

City Of Danville & Wazuh: Strengthening Municipal Cybersecurity



Executive Summary

The City of Danville (Illinois) supports critical public services including Police, Fire, Public Works, Finance and Administration. Protecting sensitive citizen data and essential infrastructure required a centralized, cost-effective cybersecurity approach aligned with regulatory standards. As log data remained distributed across multiple systems, correlating activity and responding to threats became increasingly difficult. The City needed structured monitoring, stronger compliance capabilities and improved visibility without exceeding municipal budget constraints.

Challenge

The City of Danville faced:

- Dispersed event logs across multiple systems
- Limited correlation between security events
- Slow response threats such as ransomware and credential misuse
- Compliance requirements under CJIS, NIST CSF and CIS Controls
- Budget limitations restricting access to traditional SIEM platforms

They required a unified platform capable of delivering real-time visibility, endpoint monitoring, vulnerability detection and audit-ready reporting.

Solution

Wazuh was chosen to centralize security monitoring and strengthen compliance management within a single, cost-effective platform. With Wazuh, the City of Danville now:

- Centralizes log collection across servers and workstations
- Correlates activity across its entire environment
- Detects suspicious authentication attempts and abnormal processes
- Monitor PowerShell execution
- Identifies high-risk vulnerabilities
- Enforces configuration baselines
- Receives MITRE ATT&CK-mapped alerts

This implementation enabled a transition from reactive security practices to a structured and proactive SOC workflow.



Agnel DSilva
CTO, City of Danville

"Wazuh gave us the visibility and control we needed to proactively monitor our environment, strengthen compliance, and detect threats early — all within a cost-effective platform that fits a municipal budget."

Use Cases



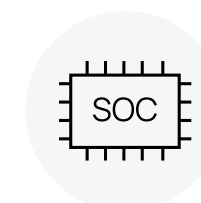
Security monitoring



Compliance reporting and audit preparation



Vulnerability management



SOC workflow enablement



Log analysis

City Of Danville & Wazuh: Strengthening Municipal Cybersecurity



Results

The City of Danville achieved:

- Real-time visibility across its environment
- Faster detection and investigation of security incidents
- Improved vulnerability identification and risk-based remediation
- Stronger compliance posture with audit-ready reporting
- Consolidation of multiple tools into a unified platform

They moved from fragmented monitoring to coordinated, proactive security operations while maintaining financial sustainability.

Key Benefits

- Centralized log visibility and correlation
- File integrity monitoring and configuration assessment
- Vulnerability detection with prioritized remediation
- Real-time threat detection aligned with MITRE ATT&CK
- Compliance support for CJIS, NIST CSF and CIS Controls

About The City of Danville

Industry

Municipal Government

Services

Public safety, public works, administrative and financial services

Location

Illinois, United States

The City of Danville provides essential public services across multiple departments while safeguarding critical infrastructure and sensitive citizen information.