CySim Overview

What is CySim?

CySim, a proposed cutting-edge cybersports complex, offers a unique platform for organizations to enhance their cybersecurity readiness through scenario-based exercises. Drawing inspiration from the world of sports, CySim enables teams to practice actual plays using scrimmages, allowing them to face numerous scenarios and prepare for the worst.

Planned to be situated in the ISU research park, CySim is a physical space designed to replicate various corporate environments and situations that users may encounter in the real working world. It features dedicated areas such as a fully operating Security Operations Center (SOC), a space for the red team (attackers), an office environment with a bullpen, offices, conference rooms, and sections for law enforcement, users, and employees. Additionally, CySim includes an observation room, server room, and areas for remote interaction, catering to scenarios involving working from home or distance learning.

At the core of CySim is a cyber platform powered by configurable software tools and servers. This platform offers the following capabilities:

1. Utilization of modern security tools for both defensive and offensive operations, allowing organizations to test and improve their cybersecurity defenses.
2. Facilitation of interaction between technical and non-technical staff, promoting collaboration and effective communication during cyber threat simulations.
3. Creation of interdisciplinary teams that can work together to navigate and mitigate various cyber threats. This interdisciplinary approach ensures a holistic understanding of cybersecurity and promotes comprehensive defense strategies.
4. Sector-based scenarios tailored to industry partners enabling organizations to simulate cyber threats specific to their sector, such as the financial sector, critical infrastructure, agriculture, manufacturing, and more.
5. Integration with various cyber testbeds, providing access to diverse environments and expanding the range of scenarios that can be simulated.

Roles within the CySim exercises encompass a wide range of participants, including defenders (blue team), attackers (red team), users, organizational members, evaluators, external organizations (such as the press and law enforcement), and support staff. CySim's dedicated personnel can assume these roles, allowing organizations to focus on the exercise itself.

The CySim exercise types are tailored to specific situations, offering organizations the flexibility to practice in scenarios that closely resemble their own environments. Through virtualization, CySim can configure its physical space to simulate diverse settings, ensuring a realistic experience for participants. Furthermore, CySim supports scenario-based exercises for educational purposes, catering to classes, students, and educators who wish to enhance their understanding and response to cyber threats. It also provides an avenue for interdisciplinary teams to collaborate and practice cyber threat mitigation strategies effectively.

Just like a sports complex, CySim allows for the setup and execution of various cyber games, promoting engagement and skill-building within the cybersecurity realm. It also serves as a hub for case study-type classes involving students from multiple disciplines, fostering a holistic approach to cybersecurity education.

In summary, CySim offers a state-of-the-art cybersports complex that combines physical and virtual elements to enable organizations to practice cybersecurity readiness. By engaging in scenario-based exercises, teams can enhance their skills, test their defenses, and prepare for real-world cyber threats in a realistic and immersive environment.

CySim use cases

Scenario-based exercises are a fundamental component of CySim, providing organizations with immersive experiences that involve multiple units within their organization. These exercises can be designed to support any aspect of training needed by your organization:

1. **Specific Scenarios:** CySim exercises focus on particular scenarios tailored to meet the needs of organizations. CySim offers a range of prebuilt scenarios based on different sectors, such as finance, critical infrastructure, agriculture, manufacturing, and more. These scenarios simulate real-world cyber threats and challenges, allowing participants to practice their responses and improve their cybersecurity readiness. Alternatively, organizations can customize scenarios to address their requirements, ensuring the exercises align closely with their unique environments and concerns.
2. **Involvement of Multiple Units:** Scenario-based exercises in CySim encourage the participation of various units within an organization. Large organizations can bring in department heads, management teams, and different units to collectively collaborate and respond to simulated cyber threats. This approach fosters cross-functional cooperation, strengthens coordination, and enhances the overall cybersecurity capabilities of the organization. On the other hand, smaller organizations have the opportunity to involve their entire staff, ensuring comprehensive engagement and awareness across the organization.
3. **Role Flexibility:** The CySim staff can assume different roles during the exercises, including blue (defenders), red (attackers), or external groups. This flexibility allows organizations to focus on the exercises while CySim personnel actively participate as adversaries or external entities, such as the press or law enforcement. By leveraging the expertise of the CySim staff, organizations can ensure dynamic and challenging exercises that push their cybersecurity teams to their limits.

In addition to scenario-based exercises, CySim offers various training, workforce development, and cybersecurity awareness exercises, catering to different educational levels:

1. **Blue Training:** Blue training exercises focus on enhancing the skills and capabilities of defenders within an organization. These exercises can cover various topics, from incident response and threat hunting to vulnerability management and security operations. By participating in blue training exercises, organizations can bolster the technical expertise of their cybersecurity teams and improve their overall defensive posture.
2. **Red vs. Blue Awareness Exercises (Adversarial Thinking**): Red vs. Blue exercises foster adversarial thinking and simulate real-world attack scenarios. These exercises involve both red team (attackers) and blue team (defenders) participants, encouraging them to think like adversaries and defenders, respectively. Red vs. Blue exercises helps organizations develop a proactive mindset, strengthen their incident response capabilities, and identify vulnerabilities within their systems and processes.
3. **Educational Exercises:** CySim supports educational exercises at various levels of academia. College-level exercises engage students pursuing higher education in

cybersecurity-related fields, allowing them to apply their knowledge and skills in realistic scenarios. High schools and community colleges can also benefit from CySim's educational exercises, which introduce cybersecurity concepts and practices to students at an earlier stage, fostering interest and awareness in this critical field.

By providing a comprehensive range of scenario-based exercises and educational opportunities, CySim empowers organizations and educational institutions to enhance their cybersecurity preparedness, develop workforce capabilities, and promote cybersecurity awareness at all levels.

Sample Exercises

Short videos have been created to showcase the uses of CySim in various scenarios and highlight its effectiveness and benefits. Here are descriptions of the videos for each scenario:

1. School District: Video Title: "Securing Education: Enhancing Cybersecurity Readiness in School Districts with CySim"

Description: This video focuses on a school district utilizing CySim to enhance its cybersecurity readiness. It starts with an introduction to the challenges faced by educational institutions in safeguarding student data and digital infrastructure. The video then demonstrates how CySim's scenario-based exercises are tailored to the specific needs of school districts, covering topics such as student data protection, incident response, and securing remote learning environments. It showcases teachers, IT staff, and administrators participating in the exercises, highlighting the collaborative nature of the training and how CySim fosters a proactive and resilient cybersecurity culture in schools.

2. Hospital: Video Title: "Protecting Patient Privacy: Strengthening Cybersecurity in Healthcare with CySim"

Description: This video highlights how CySim empowers hospitals to address the unique cybersecurity challenges they face. It showcases medical staff, IT professionals, and administrators engaging in scenario-based exercises within CySim's simulated hospital environment. The video illustrates scenarios like ransomware attacks, data breaches, and ensuring the secure operation of critical medical devices. It emphasizes the importance of interdisciplinary teamwork and demonstrates how CySim helps healthcare organizations strengthen their cybersecurity practices, protect patient privacy, and ensure uninterrupted healthcare services.

3. Local Government: Video Title: "Securing the Community: Enhancing Cybersecurity in Local Government with CySim"

Description: This video portrays how CySim assists local government entities in fortifying their cybersecurity defenses. It features government officials, IT teams, and administrators participating in scenario-based exercises in a simulated local government environment within CySim. The video highlights challenges specific to local governments, such as protecting sensitive citizen data, securing public infrastructure, and defending against cyber threats targeting government systems. It demonstrates how CySim enables collaboration among different departments and equips local governments with the skills and knowledge needed to mitigate cyber risks effectively.

4. Manufacturing: Video Title: "Building a Secure Future: Strengthening Cybersecurity in Manufacturing with CySim"

Description: This video showcases how CySim aids manufacturing organizations in safeguarding their critical operations from cyber threats. It depicts scenarios within a simulated manufacturing environment, featuring plant managers, engineers, and IT personnel participating in CySim's exercises. The video emphasizes the significance of securing manufacturing control systems, protecting intellectual property, and ensuring supply chain resilience. It demonstrates how CySim's industry-specific scenarios and practical training enable manufacturing organizations to strengthen their cyber defenses, detect vulnerabilities, and respond effectively to potential cyber incidents.

5. Municipal Utility: Video Title: "Powering Resilience: Enhancing Cybersecurity in Municipal Utilities with CySim"

Description: This video focuses on how CySim supports municipal utilities in protecting critical infrastructure from cyber attacks. It showcases scenarios involving power grids, water treatment systems, and other utility services within CySim's simulated environment. The video highlights utility operators, engineers, and IT teams engaging in exercises that simulate real-world threats to municipal utilities. It demonstrates how CySim's training enhances incident response capabilities, strengthens the security of industrial control systems, and enables utilities to maintain reliable and secure services for the community.

6. Blue Training: Video Title: "Building Cyber Champions: Empowering Defenders with CySim's Blue Training"

Description: This video emphasizes the significance of ongoing training for cybersecurity professionals. It showcases CySim's blue training exercises, where participants assume the role of defenders and enhance their skills in areas such as threat detection, incident response, and vulnerability management. The video captures participants engaging in hands-on exercises, utilizing modern security tools within CySim's realistic training environment. It highlights the impact of CySim's blue