Securing the Sky: Strategies for Protecting Against Cloud Hacking

Sena Yakut

aws security HERO

/sena-yakut

@sena_yakutt

senayakut.com

Cloud security: Management nightmare

Cloud providers

Product requirements

Shared responsibilities

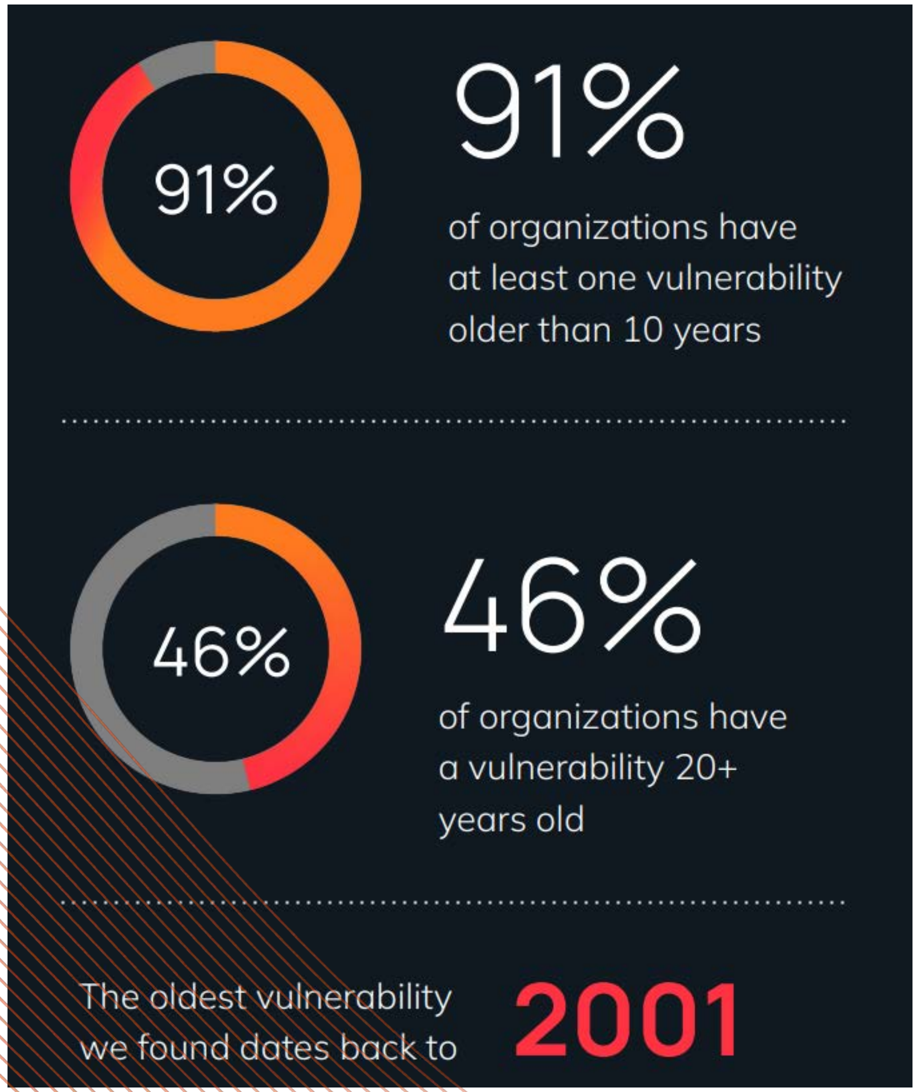
Cloud security: Management nightmare

Cloud resources

Attack surfaces

Tools & Experience

We love the cloud, so attackers do.



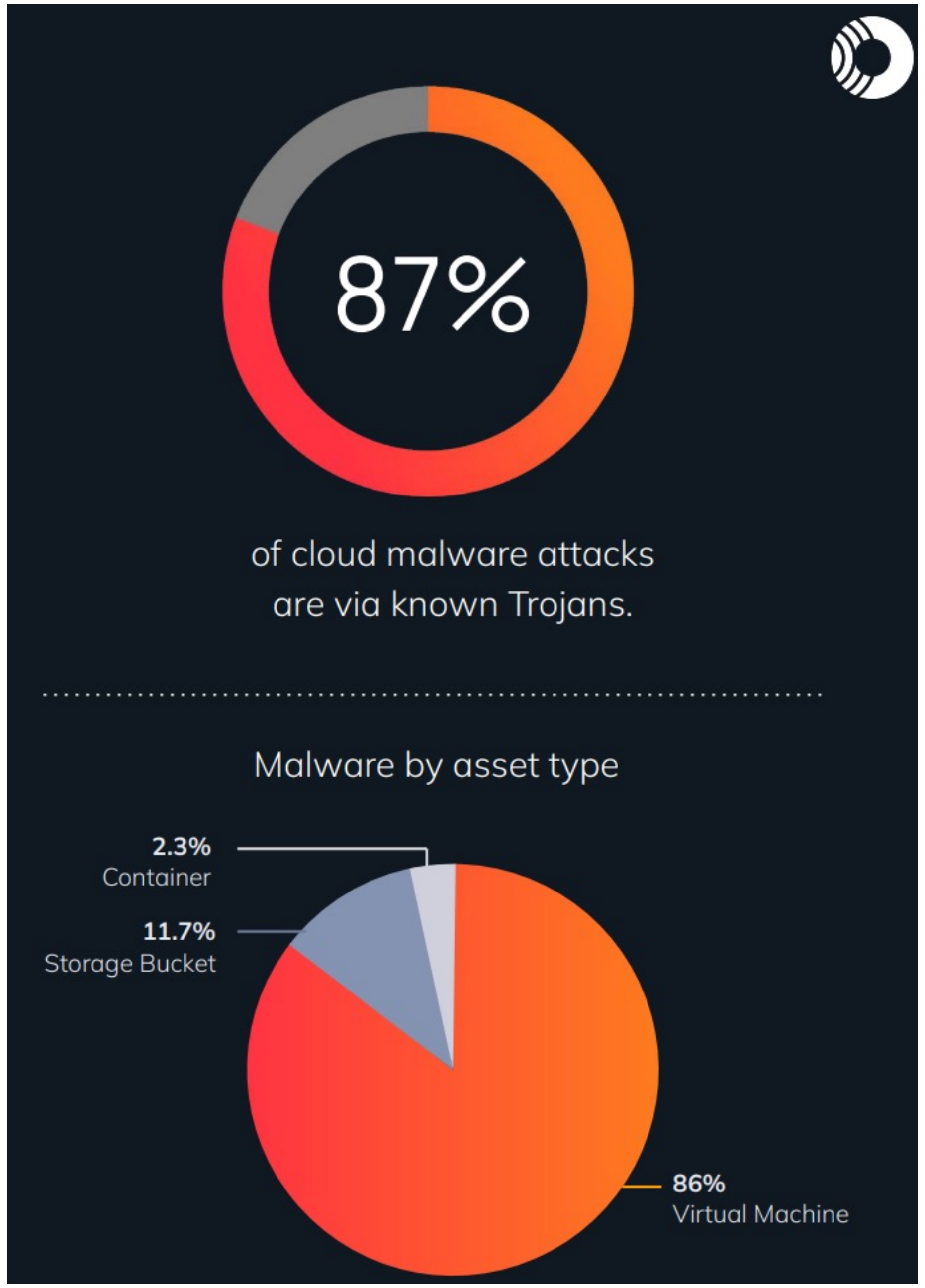
91%

of organizations have at least one vulnerability older than 10 years

46%

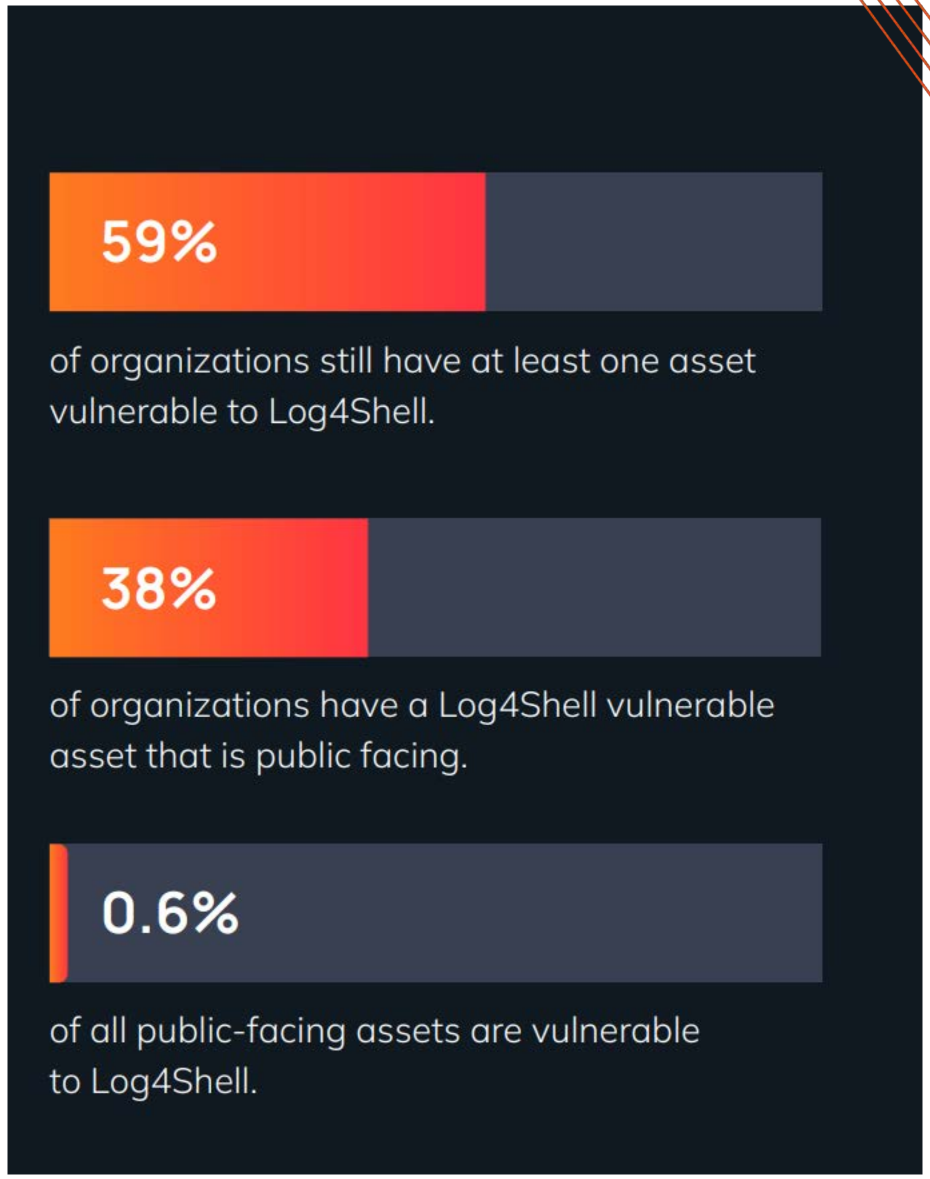
of organizations have a vulnerability 20+ years old

The oldest vulnerability we found dates back to **2001**



of cloud malware attacks are via known Trojans.

Malware by asset type



59%

of organizations still have at least one asset vulnerable to Log4Shell.

38%

of organizations have a Log4Shell vulnerable asset that is public facing.

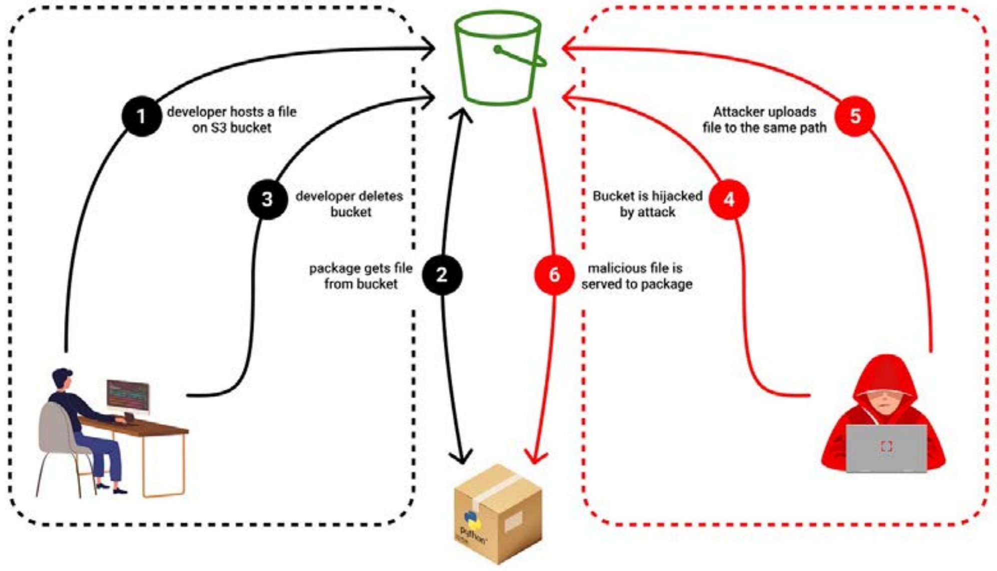
0.6%

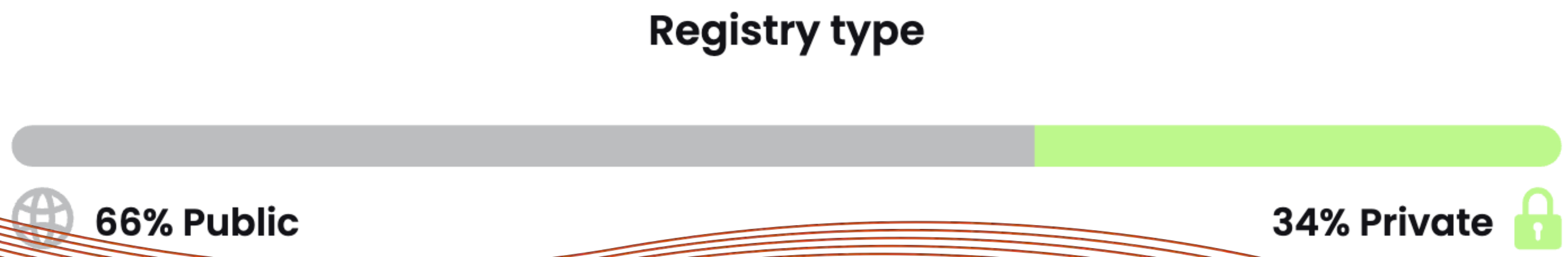
of all public-facing assets are vulnerable to Log4Shell.

Orca Security, 2024 State of Cloud Security Report

Do not use public resources unless you really really need.

- Storage resources (Azure Blob, AWS S3, EBS, EFS),
- Exposed sensitive data,
- Container registries –> Getting credentials from it,
- Write to public resources & destroy environments,
- Denial of Wallet amplification attack –> AWS S3,
- Publicly accessible databases,
- Amazon SageMaker publicly accessible notebooks.

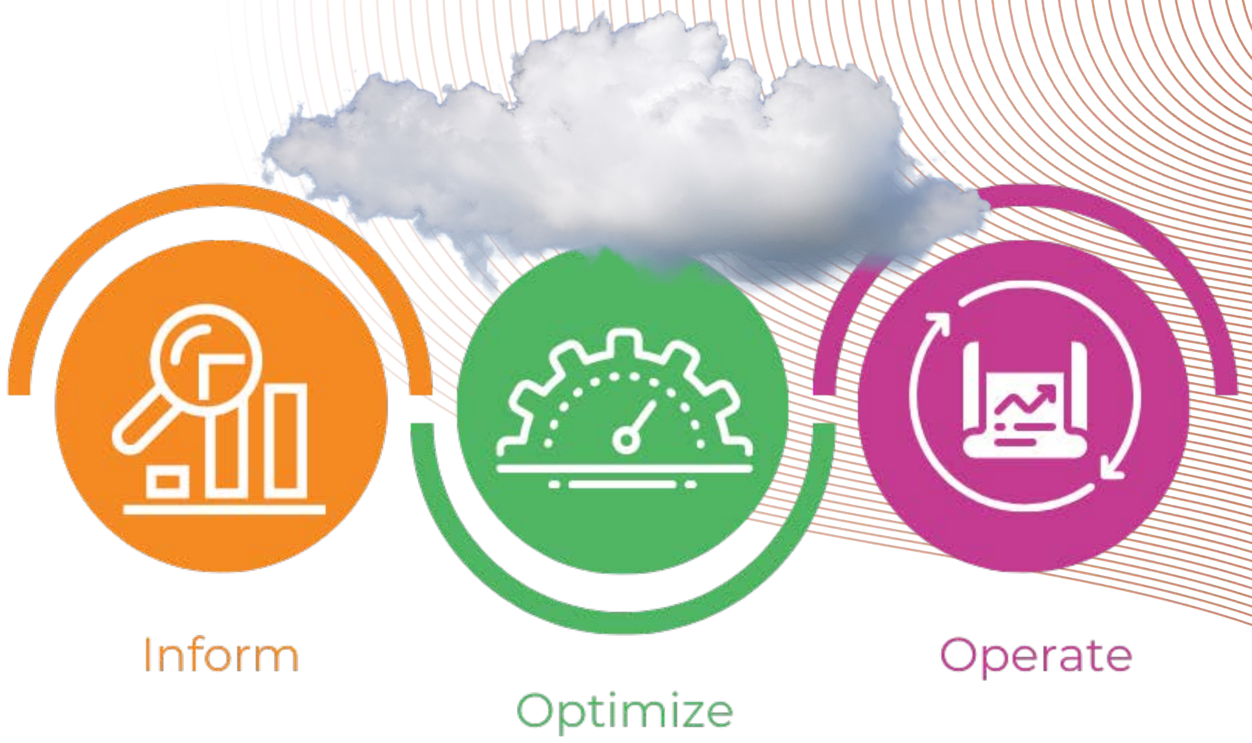

1 developer hosts a file on S3 bucket
2 package gets file from bucket
3 developer deletes bucket
4 Bucket is hijacked by attack
5 Attacker uploads file to the same path
6 malicious file is served to package
Python



Sysdig, 2024 State of Cloud Security Report

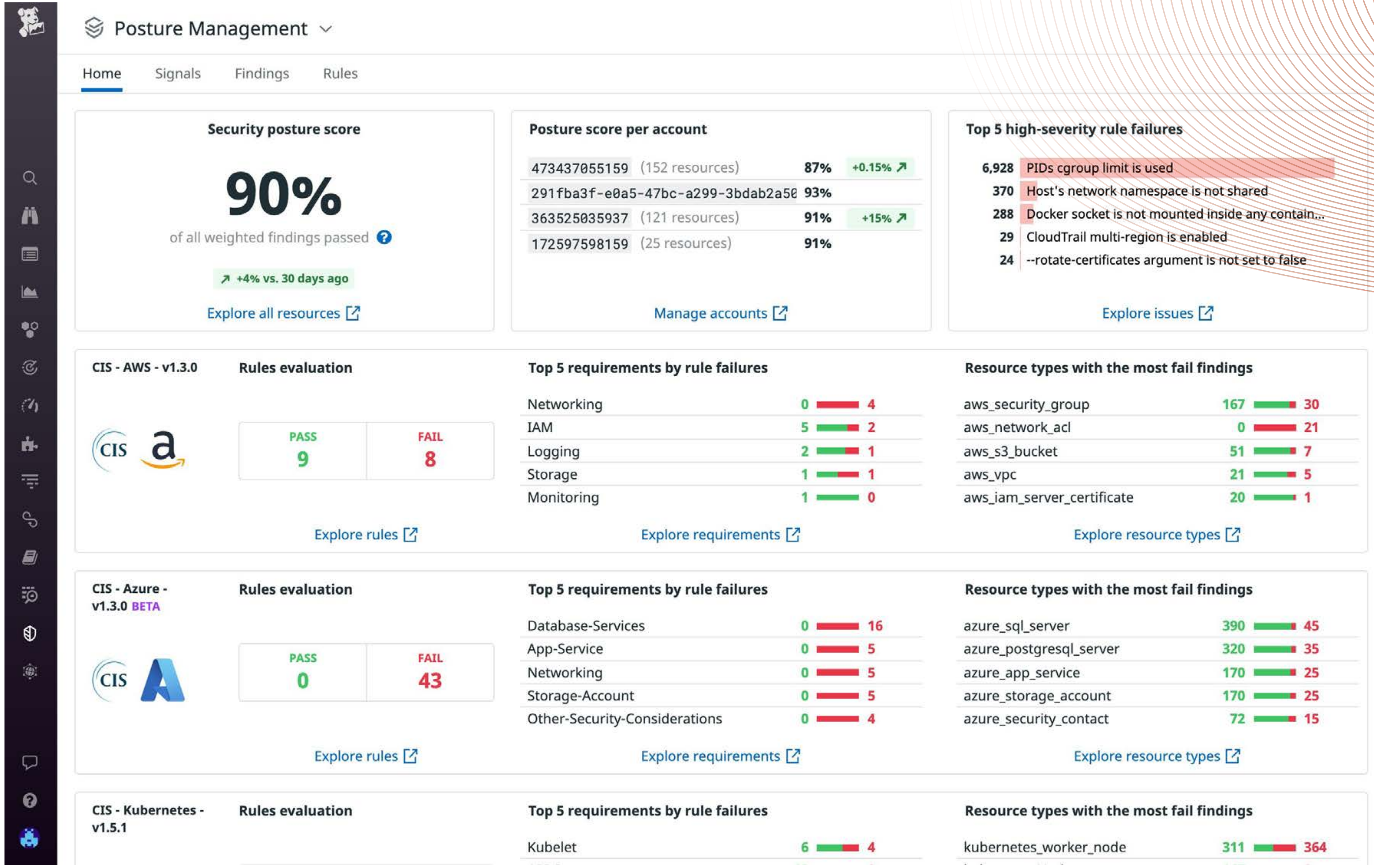
Be aware of your resources.

- Which resources, where and why?
- What are the possible vulnerabilities?
- What are the misconfigurations?
- What are the endpoints?



Be aware of your resources.

CSPM is not enough, but it is a good start.



Posture Management

Security posture score

90%

of all weighted findings passed

↗ +4% vs. 30 days ago

Explore all resources

Posture score per account

473437055159	(152 resources)	87%	+0.15% ↗
291fba3f-e0a5-47bc-a299-3bdab2a50		93%	
363525035937	(121 resources)	91%	+15% ↗
172597598159	(25 resources)	91%	

Manage accounts

Top 5 high-severity rule failures

6,928	PIDs cgroup limit is used
370	Host's network namespace is not shared
288	Docker socket is not mounted inside any contain...
29	CloudTrail multi-region is enabled
24	--rotate-certificates argument is not set to false

Explore issues

CIS - AWS - v1.3.0

Rules evaluation

PASS	FAIL
9	8

Explore rules

Top 5 requirements by rule failures

Networking	0	4
IAM	5	2
Logging	2	1
Storage	1	1
Monitoring	1	0

Explore requirements

Resource types with the most fail findings

aws_security_group	167	30
aws_network_acl	0	21
aws_s3_bucket	51	7
aws_vpc	21	5
aws_iam_server_certificate	20	1

Explore resource types

CIS - Azure - v1.3.0 BETA

Rules evaluation

PASS	FAIL
0	43

Explore rules

Top 5 requirements by rule failures

Database-Services	0	16
App-Service	0	5
Networking	0	5
Storage-Account	0	5
Other-Security-Considerations	0	4

Explore requirements

Resource types with the most fail findings

azure_sql_server	390	45
azure_postgresql_server	320	35
azure_app_service	170	25
azure_storage_account	170	25
azure_security_contact	72	15

Explore resource types

CIS - Kubernetes - v1.5.1

Rules evaluation

Top 5 requirements by rule failures

Kubelet	6	4

Resource types with the most fail findings

kubernetes_worker_node	311	364

Please read the documentation.

- The following documentation ensures that security features are configured correctly,
- Maximizing protection against threats,
- Cloud engineers are updated on new security features and best practices,
- Maximizing the use of documentation minimizes reliance on external support, saving time and resources.

Get alert from everything you need.

- Anomalies,
- Cloud resource threats,
- Cloud resources configuration changes,
- Verify alerts and get details from it,
- Have a plan for alerts.

Monitor everything.

- Constant monitoring enables early detection of suspicious activities or anomalies.
- Timely monitoring allows for rapid response to security incidents.
- Monitoring provides valuable insights into emerging threats and attack patterns.
- Monitoring resource usage helps control costs and prevent unnecessary expenses.

Dance like no one is watching. Encrypt like everyone is.

- Encrypt in transit,
- Encrypt in rest,
- Follow best practices in the encryption stage,
- Follow up cyber security world for encryption changes

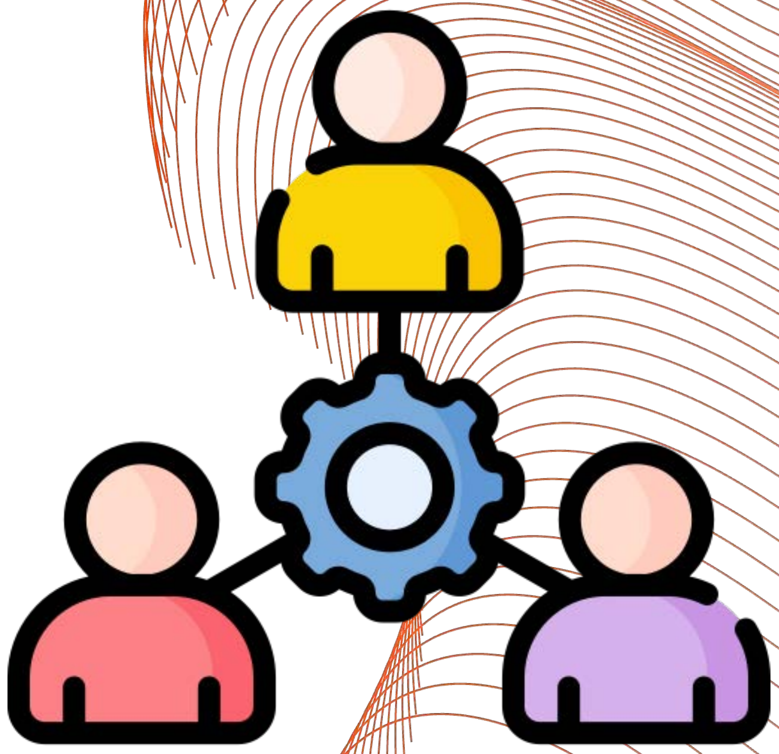
Be open to change.

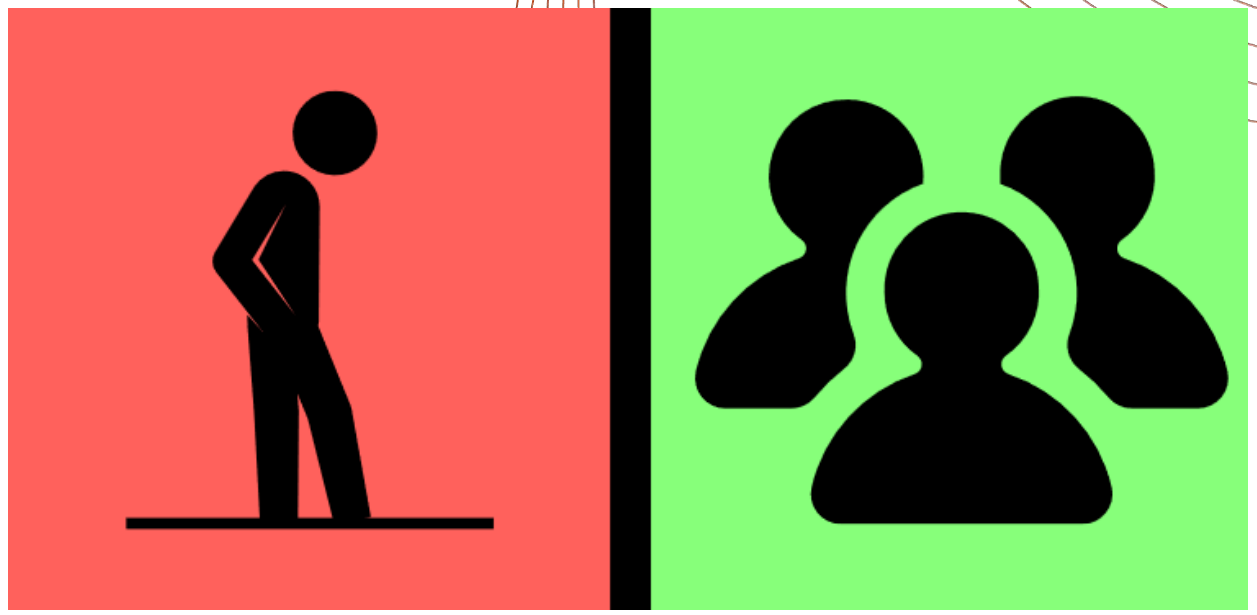
“The most dangerous phrase in the English language is: **‘We’ve always done it this way…’**”

– REAR ADMIRAL GRACE HOPPER

Do not isolate teams.

- Everyone needs security,
- Each team brings unique skills and perspectives to the table,
- Improved visibility across teams helps identify and address security risks more effectively,
- Avoid duplication of efforts and resources,





Think ‘what if’

- Consider potential scenarios and their impacts on cloud security posture,
- Identify vulnerabilities and weaknesses before they can be exploited,
- Use 'what if' scenarios to drive ongoing security enhancements and updates,
- Evaluate how different scenarios may affect regulatory compliance and take necessary precautions.

Thanks!

/sena-yakut

@sena_yakutt

senayakut.com