Wazuh Case Study

Achieving Proactive Defense

UNIVERSITY OF CHICHESTER

How Wazuh Transformed Cybersecurity at the University of Chichester

The University of Chichester, located in West Sussex, England, is renowned for its student-centered approach to education across arts, humanities, social sciences, and sciences. Emphasizing practical learning and industry connections, it fosters a supportive community for students to excel.

Cybersecurity Approach

The University of Chichester embarked on a cybersecurity enhancement initiative to fortify their defenses against threats. While their existing security architecture focused on perimeter defense, they lacked comprehensive visibility into network activities, hindering their ability to assess the effectiveness of these defenses.

This prompted a search for a solution that could centralize log management and facilitate easier analysis during potential security incidents, eliminating the need for manual log review across different sources. After evaluating several proofs of concept, they selected Wazuh based on critical factors:

1. Effective Ransomware Detection: Wazuh uniquely detected ransomware that had evaded detection during previous proof of concepts.

2. Simplicity and Customization: Unlike other solutions requiring specialized hardware and ex tensive machine learning efforts to mitigate false positives, Wazuh offered excellent support and customizable integrations that minimized administrative tasks.

Following implementation, with support from the Wazuh team, the university successfully centralized logs from different sources. They now aim to expand Wazuh's coverage across additional systems, including integration with PowerBi. Presently, they monitor three Azure tenancies and utilize Azure Sentinel, alongside integrations with Mimecast, Signal4, Shuffle, and Hive.

Haydn Tarr
IT Service Development Manager
University of Chichester

"Wazuh was a crucial factor in our journey to gain deeper insights into our internal network activities"

Why Wazuh

- Support
- Ransomware detection
- Ease of use

Why Wazuh

- **Tailored Customization and Support:** Wazuh's flexibility allowed the university to configure the tool to meet specific use case requirements with expert support.
- **Critical Ransomware Detection:** Wazuh's ability to detect ransomware in real-time proved instrumental during their evaluation phase and continues to be a cornerstone of its value proposition.
- **Ease of implementation:** Compared to alternatives, Wazuh required minimal setup to achieve significant security improvements, enhancing operational efficiency.

About Wazuh

Wazuh is a free and open-source security platform that unifies XDR and SIEM capabilities. It protects workloads across on-premises, virtualized, containerized, and cloud-based environments.

With over 20 million downloads per year, has one of the largest open-source security communities in the world. From small businesses to large enterprises, the Wazuh solution is used to collect, aggregate, index and analyze security data, helping organizations detect intrusions, threats, and behavioral anomalies.

Achievements

1 Enhanced Ransomware Detection

During their migration to Office 365, Wazuh detected ransomware that their previous EDR solution missed, highlighting its superior threat detection capabilities.

2 Improved Vulnerability Management

Wazuh's integration enabled more frequent vulnerability scans and expedited patching processes, significantly reducing manual effort and enhancing system security.