

CSA

Bangalore
Chapter

**CLOUD SECURITY
SUMMIT 2024**

Enhancing CSPM for robust cloud defence

Chandrapal Badshah &
Pranav Raghuram

Speaker Profile



Pranav Raghuram

Security Architecture & Engineering
Vice President, State Street

Pranav Raghuram is a seasoned expert in cloud engineering and security, bringing over 17 years of experience in multi-cloud engineering, security and operations.
Linkedin: www.linkedin.com/in/pranav-raghuram-626571222



Chandrapal Badshah

Cloud Security Consultant
Cloud Security Club

Chandrapal Badshah has over 5 years of experience as cloud security engineer securing FinTech multi-cloud environments.
Linkedin: <https://www.linkedin.com/in/bnchandrapal>



What is **CSPM**?

- **Cloud Security Posture Management**
- **Continuously detect and remediate misconfigurations in cloud environments**
- **Automate visibility, continuous drift monitoring, threat detection and remediation are key features**
- **Provides basic CWPP, CDR, CIEM checks while supporting integration with their full-featured versions**

Why CSPM?

Thomson Reuters collected and leaked at least 3TB of sensitive data

Updated on: November 03, 2022 8:14 AM

Vilnius Petkauskas, Deputy Editor




Image by Shutterstock.

Thomson Reuters, a multinational media conglomerate, left an open database with sensitive customer and corporate data, including third-party server passwords in plaintext format. Attackers could use the details for a supply-chain attack.

- Media giant with \$6.35 billion in revenue left at least three of its databases open
- At least 3TB of sensitive data exposed including Thomson Reuters plaintext passwords to third-party servers

Partner content

Hostinger's AI Website Builder for WordPress will build you a site from a single prompt

by Partner content by a third-party

Editor's choice

Why are subsea cables allegedly being tampered with, and what impact does it have on us all?

by Chris Stokel-Walker

Pegasus Airline breach sees 6.5TB of data left in unsecured AWS bucket

An unsecured cloud data store has left vital information from the airline's software exposed online.

Claudia Glover June 1, 2022

<https://cloudsecurityalliance.org/blog/2024/11/26/what-can-we-learn-from-recent-cloud-security-breaches#>

Summary of major incidents:

In May, Software giant **Snowflake** was made aware of a cyber incident. Initially it was thought that the attackers sought to hack Snowflake itself, but it was later discovered that they were really after Snowflake clients. More than 160 were targeted, including Santander Bank, online ticket sales platform TicketMaster, Pure Storage, Advance Auto Parts, and AT&T.

In early June, Russian Ransomware group Qilin attacked **Synnovis**, a healthcare partner that provides pathology services to several London-based hospital trusts. The attack crippled their IT systems, resulting in interruptions to many of its pathology services. The impact was wide, and hospitals and clinics had a great deal of difficulty in providing urgent services, which resulted in thousands of cancelled and delayed operations and appointments. Later that same month, **CDK Global**, a US-based software company that serves more than 15,000 car dealerships across the nation and accounts for more than half of US auto sales, suffered 2 subsequent cyber-attacks by hacking group BlackSuit. The IT systems were severely impacted, and thousands of auto dealerships were without access to the critical functions including: Sales Management, Inventory Management, Customer Relationship Management (CRM), Service and Repair Management, Finance and Insurance (F&I), Digital marketing, Data analytics, and Backoffice operations (including accounting, payroll, and human resources). The total damage of these attacks is estimated to be billions of dollars.

These are the primary factors that allowed these attacks:

- 1. Credential theft and trade:** Some of the attacks were conducted using credentials which were stolen through infostealing malware and hacking groups (including VIDAR, RISEPRO, REDLINE, RACON STEALER, LUMMA and METASTEALER).
- 2. Aging credentials which has gone years without an update:** Organizations have not purged systems of older credentials. They were completely unaware that these credentials were still valid and worse yet, were stolen. In some cases, the credentials had not been revoked or updated years after theft.
- 3. Reliance on credentials only, without utilizing "allow lists" or MFA:** Organizations were not implementing "allow lists" to enable access only from specific locations, IP addresses and domain URLs, making the use of stolen credentials easier. The impacted accounts were not configured with multi-factor authentication, meaning successful authentication only required a valid username and password.
- 4. Reliance 3rd party software and services:** The hospitals' reliance on Synnovis for the pathology

Effective CSPM Implementation



01

Cloud Asset Discovery

Ingestion of asset data is the prerequisite for effective CSPM implementation

02

Define Hardening Baselines

Each cloud service needs to have a well defined prescriptive hardening baseline document for secure configurations

03

Easy Customization

Able to easily write custom controls/queries for the hardening baselines

04

Time Based Alert Snooze

Alert rules for misconfigurations need to be snoozed only for the approved exception time period

Effective CSPM Implementation



05

Attack Surface Mapping

Identify risk path based on the affected resource and its relationship to other entities

06

Compliance Assessment

Map baselines against compliance framework to arrive at overall compliance score

07

Single Pane of Glass

Effective analytical view to easily understand the security posture of multi cloud accounts

08

Incident Response Support

Enable cloud incident response team to triage, quarantine and remediate

Thank You!

