SCADAShield
Industrial Grade Operational Continuity & Security

Challenges

국가 주요 기반시설 또는 산업시설은 안전하게 그리고 무중단으로 운영되어야 하지만, 이들 시설들의 OT 네트워크는 도입된지 오래 되었거나 표준화되지 않은 프로토콜을 사용하고 있습니다. 또한 OT 네트워크와 IT 네트워크간의 접점이 증가하는 추세에 따라 IT 네트워크로부터 기인한 사이버공격에 OT 네트워크도 공격 대상이 되고 있습니다. 이러한 공격으로부터 OT 네트워크를 안전하게 보호하기 위해서는 최신 기술을 활용하여 상시 모니터링 및 위협 탐지, OT 네트워크의 가시성 확보, 침해사고 조사 등에 대한 체계를 확보해야 합니다.

Easy & Quick Deployment

SCADAShield는 기존 OT 네트워크에 어떠한 영향도 주지 않고 간편하게 설치할 수 있습니다. 스마트 센서인 블랙박스를 네트워크 통신 허브에 탭핑하여 연결하면 SCADAShield는 보안상 취약점, 구성상의 오류, 오작동, 정책 위반 사항을 판별하기 위한 화이트 리스트와 블랙 리스트를 자동으로 생성합니다. 블랙박스는 인라인 모드로도 연결될 수 있으며 이 경우에는 차단 기능을 사용할 수 있습니다. 또한 SCADAShield는 SIEM과의 연동도 가능합니다.

SCADAShield BlackBox

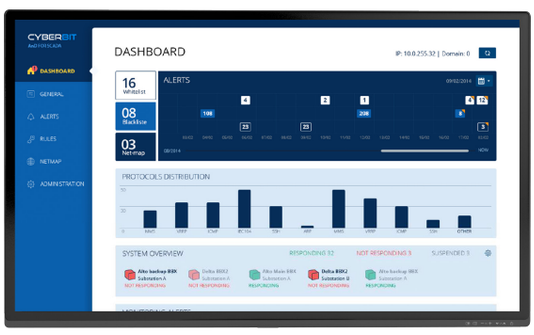
SCADAShield
-ICS Visibility and Security

SCADAShield는 OT와 IT 영역의 모든 프로토콜을 수용하여 OT 네트워크 상의 구성요소 및 이들간의 통신을 시각화하여 보여줌으로써 OT 네트워크에 대해 상시 모니터링, 위협 탐지, 침해사고의 조사, 분석 및 대응을 가능하게 해 주는 솔루션입니다. Deep Packet Inspection (DPI) 기능을 활용하여 SCADAShield는 각 계층에서 분석이 필요한 영역을 스스로 찾아내고 이와 관련된 네트워크 상의 모든 행위와 구성요소를 시각화하여 보여 줍니다. 따라서, 침해 행위에 대한 보다 정교한 탐지와 수월한 분석, 빠른 대응을 가능하게 해 줍니다.

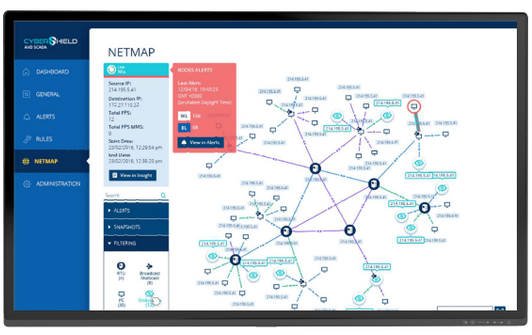
SCADAShield Capabilities

❶ NetMap - 네트워크 전체에 대한 시각화

SCADAShield의 NetMap은 OT와 IT 네트워크 접점을 포함하여 네트워크 전체에 대한 구성을 시각화하여 보여줍니다. SCADAShield가 설치되면 NetMap은 OT 네트워크 전체를 자동으로 식별한 후 화면상에 도식화하여 표현해 주고, 구성요소들간에 사용되는 프로토콜과 잠재위험요소를 표시해 줍니다.



SCADAShield Main Dashboard



SCADAShield Network and Communication Map

❷ Deep Packet Inspection (DPI)

잠재적인 위협을 조사하기 위해 RTU, PLC 또는 저장된 로그를 분석하는 기존의 보안장비와는 달리, SCADAShield는 byte 수준의 세부적인 Deep Packet Inspection (DPI)을 수행함으로써 보다 정확하고 신뢰성 높은 이상행위 탐지율을 제공합니다. SCADAShield는 전세계적으로 널리 사용되고 있는 20여가지의 ICS 프로토콜을 지원하며 새롭게 출시된 프로토콜도 지속적으로 업데이트하고 있습니다.

❸ Automatic Base-Line and Rule Generation

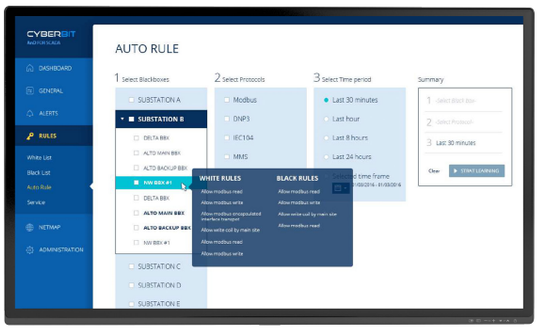
네트워크 트래픽 모니터링을 통해 SCADAShield는 정상적인 통신 패턴을 자동적으로 학습하고 이를 기반으로 비정상적인 행위, 제로데이 공격을 포함한 악성행위, 그리고 잠재적인 위협까지 구별해 냅니다. 이는 Auto-learning mode를 사용하여 화이트 리스트를 자동으로 생성하게 함으로써 가능합니다. 또한, SCADAShield는 이미 알려져 있는 ICS 네트워크, 디바이스, 프로토콜 등의 취약점에 대한 시그너처를 보유하고 있어 사이버보안 관련 위험을 경감시킬 수 있습니다.

❹ Real-Time Forensics

OT 네트워크 상의 데이터 수집 및 저장 기능을 통해 SCADAShield는 빅데이터 기반 조사/분석을 할 수 있는 포렌식 툴을 포함하고 있습니다. 따라서 실시간 이벤트 조사는 물론 이력 데이터와 실시간 데이터의 상관관계까지 추적하여 위협 행위에 대한 히스토리 분석을 통해 향후 재발 가능성을 원천적으로 차단할 수 있습니다.

❺ Customizable Dashboards and Actionable Reports

SCADAShield는 테라 바이트 규모의 방대한 모니터링 데이터를 사용자가 원하는 형태로 손쉽게 customizing하여 볼 수 있는 대시보드를 제공합니다. 대시보드 상에서는 사용자가 원하는 형태로 데이터 상호간의 조합도 가능하여 어떠한 조치가 필요한지에 대한 통찰력뿐만 아니라 광범위한 보고서 작성 도구까지 제공합니다.
예를 들어 시간 순으로 opcode 사용 내역을 조사하는 것도 가능합니다.



Auto Rule Creation

SCADAShield Customizable Dashboards

Supported Protocols

SCADAShield는 전세계적으로 널리 사용되고 있는 20여 종류 이상의 ICS 프로토콜을 지원합니다.

- Modbus TCP/RTU/+
- IEC60870 -5-101/104
- IEC60870 -5-101/104 over TCP/IP
- MDLC / MDLC over IP
- DNP3 / DNPi
- Siemens Profinet DCP/CM/IO/PTCP
- Siemens Profibus
- Siemens TIM
- SITA BSI (BagMessage Interface)
- IEC 61850 – GOOSE
- IEC 9506 -1- MMS
- IEC 60870 – 6/TASE.2
- CIP, with Ethernet IP (Common industrial protocol)

About CYBERBIT™

CYBERBIT Commercial Solutions Inc는 이스라엘 방위사업체 Elbit Systems LTD의 자회사로 SCADA/ICS 대상 사이버보안을 리딩하고 있습니다. CYBERBIT Commercial Solutions Inc는 SCADAShield의 한국내 판매를 위해 삼성SDS와 파트너십을 체결하였습니다.
제품문의: cyberbit@samsung.com