Securing Cloud-Native Applications:

Top 5 Risks and How to Mitigate Them

A S M Shamim Reza

TheTeamPhoenix
Machine Secures Machines

[~]$whoami

A S M Shamim Reza

– Founder, ***TheTeamPhoenix***

– SME & CT at ***APNIC, Australia***

– ex-CTO & CISO, ***Pipeline Inc. Japan***

– 12+ years, worked for ***Link3 Technologies Limited***

– PC Member, AI & Data Foundation, ***Open Source Summit - North America***

– PC Member, bdNOG, btNOG, npNOG

@asmshamimreza on **Linkedin**
@shamimrezasohag on **Twitter**
@ShamimRezaCNB on **Facebook**

CLOUD SECURITY STATISTICS

Preventing cloud misconfigurations was **the top security priority** for over half of companies in 2023.

80% of companies were **affected by cloud security incidents** in the past year.

More than

60% of organizations experienced security **incidents related to public cloud** usage in 2024.

of all data breaches result from **human error**.

In 2024, phishing was the most prevalent cloud security breach, **affecting 73% of organizations**.

72% of security professionals surveyed reported **underlying infrastructure compromise** as a **key concern**.

** Stat Credit: https://spacelift.io/

TheTeamPhoenix
Machine Secures Machines

Cloud Security – Major Attack

CircleCI Supply Chain Attack (2023) – Compromised CI/CD Pipeline Credentials

🔴 Attack Type: Cloud CI/CD Supply Chain Attack

🔴 Target: CircleCI (Popular DevOps CI/CD Platform)

🔴 Impact: Attackers stole API keys & secrets for thousands of companies using CircleCI, including AWS, GitHub, and Google Cloud credentials.

What Happened?

In January 2023, attackers breached CircleCI's cloud-based CI/CD platform, leading to a supply chain compromise affecting thousands of developers and major enterprises.

Attack Breakdown:

- Compromising CircleCI's Internal System
- Stealing Secrets & API Keys
- Customer Impact & Incident Response

OWASP top 10 CNAS (Cloud-Native Application Security) Risks

TheTeamPhoenix
Machine Secures Machines

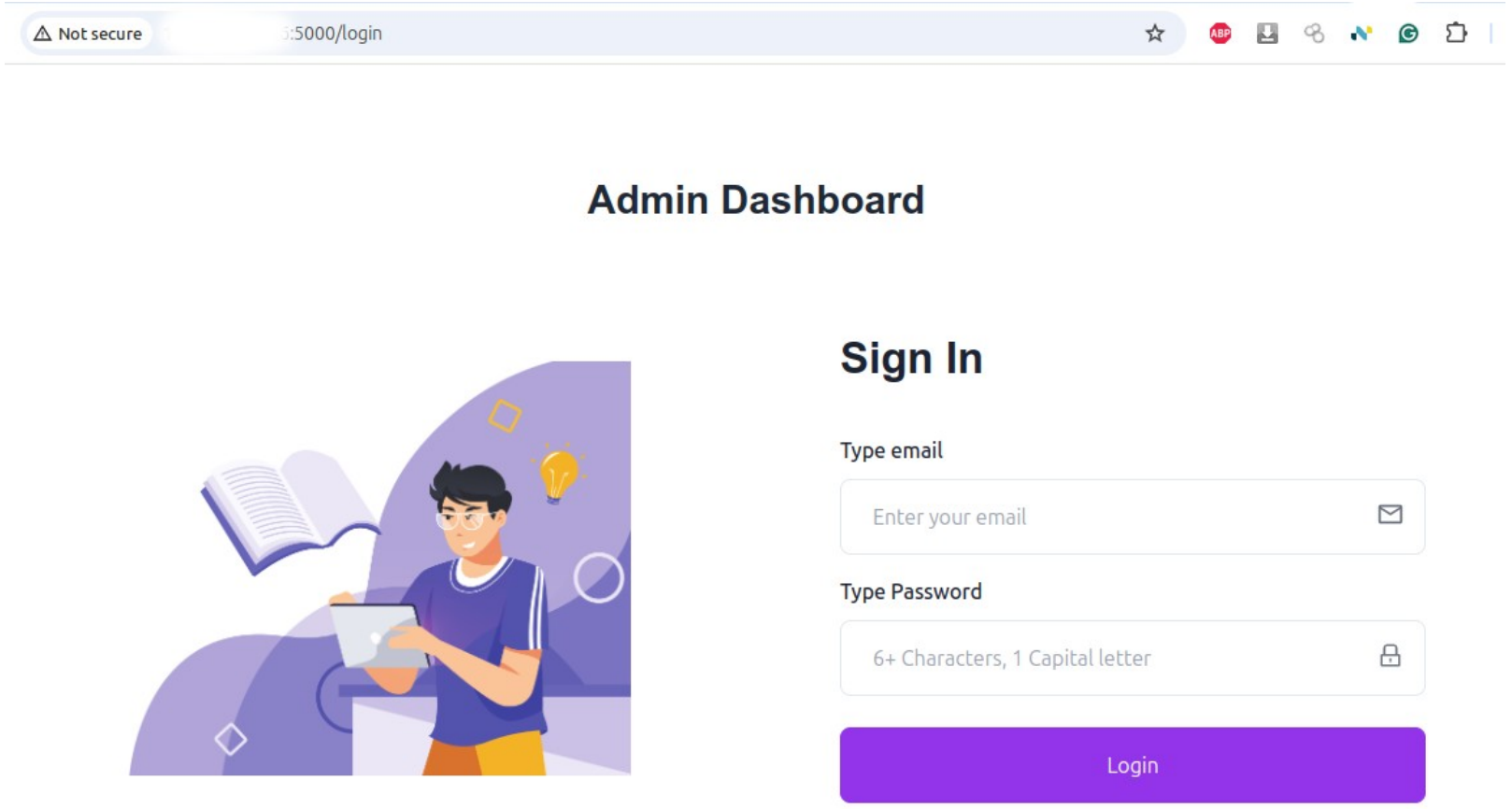
Risk 1: Misconfigured Cloud Infrastructure

Improperly set up cloud services like storage buckets, databases, and network settings can expose sensitive data and create vulnerabilities.

Mitigation:

- Cloud Security Posture Management (CSPM) tools: Continuously scan for misconfigurations and automatically remediate issues.
- Infrastructure as Code (IaC): Define cloud infrastructure configurations in code to ensure consistency and enforce security policies.
- Regular security audits: Conduct periodic reviews of cloud environments to identify and address configuration issues.

Risk 1: Misconfigured Cloud Infrastructure



20 IPs are open to Internet with several CVE for all the services its has.

TheTeamPhoenix
Machine Secures Machines

Risk 2: Insecure APIs

Unprotected APIs can be exploited by attackers to gain unauthorized access to data or systems.

Mitigation:

- API Gateway with authentication and authorization: Implement robust authentication mechanisms like OAuth and granular access controls.
- API security scanning tools: Regularly scan APIs for vulnerabilities and potential security flaws.
- Data encryption: Encrypt sensitive data transmitted through APIs.

Risk 2: Insecure APIs

Kubernetes Dashboard

TOTAL RESULTS

3,279

TOP COUNTRIES

United States	998
Canada	746
China	297
Ireland	290
India	183

More...

Only BD

TOTAL RESULTS

3

TOP PORTS

443	1
4443	1
10443	1

TOP ORGANIZATIONS

Bangladesh Computer Council	1
PLEXUS CLOUD	1
S. R. Khan Tusher T/A S. A. Online	1

Docker listening mode

TOTAL RESULTS

595

TOP COUNTRIES

China	190
Germany	131
Brazil	116
United States	48
France	10

More...

TOP PORTS

2375	543
2376	52

TOP ORGANIZATIONS

Oracle Public Cloud	76
Aliyun Computing Co., LTD	74
DigitalOcean, LLC	20
Tencent Cloud Computing (Beijing) Co., Ltd	17
Tencent cloud computing (Beijing) Co., Ltd.	16

Risk 3: Weak Identity and Access Management (IAM)

Insufficient access controls and weak password practices can lead to unauthorized access to sensitive data.

Mitigation:

- *Least privilege principle:* Grant users only the minimum permissions needed to perform their jobs.
- *Multi-factor authentication (MFA)*: Require MFA for all user logins to enhance account security.
- *Regular access reviews*: Periodically review user access and revoke unnecessary permissions.

TheTeamPhoenix
Machine Secures Machines

Risk 3: Weak Identity and Access Management (IAM)

TOTAL RESULTS

276,930

TOP COUNTRIES

China	123,712
United States	53,757
Germany	22,629
Hong Kong	9,612
Singapore	8,134

More...

TOP ORGANIZATIONS

Aliyun Computing Co., LTD	51,553
Tencent cloud computing (Beijing...	18,547
Aperack Ltd	16,033
Microsoft Corporation	15,143
Tencent Cloud Computing (Beijin...	12,619

More...

If Redis is publicly exposed without authentication, attackers can write arbitrary data or even gain remote shell access.

Risk 4: Supply Chain Security

Unverified or outdated container images can introduce vulnerabilities into your system. A developer pulls a public Docker image that contains malicious scripts.

Mitigation:

- Use trusted image registries (e.g., Docker Official Images).
- Scan images with tools like Trivy or Grype.

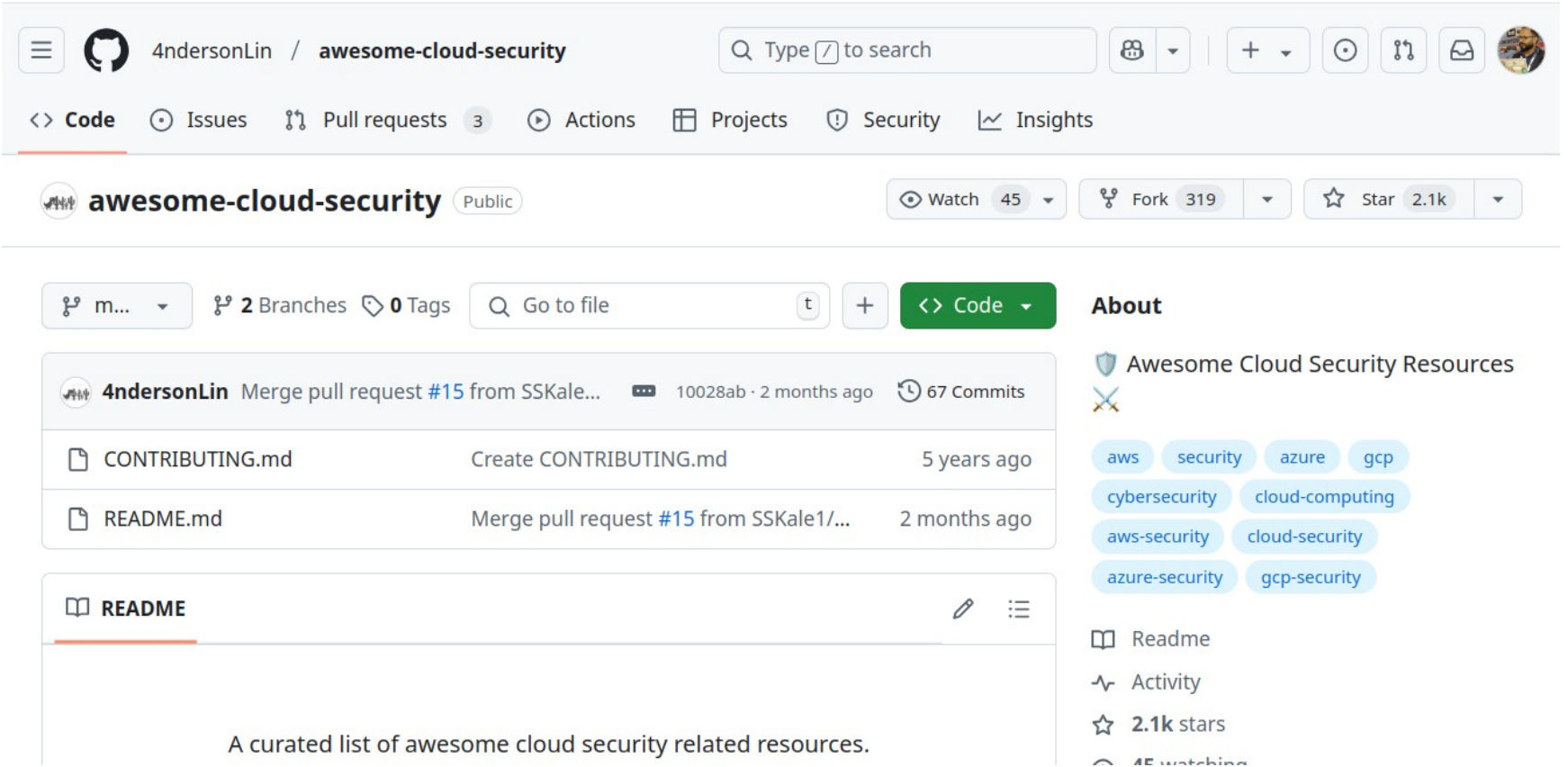
Risk 5: Inadequate Logging and Monitoring

Lack of comprehensive logging and monitoring can hinder threat detection and incident response capabilities.

Mitigation:

- Centralized logging system: Collect logs from all cloud services into a centralized platform for analysis.
- Real-time threat detection: Utilize security analytics tools to identify suspicious activity and potential threats.
- Alerting and notification systems: Set up alerts to notify security teams of critical events in real-time.

Awesome list of Cloud security



TheTeamPhoenix
Machine Secures Machines

3 Key Takeaways:

- Misconfigurations are the #1 cause of cloud breaches. Automate security audits!
- Secure your APIs, IAM roles, and secrets—they are prime attack vectors.
- Continuous logging & monitoring is critical for real-time threat detection.

Thank You

TheTeamPhoenix

Machine Secures Machines

Stay Connected

/Theteamphoenix

/company/theteamphoenix/

/tteamphoenix

/@theteam_phoenix

Need support?

Email us:

info@theteamphoenix.org