NASSCOM®

AmberFlux

ER&D NIPP Pitch Session

Schneider Electric Cyber Security – Continuous Threat Detection, Incident Management & Control for Energy Sector

From AmberFlux EdgeAI Pvt Ltd in partnership with
Scalarr Inc.

Instructions

- The applicant must **read** FAQ and meet the **pre-requirements** to submit the proposal.
- The applicant must thoroughly understand the **problem statements** either by joining the corporate connect sessions or viewing the corporate connect sessions in NIPP ER&D INNOVATION CHALLENGE website before submitting the proposal.
- The applicant is required to submit proposals to the NASSCOM through an **online system,** refer to "Submit Proposal" option in NIPP ER&D INNOVATION CHALLENGE website
- The applicant must fill all details in "online application form" and cover all sub-sections mentioned in the "Pitch Session" template to qualify in technical assessment round
- Each applicant will be given 10-15 minutes time to pitch and 10-15 minutes for Q&A. The number of slides shall not exceed 5 slides. Any additional details must be added in annexure to support technical assessment
- The applicant must submit the proposal on or before **5 November 21** and NASSCOM will not grant an extension to the above deadlines. It is applicant responsibility to ensure you follow the guidance/rules and allow sufficient time to complete all requirements described.

NASSCOM®

AmberFlux EdgeAI Pvt Ltd Overview

AmberFlux

About

AmberFlux EdgeAI is an Edge Computing and Artificial Intelligence purpose specific software products & solutions company. AmberFlux Opus enables AI on edge devices; AmberFlux Concerto enables cloud & enterprise integration with the edge and AmberFlux Opus Dashboard offers visualization & orchestration of edge devices. AmberFlux has partnered with Scalarr Inc of US to bring their cyber security solution offerings (AI EdgeLabs) to Indian market. This proposal to Schneider Electric is based on AI EdgeLabs solution of Scalarr and Opus Dashboard from AmberFlux.

Founded	**Aug, 2020**
Location	**Hyderabad, India**
Team Size	**10**
Solution Maturity	**MVP**
Industry Verticals	**Telecom, Energy, Industry 4.0 & Healthcare IT**
Funding Stage	**Bootstrapped**
Funding Amount	**NA**
Leadership	**Muralidhar Goparaju, CEO Raghavendra Rao Gudipudi, COO**

Capabilities

Deep domain capabilities related to edge computing, edge orchestration, cyber security, and artificial intelligence. Specific capabilities related to cyber security are:

- **Network Threat Detection:** DDoS, Botnets, Hacking, Ransomware, Malware, and others.
- **Autonomous Cyber AI:** Dynamic firewalling, blocking, automated shutdown protocols, and prevention playbooks.
- **0-Day Attack Detection:** Reinforcement Learning approach for unknown threats and attack detection.
- **IoMT / OT/ IT Assets Discovery & Management:** Agentless discovery of the connected assets IoT/OT assets and behavior modeling.
- **Network Visibility & Observability:** Dashboard, Rich traffic inspection for anomalous patterns, incidents of MITRE ATT&CK, forensic support.
- **Integrity:** Jira, Slack, Splunk, and other SIEM systems integration, escalation workflows, and internal Knowledge Base.
- **Opus Dashboard:** Visibility into connected devices, drill downs, orchestration rules, controls

Credentials

- AmberFlux has 1 granted patent in India and 3 granted patents in the USA in the area of energy management, resources optimization, and cognitive intelligence. More patent applications are under evaluation. AmberFlux is recognized by several industry forums as deep tech, edge computing player

Key Clients

- AI EdgeLabs has SixSQ, Ori.co - Edge Orchestration platform and Energy, Telecom, and Healthcare clients

NASSCOM®

Solution Overview

Problem statement understanding

Energy sector infrastructure is going smart, digital and connected. There are thousands of operational technologies (OT) prone to cyber security risks. Many OT equipment are not equipped to handle security. Highly vulnerable to threats. With IT/OT convergence, fraudsters can leverage IT techniques to target OT. Availability and continuity of service is more important in OT for energy sector (more imp than confidentiality of data. Schneider Electric is seeking a solution that provides for threat detection, incident management & remote control (visualization & orchestration) as key requirements.

Solution Summary

AmberFlux solution comprises of two products:

1. AI EdgeLabs from Scalarr Inc for threat detection & incident management
2. AmberFlux Opus Dashboard from AmberFlux for visualization, orchestration controls

We will install AI EdgeLabs software “sensors” (AI agents) and the edge devices/IoT & OT gateways. The sensors will monitor all traffic and Operating system telemetry data that passes through the device and provide Schneider Electric’s SOC team with OT Visibility & Asset Management, Threat & Anomaly Detection, and Remote Incident Management

AI EdgeLabs Sensors could be deployed as standalone deployments on Linux, IoT Gateways, and Edges. Cloud deployment as the backbone.

The AI Sensor capabilities:

- AI Inference and processing is lightweight (Rust, ONNX compression)
- Ready for offline work and unstable connectivity (buffering and autonomous models)
- Offers a simple integration (Linux, Kubernetes support)
- Works to unique traffic picture on the client-side node (RL, Autoencoders)

Features:

Edge/IoT Threats Detection: DDoS, Botnets, Hacking, Malware and other threats and attacks detection.
Edge/IoT Threats Prevention/ Autonomous Cyber AI: Dynamic firewalling, blocking, automated shutdown protocols.
AI-Based Anomaly Detection: Reinforcement Learning approach for 0-day threat and attacks detection.
IoT / OT Assets Discovery: Agentless discovery of the connected assets.
Network Visibility & Observability: Dashboard and integration with SIEM systems.

USPs

Specify how does the solution stand out from the competitors?

- Edge-focused design & performance
- Advanced cyber AI detection & autonomous cyber AI security
- Competitor solutions take 1 to 2 years to deploy. Our solution can go live within a few days/weeks
- Our solution can be integrated with SIEM or SCADA
- Agentless for IoT/OT
- Relying on Reinforcement Learning and AI
- Kubernetes-based or Docker-based quick installation

IPs/Patents

Details of existing IPs filed/ granted for the solution (If any)

- India Patent No: 385086; Issued in Dec 2021. Effective from Apr 2014.
- US Patent No. 9092741; Issued in Jul 2015; Effective from Jul 2014
- US Patent No. 9817422; Issued in Nov 2017; Effective from Jul 2014
- US Patent No. 10481629; Issued in Nov 2019; Effective from Jul 2014

Details of IP used/shared with another 3rd party (if any)

AmberFlux doesn’t have any shared IP with any other party. However, Scalarr Inc has the following:

- Proprietary database of network threat signatures
- Historical data about botnets and threat IP from previous product

Awards

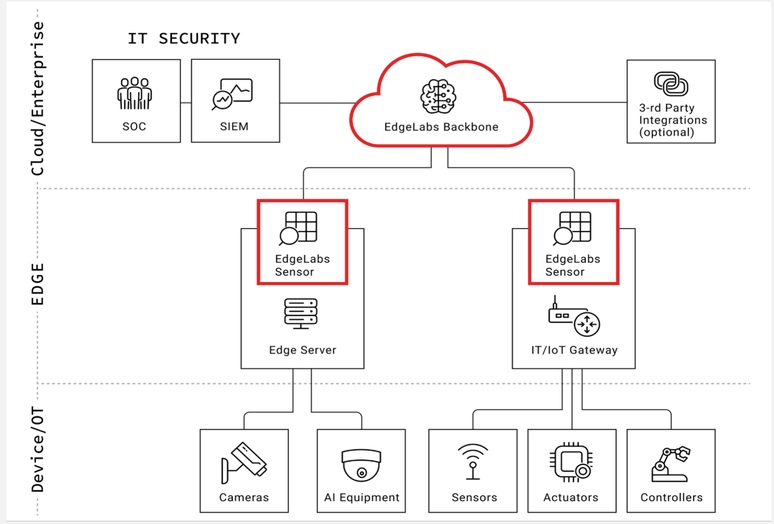
Details of awards received from credible organizations

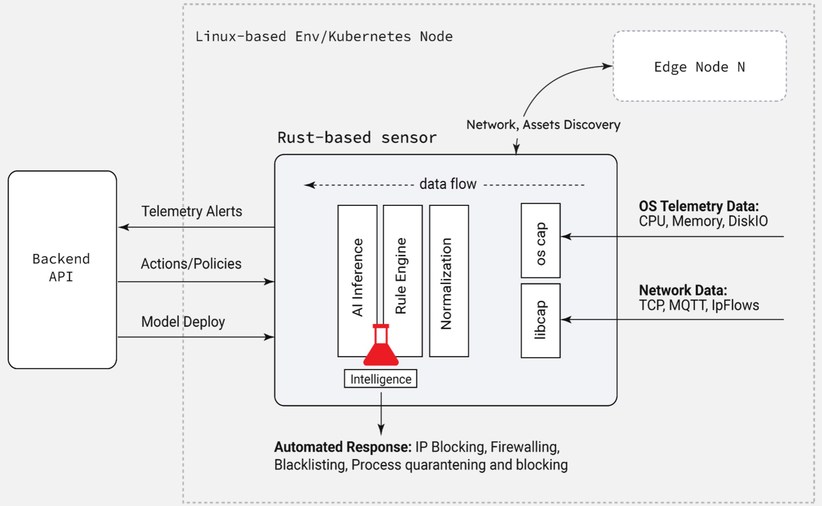
- Finalist at Startup of the Year competition Oct 2020 by Edge Computing World
- DeepTech Pioneer recognition by Hello Tomorrow France, Sep 2021
- Selected for Nasscom Cyber Security Incubation Center, Sep 2021
- Intel Network Builders Winners Golden Circle Member, Intel, Apr 2022

Solution Overview Contd..

Solution Details

Detail the entire solution, along with images, flowcharts, and related approach plans





Device Visibility
- Device attributes
- Device recognition
- Logs and logs tally
- Managed, unmanaged assets

Anomaly & Risk Assessment
- Vulnerability mapping
- Multi threat assessment
- Device risk scores
- Regulatory compliance assessments

Policy Enforcements
- Behavior segregations (trusted/untrusted)
- Multi-list (blocked, allowed, unknown, suspected)
- Automatic updates
- Random checks & escalations management

Proactive/Reactive Threat Prevention
- Detection of threats (known, unknown via payloads)
- Device risk group categories
- Command & control theft management
- Fast detection, response

Orchestration
- Workflow, deployment management
- Order management

3rd Party integrations
- Inbound/outbound APIs
- Component/micro-product approach

We will install AI EdgeLabs software “sensors” (AI agents) and the edge devices/IoT & OT gateways. The sensors will monitor all traffic and Operating system telemetry data that passes through the device and provide Schneider Electric’s SOC team with OT Visibility & Asset Management, Threat & Anomaly Detection, and Remote Incident Management

Out of Scope

- Installing directly on the OT Devices;
- Vulnerability management
- Identity access management
- SD-WAN
- Hardware
- Anything that is not explicitly agreed as in-scope

NASSCOM®

Target Operating Model

<< Please provide details on the Target Operating model >>

People

Prior to Go Live

AmberFlux, Scalarr project team and Schneider Electric Security Operations Center (SOC) and technical teams

From Go Live

SOC team would utilize the platform/API feed

Process

Prior to Go Live

Agree on Scope of Work, Roles & Responsibilities, Support requirements, Acceptance tests, Timelines, etc.

Implementation coordination, implementation, and acceptance as per agreed roles & responsibilities. AmberFlux to implement in alliance with Scalarr and Schneider Electric to provide the support agreed.

From Go Live

After being installed on the gateways/edge devices the sensors will identify anomalies, alert the SOC teams, and provide remediation options. Once trained, the system can operate in an automated manner.

Technology

Prior to Go Live

Support tools and technologies agreed as per the project plan. Generic project management tools, OS and infrastructure, etc.

From Go Live

Artificial intelligence, reinforcement learning, and machine learning are what power AI EdgeLabs. The sensor can be deployed directly onto the edge devices and IoT/OT gateways. Opus dashboard for visualization & orchestration controls.

Pricing Model

We are open to pricing models that are economical and win-win for all parties. Our preferred model is a subscription (monthly/yearly fee as SaaS). We are also open to the idea of joint go-to-market based on prime-sub contracting, revenue share, etc. While we are in principle open to joint development of IP, we will need prior clarity on ownership rights to IP.

Thank you. For more details, contact:

goparajum@amberflux.com

Raghu@amberflux.com

isaiah@edgelabs.ai