Wazuh Case Study

Securing Energy Infrastructures: Wazuh's Role in Enevo's OT Cybersecurity Strategy

Cybersecurity approach

In its early stages, Enevo Cybersec had been delivering IT and cybersecurity to Enevo Group for their energy infrastructure projects, which included hydropower plants, renewable photovoltaic parks, dispatch centers for renewable energy, and electrical substations. Their focus was on ensuring the optimal functioning of underlying IT systems to facilitate smooth automation of industrial processes.

Drawing from their extensive experience in this domain, they recognized a market need for a platform that could enhance cyber resilience and provide situational awareness in cybersecurity, particularly targeting Industrial Control Systems, also known as Operational Technology (OT). Their solution involved gathering comprehensive security telemetry from various sources such as electrical substations and automation systems, and feeding this data into a Security Information and Event Management (SIEM) engine. This is where Wazuh played a crucial role.

Prior to implementing Wazuh, their primary challenge lay in correlating and consolidating data to generate actionable alerts. Although they explored other solutions, none matched the flexibility, complexity, and proven track record of Wazuh. The versatility of Wazuh's agents allowed them to gather telemetry not only from workstations but also from diverse applications, while its capability to receive information from different sources via Syslogs further enhanced its utility. Additionally, they leveraged the MITRE Framework to fortify their configurations and overall security posture.

> “The solid experience on the fundamentals of a SIEM engine, and the flexibility offered with the agents is what made us trust in Wazuh as a long-term Strategic Partner.”
>
> Alexandru Suditu
> Co-founder and General Manager

Why Wazuh

1. **Agents flexibility:** The ease of use and the possibility of installing them on almost any device, make the agents an important ally in consolidating information and increasing the scope of OT Cybersecurity.

Alexandru Suditu
Co-founder
and General Manager
Enevo Cybersec

"The solid experience on the fundamentals of a SIEM engine, and the flexibility offered with the agents is what made us trust in Wazuh as a long-term Strategic Partner”

Key benefits

- Agents Flexibility
- Solid SIEM engine
- Open Source nature and trajectory

2. **A solid SIEM engine:** Wazuh's great foundations built through many years of improvement and evolution, transformed them into a consolidated SIEM platform, generating trust among its users.

3. **Open Source nature:** As an Open Source solution, the software receives constant feedback from its community and its users around the globe, allowing Wazuh to consistently evolve at a fast pace, and focus on generating value.

About Enevo

An interdisciplinary team of Cyber Security Experts, Automation Engineers, and DevOps trained to solve any Energy Cyber Security challenge. They developed subSIEM, a platform that enhances the security posture of energy infrastructures by providing immediate situational awareness to all stakeholders involved in a Cyber Security Incident. This ensures Incident Response and Disaster Recovery times are reduced to their absolute minimum.

The platform collects all the information needed by an Incident Response team to investigate or perform threat-hunting activities. This includes full network visibility, device and application logs, up-to-date asset inventory, and an accurate network topology of the OT network.

About Wazuh

Wazuh is a powerful, free and open-source security platform designed to enhance cybersecurity across endpoints. It serves as a comprehensive solution, integrating Extended Detection and Response (XDR) capabilities with Security Information and Event Management (SIEM) functionalities to safeguard endpoints and cloud workloads effectively.

Its open-source nature allows organizations to customize and extend its capabilities to meet their specific security needs, ensuring adaptable defense strategies against evolving threats. With over 20 million downloads per year, it has one of the largest open-source security communities in the world.

Achievements

1. Development of their Graphic Interface focused on the Cybersecurity Analysis for the Energy Industry.

2. Wazuh's fast development and evolution have allowed them to grow their project at the same speed.

3. Their efficiency and management improved thanks to a Kubernetes architecture migration with Wazuh's assistance.