CYBERSECURITY
& Information Systems Digest

JULY IS RANSOMWARE AWARENESS MONTH

Ransomware Awareness Month aims to educate individuals and organizations about what ransomware is, the dangers it poses, and protective measures they can take to combat it. Ransomware attacks involve malware encrypted to lock a computer and render its files and their systems unusable. Malicious actors then demand a ransom for decryption and its release.

The Cybersecurity and Infrastructure Security Agency (CISA) provides their #StopRansomware Guide, which outlines best practices to detect, prevent, respond, and recover from potential attacks.

Learn more and download the CISA guide: https://www.cisa.gov/stopransomware.

DID YOU MISS OUR LAST WEBINAR?

"A Journey From CRISP to ATLAS"

▶ **WATCH NOW!**

or download the slides

NOTABLE TECHNICAL INQUIRY

What artificial intelligence/machine-learning tools can perform analysis on data centralized in the Repository for Analytics in a Virtualized Environment platform?

Artificial intelligence (AI) and machine learning (ML) are transforming the ways organizations interact with data and generate insights from it. This report introduces key concepts present using AI for data analytics and highlights the most recent tools and platforms in the field. Several commercial, government, or open-source software tools were identified during research. These tools could be used to leverage AI/ML to support the inquirer in data-analytic... **READ MORE**

UPCOMING WEBINAR

Pixabay
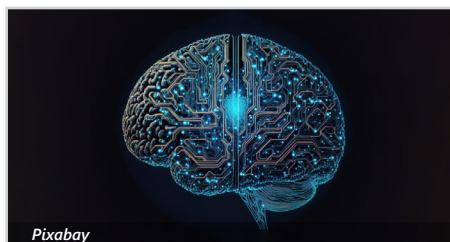
AI Reliability Risk Assessment
COMING SOON

Presenter(s): Nathan Herbert   *Host:* CSIAC

Reliability of a military system refers to its ability to complete a specific mission without failure. Failure modes in traditional acquisition systems often involve hardware, software, and human-systems integration. These failure modes are generally well-understood and can be mitigated early in design. As artificial intelligence (AI) and autonomous products are incorporated in military systems, mission completion also depends on the system's robustness and... **READ MORE**

U.S. Air Force

HIGHLIGHT

Accelerating Cyber Resilience: Air Force, DARPA Join Forces to Strengthen Cyber Defenses

A strong, lethal military demands cutting-edge and resilient software to power every weapon and support system our U.S. Warfighters depend on. However, the U.S. Department of Defense's (DoD's) reliance on aging IT infrastructure, using security policies developed over the last 30 years, creates inherent vulnerabilities in its systems, from legacy architectures to advanced weapons.

Meanwhile, threat actors are actively exploiting these vulnerabilities, targeting critical infrastructure, stealing sensitive military code, and reengineering sensitive systems to compromise national security... **LEARN MORE**

EVENTS

TechNet Emergence 2025
July 15–16, 2025
Reston, VA

Black Hat USA 2025
August 2–7, 2025
Las Vegas, NV

ISC2 Security Congress 2025
October 28–30, 2025
Nashville, TN

Want your event listed here?
Email contact@csiac.org to share your event.

VOICE FROM THE COMMUNITY

Rober Urias
Cyberspace Manager, Space Systems Command (SSC)

Rober Urias serves as the Vandenberg SFB Space Launch Delta 30 alternate information systems security manager and cyberspace manager supporting SSC and the Space Operations Command. He develops and manages base-wide cybersecurity programs, as well as computer and network security for national critical command and control systems. His focus is on establishing and publishing base-wide policy to manage the INFOSEC, COMPUSEC, COMSEC, TEMPEST, and RMF programs and providing advice and guidance on implementation and procedures used in developing and operating systems.

ARE YOU A SME?

If you are a contributing member of the information systems community and are willing to help others with your expertise, you are a subject matter expert (SME).

Join our team today.

BECOME A SUBJECT MATTER EXPERT

TECHNICAL INQUIRIES (TIs)

WHAT IS THE TI RESEARCH SERVICE?

- FREE service conducted by technical analysts
- 4 hours of information research
- Response in 10 business days or less

WHO CAN SUBMIT A TI?

- U.S. government (federal, state, or local)
- Military personnel
- Contractors working on a government or military contract

WHY UTILIZE THE TI RESEARCH SERVICE?

- Get a head start on your technical questions or studies
- Discover hard-to-find information
- Find and connect with other subject matter experts in the field
- Reduce redundancy of efforts across the government

To submit a TI, go to
https://csiac.dtic.mil/technical-inquiries

EXAMPLE CSIAC TIs

- What information is available on missile simulations and validation of physics-based models without direct access to real weapon flight test data?
- Are reinforcement learning techniques available for a next-generation threat system?
- What information is available on secure identity and access management solutions?

MORE CSIAC INQUIRIES

EXAMPLE DSIAC & HDIAC TIs

- What does ERD95 refer to when related to laser designators?
- What government-off-the-shelf or commercial-off-the-shelf tools are available to provide a human-machine interface that can be used for law enforcement and emergency management scenarios?
- Can references be provided on the Gyrodyne QH-50C—specifically, a nuclear variant?

VIEW MORE TIs

The Information Analysis Centers answer more inquiries outside the scope of CSIAC's focus areas. To search more research topics, visit our sister websites to expand your search.

DSIAC INQUIRIES   **HDIAC INQUIRIES**

FEATURED NEWS

### NIST Offers 19 Ways to Build Zero Trust Architectures

If you're trying to secure your organization's computer network from cyberattacks, traditional approaches may not work. Gone are the days when you could keep all your electronic assets inside a single building and construct a firewall between them and the wider internet. **READ MORE**

RECENT NEWS

Canva

AI Research to Improve How We Find and Use Critical Information

University of Maryland ARLIS

MIT Lincoln Lab/Atomic Physics Lab
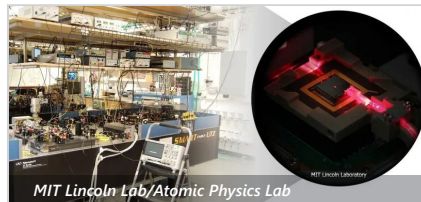
Small Business Accelerates Transition of Quantum Tech From Lab to Market

USC Institute for Creative Technologies

LLNL Lawrence Livermore National Laboratory

Stanford Professor Discusses Future of Visually Intelligent Machines and Human-AI...

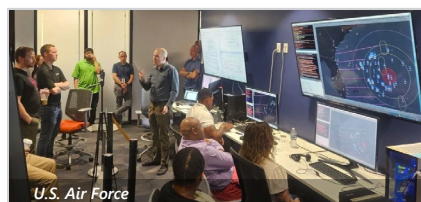Lawrence Livermore National Laboratory

U.S. Cyber Command

USCYBERCOM Demonstrates Global Cyber Superiority With Cyber Guard 25-2

U.S. Cyber Command
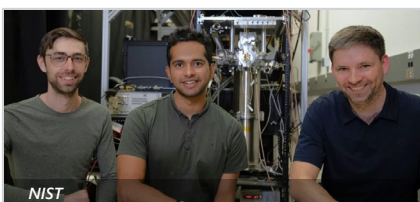
NIST

NIST and Partners Use Quantum Mechanics to Make a Factory for Random Numbers

National Institute of Standards and Technology

U.S. Air Force

Air Force DASH Sprint Pioneers Human-Machine Teaming for Faster Battle Management...

U.S. Air Force Research Laboratory

Cybersecurity

Knowledge Management & Information Sharing

Modeling & Simulation

Software Data & Analysis