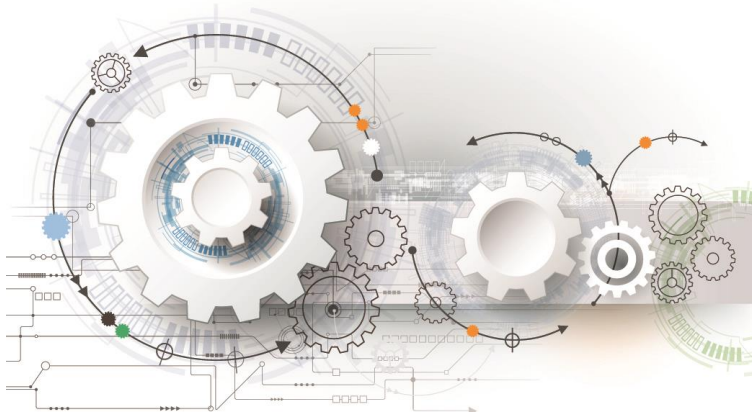


SPORT & CYBER LAB: Use Cases in Critical Infrastructure & Community Cyber Capacity Building



CYBER IS A TEAM SPORT

Cyber Capacity Building: Through Sport & For Sport

*Introducing for Summer 2020: COVID-19 Cyber
Threat Hunting & Disinformation Collection*

CrowdWatch

*A Cohort of Professional
and Apprentice Cyber
Analysts that collaborate
with CRI Sports-ISA0 pop-
up SOC operations, and
other outsourced
opportunities, to gain
valuable experience for
jobs as cyber threat
analysts.*

Powered by:

Reprivata™

&

CYBER
THREAT INTELLIGENCE

"THE ELIXIR OF SPORT " – RALLYING ITS POWER TO SPUR CAPACITY-BUILDING

SEEKING PARTNERS IN PROFILING CORONAVIRUS THREAT ACTORS FOR FUTURE USE CASES

The objective is to detect, correlate and profile threat actors during the COVID-19 pandemic for later use during Elections and other use cases. Sports-ISAO pop-up SOC operations has previously observed threat actors using sport as a proving ground for attack strategies and new malware that is later used in other attacks. Borrowing from past experience detecting these new attacks, CRI intends to use the proliferation of cyberattacks and disinformation surrounding this pandemic as a collection rich environment (i.e., a **"Hunting Season"**). This collaboration is being created by the Cyber Resilience Institute (CRI), a Cooperative Research and Development Agreement (CRADA) holder and member of the DHS information sharing community and is part of our **CrowdWatch** operations. Training in advance of live collection operations is offered through the **Watch** cyber threat training program. See <http://cyberresilienceinstitute.org/c-watch-2020/>.

Sport-themed training and **CrowdWatch** operations will return after the pandemic, with plans to return to support cyber threat detection and protection activities during **Tokyo 2021 Summer Olympics**. In recent years, CRI has launched operations in support of the 2016 Rio Summer Olympics, 2018 PyeongChang Winter Olympics, and two FIFA World Cups. Reporting during **CrowdWatch** operations is into the Joint Operations Center inside the US Embassy in the Host Country.



Additional **CrowdWatch** operations will commence after this COVID-19 scenario, with more opportunities to collaborate in cyber threat collection and analysis, and to grow and mature the virtual Sport & Cyber Lab that Sports-ISAO has established to help students gain hands-on experience and qualify for career opportunities in the cybersecurity and cyber intelligence fields. Another objective is to create jobs for **CrowdWatch** members.

Who We Are and What We Do

Sports-ISAO is a program office of CRI, a 501(c)(3) not-for-profit entity. CRI, through Sports-ISAO, volunteered its professional and **CrowdWatch** resources to provide daily cyber threat intelligence to US Government security operations in the Joint Operations Center (JOC) in Seoul during the 2018 Winter Olympics, in the Paris Embassy during the 2019 Women's World Cup in France, and during the 2018 FIFA World Cup in Russia. This is an ongoing relationship with the US Department of State OSAC Program (Overseas Advisory Council) - <https://www.osac.gov/>.

Our Training and Crowdsourced Threat Hunting Components and Stages

This figure depicts multiple stages and use cases for the training and pop-up SOC operations.



USE CASES & CHARACTERIZATION OF OUR PROGRAMS



CRI has a mission of promoting the buildout of cyber capacity at community levels, as a strategy to address the Down-Market Gap¹. The C-Watch training program is one element of this community cyber capacity building initiative.

CrowdWatch is another, along with university student club affiliation, so that the community begins to develop a workforce to support information sharing, cyber threat intelligence collection and other services, while the students develop critical experience in the field. These programs fit within an umbrella national initiative for helping communities develop their community initiative: the Cyber on Main initiative. www.cyberonmain.org. Cyber on Main provides the uniform framework and affiliation to enable national adoption and action. Additional programs will emerge through a platform, the C-Market www.c-market.us

C-Watch provides the starting point for activity, because training is where a career in cyber threat intelligence and information sharing begins. Known as an “ISAO Operations Course”, C-Watch provides students with foundational knowledge as well as tool and platform training to support intelligence collection, analysis and reporting. C-Watch course students receive experiential learning during the Capstone, which is a Live ISAO operation (a Pop-up SOC) with distributed hunters and analysts who participate during a major sports event (this year will be a COVID-19 collection scenario).

To date, students from over 30 Universities across the U.S. have participated in the C-Watch training. Below are logos depicting the of universities whose students participated in Sports-ISAO Pop-Up SOC operations, with a testimonial further below.



More information about past efforts, including both the men’s and women’s FIFA World Cups, can be found at these sites:

<http://cyberresilienceinstitute.org/c-watch-2020/>

<https://sports-isao.org>

<https://c-market.us/site/index.php/home/c-watch/c-watch-course/>

¹ The Down Market Gap refers to the lack of appetite for cyber spend below the enterprise market, and the resulting low level of cyber hygiene in communities across the country, particularly among small and mid-sized businesses. This gap presents systemic risk because of the interconnectivity and interdependencies of all Internet users, on-line financial transactions and supply chain risks.

CrowdWatch

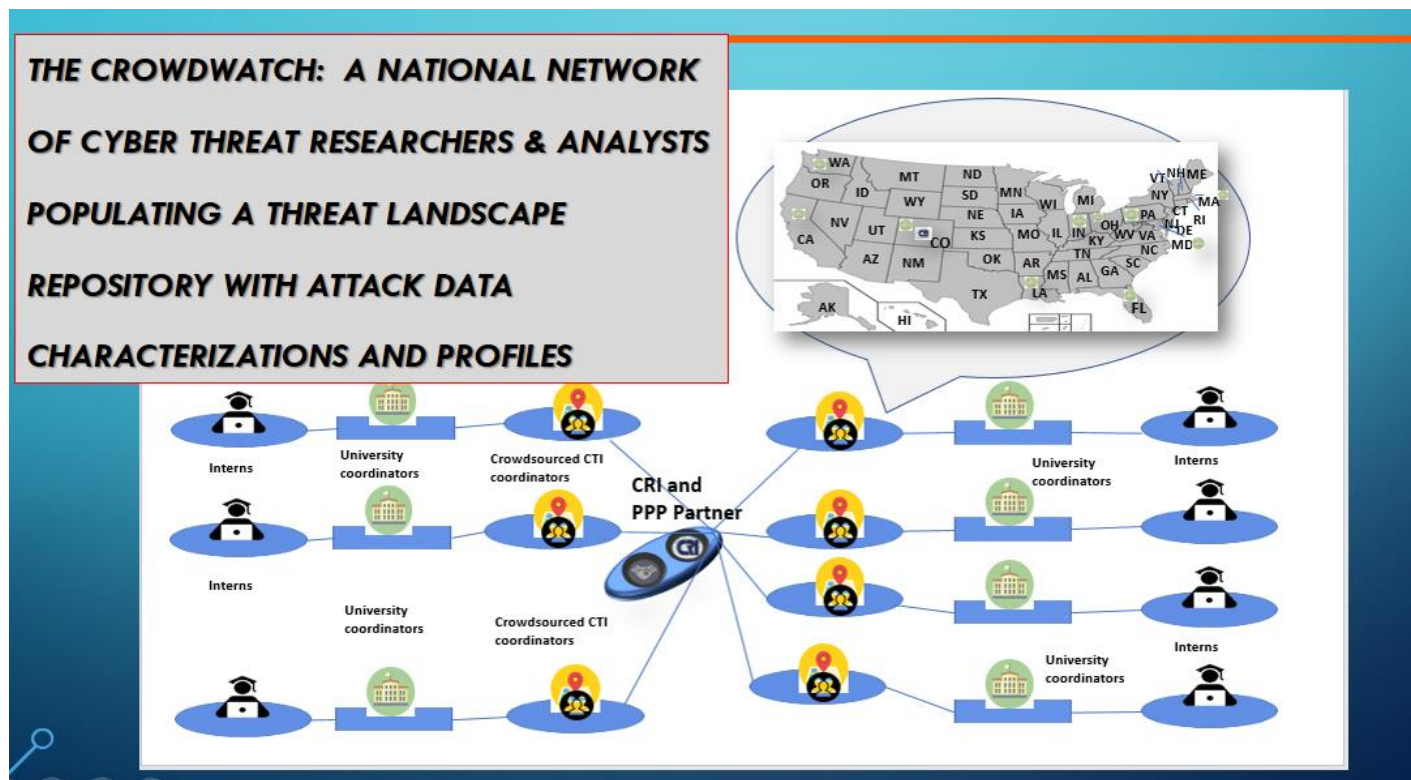
Once graduated from the **CrowdWatch** program, eligible candidates enter the **CrowdWatch**, our national network of apprentice-hunters whom we make available for staff augmentation and outsourced analytics. Two of our partners **Reprivata** and **CYBER THREAT INTELLIGENCE** are engaged in creating compensated work for **CrowdWatch** members.

Our goal is to place this talented group in jobs, and to provide compensation through **CrowdWatch** while they gain valuable experience. Many of these members are current university students, and compensation is helpful for reducing their college debt load (e.g., in lieu of college Work Study).

And, they represent a talent pool that offers cost savings to organizations needing analytic support. Accordingly, through this program, CRI is also seeking financial sponsors and contract-based opportunities. Funds will be used to help underwrite student scholarships, summer internships, projects and activities, compensation during collection operations, and for job placement.

CRI seeks to provide regular support to partners and customers from the **CrowdWatch**, along with our professional analysts, with cyber threat intelligence and information sharing support, such as:

- Surge support via Pop-Up SOC operations
- Staff augmentation
- Outsourced analytics
- Cyber Threat Intelligence training
- ISAO establishment support, consulting, or systematic engagement of ISAO support



Partners may contact CRI to seek participation or sponsorship. **CRI encourages corporate citizenship especially during the economic downturn associated with the pandemic, as so many students are losing jobs and internships.** As a 501(c)(3), charitable donations (e.g., to support student scholarships) receive favorable tax treatment. CRI will also continue to partner with universities and students, as well as with communities and ISACs and ISAOs. **And, partners looking for talent should also contact us.**

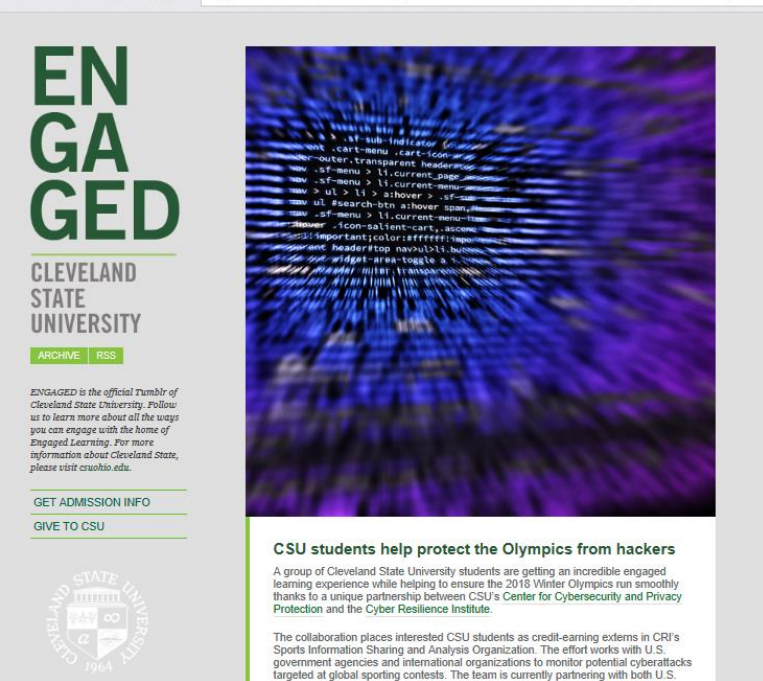
University and Community Partnerships:

We are especially interested in extending our partnership model to universities and community groups across the country. See what existing partners have said about the program, and a student testimonial here →.

"I have obtained invaluable skills in cyber threat intelligence during my internship ...during the summer of 2017. The mentors were available to help train and guide me through the process of learning how to threat hunt, and gave me continuous feedback. I am glad I had the chance to learn these skills so I can focus on pursuing a career in this field."

-- O. Hitt, Student Intern

← → ↺ 🏠 ⓘ clevelandstate.tumblr.com/post/171202207292/csu-students-help-protect-the-olympics



Center for Cybersecurity and Privacy Protection at the Cleveland-Marshall College of Law


"We work with a team of analysts to hunt for potential cyber threats and share that information with our U.S. and international partners to reduce the potential for attacks and to increase understanding of hacker profiles and activities" notes **Christopher Kolezynski**, a law student at CSU's [Cleveland-Marshall College of Law](#). (Note: Chris now has a job in the cybersecurity field)

"CRI recruits students from across the country and organizes them and a team of mentor-analysts into a crowdsourced operation to support cyber threat analytics. For the Olympics, the team is engaging in the collection, sharing and analysis of threat intelligence related to the event. The Institute previously supported cybersecurity activities for the 2017 World Track and Field Championships and will

also be assisting operations for the 2018 World Cup."

<http://clevelandstate.tumblr.com/post/171202207292/csu-students-help-protect-the-olympics-from-hackers>

Student Scholarships:

Through our generous sponsors, students may qualify for scholarship funds. Employers need cyber analysts! Our goal is to make -Watch free to all students, underwritten by employers who get access to talent.

Benefits and Outcomes of Support:

- | | |
|---|--|
| <input checked="" type="checkbox"/> Help to close the talent gap | <input checked="" type="checkbox"/> Access to top talent |
| <input checked="" type="checkbox"/> Brand benefits from social benefit action | <input checked="" type="checkbox"/> Recognition at events ² |
| <input checked="" type="checkbox"/> Recognition on marketing materials | <input checked="" type="checkbox"/> Tax benefits from contributions |
| <input checked="" type="checkbox"/> Access to university partners | <input checked="" type="checkbox"/> Access to threat intelligence |

CALL TO ACTION !!!

CRI and Sports-ISA0 have shown that the magnetism of sport is powerful for rallying interest and participation in cyber activities and capacity building. We have also observed how attractive our students are to employers.

² For example, conferences and events are conducted by the leadership team (e.g., CyberUSA Conference).

PROGRAM LEADERSHIP:



Doug DePeppe specializes in private-public partnerships in Community Cyber, and reducing cyber risk as a cyberlaw attorney. He has designed and instructed cyber courses at multiple universities, and engages

in speaking globally on cybersecurity, cyberlaw and private-public partnerships. He has published pieces and articles on the subjects, including in BNA and in Forbes. In addition to his cyberlaw practice at **eosedge** Legal, a firm he founded, he is Board President of the Cyber Resilience Institute, Co-Founder of the Sports-ISAO, and a partner in cyber intelligence firm, CTIN. Mr. DePeppe's credentials include:

- White House 60-day Cyberspace Policy Review
- Subject Matter Expert to White House-directed Electricity Sector Cybersecurity Risk Management Maturity Model
- Govt Relations WG Chair, ISAO Standards Organization
- Chair, RC3 Cyber Working Group
- Adjunct Professor, UMUC Cybersecurity Masters
- Retired, US Army JAG Corps
- LLM, George Washington University Law School



Jane Ginn has over 30 years of international business experience in engineering consulting, information technology, and cyber security threat intelligence. She has expertise in cybersecurity training program curriculum design, network design using defense-in-

depth concepts, red/blue team design and execution, cybersecurity exercise development, vendor product evaluation and ISAO member on-boarding, threat analysis and risk assessment. She is a Principal at cyber intelligence firm, CTIN, Board Treasurer at Cyber Resilience Institute, and Co-Founder of the Sports-ISAO. Ms. Ginn's credentials include:

- Co-Secretary, OASIS Cyber Threat Intelligence – Technical Committee (STIX/TAXII standards)
- Technical Adviser, European Network Information & Security Agency (ENISA) Threat Landscape Stakeholders' Group
- Adviser to five Commerce Secretaries (International Trade, 1994 – 2001)
- MS, Information Assurance, Norwich University
- Masters, Environmental Science & Regional Planning (MRP), Washington State University



Nick Sturgeon has worked in Information Technology for over 15 years, with 10 years in Cybersecurity, nine years in Law Enforcement, and 10 years in State Government. Nick has extensive experience in incident response, data governance,

digital investigations, digital media recovery, criminal investigations, criminal law, end point protection, network & log analysis, vulnerability management, security operations, incident management, academic instructor, project management, and managed security services. Throughout his career he has supported multiple industries and sectors including, State\Local\Tribal\Territorial (SLTT) Governments, academia, healthcare, Information Technology and manufacturing. As well, Nick holds multiple board appointments on.

- Adjunct Professor, University of Southern Indiana
- Senior Information Security Instructor, University of Texas San Antonio
- ITIL Foundations v3 Certified
- Master of Science Purdue University
- Bachelor of Science Indiana State University



Stephen Campbell specializes in researching and defending against cyber and physical threats from non-state actors. As founder of Non-State Threat Intelligence and strategic advisor to **eosedge** Legal, he encourages clients to take an intelligence-led approach

toward assessing and mitigating risk. This involves sizing up a client's assets, their perceived value to attackers and their unique attack surface. It requires a current appreciation of the motivations of attackers and their ever-changing tactics, techniques and procedures. And it demands up-to-date insights into evolving security technologies and best practices. Mr. Campbell's credentials include:

- Master of Arts in Law and Diplomacy, The Fletcher School, Tufts University
- Certified Information Systems Security Professional
- Research Advisor to Professor Richard H. Shultz, expert on armed groups, 2009-2014
- B.Sc. (Hons) Physics, University of Glasgow
- Graduate curriculum development on intelligence and asymmetric warfare

CONTACT INFORMATION

Doug DePeppe
Board President, CRI
719.357.8025
Doug.depeppe@cyberresilienceinstitute.org

Jane Ginn
Board Secretary, CRI
928.399.0509
rjg@sports-isao.org