NextStep HealthTech Cybersecurity Hardening

Paul Ackels, James Buchholz
Department of Computer Science (ISE), University of New Hampshire

Introduction

NextStep HealthTech is a technology company that is dedicated to the improvement of public health.

We identified an opportunity to help the development team bolster its cybersecurity protocols, and through brainstorming and research we identified multiple opportunities to better secure NextStep's data.

Our work this year has bolstered NextStep's cybersecurity protocols against attacks, data loss, billing abnormalities.

Objectives

1a. Determine a performance baseline and create fitting alarms

1b. Connect an automated 'bot' for NextStep's internal communications software to the alarms so that NextStep employees are alerted

2. Create recurring backups to make NextStep's data safe

3. Maintain and improve cybersecurity protocols

Contacts

Paul Ackels – paul.ackels@unh.edu

James Buchholz – jrb1099@wildcats.unh.edu

Methods

1a. Created CPU usage alarms for all running Cloud Server instances, to check for abnormal activity

1b. Connected alarms to NextStep's internal communications software, alerting the development team

2. Created a recurring backup schedule for NextStep's Cloud Server Databases

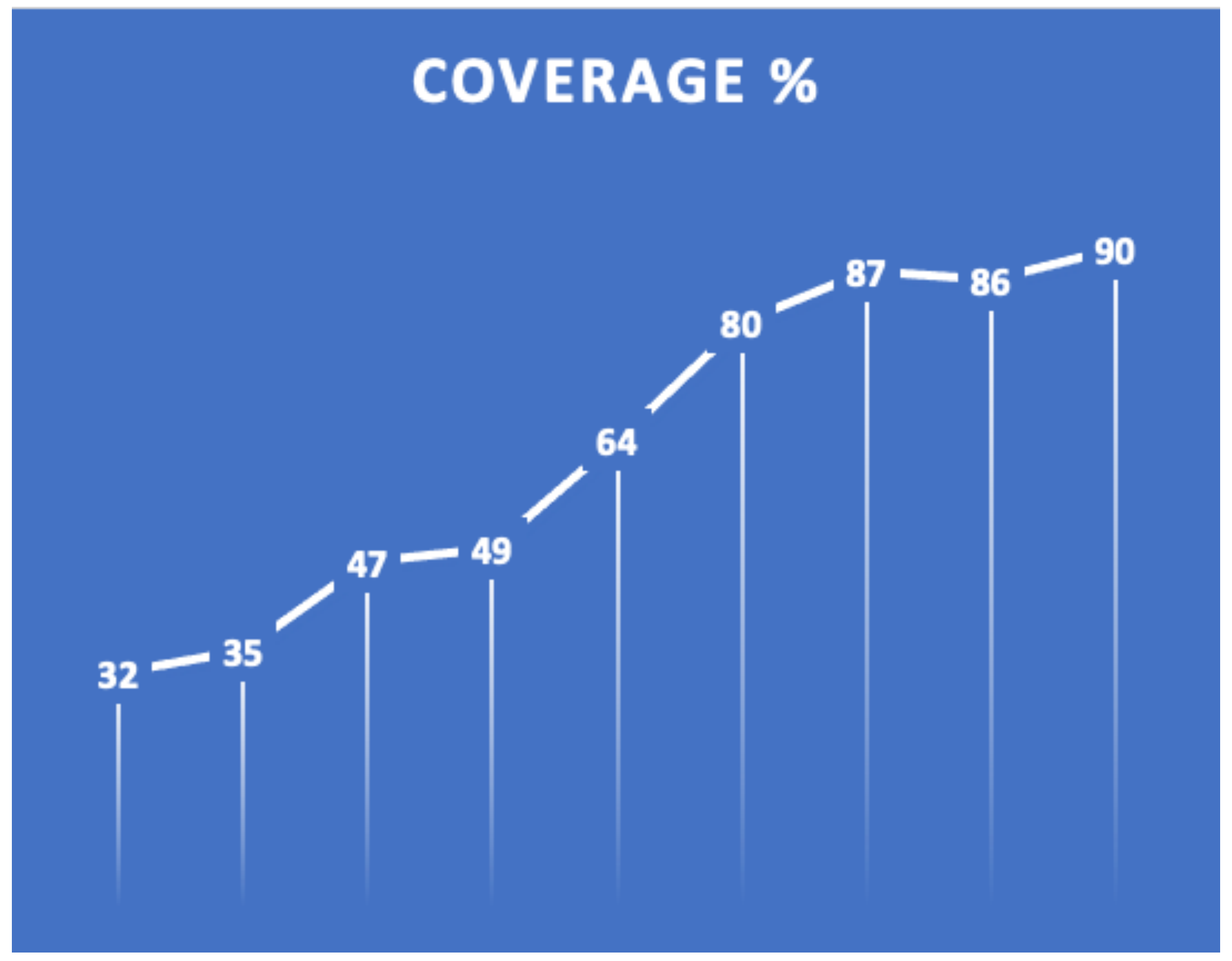
2. Created recurring backups template for Cloud Storage Buckets

3. Utilized Open-Source Security Audit Script (OSSAS) to assess and benchmark cybersecurity protocols

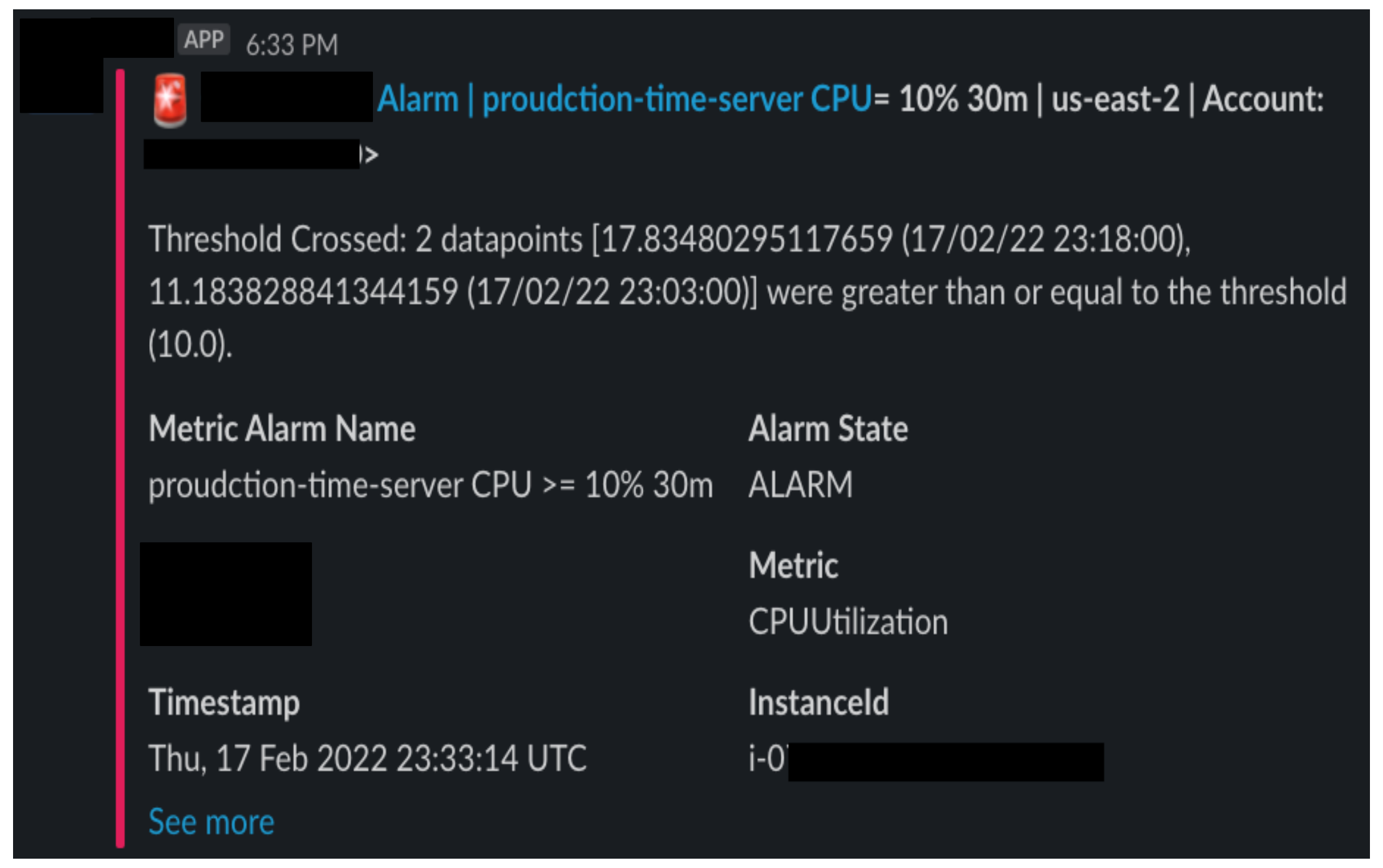
Cybersecurity Protocols

- Accounts
  - MFA: authenticating access using multiple pieces of evidence
  - Password policy: using set guidelines for stronger passwords
  - Account access keys: long-term credentials for specific account accesses
- Encryption
  - Encrypted storage volumes
  - Non-public storage: blocking public access to objects/buckets
  - Key management systems: encrypts and manages access keys
- Logging
  - Adequate logging for storage and accounts
- Alarms
  - Receiving notifications when metrics fall outside of a high or low threshold

Open-Source Security Audit Script (OSSAS) Coverage Over Time



Example of Internal Automated Communications Alarm Notification



[redacted] APP 6:33 PM

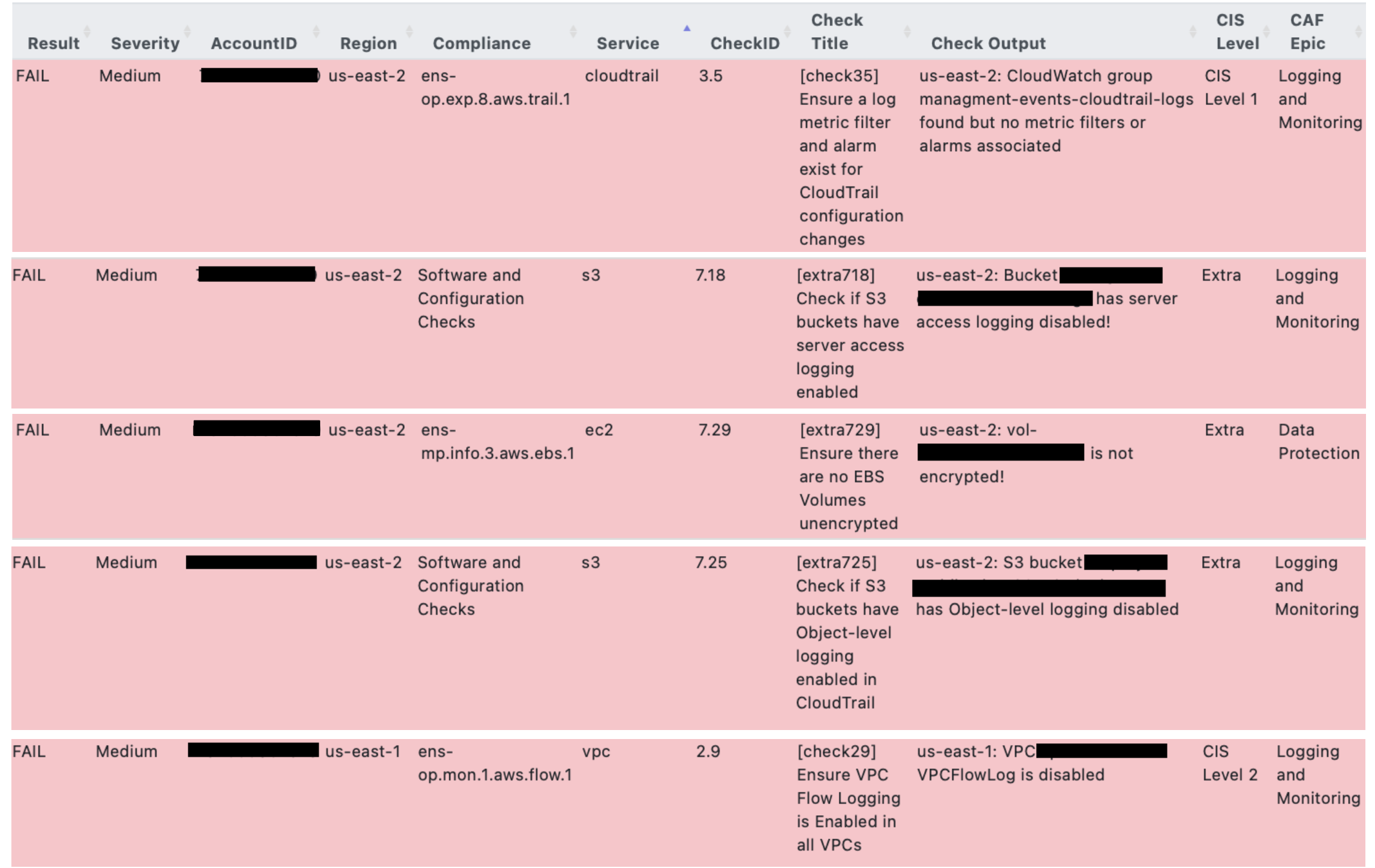
[redacted] Alarm | proudction-time-server CPU= 10% 30m | us-east-2 | Account: [redacted]>

Threshold Crossed: 2 datapoints [17.83480295117659 (17/02/22 23:18:00), 11.183828841344159 (17/02/22 23:03:00)] were greater than or equal to the threshold (10.0).

Metric Alarm Name	Alarm State
proudction-time-server CPU >= 10% 30m	ALARM
[redacted]	Metric CPUUtilization
Timestamp Thu, 17 Feb 2022 23:33:14 UTC	InstanceId i-0[redacted]

See more

Example of Now Fixed OSSAS Outputs



Result	Severity	AccountID	Region	Compliance	Service	CheckID	Check Title	Check Output	CIS Level	CAF Epic
FAIL	Medium	[redacted]	us-east-2	ens-op.exp.8.aws.trail.1	cloudtrail	3.5	[check35] Ensure a log metric filter and alarm exist for CloudTrail configuration changes	us-east-2: CloudWatch group managment-events-cloudtrail-logs found but no metric filters or alarms associated	CIS Level 1	Logging and Monitoring
FAIL	Medium	[redacted]	us-east-2	Software and Configuration Checks	s3	7.18	[extra718] Check if S3 buckets have server access logging enabled	us-east-2: Bucket [redacted] has server access logging disabled!	Extra	Logging and Monitoring
FAIL	Medium	[redacted]	us-east-2	ens-mp.info.3.aws.ebs.1	ec2	7.29	[extra729] Ensure there are no EBS Volumes unencrypted	us-east-2: vol-[redacted] is not encrypted!	Extra	Data Protection
FAIL	Medium	[redacted]	us-east-2	Software and Configuration Checks	s3	7.25	[extra725] Check if S3 buckets have Object-level logging enabled in CloudTrail	us-east-2: S3 bucket [redacted] has Object-level logging disabled	Extra	Logging and Monitoring
FAIL	Medium	[redacted]	us-east-1	ens-op.mon.1.aws.flow.1	vpc	2.9	[check29] Ensure VPC Flow Logging is Enabled in all VPCs	us-east-1: VPC [redacted] VPCFlowLog is disabled	CIS Level 2	Logging and Monitoring

Conclusions

1a. Implemented over 45 performance and billing alarms

1b. Connected all alarms to the NextStep's internal communications software

2. Created a recurring backup for Cloud Server databases, and a template for Cloud Data Storage backups

3. Bolstered NextStep's cybersecurity protocols by 60%

NextStep is in a much more secure state than it was because of the many steps we have taken to protect them

Next Steps

- Get OSASS results to 100% and create a pipeline to automate the script and send results via NextStep's internal communications channel
- Create new alarms with new instances and add to spreadsheet
- Use the incident response plan draft to create a final version
- Implement a VPN within NextStep's Cloud Storage Environment so that employees can remote work safely

References

NextStep's Website:
- *https://www.nextstep.health*

OSASS GitHub:
- *https://bit.ly/35ZsAgW*