

# Security Operations Center (SOC) and SIEM Integration

The **StationGuard** Solution provides plugins for ticketing systems, like ServiceNow, for automatically creating work tickets that respond to IDS alerts. By importing the asset inventory from StationGuard, tickets are automatically assigned to the engineer responsible for the asset or site involved in the alert.

## Access control for protecting data and networks

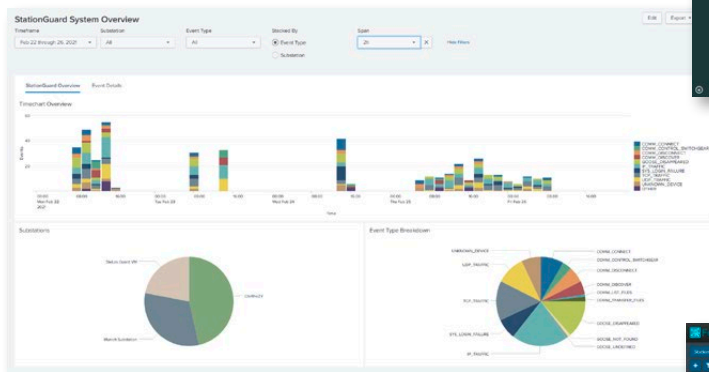
Integration into LDAP/ ActiveDirectory can be configured via the central management system. It has different user roles for controlling access to the various functions for viewing and configuring your StationGuard instances. For example, only authorized users can change the configuration or activate the Maintenance Mode. If all networks are down, StationGuard sensors can also be accessed individually using the StationGuard local client user interface.

Insider threats can be reduced and even eliminated using RBAC (Role-Based Access Control). It improves the security of the system and networks. It also enhances efficiency by minimizing the need for password changes and human error in privilege assignment.

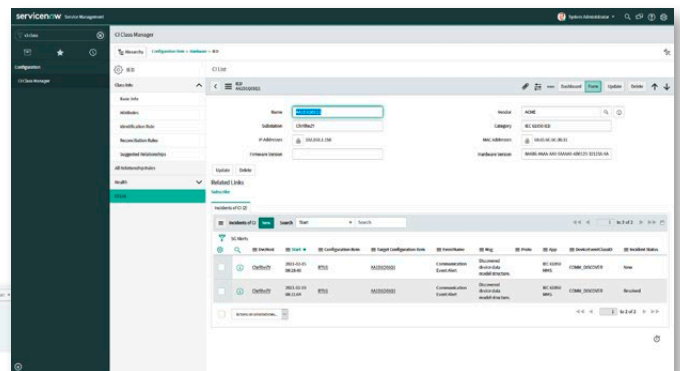
## Simple integration into your network

An effortless way to integrate StationGuard sensors into legacy systems is by using the binary outputs from the RBX1 platform. The presence of an unacknowledged alarm is signaled in the binary outputs, which can be wired to an RTU (Remote Terminal Units) and integrated into the SCADA signal list.

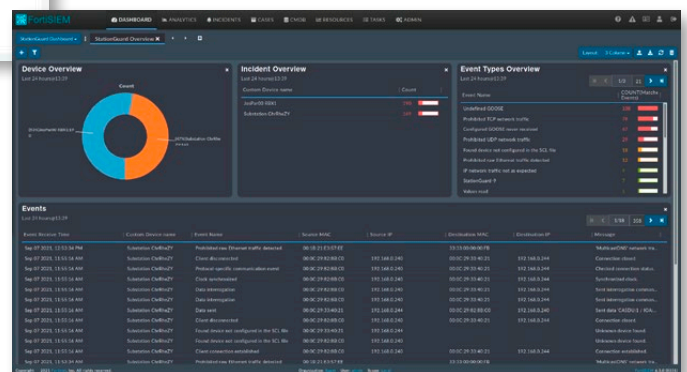
Alternatively, our easy-to-understand alert messages can also be forwarded using the syslog protocol. Various plugins are available for integrating StationGuard sensors into security information and event management (SIEM) systems and ticketing systems of different vendors.



StationGuard for Splunk App



ServiceNow integration



FortiSIEM integration