View this email in your browser


## Weekly Insights and Updates

|December 20, 2024

As 2024 concludes, the cybersecurity world faces a pivotal moment of change. Advancements in artificial intelligence (AI), the impending threats of quantum computing, and the rapid growth of the Internet of Things(IoT) are transforming how organizations approach security.

AI-driven attacks have reached new levels of sophistication, enabling cybercriminals to launch highly targeted phishing schemes and deploy self-evolving malware. To counter these intelligent threats, organizations must adopt equally advanced defense and intelligence strategies that are adaptable and allow for response in near real-time.

Meanwhile, the explosive growth of IoT devices has dramatically increased the attack surface. With billions of new connected devices expected online in 2025, stringent security protocols for IoT networks are vital for preventing mass exploitation. Given these developments, organizations must stay informed and implement cybersecurity frameworks that address complexities and prepare for unknowns.

## Ransomware Innovation and Smarter Defenses

Ransomware tactics are advancing, but defenses are adapting. Predictive analytics,collaboration across sectors, and resilience-focused strategies are helping organizations mitigate the impact of complex extortion attempts.

Read More


## Cloak Ransomware as a Hidden Threat

The Cloak ransomware variant, disguised as legitimate updates, uses sophisticated evasion techniques to bypass defenses. Strengthened endpoint protections and vigilant monitoring are essential to counter this persistent threat.

Read More

## AI Transforming the Cybersecurity Workforce

AI is revolutionizing cybersecurity and improving threat detection while reshaping workforce dynamics. Balancing AI integration with the continued value of human expertise are important for sustainable defense strategies.

Read More


## Major Breaches of 2024 and Their Lessons

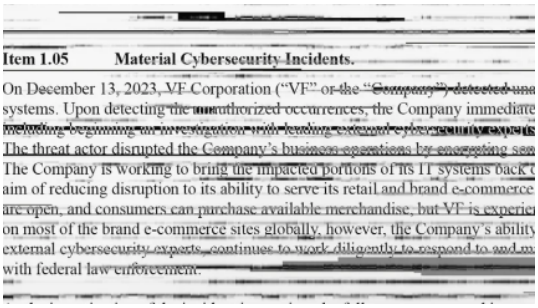
High-profile breaches, such as LoanDepot's massive data leak, reveal critical vulnerabilities in data protection. These incidents provide valuable lessons and strategies for strengthening defenses against similar attacks.

Read More

### Exploited Apache Struts Flaw Risks

A critical vulnerability in Apache Struts enables attackers to execute remote code via malicious file uploads. Mitigating this risk demands swift patching and adherence to secure coding practices.

Read More

Item 1.05 Material Cybersecurity Incidents.

On December 13, 2023, VF Corporation ("VF" or the "Company") detected una
systems. Upon detecting the unauthorized occurrences, the Company immediate
The threat actor disrupted the Company's business operations by encrypting sev
The Company is working to bring the impacted portions of its IT systems back
aim of reducing disruption to its ability to serve its retail and brand e-commerce
are open, and consumers can purchase available merchandise, but VF is experie
on most of the brand e-commerce sites globally, however, the Company's ability
external cybersecurity experts, continues to work diligently to respond to and m
with federal law enforcement.

### SEC Cyber Disclosure Compliance Challenges

The SEC's cyber incident reporting rule saw only 71 filings in its first year,highlighting gaps in compliance. Transparent incident reporting and alignment with regulatory standards are key to building trust with stakeholders.

Read More

### Continuous Penetration Testing as a Game Changer

Static pen testing is no longer sufficient in a dynamic threat landscape.Continuous penetration testing offers near real-time insights, enabling organizations to proactively address vulnerabilities.

Read More


### Cyber Threats to Expect in 2025

The year ahead brings new challenges, from advanced ransomware to evolving regulations. Building resilience and implementing layered security will be vital to staying ahead of threats.

Read More

### IAM Trends Reshaping Security

Advances in Identity and Access Management, including machine identity management and post-quantum cryptography, are redefining access controls and fortifying organizational defenses.

Read More


### CISA's Updated Incident Response Plan

CISA's updated 2025 National Cyber Incident Response Plan strengthens public-private coordination during cyber incidents. This agile framework incorporates lessons from past events to improve national resilience.

Read More

## Featured by ATS

### Dark Web Threat Intelligence

Cyber threats are growing more sophisticated, but staying ahead is possible with proactive intelligence. ATS' Threat Intelligence services monitor leaked credentials, compromised accounts, and dark web activity to identify risks before they escalate. With advanced monitoring, detailed investigations, and actionable insights, we help you secure critical assets and strengthen your defense strategy.

### Incident Response Tools: Rapid, Reliable, Resilient

Cyber incidents demand precision, speed, and expertise. ATS' Incident Response Tools—powered by 24/7 support from the Security Incident Response Team (SIRT)—deliver advanced capabilities like endpoint detection, forensic analysis, and real-time monitoring. ATS equips organizations to respond effectively and minimize impact.

### Strengthening Vendor Security with TPRM

Third-party risks can disrupt operations and expose critical assets. ATS' Third-Party Risk Management (TPRM) service blends threat intelligence with attack surface monitoring to identify vulnerabilities, reduce supply chain risks, and ensure compliance. Protect your business continuity while fostering secure and reliable vendor partnerships.

Read More | Read More | Read More

The cyber threat landscape isn’t slowing down, and neither can we. From AI-powered attacks and the looming quantum computing revolution to the IoT explosion, the challenges are piling up faster than a developer's buglist. But with the right mindset and tools, these challenges can become stepping stones to a stronger, more secure future.

This week, we unpacked strategies like continuous penetration testing, advanced IAM trends, and better-coordinated incident response plans. It’s time to ditch static defenses and get serious about being proactive. Cybersecurity in 2025 isn’t just about having the latest tech—it’s about thinking two steps ahead, staying flexible, and preparing for threats you haven’t even imagined yet.

At ATS, we’re here to keep you in the know and protect your organization against digital threats. The future of cybersecurity? It’s not something to fear—it’s something to shape. Let’s start now.

**The lessons of 2024’s breaches are written in lost data; don’t wait until 2025 to learn them.**


## 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