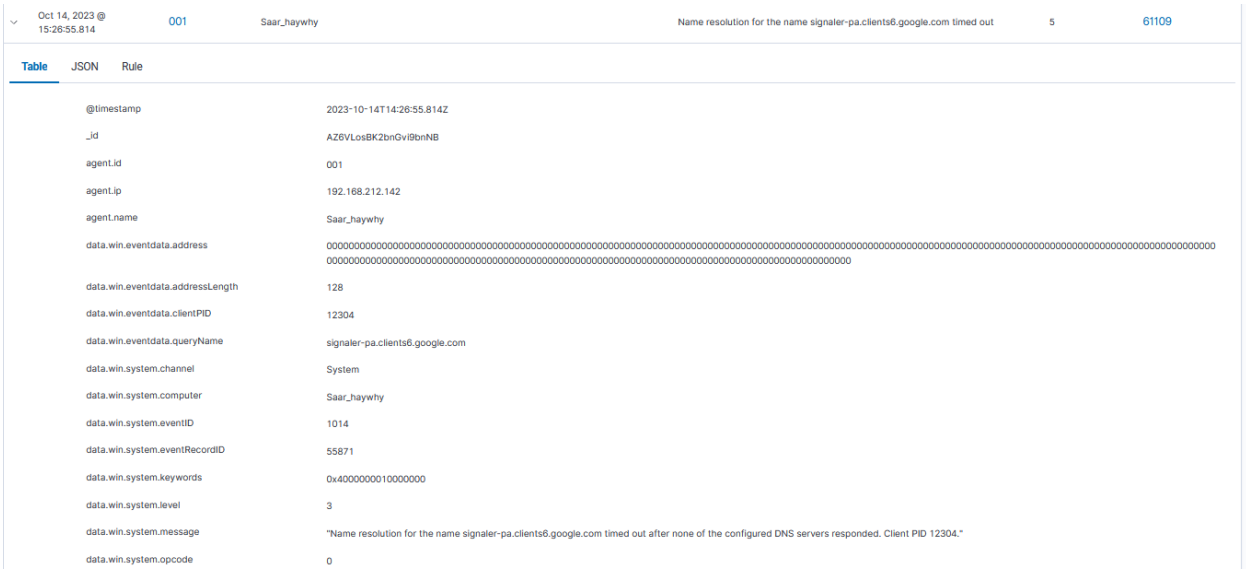
5 Security Events Logs Found In My Wazuh Dashboard

In today's complex digital landscape, maintaining robust cybersecurity measures is paramount to safeguarding sensitive data and ensuring the continuity of operations. Monitoring and analyzing security event logs play a crucial role in identifying and responding to potential threats effectively. Within the Wazuh platform, a comprehensive suite of security tools, users gain access to a wealth of valuable information through event logs.

This report covers five security event logs available within the Wazuh Dashboard, each providing valuable insights into system activity and potential vulnerabilities. From DNS resolution to categorizing threat stages, monitoring listening ports, detecting integrity checksum changes, to confirming the successful initialization of Wazuh agents, these event logs offer critical indicators of potential security breaches or system anomalies. Understanding and properly responding to these events empower users to fortify their network defenses and mitigate risks effectively.

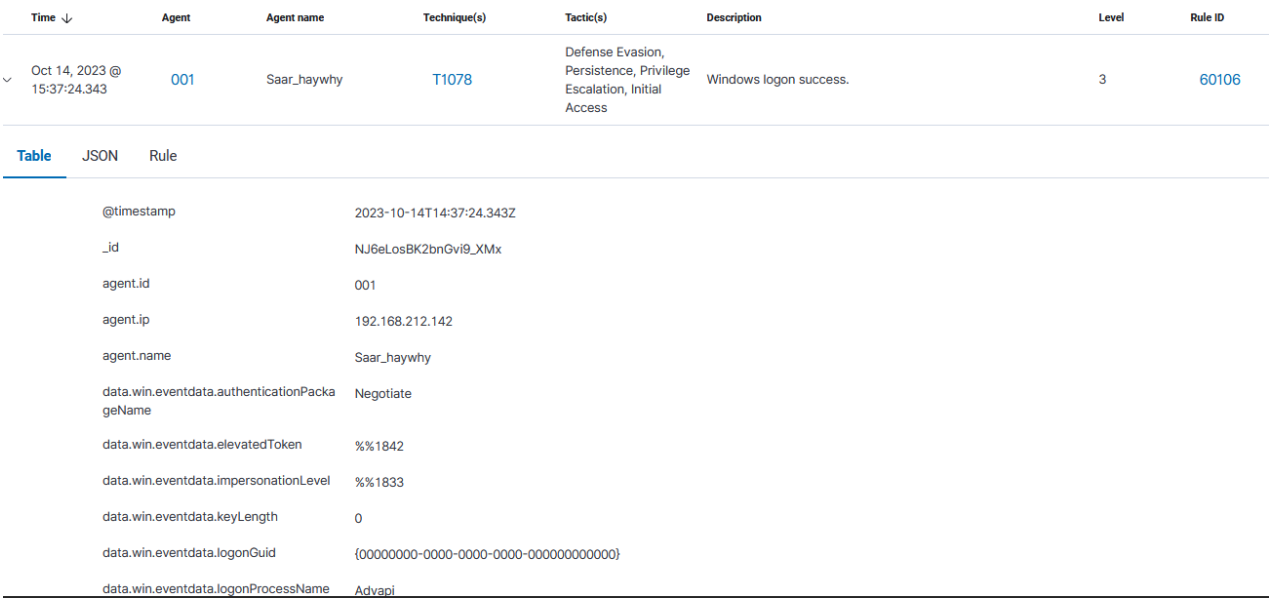
1. **Name Resolution to the name signaler.**

   This log captures an event where Wazuh monitors and records the process of DNS resolution for the hostname or IP address “signaler.” This type of event is crucial for tracking domain name requests and is generated as part of Wazuh’s monitoring and log analysis capabilities. By analyzing this event, security teams can detect unusual DNS requests that might indicate suspicious activity or potential communication with known malicious domains.



2. **Threat Categorization: Defense Evasion, Persistence, Privilege Escalation, Initial Access**

This event log classifies security incidents based on various attack stages, as outlined in the MITRE ATT&CK framework. This categorization helps in identifying tactics used in a cyberattack, including stages like Defense Evasion, Persistence, Privilege Escalation, and Initial Access. Recognizing these stages enables security teams to understand the nature of an attack and respond effectively by targeting specifics.



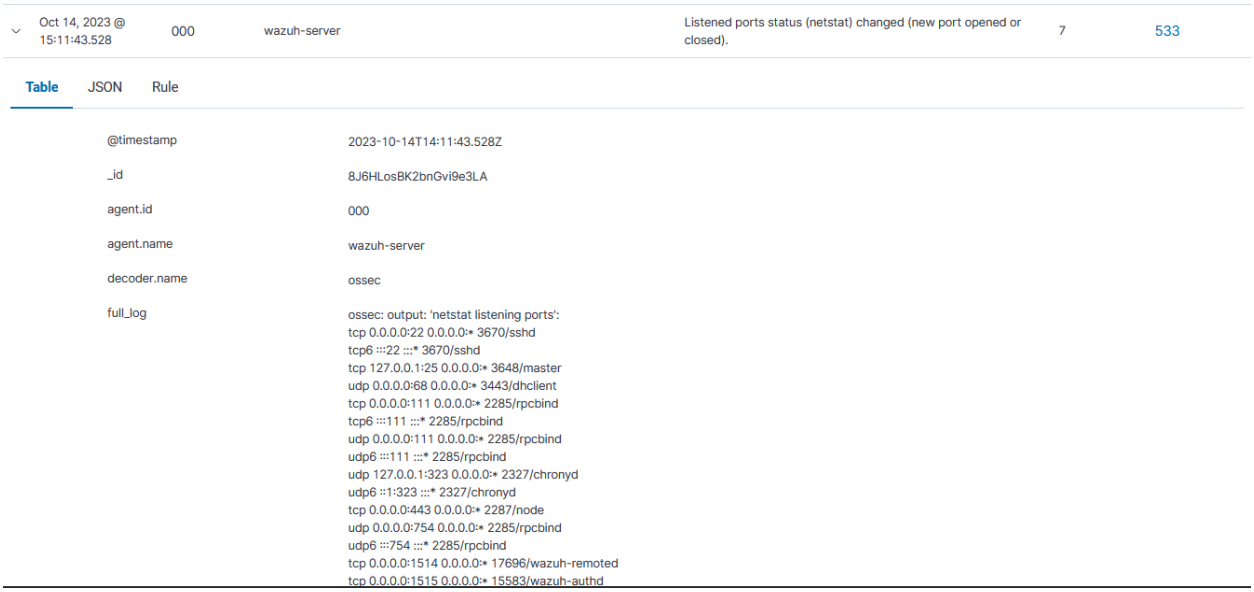
Time ↓	Agent	Agent name	Technique(s)	Tactic(s)	Description	Level	Rule ID
Oct 14, 2023 @ 15:37:24.343	001	Saar_haywhy	T1078	Defense Evasion, Persistence, Privilege Escalation, Initial Access	Windows logon success.	3	60106

Table JSON Rule

@timestamp	2023-10-14T14:37:24.343Z
_id	NJ6eLosBK2bnGvi9_XMx
agent.id	001
agent.ip	192.168.212.142
agent.name	Saar_haywhy
data.win.eventdata.authenticationPackageName	Negotiate
data.win.eventdata.elevatedToken	%%1842
data.win.eventdata.impersonationLevel	%%1833
data.win.eventdata.keyLength	0
data.win.eventdata.logonGuid	{00000000-0000-0000-0000-000000000000}
data.win.eventdata.logonProcessName	Advapi

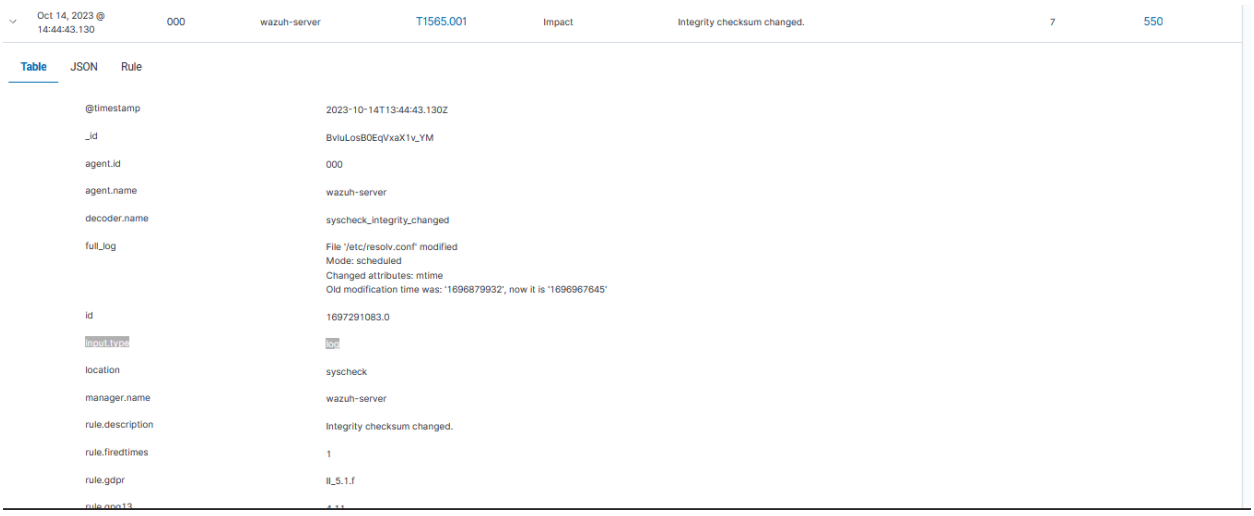
3. **Listened Port Status**

This event provides information about the status of network ports actively monitored for incoming connections. Wazuh generates alerts to notify users of changes in listening ports, helping detect unauthorized access points or suspicious network behavior. Regularly investigating these alerts ensures the security and optimal functioning of network services, as any anomalies in port status can indicate attempts to exploit open ports for malicious activity.



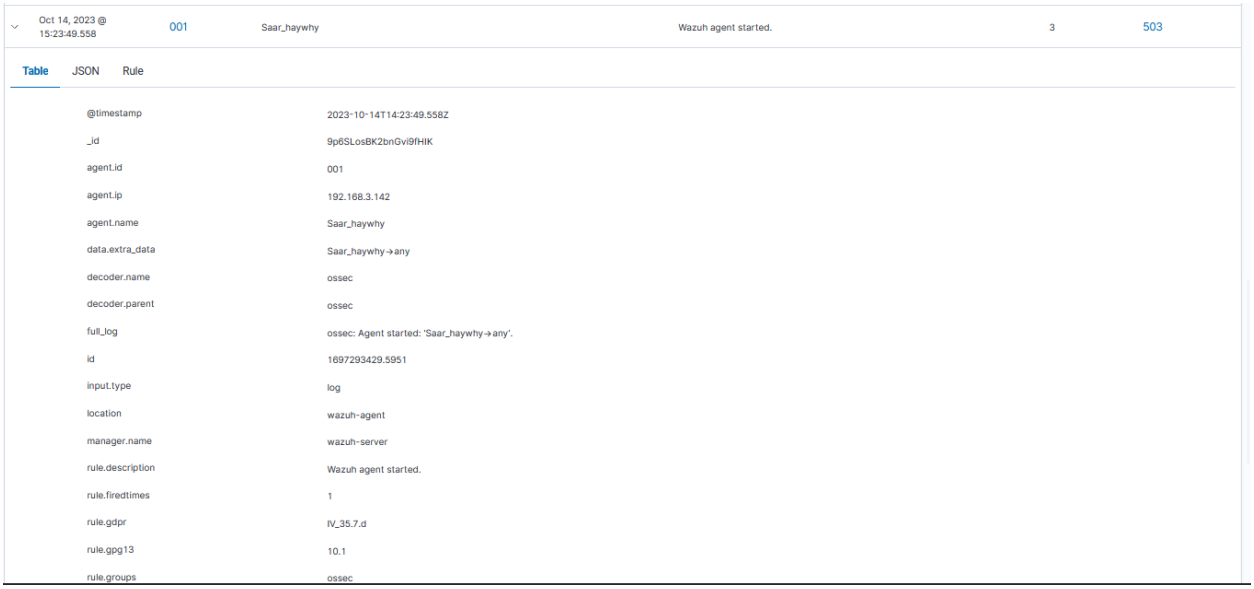
4. Integrity Checksum Changes

The integrity checksum change event signals a modification in the checksum of a monitored file or system component. Such a change may arise from legitimate updates or, alternatively, from malicious tampering. This alert is essential for maintaining file integrity, as altered checksums may signify potential security threats or unauthorized changes to critical files. Investigating these alerts within the Wazuh console allows security teams to distinguish between legitimate changes and potential security threats, enabling timely response to anomalies.



5. Wazuh Agent Started

This log records the successful initialization or restart of the Wazuh manager component, responsible for centralizing security data and logs. This event is a confirmation that the Wazuh server component is active and functioning, which is vital for consistent security monitoring. Recognizing the successful initialization of Wazuh agents helps ensure the continuous collection and processing of security data, crucial for maintaining a proactive security posture.



In conclusion, the documentation presented herein sheds light on five pivotal security event logs accessible through the Wazuh Dashboard. By comprehensively understanding and proactively monitoring these events, users can bolster their cybersecurity posture, swiftly identifying and mitigating potential threats to their systems and networks. Leveraging the insights provided by Wazuh's robust monitoring and analysis capabilities, organizations can strengthen their defenses, safeguarding against evolving cyber threats in today's dynamic digital landscape. Embracing a proactive approach to security event monitoring ensures not only the protection of critical assets but also fosters a resilient and secure computing environment for continued business success.