ASCE
ACADEMIC SECURITY AND COUNTER EXPLOITATION PROGRAM
https://asce.tamus.edu

THE OPEN SOURCE MEDIA SUMMARY

April 26, 2023

THE GOVERNMENT HAS AN ESPIONAGE PROBLEM. OPEN SOURCE SHOULD BE PART OF THE SOLUTION.

Brian Drake | The Cipher Brief | April 24, 2023

The unauthorized release of classified information and the subsequent arrest of Jack Teixeira has raised important questions. Why does the Air National Guard have staff with Top Secret clearances? If he is found guilty, was Teixeira's ego really the cause of the leak? And what can be done about preventing these leaks in the future? While these are all good questions, they do not address the central flaw in the American security apparatus: The U.S. government is not assessing security risk with the right data sources at scale. Today, the security vetting process involves filling out a lengthy form, a series of suitability interviews, a credit check, and for certain clearance types, a polygraph. Prior to 2008, every employee was reinvestigated every five to ten years. Now, under the Continuous Evaluation Program (CEP), the government performs a thorough background check once and relies on automated ingests of terrorism watch lists, foreign travel, financial, criminal, credit, public records, and prior clearance eligibility determinations. All of this data is processed manually by threat analysts across the constellation of national security agencies. There are two problems with the design of this system.

Read the full article here.

CHINA'S PLANNED CHANGES TO ESPIONAGE LAW ALARM FOREIGN BUSINESSES

Yukio Tajima | Nikkei Asia | April 25, 2023

China is preparing to restrict transfers of any information related to national security under an updated counterespionage law, raising fears of a stepped-up crackdown on foreign individuals and companies here. The Standing Committee of the National People's Congress began deliberating the changes Monday. The legislation, which will broaden the definition of espionage, is expected to pass Wednesday. This will mark the first time since 2014 that the law has been amended. The measure will expand the scope of the law -- now limited to state secrets -- to cover all documents, data, materials or items related to national security and interests. It does not provide further details on what constitutes national security and interests. A greater focus will also be put on cybersecurity. Discussions of a system's vulnerabilities to cyberattacks could run afoul of the new rules. Security authorities will be granted more power, including in inspecting baggage and electronic devices of those suspected of espionage. Chinese citizens and organizations will have to report suspected espionage.

Read the full article here.

SEVEN CRITICAL TECHNOLOGIES FOR WINNING THE NEXT WAR

Emily Harding and Harshana Ghoorhoo | Center for Strategic & International Studies | April 18, 2023

The next war will be fought on a high-tech battlefield. But which technologies will make a real difference? Where will the United States find a technological edge? This CSIS report identifies the seven technologies that could make the difference in a fight against a near-peer adversary. Three are "sprint" technologies, where the United States should aggressively pursue advancement with considerable resources and focused commitment: quantum sensing and computing, biotechnology, and secure, redundant communications networks. Four are "follow" technologies, where the United States should support and shape efforts ongoing in the private sector: high-performance batteries, artificial intelligence/machine learning, space-based sensors, and robotics. The consequences of failure on any of these technologies are tremendous—they could make the difference between victory and defeat. This report aims to focus efforts on the areas that count, across intelligence work, hybrid warfare, competition, and conflict, to prepare for competition today and potential conflict in the future.

Read the full article here.

EIGHT YEARS SINCE THE OBAMA-XI AGREEMENT, CHINESE HACKING IS WORSE THAN EVER

Derek B. Johnson | SC Media | April 24, 2023

Eight years ago, the United States and China reached an historic treaty agreement that was designed, in part, to end a persistent deluge of cyberattacks targeting American businesses to steal their corporate secrets and intellectual property. At the time, then-President Barack Obama lauded the agreement in a joint press conference with China President Xi Jinping, saying it marked a "common understanding" between the two nations "that neither the U.S. or the Chinese government will conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information for commercial advantage." Eight years later, that sentiment has aged like warmed over milk. Chinese hackers did not stop targeting American businesses, but according to security experts at Google, they have evolved to become significantly more aggressive and innovative in the years since. Prior to the agreement, hackers associated with China were broad and unfocused in the businesses they hacked.

Read the full article here.

WHAT IS THE NIST CYBERSECURITY FRAMEWORK? ALL YOU NEED TO KNOW

InstaSafe | Zero Trust Blog | September 22, 2022

The growing sophistication of cyber-attacks poses challenges to businesses of all sizes. Hence, understanding cybersecurity risks and managing them with suitable measures is the need of the hour. Organisations today need an effective cybersecurity program to secure their critical resources. Considering this, the National Institute of Standards and Technology (NIST) at the US Department of Commerce has drafted the Cybersecurity Framework. It aims to address the lack of cybersecurity standards. NIST offers a set of guidelines that organisations in different industries can use. The framework is helping organisations improve their ways of responding and recovering from cyber-attacks by analysing the root causes of such incidents. Let's find out more about the NIST framework and how it can provide a robust strategy to tackle cybersecurity challenges. While every function of the NIST framework is essential, identification is the most crucial aspect. It provides a concrete foundation for your cybersecurity program. Once you identify the assets that require protection, you can apply appropriate strategies to detect the vulnerabilities and protect them.

Read the full article here.

THE MAKING OF A BIOSAFETY OFFICER

Davis Gillum | Issues in Science and Technology | Spring 2023

The potential risks for accidents and misuse increase as biotechnology becomes more sophisticated, less expensive, and increasingly distributed. During my 28 years as a biosafety officer, I have dealt with laboratory explosions, fires, spills, needlesticks, eye contamination, accidental releases, and lost or unaccounted-for inventory—along with the day-to-day anxieties of keeping labs safe. Biosafety professionals are responsible for mitigating risks at universities, federal laboratories, health care facilities, nonprofits, and pharmaceutical and other commercial operations. While we—I am one of only a few thousand in the United States—have similar job titles, our backgrounds run the gamut from microbiology to chemistry, from high school or associate degrees to PhDs. We are so diverse that it raises the question of how people become biosafety professionals and what makes them proficient. It is in the doing that regulations on pieces of paper become realized in the world.

Read the full article here.

EU PLANS NEW RULEBOOK FOR HANDLING SENSITIVE SCIENCE LINKS WITH CHINA

Florin Zubaşcu | Science Business | April 18, 2023

The EU should not cut scientific ties with China, but it needs to ensure sensitive technologies are not being leaked to the Chinese military, EU Commission president Ursula von der Leyen told MEPs today. In her first opportunity to discuss the issue since her visit to China with French president Emanuel Macron earlier this month, von der Leyen told a plenary session of the European Parliament that the EU does not want "cut economic, societal, political and scientific ties" with China but needs to figure out urgently how to rebalance its relationship with the communist regime. "There is clearly a need for Europe to work on de-risking some important and sensitive parts of our relationship," she said. EU companies need new tools to protect themselves against Chinese attempts to scoop up technologies that have civilian and military use. "We have to look at where there are gaps in our toolbox, which allow the leakage of emerging and sensitive technologies through investments in other countries," von der Leyen said. In support of this, the Commission will publish guidelines and measures aiming to help EU companies protect their technologies and ensure EU capital and knowledge is not being used for the benefit of China's military.

Read the full article here.

U.S. TO PENALIZE COMPANIES FOR STAYING QUIET ABOUT EXPORT-CONTROL ISSUES

David Smagalla | The Wall Street Journal | April 18, 2023

The U.S. Commerce Department is cracking down on companies that discover potential export-control violations but choose not to disclose them to the government. Export controls restrict where U.S. companies can sell technologies with both commercial and military uses. The rules aim to prevent adversaries such as China, Russia and Iran from boosting their capabilities with advanced Western technology. They are administered by the Commerce Department's Bureau of Industry and Security, which can bring civil penalties against companies that allow such "dual use" items to fall into the wrong hands. Businesses that discover significant possible violations—but choose not to voluntarily disclose that information to the government—risk having the government consider that an "aggravating factor" in any penalties imposed, Matthew Axelrod, assistant secretary for export enforcement at the BIS, said in a memo seen by The Wall Street Journal. The Commerce Department can reduce penalties for companies that own up to possible export-control violations.

Read the full article here.

UNITED STATES: FIVE ESSENTIAL TOOLS FOR DUE DILIGENCE OPEN-SOURCE RESEARCH

Donald Pearce | Mondaq | April 28, 2022

Today's compliance professionals have abundant resources to make better decisions about their clients and supply chain partners faster and with greater confidence than ever before. However, accessing those resources online poses challenges: maintaining privacy, protecting computer networks from malware or intrusion, and just finding good sources among the plethora of paid and free services found online. Also, many compliance professionals are locked into a particular program or workflow, be it handed down by routine, mandated by management, or completely self-served, limiting the potential for expanding their knowledge base or confirming their conclusions. Here are five resources you may want to introduce to your open-source toolkit to enhance your security, shorten your search time, and improve your results if you are not currently using them in your due diligence workflow. The most important thing to remember about conducting open-source investigations is that you cannot trust everything you find; this includes the data or the source, the server, and websites you might explore to gather information.

Read the full article here.

EASTERLY: SECURE-BY-DESIGN AIMS TO DRIVE DOWN VULNERABILITIES

Grace Dille | MeriTalk | April 13, 2023

The Cybersecurity and Infrastructure Security Agency (CISA) published its secure-by-design and -default guidance today, which CISA Director Jen Easterly said is all about driving down cyber vulnerabilities to near zero. Easterly joined the Axonius Federal Forum 2023: Adapt event in Washington, D.C. today, where she explained how the new principles aim to keep Americans safe in today's technology ecosystem by putting the responsibility on the technology manufacturer instead of the user. "It is really about starting a conversation that helps to move the needle on incentives that have been misaligned for decades," she said. "The internet was not built for safety. Software was not built for safety … so we want to have this conversation." "At the end of the day, software makers want to produce safe tech, consumers want safe tech – it's just the incentives are now misaligned because it's about speed to market. It's about cost. And there is imperfect information," she added. "As a consumer, I don't know what's in my software."

Read the full article here.

WHAT IS BYOD (BRING YOUR OWN DEVICE) & WHY IS IT IMPORTANT

InstaSafe | Zero Trust Blog | February 20, 2023

It is commonly assumed that BYOD, or Bring Your Own Device, is primarily used by small to medium-sized businesses to save money. This assumption is understandable, as not all companies can afford to spend a significant amount of money per employee on providing them with the latest technological devices. However, it is important to note that BYOD can also significantly impact larger companies. For example, in 2010, Intel, a major technology company, reported that over 30,000 employee-owned mobile devices were covered under its Bring Your Own Device policy. They highlighted several benefits of implementing a well-structured BYOD policy, such as increased productivity, minimal security issues, and greater control over employees' workloads. Thus, it is evident that BYOD can offer advantages to businesses of all sizes, not just small to medium-sized ones. Before we state some security concerns related to BYOD, let's first examine what BYOD is and why it is important. BYOD, or Bring Your Own Device, is a trend where employees utilise their own personal devices, such as smartphones, tablets, personal computers, or USB drives, to connect to their organisational networks and gain access to work-related systems.

Read the full article here.

CONDUCTING OPEN SOURCE DUE DILIGENCE FOR SAFEGUARDING RESEARCH PARTNERSHIPS

Innovation, Science and Economic Development Canada | Government of Canada | 2022

This guide is designed to help any individual looking to identify, assess, and manage risks to research, especially risks arising from partnerships. As such, the guide is written in a way that it can be understood and apply to any and all audiences; some content may be more or less useful to each individual based on their unique situation. The guide draws on methods from Open Source Intelligence (OSINT), an intelligence discipline that collects and analyses public information to support decision-making; for this guide, we term this open source due diligence. By helping you bring structure to your thinking and approach, open source due diligence methods make the online world more discoverable. While the majority of research partnerships are transparent and provide mutual benefits to all research partners, some activities by foreign governments can pose real national security risks. This guide will provide you with tools and techniques to identify these risks to research partnerships.

Read the full article here.

THE TEXAS A&M
UNIVERSITY SYSTEM

The Academic Security and Counter Exploitation Program is coordinated by The Texas A&M University System Research Security Office as a service to the academic community.
https://rso.tamus.edu