OWASP CLOUD NATIVE TOP TEN

ISSA NoVA March 2023

INTRO

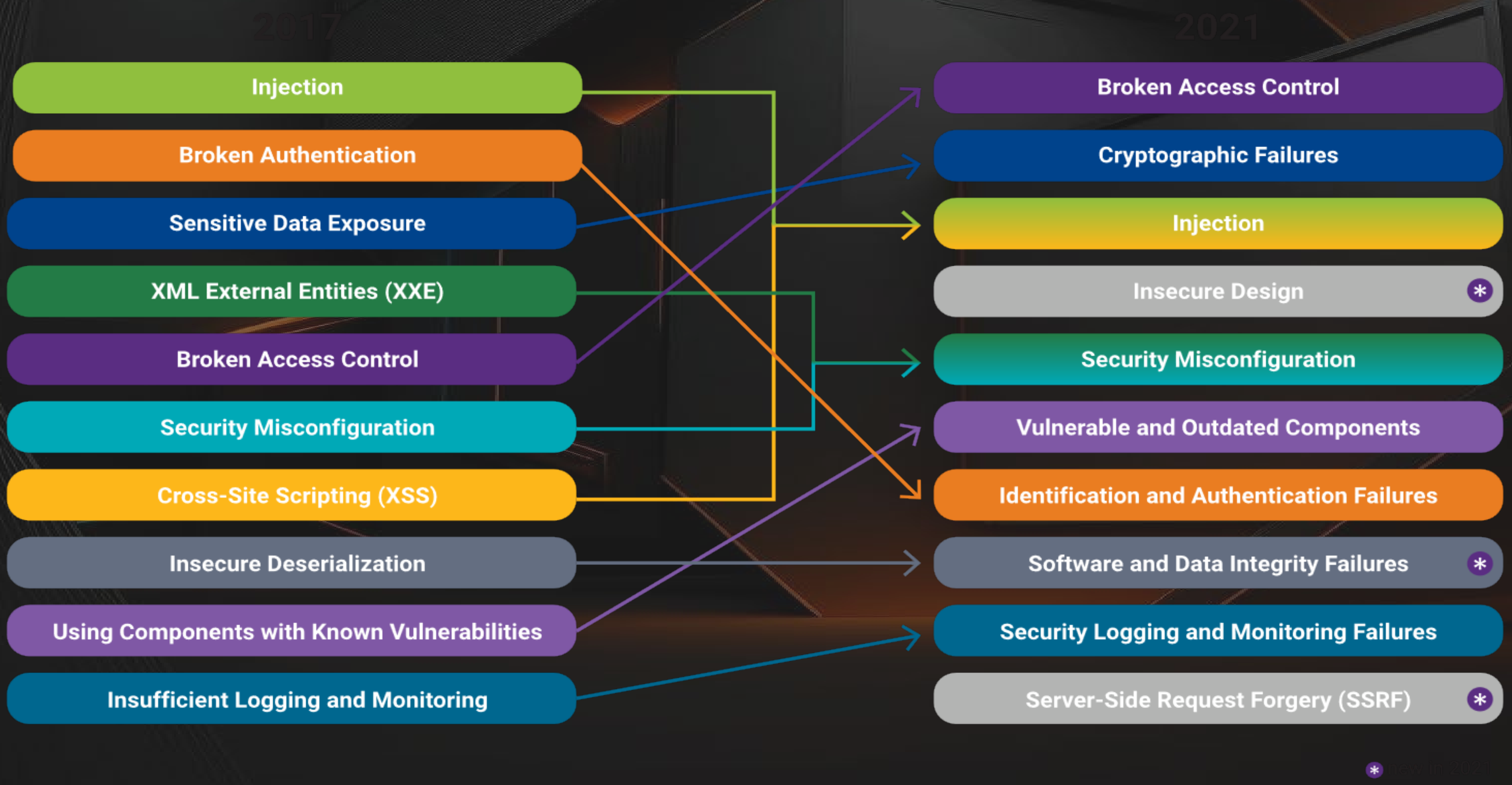
- Michael McCabe
- President - Cloud Security Partners
- Cloud security consulting and engineering
- Help migrate large workloads to the cloud
- Passionate about IAC security

CLOUD SECURITY
PARTNERS

OWASP TOP TEN

- Traditionally focused on web applications
- Apps and cloud are merging
- Expertise in both is required
- Attackers use combination of app and cloud vulnerabilities to gain access

OWASP TOP TEN



2017
Injection
Broken Authentication
Sensitive Data Exposure
XML External Entities (XXE)
Broken Access Control
Security Misconfiguration
Cross-Site Scripting (XSS)
Insecure Deserialization
Using Components with Known Vulnerabilities
Insufficient Logging and Monitoring
2021
Broken Access Control
Cryptographic Failures
Injection
Insecure Design *
Security Misconfiguration
Vulnerable and Outdated Components
Identification and Authentication Failures
Software and Data Integrity Failures *
Security Logging and Monitoring Failures
Server-Side Request Forgery (SSRF) *
* new in 2021

OWASP TOP TEN SERVERLESS..

- S1:2017 Injection
- S2:2017 Broken Authentication
- S3:2017 Sensitive Data Exposure
- S4:2017 XML External Entities (XXE)
- S5:2017 Broken Access Control

S6:2017 Security Misconfiguration

S7:2017 Cross-Site Scripting (XSS)

S8:2017 Insecure Deserialization

S9:2017 Using Components with Known Vulnerabilities

S10:2017 Insufficient Logging and Monitoring

CLOUD THREATS

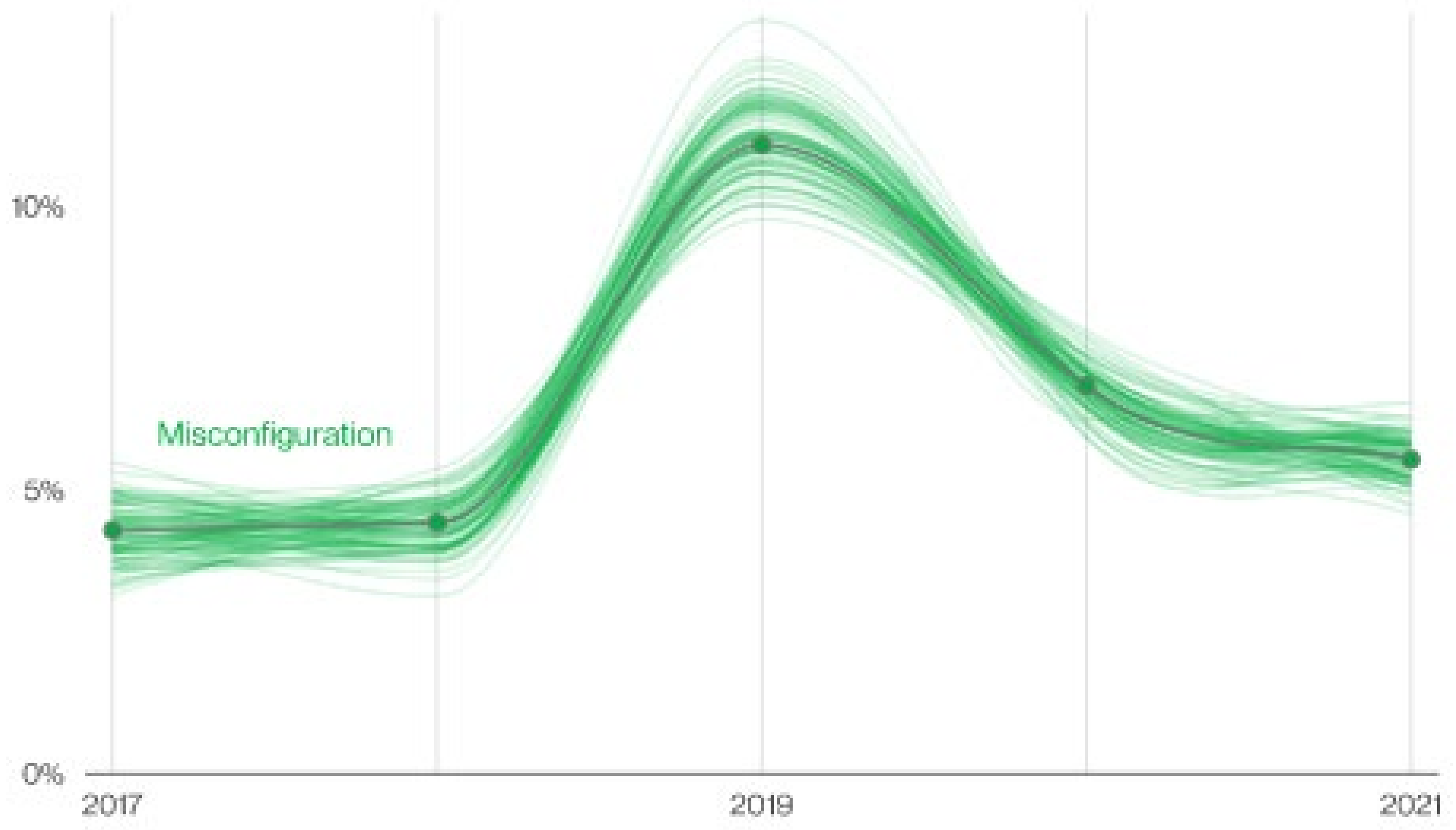


Figure 8. Misconfiguration over time in breaches

Source: 2022 DBIR

CLOUD THREATS

“Despite the advantages, cloud computing comes with an added vulnerability if data is stored incorrectly or if the provider’s own security is compromised,” says Gartner practice leader Matthew Shinkman.

47% of companies have at least one database or storage bucket exposed to the internet (either managed or non-managed), and over 20% of those cloud environments with publicly accessible buckets have buckets that contain sensitive data. -Wiz

CLOUD THREATS

- Applications and cloud provide a larger attack surface
- Cloud is a great pivot point
- Constantly evolving

CLOUD NATIVE TOP TEN

- CNAS-1: Insecure cloud, container or orchestration configuration
- CNAS-2: Injection flaws (app layer, cloud events, cloud services)
- CNAS-3: Improper authentication & authorization
- CNAS-4: CI/CD pipeline & software supply chain flaws
- CNAS-5: Insecure secrets storage
- CNAS-6: Over-permissive or insecure network policies
- CNAS-7: Using components with known vulnerabilities
- CNAS-8: Improper assets management
- CNAS-9: Inadequate ‘compute’ resource quota limits
- CNAS-10: Ineffective logging & monitoring (e.g. runtime activity)

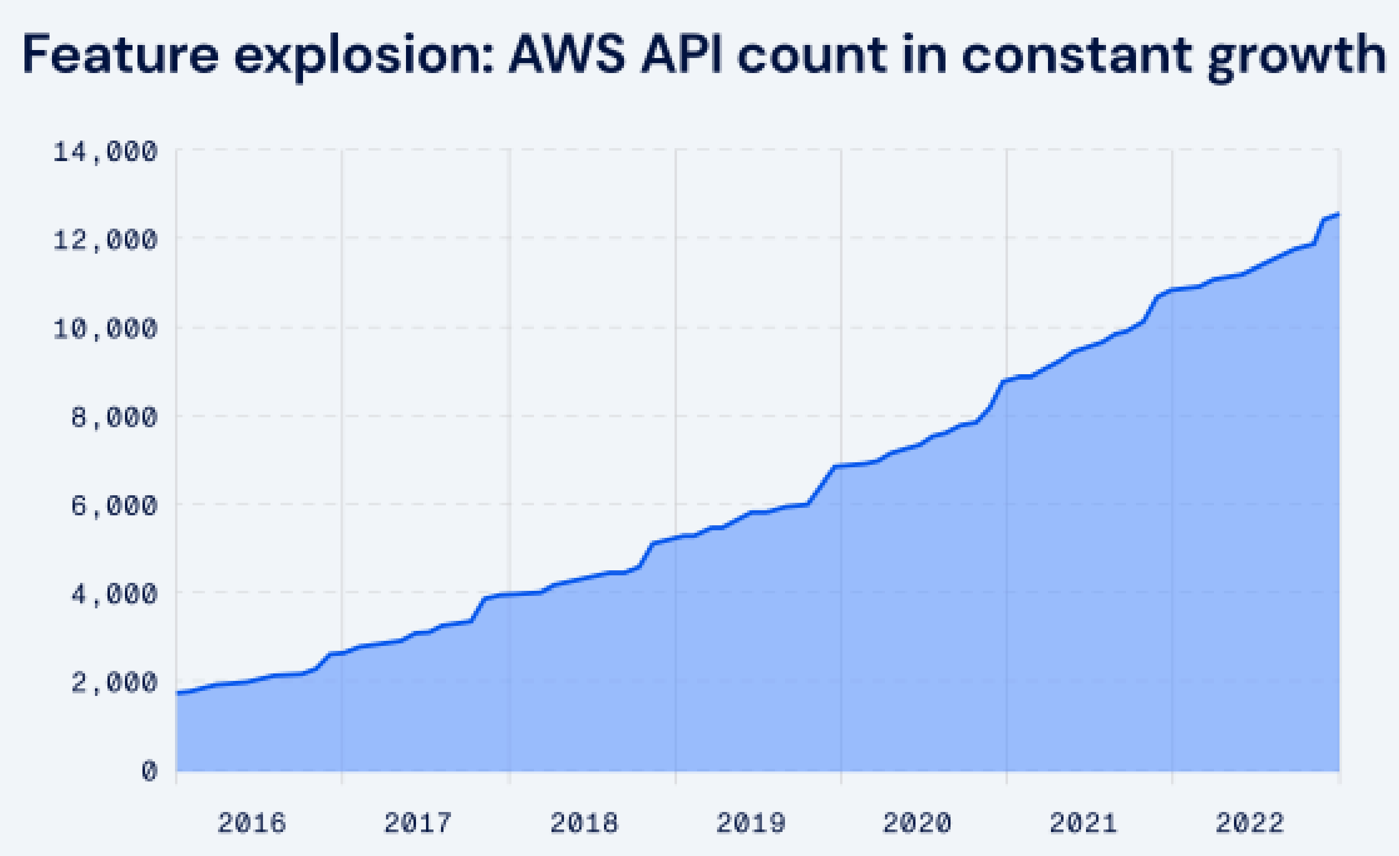
CNAS-1

Insecure cloud, container or orchestration configuration

AKA The Cloud Kitchen Sink

CNAS-1

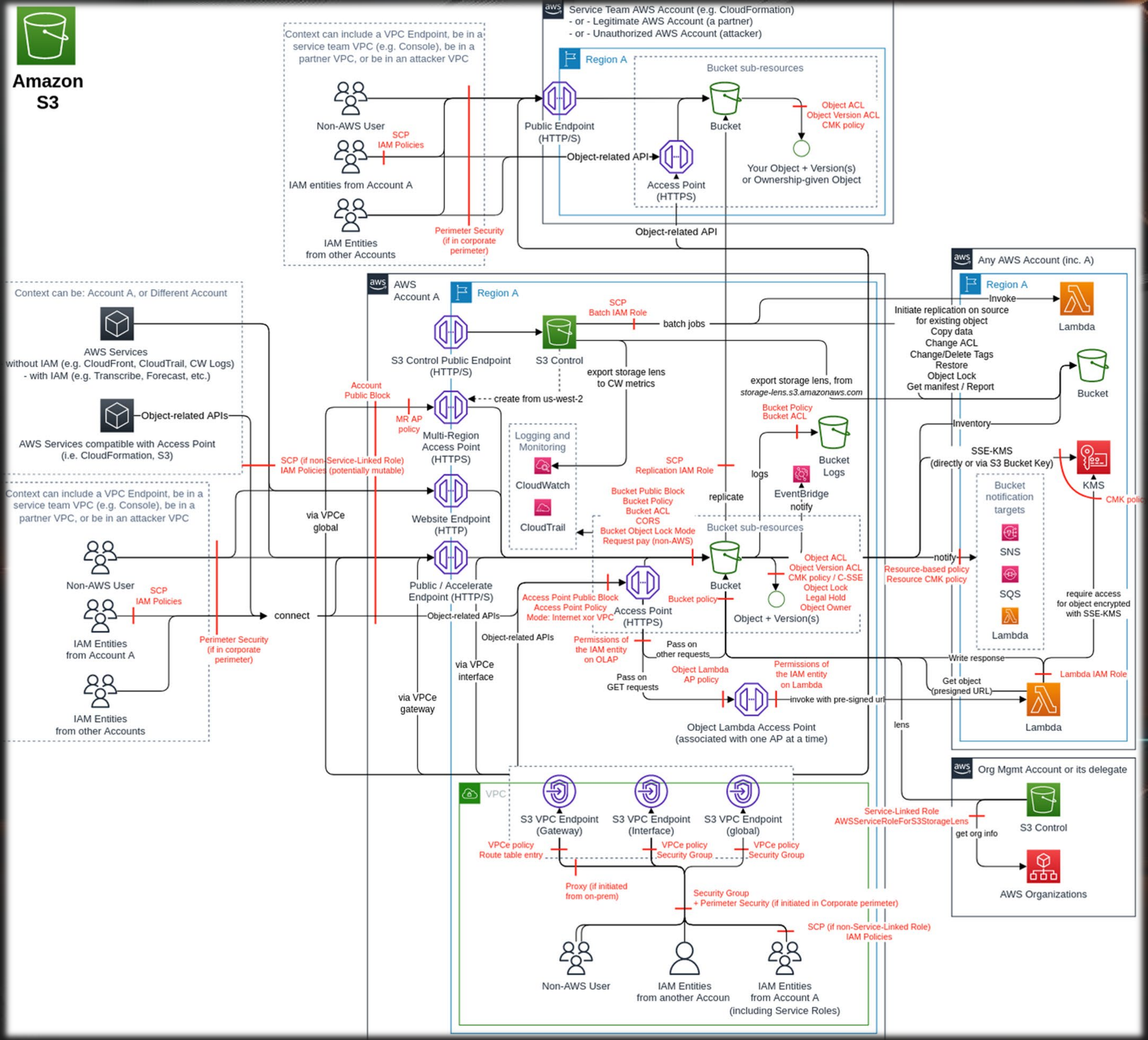
Insecure cloud, container or orchestration configuration



Source: Wiz

Insecure cloud, container or orchestration configuration

CNAS-1

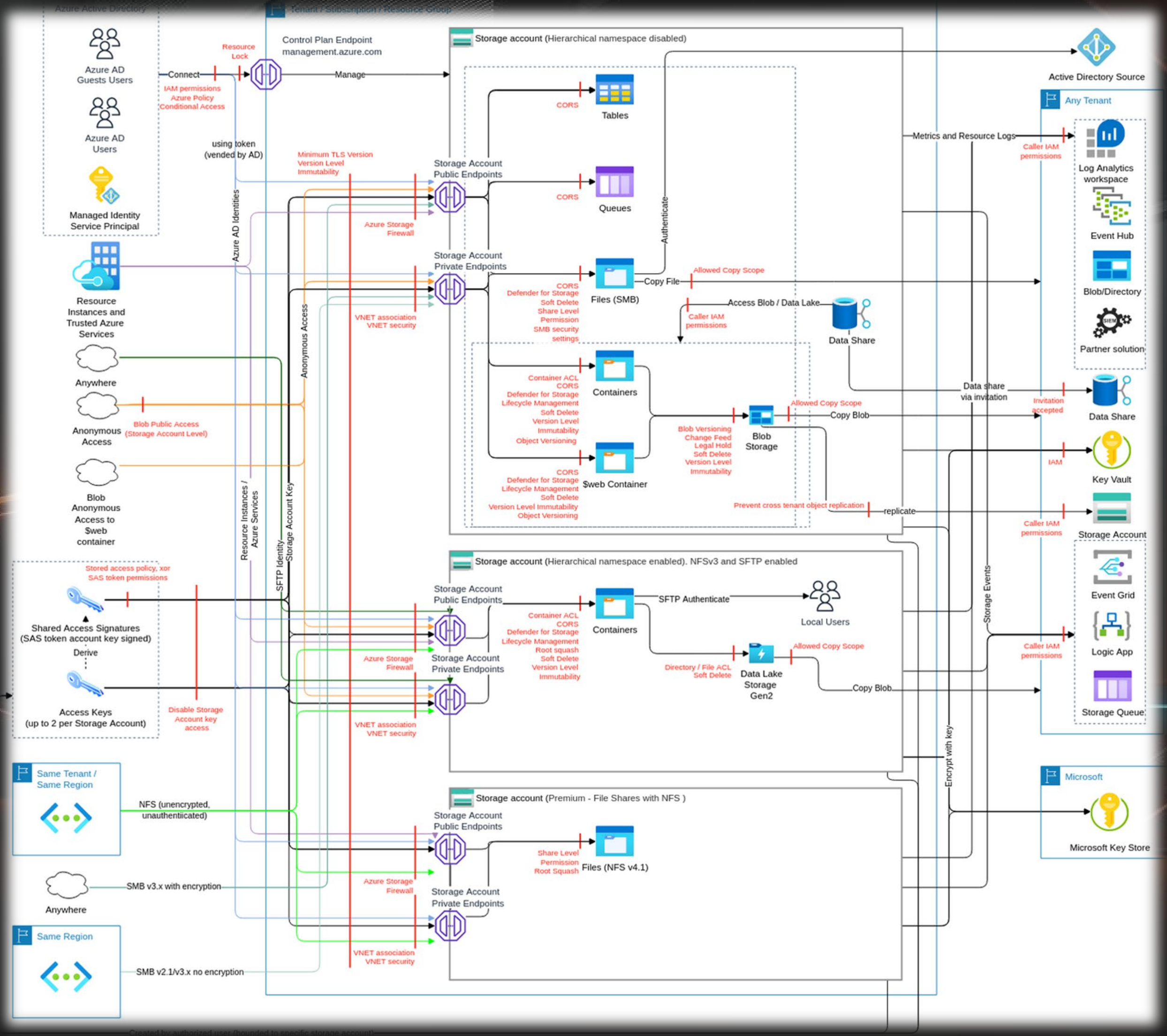


Amazon S3
Context can include a VPC Endpoint, be in a service team VPC (e.g. Console), be in a partner VPC, or be in an attacker VPC
Non-AWS User
SCP
IAM Policies
IAM entities from Account A
IAM Entities from other Accounts
Perimeter Security (if in corporate perimeter)
Service Team AWS Account (e.g. CloudFormation)
- or - Legitimate AWS Account (a partner)
- or - Unauthorized AWS Account (attacker)
Region A
Bucket sub-resources
Public Endpoint (HTTP/S)
Bucket
Object ACL
Object Version ACL
CMK policy
Object-related API
Access Point (HTTPS)
Your Object + Version(s) or Ownership-given Object
Object-related API
Context can be: Account A, or Different Account
AWS Services
without IAM (e.g. CloudFront, CloudTrail, CW Logs)
- with IAM (e.g. Transcribe, Forecast, etc.)
Object-related APIs
AWS Services compatible with Access Point (i.e. CloudFormation, S3)
SCP (if non-Service-Linked Role)
IAM Policies (potentially mutable)
AWS Account A
Region A
SCP
Batch IAM Role
batch jobs
S3 Control Public Endpoint (HTTP/S)
S3 Control
export storage lens to CW metrics
Account Public Block
create from us-west-2
MR AP policy
Multi-Region Access Point (HTTPS)
Logging and Monitoring
CloudWatch
CloudTrail
export storage lens, from storage-lens.s3.amazonaws.com
Bucket Policy
Bucket ACL
Bucket Logs
logs
SCP
Replication IAM Role
replicate
EventBridge notify
Website Endpoint (HTTP)
via VPCe global
Context can include a VPC Endpoint, be in a service team VPC (e.g. Console), be in a partner VPC, or be in an attacker VPC
Non-AWS User
SCP
IAM Policies
IAM Entities from Account A
IAM Entities from other Accounts
Perimeter Security (if in corporate perimeter)
connect
Public / Accelerate Endpoint (HTTP/S)
Object-related APIs
Object-related APIs
via VPCe interface
via VPCe gateway
Bucket Public Block
Bucket Policy
Bucket ACL
CORS
Bucket Object Lock Mode
Request pay (non-AWS)
Bucket sub-resources
Bucket
Object ACL
Object Version ACL
CMK policy / C-SSE
Object Lock
Legal Hold
Object Owner
Object + Version(s)
Bucket policy
Access Point Public Block
Access Point Policy
Mode: Internet xor VPC
Access Point (HTTPS)
Permissions of the IAM entity on OLAP
Pass on other requests
Pass on GET requests
Object Lambda AP policy
Permissions of the IAM entity on Lambda
invoke with pre-signed url
Object Lambda Access Point (associated with one AP at a time)
Any AWS Account (inc. A)
Region A
Invoke
Lambda
Initiate replication on source for existing object
Copy data
Change ACL
Change/Delete Tags
Restore
Object Lock
Get manifest / Report
Bucket
Inventory
SSE-KMS (directly or via S3 Bucket Key)
KMS
CMK polic
Bucket notification targets
SNS
SQS
Lambda
notify
Resource-based policy
Resource CMK policy
require access for object encrypted with SSE-KMS
Write response
Get object (presigned URL)
Lambda IAM Role
Lambda
lens
Org Mgmt Account or its delegate
S3 Control
Service-Linked Role
AWSServiceRoleForS3StorageLens
get org info
AWS Organizations
VPC
S3 VPC Endpoint (Gateway)
S3 VPC Endpoint (Interface)
S3 VPC Endpoint (global)
VPCe policy
Route table entry
VPCe policy
Security Group
VPCe policy
Security Group
Proxy (if initiated from on-prem)
Security Group + Perimeter Security (if initiated in Corporate perimeter)
SCP (if non-Service-Linked Role)
IAM Policies
Non-AWS User
IAM Entities from another Accoun
IAM Entities from Account A (including Service Roles)

Source: TrustOnCloud

Insecure cloud, container or orchestration configuration

CNAS-1

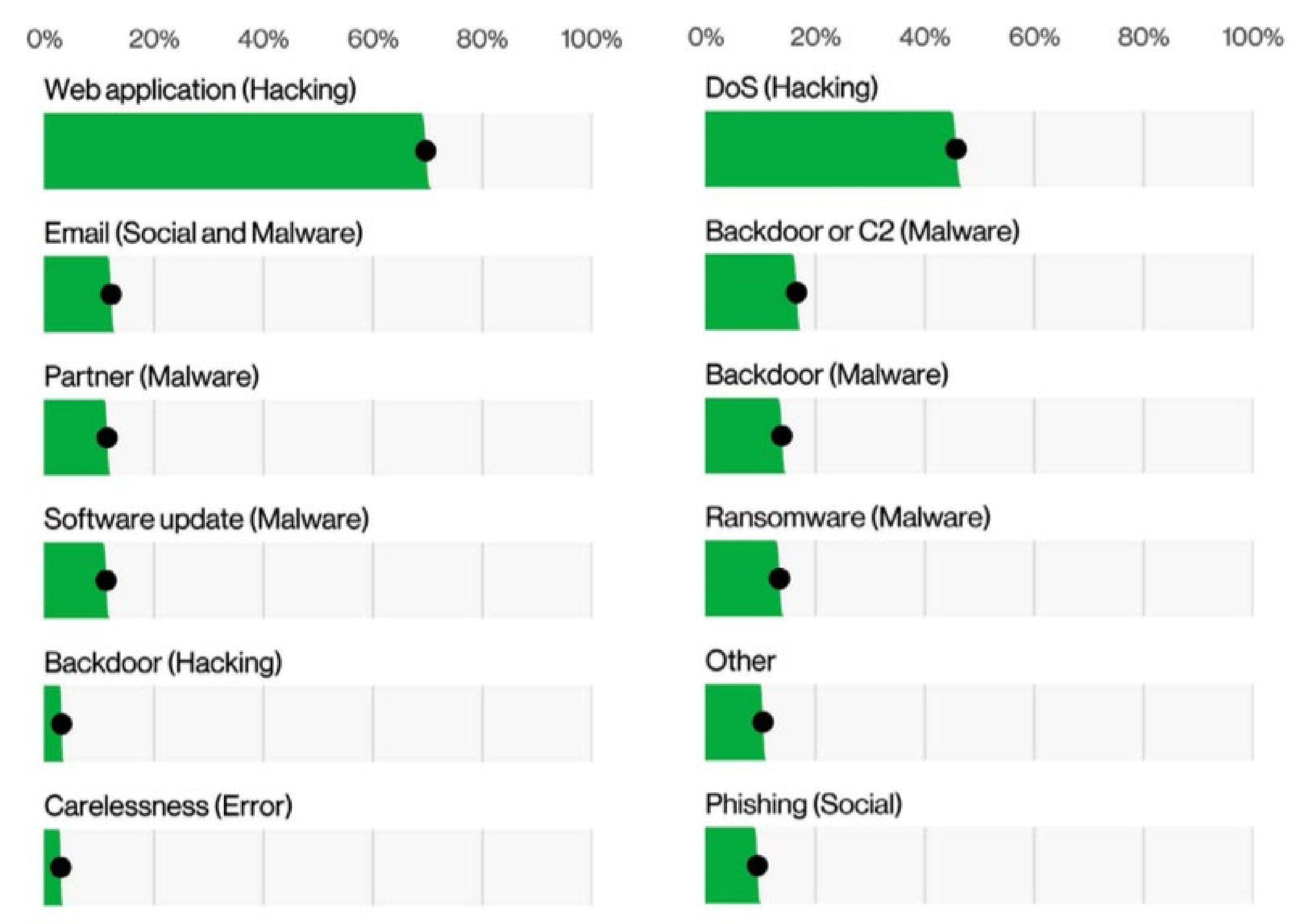


Source: TrustOnCloud

Injection flaws (app layer, cloud events, cloud services)

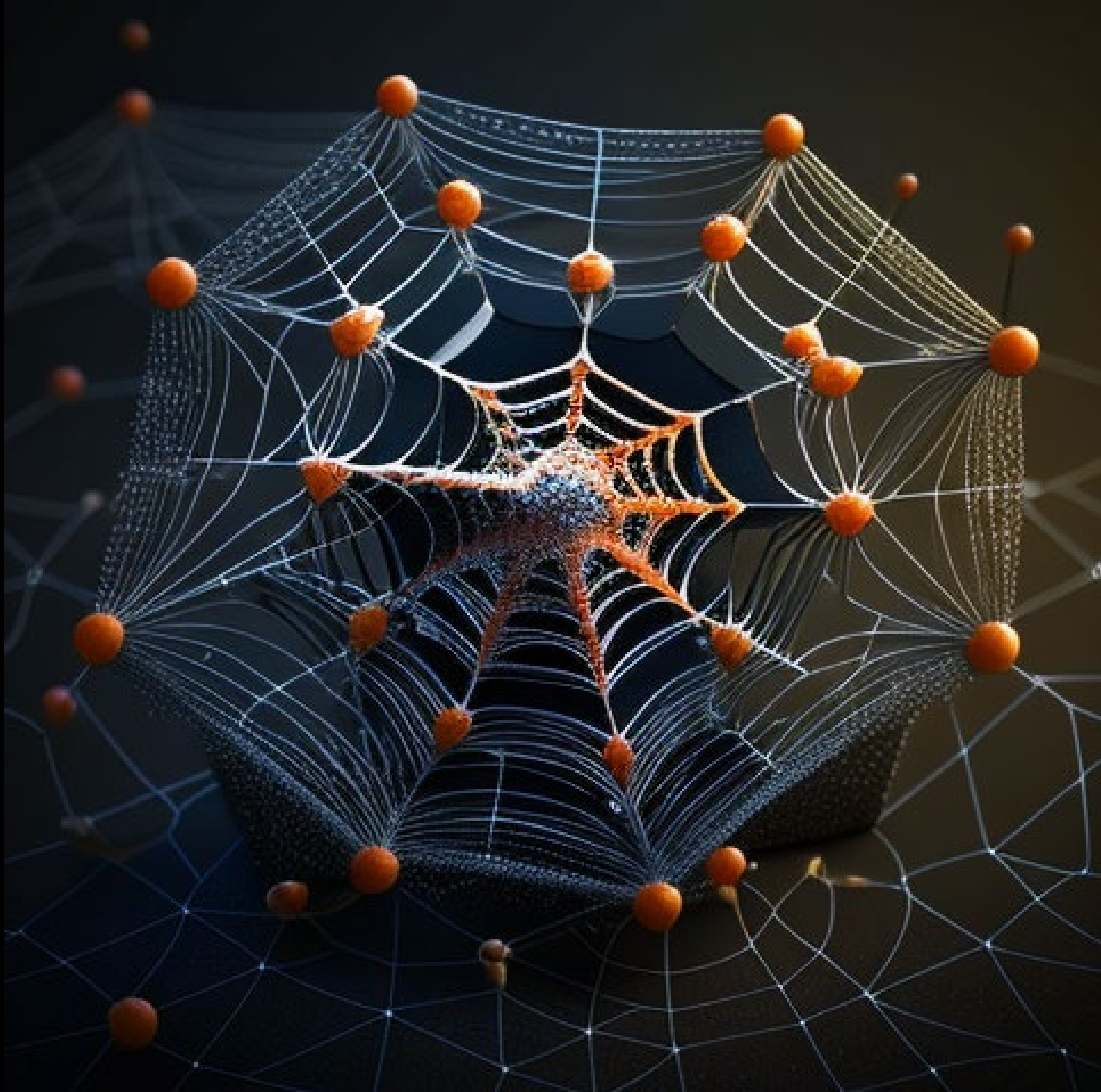
- Closest to OWASP Application Top Ten – A3 Injection

CNAS-2



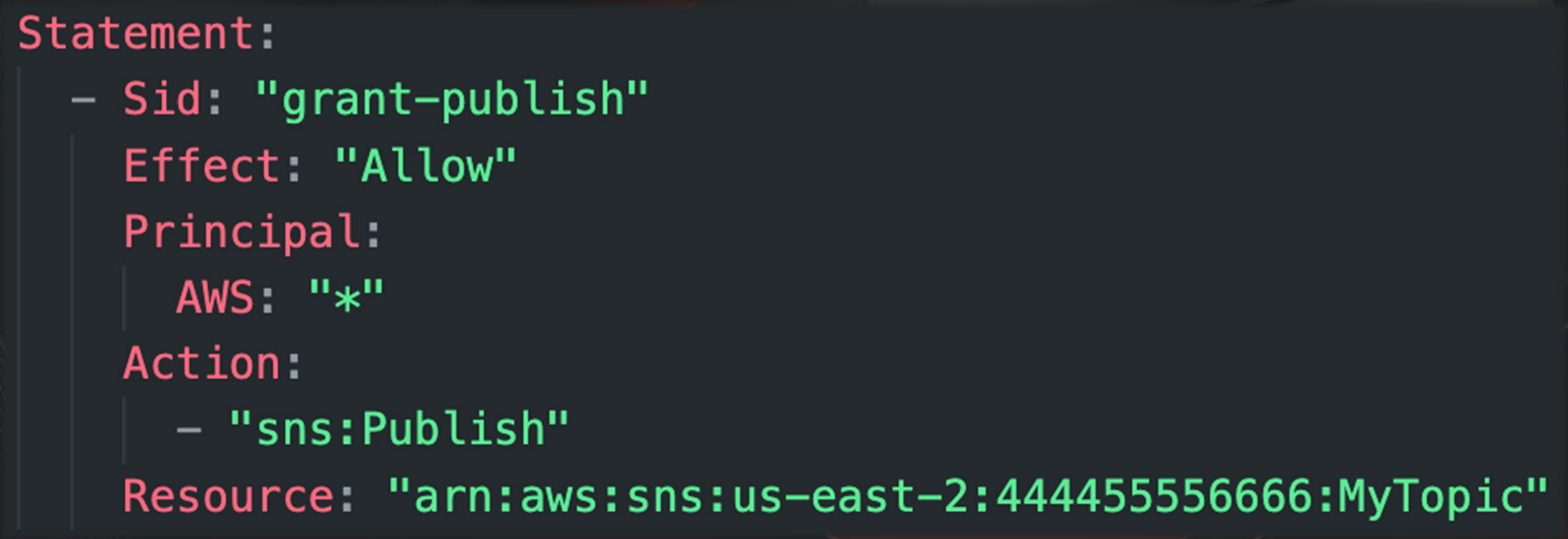
CNAS-3

Improper authentication & authorization



Improper authentication & authorization

CNAS-3

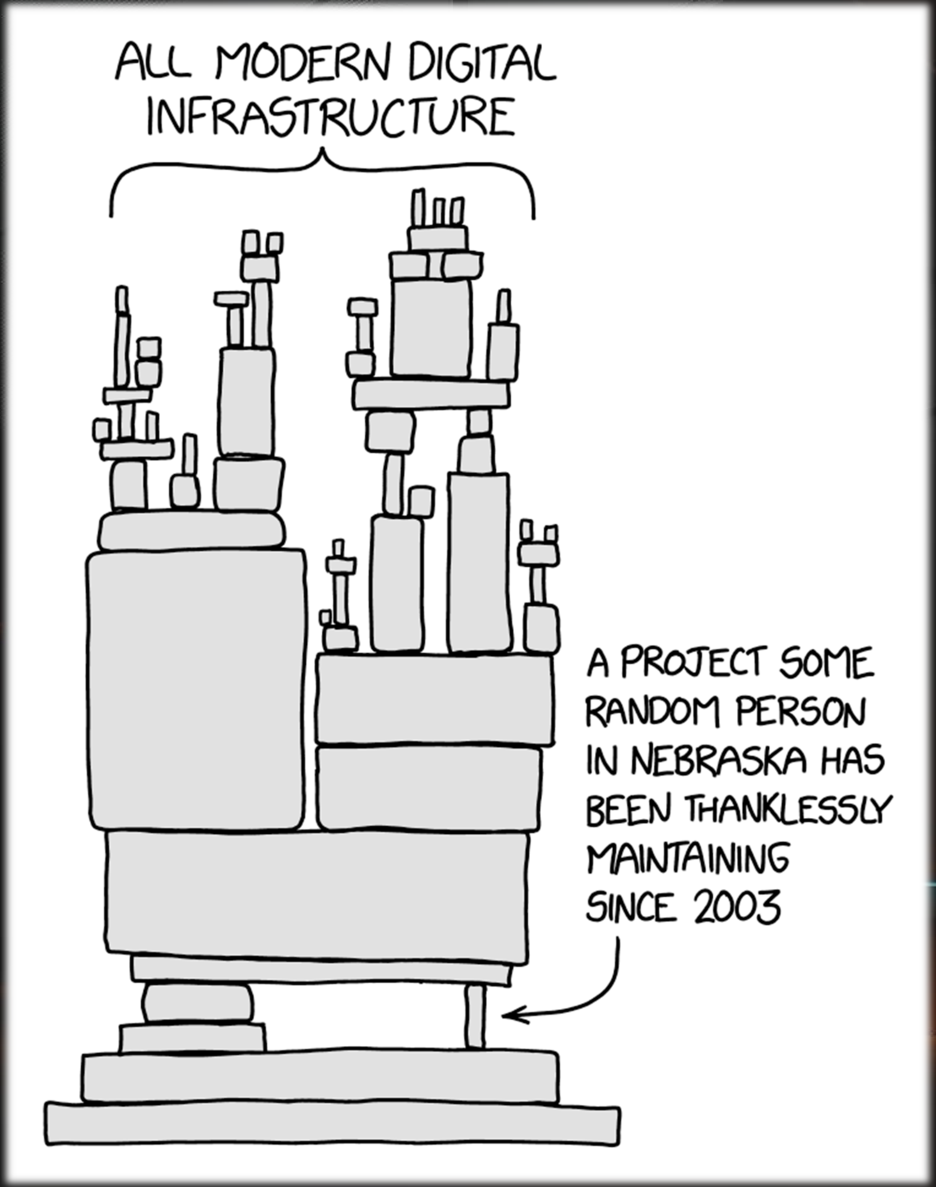


```
Statement:
  - Sid: "grant-publish"
    Effect: "Allow"
    Principal:
      AWS: "*"
    Action:
      - "sns:Publish"
    Resource: "arn:aws:sns:us-east-2:444455556666:MyTopic"
```

CNAS-4

CI/CD pipeline & software supply chain flaws

CNAS-4

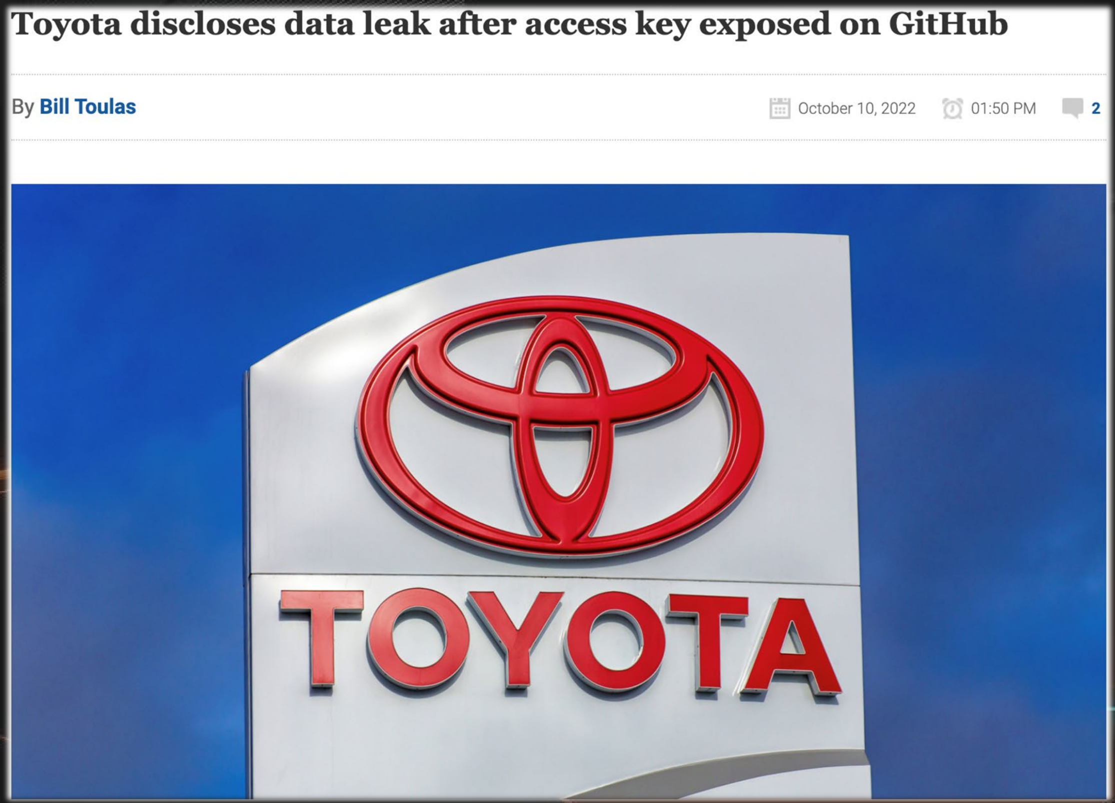

ALL MODERN DIGITAL INFRASTRUCTURE
A PROJECT SOME RANDOM PERSON IN NEBRASKA HAS BEEN THANKLESSLY MAINTAINING SINCE 2003

CNAS-5

Insecure secrets storage

Insecure secrets storage

CNAS-5



Toyota discloses data leak after access key exposed on GitHub

By Bill Toulas October 10, 2022 01:50 PM 2

“Toyota Motor Corporation is warning that customers' personal information may have been exposed after an access key was publicly available on GitHub for almost five years.”

CNAS-6

Over-permissive or insecure network policies

Over-permissive or insecure network policies

CNAS-6

- Networking is hard..
- Complexity at scale
- Egress filtering is very powerful but difficult to maintain

Cisco's law: The level of segmentation of a network is inversely proportional to its size

AKA: Networks become Florida as they scale

CNAS-7

Using components with known vulnerabilities

CNAS-8

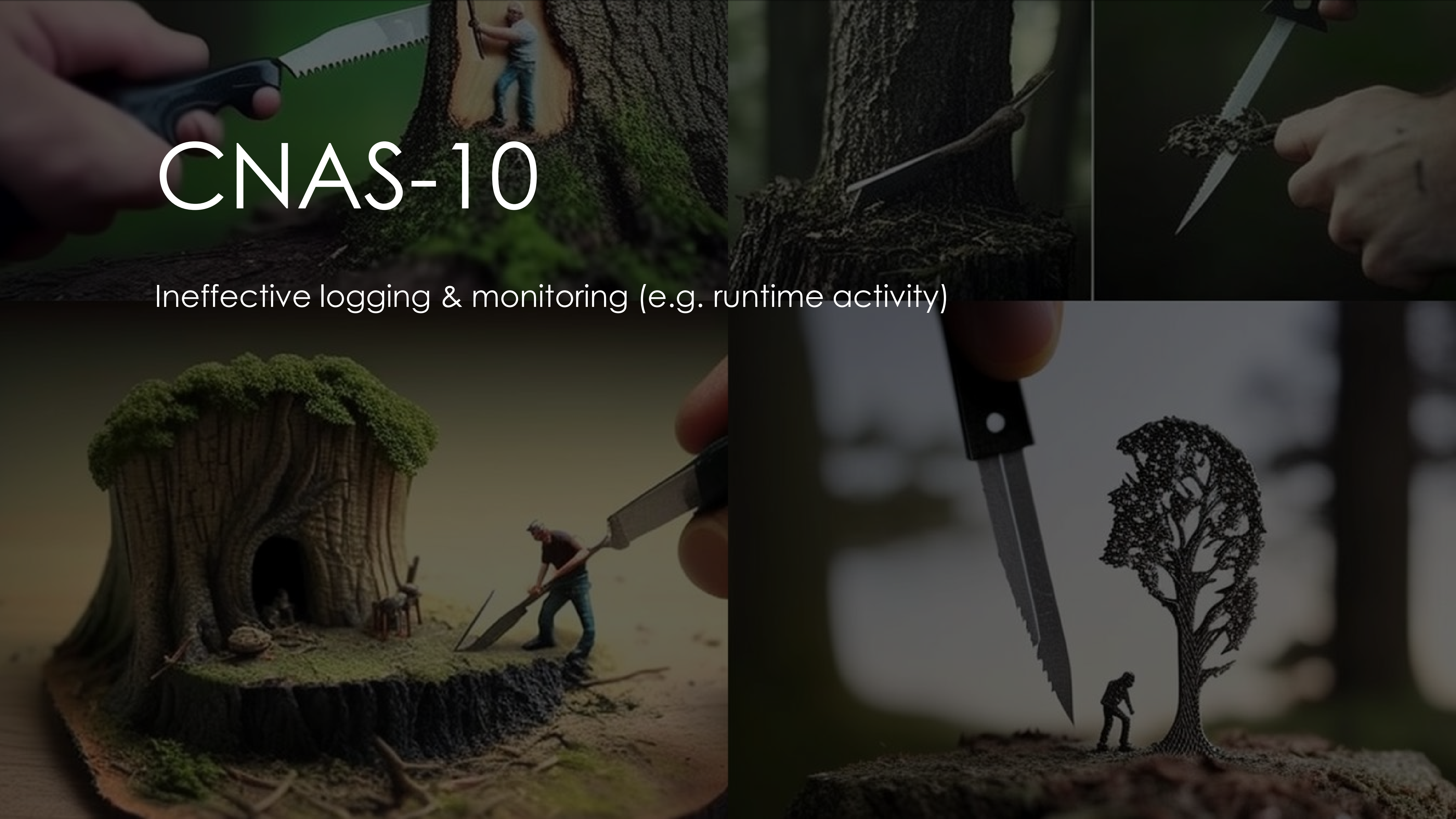
Improper assets management

CNAS-9

Inadequate ‘compute’ resource quota limits

CNAS-10

Ineffective logging & monitoring (e.g. runtime activity)



CONCLUSIONS

- Cloud and web apps have some overlapping concerns
- Cloud native applications have unique threats that should be considered
- No matter the platform we still have the same issues to consider as well
- Your feedback is needed!

- https://owasp.org/www-project-cloud-native-application-security-top-10/

FINAL THOUGHTS

- Do we need another Top Ten? Yes. No. Maybe?
- How can you use it day to day?

QUESTIONS?

- Thanks!
- Cloud Security Partners
- cloudsecuritypartners.com
- mike@cloudsecuritypartners.com

CLOUD SECURITY PARTNERS