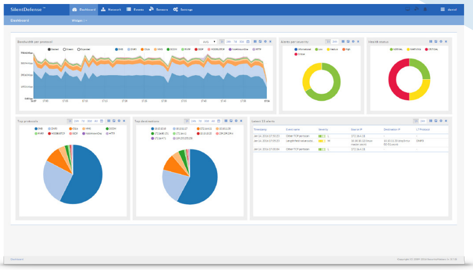
SECURITY MATTERS

eyONet DATASHEET

eyONet is **SecurityMatters**’ innovative network assessment service to easily and quickly evaluate your ICS/SCADA network cyber resilience.

By utilizing **SecurityMatters**’ **SilentDefense** platform, **eyONet** effectively identifies and visualizes existing ICS/SCADA network problems. **eyONet** will promptly inform you if:

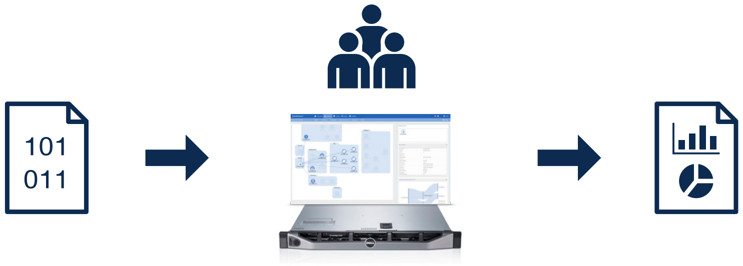
- All active devices in the network are behaving correctly
- Somebody is breaching your network perimeter
- Your process’ stability is at risk



eyONet’s actionable intelligence leads to secure and resilient ICS/SCADA networks.

Service layout

eyONet uses **SecurityMatters**’ advanced and innovative **SilentDefense** platform to quickly analyze your ICS/SCADA network.



Live network traffic or PCAP

SilentDefense

Report

BENEFITS

Easy setup and quick results

- Setup, network assessment and reporting within 2/5 days

Online or Offline analysis

- Live network traffic connecting **SilentDefense** to the span port of a network switch
- Offline PCAP analysis

No impact on your system performance and availability

- **SilentDefense** employs passive analysis approach that will not affect network devices and their operation

Broad coverage of ICS protocols

- Support for all major ICS/SCADA protocols and vendors
- Effective in both supervisory and process control networks

Superior control and protection

- Detects network misconfigurations, system misuse and operational mistakes along with bad and risky security practices

Two options: eyONet Basic and eyONet Premium

eyONet is offered in two distinctive levels, Basic and Premium.

eyONet		Basic	Premium
Duration		2 days	5 days
Analysis contents	Interactive map of active assets and device fingerprinting	✓	✓
	Used protocols	✓	✓
	Information flows	✓	✓
	Network perimeter	✓	✓
	Insecure/obsolete protocols	✓	✓
	Unusual/suspicious commands		✓
	Unusual/suspicious message content		✓
	Protocol violations		✓
	Device misconfigurations		✓
	Network timing issues		✓
	Network connectivity issues		✓
	Bad security practices		✓
Prerequisites*	• For live traffic analysis: port mirroring on selected network switches must be configured in advance • For offline analysis: a PCAP of the network traffic must be recorded in advance ***SecurityMatters** *will provide instructions to perform these activities*		
Deliverables	List of active ICS/SCADA network assets and information flows, used protocols, insecure protocols	✓	✓
	Report identifying unusual/suspicious commands and messages, protocol violations and threats to network stability		✓

SECURITY MATTERS

Gartner 2014 CoolVendor

SecurityMatters, a Gartner "Cool Vendor in Security", is an international company delivering cutting-edge network monitoring, intelligence and protection technology. **SecurityMatters** has installations across several continents in all major critical infrastructure sectors. It supports customers globally either directly or through its network of partners.

Contact us at:
info@secmatters.com
www.secmatters.com

SecurityMatters Worldwide HQ
Eindhoven, The Netherlands

SecurityMatters USA
Richmond, Virginia