Municipality

Use Case

Background

Client - A large county using a pre-existing metropolitan wide area network connecting many municipal government buildings

Situation - Our client was responsible for ensuring the health and performance of their security environment met the demands of their internal clients: government employees, law enforcement, and operations personnel. They faced previous challenges in the timely identification and resolution of security devices failing due to the far-reaching network and age of devices. Siloed support teams compounded these issues as several departments owned different parts of the Security infrastructure. A lack of productive cooperation between all parties prevented timely and simplified resolutions.

Goals - Use Vunetrix's SMART dashboard to troubleshoot and respond to both device and service failures in a timely manner. In addition, ensure security devices are visible only to the appropriate support teams, eliminating finger-pointing while expediting resolution to support a SLA for their internal customers.

Users Internal Only

Security & Facilities

- Security Program Manager - daily SMART dashboard user (in SOC)
- Security Systems Technicians - SMART dashboard users in response to security device alerts
- Security Field Technicians - Ad Hoc SMART dashboard users in response to specific troubleshooting cases

Information Technology

IT Systems Technicians - SMART dashboard users in response to IT device alerts

Vunetrix Deployment

On Premise Licensed

Interactions with Vunetrix System

Set up

1. Configure devices for SNMP community strings & WMI username/passwords.
2. Install and configure local core with appropriate license.

3. Install remote probe software locally on a Windows box and connect back to local core server through encrypted connection.
4. Create user groups unique to Security, Facilities, and IT Operations Teams.
5. Discover one device on the network per device type.
6. Create a gold standard device template per device type.
7. Discover the rest of the devices based upon the gold standard templates and place into appropriate group/container.
8. Assign appropriate access rights for various groups to be able to manage their own parts of the security network.
9. Set thresholds for alerts.
10. Configure notifications.
11. Visual SMART dashboard becomes alive with color-coded graphical representation of system wide status and performance.

Day to Day

1. SOC constantly logged into SMART dashboard to view real-time system status, alerts, and reports.
2. Security systems technicians and IT systems technicians 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 Security field or IT systems technicians to perform further onsite troubleshooting and/or device replacement.
6. Resolved issues are automatically updated to ok status on SMART dashboard.

Monthly

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

Ad Hoc

Reoccurring issue diagnostics are handled via historical data queries.

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.