Vunetrix
Always On. Always Vigilant.

SMART Dashboard for Security Professionals
Sensor Monitoring, Alerting, and Reporting Technology

Transit
Use Case

Background
Client: Municipal Light Rail Transit Authority

Situation: Customer was responsible for ensuring the health and performance of their security environment met the demands of their clients: municipal employees, law enforcement, and operations personnel as well as transit users. They faced previous challenges in the timely identification and resolution of security devices failing due to the geographically dispersed network rooms as well as where they were positioned. What's more, environmental concerns such as heat, dust and debris, etc. caused equipment to be unstable. In addition, inefficient use of man power was employed as one dedicated resource pulled each camera stream up in succession to ensure all cameras were delivering video streams. These resources worked in three consecutive eight hour shifts around the clock. Finally, a local Systems Integrator was engaged to perform much of the day to day maintenance due to limited internal technical resources and extremely inefficient use of man power.

Goals: Use the Vunetrix SMART dashboard to detect, troubleshoot, and respond to both device and service failures in a timely manner. Ensure delivery of high quality video streams and video recordings that could be used by law enforcement when prosecuting an incident. Eliminate the use of dedicated resources to pull up cameras one by one. Instead, they desired automated alerts to be delivered when a camera went offline.

Users Internal Only
Security & Facilities

- Security Operations Center Manager - daily SMART dashboard user (in SOC)
- Security Operations Center Operators – daily SMART dashboard users (in SOC) initial triage of security device and service alerts
- Integrator Systems Technicians - SMART dashboard users in response to security device alerts
- Integrator Field Technicians - Ad Hoc SMART dashboard users in response to specific troubleshooting cases

Vunetrix Deployment

Secure Hosted Cloud

Interactions with Vunetrix System

Set up

1. Configure devices for SNMP community strings & WMI username/passwords.
2. Install remote probe software locally on a Windows boxes and connect back to hosted core server through encrypted communications.
3. Discover one device on the network per device type.
4. Create a gold standard device template per device type.
5. Discover the rest of the devices based upon the gold standard templates and place into appropriate group/container.
6. Set thresholds for alerts.
7. Configure notifications.
8. Visual SMART dashboard becomes alive with color-coded graphical representation of system wide status and performance.
9. Create daily availability report showing each device and its location.

Day to Day

1. SOC constantly logged into SMART dashboard to view real-time system status, alerts, and reports.
2. SOC operators respond to anomaly alerts that are delivered via email.
3. Login to SMART dashboard to perform high level trouble shooting.
4. Remote into each site to perform further trouble shooting and issue investigation.
5. Unresolved issues are acknowledged and referred to integrator systems technicians to perform further remote and onsite troubleshooting and/or switch/server replacement.
6. Unresolved issues are acknowledged and referred to integrator field technicians to perform further remote and onsite troubleshooting and/or edge device replacement.
7. Resolved issues are automatically updated to ok status on SMART dashboard.

Ad Hoc - Reoccurring issue diagnostics are handled via historical data queries.

Monthly - System status reports run and shared with client for SLA verification. Internal reports run for uptime metrics to municipal stakeholders.

POTENTIAL EXCEPTIONS

Monitoring Windows Servers using WMI - When a user changes the username and password on a Windows server, that server's sensors go into an error state until they are reconfigured with the correct and updated user name and password.

Probe Disconnected - When a remote probe is disconnected, an alert occurs on the SMART dashboard and via email. Locally, the probe continues to monitor devices on site. When the probe is reconnected, cached monitoring data is uploaded to the dashboard.