Top 7 Cyber Threats in Cloud-Native Environments

Date: 13 November 2024

The global pandemic and its aftermath have completely changed the topography of the information technology arena. The uptake of the cloud has been rapid. Running in parallel is the growth of native cloud application development, as organisations must utilise their cloud infrastructures to provide products and services much quicker and more efficiently.

However, it's critical that organisations be aware of critical cloud security risks in this evolving landscape. We explore 6 of the top threats in this article.

1. Misconfigurations

Cloud misconfigurations and unpatched software can leave systems vulnerable to network attacks and exploitation. These misconfigurations are often due to defaults not being changed or set improperly for access. One of the most common configuration mistakes is leaving network ports open to the internet. Any open port accessible from the public internet gives malicious actors a potential entry point to launch attacks.

2. Insecure APIs

vulnerabilities include weak authentication mechanisms, excessive information disclosure, and the lack of rate limiting. These issues can lead to improper access control configurations, resulting in data breaches and leaks.

3. Poor IAM and Data Encryption

Identity and Access Management (IAM) ensures that only authorised users and services gain access to the most vital resources. If there is no good IAM policy in place, unauthorised actors or services can access data, leading to severe security threats.

Encryption is also essential in data protection in transit and at rest. When data is transmitted over a network, encryption protects it from being intercepted and read by unauthorised parties. Encryption is also important for protecting data stored on cloud storage. This safeguards the information in case of theft, unauthorised access, or physical loss of the storage medium. Common defects involve the use of old encryption algorithms or incorrect encryption keys.

ULTIMATE LIST OF THE TOP CYBER DRILL SCENARIOS,
ASSET CATEGORIES TO PROTECT & THREAT ACTORS TO WATCH FOR
GET YOUR COPY
CYBER MANAGEMENT

4. Vulnerable Container Orchestration Tools

Container orchestration platforms like Kubernetes commonly expose interfaces via APIs or web-based consoles. This exposes them directly to the Internet, inviting unauthorised access to sensitive information like infrastructure details, source code repositories, and container configuration.

Additionally, attackers who gain access to administrative or deployment consoles can cause harm by stealing credentials and keys stored in the systems, tampering with

This risk becomes greater due to the intrinsic interconnectedness of containerized applications; that is, when one container gets compromised, all are in danger. Patching on time and staying up to date with the Kubernetes Security Best Practices can best mitigate such risks.

5. Alert Fatigue

Malware is not a new phenomenon but is rapidly evolving, especially in the cloud environment. Identifying potential cloud-native malware can be challenging due to security tools' "noisy" nature. These tools generate more alerts than security teams can reasonably address, leading to "alert fatigue" and the potential for missed warning signs.

6. Application Vulnerabilities

For many organisations, the biggest risk can arise from the application development process itself. Since applications remain vulnerable even after deployment, security professionals must consider various threat vectors and secure the entire application lifecycle. From untested code changes to zero-day attacks, runtime applications will continue to require close examination.

7. Insider Threats

An insider is an individual (for instance, an employee) who has already been granted access and authorization to an organization's network and sensitive resources. With cloud computing, the organization has less visibility into the inner workings of the cloud infrastructure, making detecting an insider threat more challenging.

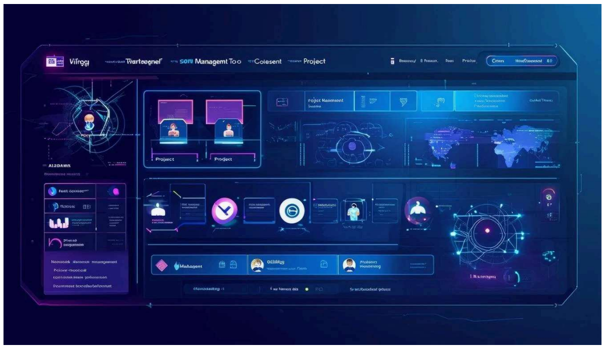
NIST INCIDENT RESPONSE PLAYBOOK TEMPLATE
GET YOUR COPY
CYBER MANAGEMENT ALLIANCE

operational efficiency and scalability, the importance of cloud security has escalated to become a critical priority. This shift is driven by the need to safeguard sensitive data and maintain the integrity of business operations in an increasingly digital world. Properly implementing robust security controls, such as advanced encryption techniques, multi-factor authentication, and continuous monitoring, is essential.

Additionally, cultivating a comprehensive awareness of the evolving cloud threat landscape is crucial for enterprises. By doing so, organisations can not only defend against potential breaches but also build trust with their clients and stakeholders, ensuring the long-term success and resilience of their cloud-based operations.

Show comments

Related posts



7 November 2024

Project Management AI Tools: Reduce Cyber Risks & Boost Collaboration

1 November 2024

How Global Malware Incidents Transformed Cybersecurity

29 October 2024

Optimizing Cybersecurity With Comprehensive Asset Visibility

24 October 2024

CYBER MANAGEMENT ALLIANCE

Call us on

+44 (0) 203 189 1422

info@cm-alliance.com

Find us at

71-75 Shelton Street, Covent Garden, London, WC2H 9JQ

Quick links:

See below list of our core services & free cybersecurity resources:

Training

Resources

Tabletop Exercises

Blog

Consultancy

About Us

Events