Electronic Guard Tour System

White paper

CONFIDENTIAL

Copyright and Statement of Conditions Page

Overview

What is SOVA?

SOVA is an online, browser-based security management service that runs on the Internet and can be accessed from any location that provides secure internet access. Security officers using the SOVA system carry Android handheld devices to conduct property tours and record activities onto their devices. When necessary, the SOVA app sends this data to our secure data center via WiFi.

SOVA:

- Allows for tracking of security officer activities for single or multiple facilities from remote locations with no software installation on any computer with internet access
- Generate DAR's (daily activity reports) by user, shift, or day
- Review tour reports showing points missed, graphs of how routes were completed, incident reports etc. from your handheld device or from the web interface
- Lone-worker protection feature adds a measure of safety by detecting when an officer's mobile device stops moving or a fall is detected allowing emergency personnel to quickly respond with help
- Comprehensive visitor and package management modules available

Business Case for Customers:

- Monthly registration fees are more affordable than software license fees; registration includes automatic upgrades and new releases system-wide, without operational interruption
- Reports can be run at any time, remotely or locally for review purposes
- Officer trend analysis and historical tracking across facilities
- Requires little training, and system-wide implementation can be completed in 1-2 days

Maintaining Data Security and Integrity for SOVA

Overall Security

SOVA Systems currently has two employees dedicated to network / data security - the System Administrator and the Senior Software Developer. All SOVA Systems employees must pass criminal background checks and drug screening processes.

The SOVA application is hosted at a state-of-the-art Incero Datacenter in Dallas Texas. Incero provides:

- 24x7x365 security
- Continuous closed circuit video surveillance
- Electronic card key access
- "Man Trap" with Biometrics and Personal Access Cards
- Redundant A, B, C and D power via four 750 KVA UPS systems
- Three 1.5 MW Cummins generators (N+1)
- Dry pipe fire detection and suppression
- Four 500-ton Trane chillers with redundant water mains

Data is stored in MySQL databases and is replicated between MySQL instances. This data redundancy allows for automatic recovery from a failure of the master server with loss of less than one-minute of data. Additionally, full backups of the master database are taken every night and kept for seven days. These backups are stored separate from internet facing servers and are also transferred daily via secure

FTP (SFTP) and stored in a secondary facility yielding two complete sets of rolling backups housed at distinct facilities.

Administrative access to servers is limited to the Senior Software Developer and the System Administrator and requires the utilization of Secure Shell (SSH) and 2048 bit SSH-2 RSA public/private key pairs. Firewalls are configured to demand a valid certificate before allowing a use of any protocol other than HTTPS.

As software and operating system patches become available, they are immediately applied to SOVA staging servers. Patches are tested on staging and then installed on production servers.

Network and Server Security

HTTPS traffic is allowed and monitored. HTTP access is prohibited to secure areas of the application. All requests and responses are scanned by a managed firewall for signatures indicating malicious code or unauthorized use. Several technologies are employed to provide reliable service and secure data storage for SOVA customers. Firewalls, encryption, SSH with secure tunnels and other security measures are employed to authenticate and monitor administrative access. Intrusion Detection and Prevention System (IDPS) software runs on the firewalls and is monitored 24x7x365.

Virus Protection software is also running on all servers within the datacenter. Updates are installed automatically and scans are scheduled for every evening. Tamper protection is enabled to prevent changes from being made without proper authentication. Email alerting is configured to alert both the Senior Software Developer and System Administrator of any potential security threats.

SOVA Systems conducts regular security audits and code reviews to detect potential vulnerabilities before they are exploited. The security audits are performed weekly during off peak hours and following any code and/or configuration changes. Code reviews are conducted on staging servers subsequent to non-html modifications and prior to production rollout. A security audit tool with the most up-to-date vulnerability knowledgebase and an intelligent scanning engine is utilized to ensure protection of all internet facing devices. Some of the elements audited include:

- DNS and Bind
- Back Doors and Trojans
- Brute Force Attacks
- CGI
- File Transfer Protocol
- Firewalls
- General Remote Services
- Hardware and Network Appliances
- Information/Directory Services
- SMB/NetBIOS Windows File Sharing
- SMTP and Mail Applications
- Databases
- eCommerce Applications
- SNMP
- TCP/IP
- Web Servers

The following vulnerabilities, at a minimum, will be scanned prior to any non-html code updates.

- Cross-site Scripting
- Parameter Tampering
- Hidden Field Manipulation
- Backdoors and Debug Options
- Stealth Commanding
- Forceful Browsing
- Application Buffer Overflow
- Cookie Poisoning
- HTTP Attacks
- SQL injection
- Suspicious Content

If a potential vulnerability is detected, the audit application will notify the System Administrator. The System Administrator will immediately determine the cause of the fault and appropriate resolution. Any network or software modifications that produce or immediately precede an unacceptable audit are rolled back. Potential vulnerabilities will be responded to immediately and closed within 2 hours.

Protection of Client Data

The application is hosted at the Incero data center in Dallas Texas. Personnel at the Incero facility do not have access to client data. Incero solely provides bandwidth and the secure data storage facility. Only two SOVA Systems employees have administrative access to client data. No vendors, partners, or third parties have access to client data.

The SQL Server records SQL logs of each transaction on the production servers. Automated reports and audit trails can be developed around the clients specific needs.

Authentication

Two factor authentication in the form of username/password combination as well as a scan of the users unique, physical RFID keyfob is required before access is granted to SOVA. When possible, authentication of user's proxy IP address is also requested.

The passwords are encrypted as they pass through the internal SOVA network. Additionally, the servers use HTTPS with 2048-bit encryption over SSL. Usernames and encrypted passwords are stored in replicated SQL Server databases, on a secure subnet in the datacenter and is remotely accessible only via SSH by the System Administrator and Senior Software Developer.

Upon request, customers have the option to configure an encrypted VPN directly to the SOVA network and/or use Single Sign-On (SSO) for authentication. SSO will bypass the use of a username and password for authentication to SOVA, using a 'Global ID' of a user for example to gain access to SOVA without requiring a secondary sign-on.

Audits

Our datacenter at Incero is SSAE16, PCI & HIPAA compliant. Datacenter reports are available upon request.

Datacenter Connectivity and Reliability

Our application and network topology have been designed from the ground up to be reliable and secure.

Some highlights:

- Hosted in a secure Incero datacenter with 24 hour staff, video surveillance and redundant power
- Web server traffic is distributed across a cluster to protect against a server failure
- IDPS with 24x7x365 monitoring on firewalls
- Multi-homed network with multiple 10 Gigabit connections
- Redundant Juniper routing with multiple 10gig uplinks
- Border Gateway Protocol (BGP4)
- HSRP failover protection
- Carrier neutrality utilizing multiple providers
- Automated IPMI/KVM firewall
- QualysGuard product used to test network security and for web application scanning
- Security vulnerability scanning done regularly to monitor for threats
- Code review performed at each major change to code

Technical Specifications

Infrastructure:

Linux server running Apache and PHP 5.5

Virtualization Technology:

OpenVZ

Node specs:

Dual Intel Xeon E5 or Xeon Westreme CPUs

384GB DDR3 RAM

8 x 10K RPM HDDs RAID10 or 8 x SATA3 SSD RAID10 or 8 x 7200 RPM HDDs RAID10 + 4 x 240GB SSD RAID10 for caching

Operating System:

CentOS with MySQL

OpenVPN (available)

Server IP Address:

162.213.195.51 (dedicated)

SOVA Functionality and Customization

SOVA can be easily customized to meet a customer's needs by requesting the addition of new features. We are continually enhancing SOVA by adding more functionality and increasing usability. Many

features added to SOVA are free to customers. If a client were to have specific requirements, we would be happy to discuss them. Depending on the specifics, there may be a one-time charge for customization work to be done to the application.