iSMG Studio

at Black Hat and DEF CON 2024

Black Hat 2024: The Best of ISMG.Studio

What happens in Vegas stays in Vegas? Not always.

This publication is evidence that what was said at Black Hat and DEF CON 2024 in August resonated. We at ISMG.Studio have preserved some of the best insights and ideas so we can share them here with you in this exclusive compendium.

For the second straight year, we opened our studio adjacent to the conference, and we produced more than 50 interviews over the course of Black Hat. CEOs, CISOs, government leaders, investors, researchers and attorneys are all represented in our interviews and are featured here. We discussed AI, secure enterprise browsers, application security, nation-state threats, the ransomware scourge and much more.

We brought our largest-ever Information Security Media Group team from around the world to Black Hat and DEF CON 2024. Within these pages, you'll find insightful interviews by our seasoned editorial team – an in-depth view of the latest information and thought leadership from these landmark events. We went to Las Vegas so you didn't have to, and we're grateful for the opportunity to share the insights we gleaned from our conversations.

Enjoy.

Tom Field

Senior Vice President, Editorial

Information Security Media Group

tfield@ismg.io

Visit us online for more ISMG at Black Hat 2024 coverage:

ismg.studio

Video Interviews

Cybercrime/Ransomware and Dark Web Activities

Most cybercriminals are still using time-honored tools and techniques, but they are constantly innovating. Despite law enforcement seizures and arrests, most cybercrime gangs have better defenses than most Fortune 100 firms. Conference speakers and experts discussed the latest ransomware trends, attacks on APIs and third-party software, emerging deepfake capabilities, and nation-state threats to critical infrastructure – including the beleaguered healthcare sector.

Hans de Vries
Chief Cybersecurity and Operations Officer, ENISA

Cybersecurity Is Everywhere: ENISA COO

Hans de Vries on Securing Europe's Digital Future With Laws and Skills Development

Europe faces unprecedented security challenges as organizations embrace digital change. That's why ENISA is focusing on critical areas to bolster Europe's digital defenses - supporting member states by enhancing their cybersecurity programs through legislation, exercises and comprehensive reports.

In this interview with Information Security Media Group at Black Hat 2024, de Vries also discussed:

- How the EU Cyber Resilience Act and the Digital Services Act aim to regulate and secure software;
- ENISA's role in enhancing election security through exercises and advisories;
- The importance of securing both IT and OT for national security.

WATCH ONLINE

> "Cybersecurity is everywhere. Information sharing and having a good understanding of what's happening during, before and after a crisis are crucial."
>
> *- **Hans de Vries***

Robert Boyce
Global Cyber Resilience Lead, Accenture

How Ransomware Group Stability Affects Payment Decisions

Robert Boyce on Accenture's Strategy for Assessing the Behavior of Ransomware Gangs

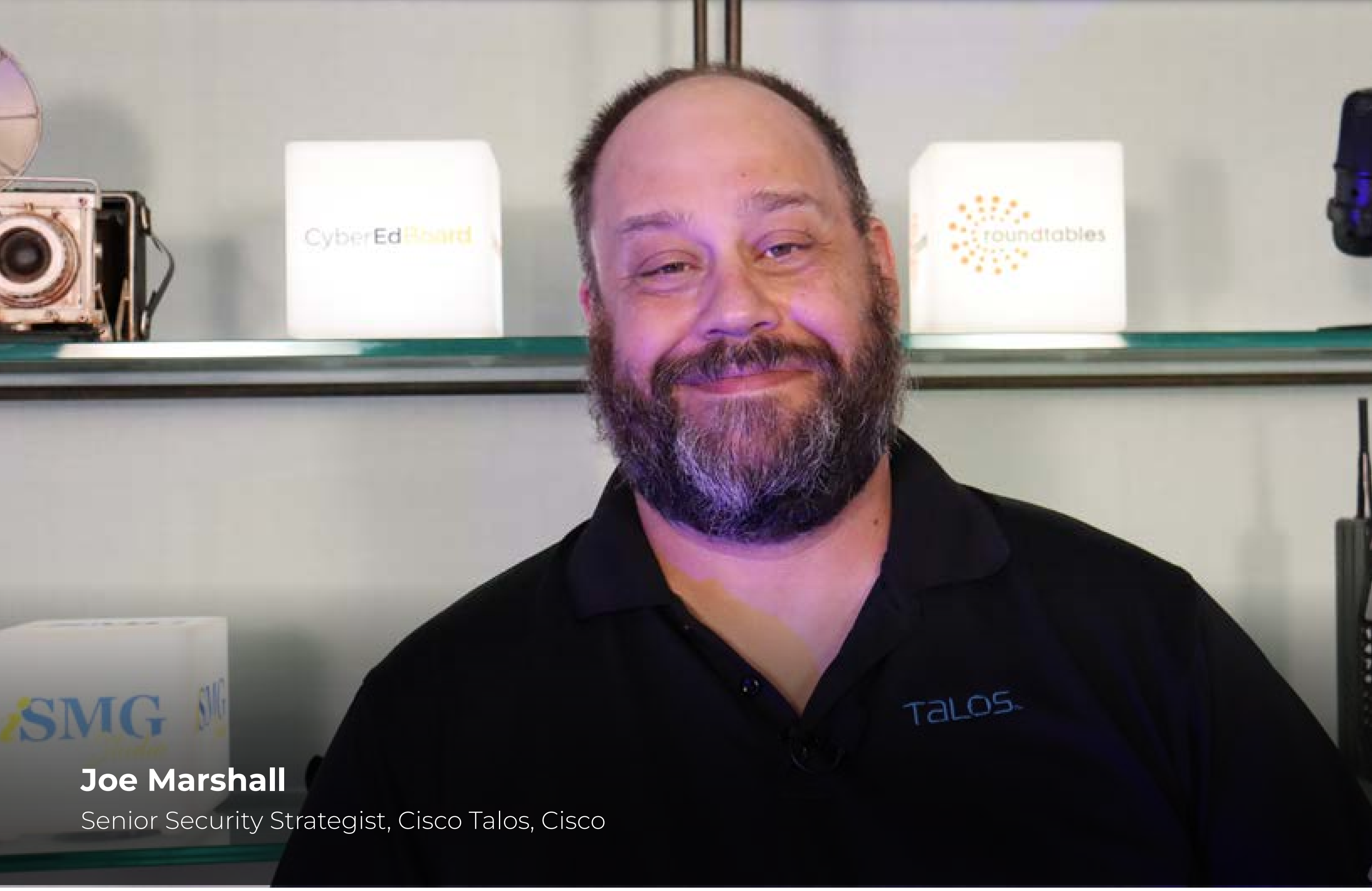
Accenture Global Cyber Resilience Lead Robert Boyce outlined why organizations must assess the stability of ransomware groups before deciding how to respond to extortion threats. He shared how trustworthiness of ransomware gangs can affect the likelihood of receiving decryption keys after payment.

In this video interview with Information Security Media Group at Black Hat 2024, Boyce also discussed:

- The importance of evaluating ransomware group stability and track records;
- The shift from encrypting data to targeting executives with stolen information;
- The rise of ransomware exit scams and their implications for future attacks.

> “This past year, we've seen a number of the prominent ransomware-as-a-service gangs disappear because they have either been the target of law enforcement or, more notably, executed exit scams.”
>
> - ***Robert Boyce***

WATCH ONLINE



Joe Marshall
Senior Security Strategist, Cisco Talos, Cisco

Critical Infrastructure Under Siege: Cisco Talos' Power Play

Joe Marshall on How Project PowerUp Helped Address Power Grid Crisis in Wartime

When the war in Ukraine disrupted its GPS capabilities - crucial for power grid synchronization - Cisco Talos assembled a team of experts to address the issue. Joe Marshall, senior security strategist at Cisco Talos, led the collaborative response, known as Project PowerUp.

In this video interview with Information Security Media Group at Black Hat 2024, Marshall also discussed:

- The challenges of maintaining power grids under attack;
- The importance of securing executive buy-in amid geopolitical conflicts;
- Lessons from Ukraine's infrastructure resilience.

WATCH ONLINE

> “Power grid work at its best is incredibly dangerous. We're talking high voltages. Something breaks in ... a storm, and we have to go do vegetation management.”
>
> *- Joe Marshall*

Michael Sikorski
Vice President, Threat Intelligence, and CTO, Unit 42, Palo Alto Networks

Exploiting Unpatched Systems: Latest in Ransomware Trends

Michael Sikorski of Palo Alto Networks on Evolving Ransomware Strategies

Russian hackers are leveraging unpatched vulnerabilities to exploit networks for more than 20 months. Michael Sikorski, vice president of threat intelligence at Palo Alto Networks, shared insights on ransomware gangs, AI's role in attacks and the importance of defense-in-depth strategies for organizations.

In this video interview with Information Security Media Group at Black Hat 2024, Sikorski also discussed:

- Using AI to automate phishing, lateral movement and malware creation;
- How defenders are integrating AI into their red-teaming efforts to simulate an adversarial activity;
- How Russian hackers exploit persistent vulnerabilities to maximize attacks.

WATCH ONLINE

> "Attackers will use what works. If it's something that's been out a long time, something that's easy for them to build, that's the best thing for them to use because then they could save their fancy capabilities, the zero-day attacks, for high-value targets."
>
> *- Michael Sikorski*

Sherrod DeGrippo

Director, Threat Intelligence Strategy, Microsoft

Defending Against SIM Swapping, AI-Driven Social Engineering

Microsoft's **Sherrod DeGrippo** on SIM Swapping, AI Exploits and Defensive Strategies

Microsoft's Sherrod DeGrippo delved into the rise of SIM swapping, the role of social engineering in cyberattacks and the emerging use of AI by threat actors. She emphasized the need for real multifactor authentication and advanced strategies to counter these evolving threats.

In this video interview with Information Security Media Group at Black Hat 2024, DeGrippo also discussed:

- Why SIM swapping has become so popular and who is being targeted;
- The role of AI in accelerating cybercrime tactics such as social engineering;
- How multifactor authentication and organizational playbooks boost resilience.

WATCH ONLINE

> “We typically say, 'Threat actors don't hack in - they log in,' which is very true most of the time.”
>
> ***- Sherrod DeGrippo***

Bryson Bort
Founder and CEO, SCYTHE, and Faculty at IANS Research

Is China's Threat to US Critical Infrastructure Overblown?

Scythe CEO **Bryson Bort** on Why US Concerns About Chinese Attacks May Be Misplaced

As concerns grow about China's cyberthreat to U.S. critical infrastructure, Scythe founder and CEO Bryson Bort suggested the actual risk may not be as severe as feared. He explained the factors that might limit China's cyber activities and the real strategic vulnerabilities that could be targeted.

In this video interview with Information Security Media Group at DEF CON 2024, Bort also discussed:

- The historical context of Chinese cyber operations against critical infrastructure;
- Challenges in defending aging infrastructure against advanced cyberattacks;
- The role of asset visibility and defensible architecture in improving resilience.

WATCH ONLINE

> “The U.S. government has been putting out declassified information to asset owners suggesting that the Chinese are ramping up those efforts.”
>
> ***- Bryson Bort***

Real-Time Deepfakes: A Growing Threat to Corporate Security

Bishop Fox's **Brandon Kovacs** on the Security Risks of Real-Time Voice, Video Cloning

The ability to create real-time deepfakes of trusted figures has transformed the landscape of corporate security threats. Brandon Kovacs, senior red team consultant at Bishop Fox, detailed how attackers can now clone voices and video in real time, enabling new forms of social engineering and fraud.

WATCH ONLINE

Ransomware Gangs Are in Decline But Still Make Lots of Noise

RedSense's **Bohuslavskiy and Smith** on How Attacks on Healthcare Show Desperation

RedSense's Yelisey Bohuslavskiy and Marley Smith believe ransomware is declining but caution that it still poses a significant threat. While attackers recycle old methods, they're taking desperate measures to target vulnerable groups such as cancer centers and to stoke fears in the marketplace.

WATCH ONLINE

How Cybercrime Fuels Human Trafficking and Gambling Scams

Infoblox Researchers on Links Between Human Trafficking, Cybercrime and Gambling

Illegal gambling operations depend on trafficked individuals to perform cybercriminal activities. Threat researchers at Infoblox explained how cybercriminals use trafficked people for pig-butchering scams and leverage European sports sponsorships to boost illegal gambling websites.

WATCH ONLINE

How Hackers Use Emergency Data Requests to Steal User Data

CyberCX's **Jacob Larsen** on Email Compromise, Doxing, Violence-as-a-Service Attacks

Cybercriminals are exploiting emergency data requests to obtain sensitive personal information from service providers and social media companies, said Jacob Larsen, team lead of security testing and assurance at CyberCX. This flaw in verification protocols puts user privacy at risk.

WATCH ONLINE

Etay Maor
Chief Security Strategist, Cato Networks

Fixing Unpatched Vulnerabilities Without Traditional Patches

Cato Networks Leader **Etay Maor** Explains Why Old Vulnerabilities Still Pose a Threat

Cato Networks Chief Security Strategist Etay Maor discussed the importance of virtual patching for defending against vulnerabilities such as Log4j, why certain enterprises struggle to patch these flaws and how visibility challenges lead to overlooked risks in critical systems.

In this video interview with Information Security Media Group at DEF CON 2024, Maor also discusses:

- The persistent challenge of patching known vulnerabilities such as Log4j;
- The effectiveness of virtual patching in mitigating exploitation risks;
- How enterprises can manage risks from AI applications and IntelBroker.

WATCH ONLINE

> “You don't actually patch the vulnerability, but you're protecting your systems against the exploitation of that vulnerability.”
>
> ***- Etay Maor***

Vangelis Stykas

Chief Technology Officer, Atropos

Ransomware Group Defenses Are Better Than Fortune 100 Firms

Atropos' **Vangelis Stykas** on How Ransomware Groups Use Custom Codes and Tor Networks

Despite their illicit activities, ransomware groups invest in custom infrastructure and maintain stringent security practices, often surpassing Fortune 100 companies. Vangelis Stykas, CTO of Atropos, explains why ransomware infrastructure is harder to exploit than enterprise systems.

In this video interview with Information Security Media Group at DEF CON 2024, Stykas also discussed:

- The role of ransomware as a service in cybercrime expansion;
- The effects of panel disruption on multiple ransomware groups;
- Predictions about how ransomware extortion schemes will evolve in 2024.

WATCH ONLINE

> “Ransomware gangs have a lot of money due to their operations, and they keep their system up to date.”
>
> ***- Vangelis Stykas***

Malachi Walker
Security Adviser, DomainTools

Tracking Elusive Cybercriminals Through Domain Analysis

Malachi Walker of DomainTools on How Scattered Spider Adapts Despite Arrests

Scattered Spider, a notorious cyberthreat group, has continued its operations despite a series of high-profile arrests. The group's decentralized structure, in which members operate independently, contributes to its resilience, said Malachi Walker, security adviser at DomainTools.

In this video interview with Information Security Media Group at DEF CON 2024, Walker also discussed:

- The decentralized operations of Scattered Spider;
- The importance of having a domain activity timeline;
- The need for proactive threat detection and incident response.

> “Once we have one domain name that we know about, we can know when this domain was spun up. That narrows our window of when we were compromised.”
>
> - ***Malachi Walker***

WATCH ONLINE

High-Profile Vulnerabilities and Exposures

Cybersecurity defenders must keep track of a constant stream of vulnerabilities and zero-days, and some of these flaws have global implications. Conference speakers and experts highlighted worrisome trends related to IT and IoT vulnerabilities in many devices, from mobile phones to EV chargers. Today. CISOs must stay vigilant for vulnerabilities on Windows, applications, websites and emerging AI tools – while preparing for the next global IT outage.

IoT Hardware Security: A Growing Concern

Alex Plaskett, security researcher, NCC Group, and Robert Herrera, senior security consultant, NCC

Hardware security remains a critical concern for IoT and embedded devices. NCC Group's Alex Plaskett, security researcher, and Robert Herrera, senior security consultant, discussed critical vulnerabilities in Sonos devices and best practices for safeguarding hardware and software.

WATCH ONLINE

Critical Remote Code Vulnerabilities in EV Chargers

Computest Sector 7's **Thijs Alkemade** on IoT and Security Risks in EV Chargers

Thijs Alkemade, security researcher at Computest Sector 7, discussed significant vulnerabilities in electric vehicle chargers. His findings highlight how attackers can exploit these flaws to remotely execute code, posing severe risks to EV infrastructure.

WATCH ONLINE

How SSH Flaws Expose Vulnerabilities, Endanger Enterprises

Rob King of runZero on SSH Misconfiguration and Best Practices for SSH Security

SSH is designed for secure communications, but common misconfigurations significantly expose systems to threats, according to Rob King, director of security research at runZero. King discussed the implications of these vulnerabilities, citing real-world breaches and best practices for SSH security.

WATCH ONLINE

How to Mitigate Downgrade Attacks Against Windows Systems

SafeBreach's **Alon Leviev** on How Organizations Can Reduce the Likelihood of Exploits

SafeBreach security researcher Alon Leviev discussed how downgrade attacks expose vulnerabilities in Windows systems. He shared insights into how attackers manipulate Windows Update processes and stressed the importance of monitoring and securing critical system components to prevent exploitation.

WATCH ONLINE

John Morello
CTO and Co-Founder, Gutsy

Unpatched Vulnerabilities Cause 60% of Cyber Compromises

Gutsy's **John Morello** on Ensuring Vulnerability Management Using Process Mining

Organizations struggle with vulnerability management, and nearly 60% of cyber compromises are caused by unpatched vulnerabilities, said John Morello, co-founder and CTO of Gutsy. He discussed how process mining can streamline remediation efforts and ensure accountability across teams.

In this video interview with Information Security Media Group at Black Hat 2024, Morello also discussed:

- How process mining improves visibility in vulnerability management;
- How Gutsy uses security process fabric to enhance traditional vulnerability management;
- How the company plans to use AI technology in vulnerability management.

WATCH ONLINE

> “We want to help you not just understand and prioritize what the most important risks are in your environment but to help you accelerate remediation and drive accountability between all the teams that are part of that.”
>
> *- John Morello*

Vivek Ramachandran
Founder, SquareX

The Inadequacies of Secure Web Gateways in Modern Security

SquareX Founder **Vivek Ramachandran** on Why Script-Based Attacks Go Unnoticed in SWGs

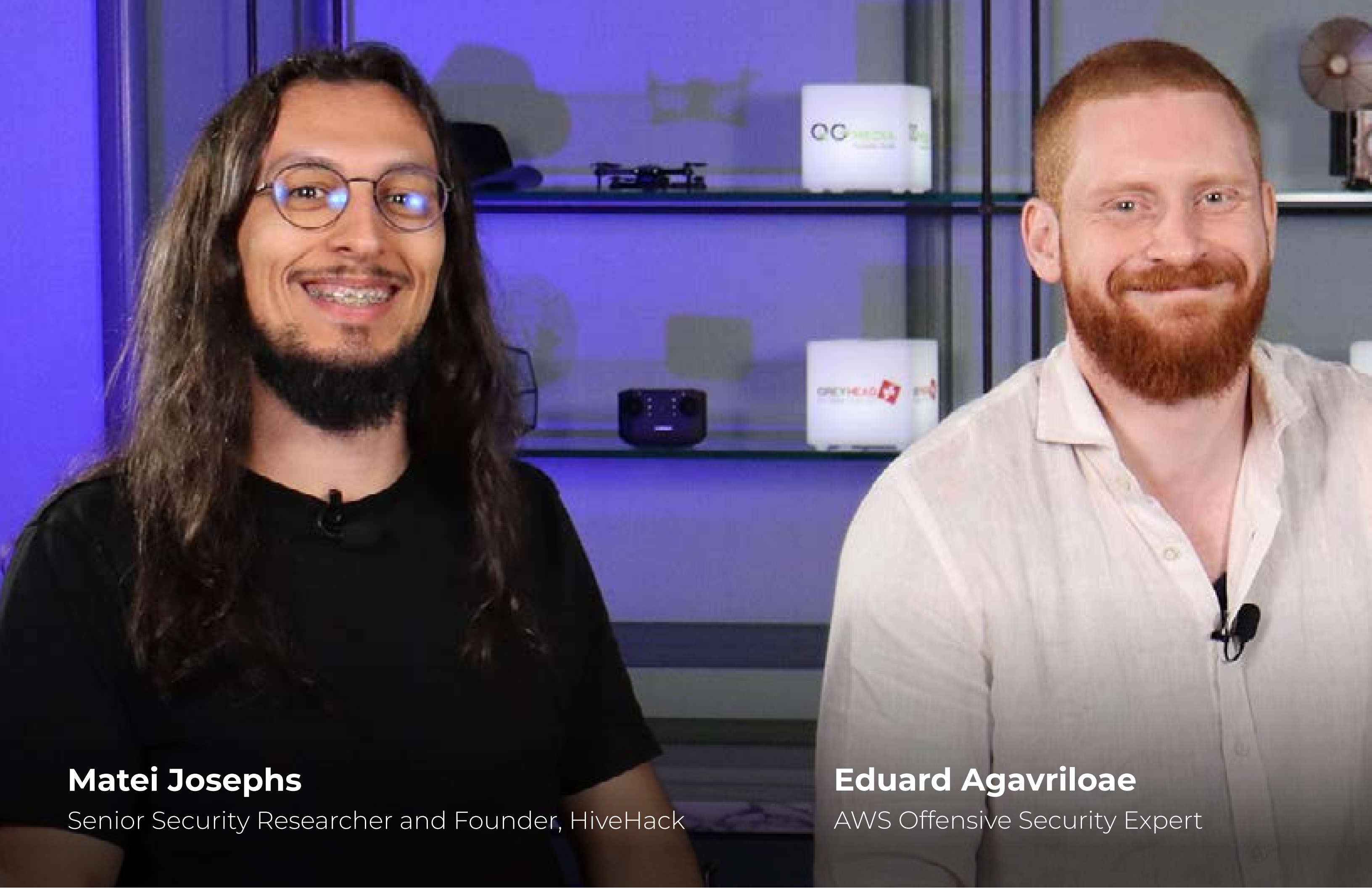
The network-centric approach doesn't capture what happens in a user's browser, and Ramachandran said attackers exploit this lack of visibility to launch script-based attacks that secure web gateways can't detect. Shortcoming make it difficult for gateways to handle attacks happening on the browser side since user interaction and dynamic page content play a critical role in delivering threats.

In this video interview with Information Security Media Group at Black Hat 2024, Ramachandran discussed:

- The limitations of secure web gateways in identifying browser-side attacks;
- How attackers exploit architectural flaws in gateways to deliver malicious content;
- The promise of browser-native security products for real-time threat detection.

WATCH ONLINE

> "Without having all of these inputs, it is impossible for them to recreate what's happening in the browser, hence making it even more difficult to detect attacks."
>
> - ***Vivek Ramachandran***



Matei Josephs
Senior Security Researcher and Founder, HiveHack

Eduard Agavriloae
AWS Offensive Security Expert

Exposed AMIs: The Hidden Risk in AWS Environments

Matei Josephs and **Eduard Agavriloae** on Public AMIs and Vulnerabilities

When developers make Amazon Machine Images public, they risk exposing sensitive data and creating vulnerabilities. Security experts Matei Josephs and Eduard Agavriloae explained how attackers can exploit these exposures, leading to unauthorized access and potential data breaches.

In this video interview with Information Security Media Group at DEF CON 2024 Agavriloae and Josephs also discussed:

- Consequences for large enterprises if sensitive data is exposed through public AMIs;
- Challenges and processes involved in responsible disclosure of vulnerabilities found in public AMIs;
- Lessons for developers and companies that use cloud services, based on the research findings.

WATCH ONLINE

> “AMI is like having a virtual machine with a snapshot, and you have access to everything that's inside the AMI. So every file, every source code, every secret that we've put in the AMI, if it's public, anyone on the internet can access it.”
>
> *- **Eduard Agavriloae***

Navigating AI-Based Data Security Risks in Microsoft Copilot

Zenity's **Michael Bargury** on AI Prompt Injection and Copilot Security Flaws

AI-powered tools such as Microsoft Copilot can be manipulated by attackers to access sensitive data and perform unauthorized actions, said Michael Bargury, co-founder and CTO of Zenity. Enterprises must address these new security challenges when adopting AI technologies.

WATCH ONLINE

Key Takeaways for CISOs From CrowdStrike's Infamous Bug

David Brumley of Mayhem Security Discusses Better Code Analysis and Staged Rollouts

The recent CrowdStrike outage has forced CISOs to rethink their approach to software updates and security practices. David Brumley, CEO of Mayhem Security, discussed why thorough code analysis, staged rollouts and stress testing are crucial for ensuring software reliability.

WATCH ONLINE

Navigating Security Threats With Return-Oriented Programming

Assistant Professor **Bramwell Brizendine** on Process Injection, Advanced Mitigation

Return-oriented programming continues to pose significant security challenges. Assistant Professor Bramwell Brizendine discussed how ROP exploits binary vulnerabilities for process injection and the advancements in tools designed to automate ROP chain generation.

WATCH ONLINE

Thomas Sermpinis
Technical Director, Auxilium Pentest Labs

The Auto Industry's Achilles Heel: Cybersecurity

Thomas Sermpinis of Auxilium Pentest Labs on Challenges of Centralized Car Systems

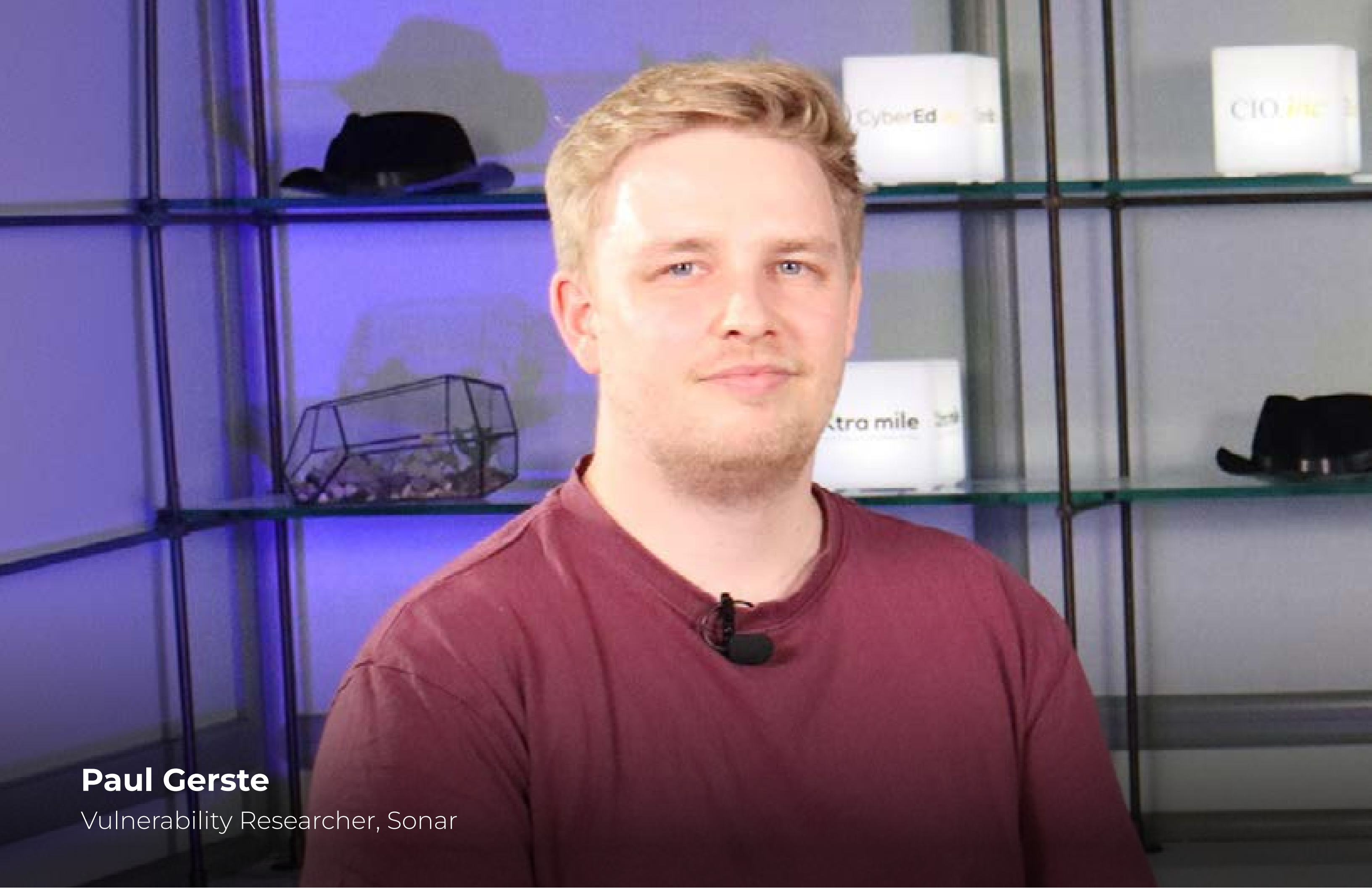
Centralized architecture in the automotive industry streamlines cybersecurity and supply chain operations by reducing hardware components and enabling quicker fixes. But that centralization also poses major cybersecurity challenges, said Thomas Sermpinis, technical director at Auxilium Pentest Labs.

In this video interview with Information Security Media Group at DEF CON 2024, Sermpinis also discussed:

- How increasing connectivity in vehicles introduces new cybersecurity risks, especially in electric and hydrogen vehicles;
- How high costs and complexity of testing in the automotive industry make it difficult to compare vulnerabilities;
- The importance of financially incentivizing researchers for robust vulnerability disclosure.

WATCH ONLINE

> “It will solve many supply chain and security issues.”
>
> *- **Thomas Sermpinis***



Paul Gerste

Vulnerability Researcher, Sonar

SQL Injection: A High-Value Target for Attackers

Paul Gerste of Sonar on Need for Developer Training to Combat SQL Injection

SQL vulnerabilities continue to plague modern applications due to their severe impact and frequent occurrence. Databases hold valuable information such as customer data and authentication details and are "high-value targets" for attackers, said Paul Gerste, vulnerability researcher at Sonar.

In this video interview with Information Security Media Group at DEF CON 2024, Gerste also discussed:

- How improper coding practices increase the risk of SQL vulnerabilities;
- The differences between traditional and memory-safe languages;
- The challenges in developer awareness and training to address vulnerabilities.

> “If you have an array and you take a random index and try to find something in that array and access something, the worst case that can happen is an error and nothing more.”
>
> ***- Paul Gerste***

WATCH ONLINE

Cybersecurity and AI Strategy and Governance

CISOs and cybersecurity teams are on the hot seat like never before, facing potential civil and criminal liability for a mishandled breach response. Experts at the conference discussed the potential effects of mandatory cybersecurity regulations as well as better guardrails for AI. With election security and federal cybersecurity strategy in the spotlight in 2024, security and risk professionals must address nagging issues related to privacy, ethics and accountability.

Jennifer Lee

Partner, Jenner & Block

CISOs on the Hook: SEC Tightens Cybersecurity Disclosures

Lee of Jenner & Block on How SolarWinds Case Ushered in New Era of Risk Management

The SolarWinds case has redefined cybersecurity disclosure obligations, especially for chief information security officers. The SEC's novel theories in this case have set a precedent for how organizations must present their cybersecurity practices, said Jennifer Lee, partner at Jenner & Block.

In this interview with Information Security Media Group at Black Hat 2024, Lee also discussed:

- The increased scrutiny on CISOs related to new cybersecurity reporting rules;
- The importance of accurate cybersecurity disclosures;
- The disconnect between CISOs' influence and their legal accountability.

WATCH ONLINE

> "SEC is going to be looking at CISOs as a subject matter expert. What CISOs need to do is have clarity on what it is that they are being asked to approve."
>
> - ***Jennifer Lee***

Brandon Pugh

Director, Cybersecurity and Emerging Threats, R Street Institute

Balancing AI Regulation: Comprehensive vs. Targeted Approach

R Street Director **Brandon Pugh** on Congress' AI Learning Curve, Future Legislation

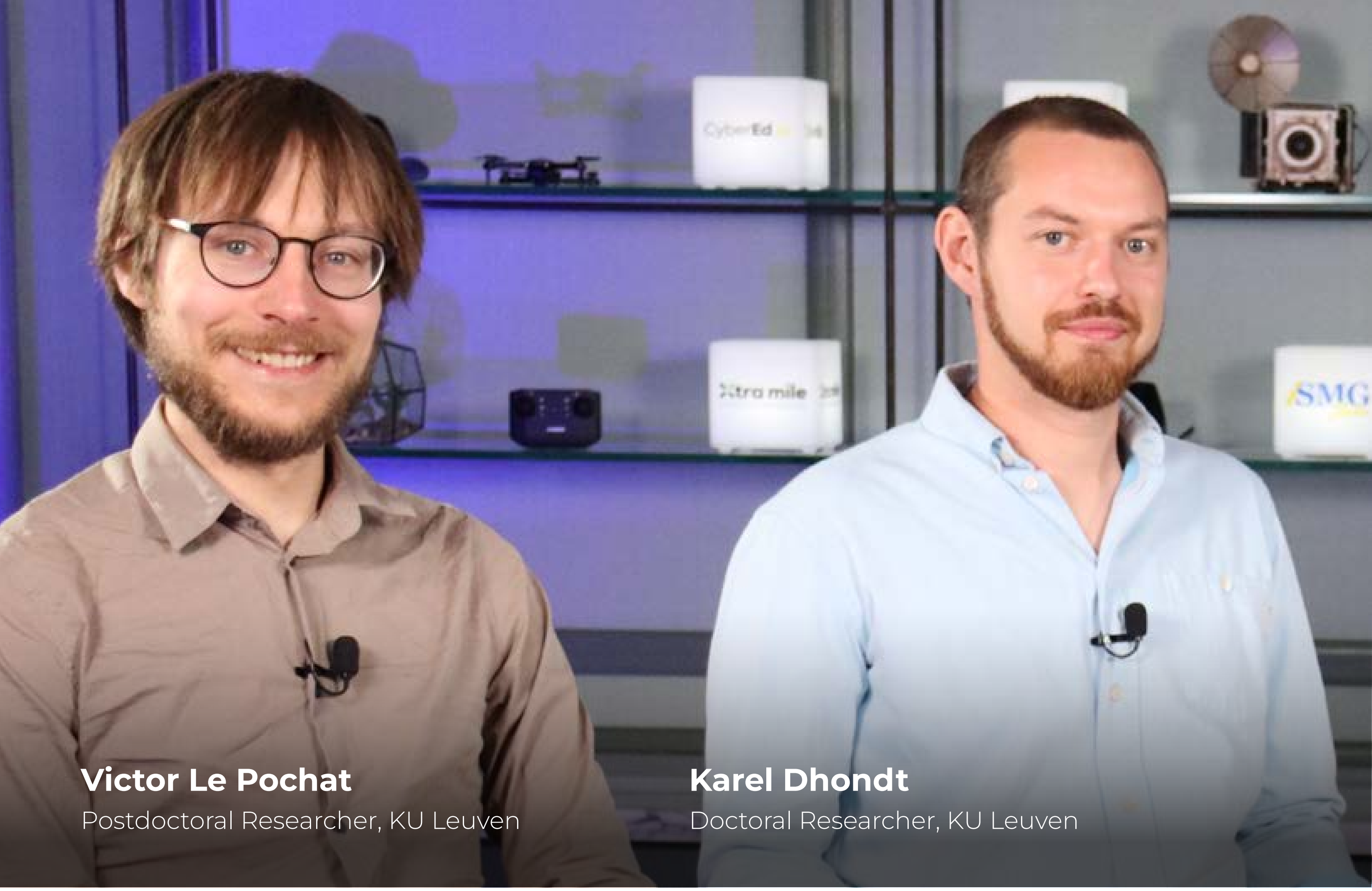
Brandon Pugh of R Street Institute discussed Congress' struggle to balance AI innovation and regulation, the U.S. approach compared to the EU, and the urgent need for privacy laws to protect AI-driven data. He emphasized education on AI technologies and the ongoing challenge of defining key terms.

> “Many are not experts when it comes to AI, and I think to their credit, they've recognized that.”
>
> ***- Brandon Pugh***

In this video interview with Information Security Media Group at Black Hat 2024, Pugh also discussed:

- The increasing complexity for multiple industries due to inconsistent state-level AI regulations;
- The contrast between the EU's strict regulatory model and the lighter-touch approach in the U.S.;
- Why there's an urgent need for federal privacy laws to protect data used by AI systems.

WATCH ONLINE



Victor Le Pochat
Postdoctoral Researcher, KU Leuven

Karel Dhondt
Doctoral Researcher, KU Leuven

Dating Apps Leak User Data, Risking Privacy and Safety

KU Leuven's Victor Le Pochat and Karel Dhondt on How API Vulnerabilities Expose PII

Dating apps collect and sell user location data, leading to significant privacy risks. Users are vulnerable to stalking, harassment and even prosecution in certain countries, said Victor Le Pochat, postdoctoral researcher at KU Leuven. Pochat and Dhont called for improved data protection measures.

In this video interview with Information Security Media Group at Black Hat 2024, Le Pochat and Dhondt also discussed:

- The types of data exposed in leaks, including personal identifiable information and usage patterns;
- How secure coding practices and encryption reduce risks associated with dating apps;
- How grid snapping can reduce location data accuracy.

WATCH ONLINE

> “Of the 15 most popular dating apps that we looked at, all of the apps leaked data.”
>
> ***- Karel Dhondt***

Michael Thiessmeier

Executive Director, U.S. National AI and Cybersecurity ISAO

Foundational Cybersecurity Is Key to Securing AI Deployment

Michael Thiessmeier of NAIC-ISAO on MLOps, Data Governance and AI Ethics

AI's integration into cybersecurity demands a strong foundational approach. Many companies seek advanced AI solutions but struggle with basic cybersecurity practices such as managing assets and patching vulnerabilities, said Michael Thiessmeier, executive director of U.S. NAIC-ISAO.

In this video interview with Information Security Media Group at Black Hat 2024, Thiessmeier also discussed:

- How deception technologies can play a significant role in AI security;
- The need to employ dynamic security configurations to disrupt attackers and enhance productivity;
- The importance of dialogue among various stakeholders - including academia, industry and the public sector - for successful AI integration.

WATCH ONLINE

> "Most companies don't understand what the assets are, but they also don't understand what that data is. It all comes first back to data governance."
>
> ***- Michael Thiessmeier***

Addressing the OT SOC Challenges in Industrial Environments

EY's **Piotr Ciepiela** Discusses Key Challenges in Implementing, Maintaining OT SOCs

Piotr Ciepiela, EMEIA cybersecurity leader at EY, discussed the challenges of securing OT systems and contrasted them with IT SOC environments. He emphasized the need for specialized tools, dedicated personnel and strong collaboration with engineering teams to manage OT SOC operations.

WATCH ONLINE

How to Account for Disinformation Risks in Election Security

CISO **Lester Godsey** on Building Custom Frameworks to Combat Election-Related Threats

Maricopa County CISO Lester Godsey highlighted the growing threat of misinformation and its impact on election security. He explained how his team is integrating cybersecurity frameworks to address both digital and physical risks, focusing on disinformation campaigns and election integrity.

WATCH ONLINE

Cyber Accountability: US Strategy Puts Onus on Big Tech

Alex O'Neill and **Lachlan Price** Discuss Key Policies of US Cybersecurity Strategy

A U.S. strategy for cybersecurity seeks to move responsibility for cybersecurity from individual users to large tech companies. Researchers Alex O'Neill and Lachlan Price explained the global implications of this shift and how corporations such as Google and Microsoft are taking the lead.

WATCH ONLINE

SolarWinds Fallout: Legal Risks for CISOs Intensify

Jess Nall of Baker McKenzie on New SEC Rules and Cybersecurity Disclosures

The SolarWinds case has intensified legal risks for CISOs. A judge validated the SEC's theory of intentional securities fraud against Tim Brown, the SolarWinds' CISO, marking the first time a federal court accepted this theory against a CISO, said Jess Nall, partner at Baker McKenzie.

WATCH ONLINE

Alberto Yépez
Co-Founder & Managing Director, Forgepoint Capital

The Cybersecurity Market: Balancing Risk and Reward

Yépez of Forgepoint Capital on AI, Economic Uncertainty, Cybersecurity Investments

Economic uncertainties and technological advancements are transforming the cybersecurity landscape. The recent breaches and the use of automation and AI by adversaries have intensified the need for robust security measures, said Alberto Yépez, co-founder and managing director of Forgepoint Capital.

In this video interview with Information Security Media Group at Black Hat 2024, Yépez also discussed:

- The need to expand cybersecurity services to underserved SMBs;
- The development of AI frameworks and standards for safe AI usage;
- The rise of shadow AI as a more insidious threat compared to shadow IT.

WATCH ONLINE

> "I wouldn't say people should be afraid of losing their jobs. They are going to be enabled to do their jobs better, and there are new skills that are going to come up. This is a great transformation."
>
> - ***Alberto Yépez***

Theresa Lanowitz
Chief Evangelist, LevelBlue

74% of Healthcare Governance Teams Vague on Cyber Resilience

LevelBlue's **Theresa Lanowitz** on Futures Report 2024 and Cybersecurity Silos

Theresa Lanowitz, chief evangelist of LevelBlue, said healthcare governance teams struggle to differentiate between cyber resilience and cybersecurity, leading to misalignment between cybersecurity and business goals. This gap exposes data and organizational operations to cyberthreats.

In this video interview with Information Security Media Group at the 2024 Healthcare Cybersecurity Summit, Lanowitz also discussed:

- How IoT devices and remote monitoring add complexity to healthcare cybersecurity;
- The challenges of digital transformation and data usage in healthcare;
- The role of cyber resilience in ensuring patient safety during IT outages.

WATCH ONLINE

> “Governance teams don't know what cyber resilience is, and they can't differentiate it from cybersecurity.”
>
> *- **Theresa Lanowitz***

AI/Machine Learning and Emerging Technologies

The technology that secures the enterprise must constantly evolve to keep pace with an onslaught of new cyberthreats. These experts in cyber defense shared the latest innovations in enterprise browser, cloud security, threat detection, and monitoring and incident response technologies. AI and machine-learning capabilities promise to simplify processes and add scale to security organizations, but they also pose emerging risks through data leakage, coding issues and hallucinations.

Mike Fey
Co-Founder and CEO, Island

Enterprise Browser Supporting Healthcare, Cyber Resilience

Island Co-Founder, CEO **Mike Fey** on How the Enterprise Browser Combats Disruption

Mike Fey, co-founder and CEO of Island, highlighted how the enterprise browser's adoption has surged across sectors. He delved into new use cases, including resilience, healthcare and inter-company collaboration.

In this video interview with Information Security Media Group at Black Hat 2024, Fey also discussed:

- Enabling secure access to critical systems in healthcare organizations;
- Enhancing productivity by automating repetitive tasks in call centers;
- Supporting enterprise resilience during outages and cyberattacks.

WATCH ONLINE

> “We have entire organizations that have integrated us in their identity stack, have us stood up on the side, and literally - in a moment's notice - can bring up their entire company on alternate devices.”
>
> - ***Mike Fey***

Ravi Ithal
Co-Founder and CTO, Normalyze

Why Discovering Shadow AI Is Key to Protecting Data

Normalyze's **Ravi Ithal** on the Rise of LLMs and the Security Challenges They Pose

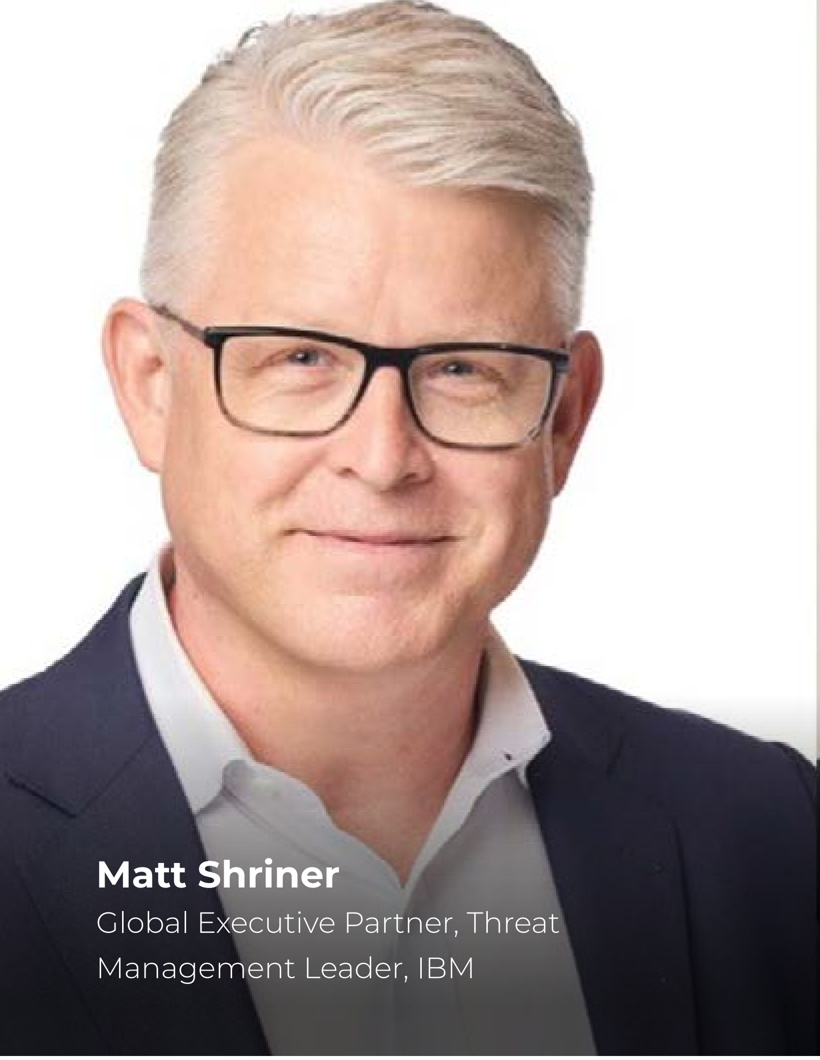
As enterprises embrace generative AI, security concerns grow. Ravi Ithal, co-founder and CTO of Normalyze, outlined how large language models, or LLMs, increase risks such as data leakage and shadow AI, and he urged businesses to prioritize discovery and data protection.

In this video interview with Information Security Media Group at Black Hat 2024, Ithal also discussed:

- Tools and strategies for protecting data in generative AI applications;
- How shadow AI presents new risks by bypassing traditional security controls;
- How Normalyze is helping clients secure LLMs.

> "The number one step is to discover shadow AIs. And number two: Think about how to protect them."
>
> *- **Ravi Ithal***

WATCH ONLINE



Matt Shriner
Global Executive Partner, Threat Management Leader, IBM

Kevin Kin
Global Vice President of Systems Engineering, Palo Alto Networks

AI-Driven Partnership for Enhanced Threat Detection

Palo Alto Networks' **Kin** and IBM's **Shriner** on Cloud Risks and AI Solutions

Kevin Kin, global vice president of systems engineering at Palo Alto Networks, and Matt Shriner, global executive partner of threat management at IBM, outlined the role of AI in the cybersecurity landscape, the evolution of threats, and collaborative solutions.

In this video interview with Information Security Media Group at Black Hat 2024, Shriner and Kin also discussed:

- How the proliferation of multiple security tools creates management challenges;
- The challenges and transformations in modern enterprise security;
- The need for security leaders to assess their current tools.

> "Organizations are making themselves easier to exploit, and 99% of cloud environments suffer from over-provisioned accounts."
>
> ***- Kevin Kin***

WATCH ONLINE

Brian Dye
Chief Executive Officer, Corelight

Corelight's Brian Dye on NDR's Role in Defeating Ransomware

Corelight CEO Shares How NDR Solution Improves Incident Response and Cloud Security

Network detection and response delivers ground truth in cybersecurity, giving organizations crucial visibility into attacker behavior before, during and after ransomware attacks. Corelight CEO Brian Dye explains how NDR helps security teams verify threats and contain incidents effectively.

In this video interview with Information Security Media Group at Black Hat 2024, Dye also discussed:

- The balance between network breadth and endpoint depth in cybersecurity;
- The importance of network visibility in validating containment after an attack;
- Effectively addressing cloud visibility challenges through network monitoring.

WATCH ONLINE

> “There's no honor among thieves. The attacker claimed they had stolen about 10 times more than they did.”
>
> *- **Brian Dye***

Nonhuman Identities: A Growing Threat in the Cloud

Entro Security's **Adam Cheriki** on Non-Human Identity Lifecycle Management & Secrets Security

As cloud adoption accelerates, the unchecked growth of nonhuman identities is exposing companies to increased risks. Adam Cheriki, CTO and co-founder of Entro Security, explained why securing these identities is crucial and how the company's platform delivers a comprehensive solution.

WATCH ONLINE

MLOps Platforms: Why Models Should Be Treated as Code

JFrog's **Shachar Menashe** on MLOps Platform Vulnerabilities and Code Execution Risks

Shachar Menashe, senior director of security research at JFrog, discussed critical security risks in MLOps platforms - including code execution vulnerabilities in machine learning models - and why organizations must treat ML models as potentially malicious code to mitigate these inherent risks.

WATCH ONLINE

Building Timely and Truthful LLMs for Security Operations

NYU's **Brennan Lodge** on Training Your Own Model With Retrieval-Augmented Generation

Many cybersecurity organizations hope generative artificial intelligence and large language models will help them secure the enterprise and comply with the latest regulations. But to date, commercial LLMs have big problems - hallucinations and a lack of timely data, said NYU professor Brennan Lodge.

WATCH ONLINE

Autonomous AI and US National Security: A Double-Edged Sword

DARPA Deputy Director **Matt Turek** on Managing Autonomous AI Risk in Critical Systems

AI systems acting autonomously bring risks of large-scale mistakes that current human defenses can't match, said Matt Turek, deputy director at DARPA. He discussed AI agents, adversarial attacks and the need for provable AI safety in both offensive and defensive capacities.

WATCH ONLINE

Chris Bisnett
CTO, Huntress

What Does an Ideal SIEM Look Like? Inexpensive

Huntress' **Chris Bisnett** on a New Approach to SIEM for Cost-Effective Security

Huntress CTO Chris Bisnett outlined the firm's innovative approach to simplifying SIEM by reducing data storage costs and focusing on relevant logs. These services support small and midsized businesses looking to enhance their security posture without the high expenses of a traditional SIEM.

In this video interview with Information Security Media Group at Black Hat 2024, Bisnett also discussed:

- The evolving role of SIEM in the cybersecurity insurance landscape;
- Why Huntress is unique in the SIEM marketplace;
- Reducing SIEM costs by focusing on storing only critical security data.

WATCH ONLINE

> "What drives that cost? Overall, it's data. So, we said: 'Let's find the things that we think are important and just throw away the noise."
>
> ***- Chris Bisnett***

John Wrobel
CRO, Menlo Security

Turning Commercial Browsers Into Secure Enterprise Products

Menlo Security Chief Revenue Officer **John Wrobel** on Thwarting Browser-Based Attacks

John Wrobel, CRO of Menlo Security, highlighted how virtual cloud browser technology stops malware, ransomware and credential harvesting. Menlo turns users' existing browsers into secure enterprise browsers, eliminating the need for new software while ensuring protection against web-based threats.

In this video interview with Information Security Media Group at Black Hat 2024, Wrobel also discussed:

- The top vulnerabilities adversaries exploit in modern browsers;
- Menlo's virtual cloud browser and how it protects against malware;
- The challenges of driving budget for secure browser adoption.

WATCH ONLINE

> "We actually render all the active content within our service and then mirror that back to the end user without any degradation in user experience, ensuring that nothing bad can come through the browser."
>
> *- John Wrobel*

Closing the Gap: Why ADR Is Crucial for Application Security

Jeff Williams of Contrast Security on the Need to Defend Apps and APIs With Application Detection

Jeff Williams, founder and CTO of Contrast Security, introduced ADR, a solution designed to address the visibility gap in security operations by monitoring applications and APIs. He explained how ADR blocks and detects attacks, preventing the exploitation of vulnerabilities.

WATCH ONLINE

AI: The Most, and the Least, Hyped Technology

Zscaler CISO **Sam Curry** on AI's Role in Offense and Defense in Cybersecurity

Artificial intelligence, much like when the internet became public, is simultaneously the most overhyped and underhyped technology in history, said Sam Curry, vice president and CISO at Zscaler. Its application in cyber defense is still evolving.

WATCH ONLINE

Security Experts Prioritize AI Safety Amid Evolving Risks

Nathan Hamiel of Kudelski Security on Security Testing and Biased Algorithms

As artificial intelligence technology continues to evolve, security professionals have become involved in areas that traditionally weren't their concern such as preventing biases in decision-making, said Nathan Hamiel, senior director of research at Kudelski Security.

WATCH ONLINE

AI/ML's Role in Cybersecurity: Balancing Innovation, Safety

Trail of Bits' **Michael Brown** on the Intersection of AI/ML and Cybersecurity Threats

Trail of Bits' Michael Brown explored the dual challenges of applying AI and ML to cybersecurity and securing these evolving technologies themselves. He discussed the complementary nature of traditional and AI/ML-based approaches and highlighted the pressing need for secure development life cycles.

WATCH ONLINE

Randall Degges

Head of Developer and Security Relations, Snyk

Why AI-Assisted Coding Tools Amplify Code Quality Gaps

Snyk's **Randall Degges** on the Crucial Role of Code Base Quality in AI Output

AI-assisted coding tools can speed up code production but often replicate existing vulnerabilities when built on poor-quality code bases. Snyk's Randall Degges discusses why developers must prioritize code base quality to maximize the benefits and minimize the risks of using AI tools.

In this video interview with Information Security Media Group at DEF CON 2024, Degges also discussed:

- The role of security flaws, code consistency and update frequency in evaluating AI coding tools;
- Best practices for maintaining high-quality code in AI-assisted environments;
- Challenges that AI tools face in identifying context-specific security vulnerabilities.

> “There's tons of code in the world. Tons of people are writing them. Most of it is not being kept up to date and perfect all the time.”
>
> - ***Randall Degges***

WATCH ONLINE

Chris Wysopal
Co-Founder & Chief Technology Officer, Veracode

AI-Generated Code: Benefits vs. Downsides

Chris Wysopal of Veracode on Addressing Vulnerabilities in AI-Assisted Development

Generative AI tools boost developer productivity, but they also generate code with similar vulnerability rates as human developers. Chris Wysopal, co-founder and CTO of Veracode, explained why enterprises must treat AI-generated code with caution and automate security testing.

In this video interview with Information Security Media Group at DEF CON 2024, Wysopal also discussed:

- Why automated security testing is crucial as AI-driven development accelerates code production;
- The potential for AI to self-inspect and address security flaws in generated code;
- The importance of curated datasets for training AI models on secure coding.

> "If we have similar vulnerability density, but we're creating code at a faster rate, we, as security people, have to think about ending up with a secure application at the end of the day."
>
> *- **Chris Wysopal***

WATCH ONLINE

About ISMG

ISMG is the world's largest media organization devoted solely to cybersecurity and risk management. Each of its 38 media properties provides education, research, and news that is specifically tailored to key vertical sectors including banking, healthcare, and the public sector; geographies from North America to Southeast Asia; and topics such as data breach prevention, cyber risk assessment, AI, OT, and fraud. Its annual global summit series connects senior security professionals with industry thought leaders to find actionable solutions for pressing cybersecurity challenges.

Contact

(800) 944-0401
info@ismg.io

Sales & Marketing

North America: +1-609-356-1499
APAC: +91-22-7101 1500
EMEA: + 44 (0) 203 769 5562 x 216

CAREERSINFO SECURITY® BANKINFO SECURITY® GOVINFO SECURITY® HEALTHCAREINFO SECURITY®

CUINFO SECURITY® Just for Credit Unions · Data Breach. Prevention. Response. Notification. TODAY · infoRisk® TODAY · AIToday.io · OT.today · CIO.inc

CyberEd.io · CyberEdBoard · DeviceSecurity.io · FraudToday.io · PaymentSecurity.io

CYBER THEORY · GREYHEAD AN ISMG COMPANY · Xtra mile LIFECYCLE MARKETING · QG MEDIA · ATHENA

iSMG

902 Carnegie Center • Princeton, NJ • 08540 • www.ismg.io