In today's world, we rely on technology and the Internet for a variety of transactions, communication and information – at home, in school and at the workplace. While we are familiar with the myriad of conveniences provided through Internet use, it is difficult to stay abreast of all the changes and the potential risks presented by the Internet. We are all "virtual neighbors" in cyberspace, and what we do, or don't do, can affect many others.

The Nebraska Cyber Security Conference will assist in raising our awareness of cyber security and help in protecting all of us in cyberspace. If we do our part individually, collectively we can have a tremendous positive impact on our state's cyber security.

This will be valuable time learning from skilled industry experts. The day will be filled with a variety of breakout sessions that will encompass different areas of information security and technology.

**For more information, visit southeast.edu/ncsc.**

**Wi-Fi Login Information**
Network: NUGuest
Username: September17
Password: Innovate2024!

# Keynote Speaker: Tim Vidas

*A*

Tim Vidas a Principal Engineer at Amazon Web Services (AWS) focused on Threat Intelligence and operational security. Prior to joining AWS, Tim collected decades of experience in a mix of academic, commercial and government settings. His endeavors span from being the development team lead for DARPA's Cyber Grand Challenge, to digital forensics research lead at CERT, to developing a high-assurance security kernel at NPS. Tim has a Ph.D. in ECE from Carnegie Mellon, and also is a DEF CON black badge holder. Tim also is a founder of both the local DC402 DEF CON group and the Kernelcon conference.

### ƒ ƒ¡ ¡mT‹ë%Ì ‹à¡ F½6 ‹ë6% 6É -Êy¡m}¡ƒ më‹Ê }ë%Ì T -6%½¡
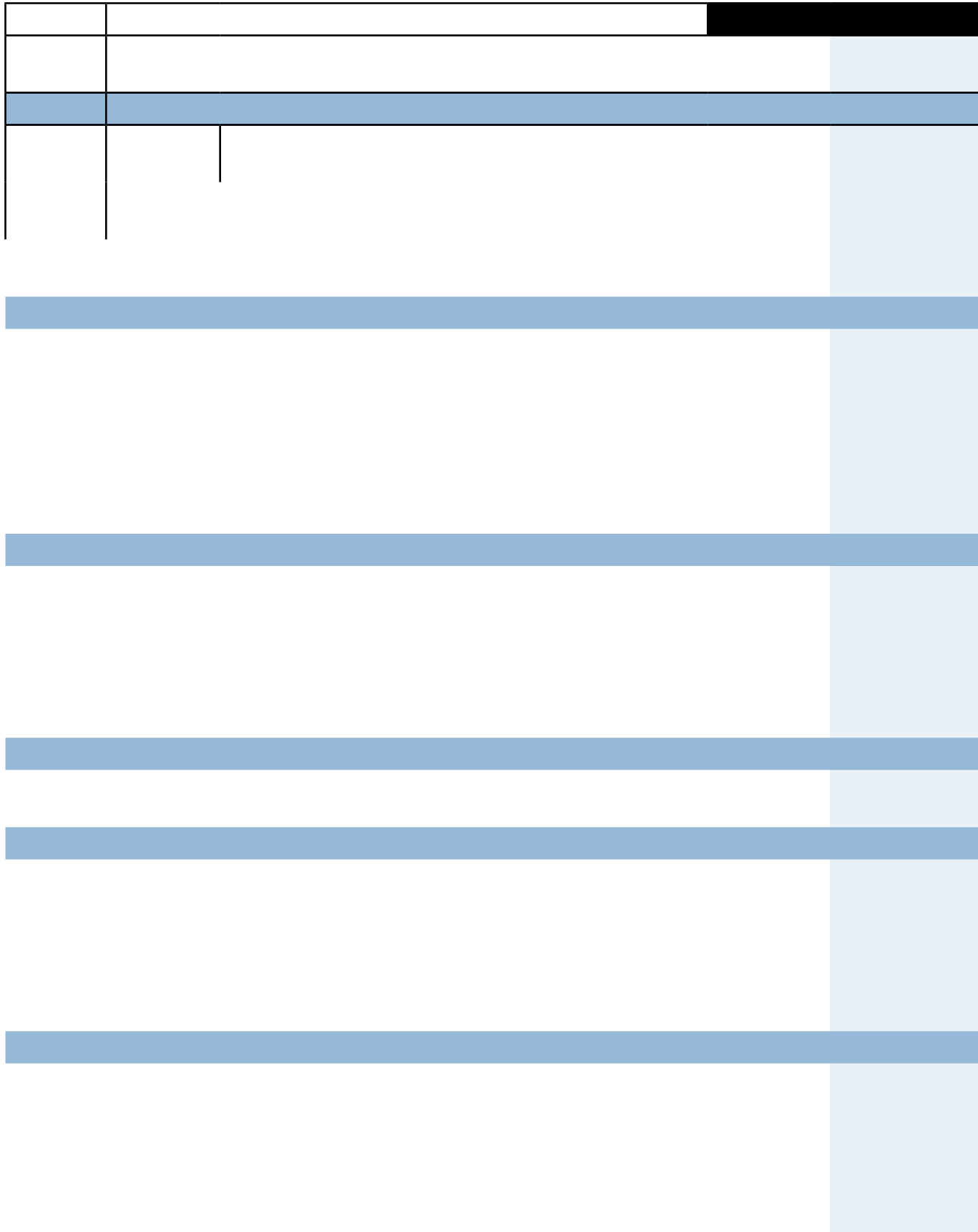
Chris Cruz, Tanium

To defend against attacks & protect critical data, Government needs a paradigm shift for complex risk & technology issues. Local Government Chief Information Officers (CIO's) and Chief Information Security Officers (CISO's) have thousands of distributed assets to see and control, but most of them cannot capture how many endpoints they have, what applications run on them, or whether they have the right access controls across them. Tanium Public Sector Chief Information Officer (CIO) Chris Cruz will discuss the convergence of real-time decisions and remediation using one plane of glass/one source of truth, unified controls, a common taxonomy and how he developed a common cybersecurity plan as a former State and County government CIO. He will discuss the need for new generations of tools and new frameworks for them to address a unified cybersecurity approach.
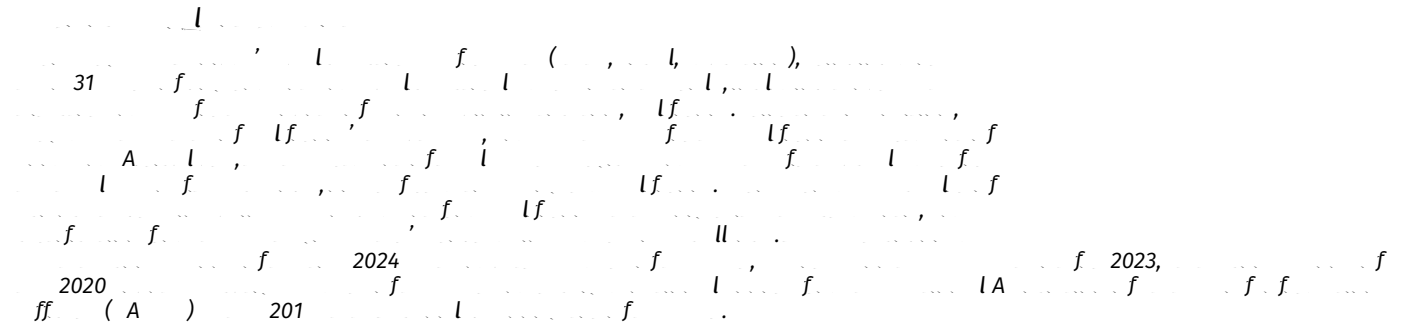
## Attack, Detect, Defend: Antisyphon Training

Kent Ickler & Jordan Drysdale, Antisyphon

In this session we will give an overview into what we call threat optics: auditing endpoints, centralizing logs and visualizing results.

Each student will leave the class having experienced a penetration test through three distinct perspectives, each building on the previous. These will include adversarial attacks, examination of defensive postures, and wrapped up with various detection methodologies using open-source or free industry threat detection and defenses.
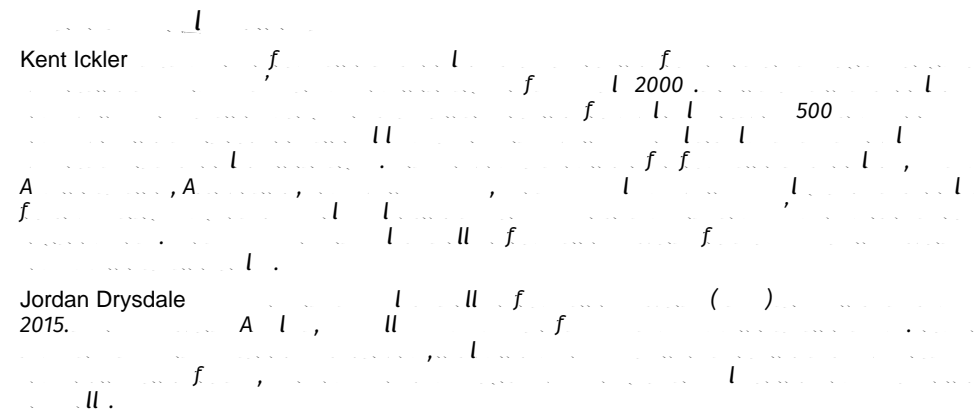
Md Rashedul Hasan, University of Nebraska-Lincoln

As cyber threats become more sophisticated, detecting software vulnerabilities earlier using artificial intelligence techniques can help secure interconnected systems. However, current commercial language models do not effectively address all criteria needed to identify and mitigate certain vulnerabilities. This talk discusses the deficiencies of language models to comprehensively assess software vulnerabilities. A comparative analysis evaluates the LLM model's performance through the usage of a benchmark data set. Results reveal limitations in providing resilient fixes for optimized vulnerability versions, often falling short in constructive suggestions. The goal is to address the criteria and limitations for diverse vulnerability properties and interactions beyond what current models can achieve. By consolidating the strengths of different models and techniques a resilience driven -based approach can be developed to detect security vulnerabilities.
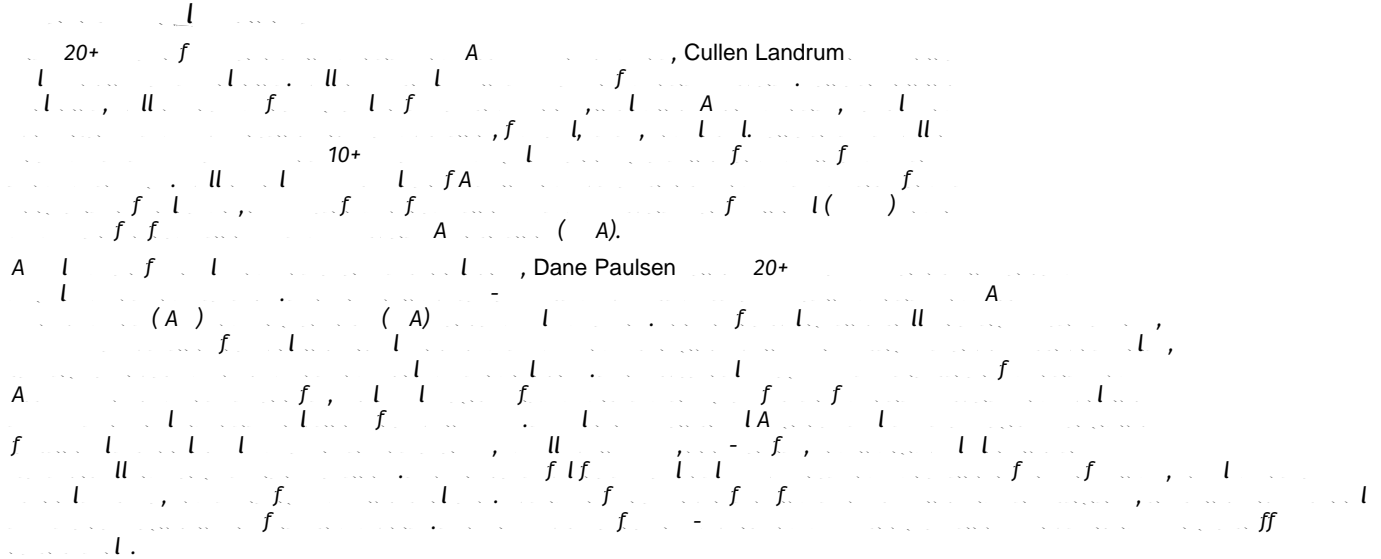

## 7¡}ëÌ%ë%Ì T ò ƒƒ¡}}É zŽ¡%‹ë‹Ê ò¡ƒ më‹Ê ám6ÌmT

### Cullen Landrum, SailPoint, & Dane Paulsen, Flatwater Services

In this session, we will discuss what it takes to have a successful Identity Security program. Identity Security is fundamental to any organization to meet audit, zero trust and more. Dane will describe what it took for his organization to decide on a solution and what it took to get a program going. Also, we will discuss his decision to migrate to a SaaS solution and what was involved in that decision.

l

20+ f A , Cullen Landrum
l l . ll l f .
l , ll f l f , l A , l
, f l, , l l. ll
10+ l f f
. ll l l f A f
f l , f f f l ( )
f f A ( A).

A l f l l , Dane Paulsen 20+
l . - A
( A ) ( A) l . f l ll ,
f l l l ’ ,
l l . l f
A f , l l f f f l
l l f . l l A l
f l l l , ll , - f , l l
ll . f l f l l f f , l
l , f l . f f f , l
f . f - ff
l .

## 76¡} ¡mr 7T‹T 7m¡T T‹ ¥ëÌà‹s

### Aamir Lakhani, Fortinet

We may fantasize about the days of Star Trek and Terminator where artificial intelligence might be able to help us

zŽ¡%‹ëÉÊë%Ì ‹à¡ Ž½¡m}TmÊ T%Ž ¶b¡mT‹ë6%T ëÖë%Ì -Êy¡m |

Richard Mendoza, Google

In this session, we will explore the critical process of identifying adversaries and their TTPs to enhance your defense

## ¥T½ëÌT‹ë%Ì ámë½TƒÊ ë% ‹à¡ Ì¡ 6É e¡%¡mT‹ë½¡ z

Ross Coudeyras, Remesh

Join us for an insightful exploration into the privacy implications surrounding the surge of Large Language Model (LLM) generative AI technology. In the wake of OpenAI's ChatGPT 3.5 release, the landscape of AI-powered innovation has evolved rapidly, prompting critical questions about data security and privacy safeguards. In this presentation, we'll delve into a real-world case study of a SaaS B2B tech company's journey to leverage this cutting-edge technology responsibly. Learn first hand how they successfully navigated the complex terrain of privacy concerns while collaborating closely with enterprise-level customers. From implementing robust data protection measures to forging secure partnerships with AI providers like OpenAI, discover actionable strategies to safeguard sensitive information without compromising innovation.
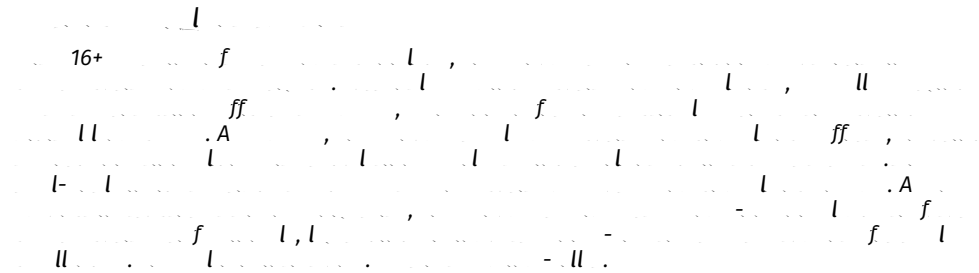
## á6 ëƒë¡} ë% ámTƒ‹ëƒ¡j è¡½ë}ë‹ë%Ì ‹à¡ þë‹T%ëƒ«} •¡}}6%} É6

Karla Carter, Bellevue University

## F7 - þz¶¥

**9 a.m. Session**

Attack, Detect, Defend: Antisyphon Training (Part 1), *l* & *l*

Designing a Successful Identity Security Program, *ll* & *l*

Navigating Privacy in the Age of Generative AI,

ÿ Tr r ò¡}}ë6%

Attack, Detect, Defend: Antisyphon Training (Part 2), *l* & *l*

Beyond Vulnerability Detection: Using Large Language Models in Security Vulnerability Analysis for Investigative Assessment, *l*

Protecting LLMs Using Splunk and the OWASP Top 10 for LLM Applications, *A*

Tr r ò¡}}ë6%

Does Mr. Data Dream at Night?, *A*

Identifying the Adversary and Operationalizing Cyber Threat Intelligence,

j   br r ò¡}}ë6%

National Cyber Security Awareness Month and CISA Cyber Security Services, *l*

Policies in Practice: Revisiting the Titanic's Lessons for Cybersecurity, *l*

## F¥7   òF è

**9 a.m. Session**

Navigating Privacy in the Age of Generative AI,

ÿ Tr r ò¡}}ë6%

Beyond Vulnerability Detection: Using Large Language Models in Security Vulnerability Analysis for Investigative Assessment, *l*

Tr r ò¡}}ë6%

Does Mr. Data Dream at Night?, *A*

Identifying the Adversary and Operationalizing Cyber Threat Intelligence,

j   br r ò¡}}ë6%

National Cyber Security Awareness Month and CISA Cyber Security Services, *l*

Policies in Practice: Revisiting the Titanic's Lessons for Cybersecurity, *l*

## ¡ ¥ eF¡F¥þ

**9 a.m. Session**

Designing a Successful Identity Security Program, *ll* & *l*

Navigating Privacy in the Age of Generative AI,

ÿ Tr r ò¡}}ë6%

Beyond Vulnerability Detection: Using Large Language Models in Security Vulnerability Analysis for Investigative Assessment, *l*

Protecting LLMs Using Splunk and the OWASP Top 10 for LLM Applications, *A*

Tr r ò¡}}ë6%

Does Mr. Data Dream at Night?, *A*

Identifying the Adversary and Operationalizing Cyber Threat Intelligence,

j   br r ò¡}}ë6%

Accelerating the Evolution of Cybersecurity Using a Converged Approach,

Securing Data in an AI Driven World,

j   br r ò¡}}ë6%

National Cyber Security Awareness Month and CISA Cyber Security Services, *l*

Policies in Practice: Revisiting the Titanic's Lessons for Cybersecurity, *l*

## þF-q¥z- •

**9 a.m. Session**

Attack, Detect, Defend: Antisyphon Training (Part 1), *l* & *l*

Navigating Privacy in the Age of Generative AI,

ÿ Tr r ò¡}}ë6%

Attack, Detect, Defend: Antisyphon Training (Part 2), *l* & *l*

Beyond Vulnerability Detection: Using Large Language Models in Security Vulnerability Analysis for Investigative Assessment, *l*

Protecting LLMs Using Splunk and the OWASP Top 10 for LLM Applications, *A*

Tr r ò¡}}ë6%

Does Mr. Data Dream at Night?, *A*

Identifying the Adversary and Operationalizing Cyber Threat Intelligence,

j   br r ò¡}}ë6%

Securing Data in an AI Driven World,

First Floor

Second Floor

## Lunch

**Fried Chicken**

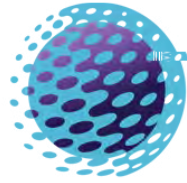**Assorted Danish**

**Afternoon Snack**

**Assorted Cookies**

**Ice Tea, Water, Coffee**

Meals are prepared in a shared kitchen.

TANDEM



Google Cloud



Americom



CROWDSTRIKE



CLOUDFLARE
PUBLIC SECTOR