CAMPUS SECURE+

Powered by CorePLUS TECHNOLOGIES

Reference Architecture for Real-Time School Safety, Asset Tracking with Situational Awareness Dashboard and Managed IT Security

Executive Overview

This reference architecture outlines a comprehensive real-time safety and monitoring solution for educational institutions, now enhanced by Managed Security Services Provider (MSSP) capabilities. In addition to leveraging Bluetooth Low Energy (BLE), WiFi, and mobile technologies, the architecture now integrates MSSP functions to deliver 24/7 threat monitoring, incident response, compliance support, and advanced analytics. MSSP integration ensures not only situational awareness but also proactive cybersecurity protection, regulatory compliance, and business continuity.

This reference architecture outlines a comprehensive real-time safety and monitoring solution for educational institutions. It leverages Bluetooth Low Energy (BLE), WiFi, and mobile technologies to provide location-based information for students, teachers, and first responders, along with mobile panic buttons, mobile incident reporting, and facility lockdown capabilities. It introduces the ability to categorize and monitor specific student populations (e.g., bullies, special needs, high-risk students), apply Geo-fencing alerts for elopement risks, track high-value assets, and monitor both registered and unregistered visitors or intruders. The solution also features a real-time dashboard to enhance situational awareness and support decision-making in critical scenarios.

Key Components

Security Operations Center (SOC) as a Service

- A remote MSSP-powered SOC continuously monitors network and endpoint activity across the school's environment, ensuring early detection of anomalies and threats.

Threat Detection & Incident Response

- MSSP tools use machine learning, threat intelligence, and behavior analytics to detect malicious activity such as unauthorized access attempts, lateral movement, and suspicious device behavior. Automated or MSSP-assisted incident response reduces response time.

Vulnerability Management

- Continuous vulnerability scanning and patch management services identify and mitigate weaknesses across connected systems (e.g., BLE infrastructure, mobile devices, access points).

Endpoint Detection and Response (EDR)

- MSSP agents installed on mobile and administrative devices protect against malware, ransomware, and phishing attacks targeting students, faculty, and infrastructure.

Compliance Monitoring & Reporting

- MSSP tools track activity relevant to FERPA, HIPAA (if applicable), and local school safety laws, and generate audit-ready reports that demonstrate adherence to data privacy and protection policies.

Location Tracking (BLE & WiFi)

BLE beacons and WiFi access points are installed throughout the campus to triangulate the position of students, staff, visitors, and assets in real-time.

Location Tracking (BLE & WiFi)

BLE beacons and WiFi access points are installed throughout the campus to triangulate the position of students, staff, visitors, and assets in real-time.

Mobile Panic Buttons

Mobile panic buttons on staff smartphones or wearable devices allow for instant distress signals, triggering alerts to first responders and campus security.

Mobile Incident Reporting

An integrated mobile app enables teachers and students to report incidents in real-time, documenting details like the type of incident, location, and people involved.

Full Facility Lockdown

The system supports mobile-triggered facility lockdown capabilities, ensuring immediate response during emergency situations like active shooters.

Student Categorization

The platform allows for the categorization of students into distinct groups, such as:
Bullies
Special needs students - Students with health issues Categorization is enhanced by a scoring system for high-risk students, dynamically adjusted based on incident reports and behavior.
Geo-Fencing and Elopement Risk Alerting - The system includes Geo-fencing capabilities to monitor specific categories of students, such as those at risk of elopement. Alerts are triggered when high-risk students (based on scores) leave designated safe zones, allowing for immediate response.
User/Visitor Registration with Biometrics & DL Scanning - The solution allows for the registration of users, visitors, and vendors using biometric identification (e.g., fingerprints or facial recognition) or driver's license (DL) scanning. This ensures that all campus entrants are properly logged and identified for security purposes.
Registered and Unregistered User Visibility - The platform provides visibility into both registered and unregistered/ intruder users depending on the existing infrastructure. Using BLE, WiFi, and biometric data, the system distinguishes between authorized users and potential intruders, alerting security teams when unregistered devices or individuals are detected.
Asset and Inventory Tracking - BLE tags are affixed to high-value assets, providing real-time tracking and monitoring across the facility, helping reduce theft and loss.

Architecture Overview

SIEM Integration:

All logs and alerts from BLE, WiFi, mobile apps, and dashboards are forwarded to a Security Information and Event Management (SIEM) platform managed by the MSSP. This centralizes security visibility.

Automated Correlation Engines:

The MSSP applies correlation rules to detect patterns (e.g., repeat elopement with concurrent access anomalies) and trigger alerts or automated remediation workflows.

Secure Cloud Hosting & Threat Intelligence Feeds:

MSSP-managed cloud infrastructure hosts critical data and receives real-time threat updates from global feeds to improve risk scoring and incident prioritization.

Security Heatmaps & Alerts:

MSSP dashboards layer cybersecurity heatmaps onto physical campus views, visualizing both physical and cyber threats.

Anomaly Detection:

MSSP systems detect outlier behaviors (e.g., an intruder's device mimicking a staff BLE ID) and escalate them for investigation.

Facility Lockdown Control:
The dashboard allows manual or automated lockdown in response to security threats, with real-time monitoring of secured versus unsecured areas.

Student Risk and Behavioral Scores:
The dashboard displays real-time risk scores for flagged students, allowing security personnel to monitor high-risk individuals and take preemptive action.

Decision Support and Analytics:
Built-in decision support tools provide suggested actions, evacuation routes, and heatmaps for areas requiring additional attention or staffing.

Geo-Fencing Alerts:
The dashboard displays Geo-fencing zones for high-risk students. Alerts are triggered when students with high elopement risk leave safe zones, and administrators are immediately notified for rapid intervention.

Registered User Monitoring:
The dashboard continuously monitors registered users (students, staff, visitors, vendors) and unregistered/intruder users based on BLE and WiFi signals.

Asset Tracking and Alerts:
High-value assets are tracked in real-time, with notifications for unusual movements (e.g., assets leaving designated areas). Inventory reports can be generated to optimize asset management.

Security and Compliance Considerations

MSSP-Backed Policy Enforcement:
Centralized enforcement of security policies across all campus devices and users (BYOD, IoT, and mobile) is ensured by MSSP platforms.

Real-Time Threat Monitoring:
MSSPs monitor all network traffic and asset activity to detect intrusions, rogue devices, and unusual user behavior—integrated with situational awareness dashboards.

Managed Identity & Access Control:
MSSP manages federated identity systems with multi-factor authentication, restricting access to sensitive systems and incident data.

Audit Logs & Reporting:
All security incidents and responses are logged with tamper-proof audit trails maintained by the MSSP. Reports are automatically generated for administrative and legal review.

Access Control and Encryption

Role-based access control ensures that only authorized personnel can access sensitive location and incident data. All data is encrypted both in transit and at rest, ensuring compliance with student privacy laws (e.g., FERPA).

Incident Audit Logs:
Comprehensive logs of all incidents, alerts, and lockdown events are maintained to ensure accountability and compliance with school safety standards.

Biometric and DL Scanning Security:
All biometric and driver's license data is handled securely, with encrypted storage and limited access to ensure compliance with privacy regulations.

Ensuring Safety and Business Continuity

24/7 MSSP Monitoring:
Around-the-clock monitoring from the MSSP ensures no event goes unnoticed—whether it's a cyber breach attempt or suspicious behavior on campus.

Disaster Recovery and Backup Services:
MSSP provides cloud-based backup and disaster recovery plans for all critical data and systems, ensuring rapid recovery in the event of a cyberattack or system failure.

Proactive Risk Posture Management:
Regular MSSP assessments and threat modeling help identify risks before they can be exploited, supporting continuous improvement of the security architecture.

Redundancy & Failover:
The architecture includes redundancy in both the data storage and communication layers, ensuring uninterrupted operation during network outages.

High Availability:
Leveraging cloud-based infrastructure ensures scalability and high availability, allowing the system to handle the needs of large school districts or university campuses.

This reference architecture presents a robust solution for enhancing safety, monitoring, and incident response in educational environments. By integrating BLE and WiFi technologies with mobile panic buttons, incident reporting, asset tracking, and a real-time situational awareness dashboard, educational institutions can take proactive steps to safeguard their students, staff, and assets. The dashboard provides a crucial decision-making tool for administrators and security personnel, ensuring informed and timely responses to any situation.

Generate: Data Collection Layer

BLE Beacons & WiFi Access Points:
BLE beacons and WiFi access points collect real-time location data from wearable devices and smartphones across the campus.

Mobile Devices & Wearables:
Students, teachers, and staff are equipped with mobile devices or BLE-enabled wearables that continuously send location data to the network.

Panic Buttons & Incident Reporting App:
Mobile applications on teachers' and administrators' smartphones serve as panic buttons and provide an interface for reporting incidents in real-time.

Ingest: Data Integration Layer

API Gateway:
An API gateway integrates real-time data from BLE beacons, WiFi access points, and mobile devices into the backend system.

Data Transformation and Normalization:
The incoming data is standardized and normalized to ensure it can be processed for real-time tracking and incident reporting.

Incident Categorization & Scoring Algorithm:
A built-in algorithm categorizes students based on behaviors and incidents, applying scores to assess risk levels for individuals flagged as high-risk.

Persist: Data Storage and Processing

Real-Time Database (e.g., Azure Data Services):
All location data, incident reports, and asset tracking information are securely stored in a scalable, real-time database for ongoing monitoring and future analysis.

Asset Tracking Platform:
The system stores information about high-value assets, linking BLE tags to specific inventory items.

Historical Incident Logs:
The platform logs historical data on incidents, facility lockdowns, and panic button activations to assist with compliance and investigations.

Situational Awareness and Decision Support Dashboard

Real-Time Monitoring:
The dashboard provides live updates on the location of students, teachers, staff, visitors, and high-value assets across the campus in an intuitive map view. It identifies movement patterns and detects intruders, offering complete campus situational awareness.

Panic Button Activation Alerts:
When a panic button is pressed, the dashboard instantly highlights the exact location of the user, triggering visual and audio alerts for security personnel.

Incident Reporting and Status Updates:
Real-time incident reports are submitted via the mobile app and logged on the dashboard, with details such as the incident type, location, and individuals involved.