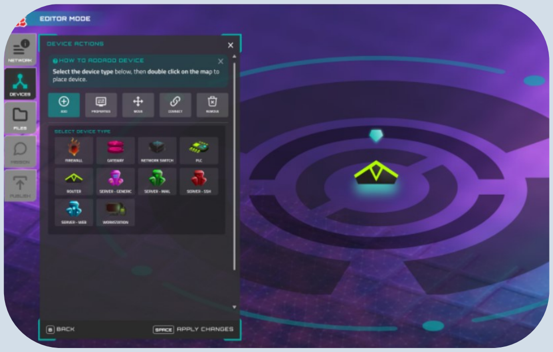
San Diego Regional Cyber Lab

Haiku Forge

Coming soon to a PC near you! Our partner, the Cyber Center of Excellence (CCOE) provides a large number of licenses for our partners to experience the benefits of Haiku.

Haiku Forge is a new tool that allows a non-technical user to create their very own cyber training course. It runs an interface using a drag-and-drop method where you can picture an immersive arena model.



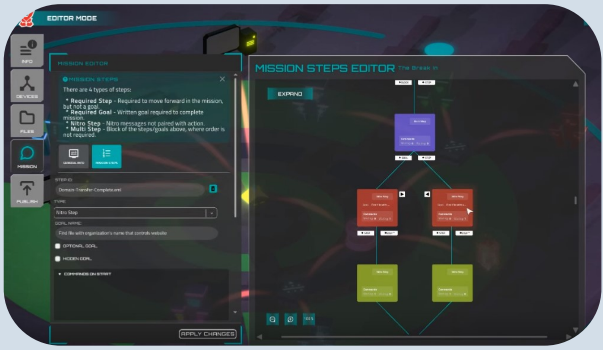
Select the device type below, then double click on the map to place device.

Pictured above: Menu to generate custom sandboxed training labs.

Upcoming Events:

- *Technical Steering Committee Call - 8/17*
- *Executive Steering Committee Call - 8/31*
- *Cybersecurity Economic Impact and Workforce Study - 10/3*

In This Issue



There are 4 types of steps:

- **Required Step** - Required to move forward in the mission, but not a goal.
- **Required Goal** - Written goal required to complete mission.
- **Nitro Step** - Nitro messages not paired with action.
- **Multi Step** - Block of the steps/goals above, where order is not required.

STEP ID: Domain-Transfer-Complete.xml

TYPE: Nitro Step

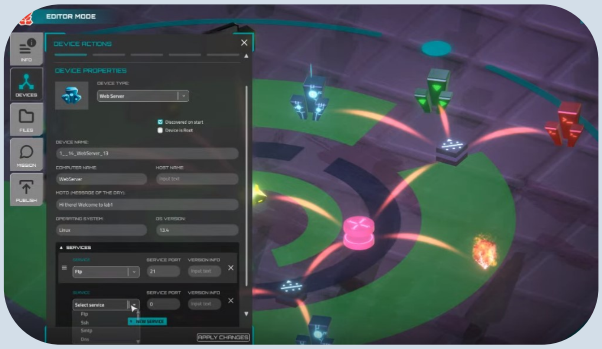
GOAL NAME: Find file with organization's name that controls website

Pictured above: Mission Steps Editor controls the flow of the experience for the player/student.

Haiku Forge can help teach...

- a specific cyber or networking tool
- an offensive, defensive or forensic cyber skill
- a process or procedure

all without prior knowledge of coding. This new tool allows the end user to build their own immersive game experiences to train their organization. Forge includes how to mitigate newly discovered exploits or other scenarios can be created and shared among other Forge users if made public.



DEVICE TYPE: Web Server

☑ Discovered on start

☐ Device is Root

DEVICE NAME: 1__14_WebServer_13

COMPUTER NAME: WebServer

HOST NAME: Input text

MOTD (MESSAGE OF THE DAY): Hi there! Welcome to lab1

OPERATING SYSTEM: Linux

OS VERSION: 13.4

SERVICE	SERVICE PORT	VERSION INFO
Ftp	21	Input text
Select service	0	Input text

Pictured above: Drag-and-drop network environment where simulations take place. Granular controls are provided for defining each endpoint in the network.

SDRCL Issue #4 - August 2023

White House to roll out array of cyber initiatives to bolster K-12 defenses

- The Federal Communications Commission will create a pilot program to provide up to $200 million over three years to strengthen cyber defenses in K-12 schools and libraries.

- The Education Department will establish a Government Coordinating Council (GCC) to act as a conduit for collaborating between federal agencies and education organizations.

- The Cybersecurity and Infrastructure Security Agency (CISA) will provide training to 300 new K-12 entities, hold monthly digital exercises and issue updated guidance for institutions.

- Amazon Web Services will offer a $20 million K-12 cyber grant program to all school districts, as well as free security training and incident response assistance to entities that come under digital assault.

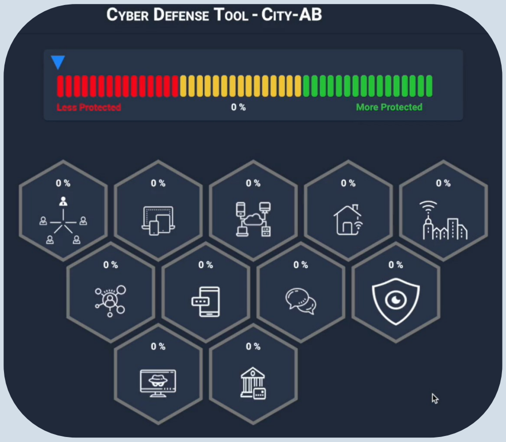
- Cloudflare will offer a suite of free Zero Trust tools to public school districts with under 2,500 students.

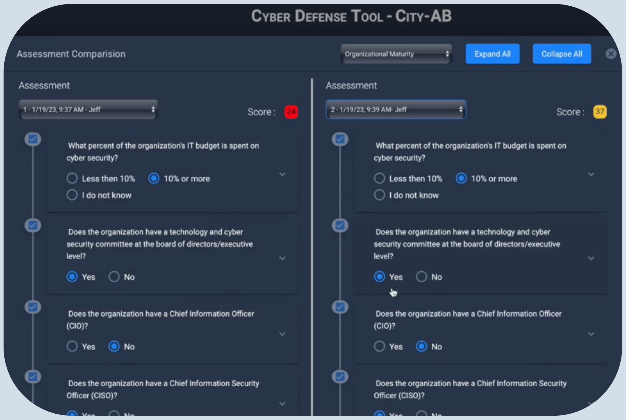
- Google will release an updated guidebook for schools on best security practices.

More info here.

Cyber Defense Tool

The Cyber Defense Tool, powered by CyberWA, allows an organization to perform a high-level assessment of its overall cybersecurity capabilities and preparedness. The assessment enables the organization to focus on key areas that will improve their cybersecurity posture and also aids in the identification and prioritization of risks that could be exploited in a successful cyberattack.




Cyber Defense Tool - City-AB

Assessment Comparision

Organizational Maturity | Expand All | Collapse All

Assessment

1 - 1/19/23, 9:37 AM - Jeff

Score : 24

What percent of the organization's IT budget is spent on cyber security?

○ Less then 10% ● 10% or more
○ I do not know

Does the organization have a technology and cyber security committee at the board of directors/executive level?

● Yes ○ No

Does the organization have a Chief Information Officer (CIO)?

○ Yes ● No

Does the organization have a Chief Information Security Officer (CISO)?

Assessment

2 - 1/19/23, 9:39 AM- Jeff

Score : 37

What percent of the organization's IT budget is spent on cyber security?

○ Less then 10% ● 10% or more
○ I do not know

Does the organization have a technology and cyber security committee at the board of directors/executive level?

● Yes ○ No

Does the organization have a Chief Information Officer (CIO)?

○ Yes ● No

Does the organization have a Chief Information Security Officer (CISO)?

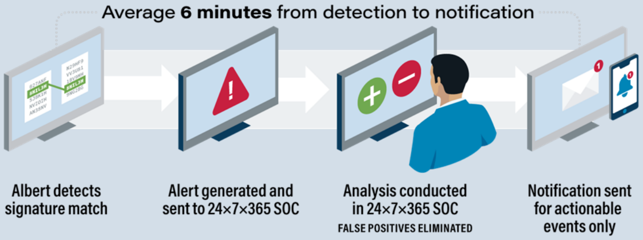
The Cyber Defense Tool is divided into eleven core focus areas: Cyber Maturity, Computing Devices, Smart City, Smart Devices, Network Infrastructure, Authentication & Access, Communications, Digital Footprint, Financial, Monitoring and Response and Threats & Compromises. More info here.

CIS Albert Network Monitoring

Albert Network Monitoring and Management is as titled, a “24x7x365 managed and monitored Intrusion Detection System (IDS) built to detect SLTT-specific threats.” It can monitor malicious traffic, serve as a second line of defense, offers 24x7x365 management and support, free incident response, serves as an extension of your security team, and provide NetFlow records. NetFlow records include a summary of a data exchange between two systems with the following characteristics: Source IP; Destination IP; Source port; Destination port; TCP Flags; Number of bytes of traffic sent and received; Timestamp information.

The Basic Life Cycle of an Albert Event

A comprehensive monthly activity report is made available to you. It summarizes the malicious activity identified by each sensor deployed in your organization’s environment. These reports provide details for all actionable alerts for the previous month, statistics on data such as total alerts generated vs. actionable alerts, as well as a review of the total volume of monitored traffic. A presentation for Albert Sensors will be provided by the Center of Internet Security (CIS) during the Cyber Lab’s Technical Stakeholder Committee call on August 17th. More info here.


Average **6 minutes** from detection to notification
Albert detects signature match
Alert generated and sent to 24×7×365 SOC
Analysis conducted in 24×7×365 SOC
FALSE POSITIVES ELIMINATED
Notification sent for actionable events only

With the use of Generative AI accelerating, is your organization ready and is your cybersecurity posture keeping pace?

Joe Rohner, vice president of the Artificial Intelligence in Booz Allen, helps defense clients apply AI and advanced analytics to yield better mission outcomes through AI adoption and strategy, systems and more. In this quarterly newsletter, Rohner adds insight for protection and prevention for known risks to understand the misuse of AI tools.

As AI dominates the news cycle with the advances and availability of Generative AI tools, it's important for an organization to pause and consider the implications, including cybersecurity, these tools will have on their organization.

Generative AI has become ubiquitous and provides the opportunity for an open dialogue on how organizations should prepare for using or operating with AI.

Here are a few basic steps:

Workforce Education: Many AI issues can be avoided by proactively training employees on the fundamentals of key AI concepts. Recognizing AI will have broad implications on your entire workforce, it is important for teams to understand how AI programs work and produce outputs. While some organizations are turning to publicly available AI courses offered by universities or big tech companies, others are creating their own programs or bringing experts in-house. Regardless of your approach, the adage, "knowledge is power", truly applies here.

Tool Understanding: With one online search, you'll quickly find very public stories of intellectual property and private data being exposed at great cost to organizations. Many of which could have been avoided through tool understanding. Fundamental questions such as, "Are you using an AI tool that you purchased? Does it use open-source code? Is it a third-party hosted tool?" can all be game changers. It's imperative for employees to be able to answer these questions and subsequently understand the different terms, conditions, and data policies for each. For example, some third-party Generative AI models will retain the rights to your input (e.g. documents, source code, etc.), using the data to fine-tune the tool. Therefore, clear guidance and guardrails around what employees can input or submit into various AI's tools can help thwart this inadvertent loss of data rights and likely security of your organization.

Practice Human-Machine Best Practices: Trust but verify. AI is only as good as the data used to train the model. In the case of Generative AI, it's only as good as the prompt used to generate the outcome. Using AI to generate a response is the first step, but the next step is validation and verification by a human. This leads to more accurate final inputs that can truly provide value to an organization.

In addition to the basic steps above, there are a set of common cybersecurity concerns emerging around Generative AI. Internal concerns include trust boundaries, data management risk, and inherent model risks like hallucinations. Additionally, external threats for Generative AI include social engineering and advanced malware. Last but not least, while the prior focused on concerns, there are opportunities for using Generative AI to augment cyber defensive capabilities that include advanced threat detection, automation of defense mechanisms, and enhanced incident response, just to name a few.

AI is finally having its moment and it will impact the way we work. Be informed, ask questions, embrace it as a tool, and use it to transform your organizations.

Strengthening Cybersecurity: Can The SEC's Landmark New Rules Be Enforced?

This past June, Microsoft identified a security breach with many companies and organizations having important data exposed. As a result, the Securities and Exchange Commission (SEC) have brought out a new requirement for cyber breach disclosure that will change the way American institutions universally operate.

Protecting information before an attack even happens is guaranteed to be costly, but the recovery of that same information following an attack will cost even more. You can see that in a new report published by IBM, researchers found that in order to rectify the impact of a breach organizations spend an average of $4.5 million per breach, which is a 15% increase over the past three years.

While many companies require a third-party authentication app, some question whether it provides sufficient security as companies with third-party apps were part of a recent data breach. This comes recently when Microsoft allowed Azure AD tokens to be forged by a China-based threat with an acquired MSA consumer signing key.

City College Cyber Security Programs

On January 23rd, 2023 the California Community Colleges Board of Governors affirmed approval of San Diego City College's Baccalaureate Degree Program (BDP) in Cyber Defense and Analysis, helping to further train the state's workforce and giving more Californians an opportunity to earn a four-year degree from a community college. The program expansion (AB 927) will benefit California by awarding more advanced degrees in high-demand workforce industries and putting Californians on a path toward employment in their field of study and in industries of greatest need for the state's economy.

Estimated Cost of Enrollment (CA Residents)

	Required Units	Cost Per Unit	Estimated Total
CSUGE (IGETC)	*36 (34)	$46	$1,656 ($1,564)
AS - Cybersecurity	*32	$46	$1,472
BS – Cyber Defense and Analysis	*54	$130	$7,020
Full Program	*122 (120)		$10,148 ($10,056)

*Some students may need additional units to meet general education, associate degree, and/or baccalaureate degree program requirements.

Dangers of New AI: Worm GPT

While ChatGPT is a useful tool, it was only a matter of time before it fell in the hands of online predators. SlashNext recently gained access to a tool known as "WormGPT" in a dark web online forum. WormGPT presents itself as an alternative for black hats to take advantage of users through malicious activities in AI form.

WormGPT boasts a range of features, including unlimited character support, chat memory retention, and code formatting capabilities. This new AI tool has the ability to pressure workers into paying monetarily with fraudulent emails. The use of stringent email verification is recommended to ensure the best protection of your users' data. More info **here**.

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

Save-The-Date

Cyber Center of Excellence (CCOE) and San Diego Regional EDC are excited to soon release the 5th biennial San Diego Cybersecurity Industry Economic Impact and Workforce Study. The data serves as a benchmark for industry growth, identifies new trends and tells our region's cyber story.

When
Tuesday, Oct 3, 2023
8:30-10:30am PDT

Where
Qualcomm
6455 Lusk Blvd
San Diego, CA 92121

RESERVE YOUR SPOT

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