SOC INCIDENT REPORT (LAB SIMULATION)

Wazuh Alerts Validation — SSH Brute Force, Sudo Privilege Escalation & File Integrity Monitoring (FIM)

Prepared by: Karan Singh Samant
Date: 18 January 2026
Platform: Wazuh (Docker-based Manager + Agents)
Monitored Endpoint (Agent): soc-server (Agent ID: 005)
Endpoint OS: Ubuntu Server
Report Type: SOC Lab / Detection Validation Report

Version: v1.0
Classification: Internal (Lab Use)

1. Executive Summary

Incident Type: Detection Validation (Lab Simulation)
Monitoring Tool: Wazuh (Manager + Agent)
Monitored Endpoint: soc-server (Agent ID: 005)
Date/Time Observed: 18 Jan 2026 (UTC)
Severity (Overall): Medium
Status: Closed (Validated)

Summary:
During a SOC lab simulation, multiple security alerts were generated and successfully detected by Wazuh for the monitored endpoint soc-server. The activity included SSH authentication abuse attempts (brute-force / invalid user), successful privilege escalation using sudo to root, and File Integrity Monitoring (FIM) alerts indicating integrity checksum changes on a monitored file. Evidence confirms that Wazuh agent logging, rule triggering, and event visibility in the dashboard were functioning as expected.

Impact:
No real compromise occurred. This was a controlled simulation to validate alert generation and detection visibility. However, the same alert pattern in a production environment could indicate credential access attempts followed by privilege escalation and potential tampering.

Actions Taken:

- Verified agent status and connectivity
- Triggered controlled authentication abuse attempts
- Executed sudo/root actions to generate privilege escalation logs
- Modified a monitored file to trigger FIM checksum change alerts
- Confirmed alerts in the Wazuh dashboard and event details

2. Environment / Lab Setup

Lab Purpose:
Validate Wazuh alert generation and visibility for common SOC detections (SSH authentication abuse, privilege escalation, and file integrity monitoring).

Architecture:

- Wazuh Manager: Docker-based deployment (single-node)
- Wazuh Agent: Installed on Ubuntu Server endpoint
- Dashboard: Wazuh Web UI used to validate alerts and event details

Endpoint Details:

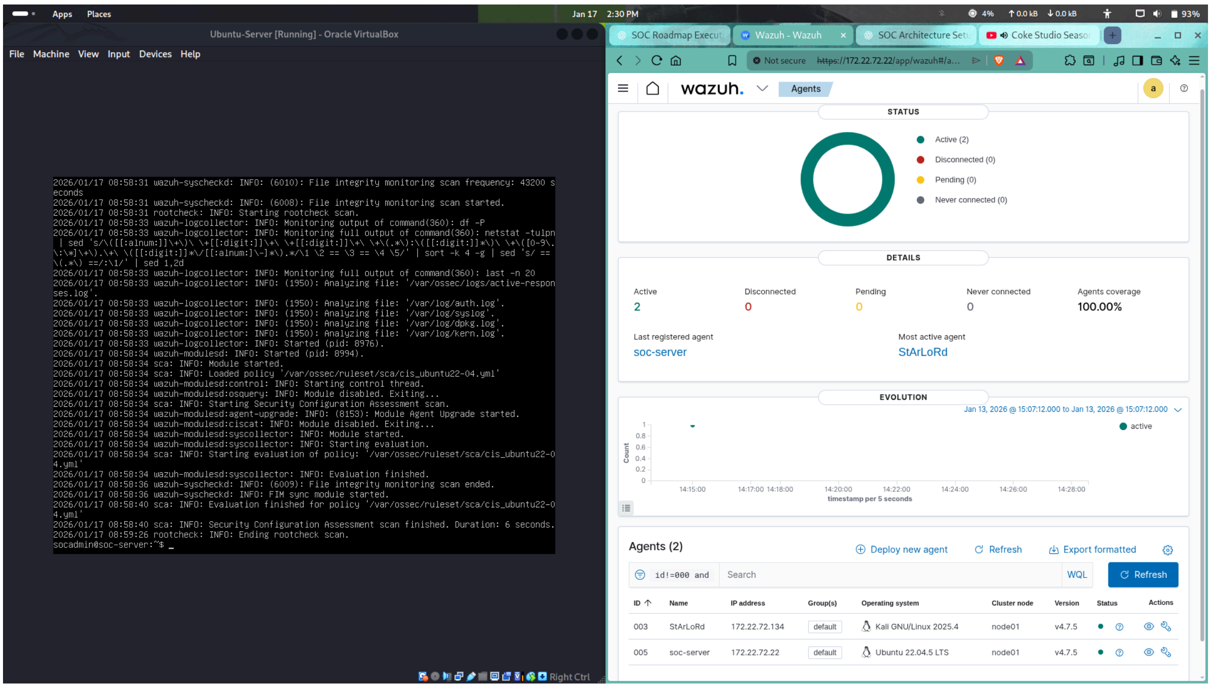
- Agent Name: soc-server
- Agent ID: 005
- Endpoint OS: Ubuntu Server
- Agent Status: Active and reporting (validated via systemctl)

Data Sources Observed:

- /var/log/auth.log (SSH + sudo events)
- Syscheck / FIM module (file integrity events)

Monitoring Features Enabled:

- SSH authentication monitoring
- Sudo activity monitoring
- File Integrity Monitoring (FIM) with real-time monitoring enabled for /etc



```
2026/01/17 08:58:31 wazuh-syscheckd: INFO: (6010): File integrity monitoring scan frequency: 43200 s
econds
2026/01/17 08:58:31 wazuh-syscheckd: INFO: (6008): File integrity monitoring scan started.
2026/01/17 08:58:31 rootcheck: INFO: Starting rootcheck scan.
2026/01/17 08:58:33 wazuh-logcollector: INFO: Monitoring output of command(360): df -P
2026/01/17 08:58:33 wazuh-logcollector: INFO: Monitoring full output of command(360): netstat -tulpn
 | sed 's/\([[:alnum:]]\+\)\ \+[[:digit:]]\+\ \+[[:digit:]]\+\ \+\(.*\):\([[:digit:]]*\)\ \+\([0-9\.
\:\*]\+\).\+\ \([[:digit:]]*\/[[:alnum:]\-]*\).*/\1 \2 == \3 == \4 \5/' | sort -k 4 -g | sed 's/ ==
\(.*\) ==/:\1/' | sed 1,2d
2026/01/17 08:58:33 wazuh-logcollector: INFO: Monitoring full output of command(360): last -n 20
2026/01/17 08:58:33 wazuh-logcollector: INFO: (1950): Analyzing file: '/var/ossec/logs/active-respon
ses.log'.
2026/01/17 08:58:33 wazuh-logcollector: INFO: (1950): Analyzing file: '/var/log/auth.log'.
2026/01/17 08:58:33 wazuh-logcollector: INFO: (1950): Analyzing file: '/var/log/syslog'.
2026/01/17 08:58:33 wazuh-logcollector: INFO: (1950): Analyzing file: '/var/log/dpkg.log'.
2026/01/17 08:58:33 wazuh-logcollector: INFO: (1950): Analyzing file: '/var/log/kern.log'.
2026/01/17 08:58:33 wazuh-logcollector: INFO: Started (pid: 8976).
2026/01/17 08:58:34 wazuh-modulesd: INFO: Started (pid: 8994).
2026/01/17 08:58:34 sca: INFO: Module started.
2026/01/17 08:58:34 sca: INFO: Loaded policy '/var/ossec/ruleset/sca/cis_ubuntu22-04.yml'
2026/01/17 08:58:34 wazuh-modulesd:control: INFO: Starting control thread.
2026/01/17 08:58:34 wazuh-modulesd:osquery: INFO: Module disabled. Exiting...
2026/01/17 08:58:34 sca: INFO: Starting Security Configuration Assessment scan.
2026/01/17 08:58:34 wazuh-modulesd:agent-upgrade: INFO: (8153): Module Agent Upgrade started.
2026/01/17 08:58:34 wazuh-modulesd:ciscat: INFO: Module disabled. Exiting...
2026/01/17 08:58:34 wazuh-modulesd:syscollector: INFO: Module started.
2026/01/17 08:58:34 wazuh-modulesd:syscollector: INFO: Starting evaluation.
2026/01/17 08:58:34 sca: INFO: Starting evaluation of policy: '/var/ossec/ruleset/sca/cis_ubuntu22-0
4.yml'
2026/01/17 08:58:34 wazuh-modulesd:syscollector: INFO: Evaluation finished.
2026/01/17 08:58:36 wazuh-syscheckd: INFO: (6009): File integrity monitoring scan ended.
2026/01/17 08:58:36 wazuh-syscheckd: INFO: FIM sync module started.
2026/01/17 08:58:40 sca: INFO: Evaluation finished for policy '/var/ossec/ruleset/sca/cis_ubuntu22-0
4.yml'
2026/01/17 08:58:40 sca: INFO: Security Configuration Assessment scan finished. Duration: 6 seconds.
2026/01/17 08:59:26 rootcheck: INFO: Ending rootcheck scan.
socadmin@soc-server:~$ _
```

STATUS

- Active (2)
- Disconnected (0)
- Pending (0)
- Never connected (0)

DETAILS

Active	Disconnected	Pending	Never connected	Agents coverage
2	0	0	0	100.00%

Last registered agent: soc-server

Most active agent: StArLoRd

EVOLUTION

Jan 13, 2026 @ 15:07:12.000 to Jan 13, 2026 @ 15:07:12.000

Agents (2)

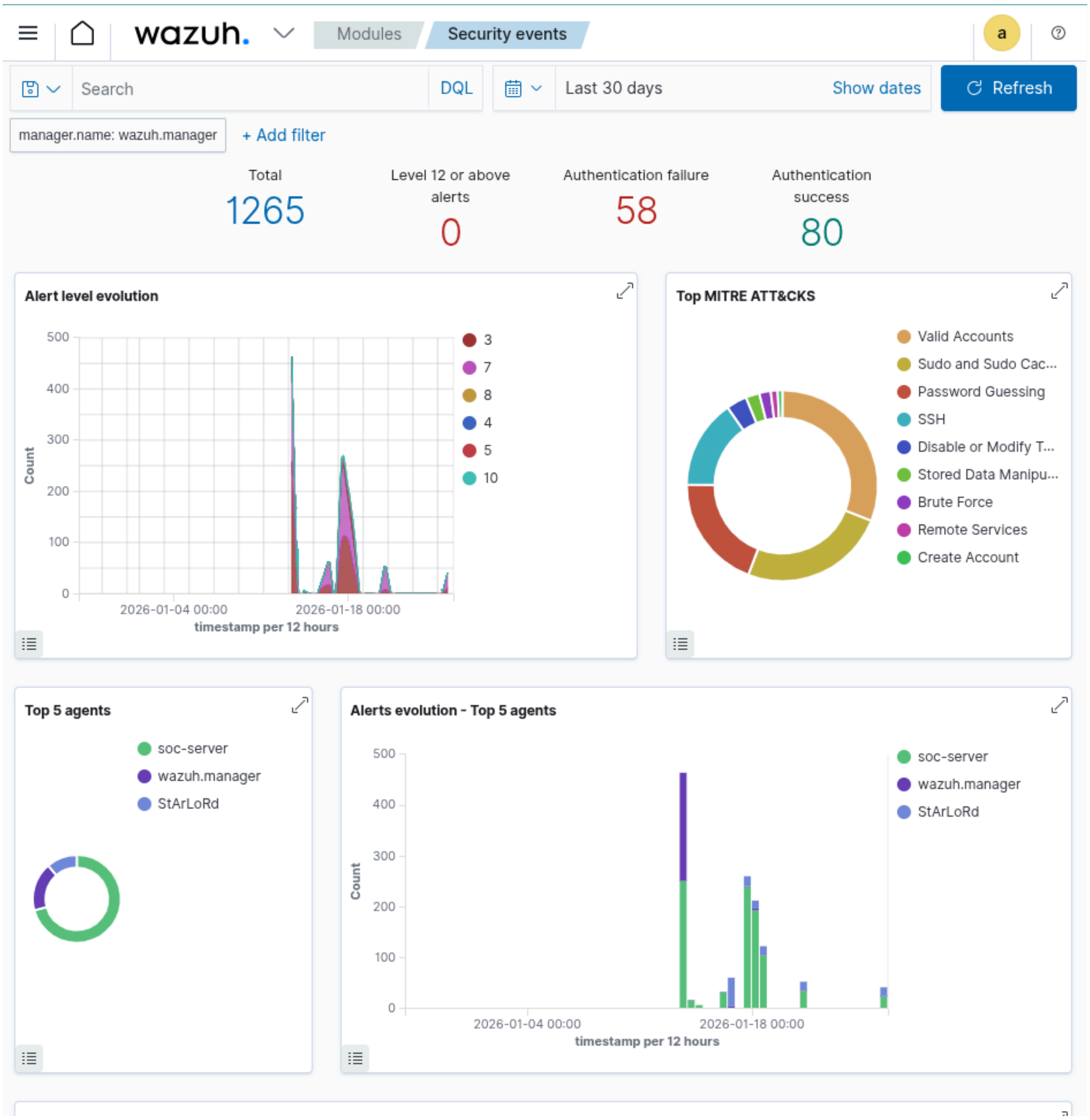
id!=000 and

ID ↑	Name	IP address	Group(s)	Operating system	Cluster node	Version	Status	Actions
003	StArLoRd	172.22.72.134	default	Kali GNU/Linux 2025.4	node01	v4.7.5	●	
005	soc-server	172.22.72.22	default	Ubuntu 22.04.5 LTS	node01	v4.7.5	●	

Figure 1: Agent onboarding and health status were verified from the Wazuh Agents panel.

3. Observed Alerts Summary

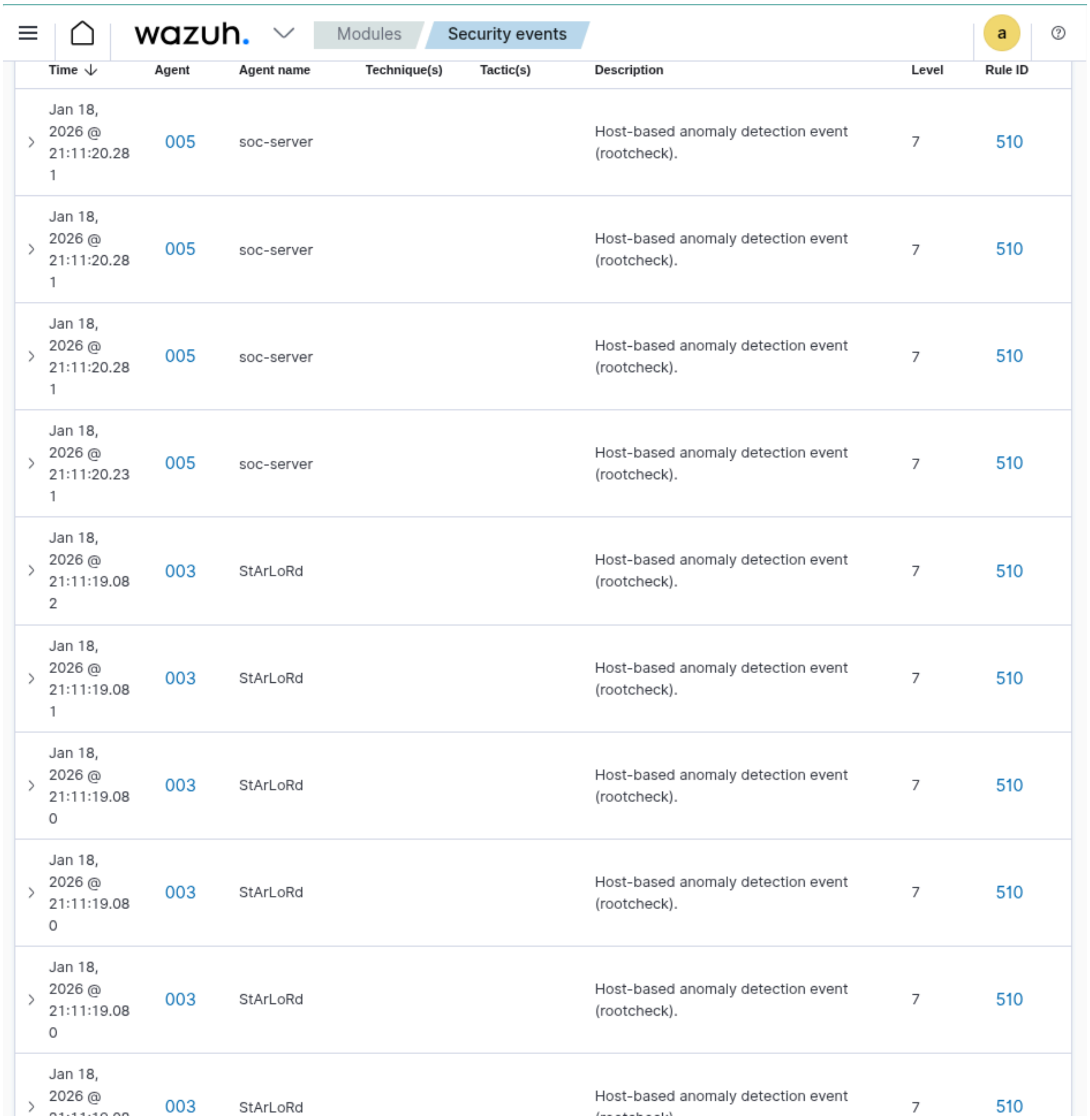
During the lab simulation, Wazuh successfully generated and displayed alerts for authentication abuse, privilege escalation, and file integrity monitoring activity on the monitored endpoint soc-server (Agent ID: 005). These alerts confirm that log ingestion, decoding, and rule-based detection are functioning correctly.



Last 30 days

manager.name: wazuh.manager

Total	Level 12 or above alerts	Authentication failure	Authentication success
1265	0	58	80



	Time	Agent	Agent name	Technique(s)	Tactic(s)	Description	Level	Rule ID
›	Jan 18, 2026 @ 21:11:20.281	005	soc-server			Host-based anomaly detection event (rootcheck).	7	510
›	Jan 18, 2026 @ 21:11:20.281	005	soc-server			Host-based anomaly detection event (rootcheck).	7	510
›	Jan 18, 2026 @ 21:11:20.281	005	soc-server			Host-based anomaly detection event (rootcheck).	7	510
›	Jan 18, 2026 @ 21:11:20.231	005	soc-server			Host-based anomaly detection event (rootcheck).	7	510
›	Jan 18, 2026 @ 21:11:19.082	003	StArLoRd			Host-based anomaly detection event (rootcheck).	7	510
›	Jan 18, 2026 @ 21:11:19.081	003	StArLoRd			Host-based anomaly detection event (rootcheck).	7	510
›	Jan 18, 2026 @ 21:11:19.080	003	StArLoRd			Host-based anomaly detection event (rootcheck).	7	510
›	Jan 18, 2026 @ 21:11:19.080	003	StArLoRd			Host-based anomaly detection event (rootcheck).	7	510
›	Jan 18, 2026 @ 21:11:19.080	003	StArLoRd			Host-based anomaly detection event (rootcheck).	7	510
›	Jan 18, 2026 @	003	StArLoRd			Host-based anomaly detection event	7	510

Figure 2: Observed Alerts Summary

3.1 Alert Category A — SSH Authentication Abuse (Brute Force / Invalid User)

Wazuh detected multiple authentication-related events, including failed login attempts and invalid/non-existent user login attempts over SSH. This behaviour is consistent with brute-force style activity and is commonly observed during credential access attempts.

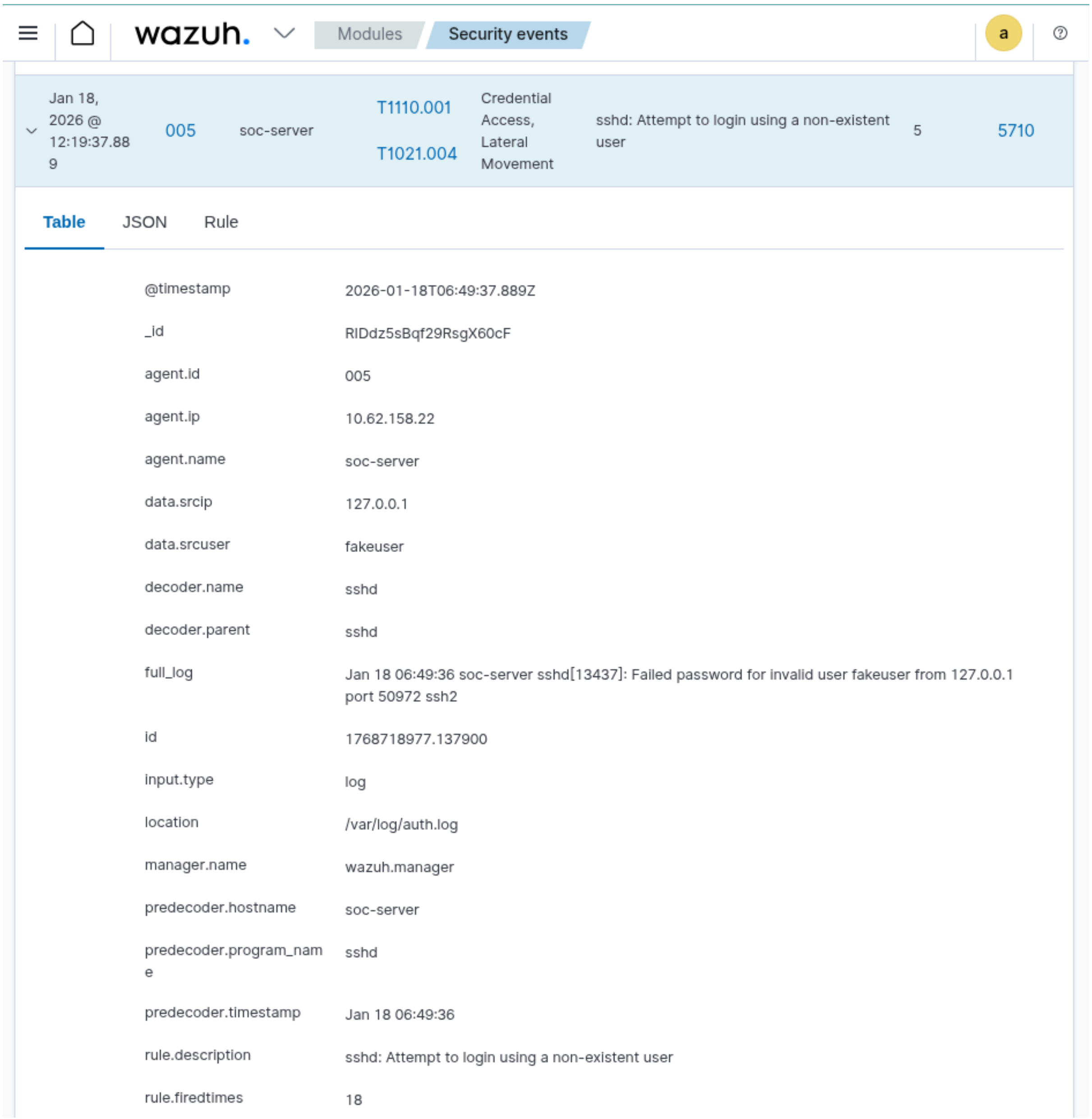
Key alert indicators observed:

- `PAM: User login failed` (Rule ID: 5503)

- `sshd: Attempt to login using a non-existent user` (Rule ID: 5710)

- `PAM: Login session opened/closed` (Rule IDs: 5501 / 5502)

Evidence:



Jan 18, 2026 @ 12:19:37.889	005	soc-server	T1110.001 T1021.004	Credential Access, Lateral Movement	sshd: Attempt to login using a non-existent user	5	5710

Table JSON Rule

@timestamp	2026-01-18T06:49:37.889Z
_id	RIDdz5sBqf29RsgX60cF
agent.id	005
agent.ip	10.62.158.22
agent.name	soc-server
data.srcip	127.0.0.1
data.srcuser	fakeuser
decoder.name	sshd
decoder.parent	sshd
full_log	Jan 18 06:49:36 soc-server sshd[13437]: Failed password for invalid user fakeuser from 127.0.0.1 port 50972 ssh2
id	1768718977.137900
input.type	log
location	/var/log/auth.log
manager.name	wazuh.manager
predecoder.hostname	soc-server
predecoder.program_name	sshd
predecoder.timestamp	Jan 18 06:49:36
rule.description	sshd: Attempt to login using a non-existent user
rule.firedtimes	18

Figure 3: Wazuh Security events list showing SSH authentication abuse alerts (`invalid user / non-existent user`) and failed login attempts.

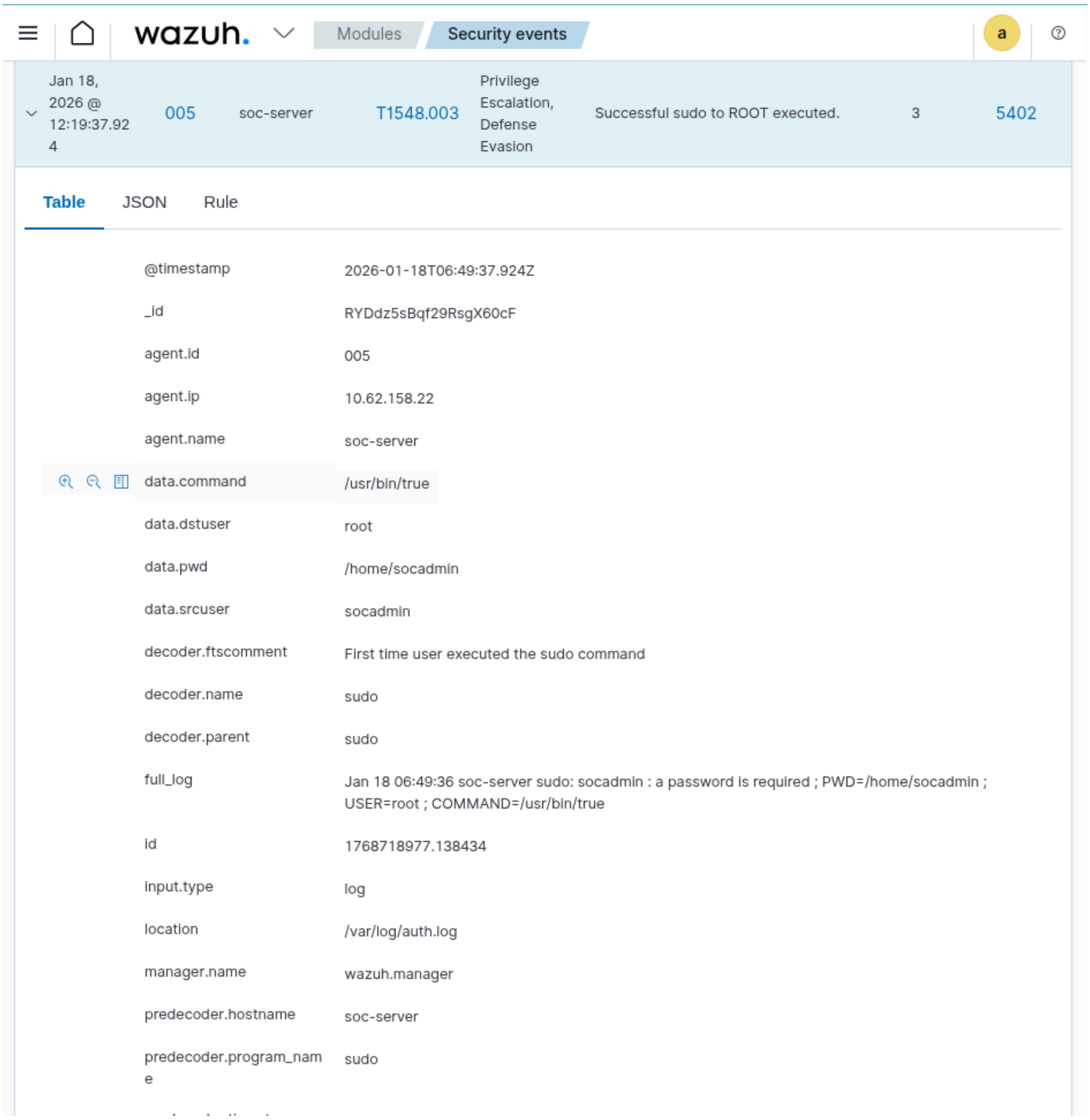
3.2 Alert Category B — Privilege Escalation via sudo (Root Access)

Wazuh detected successful privilege escalation activity where sudo was executed to obtain ROOT-level access. The alert contained sufficient execution context (user/session/command), making it useful for investigation and incident response.

Key alert indicator observed:

- `Successful sudo to ROOT executed (Rule ID: 5402)`

Evidence:



Jan 18, 2026 @ 12:19:37.924	005	soc-server	T1548.003	Privilege Escalation, Defense Evasion	Successful sudo to ROOT executed.	3	5402

@timestamp	2026-01-18T06:49:37.924Z
_id	RYDdz5sBqf29RsgX60cF
agent.id	005
agent.ip	10.62.158.22
agent.name	soc-server
data.command	/usr/bin/true
data.dstuser	root
data.pwd	/home/socadmin
data.srcuser	socadmin
decoder.ftscomment	First time user executed the sudo command
decoder.name	sudo
decoder.parent	sudo
full_log	Jan 18 06:49:36 soc-server sudo: socadmin : a password is required ; PWD=/home/socadmin ; USER=root ; COMMAND=/usr/bin/true
id	1768718977.138434
input.type	log
location	/var/log/auth.log
manager.name	wazuh.manager
predecoder.hostname	soc-server
predecoder.program_name	sudo

Figure 4: Wazuh Security event list showing sudo privilege escalation alert (`Successful sudo to ROOT executed`).

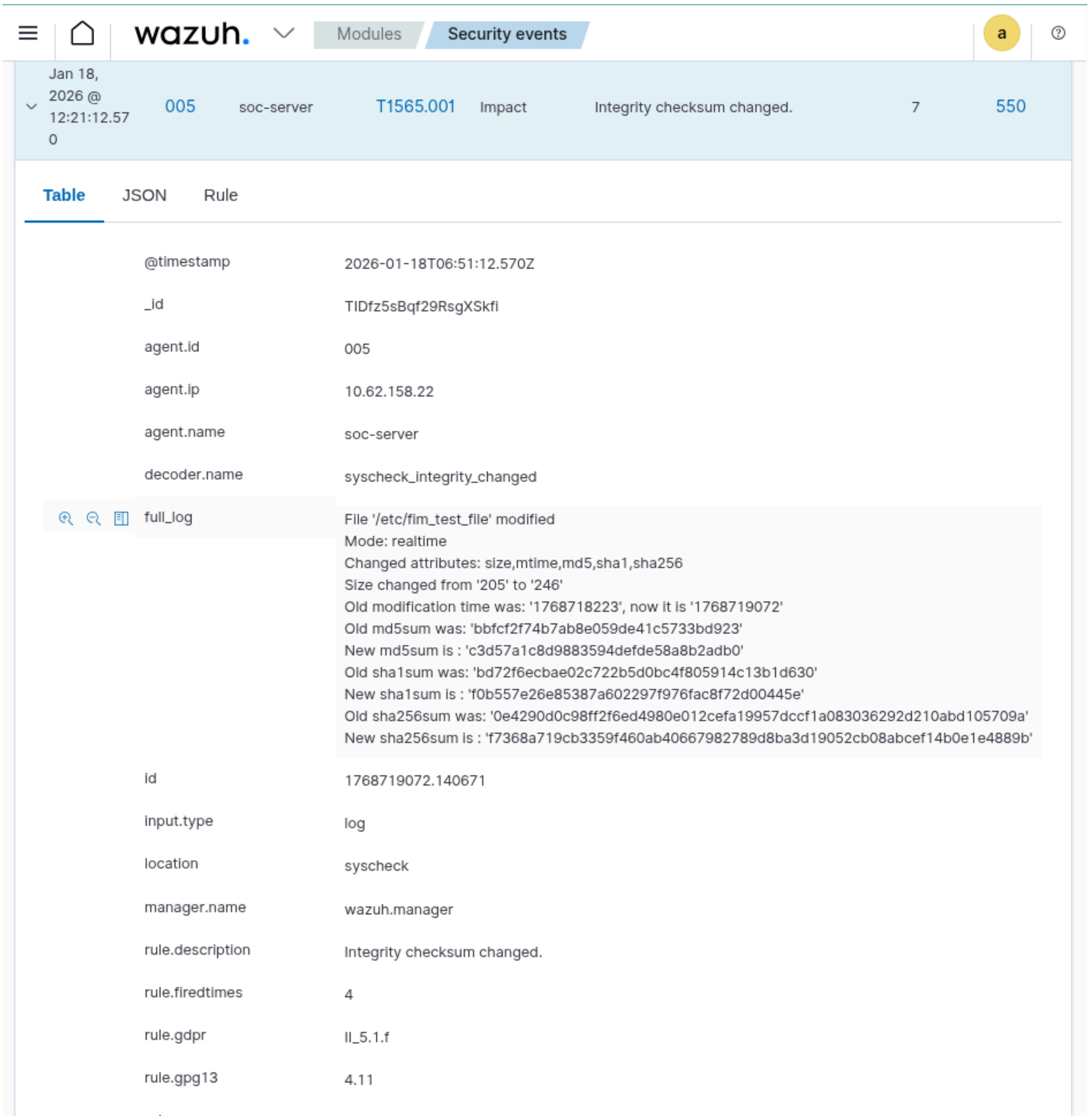
3.3 Alert Category C — File Integrity Monitoring (FIM) Integrity Checksum Change

Wazuh File Integrity Monitoring successfully detected a file modification event on a monitored path. The alert indicated an integrity checksum change, confirming that syscheck/FIM is operational and able to detect file changes in real-time.

Key alert indicator observed:

- `Integrity checksum changed` (Rule ID: 550)

Evidence:



Jan 18, 2026 @ 12:21:12.570	005	soc-server	T1565.001	Impact	Integrity checksum changed.	7	550

@timestamp	2026-01-18T06:51:12.570Z
_id	TIDfz5sBqf29RsgXSkfi
agent.id	005
agent.ip	10.62.158.22
agent.name	soc-server
decoder.name	syscheck_integrity_changed
full_log	File '/etc/fim_test_file' modified Mode: realtime Changed attributes: size,mtime,md5,sha1,sha256 Size changed from '205' to '246' Old modification time was: '1768718223', now it is '1768719072' Old md5sum was: 'bbfcf2f74b7ab8e059de41c5733bd923' New md5sum is : 'c3d57a1c8d9883594defde58a8b2adb0' Old sha1sum was: 'bd72f6ecbae02c722b5d0bc4f805914c13b1d630' New sha1sum is : 'f0b557e26e85387a602297f976fac8f72d00445e' Old sha256sum was: '0e4290d0c98ff2f6ed4980e012cefa19957dccf1a083036292d210abd105709a' New sha256sum is : 'f7368a719cb3359f460ab40667982789d8ba3d19052cb08abcef14b0e1e4889b'
id	1768719072.140671
input.type	log
location	syscheck
manager.name	wazuh.manager
rule.description	Integrity checksum changed.
rule.firedtimes	4
rule.gdpr	II_5.1.f
rule.gpg13	4.11

Figure 5: Wazuh Security events list showing File Integrity Monitoring alert (`Integrity checksum changed`).

3.4 Overall Alert Validation Outcome

The alert flow confirms that:

- SSH authentication abuse events were logged and detected correctly.
- Privilege escalation via sudo was captured successfully.
- FIM successfully detected file modifications and changes to checksums.

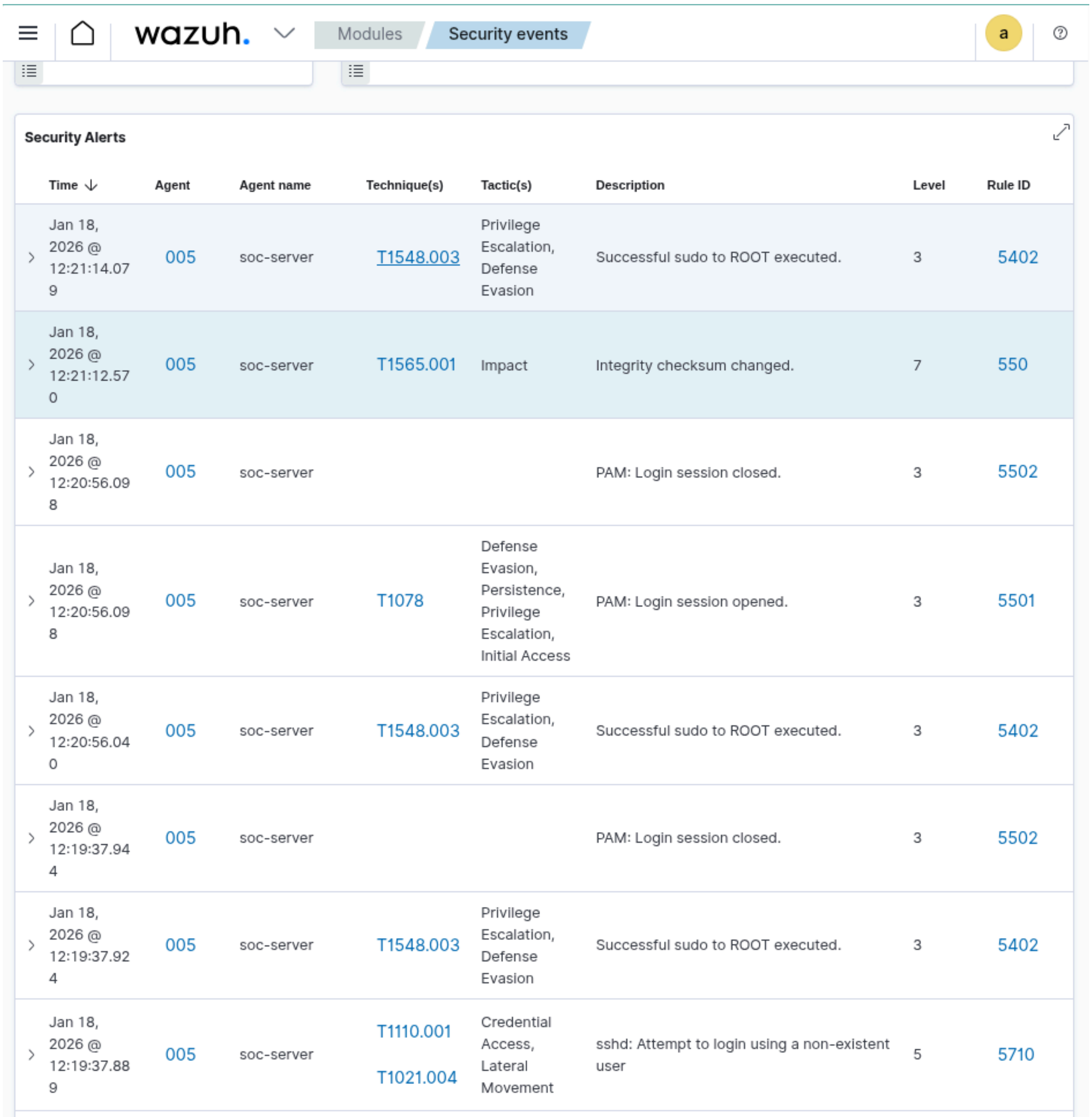
This validates that the Wazuh deployment (Manager + Agent) was operational and capable of generating actionable SOC-style detections in a controlled environment.

4. Incident Timeline (UTC)

Time (UTC)	Event Description	Rule ID	MITRE Technique	Level	Evidence
12:21:14	PAM login session opened	5501	T1078	3	Figure 7
12:21:24	PAM authentication failure	5503	T1110.001	5	Figure 7
12:21:26	SSH attempt (non-existent user)	5710	T1110.001	5	Figure 8
12:22:44	SSH authentication success	5715	T1078	3	Figure 7
12:22:53	File integrity checksum changed	550	T1565.001	7	Figure 10
12:22:54	Successful sudo to root executed	5402	T1548.003	3	Figure 9

12:22:58	PAM login session closed	5502	—	3	Figure 6

Timeline Notes:
Evidence was validated using detailed alert views from the Wazuh Security events dashboard (Figures 7–10).



Security Alerts

	Time	Agent	Agent name	Technique(s)	Tactic(s)	Description	Level	Rule ID
›	Jan 18, 2026 @ 12:21:14.079	005	soc-server	T1548.003	Privilege Escalation, Defense Evasion	Successful sudo to ROOT executed.	3	5402
›	Jan 18, 2026 @ 12:21:12.570	005	soc-server	T1565.001	Impact	Integrity checksum changed.	7	550
›	Jan 18, 2026 @ 12:20:56.098	005	soc-server			PAM: Login session closed.	3	5502
›	Jan 18, 2026 @ 12:20:56.098	005	soc-server	T1078	Defense Evasion, Persistence, Privilege Escalation, Initial Access	PAM: Login session opened.	3	5501
›	Jan 18, 2026 @ 12:20:56.040	005	soc-server	T1548.003	Privilege Escalation, Defense Evasion	Successful sudo to ROOT executed.	3	5402
›	Jan 18, 2026 @ 12:19:37.944	005	soc-server			PAM: Login session closed.	3	5502
›	Jan 18, 2026 @ 12:19:37.924	005	soc-server	T1548.003	Privilege Escalation, Defense Evasion	Successful sudo to ROOT executed.	3	5402
›	Jan 18, 2026 @ 12:19:37.889	005	soc-server	T1110.001 T1021.004	Credential Access, Lateral Movement	sshd: Attempt to login using a non-existent user	5	5710

Figure 6: Security events showing login session open/close + authentication chain

5. MITRE ATT&CK Mapping

Activity Observed	Wazuh Alert / Evidence	MITRE Technique ID	Technique Name	Tactic
Multiple failed login attempts / invalid user	“PAM: User login failed” + “sshd: Attempt to login using a non-existent user”	**T1110.001**	Password Guessing	Credential Access
Successful sudo to root	“Successful sudo to ROOT executed”	**T1548.003**	Sudo and Sudo Caching	Privilege Escalation / Defence Evasion
File modification detected by FIM	“Integrity checksum changed”	**T1565.001**	Stored Data Manipulation	Impact
SSH authentication success (login success event)	“sshd: authentication success”	**T1078**	Valid Accounts	Initial Access / Persistence / Privilege Escalation

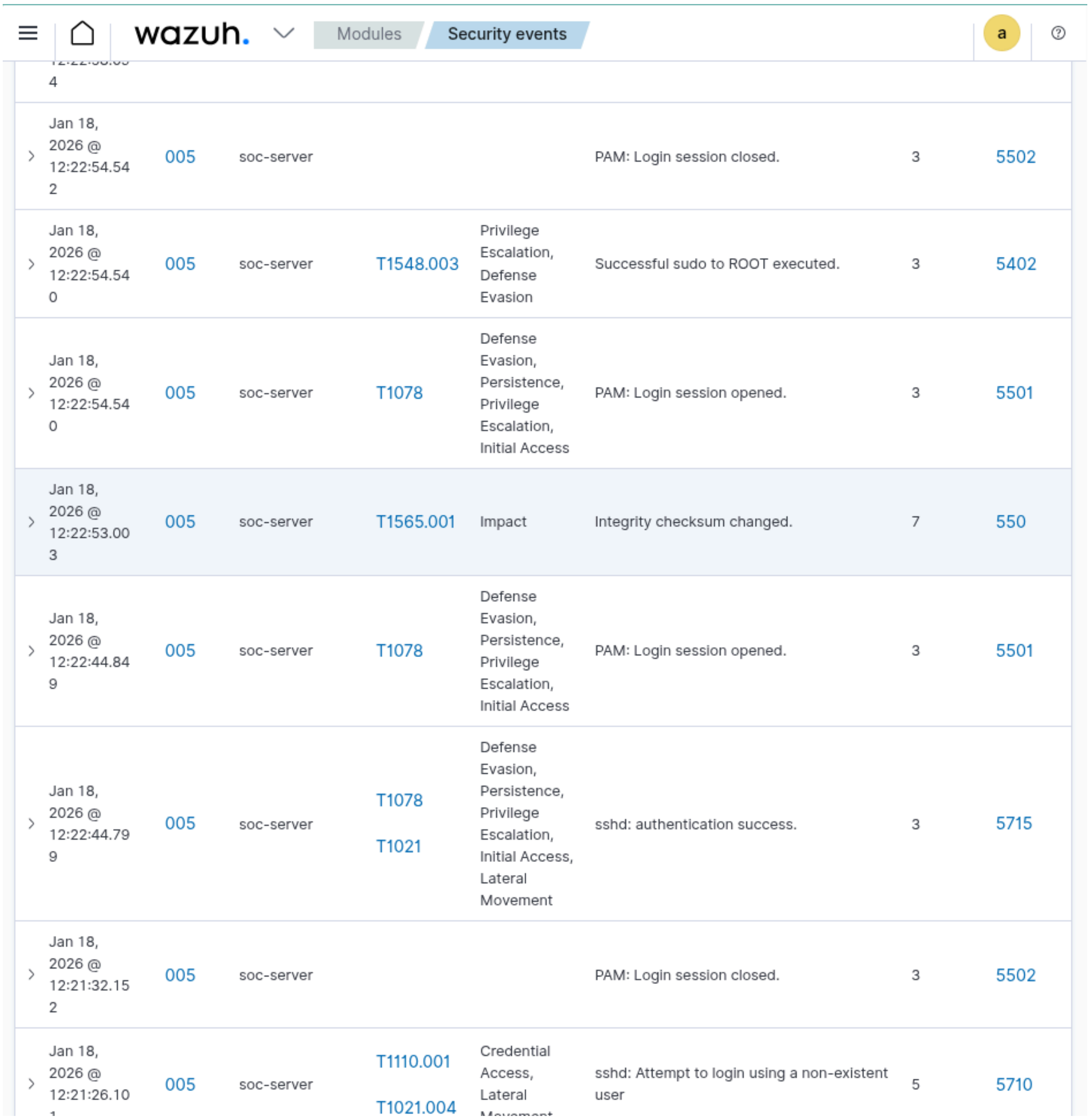
Note: These mappings are based on Wazuh rule metadata and observed alert descriptions in the lab simulation. No real compromise occurred; activity was generated to validate detection coverage.

6. Evidence

This section contains supporting evidence collected from the Wazuh dashboard during the lab simulation. The screenshots validate alert generation, rule triggering, and event visibility for SSH authentication abuse, privilege escalation, and File Integrity Monitoring (FIM).

6.1 Dashboard Timeline View (Overview Proof)

The Wazuh **Security events** dashboard was used to validate the full detection chain in sequence. The timeline/table view confirms that the monitored endpoint `soc-server` (Agent ID: 005) generated multiple correlated alerts within the same short time window, supporting the incident timeline documented earlier.

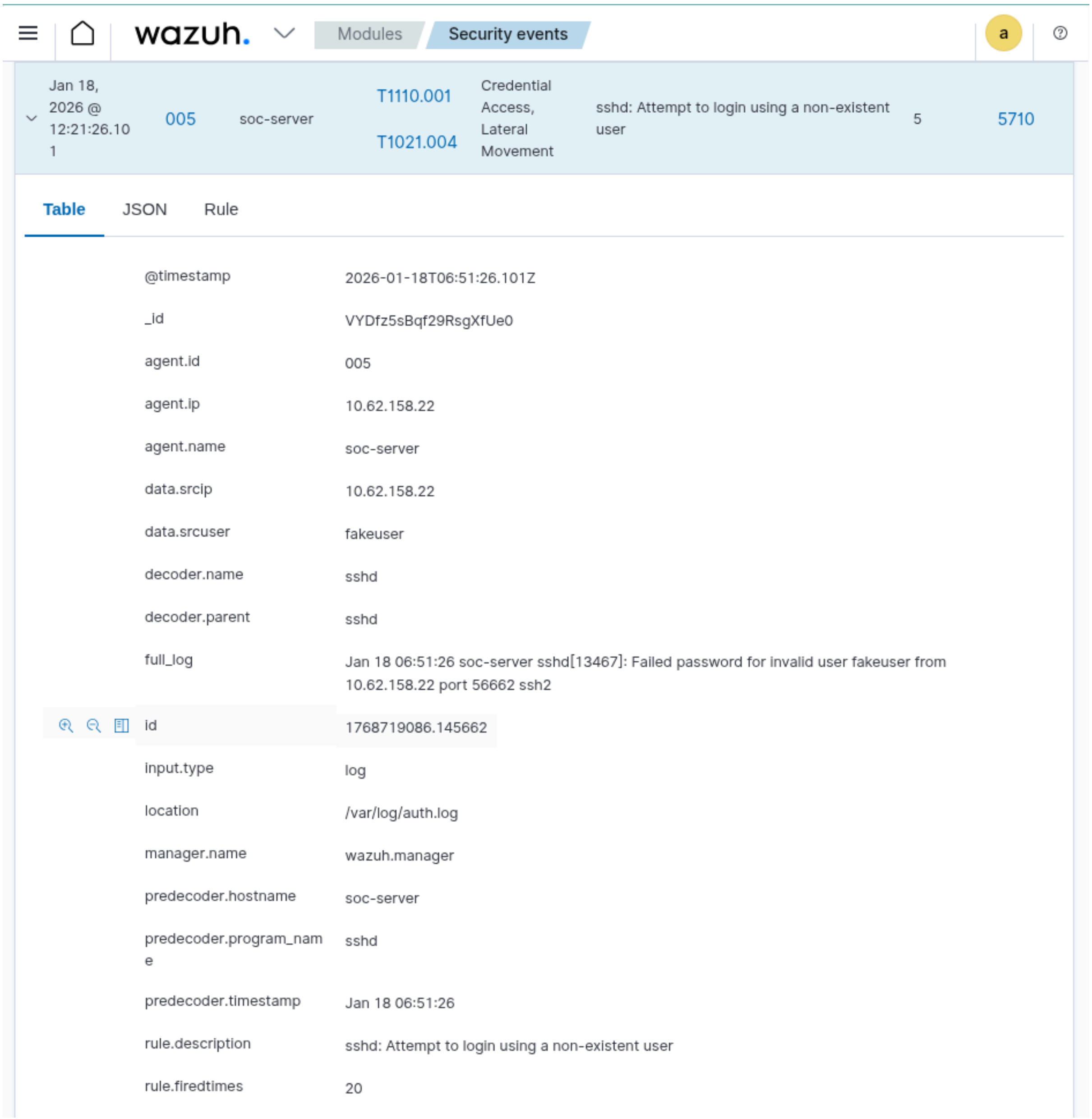


4							
Jan 18, 2026 @ 12:22:54.542	005	soc-server			PAM: Login session closed.	3	5502
Jan 18, 2026 @ 12:22:54.540	005	soc-server	T1548.003	Privilege Escalation, Defense Evasion	Successful sudo to ROOT executed.	3	5402
Jan 18, 2026 @ 12:22:54.540	005	soc-server	T1078	Defense Evasion, Persistence, Privilege Escalation, Initial Access	PAM: Login session opened.	3	5501
Jan 18, 2026 @ 12:22:53.003	005	soc-server	T1565.001	Impact	Integrity checksum changed.	7	550
Jan 18, 2026 @ 12:22:44.849	005	soc-server	T1078	Defense Evasion, Persistence, Privilege Escalation, Initial Access	PAM: Login session opened.	3	5501
Jan 18, 2026 @ 12:22:44.799	005	soc-server	T1078 T1021	Defense Evasion, Persistence, Privilege Escalation, Initial Access, Lateral Movement	sshd: authentication success.	3	5715
Jan 18, 2026 @ 12:21:32.152	005	soc-server			PAM: Login session closed.	3	5502
Jan 18, 2026 @ 12:21:26.10	005	soc-server	T1110.001 T1021.004	Credential Access, Lateral	sshd: Attempt to login using a non-existent user	5	5710

Figure 7: Wazuh Security events list view showing correlated alerts (SSH authentication activity → sudo privilege escalation → FIM checksum change) on agent `soc-server` (ID: 005).

6.2 SSH Authentication Abuse — Event Details

Detailed SSH evidence confirms authentication abuse attempts, including login attempts using a non-existent/invalid user. The event metadata confirms the log source as `/var/log/auth.log` and the decoder as `sshd`, proving that Wazuh correctly parsed and generated alerts for SSH-based credential access activity.



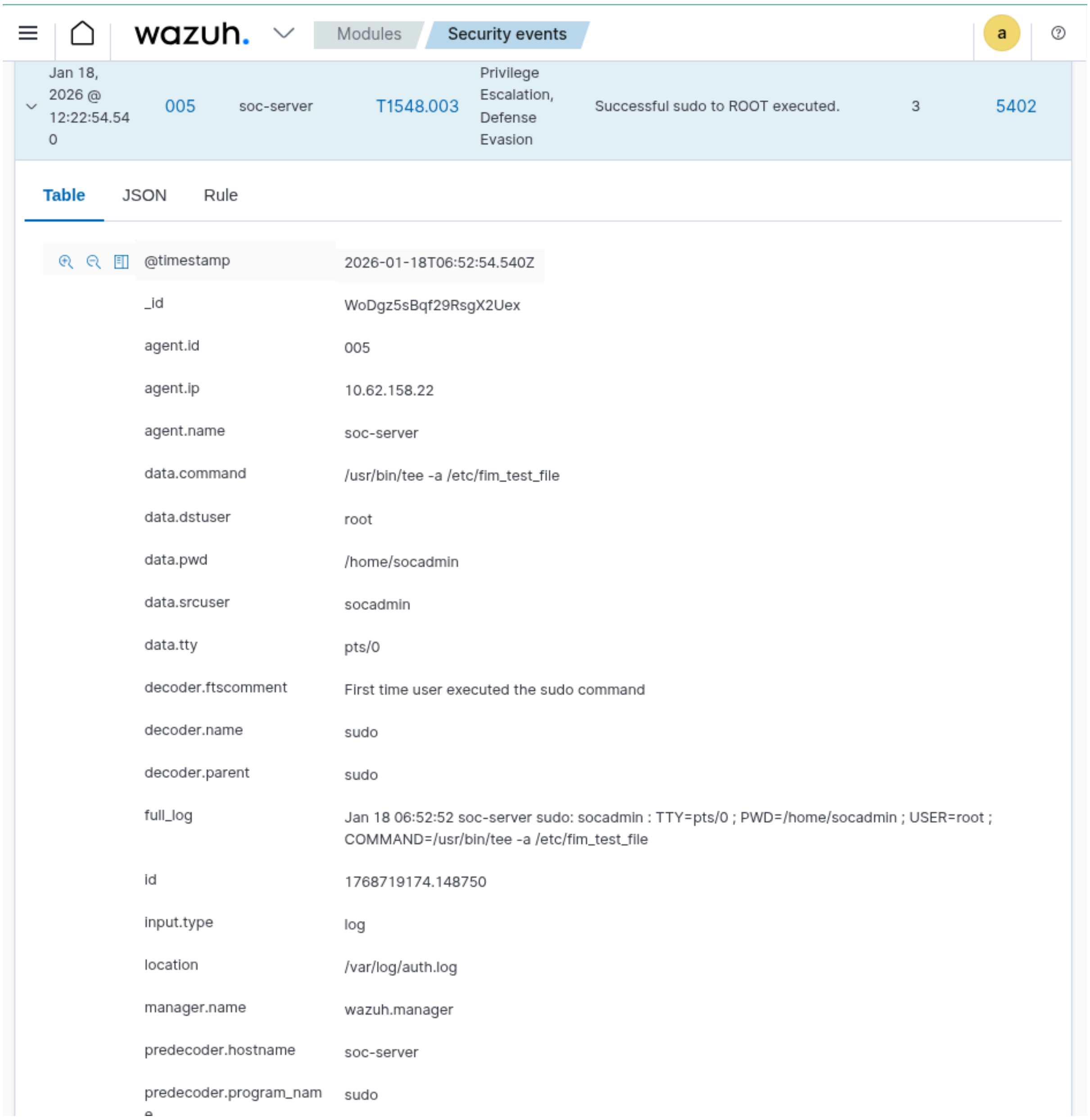
Jan 18, 2026 @ 12:21:26.101	005	soc-server	T1110.001 T1021.004	Credential Access, Lateral Movement	sshd: Attempt to login using a non-existent user	5	5710

@timestamp	2026-01-18T06:51:26.101Z
_id	VYDfz5sBqf29RsgXfUe0
agent.id	005
agent.ip	10.62.158.22
agent.name	soc-server
data.srcip	10.62.158.22
data.srcuser	fakeuser
decoder.name	sshd
decoder.parent	sshd
full_log	Jan 18 06:51:26 soc-server sshd[13467]: Failed password for invalid user fakeuser from 10.62.158.22 port 56662 ssh2
id	1768719086.145662
input.type	log
location	/var/log/auth.log
manager.name	wazuh.manager
predecoder.hostname	soc-server
predecoder.program_name	sshd
predecoder.timestamp	Jan 18 06:51:26
rule.description	sshd: Attempt to login using a non-existent user
rule.firedtimes	20

Figure 8: Wazuh alert details showing SSH authentication abuse — “sshd: Attempt to login using a non-existent user” with full log evidence and MITRE mapping.

6.3 Privilege Escalation — Sudo to Root Event Details

Privilege escalation activity was successfully detected via sudo execution. The alert confirms a successful sudo execution to ROOT and includes command context, user, working directory, and TTY session information. This validates that Wazuh correctly detects privilege escalation patterns from authentication logs.



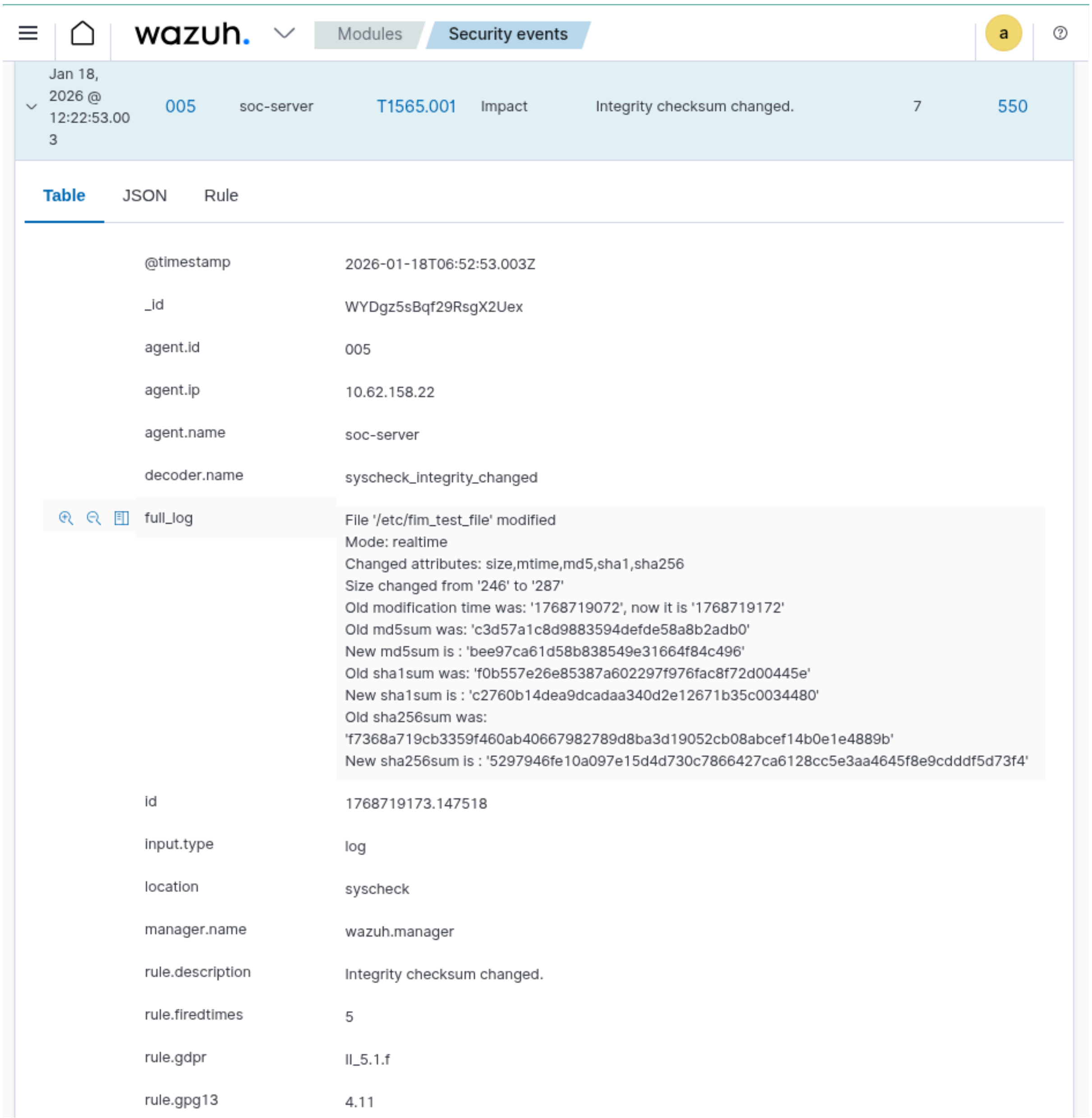
Jan 18, 2026 @ 12:22:54.540	005	soc-server	T1548.003	Privilege Escalation, Defense Evasion	Successful sudo to ROOT executed.	3	5402

@timestamp	2026-01-18T06:52:54.540Z
_id	WoDgz5sBqf29RsgX2Uex
agent.id	005
agent.ip	10.62.158.22
agent.name	soc-server
data.command	/usr/bin/tee -a /etc/fim_test_file
data.dstuser	root
data.pwd	/home/socadmin
data.srcuser	socadmin
data.tty	pts/0
decoder.ftscomment	First time user executed the sudo command
decoder.name	sudo
decoder.parent	sudo
full_log	Jan 18 06:52:52 soc-server sudo: socadmin : TTY=pts/0 ; PWD=/home/socadmin ; USER=root ; COMMAND=/usr/bin/tee -a /etc/fim_test_file
id	1768719174.148750
input.type	log
location	/var/log/auth.log
manager.name	wazuh.manager
predecoder.hostname	soc-server
predecoder.program_name	sudo

Figure 9: Wazuh alert details showing privilege escalation — “Successful sudo to ROOT executed” including command execution context.

6.4 File Integrity Monitoring (FIM) — Integrity Checksum Changed

File Integrity Monitoring (FIM) successfully detected modifications to the monitored file. The alert indicates **“Integrity checksum changed”**, which confirms that the file content changed and Wazuh recorded differences in integrity attributes such as hash values (MD5/SHA1/SHA256), file size, and timestamps. This validates real-time FIM detection and integrity verification on the endpoint.



Jan 18, 2026 @ 12:22:53.003	005	soc-server	T1565.001	Impact	Integrity checksum changed.	7	550

@timestamp	2026-01-18T06:52:53.003Z
_id	WYDgz5sBqf29RsgX2Uex
agent.id	005
agent.ip	10.62.158.22
agent.name	soc-server
decoder.name	syscheck_integrity_changed
full_log	File '/etc/fim_test_file' modified Mode: realtime Changed attributes: size,mtime,md5,sha1,sha256 Size changed from '246' to '287' Old modification time was: '1768719072', now it is '1768719172' Old md5sum was: 'c3d57a1c8d9883594defde58a8b2adb0' New md5sum is : 'bee97ca61d58b838549e31664f84c496' Old sha1sum was: 'f0b557e26e85387a602297f976fac8f72d00445e' New sha1sum is : 'c2760b14dea9dcadaa340d2e12671b35c0034480' Old sha256sum was: 'f7368a719cb3359f460ab40667982789d8ba3d19052cb08abcef14b0e1e4889b' New sha256sum is : '5297946fe10a097e15d4d730c7866427ca6128cc5e3aa4645f8e9cdddf5d73f4'
id	1768719173.147518
input.type	log
location	syscheck
manager.name	wazuh.manager
rule.description	Integrity checksum changed.
rule.firedtimes	5
rule.gdpr	II_5.1.f
rule.gpg13	4.11

Figure 10: Wazuh FIM (syscheck) alert details showing "Integrity checksum changed" for `/etc/fim_test_file`, including before/after hash values.

6.5 Evidence Validation Summary

Based on the above evidence:

- Dashboard correlation confirms multiple detections within a single simulation window (**Figure 7**).

- SSH authentication abuse attempts were detected and logged with full event context (**Figure 8**).

- Privilege escalation via sudo to root was captured and validated (**Figure 9**).

- FIM successfully detected integrity checksum/hash changes after file modification (**Figure 10**).

This confirms the Wazuh setup is operational and capable of generating visibility for common SOC detections in a controlled lab environment.

7. Findings / Analyst Notes

7.1 Analyst Observations

During the lab simulation, the monitored endpoint `soc-server` (Agent ID: 005) generated multiple security alerts that were successfully detected and correlated in Wazuh. The event chain indicates authentication abuse attempts (SSH invalid/non-existent user login attempts), followed by privilege escalation activity using `sudo` to ROOT, and finally a File Integrity Monitoring (FIM) checksum change event. The detections confirm that log collection, decoding, and rule triggering are functioning correctly for the tested use cases (**Figure 7-10**).

7.2 Key Findings

Finding 1 — SSH Authentication Abuse Detected

While Rule 5710 successfully detected an invalid user attempt, it is important to note that Wazuh's **Rule 5712** (SSHD brute force) would be the primary trigger in a production environment. This rule aggregates individual failures (Rule 5710/5716) to identify a sustained attack pattern rather than isolated typos.

- **SSH Authentication Abuse Detected**: Multiple attempts using invalid or non-existent users were detected.
- **Production Context**: While **Rule 5710** successfully flagged an invalid user attempt in this lab, a production environment relies on **Rule 5712** (SSHD brute force).
- **Detection Logic**: This rule aggregates multiple individual failures (like Rule 5710/5716) over a short window to distinguish actual brute-force attacks from simple human error or typos.
- **Evidence Validation**: Successful identification of these early-stage attack patterns was confirmed via SSH event details in **Figure 8**.

Finding 2 — Privilege Escalation via Sudo Logged

Wazuh successfully detected sudo execution to ROOT, validating privilege escalation visibility. The alert contains useful context such as command execution, user session details, and source log location, which supports investigation and response actions.

- Evidence: “Successful sudo to ROOT executed” event detected and logged (**Figure 9**)
- Risk in production: May indicate misuse of admin rights or attacker escalation after access

Finding 3 — FIM Integrity Checksum Change Triggered

File Integrity Monitoring (syscheck) successfully detected file modification events. The “Integrity checksum changed” alert confirms that monitored file content was modified, and Wazuh recorded the change with integrity attributes (hashes + metadata).

- Evidence: FIM checksum change alert with before/after hash values (**Figure 10**)
- Risk in production: Could indicate tampering with system files, persistence attempts, or log manipulation

7.3 Correlation / Attack Narrative (SOC View)

From a SOC investigation perspective, the sequence of detections can be interpreted as:

1. **Credential Access Attempt** → SSH authentication abuse attempts (invalid user/login failures)
2. **Privilege Escalation** → successful sudo execution to ROOT
3. **Impact / Tampering** → file modification detected via FIM checksum change

This pattern matches a realistic intrusion flow where an attacker attempts access, escalates privileges, and then modifies files for persistence or system manipulation. In this simulation, the events were intentionally triggered to validate detection capability, and no real compromise occurred (**Figure 6.1**).

7.4 Analyst Notes (Investigation Quality Checks)

- Agent `soc-server` was confirmed active and reporting events correctly (validated earlier in setup).
- Event visibility was consistent across the dashboard timeline and detailed alert views (**Figure 7**).

- SSH logs were parsed correctly from `/var/log/auth.log` with the `sshd` decoder (**Figure 8**).
- Sudo activity contained an adequate execution context (user, command, session) for investigation (**Figure 9**).
- FIM events confirmed real-time integrity monitoring and checksum comparison (**Figure 10**).

7.5 Limitations (Lab Context)

- This was a controlled SOC simulation; alerts were generated intentionally for validation purposes.
- No external attacker IP intelligence enrichment or automated response actions were configured in this test.
- Correlation was based on timestamp proximity and alert types, not automated incident grouping rules.

7.6 Conclusion (Analyst Closure)

The simulation confirms that Wazuh is properly collecting logs, detecting authentication abuse, recording privilege escalation activity, and triggering FIM alerts for file integrity changes. The environment is suitable for further SOC detection testing and incident report documentation.

8. Recommendations

8.1 SSH Hardening (Credential Access Prevention)

- Disable direct **root login via SSH** (`PermitRootLogin no`).
- Enforce **key-based authentication** and disable password login where possible (`PasswordAuthentication no`).
- Enable **account lockout/rate limiting** (Fail2Ban or SSH rate-limit rules).
- Restrict SSH access using firewall rules (allow only trusted IPs / VPN subnet).
- Monitor repeated invalid user attempts and alert on threshold-based brute-force patterns.

8.2 Privilege Escalation Controls

- Review `sudoers` permissions and apply **least privilege** (only required commands).
- Enable logging of all privileged commands (`sudo` logs + command auditing).
- Alert on suspicious sudo usage patterns (unusual users, off-hours, rare commands).

- Consider enabling Linux audit rules (`auditd`) for privileged command execution tracking.

8.3 File Integrity Monitoring (FIM) Improvements

- **Implement Content Diffing**: Configure the `report_changes="yes"` attribute within the agent's `ossec.conf` file for critical system paths.
- **Analyst Visibility**: This change allows the Wazuh dashboard to display the exact lines of code added, removed, or modified, rather than just reporting a hash change.
- **Configuration Example**:
  ```
   <directories report_changes="yes"
  realtime="yes">/etc</directories>
  ```
- **Verification Step**: After implementation, a baseline validation should be performed using the `agent_control` tool to ensure the agent is reporting full-text changes for monitored files.

8.4 SOC Visibility & Response Enhancements

- Configure correlation rules to group related alerts (SSH → sudo → FIM) into one incident.
- Add threat intelligence enrichment (GeoIP, reputation checks for source IP).
- Define a simple response playbook:
  - Identify source → verify user → check sudo logs → review modified file → contain if needed.

8.5 General Security Best Practices

- Keep OS packages updated and apply security patches regularly.
- Ensure a strong password policy for local users.
- Use MFA for admin accounts where possible (especially in production environments).

9. Conclusion / Closure

This SOC lab simulation successfully validated Wazuh alert generation and visibility for multiple security scenarios on the monitored endpoint `soc-server` (Agent ID: 005). The system correctly detected and logged SSH authentication abuse attempts, privilege escalation activity via `sudo`, and File Integrity Monitoring (FIM) checksum changes on a monitored file.

All observed alerts were expected and confirmed as part of controlled testing. No real compromise occurred. The incident is marked as **Closed (Validated)**, and the environment is considered functioning correctly for detection and monitoring purposes.

Final Status: Closed — Validation Complete