RICHEY MAY Technology Solutions

Discover / Develop / Deliver

Quarantining your Cloud: The Return of COVID-19

Michael Wylie, MBA, CISSP

About me:

linkedin.com/in/mwylie

twitter.com/TheMikeWylie

Michael Wylie, MBA, CISSP

Director, Cybersecurity Services

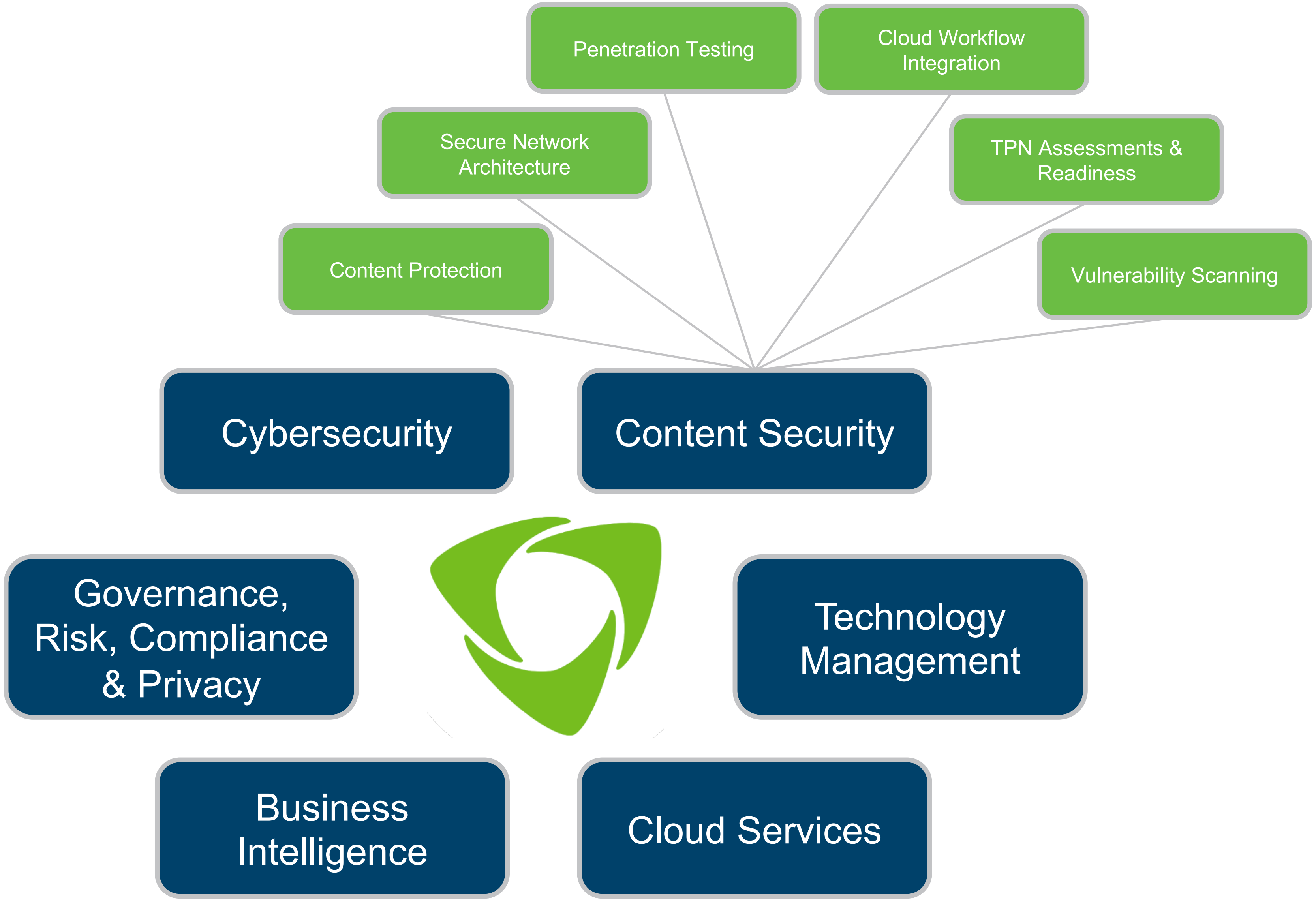
RICHEY MAY TECHNOLOGY SOLUTIONS

Additional Certifications

- GPEN
- GMON
- CEH
- CEI
- TPN
- Pentest+

- CCNA R&S
- CCNA CyberOps
- Project+
- CHPA
- Security+

About Richey May Technology Solutions



Penetration Testing

Cloud Workflow Integration

Secure Network Architecture

TPN Assessments & Readiness

Content Protection

Vulnerability Scanning

Cybersecurity

Content Security

Governance, Risk, Compliance & Privacy

Technology Management

Business Intelligence

Cloud Services

My Dream

Continuou g (CCSM)

RICHEY MAY Technology Solutions

Quarantining your Cloud: The Return of COVID-19

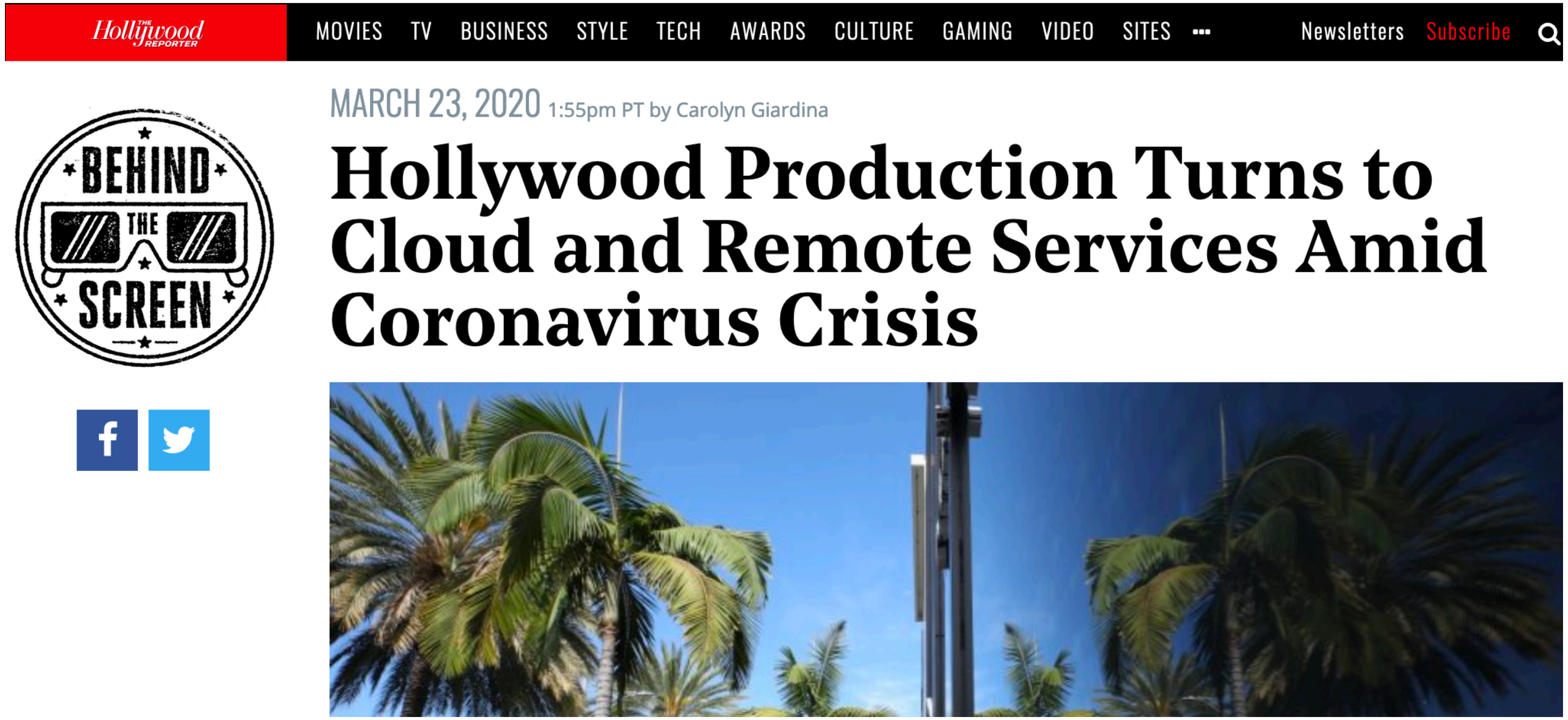
"The COVID-19 pandemic may give businesses the jolt they need to move [to] cloud computing" – Forbes

Content owner's concern with "The Cloud":

- 2019 – Capital One (~100m records)
- 2020 – MGM Resorts (~10.6m guest records)
- 2020 – Telegram (~42 million records)

Sources: logmeonce.com & forbes.com

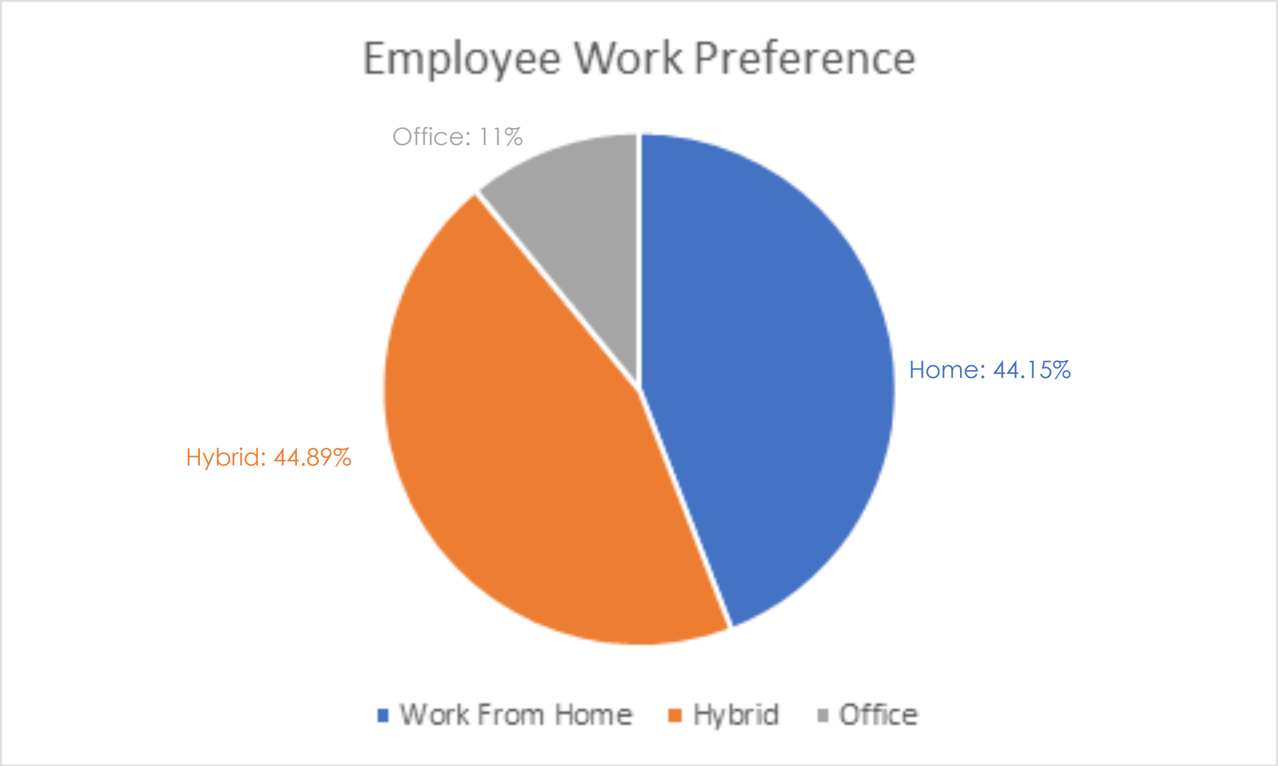
The cat's out of the bag now



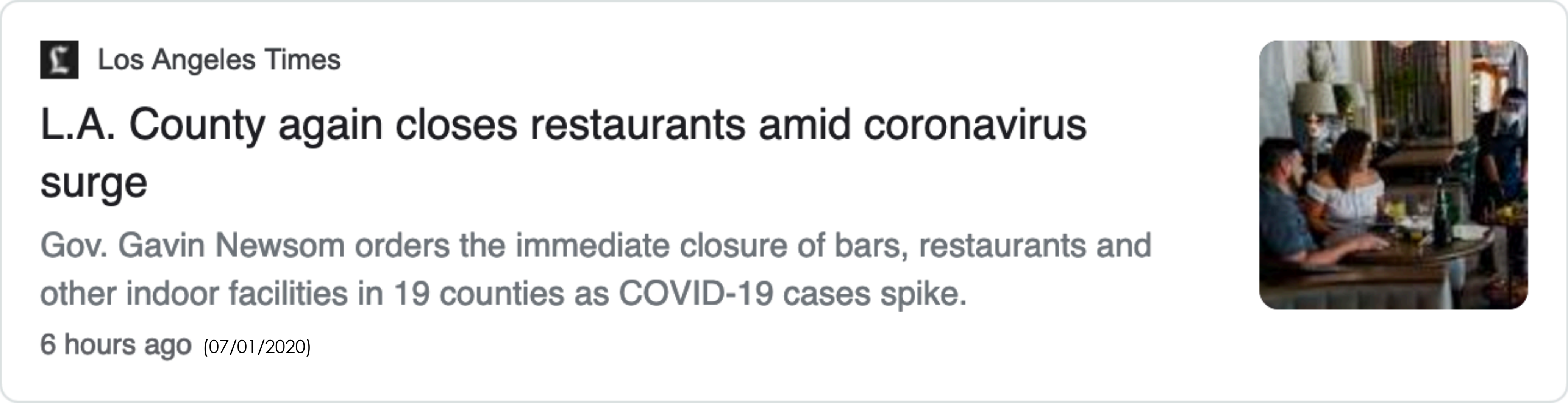
MARCH 23, 2020 1:55pm PT by Carolyn Giardina

Hollywood Production Turns to Cloud and Remote Services Amid Coronavirus Crisis

The cat’s out of the bag now



CDC: "A COVID-19 outbreak could last for a long time in your community.”



Los Angeles Times

L.A. County again closes restaurants amid coronavirus surge

Gov. Gavin Newsom orders the immediate closure of bars, restaurants and other indoor facilities in 19 counties as COVID-19 cases spike.

6 hours ago (07/01/2020)

RICHEY MAY Technology Solutions

Quarantining your Cloud: The Return of COVID-19

Continuous Cloud Security Monitoring (CCSM)

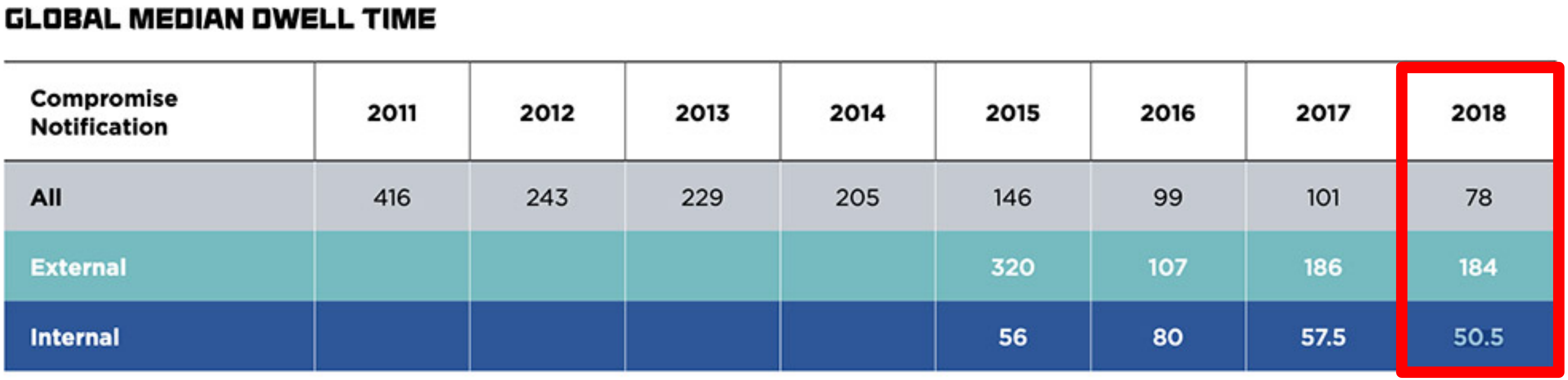
Continuous Security Monitoring (CSM)

CONTINUOUS SECURITY MONITORING (CSM)

- Strategy
- Ongoing automated detection and response to cyber threats
- Continually reassess security posture
- Keeping up with changing threat and vulnerability landscape
- Provides increased visibility
- Goal of timely incident detection
- Focus on data at rest

Dwell Time

(time from breach to detection)

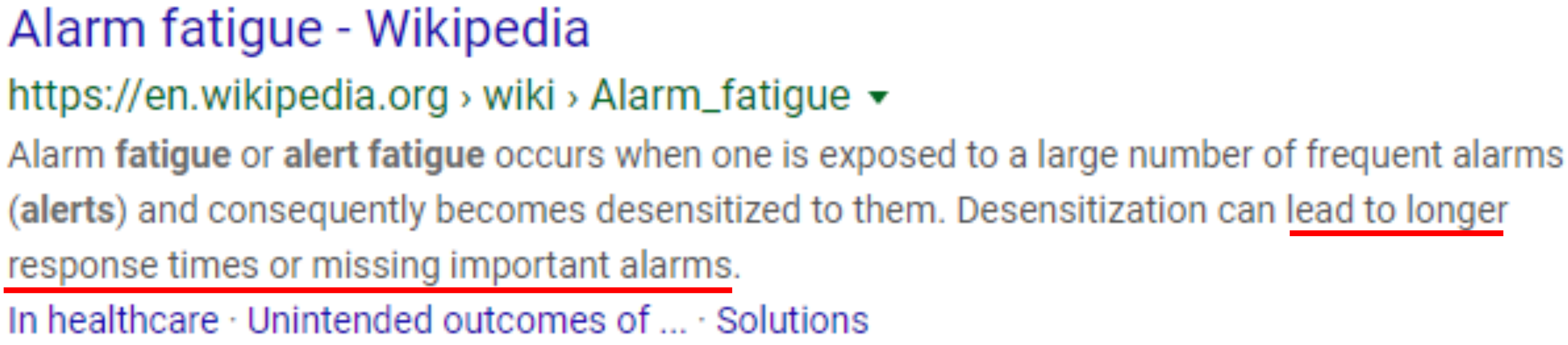


GLOBAL MEDIAN DWELL TIME

Compromise Notification	2011	2012	2013	2014	2015	2016	2017	2018
All	416	243	229	205	146	99	101	78
External					320	107	186	184
Internal					56	80	57.5	50.5

Source: FireEye's Mandiant M-Trends 2019 report

Alert Fatigue is Real

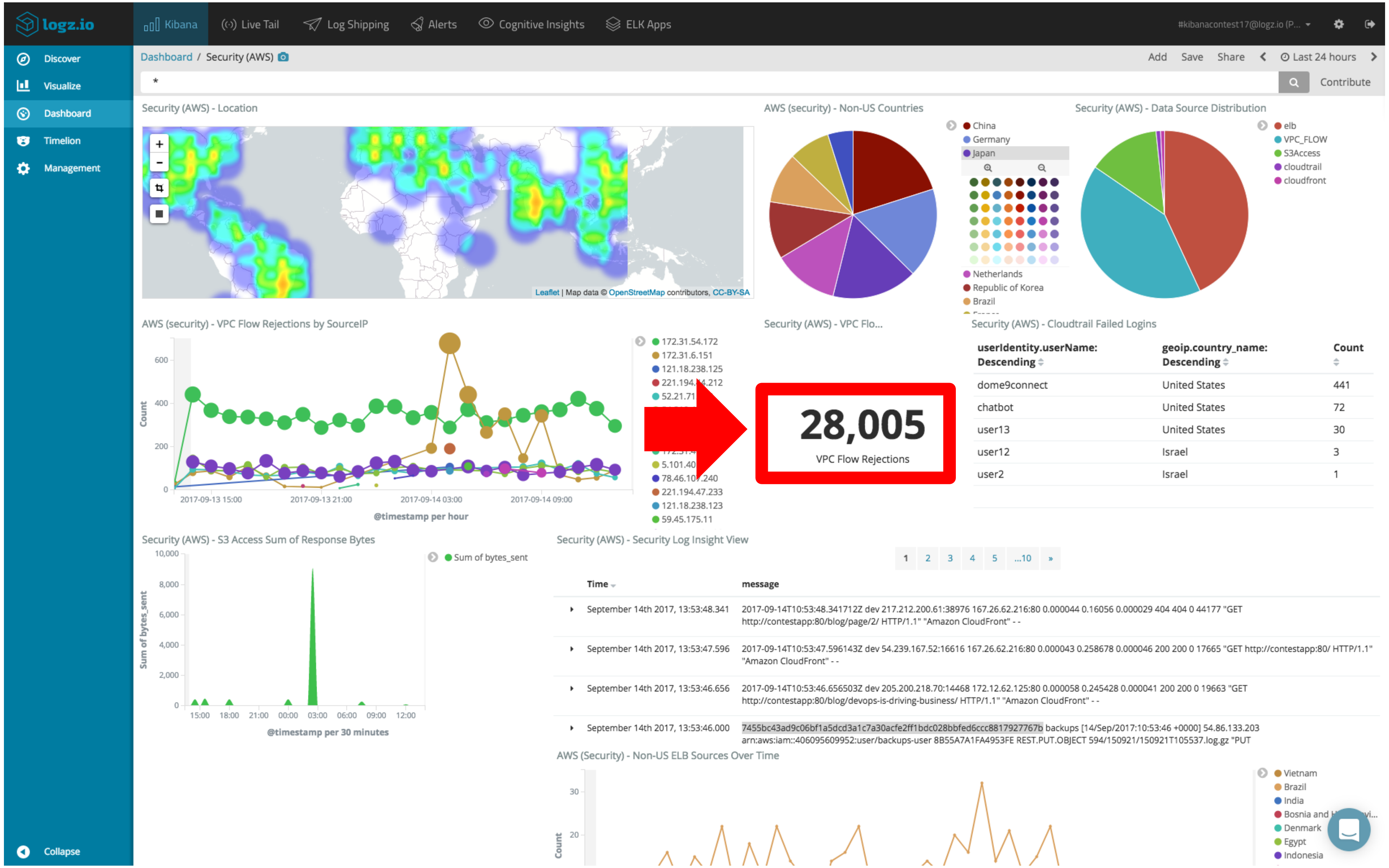


Alarm fatigue - Wikipedia

https://en.wikipedia.org › wiki › Alarm_fatigue ▾

Alarm **fatigue** or **alert fatigue** occurs when one is exposed to a large number of frequent alarms (**alerts**) and consequently becomes desensitized to them. Desensitization can lead to longer response times or missing important alarms.

In healthcare · Unintended outcomes of ... · Solutions



Security (AWS) - Cloudtrail Failed Logins

userIdentity.userName: Descending	geoip.country_name: Descending	Count
dome9connect	United States	441
chatbot	United States	72
user13	United States	30
user12	Israel	3
user2	Israel	1

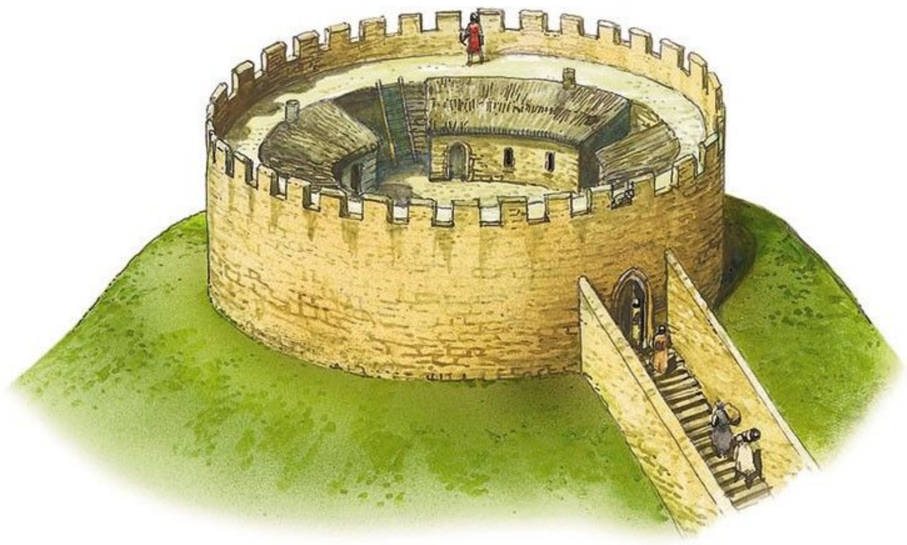
Security (AWS) - Security Log Insight View

1 2 3 4 5 ...10 »

Time	message
September 14th 2017, 13:53:48.341	2017-09-14T10:53:48.341712Z dev 217.212.200.61:38976 167.26.62.216:80 0.000044 0.16056 0.000029 404 404 0 44177 "GET http://contestapp:80/blog/page/2/ HTTP/1.1" "Amazon CloudFront" - -
September 14th 2017, 13:53:47.596	2017-09-14T10:53:47.596143Z dev 54.239.167.52:16616 167.26.62.216:80 0.000043 0.258678 0.000046 200 200 0 17665 "GET http://contestapp:80/ HTTP/1.1" "Amazon CloudFront" - -
September 14th 2017, 13:53:46.656	2017-09-14T10:53:46.656503Z dev 205.200.218.70:14468 172.12.62.125:80 0.000058 0.245428 0.000041 200 200 0 19663 "GET http://contestapp:80/blog/devops-is-driving-business/ HTTP/1.1" "Amazon CloudFront" - -
September 14th 2017, 13:53:46.000	7455bc43ad9c06bf1a5dcd3a1c7a30acfe2ff1bdc028bbfed6ccc8817927767b backups [14/Sep/2017:10:53:46 +0000] 54.86.133.203 arn:aws:iam::406095609952:user/backups-user 8B55A7A1FA4953FE REST.PUT.OBJECT 594/150921/150921T105537.log.gz "PUT

RICHEY MAY Technology Solutions

How would you build a defensible fortress?



Source: q-files.com

Defensible Agra Red Fort

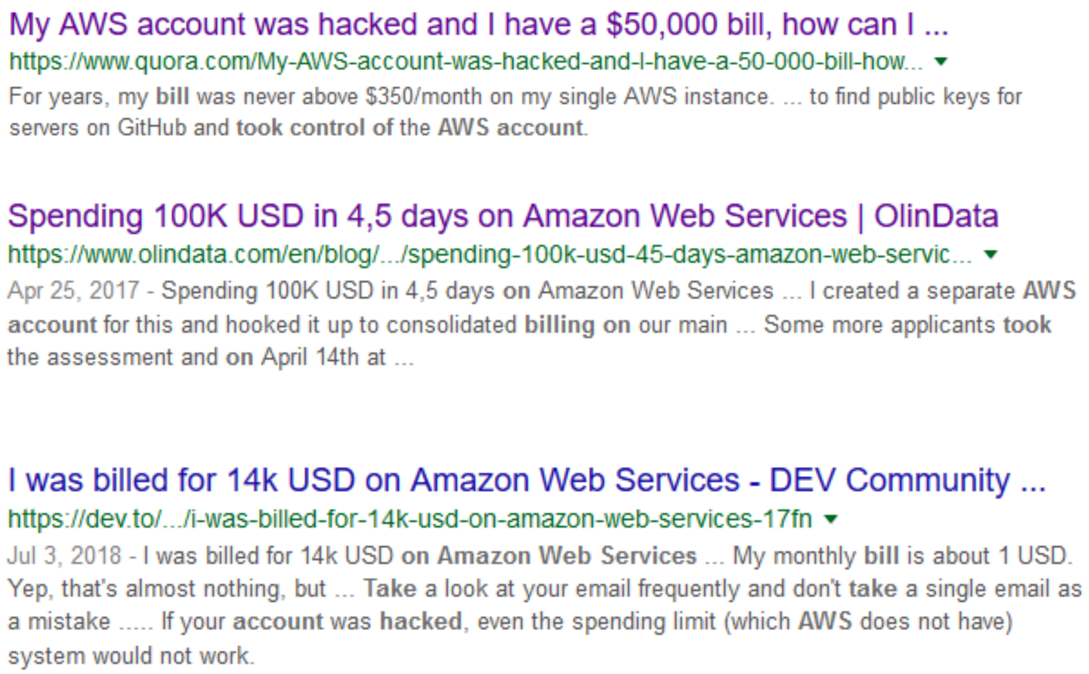
- High thick walls with archers
- Draw bridges
- Water moat with crocodiles
- Dry moat with tigers
- Layered corridors for trapping intruders
- Sloped upwards towards the inner circle
- Narrow hallways with rolling boulders
- Hot/boiling oil poured into hallways
- Controlled ingress/egress points

Source: travel.in

Normal or Evil

- New instances are spun up at 3AM in South Korea. Normal or Evil?
- 50 new instances don’t have names or tags. Normal or Evil?
- A cloud account spins up 100 new servers. Normal or Evil?
- Cloud bill tripled last month. Normal or Evil?
- 10 failed root login attempts. Normal or Evil?

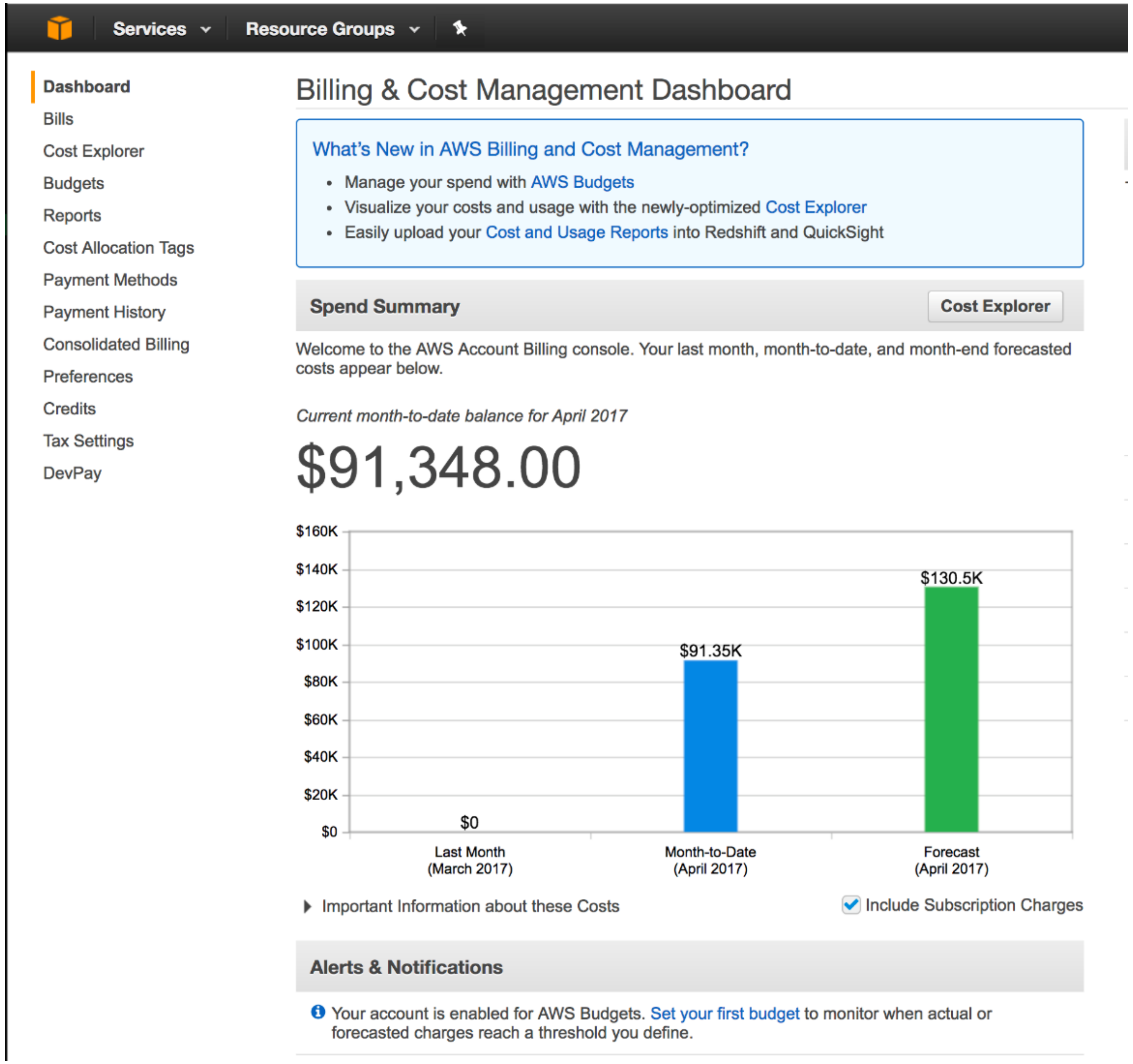
Without a Defensible Cloud, We’ll Never Know.



My AWS account was hacked and I have a $50,000 bill, how can I ...
https://www.quora.com/My-AWS-account-was-hacked-and-I-have-a-50-000-bill-how... ▾
For years, my **bill** was never above $350/month on my single AWS instance. ... to find public keys for servers on GitHub and **took control of** the **AWS account**.

Spending 100K USD in 4,5 days on Amazon Web Services | OlinData
https://www.olindata.com/en/blog/.../spending-100k-usd-45-days-amazon-web-servic... ▾
Apr 25, 2017 - Spending 100K USD in 4,5 days **on** Amazon Web Services ... I created a separate **AWS account** for this and hooked it up to consolidated **billing on** our main ... Some more applicants **took** the assessment and **on** April 14th at ...

I was billed for 14k USD on Amazon Web Services - DEV Community ...
https://dev.to/.../i-was-billed-for-14k-usd-on-amazon-web-services-17fn ▾
Jul 3, 2018 - I was billed for 14k USD **on Amazon Web Services** ... My monthly **bill** is about 1 USD. Yep, that's almost nothing, but ... **Take** a look at your email frequently and don't **take** a single email as a mistake ..... If your **account** was **hacked**, even the spending limit (which **AWS** does not have) system would not work.



Billing & Cost Management Dashboard

What's New in AWS Billing and Cost Management?

- Manage your spend with AWS Budgets
- Visualize your costs and usage with the newly-optimized Cost Explorer
- Easily upload your Cost and Usage Reports into Redshift and QuickSight

Spend Summary

Welcome to the AWS Account Billing console. Your last month, month-to-date, and month-end forecasted costs appear below.

Current month-to-date balance for April 2017

$91,348.00

▸ Important Information about these Costs

☑ Include Subscription Charges

Alerts & Notifications

Your account is enabled for AWS Budgets. Set your first budget to monitor when actual or forecasted charges reach a threshold you define.

HoneyPot

- The first public honeypot was Fred Cohen's Deception ToolKit in 1998
  - "intended to make it appear to attackers as if the system running DTK [which had] a large number of widely known vulnerabilities“
- Decreased number of false positives
- Requires less data collection
- Great way to create actionable high fiddley alerts
- Canned Example: Open Canary
- DIY Example: HoneyBucket

CANARY

Think Detection

- If you only use cloud resources in the U.S., setup alerts on any resources used in non-U.S. regions
- Use inventory control and tag cloud resources
- If your monthly bill averages $3k, set a billing alarm for $3.3k
- If 10 failed logins is normal for your users, set alerts from failed logins sourcing from different IP addresses / late at night / quick intervals
- If your cloud usage is the wild west of security, implement cyber deceptive
  - HoneyTokens
  - HoneyBuckets
  - HoneyUsers

RICHEY MAY Technology Solutions

Thank You

linkedin.com/in/mwylie

twitter.com/TheMikeWylie

Michael@RicheyMay.com
www.RicheyMayTech.com