CERIAS

The Center for Education and Research in Information Assurance and Security

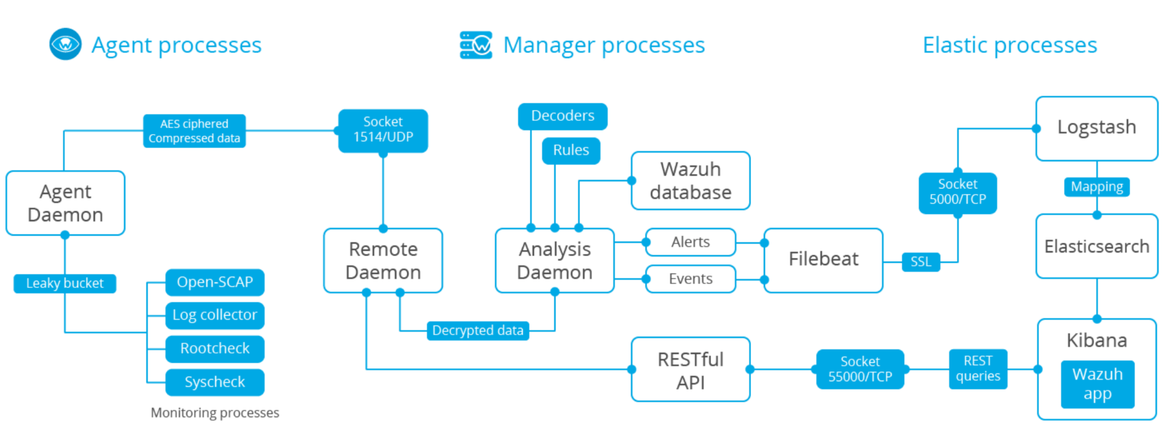
Wazuh: A Free Security Monitoring Solution for Detecting Threats and Providing Incident Response

Andrew Smith, Will Schene, and Connie Justice
Living Lab, Department of Computer and Information Technology, Indiana University – Purdue University Indianapolis

Introduction

- As the quantity and complexity of threats against information systems continues to increase, advanced monitoring and response capabilities are necessary to address these issues.
- Enterprise-ready solutions are often too expensive to implement, while Wazuh is a free and open-source software that can facilitate small to large operations with over 1000 workstations as well as cloud environments.
- Wazuh uses agents at a host-level to detect intrusions by looking for malware, rootkits, and suspicious anomalies.

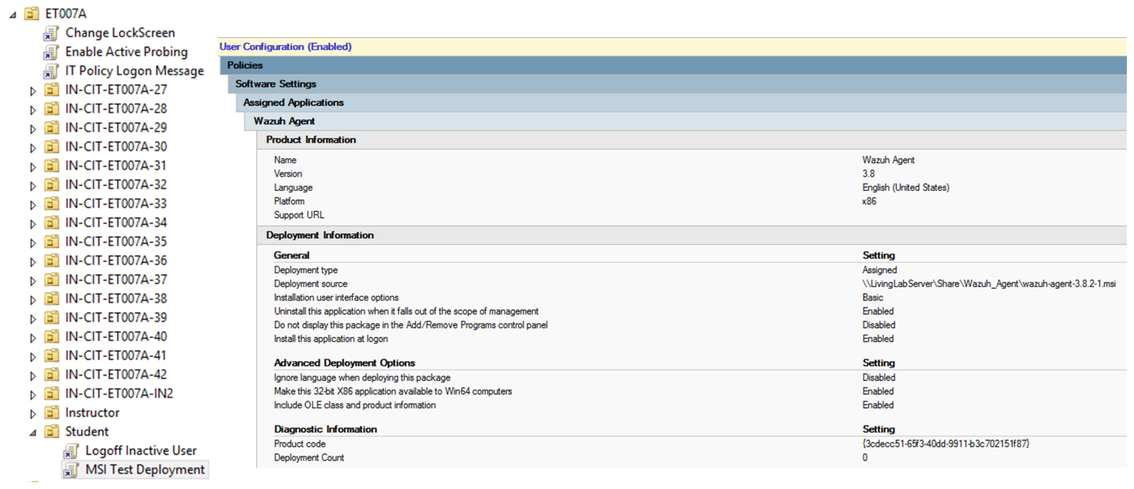
Architecture



- **Agent Daemon:** Receives and collects data from other agent components, then sends the information to management server using encrypted communications.
- **Remote Daemon:** Identifies each agent according to their pre-shared key, then either encrypts or decrypts data between agent and server.
- **Analysis Daemon:** Analyzes data using decoders to determine the type of information and rules to identify specific patterns, which can trigger alerts or respond by blocking an IP address.
- **Logstash, Elasticsearch, and Kibana:** Logstash creates logs of data, Elasticsearch compiles data, while Kibana provides the visual interface for interacting with data.

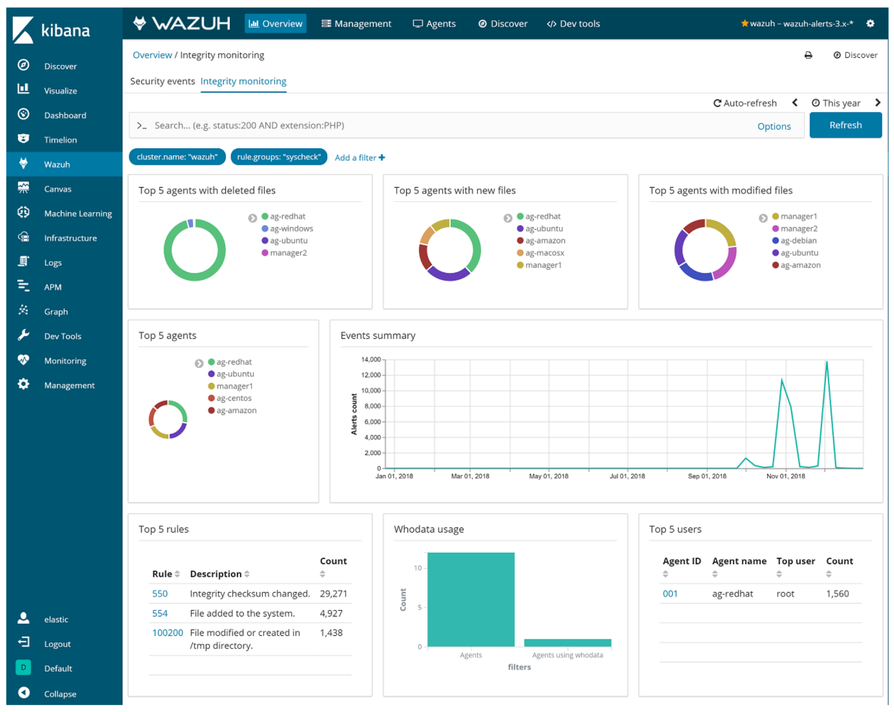
Deployment

- Agents can be easily deployed and managed through Windows Server by creating a Group Policy Object (GPO) from the Microsoft Installer package (MSI), which provides a single-source of control.



Management Interface

- Collected data is indexed on an Elasticsearch cluster, which can then be mined and analyzed using the web interface provided through Kibana.



Resources

Wazuh. (2019). Wazuh · The Open Source Security Platform. Retrieved March 25, 2019, from https://wazuh.com/

PURDUE UNIVERSITY Discovery Park

CERIAS