

CYBERSECURITY & Information Systems Digest

The Latest From the Cybersecurity & Information Systems Information Analysis Center // August 10, 2021



NOTABLE TECHNICAL INQUIRY

What is the Operational System Risk Imposed by the Infrastructure Deployment Pipeline Workflow?

Real-time data monitoring of systems and system forensics is an essential aspect to keeping your data security platform safe when relying on the use of Infrastructure as Code (IaC) and the potential vulnerabilities associated with its continuous deployment (CD). Many organizations are facing an information overload and are inadequately prepared for understanding and designing a cyber incident response plan with near-real-time monitoring, including detection, analysis of system event logs, user activities, and system access tracking. [READ MORE](#)



SNEAK PEEK

UPCOMING WEBINAR

*Cyber Resilient Weapon Systems
Body of Knowledge (CRWS-BoK)*

DATE:

August 19, 2021

TIME:

12:00 PM

PRESENTED BY:

Burhan Y. Adam
OUSD(R&E)

HOST:

CSIAC



VOICE FROM THE COMMUNITY

Philip Payne

Technical Lead, Cybersecurity & Information Systems Information Analysis Center (CSIAC)

As the new technical lead, Philip Payne (CISSP and security+ certified), comes from a rich background in cybersecurity with the C5ISR center (formerly CERDEC). At C5ISR, he led a world-class cross-domain solution (CDS) lab, where he performed lab-based security assessments on Army CDSs going through the Secret and Below Interoperability CDS Certification and Accreditation Approval process. He was a key member of the INFOSEC Branch, which has made a myriad of contributions in cyberspace for the U.S. Department of Defense at large. At SURVICE Engineering, he served as a vital member of the cyber research and development team as the senior cybersecurity engineer supporting the Data Analysis Center (formerly AMSAA) on early acquisition cybersecurity assessments for Army systems.

BECOME A SUBJECT MATTER EXPERT



Shutterstock

HIGHLIGHT

Request for Information (RFI) on an Implementation Plan for a National Artificial Intelligence Research Resource

The Office of Science and Technology Policy and the National Science Foundation are issuing this RFI to inform the work of the National Artificial Intelligence Research Resource (NAIRR) Task Force (“Task Force”). The Task Force has been directed by Congress to develop an implementation roadmap for a shared research infrastructure that would provide artificial intelligence (AI) researchers and students across scientific disciplines with access to computational resources, high-quality data, educational tools, and user support.

LEARN MORE

FEATURED NEWS

United States Government Launches First One-Stop Ransomware Resource at StopRansomware.gov

Today, as part of the ongoing response, agencies across the U.S. government announced new resources and initiatives to protect American businesses and communities from ransomware attacks. The U.S. Department of Homeland Security (DHS) and the U.S. Department of Justice (DOJ), together with federal partners, have launched a new website to combat the threat of ransomware.



READ MORE

Image: Shutterstock



DVIDS

WEBINARS

Cyber Resilient Weapon Systems Body of Knowledge (CRWS-BoK)

Presented: August 19, 2021 12:00 PM - 1:00 PM

Presenter: Burhan Y. Adam, OUSD(R&E) Office of Strategic Technology Protection and Exploitation

Host: CSIAC

The Resilient Systems (RS) Directorate in the Strategic Technology Protection and Exploitation Office, under the Office of the Under Secretary of Defense for Research and Engineering, launched the Cyber Resilient Weapons Systems Body of Knowledge (CRWS-BoK) on May 6, 2021. The CRWS-BoK provides a comprehensive repository of authoritative guidance and knowledge for science and technology (S&T) professionals who specialize in CRWS. Users (i.e., engineers, S&T managers, and researchers from across the U.S. Department of Defense (DoD) federal government, industry, and academia) can access, search, annotate, save, and share crucial engineering information needed to develop, maintain, and monitor secure CRWS programs. [LEARN MORE](#)



Network Survivability Assessment Methodology

September 22, 2021
12:00 PM–12:45 PM

EVENTS

Data Center World

August 16, 2021

Workshop on Cybersecurity Labeling Programs for Consumers: Internet of Things (IoT) Devices and Software

September 14, 2021

National Cyber Summit

September 28, 2021

2021 Security Congress

October 18, 2021

IEEE Secure Development Conference

October 18, 2021

MORS Emerging Techniques Forum

December 7, 2021

RSA Conference

February 7, 2022

Want your event listed here?

Email contact@csiac.org, to share your event.



-  Cybersecurity
-  Knowledge Management & Information Sharing
-  Modeling & Simulation
-  Software Data & Analysis

The inclusion of hyperlinks does not constitute an endorsement by CSIAC or the U.S. Department of Defense (DoD) of the respective sites nor the information, products, or services contained therein. CSIAC is a Defense Technical Information Center (DTIC)-sponsored Information Analysis Center, with policy oversight provided by the Office of the Under Secretary of Defense for Research and Engineering (OUSD(R&E)). Reference herein to any specific commercial products, processes, or services by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the U.S. government or CSIAC.

4695 Millennium Drive
 Belcamp, MD 21017
 443-360-4600 | info@csiac.org
 csiac.org
 Unsubscribe | Past Digests




RECENT NEWS



DARPA Open Sources FETT Bug Bounty Hardware Evaluation Platform, Tools

Cybersecurity and KM & Information Sharing



Automatic Proofs of Differential Privacy

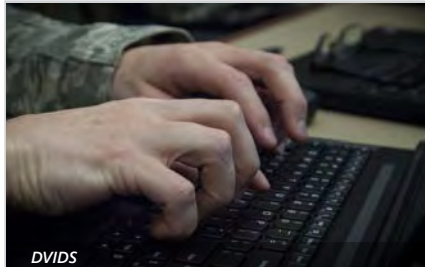
Cybersecurity and Software Data & Analysis



Chinese State-Sponsored Cyber Operations: Observed TTPs


NSA, CISA, and FBI Detail Chinese State-Sponsored Actions, Mitigations

Cybersecurity



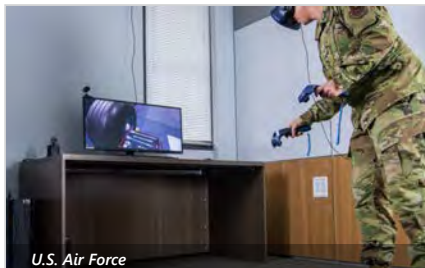
Background Press Call on Improving Cybersecurity of U.S. Critical Infrastructure

Cybersecurity



Top Routinely Exploited Vulnerabilities

Cybersecurity



Tech Training Transformation Modernizes Tech Training With Virtual Reality

Modeling & Simulation