GRAPHENE

## Advantages

- Graphene®'s passive sensing allows networks to run securely without interference
- Its management is controlled through an independent interface
- Compatible with major SIEM providers
- Compatible with all major standards:
  NIST 800-82, NIST 800-53, NERC CIP, ISA-99
- Graphene® is installed in each VLAN and monitors the traffic between all assets in the network, including HMI servers, PLCs, RTUs and VFDs, it alerts facility operators in the case of any abnormal behavior
- PLC firmware versions
- Vulnerabilities and known exploits
- PLC firmware/ logic changes
- Applies policies with the plant control engineers



ICS security
Industrial Control Systems

**ICS Security LTD.** | **www.ics-security.com**

**Address:** Gev Yam Negev Park, Be'er Sheva, 84709

GRAPHENE

# The Perfect Security Solution for SCADA Networks

ICS Security's **Graphene®** is an advanced SCADA protection system solution that provides the highest level of cyber protection with specific modules for strategic sectors:

**Energy and electric power plants · Gas and oil refineries · National desalination plants · Smart buildings · Chemical and pharmaceutical plants · Transportation service providers**

**Graphene®** is the result of the company's 18 years of experience in the SCADA field, and the insights and knowledge gained from close cooperation with leading organizations – both governmental and commercial, providing state-of-the-art User interfaces, behavioral monitoring, intrusion detection mechanisms, assetss discovery, external device protection, Network Access Control (NAC), ongoing vulnerability assessment and much more.

**By ICS Security**

ICS security
Industrial Control Systems

# Graphene | Key Features

## Full Visibility and Monitoring for ICS Networks

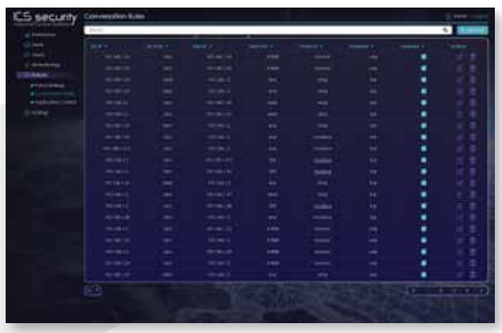
- Monitors the SCADA network's activity
- Agentless, non-intrusive
- Whitelisting on all HMI activities
- Provides asset inventory of the industrial network

## Fast, Easy Installation and Deployment

The Graphene deployment process is quite straightforward, just make sure Graphene is installed in a flat network and that the switch is configured to port mirroring.

## The Graphene Learning Phase

After deploying the Graphene in the network, the learning phase begins. The length of the learning phase is defined by the User; however, our recommendation is that the learning phase is no less than one week.



In that period, Graphene learns the network assets:

- Protocol used
- Communication type and direction
- Network throughput
- Many other parameters and states that are needed to define the network's "normal" behavior, so that Graphene can alert users of any deviation from this phase

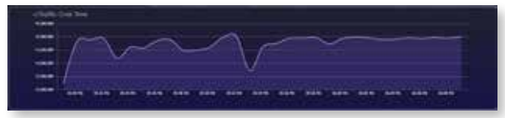
## Intrusion Detection

Graphene alerts users of any attack attempts on any of the ICS components, like:

- Firmware Version changes
- PLC attacks, DDOS Attacks, Port scanning, Ping sweep attacks, Malware attack recognition, Signature based rules, NAI – Network Access Identification

## Behavioral Monitoring

Any deviation from the "normal working curve" of the network that was sealed during the learning phase, such as:



- A new device in the network
- A dormant malware trying to act
- A new session detected. (For example, when two devices are communicating in new protocol for the first time)
- Unusual network traffic

## Asset Discovery

This feature gives an overall picture of all the components existing on the network, manufacturer type, the connection between them, communication direction and protocols used.