SECURITY MATTERS

SILENTDEFENSE™

Visibility, Detection and Control for Building Automation

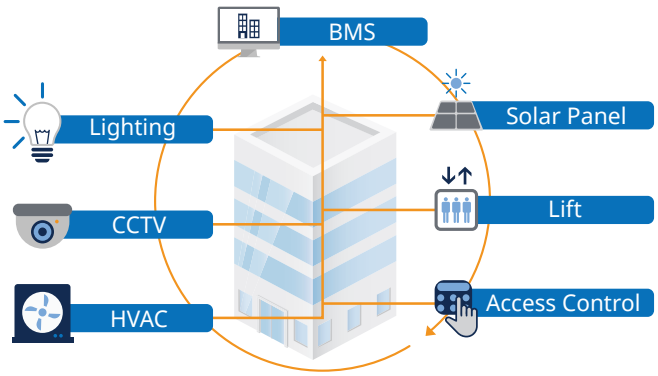
With installations worldwide, SilentDefense by SecurityMatters is the most advanced and mature building automation network monitoring and intelligence platform.

SilentDefense passively analyzes building automation 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

Landscape

Nowadays, a building is more and more a cyber-physical system (CPS) that integrates physical components such as HVAC, access control and elevators, escalators and moving walkways, with digital infrastructures. Building management systems (BMS) integrate, connect and control the building's different sub-systems to facilitate management operations. Today, data centers, hospitals, airports and other critical facilities are growing accustomed to the power of networked building automation systems (BAS) and are exploring the rapidly growing waves of Smart Buildings and the Internet of Things (IoT).



Challenge

Despite the many benefits brought by networking and IT convergence, several issues have arisen, including:

- the exposure of legacy systems with limited security mechanisms;
- the integration of technologies originally devised to address different issues;
- the increasing complexity and criticality of the managed processes.

Cases of cyber-attacks to Building Automation Systems are on the rise, and so are malfunctionings, misconfigurations and operational errors.

Solution

Exploiting the network convergence, SecurityMatters' solutions provide asset owners with full visibility into their building automation networks 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.

Benefits of SILENTDEFENSE™

SilentDefense empowers facility 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 building automation 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 building automation 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 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

- QRadar IBM
- splunk>
- ArcSight
- ALIEN VAULT

Asset & Security Management

- CISCO
- SKYBOX SECURITY
- ForeScout
- leidos

Building Automation Vendors

- CREATING A CLIMATE FOR GROWTH PRIVA
- WAGO
- Honeywell
- SIEMENS

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