Summary & Notes:
Detroit Cybersecurity & Fraud Forum - 16 April 2026

This document summarizes in detail the presentations and associated discussion points from the Detroit Cybersecurity & Fraud Forum held at Eastern Michigan University on 16 April 2026.

All of the presentations and additional reference materials, as well as summary info from supporting organizations and the full Q&A is available via for this Forum via the CxO Security Forum Online Community Portal at https://www.engagez.net/CxO#lct=customlocation-Location12.

Agenda Overview

Registration & Networking	8:30 AM
Welcome	9:20 AM
Introductions- Associations & Agencies	9:30 AM
1. Guardians of the Machine Age: AI is poised to disrupt everything **Richard Stiennon**	9:45 AM
2. Who to Call, What to Share, and How to Get Real Help **John Felker**	10:20 AM
Break	11:00 AM
3. Espionage, Negotiation, and the Battle for Digital Control	11:15 AM
5. It's Not Just Bad Hygiene—It's Criminal Negligence **Special Agent, Carlo Nastasi**	1:15PM
6. Agentic AI Meets Zero Trust: What Actually Breaks—and How to Fix It **Josh Woodruff**	1:50 PM
Break	2:15 PM
7. Degrees, Certs & Grit: What Cyber Grads Can (& Can't) Do **Panel Discussion**	2:30 PM

Kurtis Minder

4. The CVE Ecosystem Today & the AI Agents Burning Watts to Fix It — 11:50 AM

Tim Rohrbaugh

Lunch — 12:20 PM

Introduction

Michael Hiskey — Start 09:36

- Emphasized the importance of community building, and discussions surrounding Cybersecurity, and how keynotes from enterprise representatives may aid in engaging discourse to build a stronger sense of technical best practices
- Leveraged the CxO Security Forum to bring together interactive networking with the forum prioritizing depth over volume, conversation over content dumping, and peer credibility over promotion . Moreover, the CxO Security Fraud Forum brings together a wide range of credible CIOs, CISOs, Chief Security Analysts, higher-education security executives, GRC leaders, and other senior decision-makers who are responsible for protecting their organizations PII, guiding strategic risk, and navigating the evolving role of AI in security.
- **CxO Security Form** additionally aims to promote unique discussions with a chatham house rule, to effectively interact and engage with the crowd. Micheal prioritizes QA, centralized discussion forms via the CxO Security Forum Online Community Portal at www.engagez.com/cxo
- More details on can also be found on the LinkedIn Community Page at https://www.linkedin.com/company/cxosec
- This was the first “Detroit Cybersecurity & Fraud Forum,” although we pulled ideas from a long past “Detroit Cybersecurity Conference” put on by Richard Stiennon from IT-Harvest more than 10 years ago.

Supporting Organizations

Blumira

- Blumira is an open Security Operations platform that *provides busy IT teams with ransomware protection*, compliance support, detection & response and more.
- SIEM charges are not worth overall pricing or annual licensing
- More efficient logging (dump any logs needed or preferred), leveraging the platform may be much more accessible to average. end user, better for smaller teams, or organizations. Doesn't take too much time to reinforce, implement, or align within current security controls
- No volume charges; Lower the entry point for a SOC analyst; Blumira will walk through the vulnerability to assist the worker

  Contact: Zoe Lindsey zlindsey@blumira.com

EasyDMARC

Contact: Colin Heath colin.heath@easydmarc.com +1 (703) 855-6752
https://easydmarc.com/

- Trusted partner with 200,00+ connections
- National, 24/7 world-class support
- Deliver robust, scalable, and long term security solutions for domains, with easy to use reports and automated assessments
- Includes a domain scanner that provides ample risk assessment regarding vulnerabilities, threats of email impersonation attacks, and Sender Policy Framework enhancements tied to a domain.
- Trusted by over 175,000 domains

ISSA Motor City Chapter

Arun DeSouza, President arun.desouza@profortissolutions.com
https://motorcityissa.com/index.html

- A venue for cybersecurity professionals to meet, network, and discuss industry trends within the ever-growing cybersecurity landscape
- Regular meetings (virtual and in-person) featuring guest speakers, technology presentations, and "Career Corner," which connects professionals with recruiters.
- Membership is comprised of people working in automotive, banking, finance, consulting, human resources, law enforcement, communications, manufacturing, energy, education, healthcare, military, government, and retail.
- Meetings in Troy and Livonia to reach out to entire metro Detroit area

- Seminar: June 1-2 AI seminar; $300 members $500 non-members
- 120 members that are employed in more than 34 different organizations.
- Earn CPEs through Conferences and Education

ISACA Detroit Chapter

Angelo Toppi, President Angelo.Toppi@plantemoran.com
https://engage.isaca.org/detroitchapter/home

- Industry standard regarding cybersecurity for more than 55 years, hosting CISA, CGIET, CRISC, and CISM certifications.
- Heavy focus on audit governance, risk, and compliance
- Info security with AI auditing implemented within their program (1000+ members)
- Maintains updated AI certifications
- Question normalized assumptions of the current technical climate, reworking usual deployment techniques from a governance and risk perspective.
- AI auditing with concentration on GRC

ACFE Southeast Michigan Chapter - SEMCACFE

Luke Voldahl - Board Member
https://semcacfe.org/

- Expertise in Fraud examination
- ACFE: More than 95,000 members
- Committed to further educating and training qualified individuals in detecting, investigating and deterring fraud and white-collar crime.
- Hosts Chapter Dinner Meetings and Annual Conferences

Eastern Michigan University

GameAbove College of Engineering & Technology

Mohammed Qatu, Dean
Dr. Jared Olouch, Chair - Cybersecurity

https://www.emich.edu/cet/index.php

- First educational program in nation to offer all bachelors, masters and phd program for Cybersecurity
- Largest program in the college of engineering and technology. Over 400 students

- Prepares prospective students with the knowledge and skillset necessary for future computing and cybersecurity professionals to build, maintain and protect networks and computer systems in both government and industry positions.

Cloud Security Alliance- Detroit Chapter

Leon Dupree, Board Member
https://www.csadetroit.org/

- Provide scholarships for students, bring in industry leaders, host talks, panels, reduce barrier entries for students
- Provides education, networking, and mentorship opportunities & keynotes to security practitioners
- Fosters connections among local security professionals

ISC2 | Greater Detroit

Don Gates, President don.w.gates@gmail.com
https://www.isc2greaterdetroit.org/

- CISSP certification
- Co-sponsored events with other industry associations
- Goal of one million certified in cybersecurity; Goal of at least 150 users to bring into their membership program
- Local community outreach

FBI Detroit Field Office

Supervisory Special Agent Andrew Sczygielski

- Both criminal and national threat actor preventive org
- Coordinator of Cyber Crime task force
- Responsible for figuring out “Who is behind the computer” during criminal investigations (cyber related)
- Attribution, dealing with Adv. Persistent threat actors
- Hosts internship program for the FBI (comp sci as well)
- Heavy focus on incident Response
- Open ended forum to report issues – https://www.ic3.gov/

Discussion Summaries

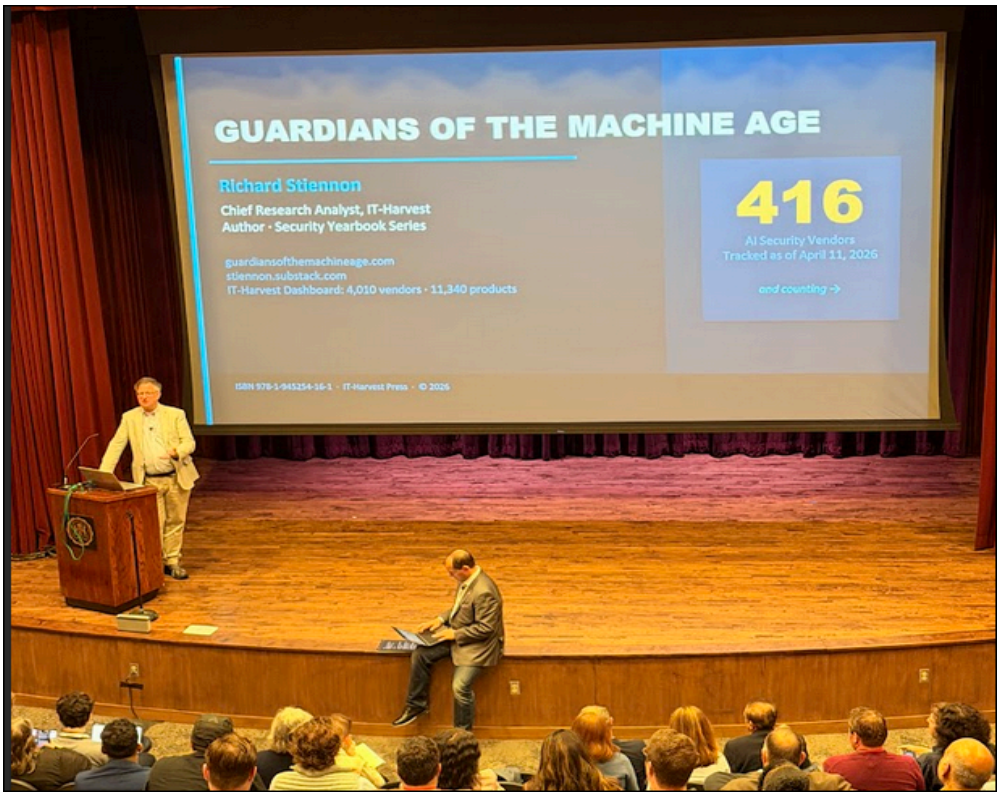
Guardians of the Machine Age: AI Security is poised to disrupt everything, including security [Discussion Pod #1]

9:45 AM

Richard Stiennon, industry analyst and author of Guardians of the Machine Age: Why AI Security defined the Future of Digital Defense, with updates on the state of AI Security He explains how he tracks and analyzes 400+ startups in the most rapidly expanding sector of cybersecurity in history. He explains why your SOC teams are going to become a thing of the past as automation proves more effective and lower cost.

This talk was not just about the numbers. Richard broke down the practical implications for executives:

- The adoption of ChatGPT was the fastest growing consumer traction in human history.
- In just three years an entire industry of 416 vendors has sprung up to either protect AI or take advantage of it.
- Get ready for massive increase in breaches assisted by AI
- SOC Automation to the rescue.



Overview:
Richard Stiennon, veteran analyst and industry provocateur will kick off the Forum, taking us on a data-rich tour of the entire cybersecurity industry—all 4,159 vendors, 660 subcategories, and $12 billion in recent funding. Drawing from his forthcoming book, Stiennon will share insights

derived from two decades of studying cyber trends at Gartner and now IT-Harvest—the only firm systematically cataloging the global cyber vendor ecosystem.
AI shocked the industry and was born in three years. It had 100 million users in 2 months and 1.5 trillion dollars funding it. Richard Stiennon's talk wanted to express why AI Security will define the future of digital defense. He wanted to catalog the entire cybersecurity field. He talked about the rise of AI start-ups securing AI in late 2022. He said that it is the fastest growing tool in human history. His book Catalogs 378 vendors that are already in AI security. They have a market value of 5.7 billion and 9% of the total cybersecurity vendor space.
"Three years ago, a million tokens of AI inference cost $60. Today? Six cents. AI is now diffusing faster than any technology in history — into every industry, every workflow, every device." — Nina Schick, AI Expert & Advisor
While AI can help with internal operations, Stiennon also mentions that it can also enhance the attacker.

- Phishing 2.0: hyper-personalized phishing emails that evade filters and context match. (596 products counter these phishing scams)
- Deepfake attacks: Videos or voice clips generated by AI that can be used for social engineering purposes.
- AI malware: LLM can assist in scripting, therefore accelerating the kill-chain for bad-actors
  Stiennon Internal Threats Areas where a companies AI model may cause issues
- Data leakage: through specific prompting, AI models may leak sensitive company data from its database
- Shadow AI: Workers will find work arounds if AI tools are blocked and therefore companies lose control
- Jailbreaks: talks about a methodology called Do Anything Now. This reveals how easy alignment goals can be overridden.
- Model Abuse: deploying hugging face models to create new surfaces with no governance

Stiennon talks about how we are in the regulatory wave and that GRC is the most important topic in AI security. Below are some frameworks that he touches on more deeply in his book:

- EU AI ACT
- NIST AI RMF
- ISO/IEC 42001
- OWASP AI Exchange

GRC is also becoming more technical and must be enforced in code. There are currently 35 AI governance vendors, 25 guardrail vendors, and 18 model protection vendors. These guardrails enforce data protection coming in and out, injection defense, and usage to avoid any exploits in AI systems
Stiennon highlighted 5 hard truths that he mentions in his book.

1. AI is a trust engine, and attackers will target the trust first.
2. Models will make decisions, and they need someone or another model to monitor the decisions
3. the risk is shifting to what the system decides instead of the user, which requires 24 hour autonomous defense systems

4. GRC is policy AND code
5. security breaches will drive the market for IA security

AI is being implemented in cyber roles as SOC analysts, pen testers, and vulnerability management. 300 million dollars in Annual Recurring Revenue are projected by the end of the year using AI automation in SOC. Stiennon ends the presentation by stating that Cybersecurity will transition into AI security in the coming years. He adds that a complete disruption in cybersecurity will start this year in which 50,000 new vulnerabilities were discovered this year alone. Stiennon left CISOs in the room with advice to look for startups and evaluate their products, monitor the vendors being used, and calculate the ROI with the company as a vendors

Key Statistics:

- Open AI platforms gaining approximately 100M new users in two months, and $1.5T dollars in global, annual spending (est.)
- Retained 300 million ARR (Annual Recurring Revenue) by the end of the year using AI automation in SOC
- Only took approximately 72 hrs. to write scripts to effectively re work spreadsheet storage / information management into an actual usable application (6 weeks after openAI model was available)
- 187 legacy vendors are additionally adding AI Security products within their core operations
- Found Open AI wrote approximately 3000 descriptions on vendors in 3 days, costing the company around only $450 dollars
- Catalog of 100 vendors that are already in AI security. Richard currently oversees 8 AI security vendors, prioritizing forward security planning, pointing out the importance of training models with a certain purpose for the model in mind
- SOC automation: 62 different vendors in SOC automation

Notable Insights:

- Points out DAN (Do anything now), “Grandma Exploits,” and role play based prompts effectively bypassing alignment goals and safeguards AI developers attempt to implement.
- Agents shift risk from ‘what a user may click’ -> ‘what a system decides’
- Out of 512 startups analyzed, only 295 included any specific model optimized for cybersecurity

GRC compliance adopting AI certifications and provisioning legal frameworks surrounding the usage of AI

Find more information from stiennon.substack.com; guardiansofthemachineage.com

QA:

Q: “ Is AI going to put Gartner out of business?” A: “We will adjust, stock was tanked originally from representatives being unable to answer crucial questions about AI (sales call)”

Q: “Where am I gonna get the most from mature offerings?”

A: AI SOC will give the best security return. Approve concepts. In the current industry, it's hard to get attention with these AI startups"

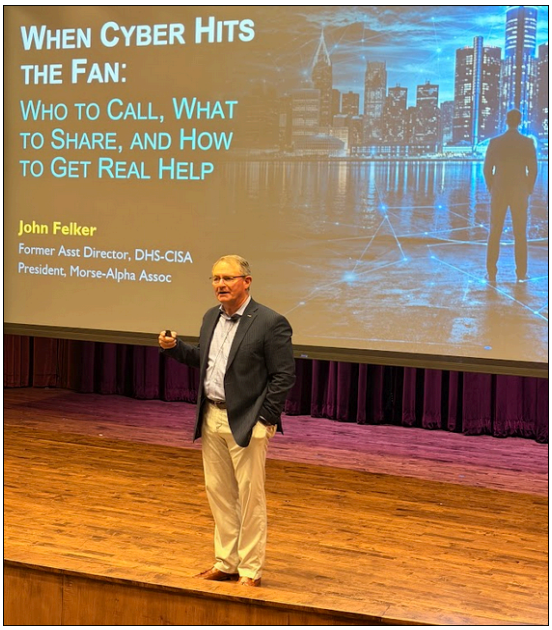
Q: What advice do you have for leaders that have legacy tech? How to get "cherries" from legacy tech?
A: Look at the startups. Evaluate the current technical climate. Monitor ALL vendors/Hardware, use automation and tooling to evaluate, and then focus on ROI.

Q: "How do you see the AI security landscape shifting in the wake of a possible market correction?"
A: "Enterprise solutions like Splunk may be too expensive via annual licensing for what they provide. I am immediately seeing solutions shifting from different companies. Market share is also shifting. SOC Analysis -> AI "

When Cyber Hits the Fan: Who to Call, What to Share, and How to Get Real Help [Discussion Pod #2]

John Felker, former Assistant Director for Integrated Operations at the Cybersecurity and Infrastructure Security Agency (CISA), led a discussion that cut through one of the most persistent challenges in cybersecurity: how to actually engage government partners when it matters most. Drawing on decades of leadership across government, military, and the private sector, Felker clarified how key agencies fit together, when each should be engaged, and how organizations could build relationships before an incident occurred.

When a serious cyber incident unfolded, most security leaders faced the same questions: who to call first, what to share, and how to get meaningful help quickly. Between CISA, the Federal Bureau of Investigation, the United States Secret Service, regulators, ISACs, state fusion centers, and InfraGard, the landscape often felt fragmented—especially under pressure. Felker emphasized that while the structure may appear complex, outcomes ultimately depend on speed and trust, not organizational charts.



A central theme of the discussion was the need to treat the private sector as a true peer—not a downstream customer. Felker noted that private-sector organizations now often develop threat intelligence as fast as—or faster than—the government, particularly as AI-driven threats accelerate. Effective defense, therefore,

depends on real-time, two-way collaboration and the ability to share actionable intelligence—not delayed reports.

He reinforced that preparation must happen long before a crisis. Building relationships with crisis management teams, legal counsel, regulators, and government agencies in advance was positioned as essential to reducing friction during incident response. ISACs and intermediary organizations were highlighted as critical mechanisms to scale trust and enable faster, more coordinated action across sectors.

Felker also challenged organizations to operationalize cybersecurity decision-making within core business functions. Incident response planning, board-level engagement, and legal alignment should not be reactive exercises—they must be embedded into how companies operate day-to-day. A lack of transparency and basic controls, such as multi-factor authentication, continues to be a root cause of avoidable failures, as seen in high-profile incidents like the Colonial Pipeline ransomware attack.

Looking ahead, Felker pointed to emerging risks tied to AI and quantum advancements, which are expected to further compress attack timelines and increase complexity. In that environment, he advocated for streamlined, common-sense regulation and a shift toward shaping adversary behavior through coordinated public-private action.

The moderated discussion that followed focused on practical, real-world scenarios: when to call CISA versus the FBI, how to engage government partners without triggering unnecessary scrutiny, how to integrate ISACs and InfraGard into an enterprise threat intelligence strategy, and how CISOs can build trusted relationships across both internal stakeholders and external partners before an incident occurs.

Key Insights

- Speed and Trust matter more than structure
- “Do we involve the board, do we bring the counsel?” – John points out the importance of a cybersecurity disaster recovery, and incidence response planning being embedded within companies usual business functions
- Proves criticality in organizations maintaining a ‘regulatory agency’ that may take the form as first hand incident response team regarding a data breach or security incident

Upcoming Trends:

- Quantum networking may be heavily focused in development after AI becomes more normalized, which will increase the speed of attacks further. Still figuring out how to network quantum computing
- Points out the normalized displacement from companies in one department or another (inner workings of departments) being on completely different pages from a cybersecurity perspective
- “Treat private sector as a peer, not a customer”
- Private or public sectors are just as talented regarding cybersecurity principles and technical best practices as government lead agencies (three letters)

- While in DHS; John was attempting to promote importance of delivering actionable intelligence, NOT reports, or drawn out technical documents
- Operationalize decision-making for industry standards. Shape advisory behavior and promote common sense regulation
- Infraguard: FBI maintained source of knowledgeable intelligence for security analysis and insight into possible vulnerabilities
- Calls out importance for institutions within the industry to build strong channels of communications with other internal orgs, for finding possible low hanging fruit attack vectors BEFORE incident response or disaster recovery is necessary
- Use ISCAS and Intermediaries to scale trust

Q&A Highlights

Q: "Many in workplaces distrust and dislike those in the CyberSec department of their work. How can we bridge the gap and help them understand we are on the same page?"
A: "Must get legal team authorization from management representatives on board for government inclusion to facilitate your companies security concerns"

Q:"Biggest mistake from the private sector?" A: References Colonial Pipeline Ransomware Attack: "Lack of MFA, shutdown of oil pipeline was mostly unnecessary due to previous isolation of systems. Biggest mistake you see: not being straight forward about the events"

Q: How can we leverage private sector collaboration A: "Start discussions with security oriented organizations, such as Palo Alto. Many companies move quicker than the FBI at times, and can provide strong assistance for aligning well tested security practices"

Q: What to do when security principles are undermined, but business interests are prioritized? A: "Get your company's representatives' attention on the business side regarding cybersecurity! – Government bodies that may aid in incident response include local law enforcement, and the NYPD - Cyber dept. Also get involved to see the logistics and background behind cybersecurity concerns"

Q: In your experience with CISA, do regulators not meet specific requirements? A: Regulators are required to provide inspections, orgs need chances to meet and personally talk to each other's auditing company

Q: What's your advice for staying up to date? A: Figure out who knows what, and understand what challenges certain people or organizations are facing. Personability and familiarity is of the utmost importance for incidence response

Inside the Mind of the Adversary: Espionage, Negotiation, and the Battle for Digital Control [Discussion Pod #3]

Kurtis Minder, Founder and CEO of GroupSense, delivered one of the most visceral and reality-grounded sessions of the Forum—pulling back the curtain on how ransomware and digital extortion actually unfold in the real world. Drawing from a decade of negotiating directly with cybercriminals, including ransomware gangs and nation-state affiliates, Minder grounded the discussion not in theory—but in lived operational experience.

Rather than focusing purely on defense, Minder reframed the conversation around resilience. He made it clear that modern ransomware is no longer just about encrypting files—it is about full-scale extortion. Threat actors exfiltrate sensitive data, weaponize it, and apply pressure not just to organizations, but to employees, customers, and partners. The audience heard firsthand how these attacks play out, including real-world ransom communications outlining stolen data, escalation tactics, and payment instructions.

A key insight: the barrier to entry for attackers has collapsed. With the rise of Ransomware-as-a-Service (RaaS), sophisticated attacks can now be launched in hours by relatively low-skill actors. Stolen access is bought and sold, and breaches are often the result of simple, preventable failures—reused credentials, weak email security, or unpatched systems. Data presented during the session reinforced the scale of the issue, with tens of millions of compromised records circulating in the ecosystem.

Minder emphasized that every incident matters—regardless of company size—because of the interconnected nature of modern business. A breach in a small organization can quickly cascade into larger ecosystems. At the same time, he challenged leaders to confront the ethical and operational realities of ransomware response, including the difficult question of whether—and when—it may make sense to pay.

From a practical standpoint, the prescription was clear: improve cyber hygiene, strengthen credential and email security, eliminate reuse of passwords, and invest in real incident response planning. Tabletop exercises and disaster simulations were highlighted as essential, not optional. Just as importantly, organizations must understand the psychology and playbook of threat actors—because successful response often

depends as much on negotiation and decision-making under pressure as it does on technical controls.

The session also underscored a broader shift: many of today's cyber incidents are highly manual, human-driven operations—not just automated exploits. That reality reinforces the need for organizations to think beyond tools and focus on readiness, coordination, and resilience.

The discussion that followed explored how threat actors adapt when they suspect deception, whether data exfiltration tactics are truly effective, and why ransomware incidents remain so difficult to navigate—even for well-prepared organizations. The takeaway was unambiguous: in today's environment, resilience—not just prevention—is what ultimately determines outcomes.

Kurtis presented real call of hacker and ransom note, which displayed the following:

1. The data they pulled
2. Links
3. What will happen if they ignore them
4. How to recover data and pay them.

Bad actors get ransomware as a service (RaaS) from a Dark web marketplace and can be deployed within hours. Hackers break into systems and sell that information to other hackers to gain access. Kurtis showed data from SpyCloud, which revealed over 64 million records pulled from ransomware.
Every single incident, small or big matters. Because everyone is connected to someone that has important user information. Kurtis argues that a value based company may struggle to pay the ransomware because the money that helps the hacker may go towards a bad cause.
How to fix this:
Kurtis talks about better cyber hygiene and culture must be implemented. Companies should strive to change habits such as updating logs and in depth security hardening. IR planning and Table top exercises where disaster recovery is simulated should also be implemented according to Kurtis. Finally, the most important protection is in the email and credential policy of a company. Proper training and blocking usage of insecure credential managers is the biggest vulnerability to a company's sensitive data.

Critical Ideas:

- Small businesses being impacted by cyberthreats are usually being undermined, or even ignored entirely
- Spycloud data: 64 million records pulled
- Every single incident, small or big matters. Everyone is connected to someone that has important user information.
- It is not only about defense. It is about resilience. Make an IR plan!
- Today's cyber incidents have generally shifted, and are heavily manual

Ransomeware, the threat no one expects until it happens:

- Operational Technology systems and infrastructure are a high point of interest with DoS or ransomware attacks
- Presented a real world call depicting a threat actor speaking about ‘KLILN’ ransomware and data exfiltration
- Threat actors attempt to scare org. representatives in releasing PII
- Criticizes recovery software that offer services to “decrypt files” during ransomware situations, in reality just MITM threat actors and the victims involved
- RaaS opens doors for less technical hackers to exfiltrate / dump data
- Charities, or different innocent orgs masquerade true intentions through blockchain or crypto, tumbling services (e.g. monero)
- Kurtis promotes the idea of better sophisticated cyber hygiene, updating firmware / legacy software & hardware, and strong incident response
- Kurtis also provides insight into the importance of not reusing emails or personal credentials regarding corporate accounts or access to sensitive resources (Use Password Managers!)

Q&A Highlights

Q: Do threat actors realize or know you're not clients A: No. Otherwise, they threaten data dumping / deletion, or generally change the subject, post on forums, etc.

Q: Does data exfiltration work? Is it effective?
A: Know the playbook. Know the psychology behind the hackers, who they operate under, and the tactics they do to get control to reduce impact.

Q: “What is one incident response instance you haven’t included in your book?”
A: “A company with really good security practices had operational problems during Thanksgiving, resulting in a data breach, from a singular, REUSED passphrase to reiterate or access EDR agents/solutions. Threat actors uninstalled the software in AD by pushing a group policy”

Q: Is there an overarching concept on why ransomware situations are so difficult to navigate?
A: Introspective from Harvard rep. stating ‘it’s complicated’, much different from a traditional negotiation sense. Leverage IR planning and TXX.

Q: If a core responsibility of security teams is the operation of the company, are there moral / values arguments to pay the ransom? A: Of course! There may be value depending on context of the situation, e.g. national security issues, or hospitals ”

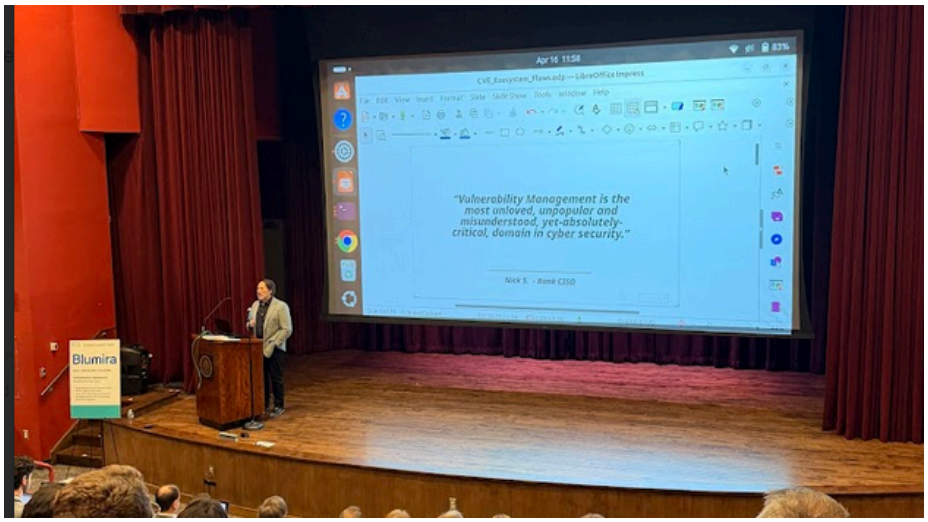
Q: Should private enterprises be allowed/able or should they use "offense as defense", aka "hack back"? A: “Attribution is hard, legal regulations or standards are difficult to work around.”

The CVE Ecosystem Today & the AI Agents Burning Watts to Fix It

[Discussion Pod #4]

Tim Rohrbaugh delivered one of the most contrarian—and practical—sessions of the Forum, challenging a core assumption that underpins modern security operations: that the CVE system is a reliable foundation for vulnerability management. His message was blunt—much of what security teams think they know about CVEs is wrong.

Drawing on a deep analysis of the CVE pipeline—including hundreds of CVE Numbering Authorities (CNAs), scoring systems, and downstream tooling—Rohrbaugh showed that the ecosystem is overwhelmed, inconsistent, and often misleading. Tens of thousands of vulnerabilities are published in short windows of time, yet many remain unscored, outdated, or never meaningfully updated. In some cases, vulnerabilities persisted for decades before being patched, while scoring systems like CVSS failed to reflect evolving risk.



The result: security teams are drowning in noise. Tools that rely on CVE data—scanners, ticketing systems, dashboards—inherit these flaws, creating false precision and wasted effort. The traditional model of "find, score, prioritize, fix" is breaking under scale.

Rohrbaugh's focus, however, was not just on what's broken—but on what to do next.

He demonstrated how small, focused teams can deploy domain-tuned AI agents to continuously ingest, analyze, and contextualize vulnerability data—effectively replacing static CVE workflows with dynamic, reasoning-driven systems. These agents can track changes over time, correlate exploit data, and generate prioritized, actionable insights tailored to an organization's environment.

A key principle: don't rely on AI to "figure it out" from the open internet. Instead, build deterministic data pipelines and controlled memory sources that AI systems can reason against.

Accuracy comes from curation—not scale alone. Techniques like model distillation and local deployment were highlighted as ways to increase precision while protecting sensitive data.

Rohrbaugh also reinforced a broader truth: vulnerability management is one of the most critical—and most neglected—disciplines in cybersecurity. It requires not just better tools, but better thinking. That includes going directly to source documentation, questioning scoring systems, and understanding how vulnerabilities evolve over time—not just when they are first published.

The discussion that followed explored the limits of current scoring models, the reality of exploit prediction systems, and how organizations can begin to operationalize AI safely in security workflows. The takeaway was clear: the future of vulnerability management won't be driven by static lists and scores—it will be driven by adaptive systems, curated data, and teams willing to rethink the foundation.

Crucial Metrics & Statistics

- First AI security solution was created and delivered in **1997, first AI programer in 1999.** *(GypSum)*
- In the last 12 months, there has been 89,000 **post-existing** vulnerabilities that have gotten re-published, often pivoting from a different layer of OSI model that the software/hardware interact with (Software vuln => Network vuln in same software)
- MITRE & ATTCK first org to originally publish vulnerabilities as CVE's, now up to **450 entities** publishing CVE's into this overarching system
- Vulnerabilities may be posted **ONCE.** If something was posted **3 years ago** and then the tactics were changed. **The score often does not change or isn't updated** in accordance with new methodologies
- **EPSS (Exploit Prediction Scoring System) -** Data driven model to estimate the probability (0 -> 1) that a software vulnerability (CVE) will be exploited in the wild within the next 30 days. Increases as a **total of 1**, is a **forward predictor** to what will happen next.

Key Thoughts and Reasoning

- Neural Networks are only 'What's going **out'**, with nothing going **in**.'
- Vulnerability management is the most unloved, unpopular and misunderstood, yet an **absolutely-critical** domain in cyber security.
- Dependence on scores - **not what you think**
- Tim points out the vital necessity for vulnerability researchers to 'go to the source', and understand publishers actual documentation surrounding the vulnerabilities ecosystem
- Tim displays demonstrations of grouping together, or amassing a TON of **public PoC scripts** regarding vulnerable systems (from open source areas e.g. github / Google Exploit DB)
- Tim points out a specific example of linux kernel maintainers, posting vulnerabilities PoC's on public github repositories **without including** a product, vendor, or score!
- Tim also points out how unproductive, and time consuming vuln testing, and PoC recreation can be! For example: Establishing the environment surrounding the actual vulnerable software to run properly
- Scale and peace of change - 'wars' occurring from each distributor pushing out genAI products
- Missing vendor and product information - **CNAs have no real governance**

- Tim now has attempted to **track CHANGES** in already found CVEs, with reworks that have been updated as time has gone on
- Uses **NVIDIAs "NEMO" LLM** to review, and print resulting NEW vulnerabilities in different architectures, software, etc. Found a wide range of new vulnerabilities
- "Never ask a model something and EXPECT an accurate answer from its own sources, instead curate AI memory from a **DETERMINISTIC DATASET**, the AI may pull from"
- Recommends **local** LLM hosting directly in WSL, docker, kubernetes, ollama
- Git blame report may be used to see **WHO** needs security training, or may have been 'hacked' based off of metrics reporting when vulns are created correlated to which person was pushing code to a certain repo

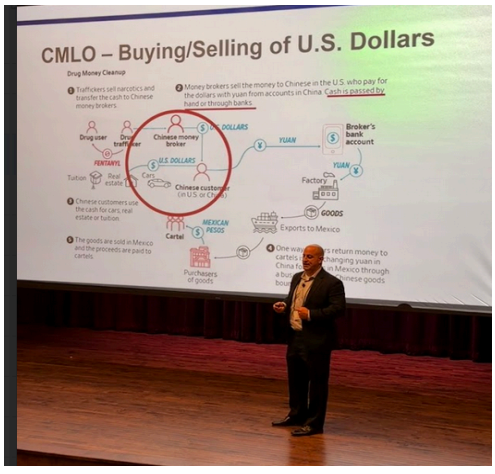
Contact Tim Rohrbaugh @ https://www.linkedin.com/in/timrohrbaugh https://radicalnotion.ai

It's Not Just Bad Hygiene—It's Criminal Negligence

What the Largest Bank Fine in U.S. History Means for Cybersecurity Leaders [Discussion Pod #5]

Special Agent Carlo Nastasi, IRS-Criminal Investigations, delivered one of the most sobering sessions of the Forum—reframing cybersecurity risk not as a technical failure, but as potential criminal negligence.

Anchored in the landmark case against TD Bank—which resulted in a record $3 billion fine under the Bank Secrecy Act (BSA)—Nastasi walked through how what appeared to be a traditional anti-money laundering failure was, at its core, a breakdown of basic controls that cybersecurity leaders would immediately recognize.



Weak identity verification. Outdated monitoring systems. Lack of escalation. Poor onboarding controls. Inadequate training. These were not edge-case failures—they were systemic gaps that enabled large-scale financial crime to persist undetected for years.

Nastasi brought the investigation to life with real operational detail: coordinated money mule networks moving funds across dozens of accounts, insiders facilitating transactions, and obvious red flags—such as repeated large deposits and suspicious behavior at the teller level—going unchallenged. In some cases, institutions could not even produce the required reporting when subpoenaed. The issue was not lack of data—it was failure to govern, interpret, and act on it.

A critical takeaway: compliance failures are increasingly inseparable from cybersecurity failures. As regulatory frameworks evolve—particularly with expanded oversight of digital assets—organizations that fail to detect and respond to illicit activity may face not just financial penalties, but legal exposure.

Nastasi emphasized that foundational disciplines like Know Your Customer (KYC), transaction monitoring, and data governance are no longer “compliance functions”—they are core security responsibilities. Without clean, trustworthy data and properly trained frontline personnel, even the most advanced detection systems will fail.

He also highlighted a recurring pattern: organizations scaling rapidly while holding budgets flat, underinvesting in training, and relying on outdated processes. In many cases, frontline employees were left to “use their gut” rather than follow structured, enforceable controls—creating inconsistent and ineffective defenses.

The discussion that followed reinforced a simple but urgent message: ask better questions, verify assumptions, and treat data integrity as mission-critical. Because in today’s environment, failing to do so is not just bad hygiene—it may be interpreted as negligence.

For cybersecurity leaders—especially those operating in fintech, banking, or digital asset ecosystems—the implications are clear: the line between breach and prosecution is getting thinner.

Once the bad actors were detained, the IRS seized 3.4 Billion dollars and began looking into internal operations of TD bank. Here is a list of the internal Problems TD bank was experiencing:

- All operational banks are required by law to have information systems in place to point out suspicious activities and fraud, but TD bank systems were unable to catch fraudulent activities or misused statistics. The IRS sent a subpoena to TD bank to get these reports and they were unable to provide the information.
- The bank also did not provide proper training on suspicious activity and were told by management to "use your gut," which explains how the tellers could not correctly identify legitimate customer transactions. Training consisted on virtual meetings, lectures, and PowerPoint presentations
- It was then discovered that there was an insider in the bank that was helping the laundering operations, as well as performing Columbian ATM topologies for Columbian drug operations.
    - Columbian ATM topologies: withdrawing cash specifically out of the country itself, and only deposited with a wide range of debit cards
- The Internal Employee was emailing fake emails from deceased victims to their own email, authorizing usage of funds or purchases.
- Budgets for the bank remained static, no ROI or growth was showing
- Zelle Transactions were unmonitored, roughly 18 trillion dollars were not documented

The number one thing to take away from this case is to Know Your Customer, ask questions, and data governance are all ways to mitigate money fraud within banking organizations. read more about the case here.

Crucial Insights & Statistics

- Analysing FinCen (Financial Crimes Enforcement Network) general trends, and technical operations, with the TD Bank Case Study
- By Feb. 2021, BSA Data exposed at least ten money mules operating multiple shell companies, with over 72 accounts at 15 financial institutions since 2016.
- Initial FinCen output noted numerous Complete Transaction Reports (CTR's) filed ranging from $10.4k to $4.7 million!
- Over 1600 CTR's totaling $531 million; TD Bank represented roughly 79% of those CTR's filed.
- Focus on fake account holders (money mules), or "smurfs" that may put fraudulent accounts in their name to facilitate withdraws / deposits in person
- Raided 5 l locations, and arrested 9 individual
- Carlo points out the lack of reporting or documentation of zell transactions, (sending or receiving) allowing 94 billion dollars in transactions to go unmonitored
- Conducted 50 interviews with faculty, to find that bank statements were not matching reports
- Seized $3.4B total in cash and bank accounts combined

How can we improve?

- Financial institutions must have functional pillar investigations put into place to point out flaws from automated systems, or banking infrastructure unable to catch or spot fraudulent activities, or misused statistics.
- Criticisms towards TDBNA, as IRS had to subpoena the org to actually get a generated report regarding certain criminals fraudulent activity
- Criminals used Colombian ATM Typology to move illicit funds to be deposited into U.S. bank accounts, and withdrawn as cash in Columbia, involving corrupt bank insiders
- Pointed out a lot of banktellers, or employees do not take the time to genuinely confirm or authenticate the legitimacy of the customers transactions (e.g. taking ID over phone)
- Threat Actors often emailing fake emails from deceased victims to their own email, authorizing usage of funds or purchases
- Must substantively update transaction monitoring system,
- Anti Money Laundering training was VIRTUAL. Additionally, reporting, auditing, and properly authenticating a possible bank transaction is heavily undermined
- Many banks may grow, or scale, but they attempt to keep budget spending the same

- Bank tellers frequently avoid assessing legitimacy of transactions to not inconvenience clients. Front line workers have the least amount of training (often being trained from a singular powerpoint presentation)
- Suspicious Actions Reports (SAR's) did not exist, so physical monitoring or analysis of transactions proved to be difficult and tedious
- Many financial institutions had poor KYC from enforcing sign ups / registration (know your customer)
- Taken from personal experience from a caught perpetrator: Before closing fraudulent accounts, banks usually give clients 30 day warnings, "Approx. 5b dollars was moved before bank is closed down"

Q&A Highlights

Q: "What is the most important thing to focus on with securing cybersecurity related financial issues?" A: Data is the most important thing! Focus on KYC, must ask the right questions. If data is being mismanaged, no matter how good automated embedded systems may be, embezzlement or fraud is more than possible still. Check check check (data governance)"

Q: What do you do with the money after it has been seized?
A: Goes back to PD and investigation officers, and goes back to families affected by 911 and people affected by ponzi schemes

Agentic AI Meets Zero Trust: What Actually Breaks—and How to Fix It

[Discussion Pod #6]

Josh Woodruff, author of *Agentic AI + Zero Trust*, delivered a forward-looking but highly practical session on where agentic AI is colliding with enterprise security—and where things are already starting to break.

His core argument: most agentic AI initiatives don't fail because the technology doesn't work—they fail because the operating model isn't ready. Organizations are deploying autonomous and semi-autonomous systems into environments that lack the identity, governance, and control frameworks required to manage them safely.

Woodruff reframed agentic AI as a "digital coworker"—one that can make decisions at scale and speed, but only within clearly defined boundaries. Without those constraints, risk compounds بسرعة. He highlighted a fundamental limitation in AI systems: context is finite. Just like a crowded whiteboard, when too much information is introduced, something gets erased—and in extreme cases, that "something" can be critical instructions or guardrails.

That's where Zero Trust must evolve.

Woodruff outlined a simple but powerful model for controlling non-human identities—one that extends traditional Zero Trust principles into agentic systems:

- Who are you → Identity (IAM)
- What are you doing → Behavior monitoring
- What data are you touching → Data governance
- Where can you go → Segmentation
- What happens if you go rogue → Incident response

He introduced his "Agentic Trust Framework," which applies structured roles to AI agents—ranging from observer ("intern") to fully autonomous operator ("principal")—ensuring that trust is earned over time, not granted by default. The goal is not to eliminate autonomy, but to bound it.

A key insight that resonated: AI will amplify whatever environment it's deployed into—good or bad. Poor processes become worse. Strong governance becomes a force multiplier.

Woodruff also pushed back on a common executive misconception—that AI will magically fix broken workflows. In reality, organizations must first understand how work gets done, where decisions are made, and where control points should exist. Only then can AI be safely introduced to enhance speed and scale.

The discussion emphasized that identity is now the control plane. Without strong IAM, visibility into non-human actors, and continuous monitoring, agentic AI introduces more risk than value.

The takeaway for CISOs and CIOs was direct: Zero Trust is no longer optional in an AI-driven enterprise. It is the prerequisite. Organizations that define clear boundaries, enforce accountability, and instrument their environments for visibility will unlock real value from agentic AI. Those that don't will face faster, more opaque failures—with higher stakes.

Example Scope

1. Who are you: identity management.
2. What are you doing: behavior monitoring
3. What data are you touching: data governance
4. Where can you go: segmentation
5. What if you go rogue: incident response

Josh then explains his way of implementing AI in zero trust by introducing is Agentic Trust Framework, which is explained in more detail in his book, Agentic AI + Zero Trust: A Guide for Business Leaders

- Trust is earned not granted
- Principal: Act autonomously within bounds
- Senior act with notification
- Junior make recommendations
- Intern: observe and report

Deploy AI agents with governance to avoid disaster. Always make sure reports are being generated on what they are doing in case of disaster. This methodology allows a zero trust architecture in combination with agentic AI, providing faster decision making, contained AI models with predefined tasks, and a greater ROI for upper management. For seeing how your organization is adapting to AI usage, Josh provides a 90 minute Agentic AI readiness assessment, which identifies users gaps where they may lack in technical or security knowledge.

Crucial Thoughts and Ideologies

- AI 10x's whatever you currently are, e.g. 10x worse, or 10x better
- Business transformation. It cannot be driven by tech, it has to be led by security. AI makes zero trust non-negotiable
- Real ROI is improving overall decision making and requires strong leadership, to re-examine how business gets done. Security is not profitable. Enabling 0-trust will not bring profit, but reduce loss of profits
- Identity (IAM) is of utmost importance for improving and securing org. Infrastructure, and deploying agentic AI safely. Also, for ensuring CIA (confidentiality, integrity and accountability in data access or transmit). E.g. Entra Agent ID (Cloud solution)
- Agentic trust website: 25 controls 80 subcontrols
- "How does work flow from one business to the next?" Where would the interjection of AI improve this?
- Use open-source frameworks to implement zero trust on open AI
- Clear boundaries make agents perform better, point blank. Josh gives a comparison to this idea by giving strict OKR's to a senior hire.
- Promotes a 90 minute Agentic AI readiness assessment, providing users gaps where they may lack in technical or security knowledge. Maps non-human identities, accountability gaps, and governance blind spots. (FREE)
- Execs automatically presume AI may 'clean' mistakes by default, or reiterate how their work flows, for massive improvements, with no attached effort or work. Results are the opposite.
- If you include AI in your business model, ask yourself: "How do you know when AI makes irreversible decisions? Have you given it tools to do so?"

Find more information about Josh's work and experience at:
https://www.linkedin.com/newsletters/agentic-for-the-win-7365854373530206210

Degrees, Certs & Entry-Level Grit: What Cyber Grads Can (& Can't) Do

This panel discussion brought together academic leaders and enterprise practitioners for a candid look at one of the industry's most persistent challenges: why a market with hundreds of thousands of open roles still struggles to hire entry-level talent.

Educators, including Dr. Jared Oluoch, Chris Krieger, and Dr. Tauheed Khan Mohd, outlined how programs are evolving—emphasizing hands-on labs, capstone projects with real companies, and deeper integration with industry. The goal is clear: produce graduates who can contribute on day one, not just understand theory. Experiential learning, tool familiarity (e.g., Kali Linux, Splunk, pfSense), and exposure to real-world problems were positioned as essential to closing the gap.

Panelists

- Dr. Jared Oluoch - Head of Cybersecurity - EMU GACET
- Chris Krieger - Adjunct Professor, EMU
- Dr. Tauheed Khan Mohd - Associate Professor, EMU
- Doug Copley, CISO - AtlantiCare
- Lindsey DeBouver, Deputy CISO - Lear
- Nathan Wolf, SVP CISO IT Security & Risk Services - Planet Home Lending

From the practitioner side, leaders like Doug Copley, Lindsey DeBoever, and Nathan Wolff reinforced a hard truth: credentials alone are not enough. Hiring decisions increasingly come down to curiosity, initiative, and the ability to apply knowledge in practical settings. As one framing put it—can a candidate "wind themselves up," or do they require constant direction?

A consistent theme across the panel was the importance of soft skills. Communication, critical thinking, and adaptability were repeatedly highlighted as differentiators, especially in an AI-driven environment where technical skills can evolve quickly. At the same time, panelists stressed that AI should be embraced—not feared—but with clear expectations that it enhances, rather than replaces, human judgment.

Internships and mentorships emerged as critical—but constrained—levers. Organizations recognize their value but struggle with budget, time, and structural limitations. Still, the consensus was clear: companies must find ways to invest earlier in the talent pipeline if they expect better outcomes later.

The discussion ultimately reframed the issue: this is not a supply problem—it's an alignment problem. Bridging the gap will require tighter collaboration between academia and industry, clearer expectations for entry-level roles, and a renewed focus on developing professionals who can think, adapt, and execute—not just pass exams.

Key Points, Summarized by Panelist

Dr. Jared Oluoch

Jared Oluoch emphasizes that four-year degrees still play a critical role, but only when they evolve alongside industry needs. He highlights the importance of strong partnerships between universities and industry, integrating modern tools, and creating more opportunities for students. By working closely with community colleges and industry sponsors, institutions can also shorten time to graduation while maintaining quality, giving students faster entry into the workforce without sacrificing depth.

He stresses that the most valuable graduates are those who can think on their feet and adapt to rapidly changing environments. Eastern Michigan University is focused on experiential learning, ensuring students engage with real-world problems before they graduate. Oluoch also points to emerging programs at EMU such as AI degree programs and minors in AI security, which reflect the growing importance of preparing students for the future of cybersecurity.

Chris Krieger

Krieger places significant emphasis on soft skills, suggesting they are often more critical than technical abilities early in a career. Communication, adaptability, and critical thinking enable professionals to grow quickly, while technical skills can be developed more easily over time. He also strongly advocates for integrating AI into all levels of cybersecurity work, from interns to senior professionals, saying that he personally uses AI tools to assist with scripting and problem-solving.

Additionally, he believes educators must remain active practitioners in the field. Professors who engage with real-world cybersecurity challenges are better equipped to bring current knowledge into the classroom, ensuring students are learning relevant and up-to-date material. This connection between academia and industry is essential for keeping pace with next-generation threats.

Doug Copley

Doug Copley highlights the challenges organizations face in hiring and developing entry-level talent, especially within smaller teams. While he strongly advocates for expanding internship opportunities, he acknowledges structural barriers such as budget constraints and policies around unpaid internships. Despite these limitations, he wants organizations to find ways to invest in internship programs.

From a hiring perspective, Copley prioritizes curiosity over credentials. While a bachelor's degree may be required, he is ultimately looking for individuals who demonstrate a deep interest in understanding root causes and ask questions. He mentioned that mentorships are critical in this process because it helps new hires develop opinions on industry tools.
He also raises concerns about the rapid evolution of AI, particularly agentic systems that introduce new challenges around identity and permissions. These systems can access sensitive data in unexpected ways, making governance and security controls more important than ever.

Dr. Tauheed Khan Mohd

Tauheed Khan Mohd focuses on the importance of practical, tool-based learning in cybersecurity education. Drawing from both academic and industry experience, he emphasizes exposing students to widely used tools such as Kali Linux and pfSense so they can understand how security concepts are applied in real business environments. This exposure helps students build confidence and develop skills that are directly transferable to the workplace.
He encourages students to form their own opinions about technology, including AI, rather than relying on it blindly. Staying up to date with tools and technologies is also essential, as the cybersecurity landscape evolves rapidly and demands continuous learning. By combining foundational knowledge with practical skills and experience, students can build strong resumes that demonstrate knowledge that can translate to a job after graduation.

Lindsey DeBoever

Lindsey DeBoever brings a leadership perspective on developing talent pipelines within organizations. She emphasizes hiring from local colleges and investing in structured internship programs that provide meaningful, real-world experience. At Lear Corporation, internships are treated as serious opportunities where students contribute to actual projects, helping bridge the gap between academic learning and professional expectations. She also highlights the importance of extending learning opportunities beyond traditional summer internships through accelerated programs and ongoing engagement.
DeBoever sees AI as a powerful tool that can enhance both learning and operations. Rather than fearing its impact on talent development, she believes emerging professionals can use AI to improve operations. A key skill for DeBoever is the ability to critically evaluate AI outputs and understand when information may be incorrect or misleading.

Nathan Wolff

Nathan Wolff underlines the importance of applied experience when evaluating new graduates. While theoretical knowledge is valuable, he is primarily interested in how candidates have used their skills in practical settings. He frames this in simple terms: can a candidate take initiative and "wind themselves up," or do they require constant direction?
Wolff also addresses the role of AI in cybersecurity, cautioning against overreaction to its capabilities. While AI is a valuable tool, it should not replace human intelligence or critical

thinking. He encourages students to actively demonstrate their use of AI in interviews, showing how it has helped them solve problems or improve workflows.

Dr. Samir Tout

Samir Tout focuses on preparing students to become active contributors in the cybersecurity industry through experiential learning. He highlights Eastern Michigan University's capstone programs where students are paired with real industry clients, allowing them to work on practical problems and gain firsthand experience before graduating. Dr. Tout said his approach helps bridge the gap between academic theory and professional expectations.
Tout also emphasizes the importance of developing the “human side” of cybersecurity in an AI-driven world. While technical skills remain essential, soft skills such as communication, collaboration, and critical thinking are what enable professionals to work alongside AI systems. Preparing students to coexist with AI is a central goal of modern education. He would like to see more integration of AI education in elementary and high school institutions as well as advanced research in higher education.

Key Panelist Ideas & Answers

- Professors aim to both prepare, and engage students with real industry leaders or clients within Cybersec. Also, include students in hands on activities – Jared Olouch
- Currently aiding students to conduct national pentest audit - Krieger
- “Will AI take your job?” Professors will prepare you to co exist WITH AI, to become more effective than fully autonomous systems, e.g. soft skills or effective logistics and reasoning, you cannot find these in AI agents
- Two majors; IT/Cybersec include a Co-Op: Students must find a job and work a minimum of 600 hrs within the program to prove knowledgability (both paid/unpaid). Additionally, EMU hosts approx.. 64 students in the capstone program
- Many companies look for candidates who don’t wait to be notified or told when there is an issue, they fix it themselves, taking initiative.
- Curiosity: Key characteristic for interns and students looking to better their work; applicable skills must be proven and shown on their own
- Theoretical is important, but how have you applied those skills? “Can you wind yourself up or do I have to wind you up?”
- Within Doug’s company at AtlantiCare, he’s seen metrics including more than ONE AGENT A DAY being deployed in their Azure tenants infrastructure
- Pen testers say that they fool autonomous systems with simple signs. AI should not replace every operation.
- Professors should also be practitioners. Be in the field to see the changes and incorporate changes- Krieger
- Hopeful new talent may leverage AI to become more effective in their tasks - Lindsey DeBouver

- Constantly adapt, as industry and technical skills are also frequently changing. Must be capable of thinking on their feet
- “If you're not using AI in cyber-defense, you need to be.”
- Most commonly, entry level folks apply AI regarding their job or position, not the other way around
- Hands-on learning is extremely important, as students work on real world projects. For example, students in the program will gain experience using pfsense, splunk, wireshark, kali, and more.We want the students to make their own opinion and use it as an aid

Discussion Leaders

Kurtis Minder

CEO & Co-Founder, GroupSense
Author, *Cyber Recon: My Life in Cyber Espionage and Ransomware Negotiation*

Kurtis Minder is one of the world’s foremost experts in ransomware response and cyber threat intelligence. As CEO and co-founder of GroupSense, he has led negotiations in some of the largest ransomware and data extortion cases globally, engaging directly with threat actors and nation-state affiliates.

With over 25 years in cybersecurity—including roles at Fortinet, AT&T, and Citrix-acquired Caymus Systems—Kurtis has combined operational security, cyber reconnaissance, and real-world intelligence tradecraft into a uniquely effective digital risk strategy. His pioneering work and insights have been featured in *The New Yorker*, *BBC*, *The Wall Street Journal*, and *Fortune*.

Kurtis will deliver a TED-style keynote and participate in a moderated discussion on themes from his acclaimed new book, *Cyber Recon*, offering a rare behind-the-scenes look at the people, tools, and tactics behind today’s cyber espionage and ransomware ecosystem.

Richard Stiennon

Chief Research Analyst, IT-Harvest

Richard Stiennon is one of the most respected and provocative voices in the cybersecurity industry. As Chief Research Analyst at IT-Harvest—the firm he founded in 2005—he leads the only comprehensive effort to map, track, and analyze the entire global cybersecurity vendor landscape. His research underpins the *Security Yearbook* series, offering deep data and sharp insight into the trends shaping the industry.

A former VP of Research at Gartner, Richard has held senior roles at Fortinet, Webroot, and Blancco Technology Group, and has advised government agencies and Fortune 500 companies alike. His past publications include *There Will Be Cyberwar*, a Washington Post bestseller, and *Surviving Cyberwar*. His thought leadership spans over three decades and 32 countries, blending strategic analysis with operational depth.

Richard holds a B.S. in Aerospace Engineering from the University of Michigan and an M.A. in War in the Modern World from King's College London. He is also an active commentator on LinkedIn, Substack, and X (formerly Twitter), where he regularly challenges assumptions and surfaces the next wave of cybersecurity innovation.

Tim Rohrbaugh

Founder - RadicalNotion.AI, 3x Public Co. CISO

Tim Rohrbaugh brings 20+ years of C-level cybersecurity leadership to the frontier of AI for security and applied engineering. As founder of RadicalNotion.AI and former CISO of JetBlue Airways, he has built and operated enterprise programs that protect high-value, regulated data— including responsibility for safeguarding more than 40 million consumer records at a public financial services company.

A career security architect and systems engineer, Tim advances a practical view of GenAI as "augmented intelligence": trustworthy, domain-tuned reasoning agents that reduce noise, challenge bias, and accelerate evidence-backed decisions without exposing IP. He has served as Vice Chair of the Airlines for America Cyber Security Council and as a board member of the Online Trust Alliance, where he contributed to national privacy and security policy. His work has been recognized with multiple awards, including Top Global CISO by Cyber Defense Magazine. Tim holds two joint patents in identity verification and authentication and is a frequent speaker and advisor to boards and engineering teams alike.

John Felker

Former Asst Director, DHS-CISA

John Felker is the former **Assistant Director for Integrated Operations at the U.S. Cybersecurity and Infrastructure Security Agency (CISA)**, where he led efforts to coordinate intelligence, operational planning, and mission execution across the agency's regional and national cybersecurity operations. Prior to that, he served as **Director of the National Cybersecurity and Communications Integration Center (NCCIC)**, the federal government's primary hub for cyber threat analysis, incident response coordination, and information sharing with critical infrastructure operators.

Following his government service, Felker founded **Morse Alpha Associates**, a cybersecurity leadership consultancy advising senior executives and boards on cyber risk, resilience, and national security issues. He also serves as a **Senior Advisor to The Chertoff Group** and the **Maritime Transportation System ISAC**, and participates on multiple cybersecurity and national security advisory boards.

Earlier in his career, Felker served **30 years in the U.S. Coast Guard**, including as **Deputy Commander of Coast Guard Cyber Command**, Commander of the Coast Guard Cryptologic Group, and Executive Assistant to the Director of Coast Guard Intelligence. His service earned numerous honors, including the **Department of Homeland Security Outstanding Public Service Medal**, the **Defense Superior Service Medal**, and the **Legion of Merit**.

Special Agent Carlo Nastasi

IRS Criminal Investigation (IRS-CI)
Lead Agent – SAR Review Team & Liaison to the Private Banking Industry

Carlo Nastasi is a senior Special Agent with the Internal Revenue Service Criminal Investigation (IRS-CI), where he has led high-profile financial crime investigations for over 16 years. Specializing in money laundering, cyber-enabled financial crimes, and Bank Secrecy Act (BSA) violations, he currently serves as the lead agent on the Suspicious Activity Report (SAR) Review Team and as a key liaison to the private banking industry.

Agent Nastasi was instrumental in the groundbreaking $3 billion TD Bank case—the largest BSA-related fine and first major criminal plea of its kind—where his team uncovered systemic failures in onboarding, transaction monitoring, and compliance reporting. His insights into how traditional financial blind spots intersect with modern cyber threats have made him a sought-after speaker for both regulatory and cybersecurity audiences.

Before joining IRS-CI in 2008, Carlo was an Audit Senior at Deloitte & Touche and holds a degree in finance and accounting from Pace University. Over the course of his career, he has investigated international tax fraud, Ponzi schemes, political corruption, and cybercrime across fiat and cryptocurrency domains. He also previously served on an FBI task force supporting white-collar and political corruption investigations.

Carlo brings a unique perspective at the intersection of cyber risk, financial regulation, and criminal enforcement—and helps organizations understand the real-world consequences of getting it wrong.

Josh Woodruff

Author of *Agentic AI + Zero Trust: A Guide for Business Leaders*

Josh Woodruff is the author of *Agentic AI + Zero Trust: A Guide for Business Leaders*, a practical framework for safely operationalizing autonomous AI using Zero Trust principles. Drawing on nearly 30 years of experience as both a CIO and CISO, Josh translates real-world enterprise deployments into clear executive guidance on trust, governance, and risk in agentic systems.

The book—co-authored with Michelle Savage and featuring a foreword by Zero Trust pioneer John Kindervag—cuts through AI hype to explain why most AI initiatives stall in pilot mode, and what successful organizations do differently. Josh is also the Founder and CEO of Massive Scale Consulting, co-leads the Cloud Security Alliance Zero Trust Working Group, and serves as IANS Faculty, advising enterprises across regulated and high-risk industries.

Known for his ability to frame complex AI and security challenges in plain executive language, Josh focuses on helping leaders design guardrails that accelerate innovation without sacrificing control, accountability, or resilience.

Doug Copley

[Panelist] CISO, AtlantiCare

Doug Copley is a nationally recognized cybersecurity and privacy leader with more than 30 years of experience protecting sensitive data, managing regulatory risk, and guiding organizations through fast-moving technology change. As Chief Information Security Officer at AtlantiCare, he leads enterprise efforts to secure patient information and safeguard one of New Jersey's most vital healthcare systems.

Doug co-founded and served as chairman of the Michigan Healthcare Cybersecurity Council, and later established Data Protection Partners to help organizations build, strengthen and evolve their information security and privacy programs. Doug has experience building and managing information security, IT and data privacy programs with particular expertise in the healthcare industry. As an executive Risk and IT leader, Doug has held executive roles as CIO, CISO, and Chief Privacy Officer and has experience across the healthcare, financial services and manufacturing industries, working with organizations of all sizes.

Doug is also a frequent keynote speaker, blogger, and media contributor. His insights draw on hands-on leadership across both large enterprises and smaller, fast-moving entities—bringing a rare perspective on how organizations can innovate quickly without sacrificing maturity or compliance.

At the Detroit CyberSecurity & Fraud Forum, Doug will lead a candid discussion on the frontlines of healthcare security—exploring how CISOs are governing AI platforms, managing data integrity, and addressing the unique challenges of one of the most regulated and risk-sensitive industries. Expect practical lessons on balancing innovation with protection, defending against evolving threats, and building governance models that keep pace with AI-driven transformation.

Dr. Jared Oluoch

Professor and Director of the School of Information Security and Applied Computing (SISAC)

Dr. Jared Oluoch is Professor and Director of the School of Information Security and Applied Computing (SISAC) at Eastern Michigan University. He received a PhD in Computer Science and Informatics from Oakland University in Rochester, MI, in 2015, and a Master of Science in Management Information Systems from the University of Nebraska at Omaha, in 2009. His research interests are in cybersecurity for connected and autonomous vehicles, localization for Wireless Sensor Networks (WSNs), and physical layer security. He has received close to three million dollars in external funding from the National Science Foundation as a PI or Co-PI. He has advised several master's and doctoral students in Computer Science and/or Cybersecurity. He is a Program Evaluator for ABET and a senior member of IEEE.

Chris Krieger

[Panelist] Staff, Faculty, Part-Time Lecturer

Chris currently works as a Principal Technical Consultant - Security for a Chicago-based technology firm. Chris has been teaching at EMU for 11 years, building and delivering a variety of classes on different cybersecurity topics. Chris is a cybersecurity professional with experience dating back to 2006, combining deep industry expertise with a strong presence in the classroom. He works closely with Fortune 500 organizations to strengthen defenses against evolving threats such as ransomware, leading initiatives in cyber resilience, identity and access management, and security architecture. His work spans areas including Splunk architecture, privileged access management, multifactor authentication, and cyber-resilient backup design. Chris's core expertise includes digital forensics, incident response, cloud security, vulnerability management, and cyber recovery.

Dr. Khan Mohd

[Panelist] Assistant Professor, Information Security & Applied Computing

An Assistant Professor at Eastern Michigan University's School of Information Security & Applied Computing, Dr. Khan Mohd brings a blend of academic excellence and global industry experience. They hold a Ph.D. in Human-Computer Interaction from The University of Toledo, along with an M.S. from the same institution and a B.Tech in Computer Engineering from Jamia Millia Islamia in New Delhi. Before transitioning to academia, Dr. Mohd spent several years in industry as a software engineer with HCL Technologies and SOPRA, including international experience supporting AIRBUS in France. Their research spans Human-Computer Interaction, cybersecurity, autonomous vehicles, and embedded systems such as Arduino and Raspberry Pi. In recognition of their contributions to the field, he was named a Senior Member of IEEE in 2023.

Lindsey DeBoever

[Panelist] Deputy CISO, Lear Corporation

Lindsey helps lead Lear's cybersecurity strategy across incident response, threat intelligence, vulnerability management, identity, network security, and governance. She partners closely with executive leadership to translate complex cyber risk into clear business impact while driving practical, scalable security programs across a global enterprise.

With a career that spans information security, IT operations, and HR technology, Lindsey brings a unique perspective to the intersection of people, process, and technology. Prior to her current role, she served as Global HRIS Director and led large-scale digital transformation initiatives focused on data, access, and the digital employee experience. This background informs her approach to cybersecurity by designing security controls that are both effective and usable, reducing friction while strengthening resilience.

Lindsey holds a Bachelor of Science in General Management with a minor in Applied Technology in Business from Oakland University.

Michael Hiskey

[moderator] CSO & Founder, CxO Security Forum

Michael is the Founder and Chief Strategy Officer of the CxO Security Forum, a community-led initiative built to reshape how cybersecurity, risk, compliance, and AI leaders engage with one another. He hopes to create a trusted environment for executive dialogue—one that prioritizes peer-to-peer exchange, practical insight, and meaningful connection over vendor-driven agendas.

Michael holds an MBA from Columbia Business School. During his 10 years at IBM, he lived and worked on three continents, and has traveled to 38 countries. He lives on Long Island, in New York, with one current and two future women in technology, all of whom are smarter than him.

Nathan Wolff

[Panelist] Chief Information Security Officer, Planet Home Lending

Nathan leads the Planet Home Lending’s enterprise-wide information security strategy. With more than 15 years of experience across cybersecurity and infrastructure, he oversees security operations, compliance, engineering, vulnerability management, and privacy—ensuring protection of critical systems while enabling business growth.

Nathan has built and scaled comprehensive security programs within complex financial services environments, including developing cloud engineering capabilities across Azure and AWS and designing resilient network architectures spanning dozens of locations. He is known for translating complex risk into clear, actionable insights for executives, boards, and regulators.

A CISSP and recipient of the HW Rising Star award, Nathan is recognized for making cybersecurity practical and approachable—helping organizations strengthen defenses while maintaining operational agility.

Supporting Solution Providers

Blumira

Blumira (blumira.com) provides a cloud-based security operations platform that simplifies threat detection and response for small and mid-sized organizations. Its integrated SIEM and XDR solution deploys rapidly, offering automated detection, prioritized alerts, and guided response actions across cloud and on-premises environments.

By combining endpoint visibility, built-in integrations, and 24/7 SecOps support, Blumira enables IT and security teams to identify and contain threats quickly while reducing complexity and operational overhead. The platform's accessible design and automated workflows help organizations meet compliance and cyber insurance requirements, strengthen resilience, and enhance overall security posture.

CISOs within the CxO Security Forum Community have endorsed Blumira, citing a responsive account team and thoughtful, efficient pricing options.

EasyDMARC

EasyDMARC (easydmarc.com) is a cybersecurity company focused on email authentication and domain protection, helping organizations prevent phishing, spoofing, and email-based fraud. The company provides a SaaS platform that simplifies the implementation and management of DMARC, SPF, and DKIM protocols, enabling businesses to secure their email ecosystems and improve deliverability.

EasyDMARC primarily serves small to mid-sized businesses as well as enterprises looking for automated, user-friendly tools to enforce email security policies without requiring deep technical expertise. Its platform includes real-time monitoring, reporting, policy enforcement, and threat intelligence to identify and remediate unauthorized email activity.

The company operates as a cloud-based SaaS provider with a global customer base, positioning itself as a streamlined alternative to more complex enterprise email security solutions.

Data Protection Partners

Data Protection Partners (datapropartners.com/) helps organizations turn cybersecurity and data privacy into a business advantage. Through expert advisory and fractional leadership, they deliver practical, executive-level guidance to strengthen security programs, meet regulatory requirements, and reduce risk—without the overhead of a full-time team. From building scalable security frameworks to navigating complex compliance challenges, Data Protection Partners empowers organizations to protect what matters most while enabling growth.