View this email in your browser

AMERICAN
TECHNOLOGY
SERVICES

American Technology Services

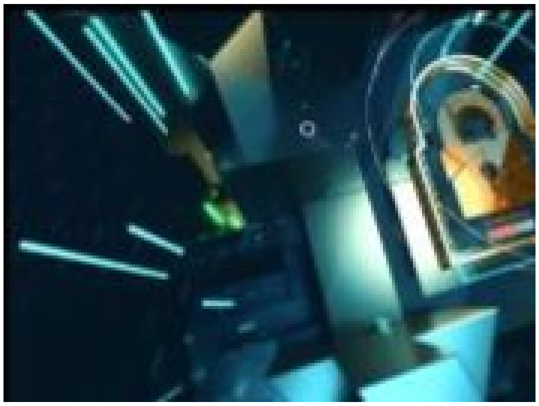
Cybersecurity News Roundup

Weekly Insights and Updates

| August 2 2024

Cyber threats are rapidly becoming more sophisticated. Keeping up with the latest cybersecurity news is important to protect yourself and your organization. This week's roundup dives into the blind spots affecting CISOs,the evolution of the cyber threat landscape, and innovative defense strategies.

This week’s newsletter highlights critical cybersecurity challenges and solutions, including addressing blind spots, evolving threats,and strategies for improving your organization's defenses. From understanding the implications of new cybersecurity requirements to learning how AI and cybersecurity can cooperate for stronger defenses, this edition is packed with insights to help you stay ahead of the curve.



The Three Cybersecurity Blind Spots

Gain insights into the common blind spots CISOs face and discover proactive measures to address vulnerabilities. Learn how comprehensive audits, threat intelligence integration, and zero-trust architectures can enhance your cybersecurity posture.

Read More

The Cyber Threat Landscape: 12 Month Update

Explore the rapidly changing cyber threat landscape, where advanced threats like ransomware and supply chain attacks demand adaptive strategies. Discover steps to bolster your defenses with advanced threat intelligence and employee training.

Read More

Social Engineering Alert: North Korean Hacker

A North Korean hacker posing as an IT employee was caught, emphasizing the need for diligent identity verification and company data access control. This case study provides lessons on strengthening security protocols against social engineering attacks.

Read More

Adaptive Malware Solutions for Innovative Defense

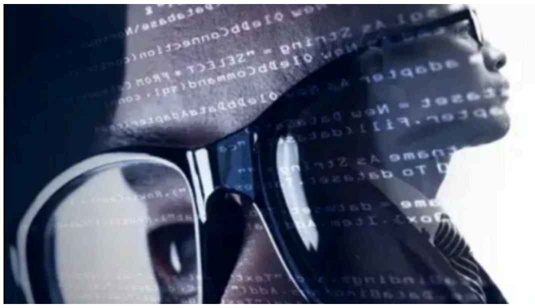
Discover how HYAS is transforming malware defense with machine learning for real-time threat detection. Learn about predictive threat detection and protective DNS solutions that can enhance your organization's cybersecurity.

Read More

Build a Strong Patch Management Framework

Learn best practices and strategies for an efficient patch management approach. Prioritize critical patches and automate deployment to reduce vulnerabilities and improve security.

Read More



Cooperative Approach with AI and Cybersecurity

Uncover the benefits of cooperation between AI and cybersecurity for enhanced compliance and threat detection. Understand how collaboration between developers and security experts can create a safer digital environment.

Read More

Essential Dark Web Monitoring for CFOs

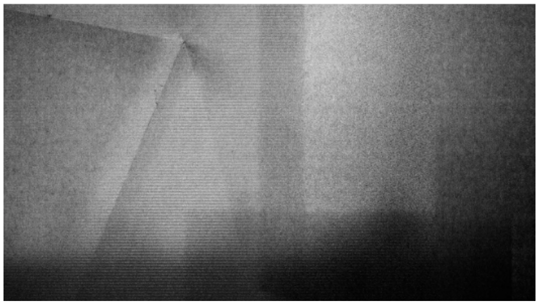
Understand the importance of dark web monitoring in detecting early signs of data breaches. Learn practical steps CFOs can take to integrate monitoring into cybersecurity strategies and protect financial data.

Read More

New Cybersecurity Requirements for Critical Infrastructure

Learn about CISA's proposed cybersecurity requirements for critical infrastructure sectors. Prepare your organization for compliance with mandatory incident reporting and stronger security measures.

Read More



Cyber Insurance: Adapting to Evolving Threats

Explore the evolving landscape of cyber insurance coverage.Regularly review and update your policies to ensure protection against emergingthreats and optimize your organization's coverage.

Read More

Government Warnings of Heightened Hack Threats

The FBI and GCHQ warn organizations about increased hack threats across sectors. Improve your cybersecurity measures by refining incident response plans and conducting regular security assessments.

Read More

Featured Articles by ATS

Mastering HIPAA Compliance

Ensuring HIPAA compliance is essential for safeguarding patient data in the healthcare sector. This article highlights the importance of regular risk assessments, employee training, and technological safeguards to protect sensitive information and maintain cybersecurity standards.

Read More

The Threat of Deepfakes

Deepfake technology poses serious cybersecurity risks, from disinformation to fraud. This article explores the rise of deepfakes, their potential threats, and the importance of detection tools and public awareness in combating these digital manipulations.

Read More

Time to Upgrade Your Cybersecurity?

Frequent breaches and outdated security measures are key signs it's time to upgrade your cybersecurity provider. This article highlights the importance of advanced solutions, scalability, and industry expertise in choosing the right provider to meet evolving security needs.

Read More

As we wrap up this week's cybersecurity roundup, it's clear that staying ahead of threats requires a multi-faceted approach. From addressing blind spots in your security to leveraging AI, there's no shortage of action items on our cybersecurity to-do list. Remember, it's not just about technology – your team's awareness is important too, especially when it comes to social engineering tactics. Don't forget to keep your patches up to date, take a peek at what's happening on the dark web, and make sure your cyber insurance aligns with your business needs and regulatory requirements .

With new regulations on the horizon and government warnings to heed, it's more important than ever to stay on your toes. By implementing these strategies, you're not just ticking boxes – you're building a strong defense against an ever-changing threat landscape.

When it comes to cybersecurity, staying still is moving backward.

Contact us

INT. +1 888 876 0302
USA +1 703 876 0300

info@networkats.com
networkats.com

Our Offices

New York | Virginia | Atlanta

Share the insights!
Forward this email to a friend.

Our mailing address is:
250 Broadway, Suite 610
New York, NY 10007