Wazuh Case Study

Scalable Cybersecurity for a Dynamic City: How Los Angeles ITA-ISOC Optimized Operations with Wazuh Cloud

ITA | INFORMATION TECHNOLOGY AGENCY
CITY OF LOS ANGELES

About the City of Los Angeles Information Technology Agency (ITA)

The Information Technology Agency (ITA) of Los Angeles manages a diverse range of services for both internal and external stakeholders, with an annual budget of $90 million. Their responsibilities span from traditional IT services, such as computer support, enterprise applications, data networks, and a 24/7 data center, to advanced digital services like LA Cityview TV, the 3-1-1 Call Center, public safety communications, helicopter avionics, and enterprise social media.

Collaborating with various agencies and departments across Los Angeles, the ITA aims to develop a robust IT infrastructure and applications, providing citizens, businesses, and visitors with essential digital services. One of the ways that the ITA helps secure those applications is through the Integrated Security Operation Center or ITA-ISOC, which is a subdivision of the ITA.

Cybersecurity Approach

With over 40 departments, each with its own Infrastructure, the ITA-ISOC faced a significant challenge in managing cybersecurity across the city. Departments range from large entities like the Department of Power, the Port of Los Angeles, and Los Angeles World Airports to smaller ones like the Department of Neighborhood Empowerment and the Department of Aging.

To address these challenges, the ITA-ISOC turned to Wazuh Cloud. This solution enabled the agency to collect logs at scale, particularly focusing on Windows events, which streamlined the management and maintenance of servers and infrastructure across Los Angeles. The visibility provided by Wazuh Cloud allowed the ITA-ISOC to collaborate closely with larger departments when unusual activities were detected. They developed custom rules for specific event channels of interest, covering use cases like Google Password Sync, Netscaler, and integrations with Azure, GCP, GitHub, AWS, BitLocker, and SysMon.

Wazuh Cloud also complements the city's existing security tools, adding additional layers of protection. By collecting logs from Windows Defender and their EDR, the ITA-ISOC can detect bypasses or tampering without needing to individually access each endpoint. This scalability and flexibility are crucial for the ITA-ISOC operations.

Their objectives are twofold:

1. Integrate all security personnel throughout the city, consolidating logs, telemetry data, alerts, investigations, and incidents, and sharing this information across departments.
2. Ensure a minimum level of cybersecurity for smaller departments.

Joanne Scott
ITA LA
Primary Administrator

"I personally love the flexibility of Wazuh because, as a Sysadmin, I can think of any use case and know I'll be able to use Wazuh to pull in the logs and create the alerts that I need."

Why Wazuh

- Scalability for Log Collection
- Flexibility
- Support

Scalable Cybersecurity for a Dynamic City: How Los Angeles ITA Optimized Operations with Wazuh Cloud

ITA | INFORMATION TECHNOLOGY AGENCY CITY OF LOS ANGELES

Why Wazuh

- **Scalability for Log Collection:** Wazuh enables easy scalability to monitor additional devices as needed, maintaining oversight across departments with minimal hassle.
- **Flexibility:** Wazuh's ability to collect logs for specific use cases allows for the creation of tailored alerts and rules.
- **Support:** The ITA-ISOC values their relationship with the Wazuh team, noting their quick responses and above-average support, which aids in resolving challenges swiftly.

Achievements and Work in Progress

- **New Emerging Threats Detection:** Wazuh enabled the ITA-ISOC to identify and respond to new security threats within hours, significantly reducing detection times.
- **Custom Rules Deployment:** Custom rules can be deployed across 40+ departments in minutes.
- **Use Case Applications:** Wazuh's blog posts have been instrumental in helping the ITA-ISOC identify new use cases, saving time and resources by avoiding the need to reinvent solutions.

About Wazuh

Wazuh is a free and open-source security platform that combines XDR and SIEM capabilities to protect workloads across on-premises, virtualized, containerized, and cloud-based environments. With over 20 million downloads annually, it supports one of the largest open-source security communities globally.

Organizations of all sizes use Wazuh to collect, aggregate, index, and analyze security data, aiding in the detection of intrusions, threats, and behavioral anomalies.

Achievements

1

Wazuh enabled the ITA to identify and respond to new security threats within hours, significantly reducing detection times.

2

Custom rules can be deployed across 40+ departments in minutes.

3

Wazuh's blog posts have been instrumental in helping the ITA identify new use cases, saving time and resources by avoiding the need to reinvent solutions.