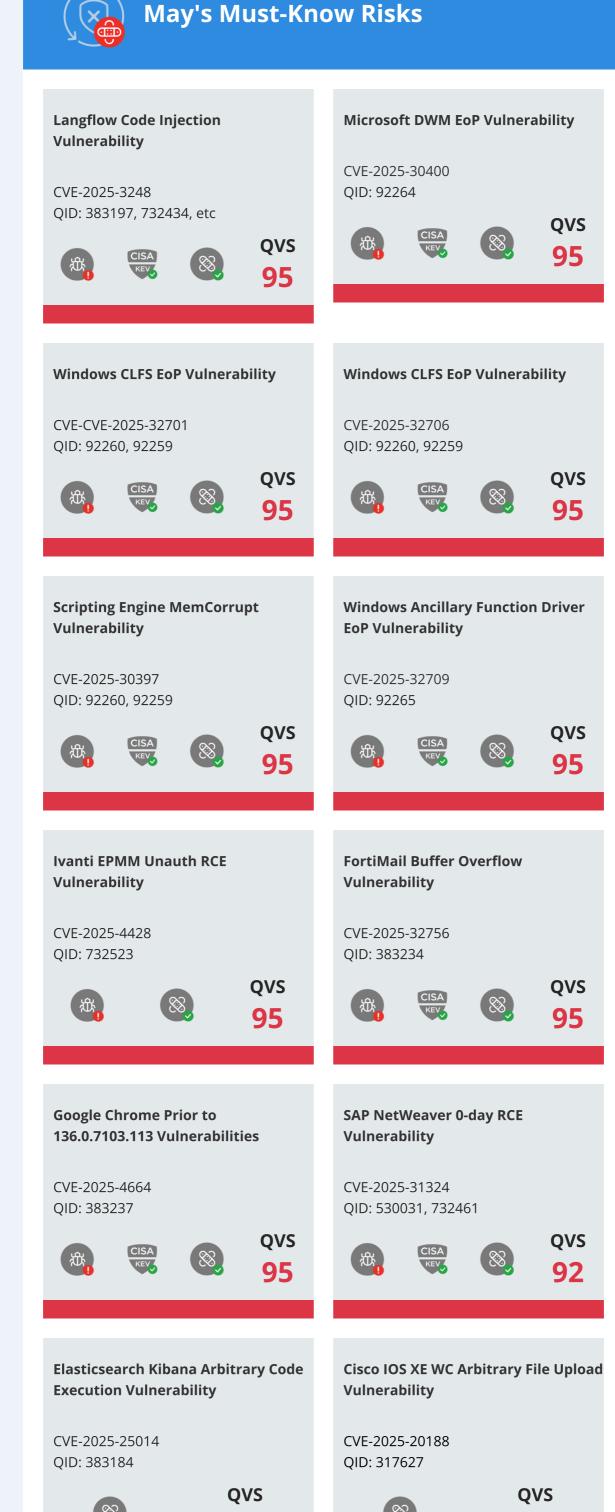




cyber risk—before it escalates into a crisis.

Measure, communicate, and eliminate your



**Cloud Security Snapshot: Key** 

Misconfigurations

before it's too late.

Misconfiguration

Misconfiguration

Spanner databases

instances

passwords

groups

For more in-depth knowledge and details, visit **Qualys ThreatPROTECT** page and

These vulnerabilities pose significant risks to your systems. To understand

and address these critical threats, get your **personalized TruRisk Report**.

Contact your Technical Account Manager today to get yours.

subscribe to receive the latest updates on threats and vulnerabilities.

65

Unveiled by our expert analysts: the top risk combinations threatening your cloud today. Discover critical cybersecurity dangers facing your organization

(%)

57.25%

5.12%

94.88%

14.48%

1.22%

Resources

99.80%

100.00%

99.44%

99.25%

99.16%

Affected (%)

and master the strategies to neutralize them. Act fast—secure your cloud

**Amazon Web Services (AWS)** Resources Affected

**Enable MFA for all IAM users with console** 

Restrict SSH (port 22) from 0.0.0.0/0 in security

Avoid attaching wildcard (:) IAM admin policies

**Enable Confidential Computing on Compute** 

**Use Customer Managed Encryption Keys for** 

Set object retention policy on storage buckets

Turn on deletion protection for VM instances

**Enable sandboxing on GKE clusters** 

**Enable CloudTrail in all regions** 

**Monitor unauthorized API calls** 

Microsoft Azure	
Misconfiguration	Resources Affected (%)
Encrypt OS and data disks with Customer Managed Keys (CMK)	93.97%
Disallow public Blob access on storage accounts	29.43%
Disable public network access for storage accounts	91.19%
Configure Network Policies on AKS clusters	39.59%
Enable Azure Defender for Kubernetes	85.08%
Google Cloud Platform (GCP)	

Oracle Cloud Infrastructure (OCI)		
Misconfiguration	Resources Affected (%)	
Encrypt DB Systems databases with CMK	100.00%	
Encrypt boot volumes with CMK	97.98%	
Rotate Customer Secret Keys every 90 days or less	97.56%	
Set IAM password minimum length to 14+ characters	96.33%	
Configure Event Rule for NSG (network security group) changes	95.41%	
<b>Note:</b> Percentages reflect how many resources across all customers, have these misconfigurations.		

risks and provides actionable steps to remediate them. Contact your Technical Account Manager today to get your personalized report and secure your cloud.

**Inside LockBit: Defense Lessons from** 

the Leaked LockBit Negotiations

A rare breach has turned the tables on one of the world's most notorious

These misconfigurations pose significant risks to your cloud. To

understand and address these critical issues, get your Cloud TruRisk

**Insight Report**. This report identifies which misconfigurations are causing

<u>In this detailed analysis blog post</u>, the Qualys Threat Research Unit explores: How LockBit's tactics have evolved? • Which vulnerabilities they routinely exploit?

ransomware groups—LockBit. With over 4,000 leaked negotiation transcripts and

tens of thousands of cryptocurrency addresses exposed, defenders now have a

unique window into the inner workings of a major cybercriminal operation.

From targeting patterns to cryptocurrency preferences, this leak reveals critical intelligence that security teams—from CISOs to SOC analysts—can use to

strengthen defenses, fine-tune response strategies, and close gaps before they're

exploited. This blog post offers actionable insights and a rare chance to learn directly from

Defense lessons from the LockBit ransomware playbook

What drives their negotiation strategy?

the adversary's own words. For a deep dive into understanding this ransomware, visit our blog.

Stay protected by leveraging Qualys' comprehensive vulnerability detection and management.

Reach out to your Technical Account Manager today to discuss the

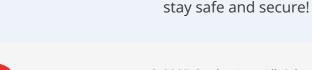
fastest ways to remediate these critical risks and strengthen your security posture. Don't wait—proactive steps now can prevent costly breaches later.

Thank you

for being part of our May newsletter! We hope these insights empower you to

enhance your security posture. Get ready for next month's edition, filled with the latest updates and expert threat research tips.

We value your input—what topics would you like us to explore next? Drop us a line anytime at <a href="mailto:researchNewsletter@qualys.com">researchNewsletter@qualys.com</a>. Until then,



Qualys.

© 2025 Qualys, Inc. All rights reserved. Privacy Policy. Accessibility. Notice at Collection. Trust. Cookie Consent.