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		Deployment		
•	As the quantity and complexity of threats against information systems continues to increase, advanced monitoring and response capabilities are necessary to address these issues.	 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. 		

- 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.

C										
⊿ 💼 ET007A										
Change LockScreen										
	Delision									
▶ IN-CIT-ET007A-27	on Message									
	Assigned Applications									
D IN-CIT-ETUU/A-28	Wazuh Agent									
IN-CIT-ET007A-29	Product Information									
▷ 💼 IN-CIT-ET007A-30										
IN-CIT-ET007A-31	Name Version	Wazuh Agent 3.8								
IN-CIT-ET007A-32	Language	English (United States)								
IN-CIT-ET007A-33	Platform	x86								
IN-CIT-ET007A-34	Support URL									
IN-CIT-ET007A-35	Deployment Information									
IN-CIT-ET007A-36	General	Setting								
IN-CIT-ET007A-37	Deployment type									
▷ IN-CIT-ET007A-38	Deployment source Installation user interface options	\\LivingLabServer\Share\Wazuh_Agent\wazuh-agent-3.8.2-1.msi Basic								
	Uninstall this application when it falls out of the scope of management	Enabled								
▷ 10-CIT-ET007A-39	Do not display this package in the Add/Remove Programs control panel	Disabled								
IN-CIT-ET007A-40	Install this application at logon	Enabled								
▷ 📓 IN-CIT-ET007A-41	Advanced Deployment Options	Setting								
▷ 📓 IN-CIT-ET007A-42	Ignore language when deploying this package	Disabled								
IN-CIT-ET007A-IN2	Make this 32-bit X86 application available to Win64 computers	Enabled								
▷ instructor	Include OLE class and product information	Enabled								
⊿ 🗐 Student	Diagnostic Information	Setting								
Logoff Inactive User	Product code	{3cdecc51-65f3-40dd-9911-b3c702151f87}								
MSI Test Deployment	Deployment Count	0								



Management Interface

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

kibana		🗮 Management	🖵 Agents	Ø Discover	<>> Dev tools	🜟 wazuh – wazuh-alerts-3.x-* 🔹 🔅
Overview / Integrity monitoring						🖨 🛛 Ø Discover
U Visualize	Security events Integrity monitoring					
						C Auto-refresh < 🧿 This year 🗦

- **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.



Resources

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



