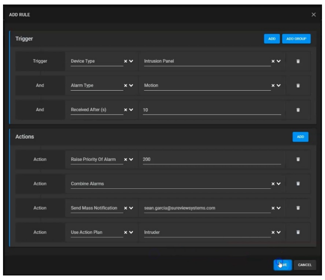
sureview

SureView Automate

CREATE UNIQUE WORKFLOWS TO AUTOMATE MANUAL OPERATIONS AND INCREASE THE EFFICIENCIES OF THE SOC

Introducing SureView Automate, an advanced rules engine for developing unique security operation workflows. Automate's intuitive user interface allows administrators to build their own sophisticated rules without the need for an engineer or developer support.



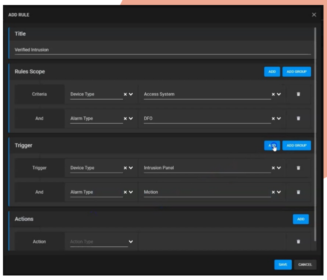
ADD RULE

Trigger

Trigger	Device Type	Intrusion Panel
And	Alarm Type	Motion
And	Received After (s)	10

Actions

Action	Raise Priority Of Alarm	200
Action	Combine Alarms	
Action	Send Mass Notification	sean.garcia@sureviewsystems.com
Action	Use Action Plan	Intruder



ADD RULE

Title

Verified Intrusion

Rules Scope

Criteria	Device Type	Access System
And	Alarm Type	DFO

Trigger

Trigger	Device Type	Intrusion Panel
And	Alarm Type	Motion

Actions

Action	Action Type	

THE CHALLENGE

Security Operations teams need to develop processes and procedures in order to respond quickly and consistently across a range of different systems, alarms, locations, and teams. Many of the steps involved are manual, so can be time-consuming and susceptible to human error.

THE SOLUTION

SureView Automate provides a simple way for security teams to build their own rules to automate common tasks in their operation. Using a simple Trigger and Actions approach, teams identify the process that will trigger their rules and then assign the actions they want SureView to automate when these occur. No development or scripting knowledge is required, administrators can build rules straight into the SureView Automate user interface.

COMMON SCENARIOS

Below are examples of some common workflows that can be built using SureView Automate.

Double Knock: *Two alarms indicate that the event is likely a 'real' intrusion*

TRIGGER
An "Intrusion" and then a "Door Forced Open" at the same location within 10 seconds

ACTION
Combine the 2 alarms into one event and present at a higher priority

Present the "Verified Intrusion" access plan to assist the operator with the correct procedure for this type of incident

Send an email notification to the shift supervisor

Debounce: *Door bounces as it closes, causing "Door Forced Open" alarms*

TRIGGER
An "Access Grant" and then one or more "Door Forced Open" alarms at the same door within 5 seconds

ACTION
Ignore the Door Forced Open alarm(s) and do not present to operators

Single Knock Ignore: *One 'unreliable' alarm by itself*

TRIGGER
A video "Motion Detected Alarm" without any further alarms at the same site within 10 seconds

ACTION
Ignore the video motion alarm and do not present to operators

Network Issue: *Offline then quickly back online*

TRIGGER
An "Offline" and then an "Online" alert on the same alarm point within 5 seconds

ACTION
Ignore both alarms and do not present to operators

Rejected Spam: *User holds up their wallet to the reader with multiple cards*

TRIGGER
One or more "Card Rejected" events around 5 seconds of an "Access Granted"

ACTION
Ignore the "Card Rejected" alarms and do not present to operators

Try Door: *A user pulls the door then realizes it needs a badge*

TRIGGER
A "Door Forced Open" and then an "Access Granted" at the same door within 5 seconds

ACTION
Ignore the "Door Forced Open" and do not present to the operator

Badge Holder Location: *A person indicating which door they're at*

TRIGGER
A number of "Access Granted" at the same door within 10 seconds

ACTION
Combine alarms events and raise the priority

Runaway: *Faulty device causing many alarms*

TRIGGER
A large number of the same alarm within 10 seconds

ACTION
Start ignoring the alarms and do not present to the operator

Send an email notification to the maintenance team