



SpyGOOSE Technical Data Sheet

Operating System: Ubuntu Linux 14.1 or newer.

Required Libraries (for application installation): libpcap-dev, libdumbnet-dev

Minimum Required Hardware: 2 processor cores, 2GB RAM, 60GB disk space

Network Connection: copper/fiber, port must be set to promiscuous mode

ICS/SCADA Protocols Monitored

IEC61850 GOOSE, DNP3, ModBus(beta)

All Layer 2 Traffic

Alert Format: Syslog or UDP (Depending on Installation and Integration)

Inbound Ports (at least one): sftp/scp/ssh(TCP 22)

Outbound Ports: syslog (TCP/UDP 514) (configurable for integration with Palo Alto Networks)

Setup Configuration

Baseline Timeline: Default 59 seconds (configurable by user)

Protocols Monitored: DNP#, ModBus, IEC61850 (GOOSE)

Quantity of Alert Output

Output format: syslog or other UDP

Specify monitoring interface

Ability to save violating packets to pcap file

IEC61850 GOOSE Alerts

GOOSE: INVALID GOOSE PACKET

GOOSE: MALFORMED PACKET - INVALID LENGTH

GOOSE: RESERVED BITS WRONG

GOOSE: NEW GOCBref DETECTED

GOOSE: STATE NUMBER OUT OF ORDER

GOOSE: TIME NOT UPDATED WITH STATE NUMBER

GOOSE: SEQUENCE OUT OF ORDER

DNP3 Alerts

Alerts configurable based on customer's data dictionary

DNP3: RESTRICTED OBJECT AND VARIATION COMBINATION

DNP3: RESTRICTED FUNCTION CODE

DNP3: RESTRICTED OBJECT

DNP3: RESTRICTED VARIATION

DNP3: RESTRICTED CONTROL FUNCTION CODE

DNP3: DID NOT RECEIVE FIRST FRAGMENTED PACKET

DNP3: DID NOT RECEIVE FINAL FRAGMENTED PACKET

DNP3: INVALID DATA LINK CRC

DNP3: INVALID APPLICATION CRC
DNP3: INVALID INTERNAL INDICATIONS - DEVICE TROUBLE
DNP3: INVALID CONTROL FUNCTION CODE
DNP3: INVALID FUNCTION CODE
DNP3: INVALID OBJECT
DNP3: INVALID VARIATION
DNP3: INVALID FUNCTION AND QUALIFIER
DNP3: INVALID QUALIFIER
DNP3: INVALID OBJECT-VARIATION COMBINATION
DNP3: INVALID INTERNAL INDICATIONS - DEVICE RESTART
DNP3: INVALID INTERNAL INDICATIONS - FUNCTION CODE NOT SUPPORTED
DNP3: INVALID INTERNAL INDICATIONS - OBJECT UNKNOWN
DNP3: INVALID INTERNAL INDICATIONS - PARAMETER ERROR
DNP3: INVALID INTERNAL INDICATIONS - EVENT BUFFER OVERFLOW
DNP3: INVALID INTERNAL INDICATIONS - CONFIGURATION CORRUPT

ModBus Alerts: (beta)

MODBUS: ILLEGAL FUNCTION CODE
MODBUS: ILLEGAL VALUE
MODBUS: SLAVE FAILURE
MODBUS: ACKNOWLEDGE
MODBUS: SLAVE BUSY
MODBUS: NEGATIVE ACKNOWLEDGMENT
MODBUS: MEMORY ERROR
MODBUS: GATEWAY UNAVAILABLE
MODBUS: GATEWAY TARGET FAILURE
MODBUS: INVALID MODBUS PACKET
MODBUS: READ COILS- REQUEST STARTING ADDRESS
MODBUS: READ COILS- REQUEST QUANTITY OF COILS
MODBUS: READ DISCRETE INPUTS- REQUEST STARTING ADDRESS
MODBUS: READ DISCRETE INPUTS- REQUEST QUANTITY OF INPUTS
MODBUS: READ HOLDING REGISTERS- REQUEST STARTING ADDRESS
MODBUS: READ HOLDING REGISTERS- REQUEST QUANTITY OF INPUTS
MODBUS: READ INPUT REGISTERS- REQUEST STARTING ADDRESS
MODBUS: READ INPUT REGISTERS- REQUEST QUANTITY OF INPUT REGISTERS
MODBUS: WRITE SINGLE COIL- REQUEST OUTPUT ADDRESS
MODBUS: WRITE SINGLE COIL- REQUEST OUTPUT VALUE
MODBUS: WRITE SINGLE REGISTER- REQUEST REGISTER ADDRESS
MODBUS: WRITE SINGLE REGISTER- REQUEST REGISTER VALUE
MODBUS: WRITE MULTIPLE COILS- REQUEST STARTING ADDRESS
MODBUS: WRITE MULTIPLE COILS- REQUEST QUANTITY OF OUTPUTS
MODBUS: WRITE MULTIPLE COILS- REQUEST BYTE COUNT
MODBUS: WRITE MULTIPLE COILS- REQUEST OUTPUT VALUE SIZE
MODBUS: WRITE MULTIPLE REGISTERS- REQUEST STARTING ADDRESS
MODBUS: WRITE MULTIPLE REGISTERS- REQUEST QUANTITY OF REGISTERS
MODBUS: WRITE MULTIPLE REGISTERS- REQUEST BYTE COUNT

MODBUS: WRITE MULTIPLE REGISTERS- REQUEST REGISTERS VALUE SIZE
MODBUS: READ FILE RECORD- REQUEST BYTE COUNT
MODBUS: READ FILE RECORD- REQUEST REFERENCE TYPE
MODBUS: READ FILE RECORD- REQUEST FILE NUMBER
MODBUS: READ FILE RECORD- REQUEST RECORD NUMBER
MODBUS: READ FILE RECORD- REQUEST RECORD LENGTH
MODBUS: WRITE FILE RECORD- REQUEST DATA LENGTH
MODBUS: WRITE FILE RECORD- REQUEST REFERENCE TYPE
MODBUS: WRITE FILE RECORD- REQUEST FILE NUMBER
MODBUS: WRITE FILE RECORD- REQUEST RECORD NUMBER
MODBUS: WRITE FILE RECORD- REQUEST RECORD LENGTH
MODBUS: WRITE FILE RECORD- REQUEST RECORD DATA SIZE
MODBUS: MASK WRITE REGISTER- REQUEST REFERENCE ADDRESS
MODBUS: MASK WRITE REGISTER- REQUEST AND_MASK
MODBUS: MASK WRITE REGISTER- REQUEST OR_MASK
MODBUS: READ/WRITE MULTIPLE REGISTERS- REQUEST READ STARTING ADDRESS
MODBUS: READ/WRITE MULTIPLE REGISTERS- REQUEST QUANTITY TO READ
MODBUS: READ/WRITE MULTIPLE REGISTERS- REQUEST WRITE STARTING ADDRESS
MODBUS: READ/WRITE MULTIPLE REGISTERS- REQUEST QUANTITY TO WRITE
MODBUS: READ/WRITE MULTIPLE REGISTERS- REQUEST WRITE BYTE COUNT
MODBUS: READ/WRITE MULTIPLE REGISTERS- REQUEST REGISTERS VALUE SIZE
MODBUS: READ FIFO QUEUE- REQUEST FIFO POINTER ADDRESS
MODBUS: ENCAPSULATED INTERFACE TRANSPORT- REQUEST MEI TYPE
MODBUS: ENCAPSULATED INTERFACE TRANSPORT- REQUEST READ DEVICE ID CODE
MODBUS: ENCAPSULATED INTERFACE TRANSPORT- REQUEST OBJECT ID

General Alerts (beta)

UNAUTHORIZED HOST DETECTED (beta)
NEW IP ADDRESS DETECTED (beta)
NEW MAC ADDRESS DETECTED (beta)
IP ADDRESS CHANGE FOR MAC ADDRESS (beta)
POSSIBLE MAN-IN-THE-MIDDLE ATTACK DETECTED (beta)
NEW TCP DESTINATION PORT
NEW UDP DESTINATION PORT
NEW CONNECTION - IP-PORT PAIR

Integrated Systems

Cisco FirePower
Palo Alto Networks
Splunk
ArcSight