



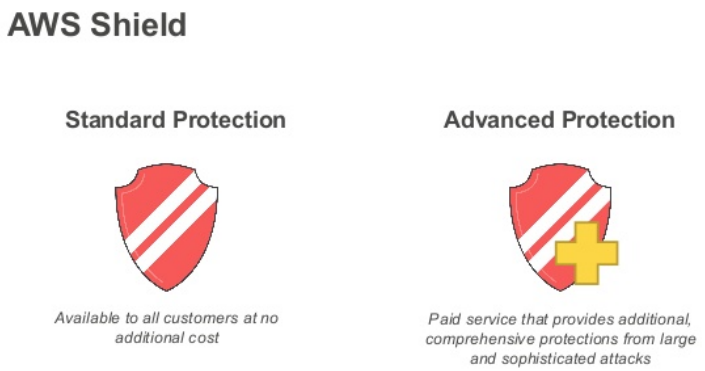
simon.whittaker@verticalstructure.com

Cloudwatch



simon.whittaker@verticalstructure.com

Shield – Managed DDoS Protection



simon.whittaker@verticalstructure.com

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.

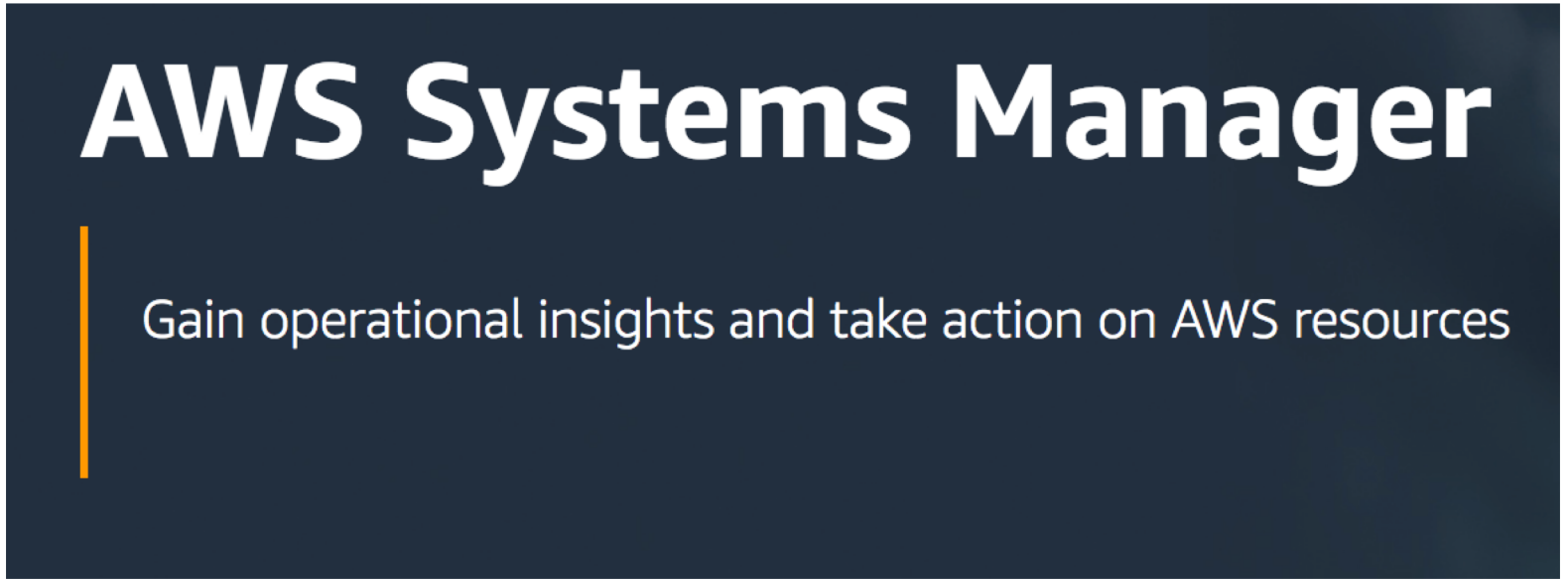
Features	AWS Shield Standard	AWS Shield Advanced
Active monitoring		
Network flow monitoring	✔	✔
Automated application (layer 7) traffic monitoring	-	✔
DDoS mitigations		
Helps protect from common DDoS attacks, such as SYN floods and UDP reflection attacks	✔	✔
Access to additional DDoS mitigation capacity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

simon.whittaker@verticalstructure.com

WAF – Web Application Firewall

simon.whittaker@verticalstructure.com

AWS Systems Manager



simon.whittaker@verticalstructure.com

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

simon.whittaker@verticalstructure.com

Fancy trying your hand?

https://vsltd.co/devopsbelfastnov18