SANS | GIAC CERTIFICATIONS

RSAC 2024 Keynote Session Reveals:

The Five Most Dangerous New Attack Techniques

Moderated by
Ed Skoudis
SANS Technology Institute College President

Each year at RSA Conference, the SANS Institute provides an authoritative briefing on the most dangerous new attack techniques leveraged by modern-day attackers, including cyber criminals, nation-state actors, and more. The annual briefing brings together some of the best and brightest minds shaping SANS core curricula to discuss emerging threat actor tactics, techniques, and procedures, assess what they mean for the future, and guide organizations on how to prepare for them.

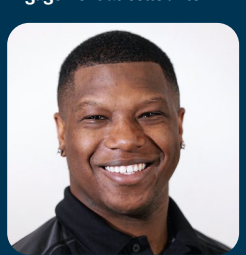
Heather Barnhart
SANS DFIR Curriculum Lead and Senior Director of Community Engagement at Cellebrite

ATTACK TECHNIQUE

AI-Powered Child Sextortion

Heather highlights the rise of nefarious AI-sextortion campaigns targeting minors and their families.

ACTION: Parents, educate your kids on the real dangers of seemingly harmless online interactions.



Terrence Williams
SANS DFIR Certified Instructor and Security Engineer

ATTACK TECHNIQUE

Using Generative AI to Skew Public Perception

Terrence exposes the societal danger posed by generative AI's impact on the 2024 U.S. elections—detailing how nation-state adversaries are weaponizing deepfakes and AI-generated content to blur the lines of truth and undermine election integrity.

ACTION: Strengthen collaborations to protect the integrity of democracy.

Steve Sims
SANS Offensive Cyber Operations Curriculum Lead and Fellow

ATTACK TECHNIQUE

AI LLMs Hyper Accelerate Exploitation Lifecycles

Steve examines how Generative AI Large Language Models (LLMs) are hyper-accelerating the exploitation lifecycle, making security professionals' jobs even more time-sensitive and hectic. Attackers are actively working on automating the exploit development process to streamline exploitation, while defenders likewise leverage AI to level up defenses.

ACTION: Develop more efficient defensive and patching capabilities.

Dr. Johannes Ullrich
SANS Technology Institute Dean of Research, Internet Storm Center Founder

ATTACK TECHNIQUE

Exploitation of Technical Debt

Dr. Ullrich assesses the consequential ramifications of technical debt on enterprise security. Many organizations are still utilizing decades-old legacy code across their critical systems, creating technical debt that hinders VPN and firewall effectiveness and leads to maintenance cost increases, incident response complexity, and compatibility issues.

ACTION: Prioritize modernization and reduce legacy vulnerabilities.

ATTACK TECHNIQUE

Deepfakes Complicating Identify Verification

He also details the challenges associated with verifying user identity in the advanced AI era. As ransomware groups deploy AI-enabled deepfakes for social engineering and vishing campaigns, modern enterprises operationalizing hybrid working models are in the crosshairs of highly sophisticated threats that are difficult to defend against.

ACTION: Facilitate more in-person collaboration to verify identity of employees and vendor partners.

SANS Institute is celebrating its 35-year anniversary in 2024. Launched in 1989 as a cooperative for information security thought leadership, SANS helps mitigate cyber risk by empowering security practitioners and teams with world-class training, certifications, and degrees that are critical for safeguarding organizations and advancing careers.

RSAConference™2024

SANS | Celebrating 35 Years