SECURITY MATTERS

SILENTDEFENSE™

Visibility, Detection and Control for Industrial Networks

With installations worldwide, SilentDefense by SecurityMatters is the most advanced and mature ICS network monitoring and intelligence platform.

SilentDefense passively analyzes industrial network communications, provides rich information about network assets and alerts in real-time for any threat to operational continuity.

- Asset Inventory
- Network Assessment
- Network Monitoring
- Threat Hunting
- Incident Response
- Compliance & Standards

One Goal: Industrial Cyber Resilience

In the last 15 years, industrial environments have experienced a massive digitalization, driven by demand to boost efficiency and reduce costs. Although this digitalization has brought significant advantages, it has also dramatically increased the complexity of industrial environments, leading to an increased number of ICS-specific problems and threats, over which asset owners have no visibility.

SecurityMatters' solutions provide asset owners with full visibility into their network and detect threats before they lead to operational or cyber incidents. The benefits of our solutions extend to every organizational level and go beyond traditional cyber security.

> *We found a misconfiguration that was directly affecting our bottom line revenue that essentially paid for SilentDefense many times over in the first few days of operation.*
>
> **Frank at a US Independent System Operator**

> *Operational Technology security and monitoring needs to be able to adapt to rapid change, be self-sufficient and add value quickly and seamlessly, SilentDefense does all of these things for our customers.*
>
> **Jerry at a Major Industrial Control Security Integrator**

Benefits of SILENTDEFENSE™

SilentDefense empowers industrial operators with unrivaled visibility, threat detection capability and control of their network.

VISIBILITY

- See in real-time what your network devices are doing
- Assess risks, threats and vulnerabilities
- Understand the current resiliency of your network

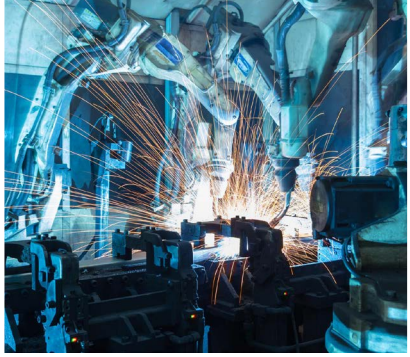
DETECTION

- Catch known and unknown threats at their earliest stages
- Pinpoint weak spots and current inefficiencies
- Gather all evidence required for incident response

CONTROL

- Know what's going on at all times
- Prioritize incident response and mitigation activity
- Anticipate problems and threats






Applications

Asset Inventory

- Automatic asset and communication inventory and network map
- Passive device fingerprinting, including device model, firmware version and modules
- Integration with IT/OT asset management tools
- At a glance view of host properties, network activity and configuration change logs

Network Assessment

- Automatic assessment of ICS device vulnerabilities, exposure to cyber threats and existing networking and operational problems
- Quick and comprehensive input for risk assessment with zero impact on the monitored network

Network Monitoring

- Continuous network monitoring and real-time alerting for operational and cyber threats
- Deep packet inspection for all common industrial protocols and vendors
- Rich alert details facilitate root cause analysis and reduce mitigation effort and cost
- Integration with major SIEM solutions and Syslog-enabled devices in a matter of minutes

Threat Hunting

- Comprehensive search for indicators of incidents in network traffic and protocol messages
- Continuous traffic recording for real-time and historical traffic analysis
- Flexible framework for definition and identification of recurring suspicious behavior

Incident Response

- Identification of incident source and spread through interactive network map
- Visual real-time and historical data analysis to speed-up recovery and mitigation
- Enterprise case management with smart grouping and automatic assignment of alerts to cases

Compliance & Standards

- Inventory information and controls enabling compliance with standards and guidelines such as NERC CIP and NIST Cybersecurity Framework
- Support network segmentation, policy enforcement and timely response for compliance with IEC 62443

Product Deployment and Operation

Integration and Support

Firewalls & Data Diodes

- paloalto NETWORKS
- FORTINET
- Check Point SOFTWARE TECHNOLOGIES LTD.
- PHOENIX CONTACT
- WATERFALL

SIEM Solutions

- IBM QRadar
- splunk>
- ArcSight
- ALIEN VAULT

Asset & Security Management

- cisco
- SKYBOX SECURITY
- ForeScout
- leidos

ICS Vendors

- ABB
- SEL
- EMERSON
- Schneider Electric
- SIEMENS
- Honeywell
- Rockwell Automation
- GE
- BECKHOFF
- YOKOGAWA

SECURITY MATTERS

SecurityMatters empowers critical infrastructure and manufacturing organizations with the ability to identify, analyze, and respond to industrial threats and flaws, minimizing troubleshooting costs and unexpected downtime. We leverage ICS-specific knowledge and understanding to provide visibility into critical assets and their activity, and detect operational problems and cyber security threats. Our revolutionary network monitoring platform has been successfully deployed by customers worldwide.

www.secmatters.com | info@secmatters.com