AI Threat Detection in Visium's Campus Security Solution with IREX's ELI

Under Visium Technologies, in partnership with IREX.AI, the Ethical Layered Intelligence (ELI™) framework integrated with TruContext™ provides advanced AI-driven threat detection for campus environments like Brown University. This system transforms passive video surveillance into proactive, real-time intelligence, addressing gaps exposed by the December 13, 2025, shooting at Brown's Barus & Holley building. By fusing AI analytics with ethical governance, it enables early threat identification while prioritizing privacy and trust.

Core Mechanisms of AI Threat Detection

The AI threat detection operates through a multi-layered architecture that processes video feeds and sensor data in real time. At its foundation, ELI ingests data from cameras, access controls, and other sources, normalizing it for analysis. TruContext then correlates these streams, applying contextual scoring to differentiate benign activities from potential risks.

Key detection processes include:

- **Object Detection and Classification**: AI-assisted scene interpretation identifies threats like weapons or suspicious objects. Using computer vision models, the system tags and classifies elements in video frames, such as detecting a firearm or unattended bag.
- **Behavioral Analytics**: Algorithms monitor for abnormal motion patterns, like erratic movements or loitering in restricted areas, and crowd behavior anomalies, such as sudden gatherings or dispersal indicative of panic.
- **Predictive Insights**: Beyond reactive detection, AI analyzes patterns to forecast risks, such as escalating crowd density leading to potential unrest.
- **Real-Time Processing**: Detections occur within seconds via low-latency AI inference, triggering automated alerts to dispatch centers or mobile devices for immediate response.

This integration allows for sub-second threat identification, turning raw data into actionable intelligence without requiring constant human monitoring.

Artificial intelligence-driven cybersecurity system for internet of things using self-attention deep learning and metaheuristic algorithms | Scientific Reports

Integrated Architecture Supporting Detection

The solution couples IREX's ELI with Visium's TruContext for seamless operation:

- **Sensors & Inputs Layer**: Ingests video from ~1,200 cameras at Brown, plus multi-modal data like access logs and motion sensors.
- **AI Analytics Layer**: Performs real-time threat analysis, including object detection, tagging, and event correlation using graph-based analytics to link cameras, objects, and alerts.
- **Response & Coordination Layer**: Generates automated dispatch alerts, escalating prioritized incidents to public safety staff.
- **Reporting & Insights Layer**: Provides predictive security insights and audit trails for post-event review.

Standards-based connectors (e.g., RTSP, ONVIF) ensure compatibility with existing VMS, enabling retrofitting without hardware overhauls. For Brown, this includes unified ingestion from card access systems and real-time alerts via the 800 MHz radio network.

AI-driven cybersecurity framework for software development based on the ANN-ISM paradigm | Scientific Reports

Ethical Safeguards in AI Detection

Visium and IREX embed ethics at every level to ensure responsible use:

- **Privacy-by-Design**: Analytics focus on events and patterns, avoiding persistent identity tracking unless justified (e.g., during an active threat).
- **Bias Mitigation**: Continuous model evaluation prevents discriminatory outcomes across demographics, with stewardship processes to maintain fairness.
- **Policy-Driven Controls**: Role-based access and governance ensure compliance, logging every alert and access for accountability.
- **Audit and Redaction**: Time-stamped trails support transparency, with tools for redacting sensitive data in forensic reviews.

These features make the system suitable for academic settings, balancing safety with civil liberties.

Use Cases and Benefits for Campus Threat Detection

- **Active Threat Scenarios**: Detects weapons or unusual behaviors in real time, alerting 65+ public safety staff at Brown to minimize latency—potentially reducing response times by 40%.
- **Situational Awareness**: Dashboards fuse video with logs and alerts, offering a comprehensive view for proactive intervention.
- **Forensic and Efficiency Gains**: Automated tagging speeds investigations, reconstructing timelines swiftly while reducing false alarms.
- **Proven Impact**: At peer institutions, similar deployments achieved 40% fewer critical incidents, 30% faster responses, and 95% positive feedback. For Brown, projections include 35% more proactive prevention and 50% operational efficiency gains.

AI-Driven Anomaly Detection for Securing IoT Devices in 5G-Enabled Smart Cities

Implementation Considerations

Scalable from single buildings (e.g., Barus & Holley pilot) to full campuses, the system handles thousands of feeds with minimal latency. A 90-day roadmap for Brown starts with assessment, moves to pilot in areas like Keeney Quad, and ends with rollout and training. This ethical, AI-powered approach under Visium with IREX/ELI empowers universities to act swiftly and responsibly, enhancing community trust in safety infrastructure.