San Diego Regional Cyber Lab

My eCISO: San Diego County's Newest No-Cost Cyber Resource

Last year, the San Diego Regional Cyber Lab partnered with Cal Poly and Amazon to develop a proof-of-concept cyber evaluation tool aimed at providing agencies and individuals with a no-cost option to evaluate their cyber defenses/practices. Following initial testing efforts with a variety of regional partners, a functional prototype was developed and delivered to the Cyber Lab working group. The tool was promptly named My eCISO: A Large Language Model (LLM) AI resource hosted in AWS and powered by Anthropic's Claude AI model. The initial capabilities of My eCISO were immediately identified as a groundbreaking new opportunity to empower users to evaluate their current cyber maturity and obtain prioritized recommendations based on the NIST framework without the need to spend a dime. The target audience for My eCISO is any given user or organization who does not have the luxury of an in-house Chief Information Security Officer or similar cyber resources.

In early 2024, the San Diego Regional Cyber Lab and City of San Diego contracted with 11:59 to develop a full scale production-ready version of My eCISO. Development is currently underway and several of the Cyber Lab's regional partners have agreed to assist with the final testing efforts prior to My eCISO's release. Thank you to all who have volunteered to be a part of this ongoing effort.

Given the sensitive nature of an agency's cyber practices, we know that users may be initially hesitant to speak with My eCISO. This consideration has been at the forefront of all development efforts and we believe you will be pleased with the levels of transparency surrounding its design and the security precautions implemented to protect your data. For starters, your conversations will never be used to further train the LLM model, limiting capabilities for sensitive data extraction via prompt injection. Further, your conversations will be completely erased after 30 days, but can also be deleted at any time with a click of a button. The technology used to power My eCISO will also be explained in detail for users to explore. Last but not least, user accounts will all be integrated through Auth0, ensuring that MFA is always required for access.

If you are able to attend the Cyber Lab's upcoming Stakeholder Steering Committee calls in April, you may just be the first to preview this new regional resource. Invitations to our upcoming calls will be sent out shortly.

Upcoming Events:

- *BSides San Diego - Hacker Spring Break (3/30)*
- *Quarterly Technical Stakeholder Committee Meeting (4/11)*
- *Quarterly Executive Stakeholder Committee Meeting (4/25)*

In This Issue

IBM Cost of a Data Breach Report 2023

- In 2023, IBM found data breach costs hit a record high of $4.45 million, up 2.3% from 2022 and 15.3% since 2020.
- 51% of organizations plan to boost security investments post-breach. Top priorities include incident response, employee training, and threat detection.
- On average, organizations experienced a $1.76 million reduction in breach costs and a 108-day shorter time to identify and contain breaches through extensive use of security AI and automation.
- Only 67% were detected internally, underscoring the need for enhanced threat detection, with attackers' disclosure costing organizations nearly $1 million more than internal detection.
- Since 2020, healthcare data breach costs have surged by 53.3%, marking the industry's 13th consecutive year reporting the highest average breach costs of $10.93 million.
- In 2023, 82% of breaches involved data stored in cloud environments, which were common targets for cyberattacks, often spanning multiple environments and resulting in above-average costs of $4.75 million.

Read more here.

Girl Scouts and Greater Than Tech Workshops

Due to popular demand, The Cyber Center of Excellence (CCOE) and the Girl Scouts of San Diego will be hosting two Cybersecurity Workshops this year. They will be expanding the program to include Junior–Ambassador Scouts (grades 4-12) with the opportunity to earn all three cyber badges and learn about cyber careers. The first in-person program will be hosted at Girl Scouts San Diego Headquarters on Saturday, May 4 from 9:00 – noon.

They are seeking corporate sponsors and 10 cyber pros to join their return volunteers to help the Girl Scouts with defined activities that teach basic cybersecurity hygiene and online security, as well as mentoring and career guidance. If you are interested in volunteering and/or joining Booz Allen, First Citizens Bank and Haiku as a sponsor, contact CCOE and they will provide you with all the details.

CCOE and National University are also partnering with Greater Than Tech (GTT) to expand last year's Cybersecurity Field Trip to a spring break Girl Meets Cyber Camp for 20 high schoolers on April 1-3. The curriculum will be similar to the Girl Scouts Workshops and they are looking for volunteers to lead 1-hour sessions. Please let Jasmine LeFlore and Lisa Easterly know if you or a member of your team might be interested in participating.

Cyber Ranges - Available Now

Step into the San Diego Regional Cyber Lab to bolster your cybersecurity skills! Our lab team has recently deployed two distinct ranges (1 in AWS and 1 on-premise) for your exploration. These ranges can be utilized for a variety of use cases, including CTF events, training/team-building activities, and more. In AWS, several Kali Linux virtual machines, integrated with Apache Guacamole, are now available for anyone interested in developing their own custom ranges remotely, without the need to visit our downtown lab space. As of right now, the ranges are in a fairly basic, undeveloped format and we are looking for community members who may be interested in building them out into a mature environment for their own teams and other regional cyber professionals to utilize.

Within our physical lab space in downtown San Diego, additional VMs are hosted within our on-premise architecture. The lab team is currently reconfiguring this environment utilizing Microsoft Hyper-V. If you are interested in contributing to the development of these ranges, or perhaps bringing your team in to test out larger scale efforts in a sandbox environment, please reach out to the Cyber Lab team at SDRCL@sandiego.gov.

For training purposes, our cyber ranges provide access to cyber tools such as Metasploit. Metasploit offers a comprehensive framework for simulating cyberattacks and enables simulated penetration testing scenarios ranging from reconnaissance to exploitation. Visitors can explore Metasploit in the range to enhance your skills and prepare for real-world cybersecurity challenges.

Cyberattack Disrupts US Prescription Market

The US prescription market was disrupted for nine days due to a ransomware attack by the AlphV crime group. This recent attack affected pharmacies, healthcare providers, and patients who faced challenges in filling life-saving prescriptions. UnitedHealth Group accused the AlphV gang of hacking its subsidiary, Optum, which manages customer payments and insurance claims. Optum disclosed the cyber security issue on February 21st and has been working to restore services since then. The attack underscores the threat of ransomware to critical parts of the US infrastructure. Change Healthcare, managed by Optum, processes billions of transactions related to healthcare operations. The outage disrupted various operations such as eligibility verifications, pharmacy operations, and claims payments.

Over 90 percent of US pharmacies had to change how they processed electronic claims due to the outage. The incident highlights the devastating effects ransomware can have on critical infrastructure, similar to the Colonial Pipeline closure caused by the Darkside group. AlphV has been a significant contributor to the ransomware menace, collecting over $300 million in ransoms and affecting operations in major establishments like casinos in Las Vegas including MGM. Read more about it here.

Canadian Authorities Respond to Cyber Attacks

Canadian authorities recently responded to cyber attacks targeting the Royal Canadian Mounted Police (RCMP) and Global Affairs Canada. The RCMP disclosed the attack on its network and is actively managing the situation in collaboration with other government agencies. While details of the attack remain undisclosed, efforts are underway to assess the breach and ensure accountability.

Despite the breach, the RCMP assures that its operations and the safety of Canadians remain unaffected, although its website experienced temporary downtime. The RCMP emphasizes its quick response and mitigation strategies as evidence of its commitment to detecting and preventing such threats. Meanwhile, the Office of the Privacy Commissioner (OPC) launched an investigation into a data breach resulting from a cyberattack on Global Affairs Canada's internal network. The breach compromised personal information, prompting the OPC to assess safeguards and ensure compliance with privacy regulations.

As investigations continue, it's uncertain if the cyber incidents at the RCMP and Global Affairs Canada are connected. Canadian authorities are expected to provide further updates as the situation unfolds.

Biden is boosting cybersecurity at US ports where online attacks can be more ravaging than storms

President Biden has taken steps to improve cybersecurity at the nation's ports by signing an executive order and establishing a new federal rule. National Security official Anne Neuberger emphasizes the importance of these decisions, citing the damage to our ports and economy that these attacks can cause.

Nationwide, ports employ around 31 million people and contribute $5.4 trillion to the economy. Cyberattacks, like the one on the Colonial Pipeline, can cause big problems for ports. These new rules aim to prevent similar attacks from happening in the future. As part of this effort, the federal government wants port operators to report any cyberattacks they encounter, with the Coast Guard being made available for future cyberattacks. For more information, click here.

City of Oakley Investigates Ransomware Attack

In February, the City of Oakley experienced a ransomware attack, prompting a state of emergency declaration by City Manager Josh McMurray. The City's IT Division swiftly responded, working with law enforcement and cybersecurity experts to address the issue. Activation of the Emergency Operations Center expedited resource procurement, with all employees placed on standby. While emergency services remained intact, non-emergency functions, like code enforcement, saw delays. Despite some services returning to normal by February 26, the city continues to provide updates as the investigation progresses. Read more here.

Spring Cyber Solutions Fest 2024

Don't miss the Spring Cyber Solutions Fest 2024, a FREE virtual event from Wednesday, April 17th to Friday, April 19th, where attendees can earn valuable CPE credits (6+ per track) while exploring the latest cybersecurity solutions, technologies, and techniques.

The first inaugural SANS Emerging Technologies Track on April 17th, this event features cutting-edge innovations and practical solutions to fortify network defenses. Led by industry experts, this track promises game-changing insights, engaging demos, and invaluable networking opportunities. Secure your spot today right here!

BSides San Diego Hacker Spring Break 2024

BSides San Diego is returning for a one day extravaganza this March 30th, 2024 at San Diego State University. They are coming back in full force next year with enthusiastic talks, engaging trainings, extraordinary giveaways, hacker jeopardy, and enraging villages.

BSides SD is an independent, community-driven information security conference that aims to bring together professionals, enthusiasts, and anyone interested in cybersecurity. These conferences typically feature presentations, workshops, and discussions related to cybersecurity.

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

CCOE Spring Soiree

The Cyber Center of Excellence (CCOE) invites their members and partners for networking and street tacos at CCOE's upcoming spring reception.

Mingle with San Diego's cybersecurity leaders and learn more about their programs and offerings aimed at growing the regional cyber economy and creating a more secure digital community for all.

The event will be help on Wednesday, March 27th from 5:00-7:00pm. If you are interested in attending, click here for additional details.

Free Web App Scanning

Interested in free web app scans? CISA offers this service at no cost. Click here for more information.

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