San Diego Regional Cyber Lab

Cyber Lab x United Way of San Diego

On July 23rd, the San Diego Regional Cyber Lab and Cyber Center of Excellence (CCOE) partnered with United Way of San Diego to bring 35 students into our downtown lab space to learn more about what it takes to secure a career in cyber security. As part of United Way's STEAM-to-Careers program, students navigated through several educational lessons focused on Linux command-line interfaces through the lab's Haiku game offerings.

Students also sat in on several career-oriented presentations, including an extensive exploration of cyber career opportunities provided by the City of San Diego's Chief Information Security Officer **Brendan Daly** and several members of his cyber security team.

A presentation was also provided by **Bianca Arce**, former Cyber Lab intern and member of the San Diego Chapter of Women in CyberSecurity (WiCyS). As an appointed membership chair and recently elected secretary for WiCyS, Bianca shared insights into her organization's capabilities to support these students if they wish to explore careers in cyber.

(Cont...)

Upcoming Events:

- *July 31: Quarterly Cyber Lab Regional Stakeholder call*
- *Sept. 10: Cybersecurity Summit*

In This Issue

Local Threat Intelligence Support

The San Diego Law Enforcement Coordination Center (SD-LECC), our fusion center and Regional Threat Assessment Center, provides cyber threat intelligence and incident support to SLTT agencies and critical infrastructure across San Diego and Imperial Counties.

Through the Cyber Lab partnership, SD-LECC leverages Recorded Future's Threat Intelligence and Brand Intelligence to deliver real-time alerts and proactive hunting across adversaries, infrastructure, and targets.

Capabilities include leaked credential discovery, typosquat/ domain monitoring, code leak detection, dark web brand monitoring, and rapid takedowns via PhishFort credits.

To onboard your domains/brands or request support, contact cyber@sdlecc.org and visit sdlecc.org.

Cyber Lab x United Way of San Diego (Continued)

An incredibly insightful presentation was also provided by **Shriya Paladugu**, a brilliant high school student who presented on her "AI on the Streets" Girls Scouts Gold Award project, focusing on the tangible benefits to vehicle traffic patterns and anticipated technical/security concerns in integrating Artificial Intelligence in critical public infrastructure like traffic signals. She developed and released an online traffic signal simulator to visually display the calculations and metrics behind her project. On her site, she also provides educational opportunities for visitors to learn more about AI, cybersecurity in smart cities, the direct impact her project has had on the San Diego community, and more.

We are so thankful to have such brilliant minds in San Diego and we look forward to hosting more opportunities like this in the lab in the future.

Students and educators impacted by recent Canvas breach

In May 2026, the hacker group **Shiny Hunters** successfully targeted **Instructure**, the parent company of the education platform Canvas, with a ransomware attack. Through this attack, the group successfully acquired student and faculty names, emails, ID numbers, and direct messages within the Canvas platform. Shiny Hunters used this stolen personal information to demand a ransom from **Instructure**, resulting in an agreement to pay the ransom in exchange for "digital confirmation" of the data's deletion.

The timing of the attack was especially impactful as the shutdown of Canvas caused significant issues across all campuses using the platform as students were preparing for, or actively taking, their final exams during this time. Instructure stated that no passwords, dates of birth, government identification numbers, or financial information were exposed, however there is no definitive way to know.

As is the case following any confirmed data breach, it is highly recommended that you change any relevant passwords if you believe your information may have been leaked during this event. For more information, click here.

How Agentic AI Tools Can Improve Productivity With Caution

The **Cybersecurity and Infrastructure Security Agency** (CISA), together with the **Australian Signals Directorate's Australian Cyber Security Centre** (ASD's ACSC) and other international partners, has released guidance to help organizations use agentic artificial intelligence (AI) systems safely. Their guide explains the main security challenges and risks that come with agentic AI and offers practical steps for building, launching, and managing those systems responsibly. It also helps organizations match their AI risk management practices with existing cybersecurity frameworks and improve oversight as agentic AI becomes more widely used.

The guide encourages organizations, especially those in government, industry, and critical infrastructure, to:

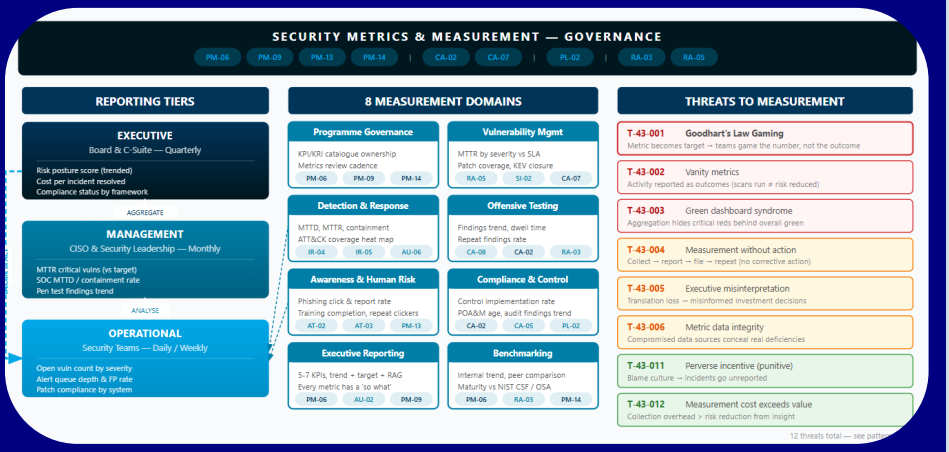
- Leverage existing cybersecurity frameworks rather than creating separate AI policies.
- Apply "least privilege" principles and tightly control agent permissions.
- Design incrementally, deploying agentic AI only for low-risk, non-sensitive tasks while continuously monitoring their operations.
- Keep humans involved in overseeing high-impact actions, and ensure strong identity and access management to prevent unauthorized or malicious behavior.

Overall, the guidance helps organizations balance innovation with risk mitigation, offering practical steps to safely pilot, deploy, and scale agentic AI while maintaining robust cybersecurity hygiene and governance.

Link to article for more information on this topic: [link]

Open-Source Security Patterns and Control Mappings

If you're looking for another tool to add to your cyber tool belt, we recommend you explore [Open Source Security Architecture]. Their site has an enormous amount of data to parse through and likely has something useful for anyone working in a more technical role within a cyber team. Whether you are looking to dig deeper into specific security patterns, frameworks, policies, or control mechanisms, we believe this site can provide some valuable insights for you and your team.



TeamPCP's Recent Multi-Layered Supply Chain Attack Inside Security Infrastructure

Users still often view cyber attacks as primarily targeted towards their computers or accounts directly, but we in cyber know better. Hacking groups know that the weakest point of security is often not within your operational environments themselves, but further up your supply chains.

Recently, the threat group TeamPCP placed malicious code into well-known open-source applications used by thousands of organizations around the world. These attacks allowed TeamPCP to inject malicious infostealer payloads directly into GitHub actions and Python Package Index registries.

From here, the malicious code collected customer information, confidential business information, API keys and passwords, cloud account credentials, and more. The data, totaling over 300GB, was collected from more than half a million infected machines.

Their attack methods included exploiting incomplete credential rotations following prior data breaches, exploiting vulnerable cloud endpoints, utilizing a targeted compromise of a popular open-source infrastructure-as-code scanner, and more.

For a full breakdown of their attack methods, the affected systems, and the interim guidance provided to potentially affected users, click here.

San Diego Cybersecurity Summit Fall 2026

The Official Cybersecurity Summit

The Official Cybersecurity Summit in San Diego, which will be held on September 10, 2026 at the Marriott Marquis San Diego Marina, will offer a full day of expert-led panels, solution demonstrations, and networking opportunities for vetted cybersecurity and IT practitioners, with CPE/CEU credits available for full attendance. The event covers practical, business-focused topics including AI and automation risk, supply chain and identity security challenges, and methods for aligning cybersecurity resilience with organizational objectives.

Speakers will share real-world insights and frameworks that attendees can apply directly within their teams. Overall, the summit is designed to provide actionable guidance that helps security leaders strengthen defenses, address emerging threats, and communicate cyber risk effectively across their organizations.

For more information, click here.

White House Notice: National Quantum Strategy

In anticipation of the rollout of PQC (postquantum cryptography), the White House has announced a variety of initiatives to support quantum info science and technology (QIST) efforts, with an emphasis in unified government actions to ensure federal agencies assist in securing a strategic advantage in QIST research and widespread alignment with new PQC policies.

To read more about the specific affected agencies and associated policies, click here.

Connect With Us

LinkedIn

Contact Us

SDRCL Program Lead
Ian Brazill
IBrazill@sandiego.gov

SDRCL Cyber Lead
Brendan Daly
BMDaly@sandiego.gov

Cyber Center of Excellence (CCOE), Community Partner
Lisa Easterly
Lisa.easterly@sdccoe.org

San Diego Regional Cyber Lab
1200 Third Avenue, Suite 1800
San Diego, CA 92101
http://www.sandiego.gov/cyber-lab

SAN DIEGO REGIONAL CYBER LAB