Very easy to enable Sysdig security and compliance tools on AWS and Containers running on ECS, Fargate and EKS.

1/ Workshop step by step guide - https://sysdig.awsworkshop.io/ very easy to follow

2/ Free Sysdig trail account sign up - https://sysdig.com/company/free-trial/?utm_campaign=aws-workshop (good for 1 month)

3/ Sysdig learning videos - https://learn.sysdig.com/series/secure-101

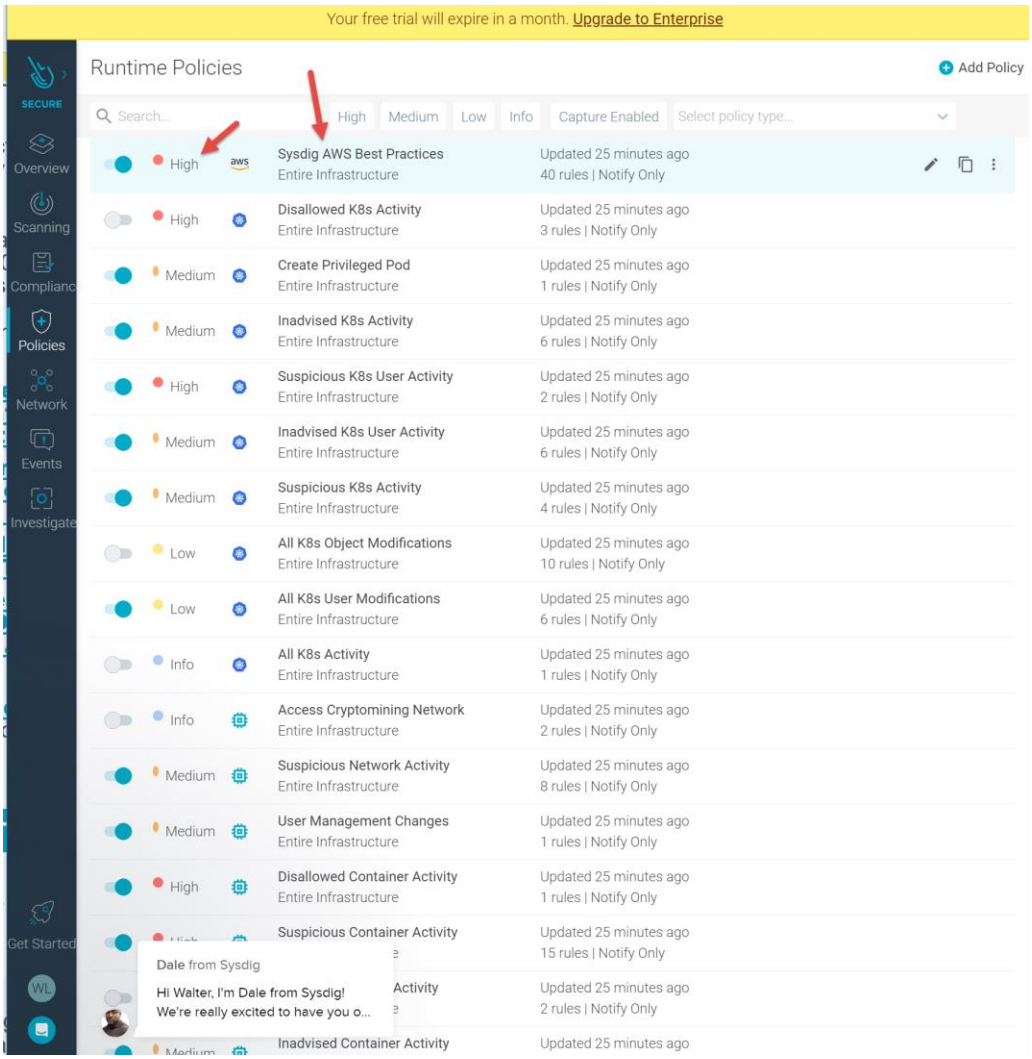
4/ Screen dumps of different features in the workshop as follows

---

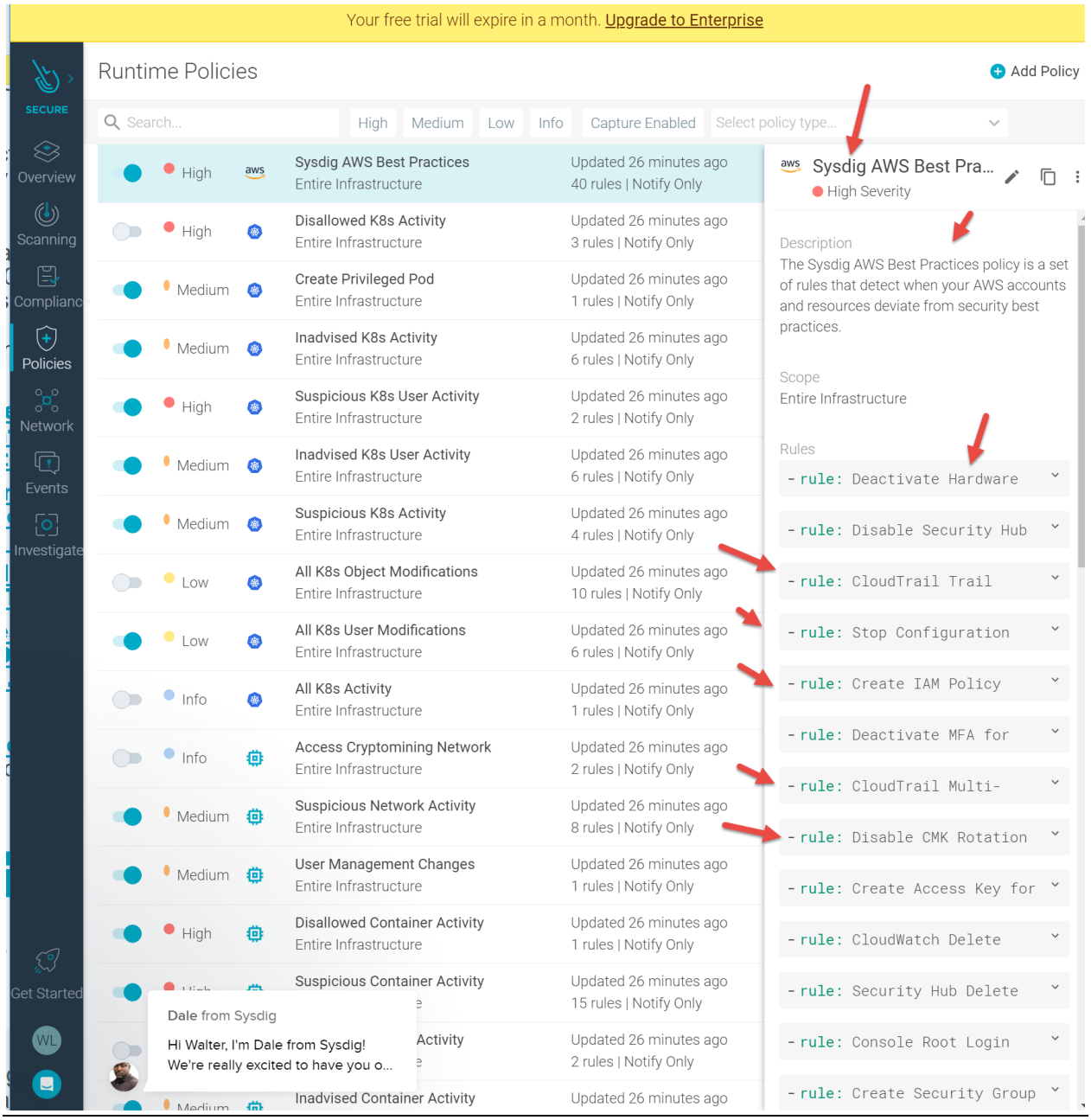
4.1/ easy to add Sysdig with their CF template at https://cf-templates-cloudvision-ci.s3-eu-west-1.amazonaws.com/latest/entry-point.yaml

Easy onboarding: https://us2.app.sysdig.com/secure/#/onboarding

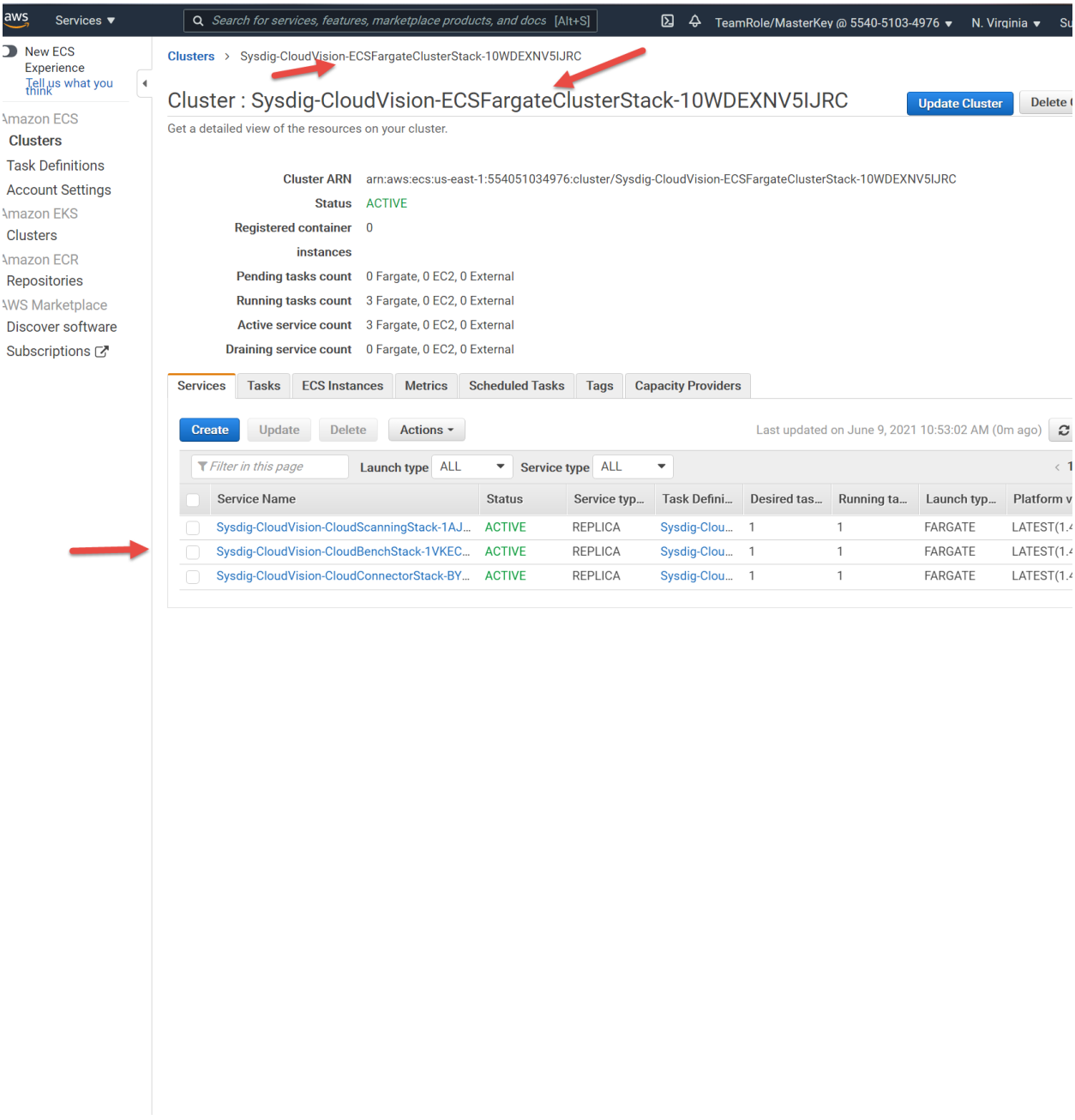
4.2/ default AWS best practices/policy:



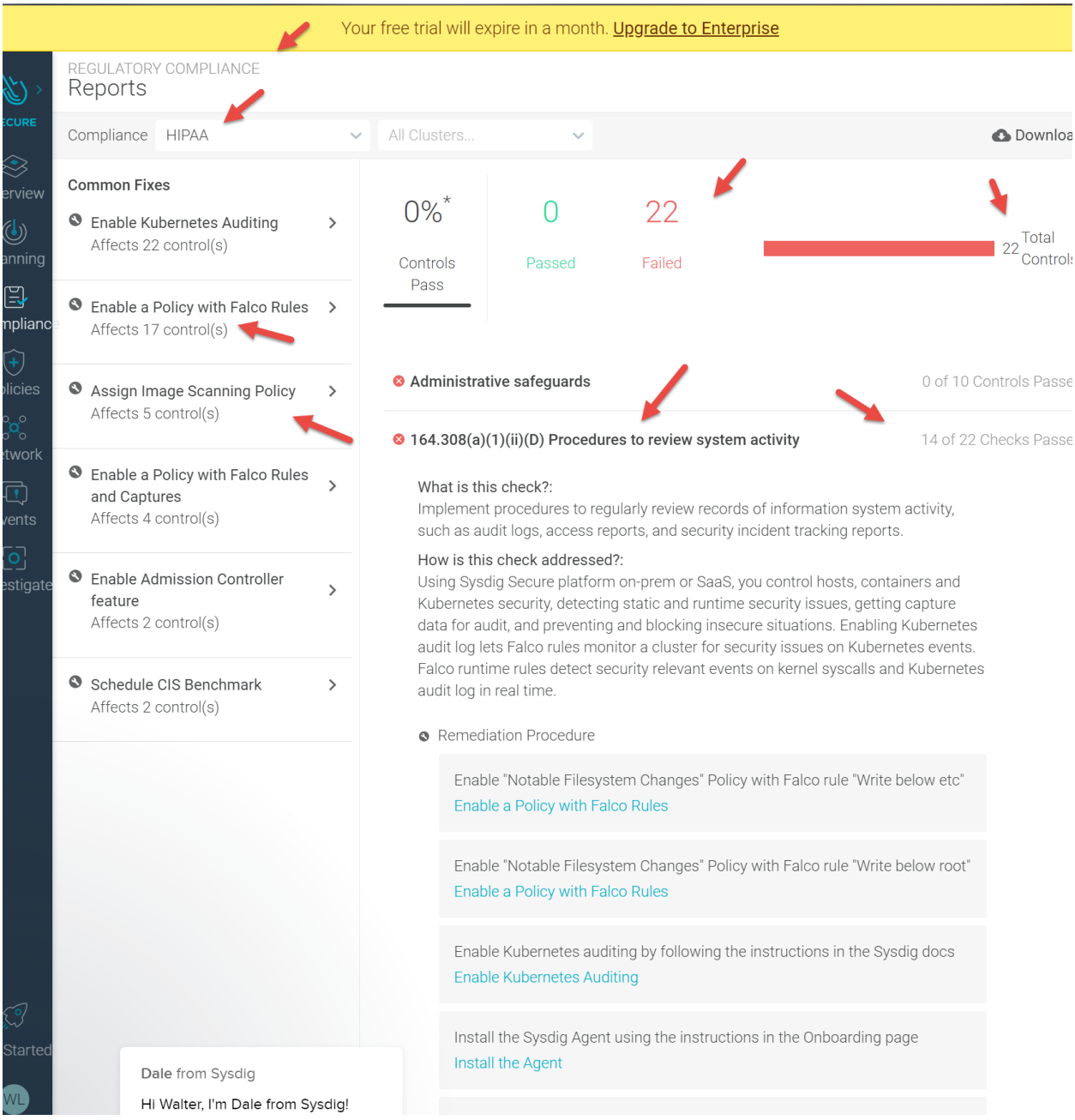
4.3/ many ready to use security rules in AWS policy:



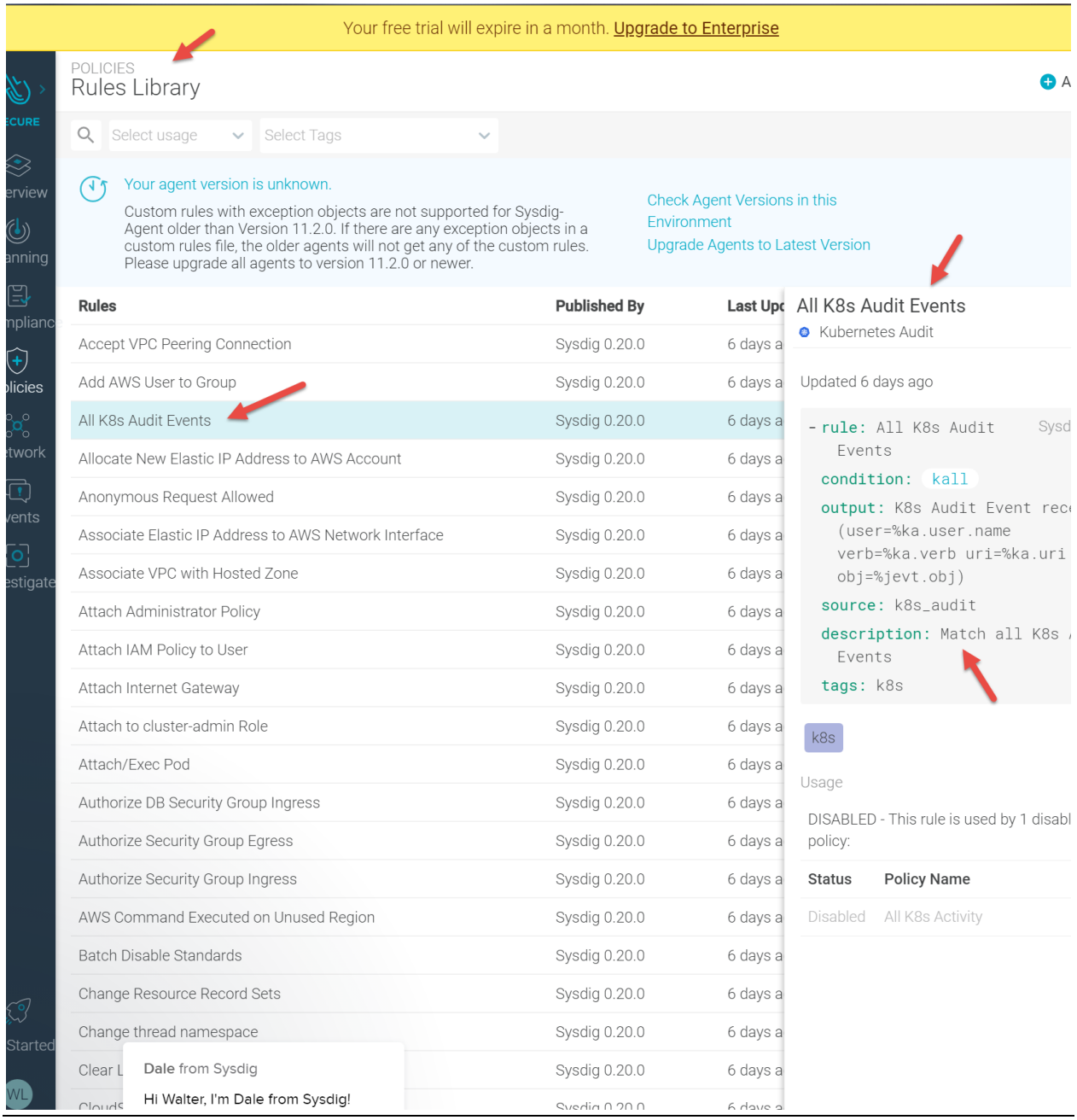
4.4/ easy to monitor with Sysdig scanning and others running as ECS Fargate tasks:



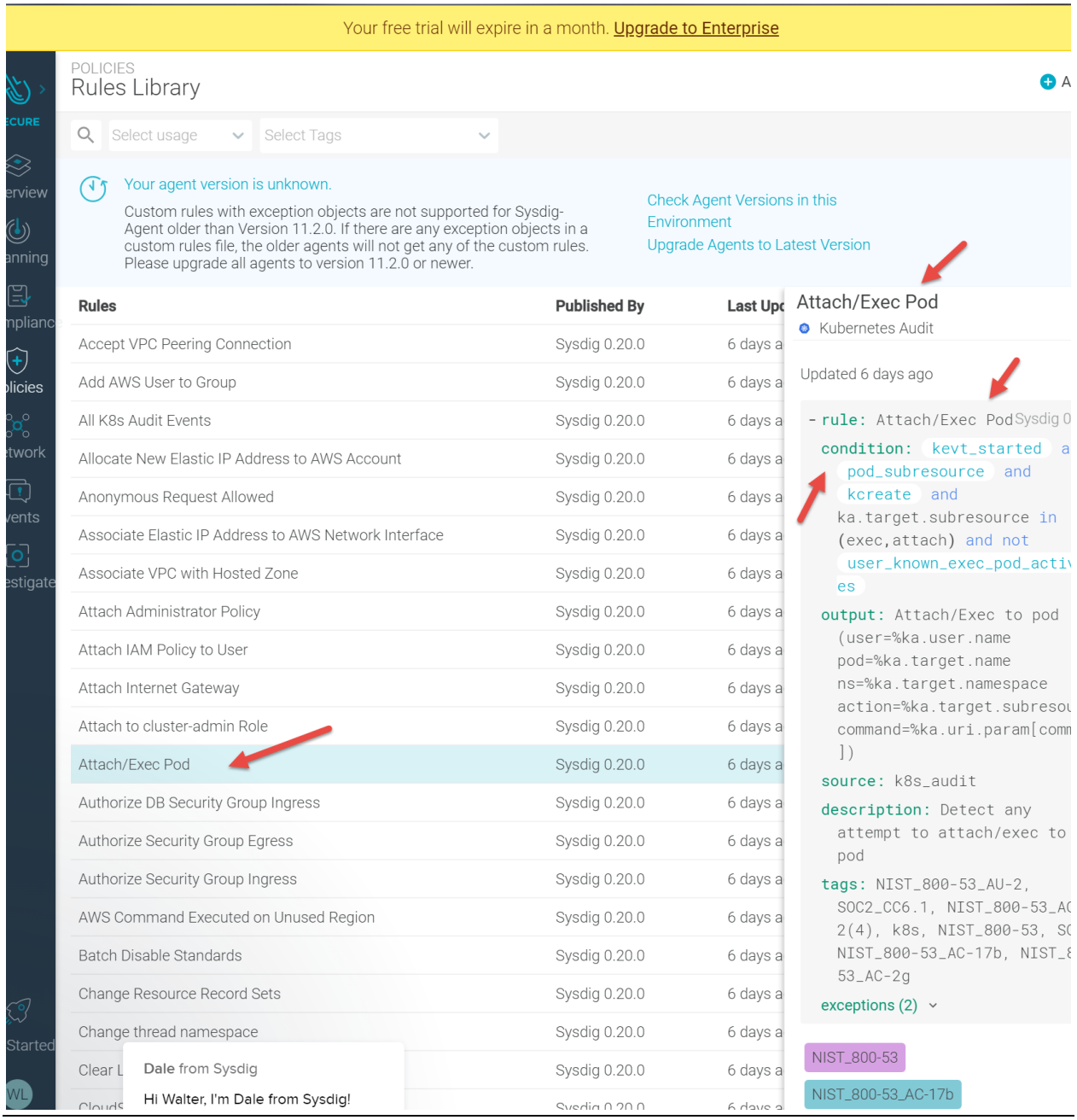
4.5/ Sysdig Secure Compliance report for HIPAA:



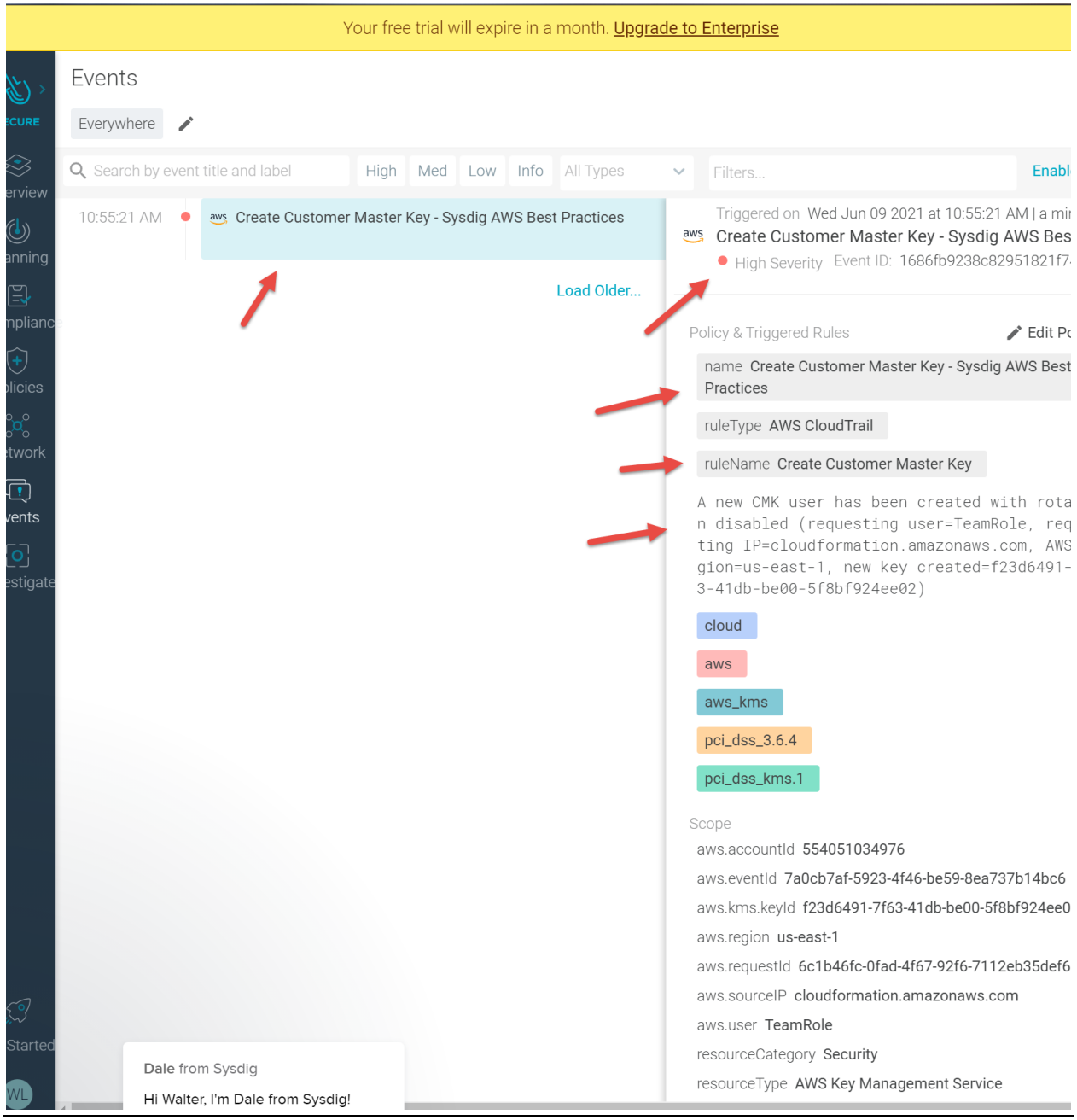
4.6/ Sysdig Secure sample rules, e.g. ALL k8s Audit events:



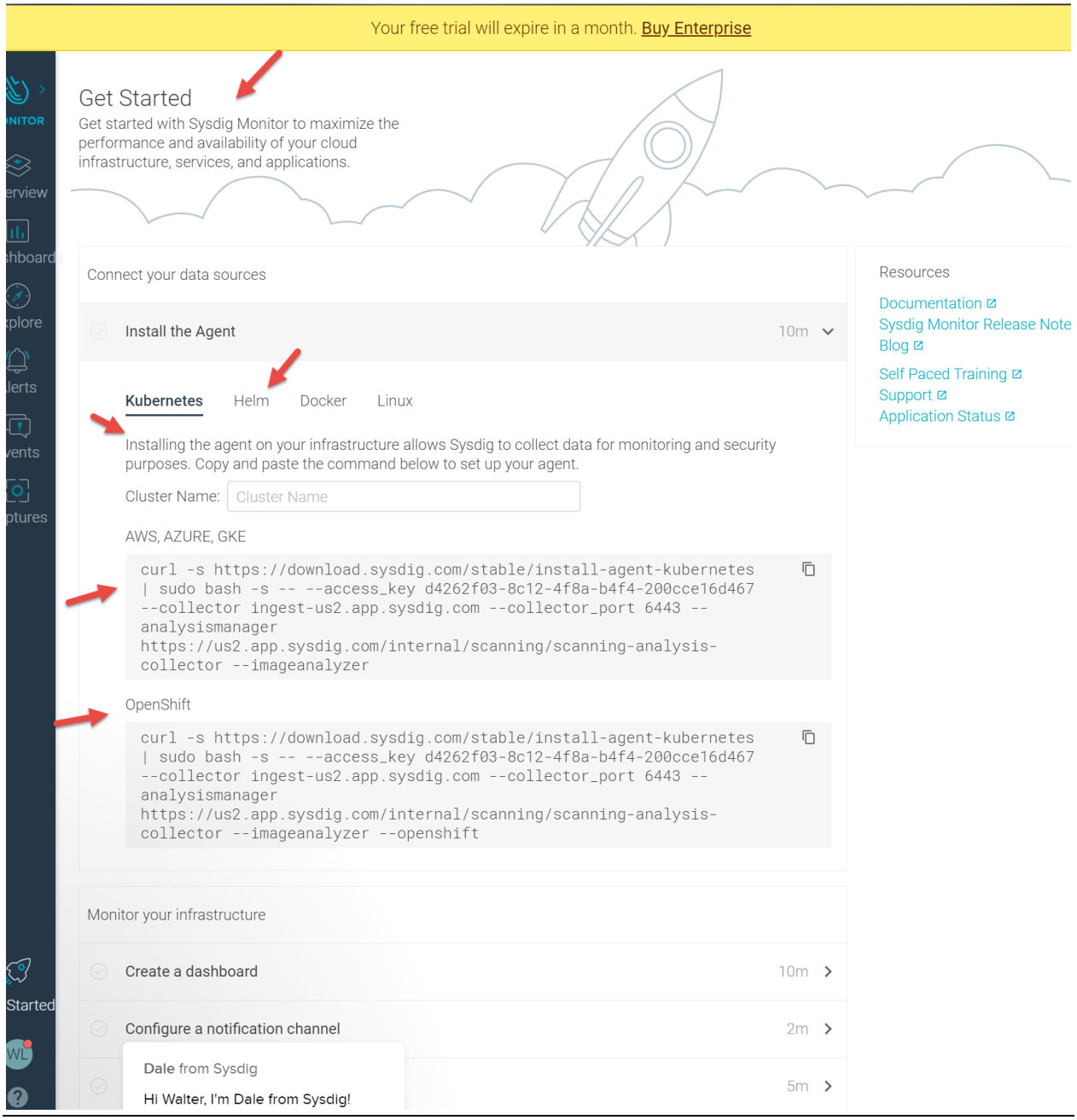
4.7/ Sysdig Secure sample rules, e.g. k8s audit attach/exec pods:



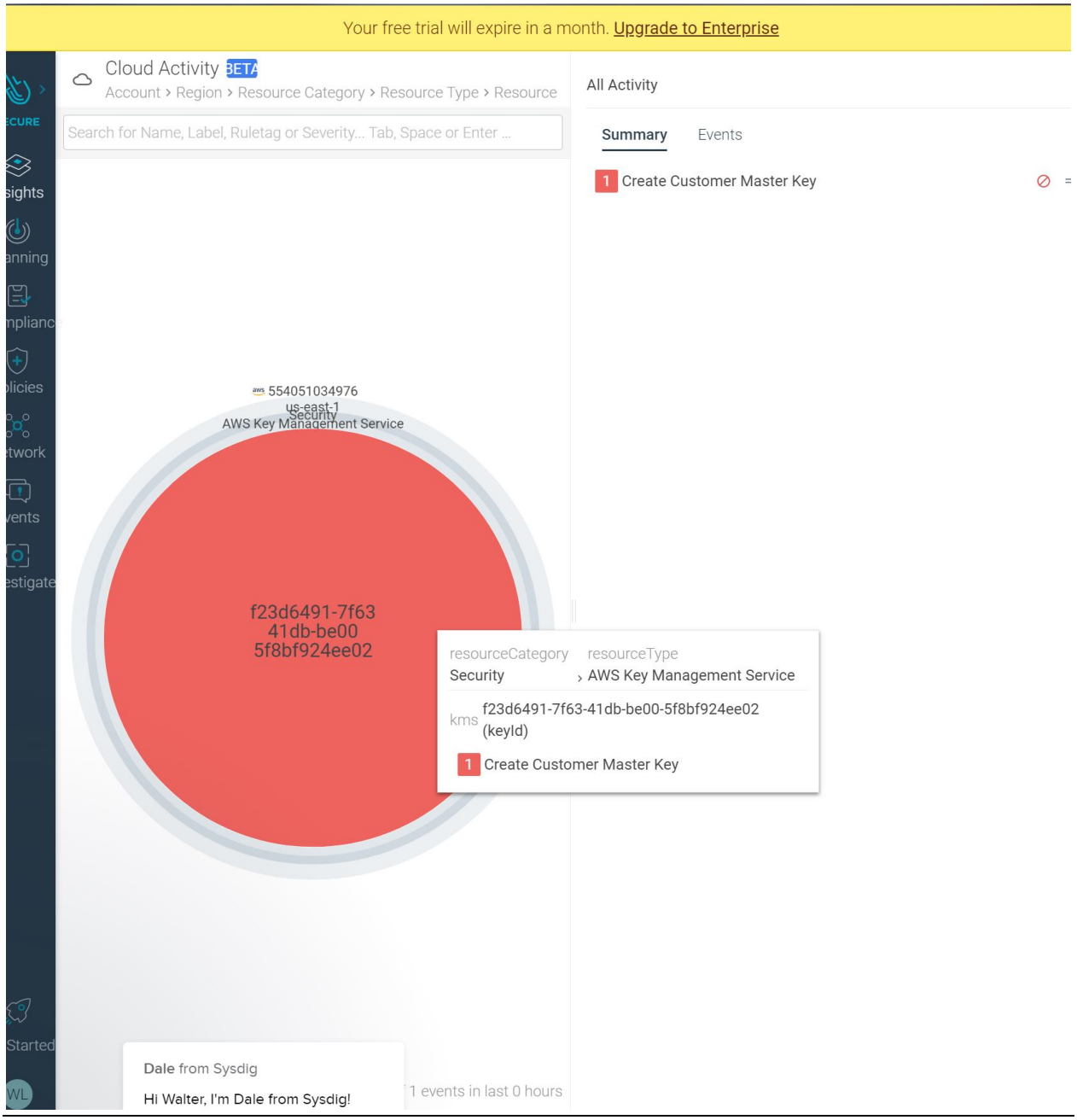
4.8/ sample Events when I create CMK with rotation disabled:



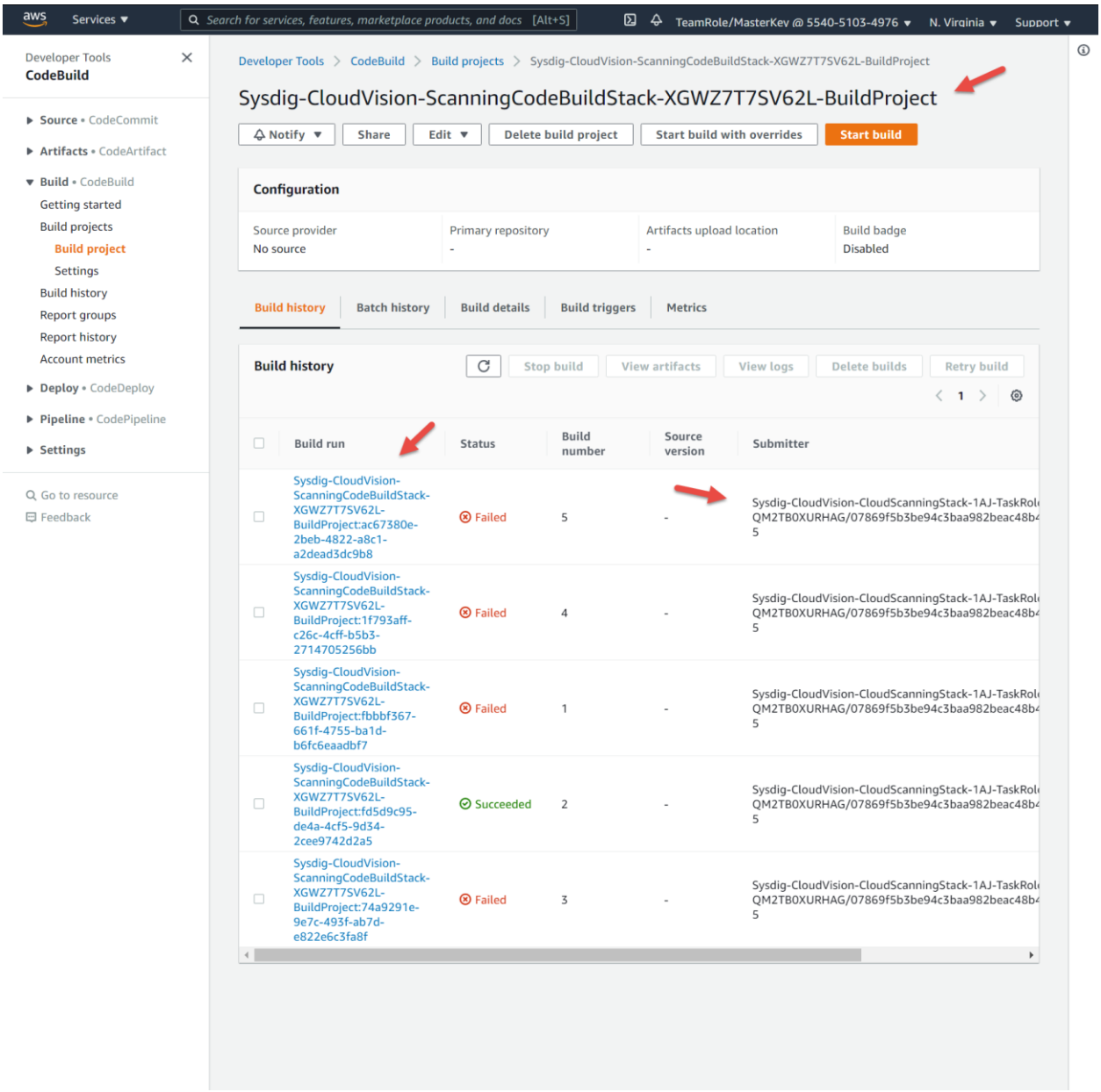
4.9/ Sysdig Monitor – get started with k8s easily:



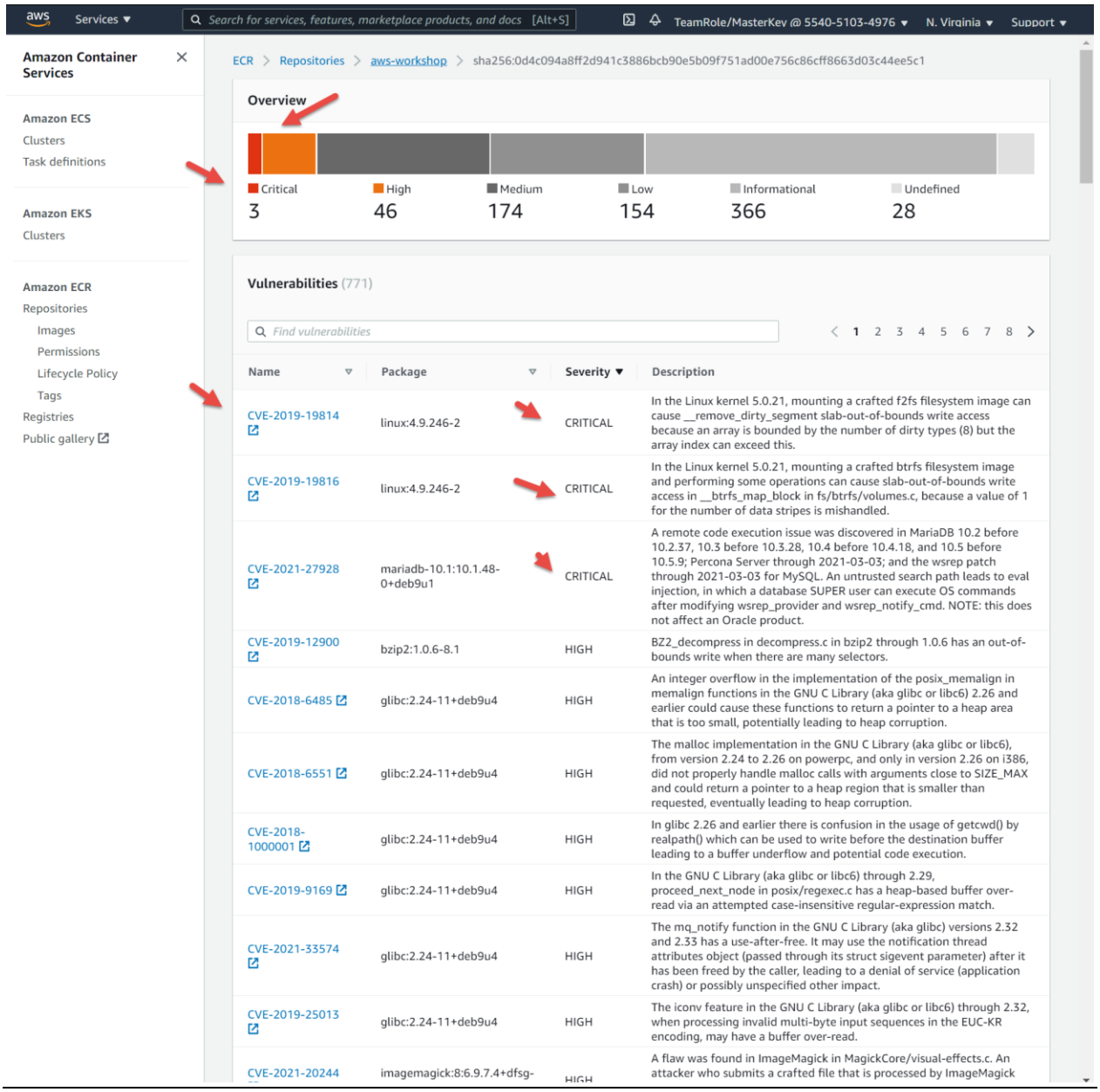
4.10/ Sample Cloud Activity/Event:



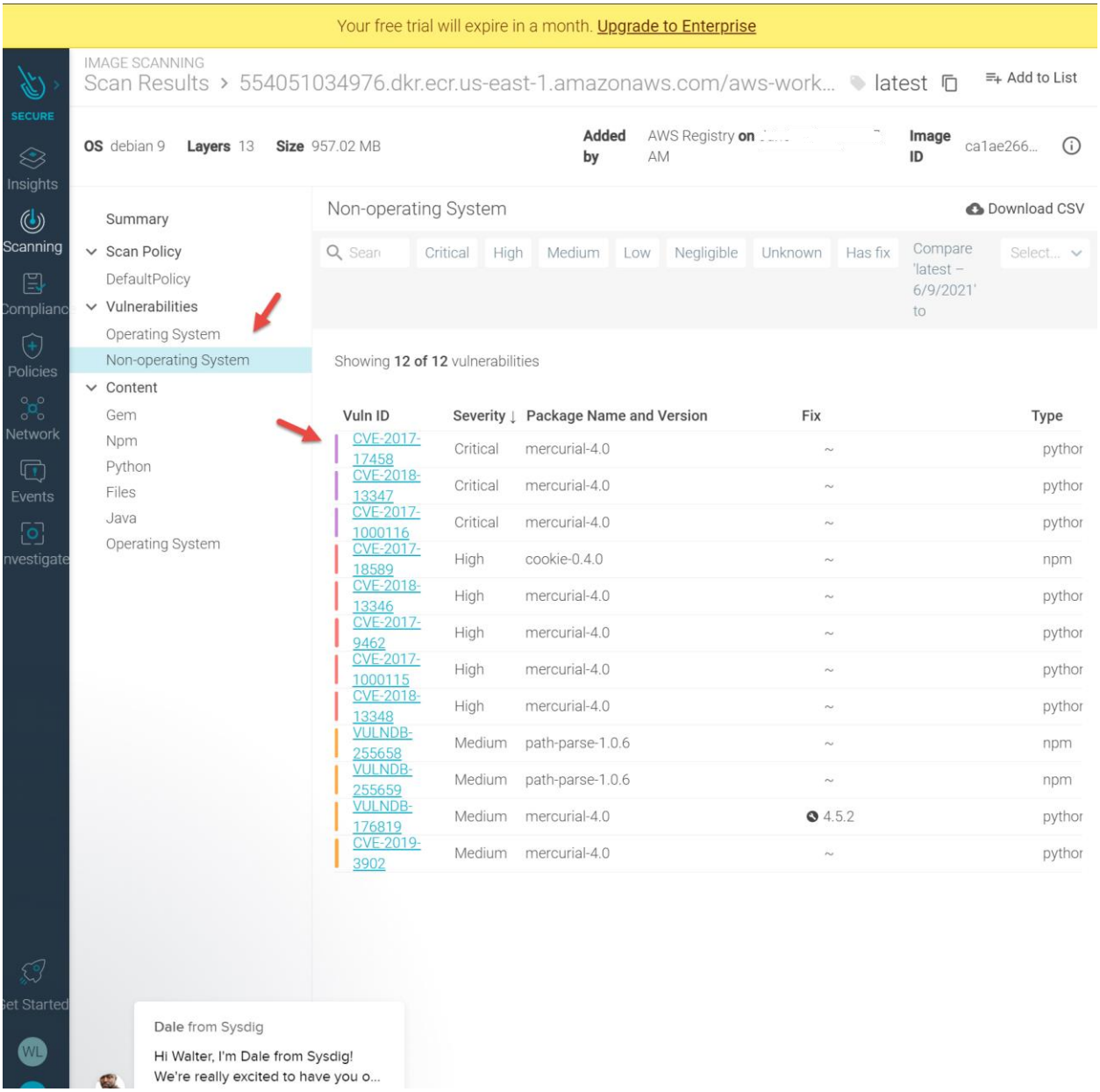
4.11/ Sample Codebuild failure when we got vulnerability in our docker build packages:



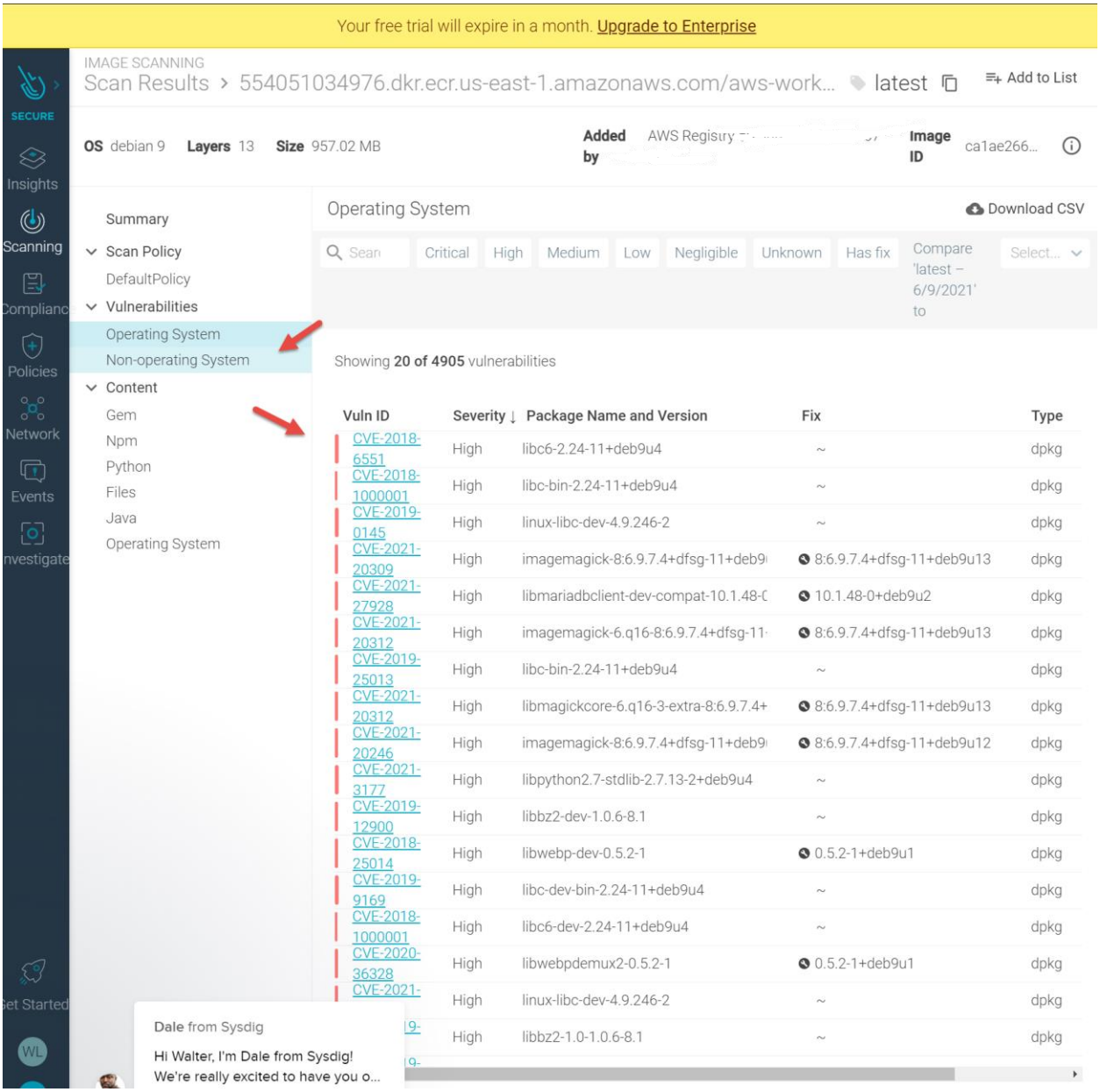
4.12/ ECR Vulnerabilities:



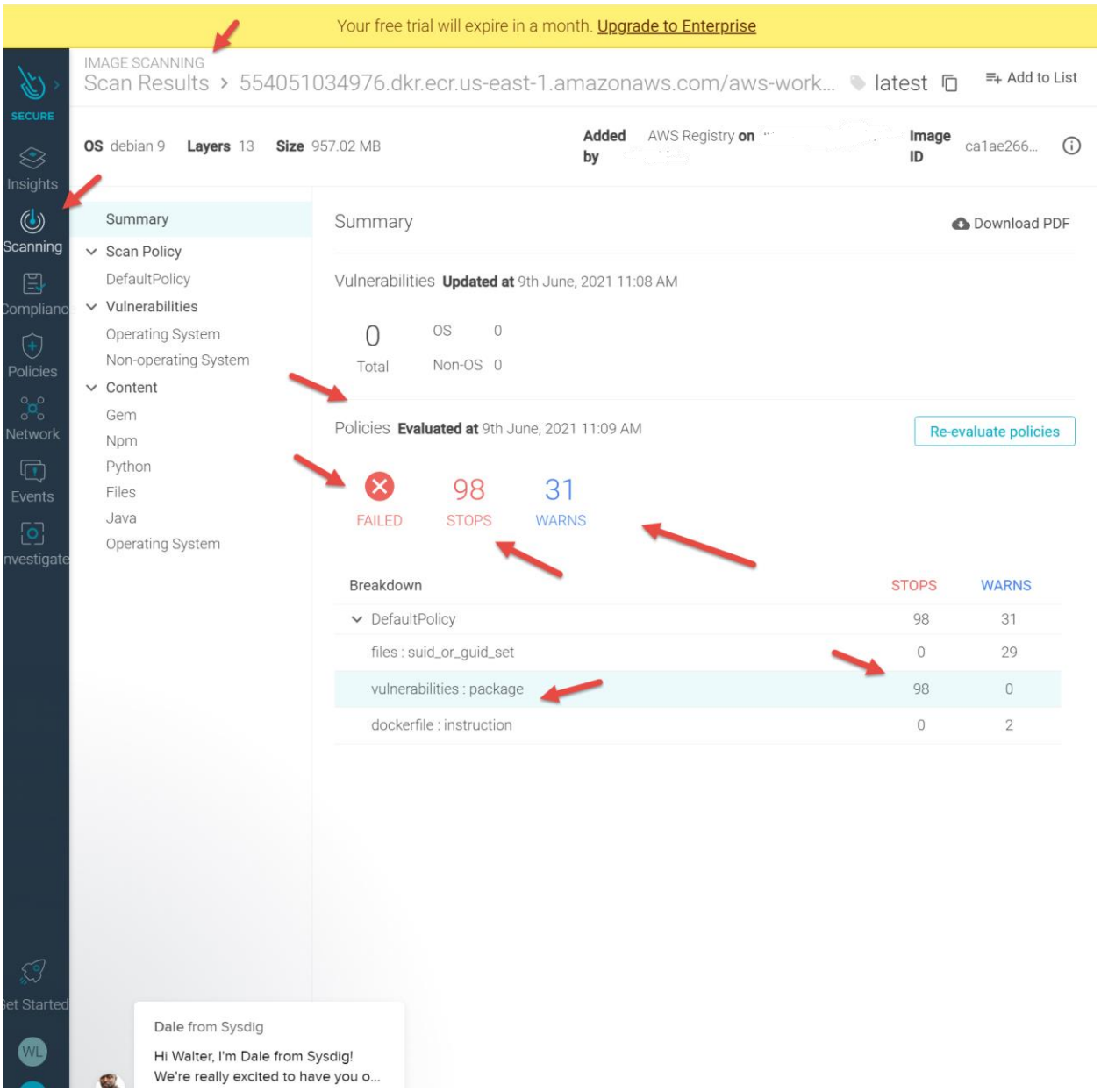
4.13/ show Vulnerabilities ID and fix (non-OS)



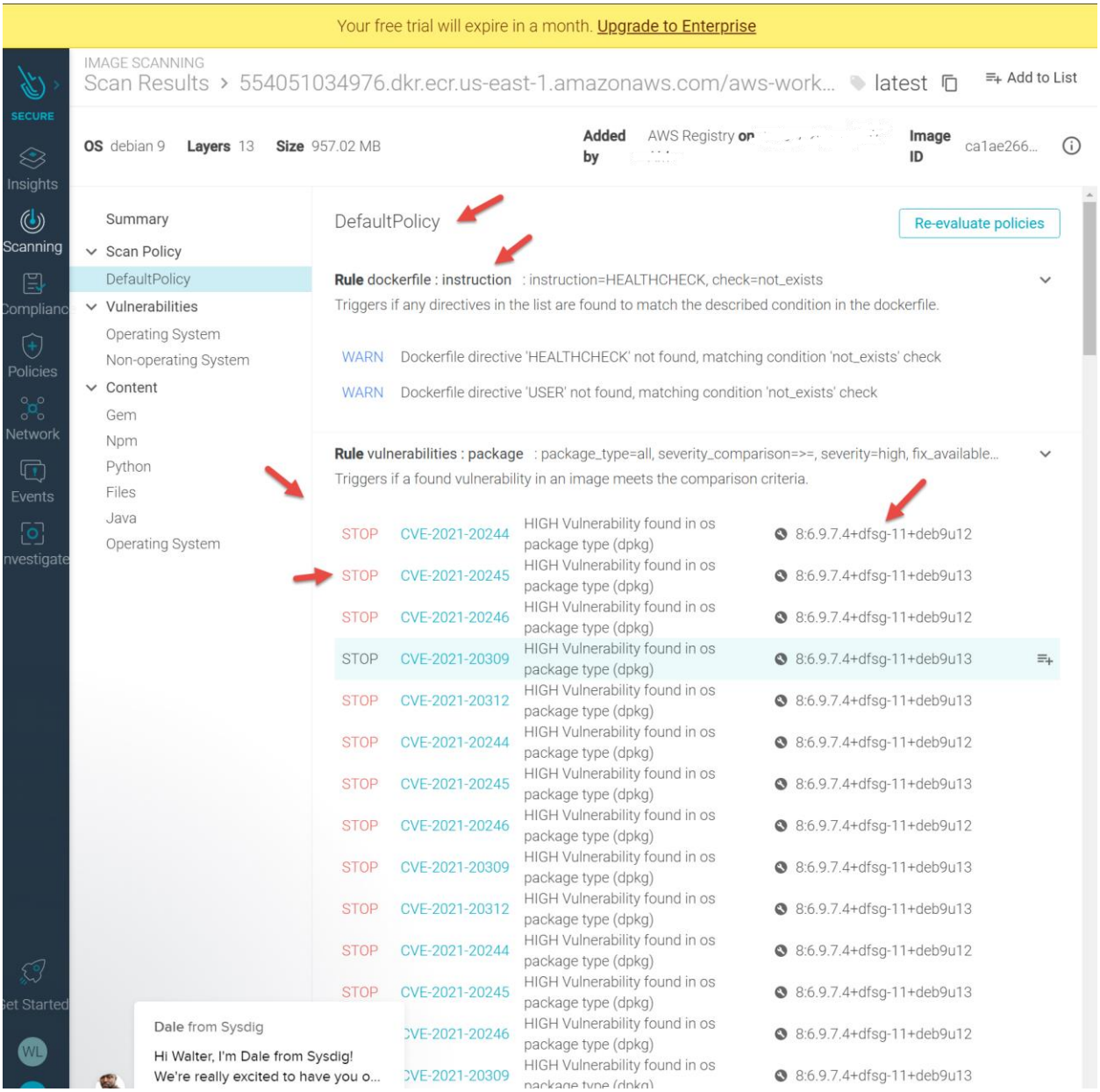
4.14/ show Vulnerabilities ID and fix (OS):



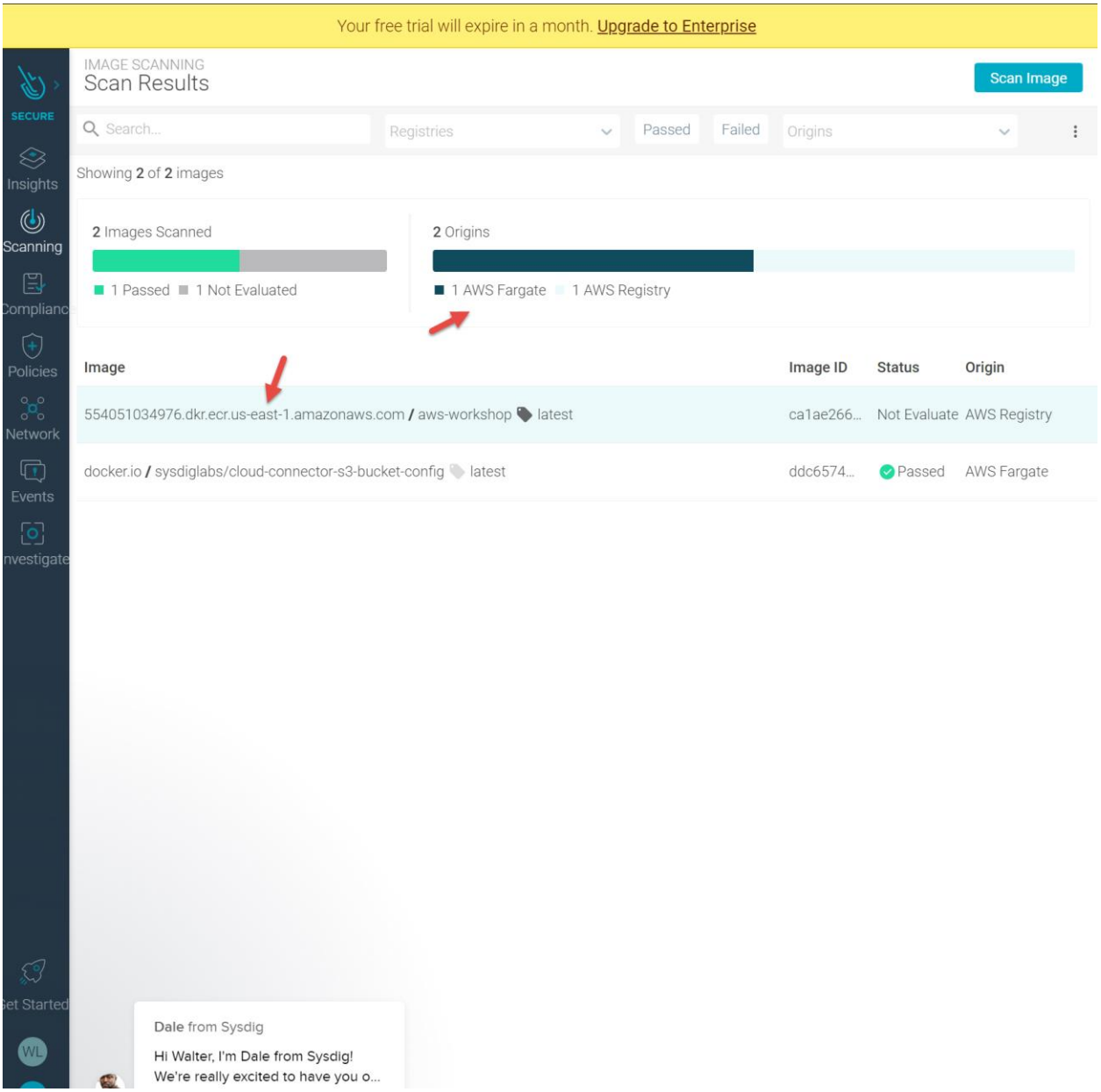
4.15/ Image scanning results:



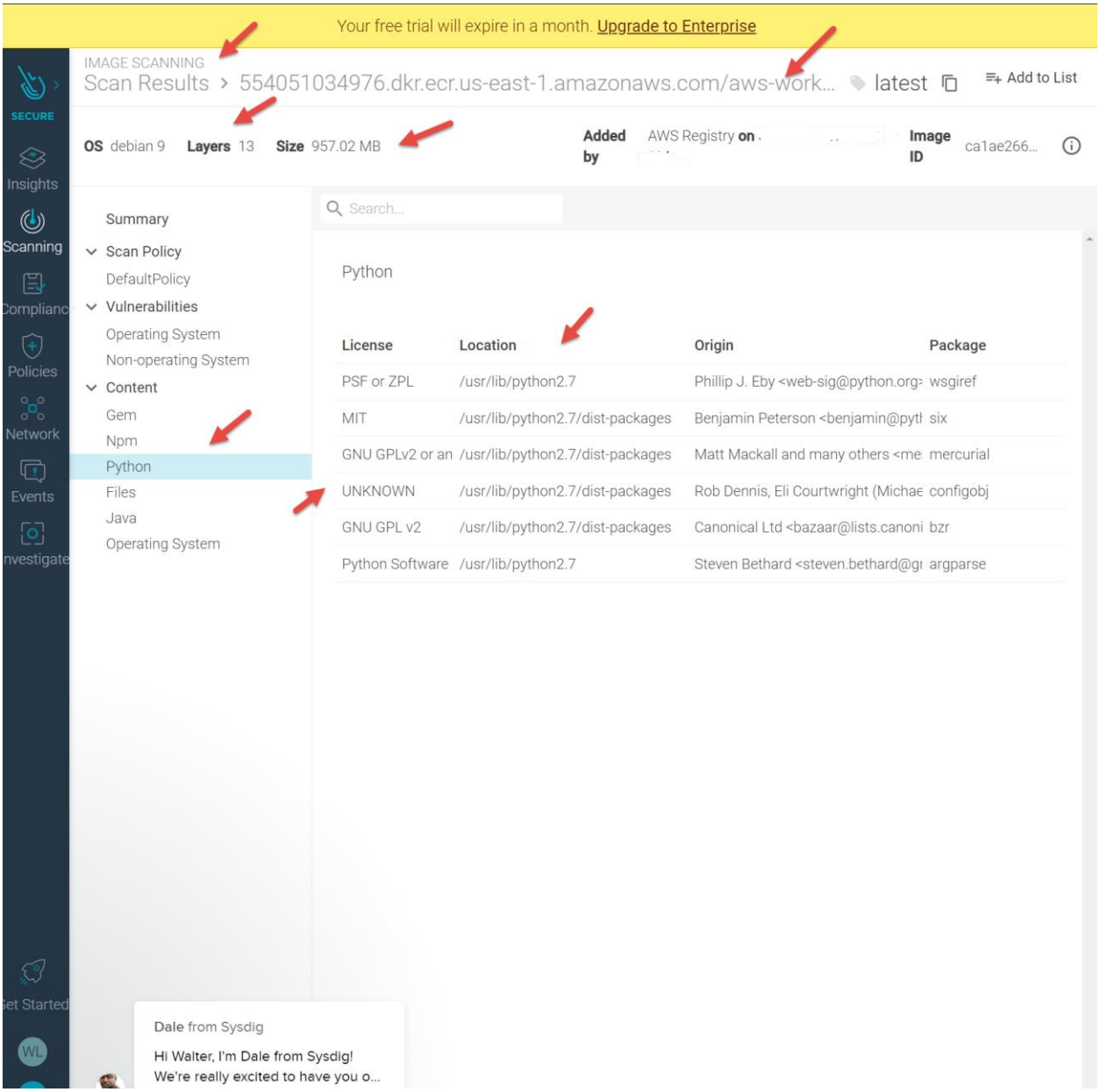
4.16/ Default Scan Policy Rule:



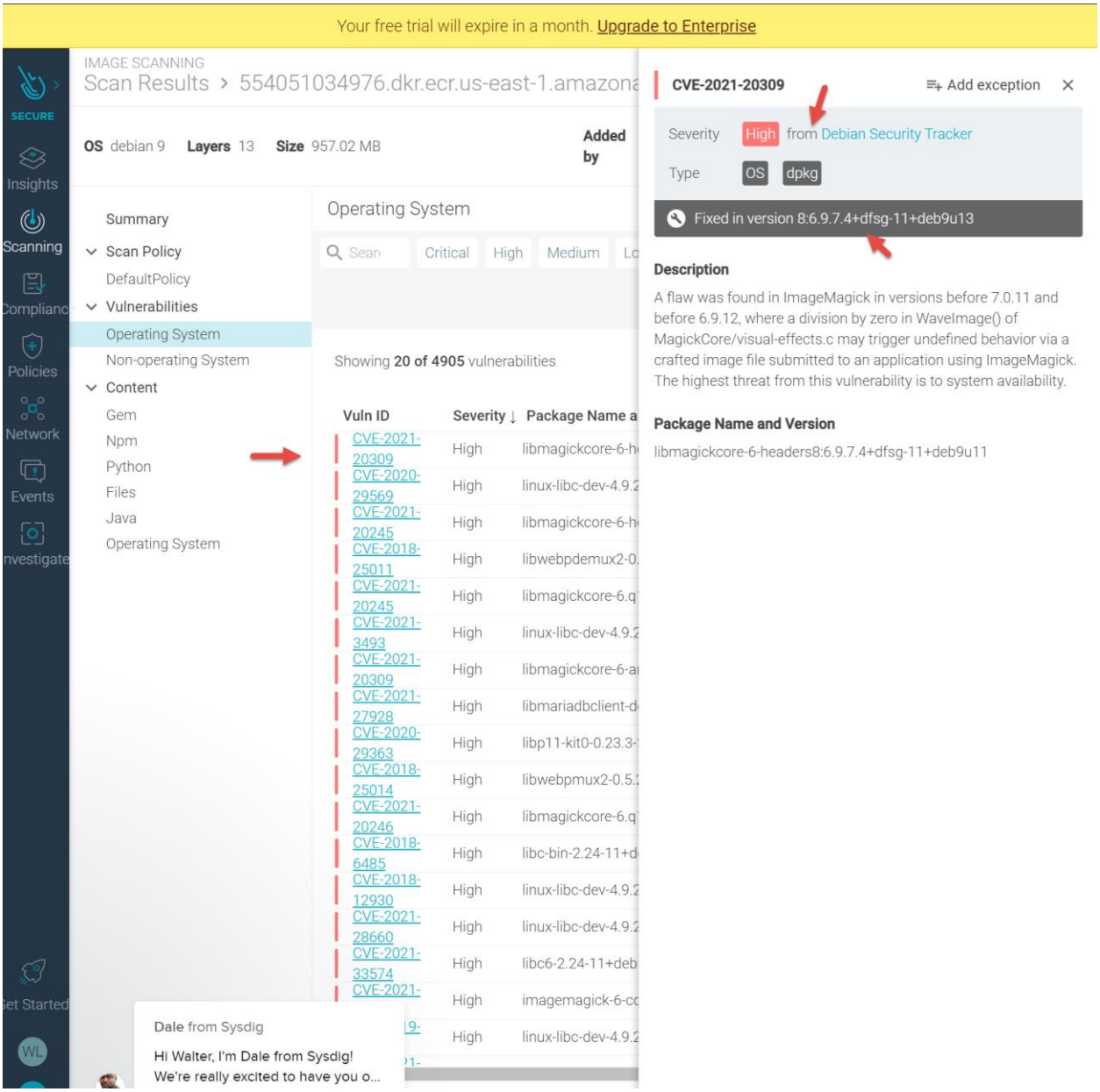
4.17/ Image scanning result for sample aws-workshop image:



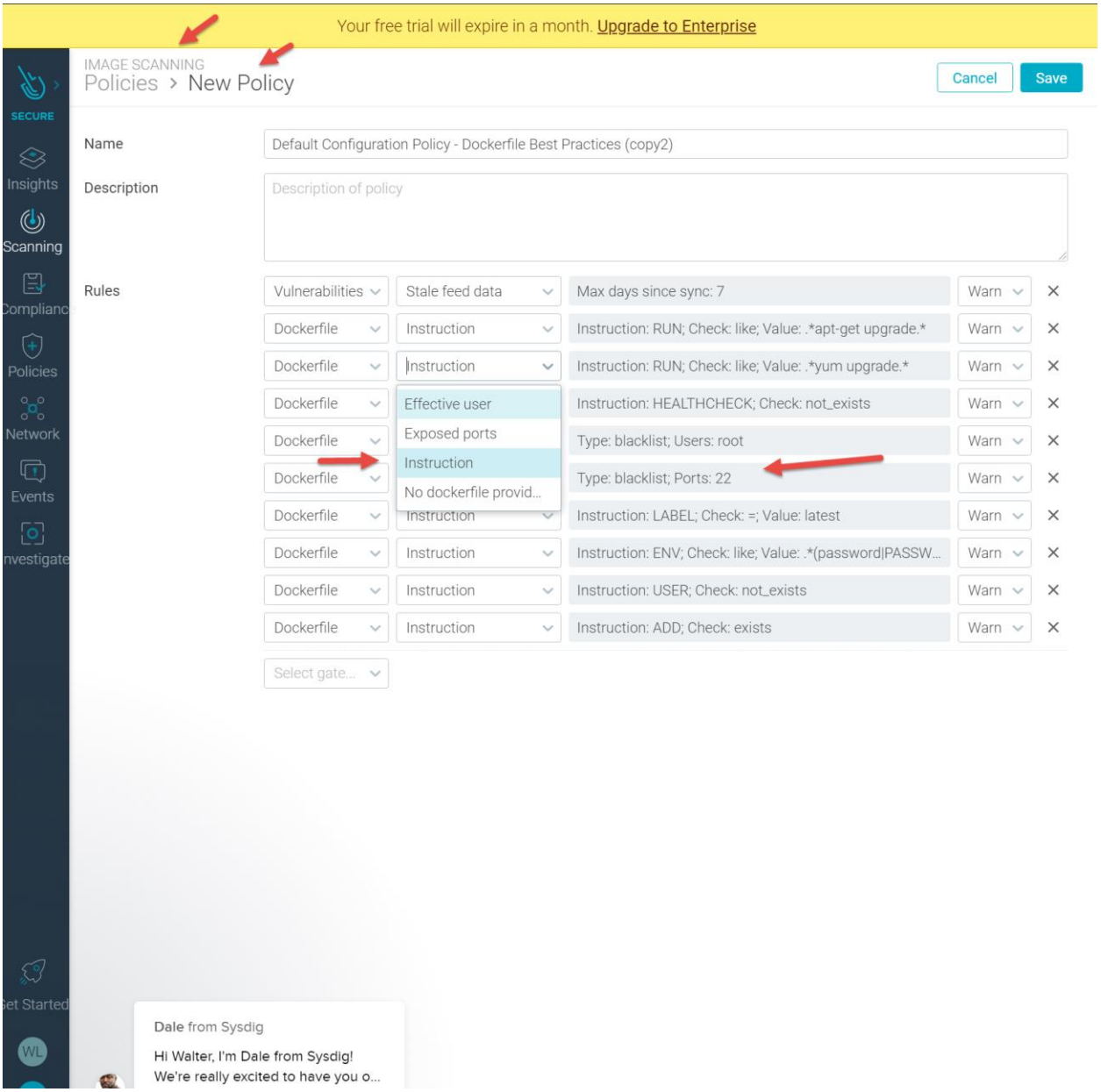
4.18/ Image scanning content:



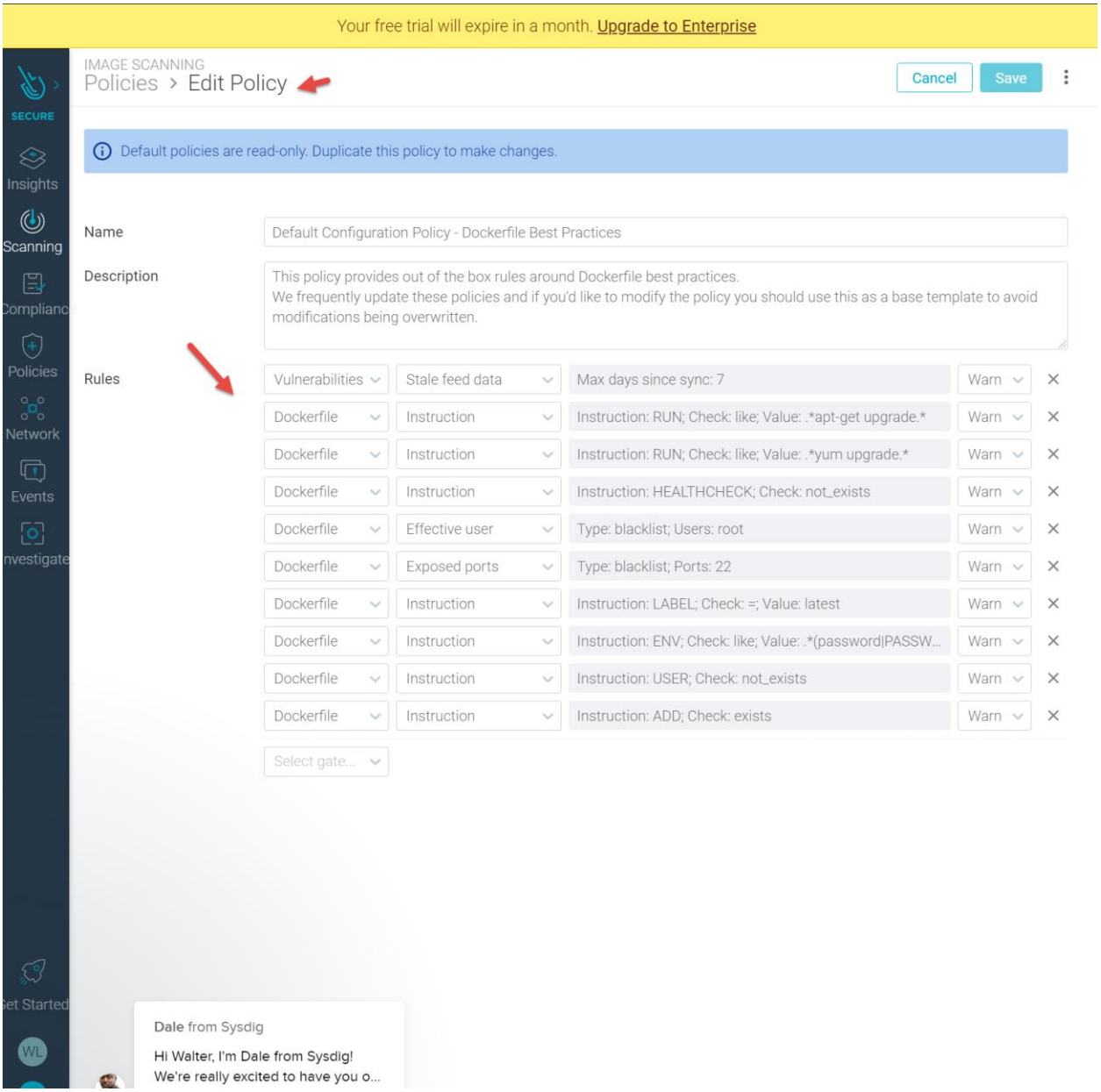
4.19/ Image scanning Vul. details:



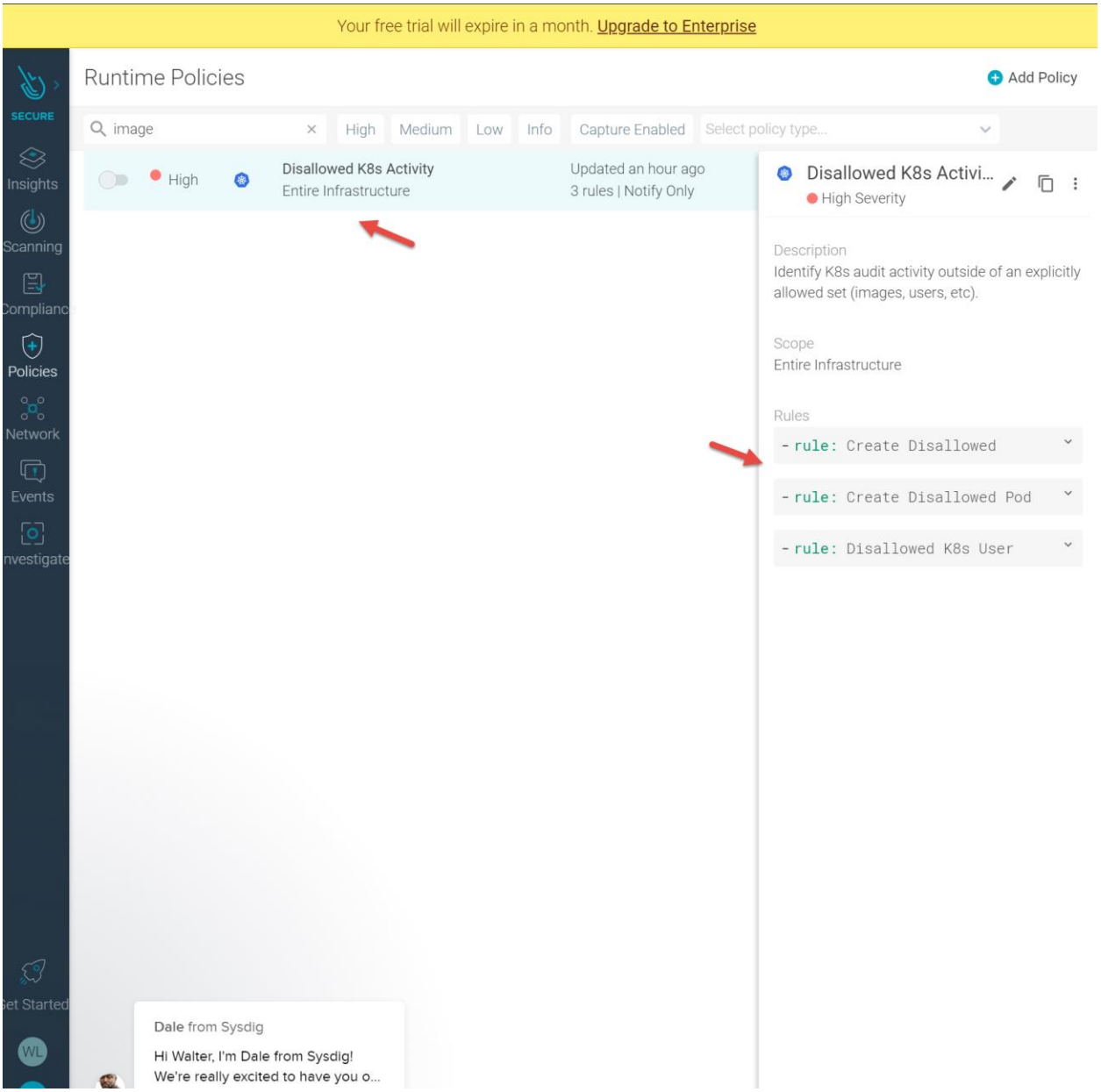
4.20/ easy to add custom image scanning rules/policies:



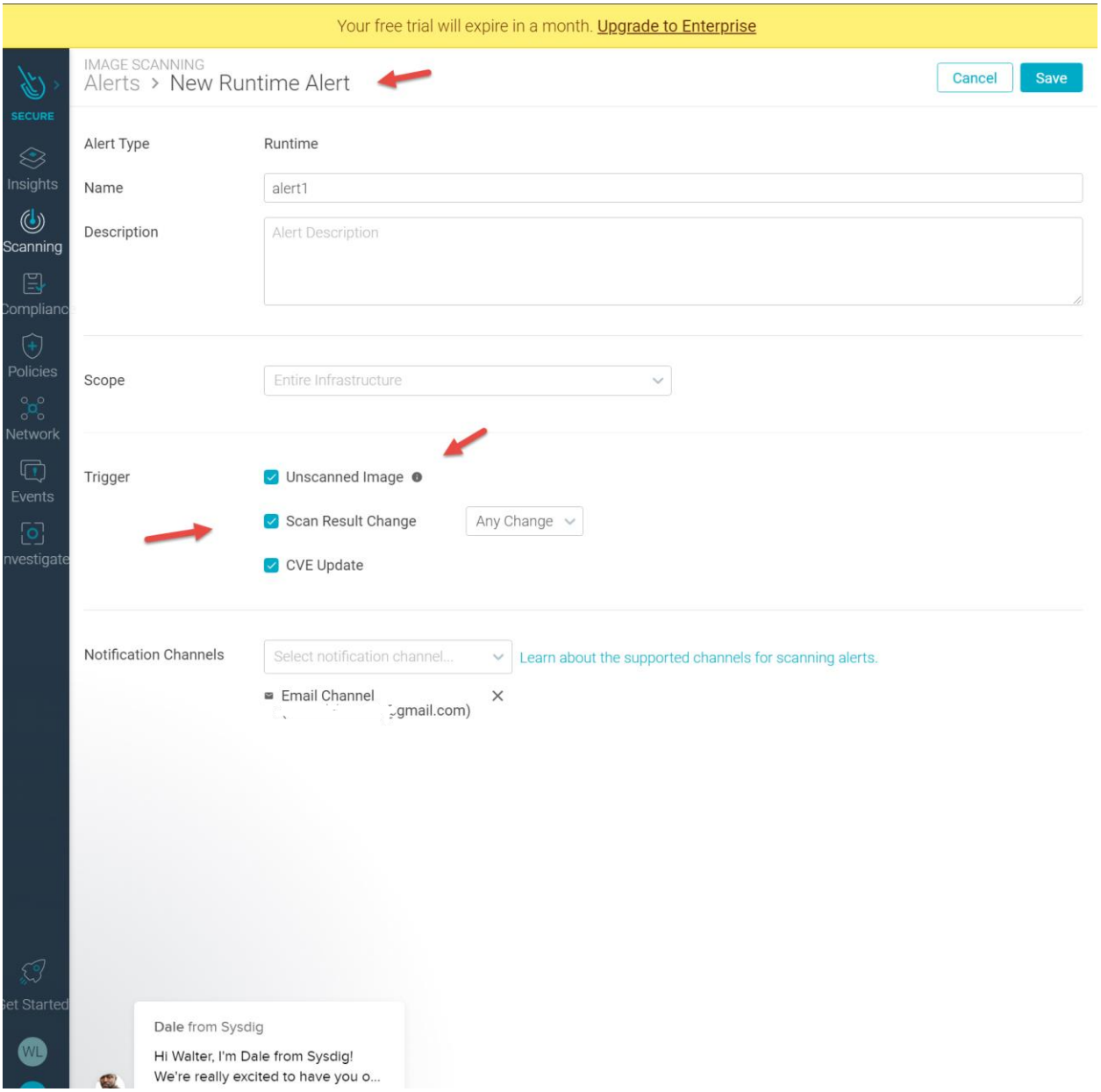
4.21/ sample docker image scanning rules:



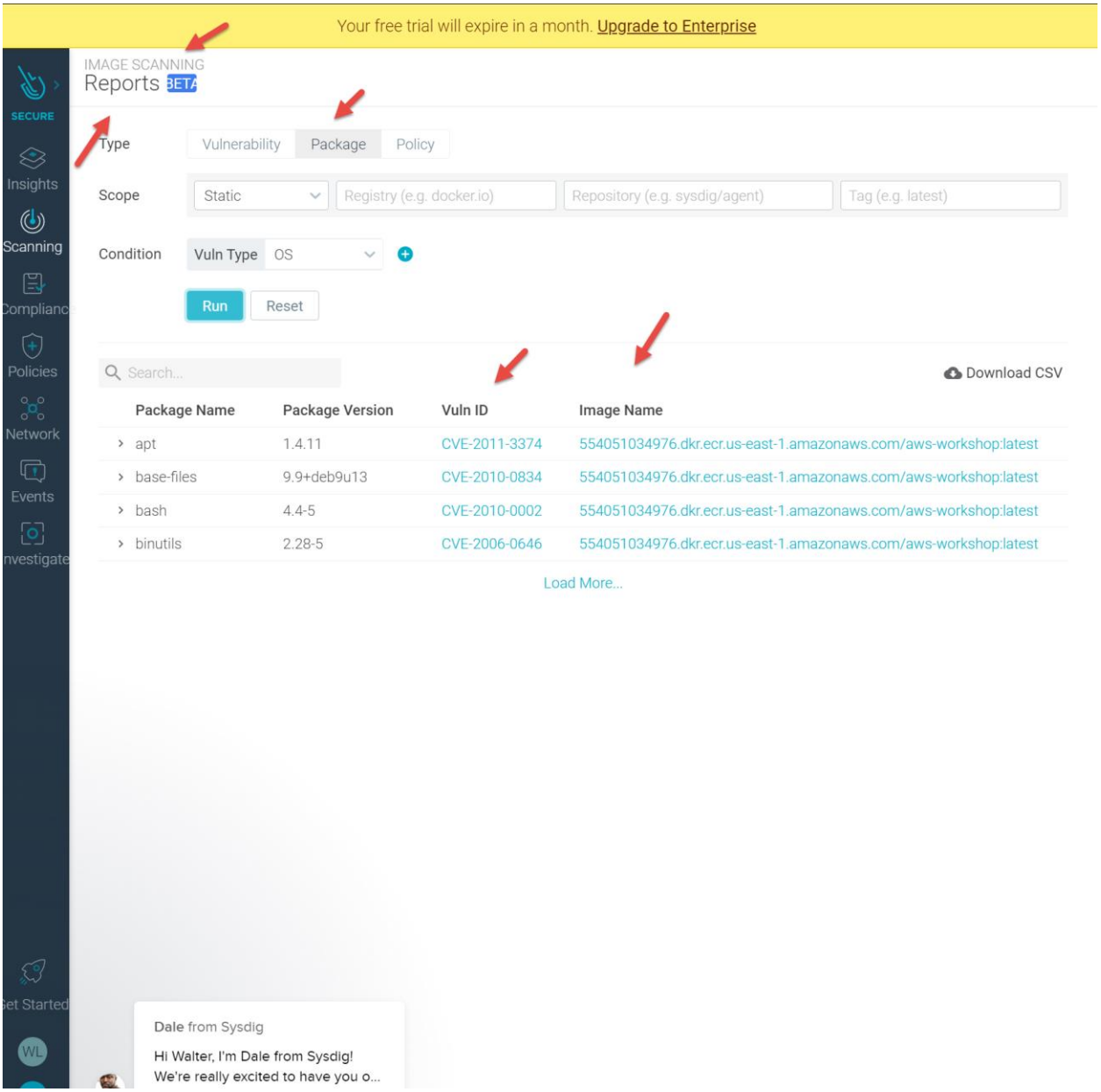
4.22/ sample runtime disallowed k8s activity:

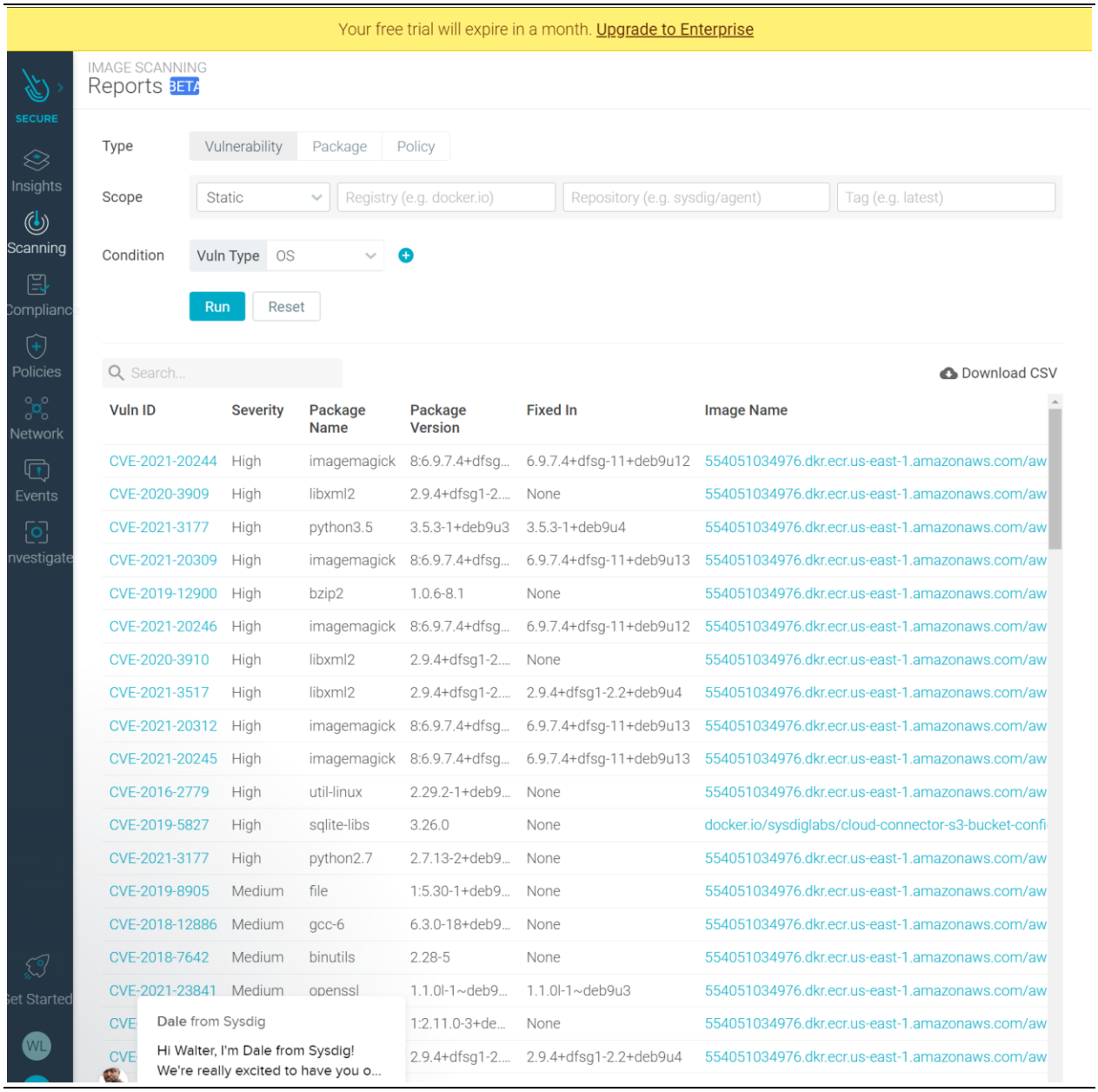


4.23/ easy to set up alert:

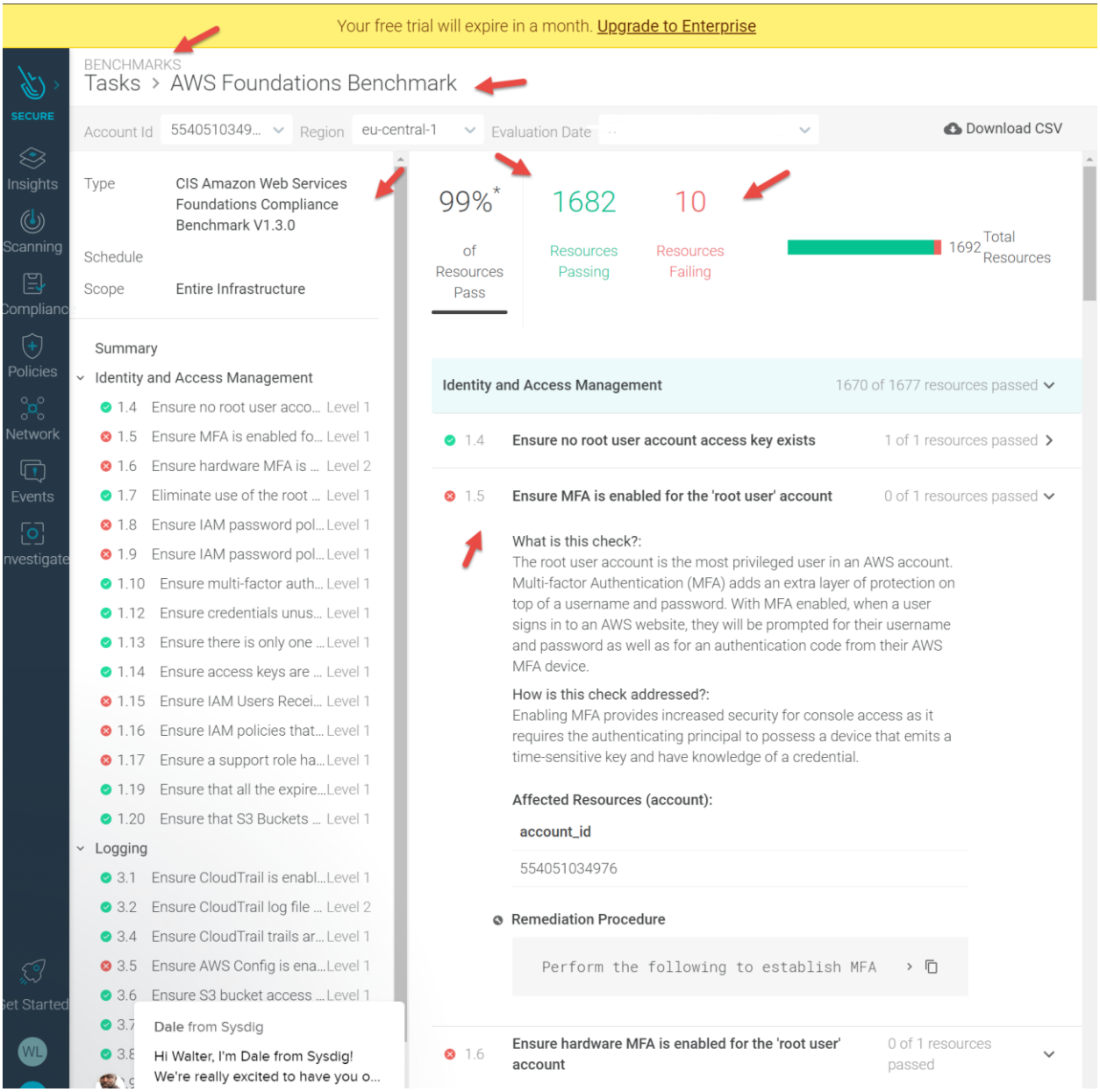


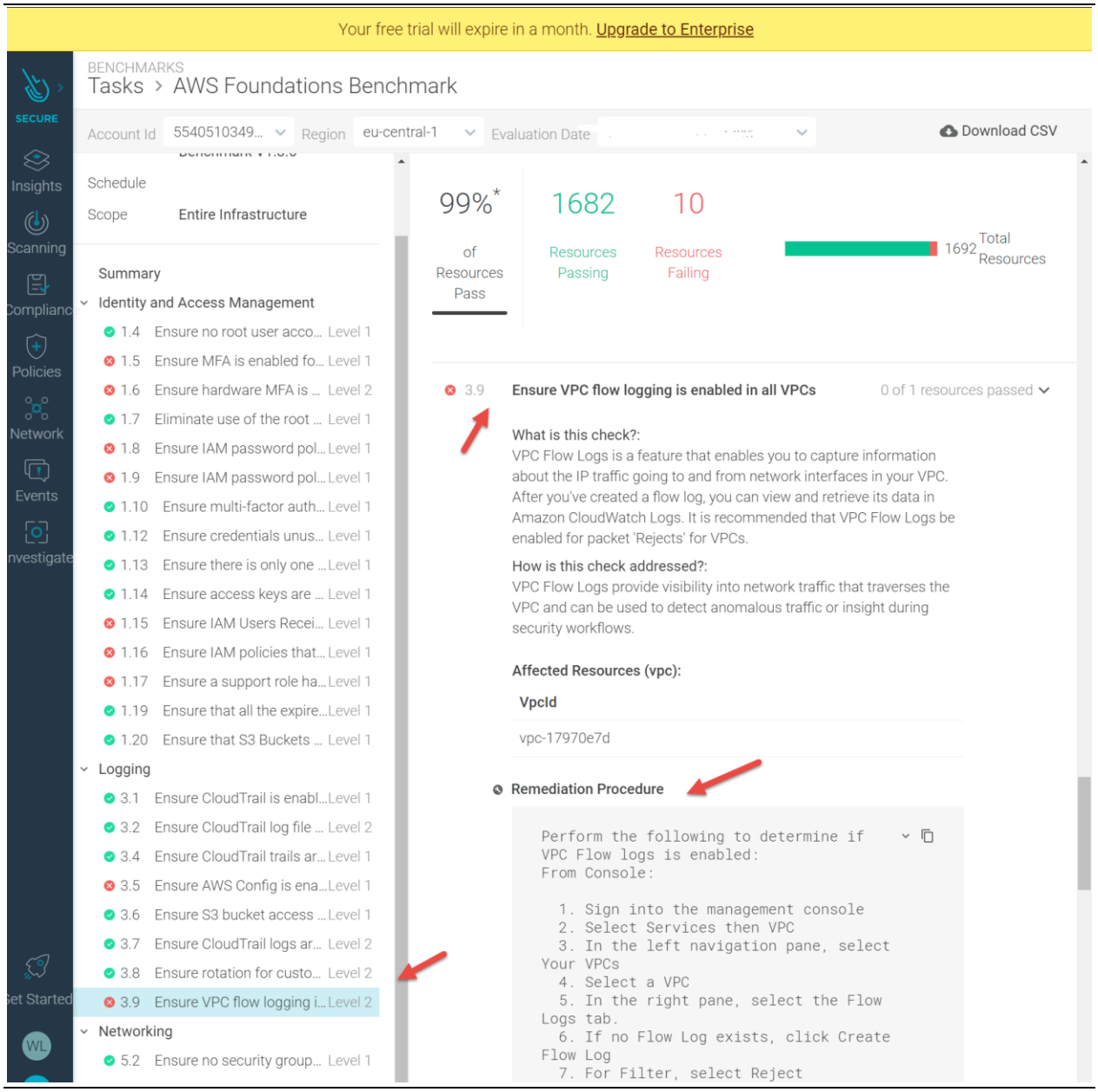
4.24/ sample Image scan reports:

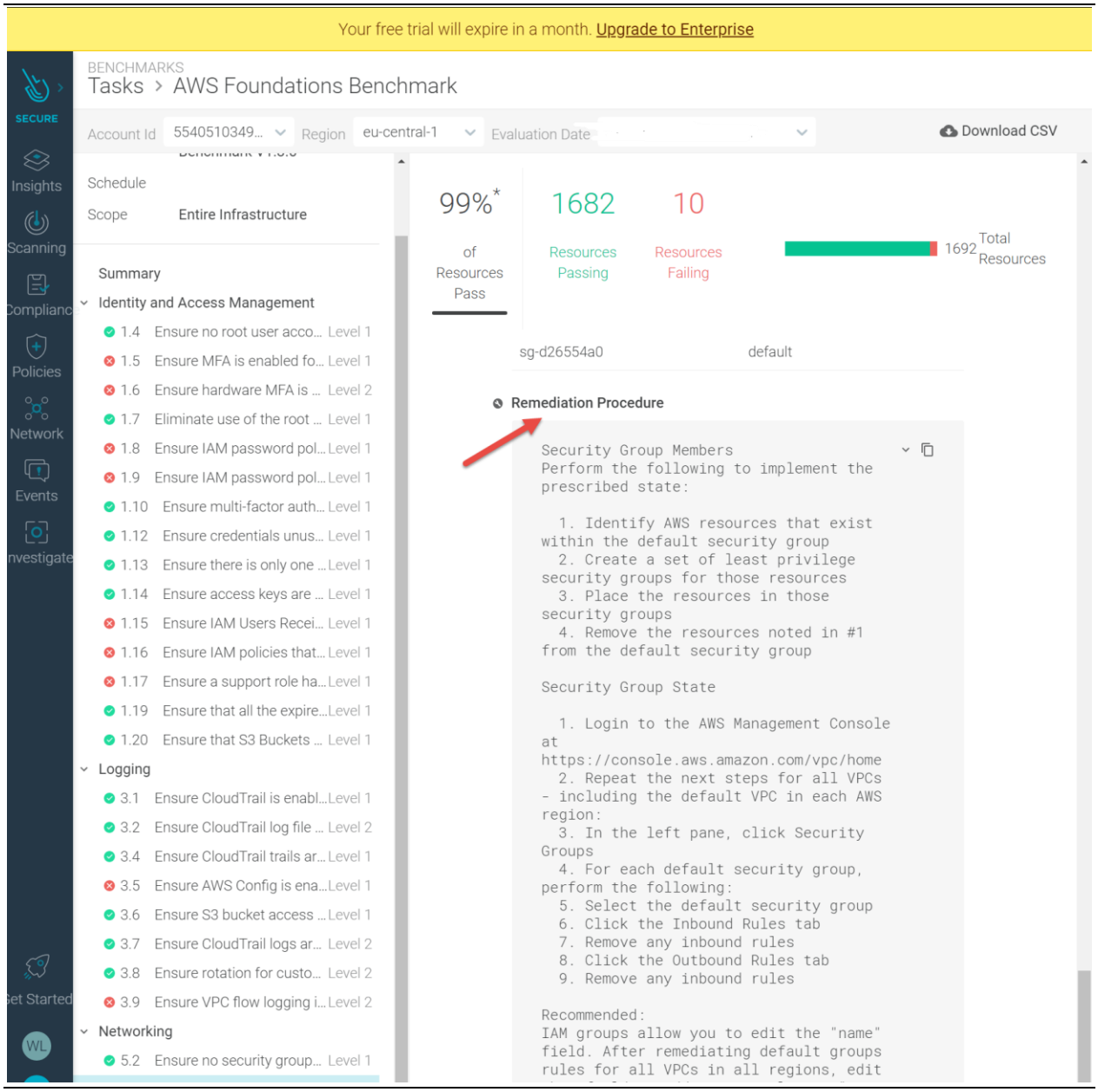


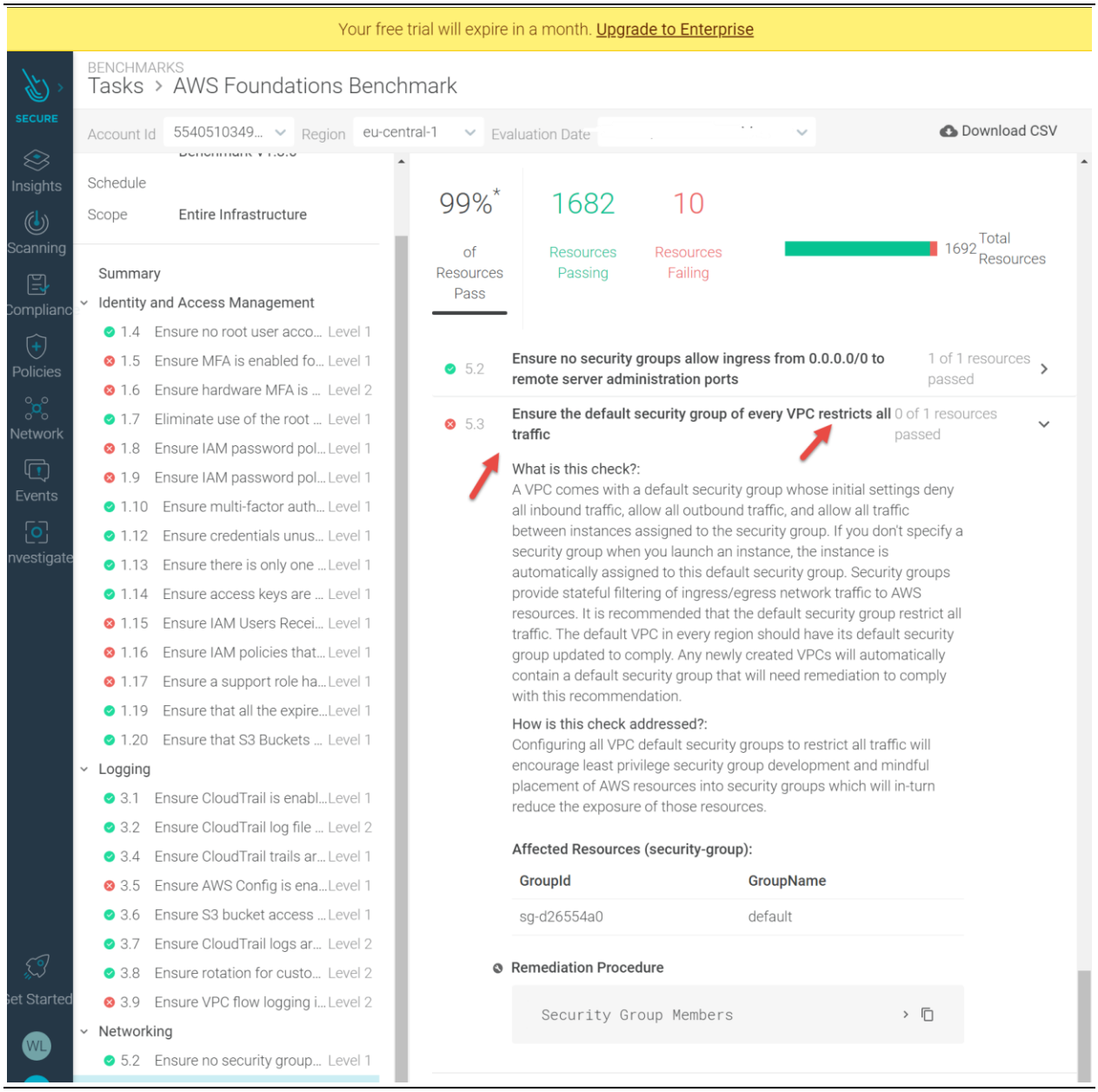

Your free trial will expire in a month. Upgrade to Enterprise
SECURE
Insights
Scanning
Compliance
Policies
Network
Events
Investigate
Get Started
IMAGE SCANNING
Reports BETA
Type
Vulnerability
Package
Policy
Scope
Static
Registry (e.g. docker.io)
Repository (e.g. sysdig/agent)
Tag (e.g. latest)
Condition
Vuln Type
OS
Run
Reset
Search...
Download CSV
Vuln ID
Severity
Package Name
Package Version
Fixed In
Image Name
CVE-2021-20244 High imagemagick 8:6.9.7.4+dfsg... 6.9.7.4+dfsg-11+deb9u12 554051034976.dkr.ecr.us-east-1.amazonaws.com/aw
CVE-2020-3909 High libxml2 2.9.4+dfsg1-2.... None 554051034976.dkr.ecr.us-east-1.amazonaws.com/aw
CVE-2021-3177 High python3.5 3.5.3-1+deb9u3 3.5.3-1+deb9u4 554051034976.dkr.ecr.us-east-1.amazonaws.com/aw
CVE-2021-20309 High imagemagick 8:6.9.7.4+dfsg... 6.9.7.4+dfsg-11+deb9u13 554051034976.dkr.ecr.us-east-1.amazonaws.com/aw
CVE-2019-12900 High bzip2 1.0.6-8.1 None 554051034976.dkr.ecr.us-east-1.amazonaws.com/aw
CVE-2021-20246 High imagemagick 8:6.9.7.4+dfsg... 6.9.7.4+dfsg-11+deb9u12 554051034976.dkr.ecr.us-east-1.amazonaws.com/aw
CVE-2020-3910 High libxml2 2.9.4+dfsg1-2.... None 554051034976.dkr.ecr.us-east-1.amazonaws.com/aw
CVE-2021-3517 High libxml2 2.9.4+dfsg1-2.... 2.9.4+dfsg1-2.2+deb9u4 554051034976.dkr.ecr.us-east-1.amazonaws.com/aw
CVE-2021-20312 High imagemagick 8:6.9.7.4+dfsg... 6.9.7.4+dfsg-11+deb9u13 554051034976.dkr.ecr.us-east-1.amazonaws.com/aw
CVE-2021-20245 High imagemagick 8:6.9.7.4+dfsg... 6.9.7.4+dfsg-11+deb9u13 554051034976.dkr.ecr.us-east-1.amazonaws.com/aw
CVE-2016-2779 High util-linux 2.29.2-1+deb9... None 554051034976.dkr.ecr.us-east-1.amazonaws.com/aw
CVE-2019-5827 High sqlite-libs 3.26.0 None docker.io/sysdiglabs/cloud-connector-s3-bucket-confi
CVE-2021-3177 High python2.7 2.7.13-2+deb9... None 554051034976.dkr.ecr.us-east-1.amazonaws.com/aw
CVE-2019-8905 Medium file 1:5.30-1+deb9... None 554051034976.dkr.ecr.us-east-1.amazonaws.com/aw
CVE-2018-12886 Medium gcc-6 6.3.0-18+deb9... None 554051034976.dkr.ecr.us-east-1.amazonaws.com/aw
CVE-2018-7642 Medium binutils 2.28-5 None 554051034976.dkr.ecr.us-east-1.amazonaws.com/aw
CVE-2021-23841 Medium openssl 1.1.0l-1~deb9... 1.1.0l-1~deb9u3 554051034976.dkr.ecr.us-east-1.amazonaws.com/aw
CVE- 1:2.11.0-3+de... None 554051034976.dkr.ecr.us-east-1.amazonaws.com/aw
CVE- 2.9.4+dfsg1-2.... 2.9.4+dfsg1-2.2+deb9u4 554051034976.dkr.ecr.us-east-1.amazonaws.com/aw
Dale from Sysdig
Hi Walter, I'm Dale from Sysdig!
We're really excited to have you o...
WL

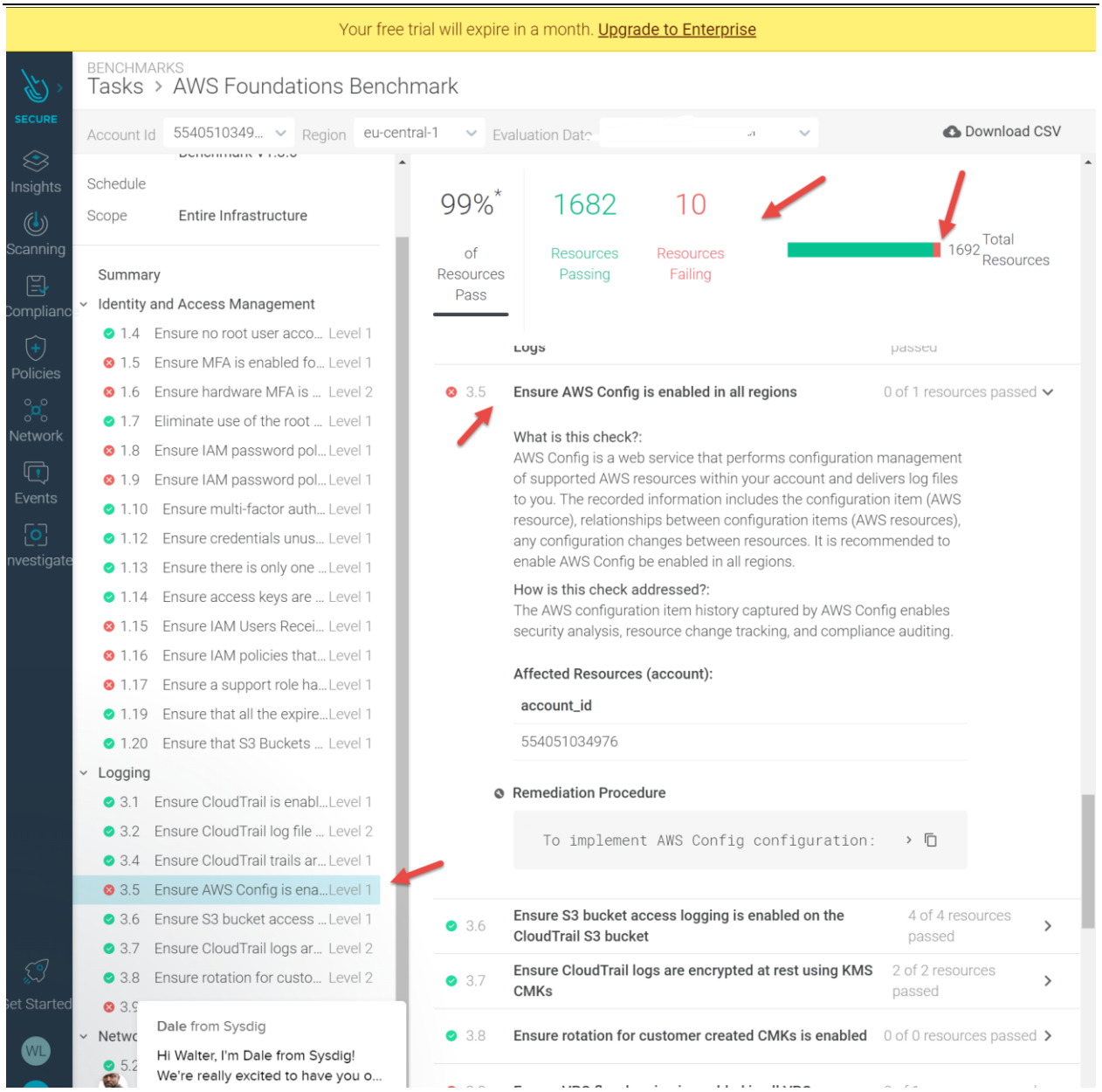
4.25/ Benchmarks of AWS security – many checks:



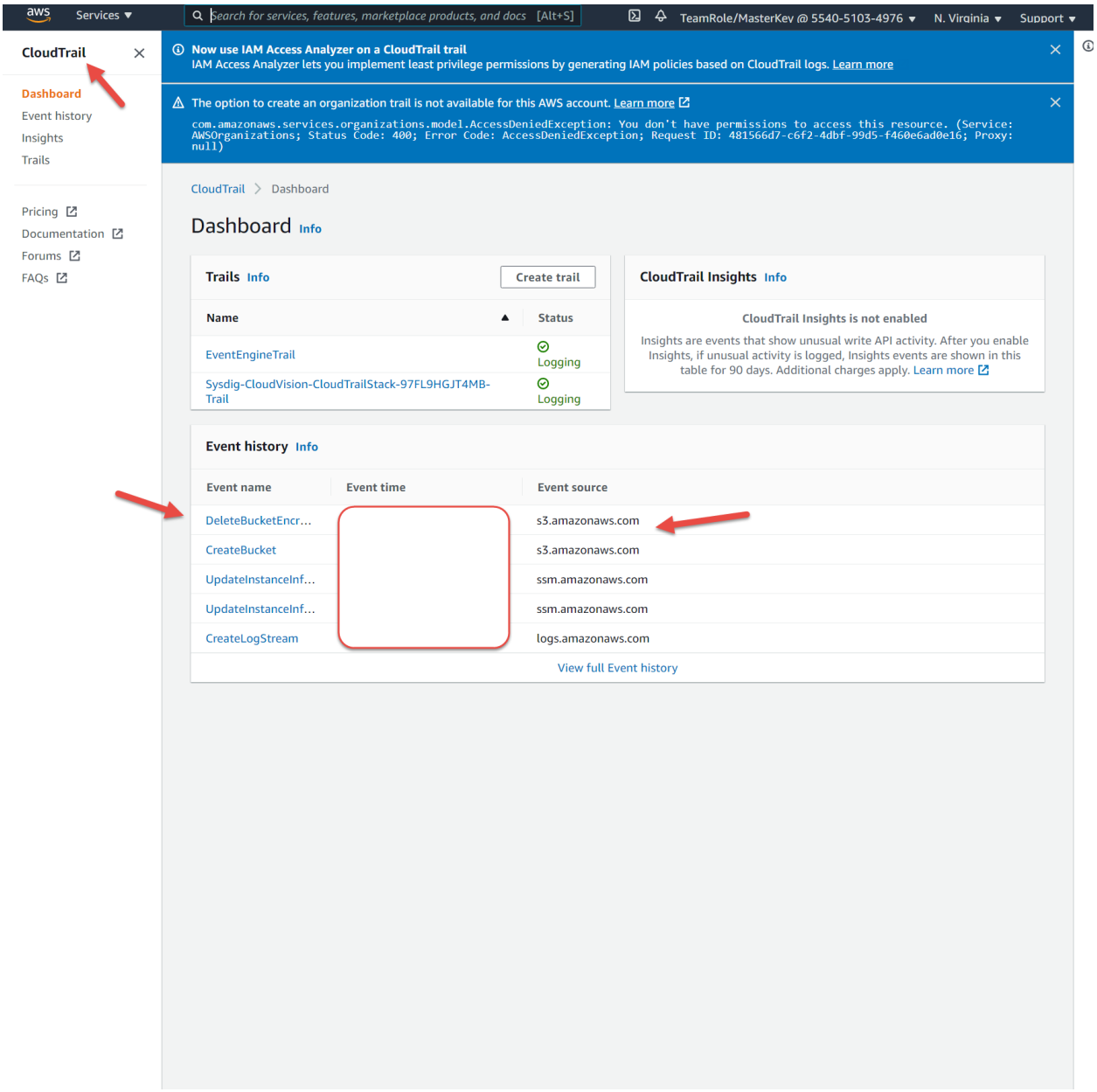

Your free trial will expire in a month. Upgrade to Enterprise
SECURE
Insights
Scanning
Compliance
Policies
Network
Events
Investigate
Get Started
BENCHMARKS
Tasks > AWS Foundations Benchmark
Account Id 5540510349...
Region eu-central-1
Evaluation Date
Download CSV
Schedule
Scope Entire Infrastructure
Summary
Identity and Access Management
1.4 Ensure no root user acco... Level 1
1.5 Ensure MFA is enabled fo... Level 1
1.6 Ensure hardware MFA is ... Level 2
1.7 Eliminate use of the root ... Level 1
1.8 Ensure IAM password pol... Level 1
1.9 Ensure IAM password pol... Level 1
1.10 Ensure multi-factor auth... Level 1
1.12 Ensure credentials unus... Level 1
1.13 Ensure there is only one ... Level 1
1.14 Ensure access keys are ... Level 1
1.15 Ensure IAM Users Recei... Level 1
1.16 Ensure IAM policies that... Level 1
1.17 Ensure a support role ha... Level 1
1.19 Ensure that all the expire... Level 1
1.20 Ensure that S3 Buckets ... Level 1
Logging
3.1 Ensure CloudTrail is enabl... Level 1
3.2 Ensure CloudTrail log file ... Level 2
3.4 Ensure CloudTrail trails ar... Level 1
3.5 Ensure AWS Config is ena... Level 1
3.6 Ensure S3 bucket access ... Level 1
3.7 Ensure CloudTrail logs ar... Level 2
3.8 Ensure rotation for custo... Level 2
3.9 Ensure VPC flow logging i... Level 2
Networking
5.2 Ensure no security group... Level 1
99%*
of Resources Pass
1682
Resources Passing
10
Resources Failing
1692 Total Resources
3.9 Ensure VPC flow logging is enabled in all VPCs
0 of 1 resources passed
What is this check?:
VPC Flow Logs is a feature that enables you to capture information about the IP traffic going to and from network interfaces in your VPC. After you've created a flow log, you can view and retrieve its data in Amazon CloudWatch Logs. It is recommended that VPC Flow Logs be enabled for packet 'Rejects' for VPCs.
How is this check addressed?:
VPC Flow Logs provide visibility into network traffic that traverses the VPC and can be used to detect anomalous traffic or insight during security workflows.
Affected Resources (vpc):
VpcId
vpc-17970e7d
Remediation Procedure
Perform the following to determine if VPC Flow logs is enabled:
From Console:
1. Sign into the management console
2. Select Services then VPC
3. In the left navigation pane, select Your VPCs
4. Select a VPC
5. In the right pane, select the Flow Logs tab.
6. If no Flow Log exists, click Create Flow Log
7. For Filter, select Reject

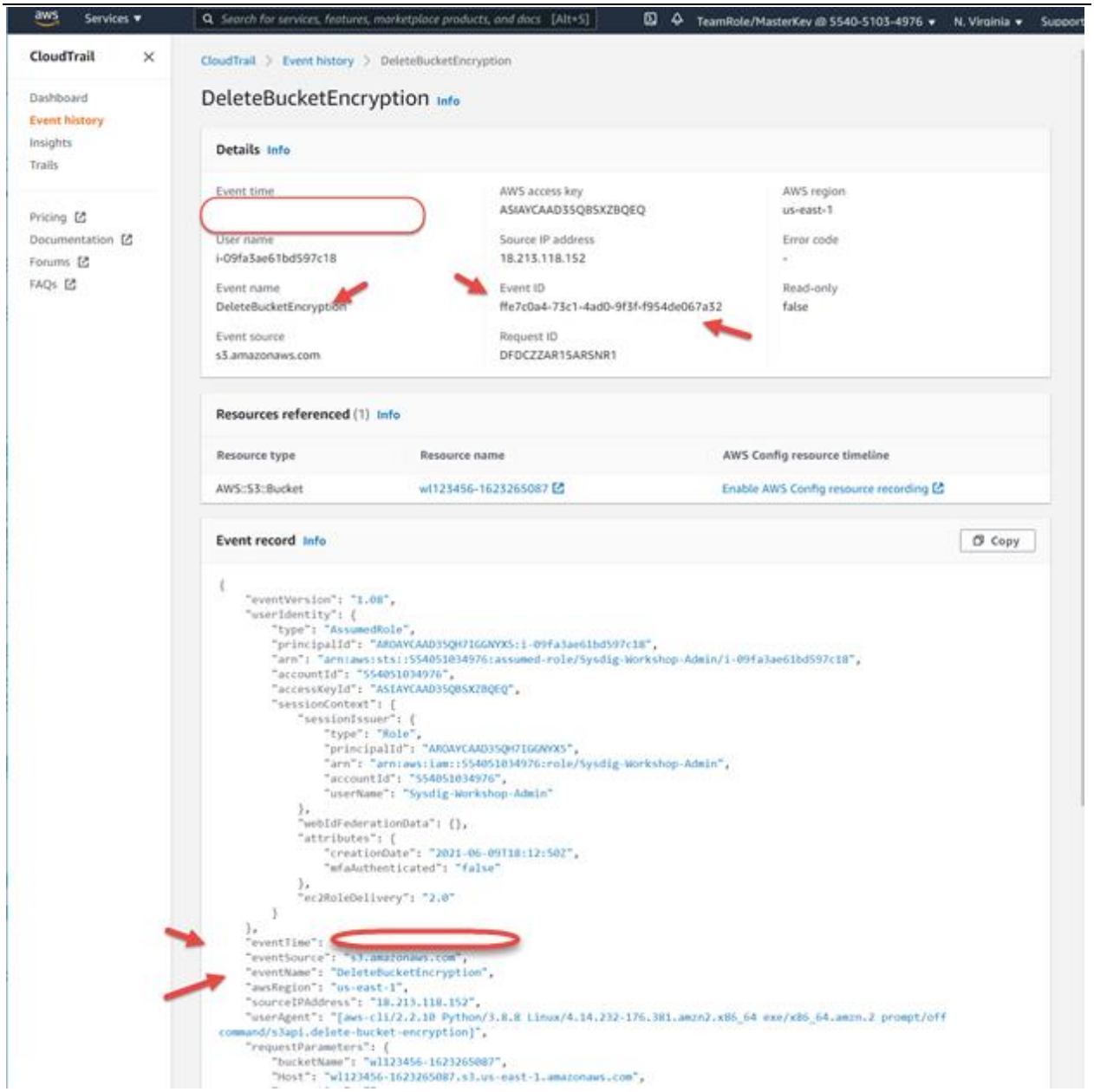

Your free trial will expire in a month. Upgrade to Enterprise
SECURE
Insights
Scanning
Compliance
Policies
Network
Events
Investigate
Get Started
BENCHMARKS
Tasks > AWS Foundations Benchmark
Account Id 5540510349...
Region eu-central-1
Evaluation Date
Download CSV
Schedule
Scope Entire Infrastructure
Summary
Identity and Access Management
1.4 Ensure no root user acco... Level 1
1.5 Ensure MFA is enabled fo... Level 1
1.6 Ensure hardware MFA is ... Level 2
1.7 Eliminate use of the root ... Level 1
1.8 Ensure IAM password pol... Level 1
1.9 Ensure IAM password pol... Level 1
1.10 Ensure multi-factor auth... Level 1
1.12 Ensure credentials unus... Level 1
1.13 Ensure there is only one ... Level 1
1.14 Ensure access keys are ... Level 1
1.15 Ensure IAM Users Recei... Level 1
1.16 Ensure IAM policies that... Level 1
1.17 Ensure a support role ha... Level 1
1.19 Ensure that all the expire... Level 1
1.20 Ensure that S3 Buckets ... Level 1
Logging
3.1 Ensure CloudTrail is enabl... Level 1
3.2 Ensure CloudTrail log file ... Level 2
3.4 Ensure CloudTrail trails ar... Level 1
3.5 Ensure AWS Config is ena... Level 1
3.6 Ensure S3 bucket access ... Level 1
3.7 Ensure CloudTrail logs ar... Level 2
3.8 Ensure rotation for custo... Level 2
3.9 Ensure VPC flow logging i... Level 2
Networking
5.2 Ensure no security group... Level 1
99%*
of Resources Pass
1682
Resources Passing
10
Resources Failing
1692 Total Resources
sg-d26554a0 default
Remediation Procedure
Security Group Members
Perform the following to implement the prescribed state:
1. Identify AWS resources that exist within the default security group
2. Create a set of least privilege security groups for those resources
3. Place the resources in those security groups
4. Remove the resources noted in #1 from the default security group
Security Group State
1. Login to the AWS Management Console at https://console.aws.amazon.com/vpc/home
2. Repeat the next steps for all VPCs - including the default VPC in each AWS region:
3. In the left pane, click Security Groups
4. For each default security group, perform the following:
5. Select the default security group
6. Click the Inbound Rules tab
7. Remove any inbound rules
8. Click the Outbound Rules tab
9. Remove any inbound rules
Recommended:
IAM groups allow you to edit the "name" field. After remediating default groups rules for all VPCs in all regions, edit

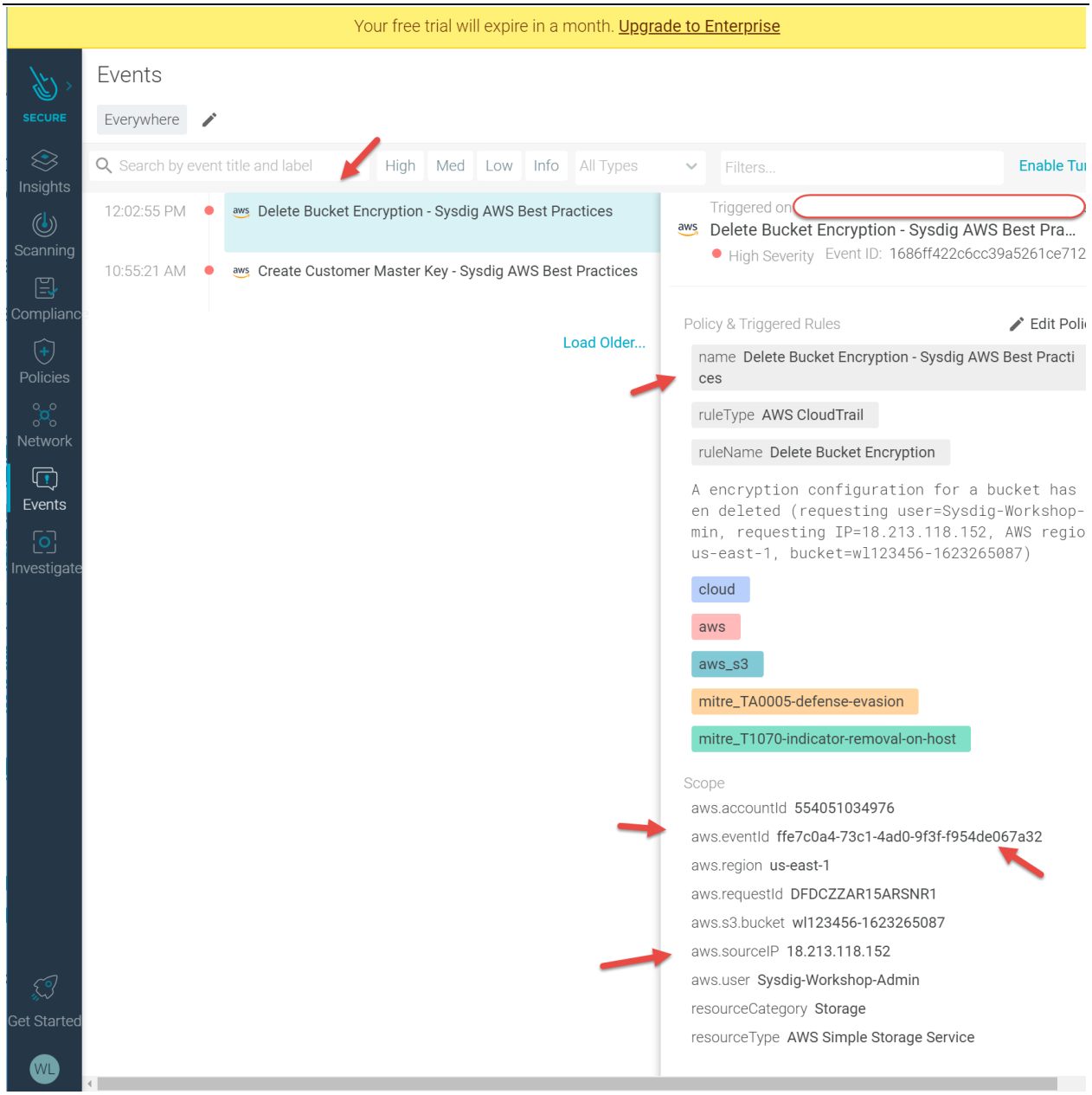

Your free trial will expire in a month. Upgrade to Enterprise
SECURE
Insights
Scanning
Compliance
Policies
Network
Events
Investigate
Get Started
BENCHMARKS
Tasks > AWS Foundations Benchmark
Account Id 5540510349...
Region eu-central-1
Evaluation Date
Download CSV
Schedule
Scope Entire Infrastructure
Summary
Identity and Access Management
1.4 Ensure no root user acco... Level 1
1.5 Ensure MFA is enabled fo... Level 1
1.6 Ensure hardware MFA is ... Level 2
1.7 Eliminate use of the root ... Level 1
1.8 Ensure IAM password pol... Level 1
1.9 Ensure IAM password pol... Level 1
1.10 Ensure multi-factor auth... Level 1
1.12 Ensure credentials unus... Level 1
1.13 Ensure there is only one ... Level 1
1.14 Ensure access keys are ... Level 1
1.15 Ensure IAM Users Recei... Level 1
1.16 Ensure IAM policies that... Level 1
1.17 Ensure a support role ha... Level 1
1.19 Ensure that all the expire... Level 1
1.20 Ensure that S3 Buckets ... Level 1
Logging
3.1 Ensure CloudTrail is enabl... Level 1
3.2 Ensure CloudTrail log file ... Level 2
3.4 Ensure CloudTrail trails ar... Level 1
3.5 Ensure AWS Config is ena... Level 1
3.6 Ensure S3 bucket access ... Level 1
3.7 Ensure CloudTrail logs ar... Level 2
3.8 Ensure rotation for custo... Level 2
3.9 Ensure VPC flow logging i... Level 2
Networking
5.2 Ensure no security group... Level 1
99%*
of Resources Pass
1682
Resources Passing
10
Resources Failing
1692 Total Resources
5.2 Ensure no security groups allow ingress from 0.0.0.0/0 to remote server administration ports 1 of 1 resources passed
5.3 Ensure the default security group of every VPC restricts all traffic 0 of 1 resources passed
What is this check?:
A VPC comes with a default security group whose initial settings deny all inbound traffic, allow all outbound traffic, and allow all traffic between instances assigned to the security group. If you don't specify a security group when you launch an instance, the instance is automatically assigned to this default security group. Security groups provide stateful filtering of ingress/egress network traffic to AWS resources. It is recommended that the default security group restrict all traffic. The default VPC in every region should have its default security group updated to comply. Any newly created VPCs will automatically contain a default security group that will need remediation to comply with this recommendation.
How is this check addressed?:
Configuring all VPC default security groups to restrict all traffic will encourage least privilege security group development and mindful placement of AWS resources into security groups which will in-turn reduce the exposure of those resources.
Affected Resources (security-group):
GroupId
GroupName
sg-d26554a0
default
Remediation Procedure
Security Group Members


Your free trial will expire in a month. Upgrade to Enterprise
SECURE
Insights
Scanning
Compliance
Policies
Network
Events
Investigate
Get Started
BENCHMARKS
Tasks > AWS Foundations Benchmark
Account Id 5540510349...
Region eu-central-1
Evaluation Date
Download CSV
Schedule
Scope Entire Infrastructure
Summary
Identity and Access Management
1.4 Ensure no root user acco... Level 1
1.5 Ensure MFA is enabled fo... Level 1
1.6 Ensure hardware MFA is ... Level 2
1.7 Eliminate use of the root ... Level 1
1.8 Ensure IAM password pol... Level 1
1.9 Ensure IAM password pol... Level 1
1.10 Ensure multi-factor auth... Level 1
1.12 Ensure credentials unus... Level 1
1.13 Ensure there is only one ... Level 1
1.14 Ensure access keys are ... Level 1
1.15 Ensure IAM Users Recei... Level 1
1.16 Ensure IAM policies that... Level 1
1.17 Ensure a support role ha... Level 1
1.19 Ensure that all the expire... Level 1
1.20 Ensure that S3 Buckets ... Level 1
Logging
3.1 Ensure CloudTrail is enabl... Level 1
3.2 Ensure CloudTrail log file ... Level 2
3.4 Ensure CloudTrail trails ar... Level 1
3.5 Ensure AWS Config is ena... Level 1
3.6 Ensure S3 bucket access ... Level 1
3.7 Ensure CloudTrail logs ar... Level 2
3.8 Ensure rotation for custo... Level 2
Dale from Sysdig
Hi Walter, I'm Dale from Sysdig!
We're really excited to have you o...
99%*
of Resources Pass
1682
Resources Passing
10
Resources Failing
1692 Total Resources
3.5 Ensure AWS Config is enabled in all regions
0 of 1 resources passed
What is this check?:
AWS Config is a web service that performs configuration management of supported AWS resources within your account and delivers log files to you. The recorded information includes the configuration item (AWS resource), relationships between configuration items (AWS resources), any configuration changes between resources. It is recommended to enable AWS Config be enabled in all regions.
How is this check addressed?:
The AWS configuration item history captured by AWS Config enables security analysis, resource change tracking, and compliance auditing.
Affected Resources (account):
account_id
554051034976
Remediation Procedure
To implement AWS Config configuration:
3.6 Ensure S3 bucket access logging is enabled on the CloudTrail S3 bucket
4 of 4 resources passed
3.7 Ensure CloudTrail logs are encrypted at rest using KMS CMKs
2 of 2 resources passed
3.8 Ensure rotation for customer created CMKs is enabled
0 of 0 resources passed

4.26/ CloudTrail – can see ALL events in Sysdig as in AWS, e.g. delete a test s3 bucket event below:




Services
Search for services, features, marketplace products, and docs [Alt+S]
TeamRole/MasterKev @ 5540-5103-4976
N. Virginia
Support
CloudTrail
Dashboard
Event history
Insights
Trails
Pricing
Documentation
Forums
FAQs
CloudTrail > Event history > DeleteBucketEncryption
DeleteBucketEncryption Info
Details Info
Event time
User name
i-09fa3ae61bd597c18
Event name
DeleteBucketEncryption
Event source
s3.amazonaws.com
AWS access key
ASIAYCAAD35QBSXZBQEQ
Source IP address
18.213.118.152
Event ID
ffe7c0a4-73c1-4ad0-9f3f-f954de067a32
Request ID
DFDCZZAR15ARSNR1
AWS region
us-east-1
Error code
-
Read-only
false
Resources referenced (1) Info
Resource type
Resource name
AWS Config resource timeline
AWS::S3::Bucket
wl123456-1623265087
Enable AWS Config resource recording
Event record Info
Copy
{
"eventVersion": "1.08",
"userIdentity": {
"type": "AssumedRole",
"principalId": "AROAYCAAD35QH7IGGNYX5:i-09fa3ae61bd597c18",
"arn": "arn:aws:sts::554051034976:assumed-role/Sysdig-Workshop-Admin/i-09fa3ae61bd597c18",
"accountId": "554051034976",
"accessKeyId": "ASIAYCAAD35QBSXZBQEQ",
"sessionContext": {
"sessionIssuer": {
"type": "Role",
"principalId": "AROAYCAAD35QH7IGGNYX5",
"arn": "arn:aws:iam::554051034976:role/Sysdig-Workshop-Admin",
"accountId": "554051034976",
"userName": "Sysdig-Workshop-Admin"
},
"webIdFederationData": {},
"attributes": {
"creationDate": "2021-06-09T18:12:50Z",
"mfaAuthenticated": "false"
},
"ec2RoleDelivery": "2.0"
}
},
"eventTime":
"eventSource": "s3.amazonaws.com",
"eventName": "DeleteBucketEncryption",
"awsRegion": "us-east-1",
"sourceIPAddress": "18.213.118.152",
"userAgent": "[aws-cli/2.2.10 Python/3.8.8 Linux/4.14.232-176.381.amzn2.x86_64 exe/x86_64.amzn.2 prompt/off
command/s3api.delete-bucket-encryption]",
"requestParameters": {
"bucketName": "wl123456-1623265087",
"Host": "wl123456-1623265087.s3.us-east-1.amazonaws.com",



Can see the same eventId in Sysdig as in AWS CloudTrail!