PRESS RELEASE

CYBERLENS® BETA ANNOUNCEMENT

On March 17th, the control system cyber security company Dragos Security LLC announced the beginning of Beta testing for their flagship product – CyberLens®. CyberLens® is a suite of tools that enable passive discovery and identification of cyber assets and data on control system networks.

“Normally, identifying assets can be difficult or impossible on sensitive networks because network mapping generally involves active scanning.” stated Dragos Security Co-Founder Robert M. Lee “active scanning can damage or deny service to sensitive network-enabled devices.”

In the Industrial Control System (ICS) community some of the sensitive devices include Programmable Logic Controllers (PLCs) and Remote Terminal Units (RTUs) which are vital to critical infrastructure such as energy, transportation and water utilities.

ICS asset owners and operators are challenged to maintain constant visibility in to what is on their network and how it is speaking. CyberLens® enhances satisfying compliance standards such as North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) through cyber asset and communication link identification. The suite of tools can also be used to identify changes in system connectivity and communication links using it's timeline feature serving as a strategic asset for incident responders. “Understanding your network and having a current map of what assets are on it down to the type of data flows is security. Knowledge of the network is a foundational element security teams should have over the adversaries,” said Co-Founder Matthew E. Luallen.

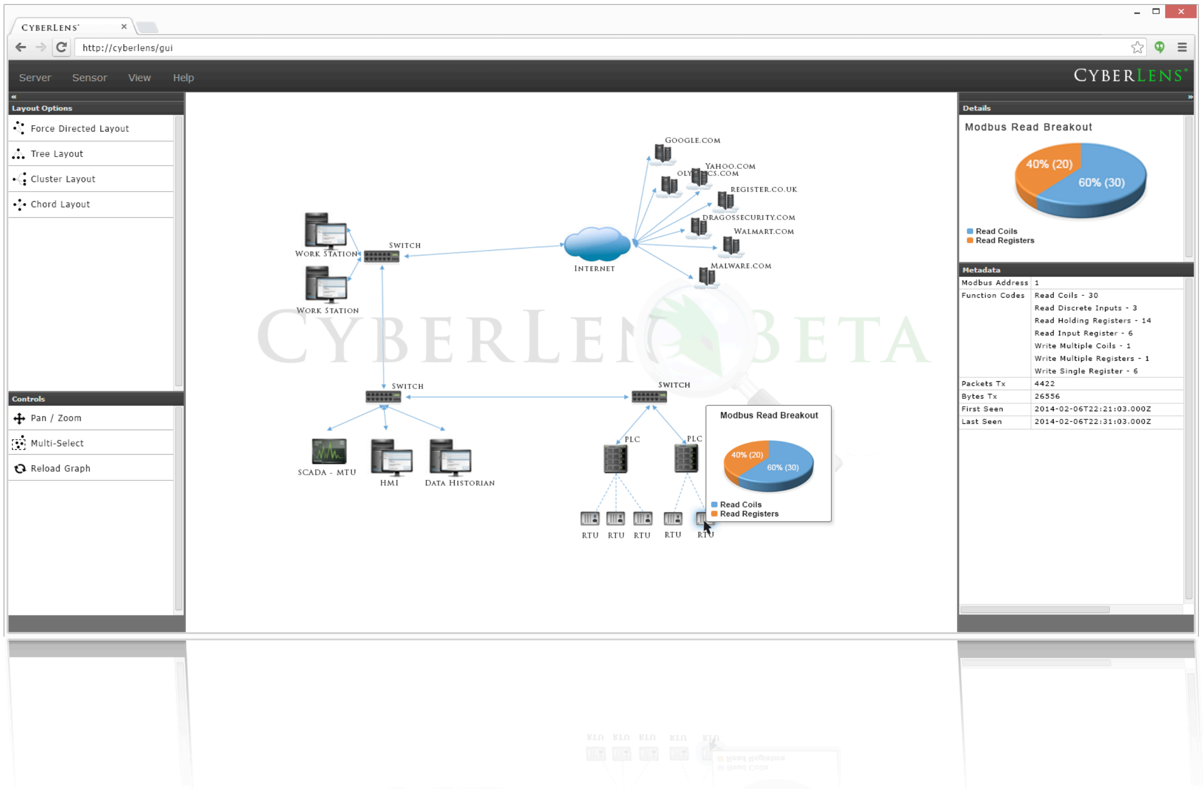
CyberLens® gives an unmatched view into the network and has optional customizable security features to meet the needs of the user.

Industrial Control System asset owners and operators with appropriate permission to deploy and operate a tool such as CyberLens® on the network are eligible to request Beta participation. To inquire further about the Beta and gain access to the application email: info@DragosSecurity.com

OUR MISSION

EMPOWERING OTHERS WITH THE TOOLS AND RESEARCH FOR SUCCESS

Co-Founders Justin Cavinee, Jon Lavender, Robert M. Lee, and Matt Luallen created Dragos Security LLC in August 2013. Each of the members recognized the importance of control systems to the security of critical infrastructure and decided to pool their experience and passion into creating a company that could assist the global community. As academics, developers, and operators the team members knew first hand what it means to develop and research products the community needs. The desire of the team was thus to create effective products and provide well thought out research that enabled the community to better achieve security, availability, and reliability.



Metadata

Modbus Address	1
Function Codes	Read Coils - 30 Read Discrete Inputs - 3 Read Holding Registers - 14 Read Input Register - 6 Write Multiple Coils - 1 Write Multiple Registers - 1 Write Single Register - 6
Packets Tx	4422
Bytes Tx	26556
First Seen	2014-02-06T22:21:03.000Z
Last Seen	2014-02-06T22:31:03.000Z

CyberLens® features include:

- Perform live and passive network data captures through the deployment of one or more sensors around the network
- Operate standalone processing pre-obtained packet captures and mapping the results offline
- Generate an interactive graphical map for users to see all network devices, how they are connected, and in what ways they communicate
- Save or print off the maps and any of your settings for future use
- Display a printable and easy to read list of all the devices on the network
- Use available data to perform timeline analysis to see network changes or aid incident response
- Show network statistics for each link including the type of protocols, volume, and netflow
- Enable a variety of alerts including the identification of new devices or failing of old devices
- Create multiple user accounts with secure logins
- Easily deploy the tool with a complete installer on multiple Operating Systems
- Full packet inspection and dissection of traditional Information Technology protocols as well as control system protocols through unique protocol lenses such as DNP3, ModbusTCP, BACNet, AB PCCC, ISO-TSAP, S7 and more.
- Extensions to enable additional data flows to asset inventory, centralized logging and intrusion analysis programs
- Custom lens and API support to perform deep packet inspection within proprietary ICS protocols
- Observe commands sent to control devices and validate devices such as Data Historians