

Recap and Key Takeaways from "Cyberattacks in Hospitality: Defense, Awareness, and Timely Response!"

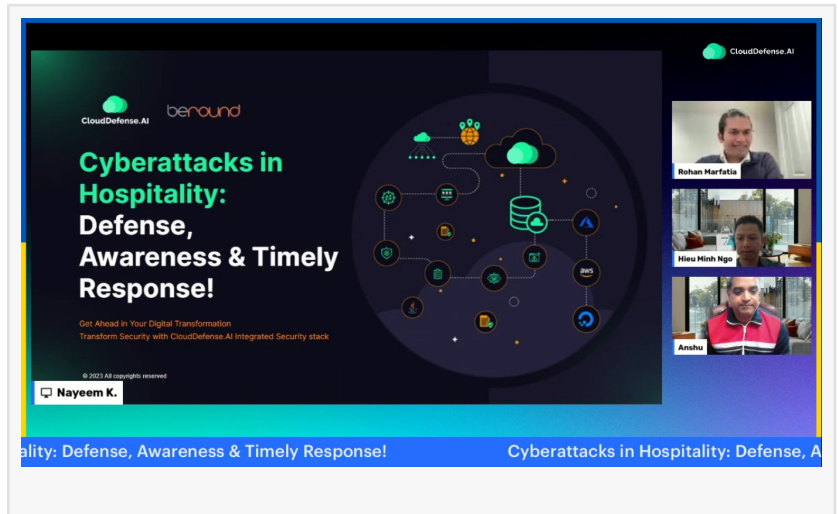
CloudDefense.AI and Beround recently hosted a live webinar titled "Cyberattacks in Hospitality: Defense, Awareness, and Timely Response!"

PALO ALTO, CALIFORNIA, UNITED STATES, December 1, 2023

[/EINPresswire.com/](https://EINPresswire.com/) -- CloudDefense.AI,

a leading cybersecurity solutions provider, and Beround, a specialized software consultancy company, recently hosted a live webinar titled

"Cyberattacks in Hospitality: Defense, Awareness, and Timely Response!" The webinar featured insights from a panel of experts, including:



“

In the face of escalating cyber threats, proactive readiness is key. Hacker’s View™ provides a unique perspective to identify vulnerabilities and fortify defenses without installation.”

Anshu Bansal, CEO of CloudDefense.AI

Anshu Bansal: CEO, CloudDefense.AI

Rohan Marfatia: CEO, Beround

Hieu Ngo: Ex-convicted Hacker and Chief Ethical Hacking Officer of CloudDefense.AI

The webinar highlighted the growing threat of cyberattacks targeting the hospitality industry. Hieu Ngo, ex-Hacker and CEHO of CloudDefense.AI, pointed to the projected increase in cybersecurity spending from \$347 billion in 2023 to \$458.9 billion by 2025, indicating a clear escalation in cyber threats.

The panel also discussed the specific vulnerabilities of the hospitality sector. Rohan Marfatia, CEO of Beround, stressed the importance of skilled professionals, training, and security audits, stating that relying solely on tools is inadequate for protection.

The discussion also included real-world examples of successful cyberattacks against hospitality companies. Hieu Ngo explored hacker attack vectors, highlighting the industry's susceptibility to reconnaissance and exploitation. Notable incidents like the MGM Resorts ransomware attack and the Caesars Entertainment data compromise further emphasized the need for heightened vigilance.

Anshu Bansal, CEO of CloudDefense.AI, concluded the webinar by showcasing Hacker's View™, a user-friendly tool that provides a 360° system view to identify hidden vulnerabilities without installation.

CloudDefense.AI encourages hospitality businesses to take a proactive approach to cybersecurity. The company is offering a free vulnerability assessment to help identify potential weaknesses and implement effective security measures.

For those who missed the live webinar, a recording is available online. You can [watch it here](#).

About CloudDefense.AI

CloudDefense.AI, headquartered in Palo Alto, is a complete Cloud-Native Application Protection Platform (CNAPP) that secures the entire cloud infrastructure and applications. Considering the evolving threat landscape, they blend expertise and technology seamlessly, positioning themselves as the go-to solution for remediating security risks from code to cloud.

Their integrated CNAPP suite comprises various security solutions, including CSPM, CIEM, Threat Detection, CWPP, SAST, DAST, SCA, KSPM, Hacker's View™, Container Security, and API Security. Their attack path and graph-based technology empower businesses to automatically detect,

The image displays three sequential screenshots from a webinar recording. Each screenshot features a central slide with text and graphics, and a vertical sidebar on the right with three video thumbnails of the speakers: Rohan Marfatia, Hieu Minh Ngo, and Anshu. The bottom of each slide includes the CloudDefense.AI and beround logos, and a blue banner with the text "Cyberattacks in Hospitality: Defense, Awareness & Timely Response!".

Slide 1: Speaker Introduction
Speakers listed: Anshu Bansal (Founder & CEO, CloudDefense.AI), Rohan Marfatia (Chief Executive Officer, beround), and Hieu Ngo (Cyber Security Specialist & Former Convicted Hacker). A moderator, Nayeem K., is also visible.

Slide 2: Threat Overview
Title: GLOBAL CYBERSECURITY SPENDING
Subtitle: \$1.75 TRILLION CUMULATIVELY 2021 TO 2025
Source: CYBERSECURITY VENTURES
Bar chart showing spending by year in billions of dollars:
2021: \$262.4B
2022: \$301.8B
2023: \$347B
2024: \$399B
2025: \$458.9B

Slide 3: Breach Analysis
Text: "The following are some specific findings from the breach analysis:"
Findings:
- MGM Resorts: The attackers attempt to gain access of MGM Resorts' network was - via phone call (Voice Phishing Attack) to IT Desk and reset the MFA of a Victim User. Compromised Okta Super administrator and then more admins. The attackers control over the Domain admins, Admins on the Okta Syncing Server, Global Administrator in Azure. By this they Exfiltrate sensitive data from the network, Encrypt 100 ESXi servers and disrupt all VMs & services that run on top of them. Source: CYBERSECURITY DIVE CYBERARK
- Caesars Entertainment: The attackers gained access to Caesars Entertainment's network by exploiting a vulnerability in its web application firewall. The vulnerability allowed the attackers to inject malicious code into the web application, which they then used to steal data from the database. Source: The Register
Summary statistics:
- Financial Loss: \$100M Approx
- Customers Data: Compromised
- Shutdown: ATMs & Several Systems
- Control over: MGM Resorts Network
- Ransom Negotiation: \$15M reported
- Affected: 41,000+ Home residents
- Offers effected: 2 years complimentary Service
- Attack Linked to: MGM Resorts

prioritize, and remediate various security issues, from system vulnerabilities to misconfigurations.

Going above and beyond, their innovative solution actively tackles zero-day threats and effectively reduces vulnerability noise by forging a connection between applications and the cloud. This unique approach delivers up to five times more value than other security tools, establishing them as comprehensive and proactive digital defense pioneers.

If you want to learn more about CloudDefense.AI and its suite of services, please [book a free demo](#) or contact here gtm@clouddefense.ai

Emily Thompson

CloudDefense.AI

media@clouddefense.ai

Visit us on social media:

[Twitter](#)

[LinkedIn](#)

[Instagram](#)

[YouTube](#)

The image shows a screenshot of a webinar slide. The slide is titled "Solution Mapped" and contains a bulleted list of security solutions. The list includes: Social Engineering (Phishing Attacks Widely) - Phishing Stimulation & Cyber Security Awareness Training from Board to End Users; Ransomware - Business Continuity Planning & Disaster Recovery Planning with SOC in Place; DDoS - High Availability with Multiple Infrastructure Security Controls; Payment Card Attacks - Identification of Crucial Card Data, Encryption with Privileged Access Controls; Wireless Attacks - Hardening and Implementation of Wireless and Network Devices; Customer Data & Identity Theft - Physical Security Controls and Encryption of Data with Proper SIEM and SOAR in Place; Compliance Issues - Implementation of International Cyber Security Compliance and Standards like ISMS, HIPAA, SOC2, PCI DSS; and Absence of IT Security Team - Providing High Skilled and Certified & Experience Resources. The slide also features the CloudDefense.AI and Beround logos. On the right side of the slide, there is a video call interface with three participants: Rohan Marfatia, Hieu Minh Ngo, and Anshu. The slide footer contains the text "Cyberattacks in Hospitality: Defense, Awareness & Timely Response!" and "Cyberattack".

This press release can be viewed online at: <https://www.einpresswire.com/article/672289658>

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.

© 1995-2023 Newsmatics Inc. All Right Reserved.