Funded By:-
Science and Engineering Research Board,
Department of Science and Technology,
Govt. of India

This document contains material, copyright of which rests with the C3i Center. This document, either fully or partially, may not be reproduced or copied without permission in writing. The commercial/non-commercial use of any information in this document may require a license from the proprietor of that information.
Contents

Messages ................................................................. 9
Mission & Vision .................................................... 15
Executive Summary ........................................... 17
List of Authors .................................................... 21

C3i Center

I
1 History ............................................................. 25
2 Objectives .......................................................... 27
3 Deliverables ....................................................... 29
4 Infrastructure .................................................... 31

Achievements

II
5 Vulnerability Assessment ........................................ 37
6 Publications ........................................................ 39
7 Book ................................................................. 41
8 Thesis ............................................................... 43
<table>
<thead>
<tr>
<th></th>
<th>Solutions</th>
<th></th>
<th>Outreach</th>
</tr>
</thead>
<tbody>
<tr>
<td>9</td>
<td>Network Intrusion Detection System</td>
<td>47</td>
<td>Collaboration</td>
</tr>
<tr>
<td>10</td>
<td>Malware Analysis</td>
<td>51</td>
<td>Education, Awareness &amp; Events</td>
</tr>
<tr>
<td>11</td>
<td>Honeypot - SOAR</td>
<td>55</td>
<td>Start-Ups</td>
</tr>
</tbody>
</table>
## List of Figures

<table>
<thead>
<tr>
<th>Figure</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1</td>
<td>History of C3i Center</td>
<td>25</td>
</tr>
<tr>
<td>4.1</td>
<td>Control system for power testbed</td>
<td>32</td>
</tr>
<tr>
<td>4.2</td>
<td>Smart load bank for power testbed</td>
<td>33</td>
</tr>
<tr>
<td>4.3</td>
<td>Intelligent electronic device for power system</td>
<td>34</td>
</tr>
<tr>
<td>7.1</td>
<td>Book</td>
<td>41</td>
</tr>
<tr>
<td>9.1</td>
<td>Dashboard of DAAMS</td>
<td>48</td>
</tr>
<tr>
<td>9.2</td>
<td>Auto-generated network topology</td>
<td>48</td>
</tr>
<tr>
<td>9.3</td>
<td>Asset details</td>
<td>49</td>
</tr>
<tr>
<td>10.1</td>
<td>Malware analysis</td>
<td>51</td>
</tr>
<tr>
<td>10.2</td>
<td>Overall statistics &amp; Top 10 file submissions</td>
<td>52</td>
</tr>
<tr>
<td>10.3</td>
<td>File upload page &amp; User submission history section</td>
<td>52</td>
</tr>
<tr>
<td>10.4</td>
<td>C3i MAF sample scan results for PE file</td>
<td>53</td>
</tr>
<tr>
<td>11.1</td>
<td>Number of times the honeypots were deployed</td>
<td>55</td>
</tr>
<tr>
<td>11.2</td>
<td>Number of attacks of each type per instance</td>
<td>56</td>
</tr>
<tr>
<td>12.1</td>
<td>Dashboard</td>
<td>58</td>
</tr>
<tr>
<td>12.2</td>
<td>Dashboard analytics</td>
<td>58</td>
</tr>
<tr>
<td>12.3</td>
<td>Scanned target information</td>
<td>59</td>
</tr>
<tr>
<td>12.4</td>
<td>Custom vulnerability scan</td>
<td>59</td>
</tr>
<tr>
<td>12.5</td>
<td>Custom CVE scan</td>
<td>60</td>
</tr>
<tr>
<td>12.6</td>
<td>Hidden directory bruteforce</td>
<td>60</td>
</tr>
<tr>
<td>14.1</td>
<td>CSAW’20</td>
<td>65</td>
</tr>
</tbody>
</table>
List of Tables

6.1 Publications of C3i Center .................................................. 39
8.1 Thesis submitted since October’19 to March’20 .............................. 43
10.1 Malware classification ....................................................... 52
Message from the Joint Coordinators

“Science and Engineering Research Board funded the C3i Center in 2017. Since then, C3i Center has built industry scale critical infrastructure testbeds, found vulnerabilities, developed protection mechanisms against attacks, developed malware analysis tools with AI/ML, developed honeypot techniques for threat intelligence collection, and worked on various other aspects of cyber security of cyber physical systems. In 2020, the Department of Science and Technology (DST) established a technology innovation hub (C3i Hub) at IIT Kanpur. This may be considered a success of the continued value addition to India’s cyber security research landscape in India by the C3i center researchers and students. C3i Center is India’s first academic research center on critical infrastructure security, and has been working with various government and PSUs on Cyber Security.”

Prof. Manindra Agrawal
Message from the Joint Coordinators

“In spite of various phases of Covid-19 related lockdowns, C3i Center researchers have been working hard not to let the sporadic lockdowns slow down progress. In the past year, C3i Center not only augmented its testbeds, but also provided cyber security consultancy, vulnerability assessment and penetration testing (VAPT), policy formation, risk-based analysis of projects undertaken by multiple government agencies – such as NHAI (National Highway Authority of India), THDC (Tehri Hydroelectric Development Corporation), Niti Aayog, CDOT etc. C3i has also participated in various committees for framing cyber security regulations, and guidelines. The Center has also launched various training programs (certification program in Cyber Security, Blockchain etc.). The upgradation of the center into a Technology Innovation Hub by the DST is a testimony to the contributions of the center in the Indian Critical Infrastructure Security.”

Prof. Sandeep K. Shukla
Message from the Lead Engineer

“As a leading research center in the critical infrastructure security space, we have been planning, and executing research, vulnerability assessment & penetration testing, interfacing with the government and private sector players in the critical infrastructure space. 2020-21 has been a successful year on various fronts, especially in engaging with PSUs and in spinning off startups and in augmenting our testbeds.”

Mr. Rohit Negi
Mission & Vision

Mission:
To be a leading research, education and technology innovation center in the space of cyber security and cyber defense of critical infrastructure.

Vision:
Critical Infrastructure such as the power grid, waste water treatment, oil and gas pipeline, transportation etc., are digitally controlled, and the physical processes under control are measured through sensors, and control is exerted through actuators. The data between sensor, control and actuation are communicated over network using industrial communication protocols – which are often not designed to be secured. This provides an extensive attack surface for cyber attackers to exploit. Nation state attackers, and ransomware gangs are using this opportunity to do harm to other countries important national critical infrastructure.

Therefore, preparedness for securing and defending such systems from cyber attacks is of paramount importance. It is in this space, C3i Center focuses and creates capabilities in terms of technology research, technology transfer, awareness and education, and services to various government and private sector entities in this space.
We are delighted to present the fourth annual report of the C3i Center. This report covers C3i center activities between September 2020 till September 2021. We acknowledge the Science and Engineering Research Board (SERB), under the department of science and technology (DST) of the government of India, for funding the “National Interdisciplinary Center for Cyber Security and Cyber Defense of Critical Infrastructure” (C3i Center) at IIT Kanpur, in March 2017.

Major highlights of this year are research progress, development of multiple advanced educational programs including certificate courses and degree courses in Cyber security, our successful projects with multiple PSUs, augmentation of our cyber security testbeds, and multiple technology development which are transferrable to industry. This progress report summarizes the activities and achievements of the center from September 2020 till September 2021.

The center has several deliverables, namely (i) a national scale SCADA/ICS testbed for cybersecurity studies, (ii) developing tools and techniques for malware collection, benchmarking of malware detection and classification algorithms, (iii) developing tools and techniques for vulnerability, and penetration testing and discovery of yet to be uncovered vulnerabilities in ICS software (iv) developing tools and techniques for insider-threat proofing (v) working with power utilities to build analytic data techniques on PMU data to detect on-going cyber-attacks (vi) creating at
least one start-up on the developed technologies (vii) developing mobile malware and their analysis techniques.

Even though in the last 12 months, the center’s work has been punctuated by multiple lockdowns due to the prevailing Covid-19 pandemic, the progress towards the goals has not suffered any setback.

The testbed creation in the various critical infrastructure sectors continued. At this time, the installed testbeds are power distribution, solar and diesel generation and synchronization test bed to the institute grid, water treatment plant, industrial manufacturing testbeds, and the power transmission testbed. Even though in 2020, there was some delays due to lock down, this year, we have successfully installed and commissioned the power transmission testbed, with 1.1 KV scaled down transmission system model fitted with substation automation, power protection relays, and phasor measurement units (PMUs). The SCADA based control is under configuration at this time. The procurement of DCS controller is under progress. Overall, after the DCS is procured, installed and integrated, we will have the full-fledged power grid testbed with industrial automation equipment such as programmable logic controllers, sensors of various kinds, actuators of various types, distributed control system, remote terminal units, SCADA, relays and PMUs of various makes and models – giving us ample opportunity to not only discover hitherto unknown vulnerabilities, but also, develop and test compliance testing tools, developing protection and intrusion detection methods, and risk driven security architecture.

The C3i honeypots have been deployed in various locations via cloud based virtualization, as well as inside the C3i center network to collect malware. The honeypots deceiving attackers either as IT systems or OT systems have been helpful in collecting threat intelligence, and in developing SIEM (Security Incident and Event Management Tools) to make sense of the collected threat intelligence.

The machine learning based malware analysis tools have been augmented to detect malware in JPEG files, Javascript files, and further improvements in performance of some of the previously
developed models have also been done. Three papers on malware analysis work by C3i researchers got published in International Conference Proceedings – including one on adversarial malware generation and use of such samples to robustify the machine learning models.

Multiple anomaly based intrusion detection methods have been developed and validated. These methods are robust to outliers, training data poisoning attacks, and boiling frog attacks. Two papers in this topic have been accepted at international conferences.

In the vulnerability and penetration testing, while C3i Center researchers have carried out vulnerability assessment of products from CDoT, SamShiksha (Niti Aayog product), NHAI and multiple other systems, due to prolonged absence from the lab during lockdowns, critical infrastructure vulnerability discovery process was slow.

A start-up on deception technology developed at C3i center has been incubated under the C3iHub Prayas and Nidhi Prayas program.

A lot of interaction with government agencies such as the National Cyber Security Coordinator, Central Electric Authority, National Thermal Power Corporation, National Highways Authority of India, Tehri Hydro Development Corporation India Limited (Tehri, Uttarakhand), are on-going. Several industries, such as Schneider Electric, Tech-Mahindra, LTTS, SMC, have been interacting quite often. Disclosures of vulnerabilities have been made to many ICS vendors – Aveva, Schneider Electric, Rockwell, WAGO and Synergy, in particular.

C3i center also promotes awareness and education in cybersecurity. Yearly cyber-security competition event CSAW, in cooperation with New York University, has been an on-going activity every year. In November 2020, for the first time, the competition was held completely in online mode.

C3i also hosted 20+ summer interns during the summer who worked for 2 months on various cybersecurity projects.

A few training sessions have been organized for NPTI (National Power Training Institute). C3i, IIT Kanpur, in association with
TalentSprint, has designed a six-month Advanced Certification Program in Cyber Security and Cyber Defense for current and aspiring professionals from various organizations who are keen to explore and learn the latest trends in Cyber Security Technologies. Three cohorts have been completed and the fourth cohort is about to start. There are several new educational programs that launched this year or got IIT Kanpur approval this year. Talent Sprint launched a fresh graduate cyber security education program online with C3i Center which will be open to participants who are within 2 years of their graduation – and want to enter the cyber security field.

We also started a Blockchain Technology Certification program with Simplilearn – another online educational technology platform. The IITK Senate also approved MTech and MS in cyber security program, and also e-Masters (fully online) in Cyber Security.
## List of Authors

| Authors           | Prof. Manindra Agrawal  
|                  | Prof. Sandeep K Shukla  
| Project Title     | National Interdisciplinary Center for cyber security and cyber defense of critical Infrastructure  
| Security          | RESTRICTED (RE)  
| Version           | 4.0  
| Total number of pages | 70  
| Prepared By       | Mr. Amit Negi  

In March 2017, SERB/DST sanctioned the establishment of the National Interdisciplinary Center for Cyber Security and Cyber Defense of Critical Infrastructures (also known as ‘C3i center’). An amount of 14.43 crores INR was sanctioned over a five year period (March 2017 – March 2022) to establish this center as a center of excellence in securing critical infrastructures of the country. In the last few years, it has been recognized for its work internationally.
In 2020, The department of Science & Technology established a Technological Innovation Hub (TIH) on cyber security and cyber security for Cyber-Physical System, which is known as The C3i hub, C3i center is the research and academic nerve center of the C3i hub.
2. Objectives

**Major Objectives**

- Design and Development of Machine learning algorithms for detecting on-going cyber-attacks and advanced persistent threats on power systems.
- Build methodology and techniques for deploying honey nets to develop a malware repository and malware analysis and trend forecasting capabilities.
- Apply formal methods to develop effective algorithms for vulnerability and malware detection in applications, systems, and firmware – and transfer such technology to a startup ecosystem.
- Develop protocol reverse engineering tools and capabilities to detect presence of botnets, trojans and other advanced persistent threats.
- Develop light weight cryptography and block chain-based authentication, identity management and key management schemes for network of devices (IoT and M2M).
- Develop cryptographic co-processors and side-channel proofing techniques for cryptographic hardware, and software systems.
- Field testing security techniques, architectures, and protocols on the IITK smart city project.
Major Objectives

- Develop security architecture, perimeter defense, network and Cloud security for critical infrastructure, and inform the policy formulation and best practices guidance for National Critical.
3. Deliverables

1. A national scale SCADA testbed for research, training, and hardware / software in-the-loop testing by vendors at IIT Kanpur

2. Tools and techniques for malware collection and benchmark creation for malware analysis

3. Tools and techniques for application software vulnerability detection

4. Tools and techniques for Insider threat-proofing critical infrastructure IT system

5. Work with a power utility or smart grid corporation to experimentally use our PMU data analytics-based tools for detecting advanced persistent threats

6. Create at least one startup with IIT Kanpur incubation enterprise in the cyber security of critical infrastructure space by licensing IP in vulnerability detection, protocol reverse engineering, malware detection etc.
Creation of malware for exploitation of criminal information system and mobiles for offensive security.
4. Infrastructure

The interdisciplinary center for cybersecurity and cyber defense of critical infrastructures (C3i) at the Indian Institute of Technology Kanpur facilitates researchers to work with the pilot setup of critical infrastructures.

1. Control System (Power Testbed)
2. Smart load bank
3. Intelligent electronics device for power system
Figure 4.1: Control system for power testbed

- This testbed facilitates researchers to design and develop cyber security solutions for power industry.

- Hardware/Software in loop testing facility.

- Major features of the testbed are 100KM long transmission line, Transmission voltage upto 1.1 KV, integrated Industrial automation and control system (IACS), multiple communication protocols, etc.
Figure 4.2: Smart load bank for power testbed

- Emulate an electrical load, to test an electric power source without connecting it to its normal operating load during testing, adjustment, calibration, or verification procedures. Load bank is connected to the output of a power source in place of its usual load.
Figure 4.3: Intelligent electronic device for power system

- Take a deep dive in protection system.
- Hardware/Software in loop testing.
- Major features of the testbed are protection protocols, timestamped data etc.
## Achievements

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>5       Vulnerability Assessment</td>
<td>37</td>
</tr>
<tr>
<td>6       Publications</td>
<td>39</td>
</tr>
<tr>
<td>7       Book</td>
<td>41</td>
</tr>
<tr>
<td>8       Thesis</td>
<td>43</td>
</tr>
</tbody>
</table>
5. Vulnerability Assessment

The assessment of hardware and software about operational technologies in the industrial control system is carried out at C3i in a controlled environment. Team C3i has successfully identified a large number of vulnerabilities in the products and the systems. A few of them already received international recognition.

Acknowledgement of Responsible disclosures

- 1 CVE disclosed

**CVE ID: CVE-2020-7536**

CVSS v3.0 Base Score 7.5 (High)
Vendor: Schneider Electric.
Equipment: Modicon M340 CPUs.
Vulnerability: Improper Check for Unusual or Exceptional Conditions vulnerability exists that could cause the device to be unreachable when doing an unattended modification of network parameters over SNMP.

C3i Center has done VAPT of CDOT product’s, Samshiksha platform (Niti Aayog), complete infrastructure of NHAI, etc.
6. Publications

Table 6.1: Publications of C3i Center

<table>
<thead>
<tr>
<th>Year</th>
<th>Title and Authors</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Year</td>
<td>Publications</td>
<td></td>
</tr>
<tr>
<td>------</td>
<td>--------------</td>
<td></td>
</tr>
</tbody>
</table>
7. Book


Figure 7.1: Book
Book Chapters in Other Books


8. Thesis

Table 8.1: Thesis submitted since October’19 to March’20

<table>
<thead>
<tr>
<th>No.</th>
<th>Title</th>
<th>Author</th>
<th>Year</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Automated Windows behavioural tracing for Malware Analysis.</td>
<td>Shubham Rana, MTech</td>
<td>2021</td>
</tr>
<tr>
<td></td>
<td>Analyzing and improving the effectiveness of side channel attack</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>on Intel SGX.</td>
<td>Kuldeep Kumar Solanki, MTech</td>
<td>2021</td>
</tr>
<tr>
<td>2</td>
<td>Analysis of Developer Patches in smart contracts.</td>
<td>Suraj Gour, MTech (2021)</td>
<td>2021</td>
</tr>
<tr>
<td>4</td>
<td>Towards Malicious account identification in Bitcoin.</td>
<td>Deepesh Chaudhari, MTech (2021)</td>
<td>2021</td>
</tr>
<tr>
<td>5</td>
<td>Understanding Money Trails of Suspicious Activities in the</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Intrusion Detection in IoT devices using Zero Shot Learning.</td>
<td>Anurag Kansara, MTech (2021)</td>
<td>2021</td>
</tr>
<tr>
<td>9</td>
<td>Endpoint security for corporate infrastructure with windows devices.</td>
<td>Raunak Kumar, MTech (2021)</td>
<td>2021</td>
</tr>
<tr>
<td>No.</td>
<td>Title</td>
<td>Author</td>
<td>Year</td>
</tr>
<tr>
<td>-----</td>
<td>------------------------------------------------------------------------------------------------</td>
<td>-------------------------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
Network Intrusion Detection System ... 47
Malware Analysis .................... 51
Honeypot - SOAR .................... 55
ReconAID .......................... 57
9. Network Intrusion Detection System

C3i center is developing a Network intrusion detection system which has two major components i.e., “Infrastructure Mapper & Processor (IMP)” & “Data Acquisition, Analysis & Monitoring Server (DAAMS)”. IMP and DAAMS is a customized solution to enhance the cybersecurity of operational technologies (OT) networks. The solution auto-discover of all IoT and ICS assets and maintains a constantly up-to-date inventory of them along with associated vulnerabilities, a detailed dynamic network topology, classification of logs via machine learning, network intrusion results, etc.

This application can read packets (passive monitoring) from the network and extract useful information based on assets’ information. The application shall have a feature to update the database for the new patches/guidelines. The application shall notify the user of any detected anomaly, threat or vulnerability which shall also be logged as an Event Log.
Figure 9.1: Dashboard of DAAMS

Figure 9.2: Auto-generated network topology
Figure 9.3: Asset details
10. Malware Analysis

C3i center offers an indigenous web-based malware analysis tool. This tool can detect and classify malware in near real-time. The tool contains various types of analysis for various filetypes but not limited to PE, ELF, apk, doc/docx, pdf, is XLS, PNG, HTML, JPEG, etc. It uses an ensemble of machine learning models. C3i center analyzed 2,423,124 Malware samples.
Table 10.1: Malware classification

<table>
<thead>
<tr>
<th>Classification accuracy for new models</th>
</tr>
</thead>
<tbody>
<tr>
<td>Word documents malware detection – doc, docx</td>
</tr>
<tr>
<td>JS malware</td>
</tr>
<tr>
<td>Independent static analysis model for ransomware</td>
</tr>
<tr>
<td>up to 97.3 %</td>
</tr>
<tr>
<td>up to 97 %</td>
</tr>
<tr>
<td>up to 98 %</td>
</tr>
</tbody>
</table>

C3i Malware analysis Framework:

This GUI shows the overall statistics like total submission done till date for file analysis, the total number of users registered for accessing the framework, the number of servers for dynamic analysis, and the malicious files detected by the framework.

The malware analysis framework can be accessed only after the login and new users can register to use the service after approval.
This GUI shows the file upload service with the available servers which can perform the dynamic execution the sample being uploaded and the submission history for a user.

![GUI showing file upload service and sample results]

**Figure 10.4: C3i MAF sample scan results for PE file**

The GUI shows the sample results after the file scan is completed. The Screenshot shows the scan results for the PE file with the basic properties and the structural information.
11. Honeypot - SOAR

Security Orchestration and Automated Response: Developed an orchestration engine for deploying honeypots based on attacker behavior. The engine can dynamically deploy desired honeypots. Test results of the engine in a network with live traffic are given below:

![Graph showing number of times honeypots were deployed](image)

**Figure 11.1:** Number of times the honeypots were deployed

Dynamically deployed honeypots are the ones deployed by the engine according to attacker behavior in the network. We also placed some static honeypots to capture attacks. The figure shows the efficiency of the dynamically deployed web-server honeypots...
as they captured more attacks and are more convincing. Attacks on dynamically deployed web-server honeypots vs statically deployed web-server honeypots

![Graph showing number of attacks of each type per instance](image)

**Figure 11.2:** Number of attacks of each type per instance
12. ReconAID

It is reconnaissance automation, having default and custom scan features. It uses the power of Multitasking and multi-threading to make the recon process faster and smoother. It analyzes domains, collects subdomains through multiple sources, and gathers information from its network analysis to its exploitation phase.

It manages to collect Basic Info of DNS to IP, PORT, ASN CIRD Range, Technology Stack, Visual Recon, Network Map, and open port running services & version. It can collect hidden endpoint and directory and scan and search Hidden endpoints and tokens in JS files and Github. It used publically available exploit engines to gather critical information from Shodan, Censys, Securitytrail, Binaryedge, crt.sh, etc. It has the functionality to search any vulnerable service in the CVE engine and has reporting and notification feature.

This GUI shows the overall statistics like total scan domain and have functionality to delete results from database. It also shows dynamic results in pie-chart of total end point discovered in all scan domain.
Chapter 12. ReconAID

Figure 12.1: Dashboard

This shows dynamic results in pie-chart of total scanned domain, subdomains and end point discovered in all scanned domain.

Figure 12.2: Dashboard analytics

Scanned result of domains, (subdomain, Cname, IP, ports, services running in particular port, tech stacks, screenshot, & ASN number with Shodan query.)
Figure 12.3: Scanned target information

Figure 12.4: Custom vulnerability scan

Scanned domain running applications known vulnerability searched through CVE database. This will give the know publicly available exploits details.
Figure 12.5: Custom CVE scan

Figure 12.6: Hidden directory brute-force
IV Outreach

13 Collaboration .......................... 63
14 Education, Awareness & Events ...... 65
15 Start-Ups ............................... 67
13. Collaboration

C3i has signed 3 MoUs (2020-21) with the following industry partners:

HCL Technologies
Chapter 13. Collaboration

Indian Port Association

Indian Ports Association
An apex body of Major Ports under Administrative Control of Ministry of Ports, Shipping and Waterways

Cyber Security Karnataka

CySecK
Cyber Security Karnataka
K-Tech CoE for Cyber Security
14. Education, Awareness & Events

Education
126+ Trainee  40+ Fellowships  19+ Internships

Awareness & Event
Cyber Security Awareness Week (Online Mode)

Figure 14.1: CSAW'20
Incubated 13 startups in cyber security domain.

**Asatrobo**

UAV Security and they are developing indigenous technologies for anti-drone applications by GPS spoofing.

**CDSpace**

Which is into UAV Security, and they are developing Secure Long Range Video Telemetry for UAV ISR Applications.

**COSGrid Systems**

Intrusion Detection & Prevention and they are developing Holistic solution for Secure Access in borderless Networks.

**Egyanam Technologies**

Integrated SOC solution and they are developing Integrated Automation, Intelligence & Diagnostics platform for warning and automation response.
Hack-X Security
A cyber asset management startup developing a centralized platform that helps connect security testers and client developers for prioritizing and quick fixing of vulnerabilities.

X-Ten Networks
Builds firewalls and other filters they are developing an Intelligent Threat Gateway that creates a logical cyber border at network perimeter and deploys virtual forces to guard digital assets.

T-Sanct Technologies
Provide security through AI-Enabled SaaS and are developing SaaS modelled digital risk monitoring platform to detect and tackle cyber threats.

OPT-Cyber Security
Works in cyber Risk Evaluation & Mitigation and are developing Cyber Insurance SOC for cyber protection, cyber-attack prevention & cyber risk measurement and modelling.

Secure Blink
An application security management service provider and are developing an automated application security management platform that provides comprehensive assessments using AI-enabled capabilities.
**Treacle Technologies**

Works in Honey Pot & Deception Technologies and they are developing deception tools for IT/OT infrastructure which are comprehensive & scalable to deceive potential attackers.

**WUS**

Cyber Literacy and Awareness startup, which is developing a software tool that integrates cyber literacy for blue-collar workers in 10 Indian languages.

**Disecto**

A privacy-preserving security tool based startup and they are developing decentralized, privacy-preserving data sharing/analytics framework which is highly modular & scalable.

**Cyberwarfare labs**

Providing cyber range solutions and are developing an on-demand dedicated lab environment for red, blue and purple team-based cyber wargaming.