Security Incident Report

Analyst: enigma code

Environment: Home Lab – Wazuh SIEM

Windows Account Manipulation

#	Event	Account / Agent / Source IP	Time ([timezone])	Rule / Event ID	Severity
1	User account changed	Student1 192.168.5.131	Sep 16, 2026 @ 10:19:58.943	4738	
2	Users Group Changed	Student1 192.168.5.131	Sep 16, 2026 @ 10:19:59.005	4732	
3	Administrators Group Changed	Student1 192.168.5.131	Sep 16, 2026 @ 10:20:50.008	4732	
4	User account disabled or deleted	Student1 192.168.5.131	Sep 16, 2026 @ 10:22:01.101	4726	
5	User account disabled or deleted	Guest 192.168.5.131	Sep 16, 2026 @ 11:29:19.801	4725	
6	User account changed	Guest 192.168.5.131	Sep 16, 2026 @ 11:29:19.832	4738	
7	Windows: MYDFIR-enigma-code Guest account has been enabled on mydfir-enigma-win	Guest 192.168.5.131	Sep 16, 2026 @ 11:34:39.479	100210	
8	User account changed	Guest 192.168.5.131	Sep 16, 2026 @ 11:34:39.510	4738	

Wazuh rule reference: 100210 = if_group: windows = win.system.eventID:4722

= win.eventdata.targetUserName: Guest.

Time	rule.description	data.win.eventdata.subjectUserName	data.win.eventdata.targetUserName
Sep 16, 2026 @ 11:34:39.510	User account changed	mydfir-enigma	Guest
Sep 16, 2026 @ 11:34:39.479	Windows: MYDFIR-enigma-code Guest account has been enabled on mydfir-enigma-win	mydfir-enigma	Guest
Sep 16, 2026 @ 11:29:19.832	User account changed	mydfir-enigma	Guest
Sep 16, 2026 @ 11:29:19.801	User account disabled or deleted	mydfir-enigma	Guest
Sep 16, 2026 @ 10:22:01.101	User account disabled or deleted	mydfir-enigma	student1
Sep 16, 2026 @ 10:20:50.008	Administrators Group Changed	mydfir-enigma	Administrators
Sep 16, 2026 @ 10:19:59.005	Users Group Changed	mydfir-enigma	Users
Sep 16, 2026 @ 10:19:58.943	User account enabled or created	mydfir-enigma	student1

The Guest account on the windows host 192.168.5.131 which is disabled by default (confirmation of down status Sep 16, 2026 @ 11:29:19.801), was enabled during the observed window. at 11:34:39, The enable event triggered a corresponding "User account changed" event (Event ID 4738) a few milliseconds later, consistent with Windows logging the account-state change itself as a separate audit event from the enable action. Rule 100210 is a custom Wazuh rule written specifically to catch Guest account activation. It fires on the underlying Windows Event ID 4722 ("a user account was enabled"), but narrows that generic trigger to alert only when the affected account is Guest, rather than raising an alert for every account enablement across the environment. This matters because 4722 alone is far too noisy to act on directly.

Prior to the Guest event, a temporary account (Student1) was created, added first to the default Users group and then to the local Administrators group, and subsequently deleted. A sequence that moves from account creation directly to privileged group membership (event ID 4732) within roughly a minute. Follwed by deletion of the account (event ID 4726).

File Integrity Monitoring was configured in real-time mode on both the Windows agent (C:\companydata) and the Ubuntu agent (/opt/company-data), and validated by performing an identical add–modify–delete sequence against a test file on each host.

File Integrity Monitoring (Window)

#	Event	File Path	Time (GMT)	Rule ID	Severity
1	File added	c:\companydata\payroll.txt	Sep 16, 2026 @ 11:14:35.076	554	5
2	File Modified	c:\companydata\payroll.txt	Sep 16, 2026 @ 11:17:13.687	550	7
3	File deleted	c:\companydata\payroll.txt	Sep 16, 2026 @ 11:19:27.002	553	7

Wazuh rule reference: 550 = Integrity checksum changed, 553 = File deleted, 554 = File added.

↓ timestamp	agent.name	syscheck.path	syscheck.event	rule.description	rule.level	rule.id
Sep 16, 2026 @ 11:19:27.002	Win_Agent	c:\companydata\payroll.txt	deleted	File deleted.	7	553
Sep 16, 2026 @ 11:17:13.687	Win_Agent	c:\companydata\payroll.txt	modified	Integrity checksum changed.	7	550
Sep 16, 2026 @ 11:14:35.076	Win_Agent	c:\companydata\payroll.txt	added	File added to the system.	5	554

On the Windows host, payroll.txt was created, modified, and deleted between 11:14:35 and 11:19:27;

File Integrity Monitoring (Linux)

#	Event	File Path	Time (GMT)	Rule ID	Severity
1	File added	/opt/company-data/test.txt	Sep 16, 2026 @ 11:14:35.076	554	5
2	File Modified	/opt/company-data/test.txt	Sep 16, 2026 @ 11:17:13.687	550	7
3	File deleted	/opt/company-data/test.txt	Sep 16, 2026 @ 11:19:27.002	553	7

Wazuh rule reference: 550 = Integrity checksum changed, 553 = File deleted, 554 = File added.

	↓ timestamp	agent.name	syscheck.path	syscheck.event	rule.description	rule.level	rule.id
	Sep 16, 2026 @ 11:28:39.709	Ubuntu_Agent	/opt/company-data/test.txt	deleted	File deleted.	7	553
	Sep 16, 2026 @ 11:23:25.299	Ubuntu_Agent	/opt/company-data/test.txt	modified	Integrity checksum changed.	7	550
	Sep 16, 2026 @ 11:22:21.973	Ubuntu_Agent	/opt/company-data/test.txt	added	File added to the system.	5	554

the same sequence was then repeated against test.txt on the Ubuntu host between 11:22:21 and 11:28:39,

All six events were correctly captured by Wazuh's built-in FIM rules (554, 550, 553) on both platforms, with consistent rule levels across operating systems. Confirming that syscheck real-time monitoring is functioning correctly and consistently regardless of host OS.

SSH Brute Force attack

#	Event	SrcIP	Agent	Agent IP	Time	Rule id
1	PAM: User login failed.	192.168.5.131	Ubuntu_Agent	192.168.5.132	Sep 16, 2026 @ 11:41:24.467	5503
2	sshd: authentication failed.	192.168.5.131	Ubuntu_Agent	192.168.5.132	Sep 16, 2026 @ 11:41:28.462	5760
3	sshd: authentication failed	192.168.5.131	Ubuntu_Agent	192.168.5.132	Sep 16, 2026 @ 11:41:30.464	5760
4	Multiple SSH login failures observed from the same source IP	192.168.5.131	Ubuntu_Agent	192.168.5.132	Sep 16, 2026 @ 11:41:34.465	100101
5	Blocked by firewall-drop Active Response	192.168.5.131	Ubuntu_Agent	192.168.5.132	Sep 16, 2026 @ 11:41:35.716	651

The source host at 192.168.5.131 (Win_agent) made three failed SSH authentication attempts against the Ubuntu agent (192.168.5.132) between 11:41:24 and 11:41:30 Sep 16, 2026 (PAM rule 5503, sshd rule 5760 x2). A custom Wazuh rule (100101) correlated these as repeated failures from a single source

	timestamp	rule.description	agent.ip	data.srcip	rule.id
>	Sep 16, 2026 @ 11:41:35.71	Host Blocked by firewall-drop Active Response	192.168.5.132	192.168.5.131	651
>	Sep 16, 2026 @ 11:41:34.465	Multiple SSH login failures observed from the same source IP	192.168.5.132	192.168.5.131	100101
>	Sep 16, 2026 @ 11:41:30.464	sshd: authentication failed.	192.168.5.132	192.168.5.131	5760
>	Sep 16, 2026 @ 11:41:28.462	sshd: authentication failed.	192.168.5.132	192.168.5.131	5760
>	Sep 16, 2026 @ 11:41:24.467	PAM: User login failed.	192.168.5.132	192.168.5.131	5503

and raised a dedicated alert four seconds later. Wazuh's Active Response then blocked the source IP via

firewall-drop (rule 651) within roughly 1.25 seconds. The full chain, from first failed login to automated block, completing in under 12 seconds.
Two hypotheses are consistent with the evidence: authorized administrative / testing activity, or an insider threat / compromised credential.

Recommendations

1.Keep the Guest account disabled by default. Guest re-enablement is a known persistence/defense-evasion technique — any future occurrence should trigger investigation, not be treated as routine.

2.Verify the Active Response scope for rule 651. *Confirm the firewall-drop action only blocks the offending source IP (192.168.5.131), has a defined timeout, and doesn't risk catching legitimate hosts — and test the unblock path so the response is confirmed reversible, not just confirmed to fire*

3.Escalate FIM alerting on sensitive file paths. *C:\companydata\payroll.txt represents financially sensitive data; consider raising its severity above the default Medium and adding keyword-based escalation (payroll, invoice, finance) so sensitive-path changes stand out from routine FIM noise.*

4.Add a follow-on rule for successful logins after repeated failures. *Rule 100101 correctly detects the failure pattern itself, but a brute-force attempt that eventually succeeds would currently generate the same alert as one that's fully blocked. A rule that flags a successful authentication immediately following multiple failures would close that gap.*

5.Baseline legitimate account-management activity. *Alert on any account creation, enablement, or group-change event where the acting account isn't a recognized admin or automation identity*

6.Harden SSH authentication on the Ubuntu endpoint. *Given it was the actual target of the observed brute-force attempt, move to key-based authentication and disable password login to remove the attack surface rule 100101 is currently compensating for.*

End Report