info@wazuh.com
https://wazuh.com

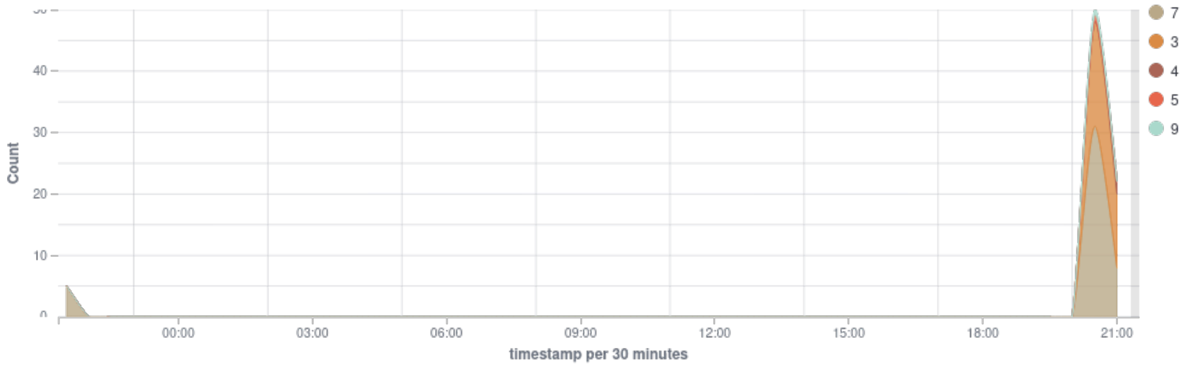
Threat hunting report

Browse through your security alerts, identifying issues and threats in your environment.

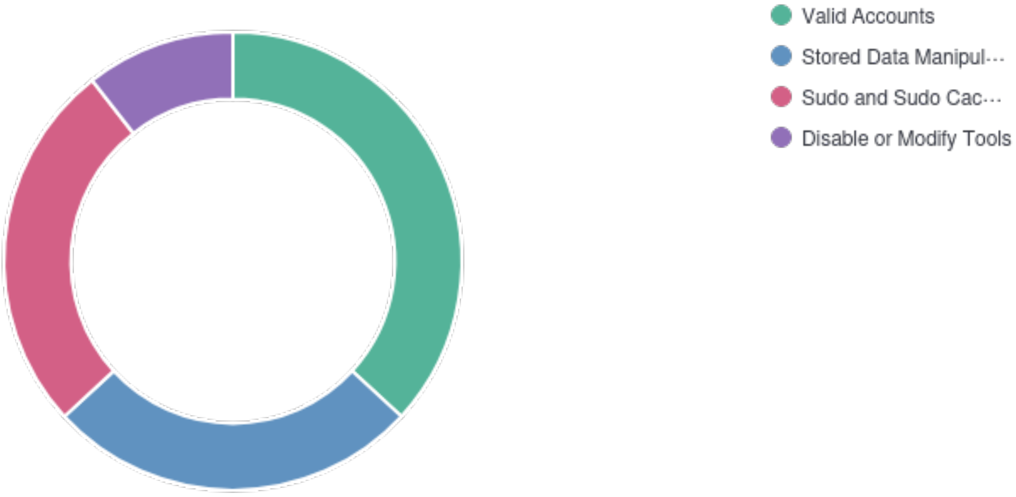
2024-10-01T21:18:31 to 2024-10-02T21:18:31

manager.name: wazuh-server

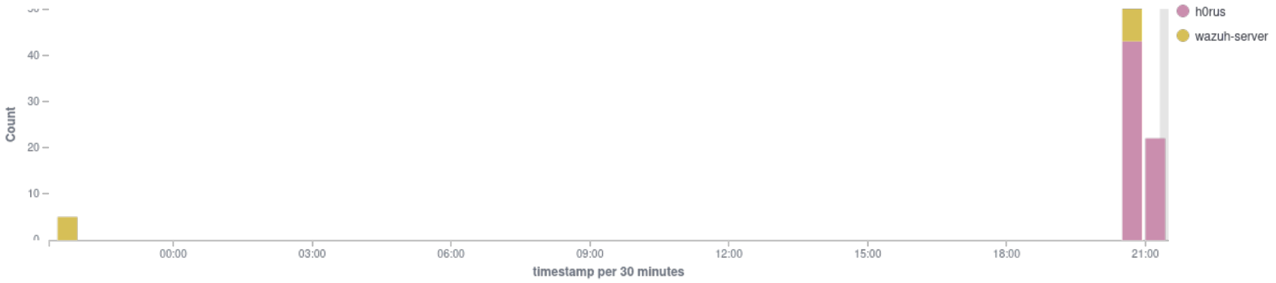
Top 10 Alert level evolution



Top 10 MITRE ATT&CKS



Alerts evolution - Top 5 agents



77

- Total -

0

- Level 12 or above alerts -

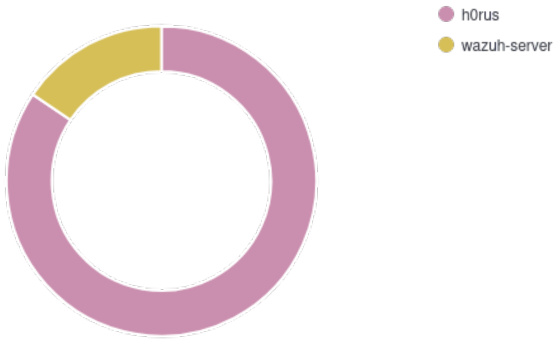
1

- Authentication failure -

7

- Authentication success -

Top 5 agents



Alerts summary

Rule ID	Description	Level	Count
510	Host-based anomaly detection event (rootcheck).	7	24
5501	PAM: Login session opened.	3	7
550	Integrity checksum changed.	7	5
5402	Successful sudo to ROOT executed.	3	3
5502	PAM: Login session closed.	3	3
503	Wazuh agent started.	3	2
506	Wazuh agent stopped.	3	2
533	Listened ports status (netstat) changed (new port opened or closed).	7	2
5403	First time user executed sudo.	4	2
19007	System audit for Unix based systems: Ensure auditd service is enabled	7	1
19007	System audit for Unix based systems: Ensure lockout for failed password attempts is configured	7	1
19007	System audit for Unix based systems: Ensure password expiration is 365 days or less	7	1
19007	System audit for Unix based systems: SSH Hardening: Empty passwords should not be allowed	7	1
19007	System audit for Unix based systems: SSH Hardening: Ensure SSH HostbasedAuthentication is disabled	7	1
19007	System audit for Unix based systems: SSH Hardening: Grace Time should be one minute or less.	7	1
19007	System audit for Unix based systems: SSH Hardening: No Public Key authentication	7	1
19007	System audit for Unix based systems: SSH Hardening: Password Authentication should be disabled	7	1
19007	System audit for Unix based systems: SSH Hardening: Port should not be 22	7	1
19007	System audit for Unix based systems: SSH Hardening: Protocol should be set to 2	7	1
19007	System audit for Unix based systems: SSH Hardening: Rhost or shost should not be used for authentication	7	1
19007	System audit for Unix based systems: SSH Hardening: Root account should not be able to log in	7	1
19007	System audit for Unix based systems: SSH Hardening: Wrong Maximum number of authentication attempts	7	1
19009	System audit for Unix based systems: Ensure password hashing algorithm is SHA-512	3	1
19009	System audit for Unix based systems: Ensure passwords are longer than 14 characters	3	1
19009	System audit for Unix based systems: Ensure passwords contain at least one digit	3	1
19009	System audit for Unix based systems: Ensure passwords contain at least one lowercase character	3	1
19009	System audit for Unix based systems: Ensure passwords contain at least one special character	3	1
19009	System audit for Unix based systems: Ensure passwords contain at least one uppercase character	3	1
19009	System audit for Unix based systems: Ensure retry option for passwords is less than 3	3	1
19008	System audit for Unix based systems: Ensure CUPS is not enabled	3	1
19008	System audit for Unix based systems: Ensure SELinux or AppArmor are installed	3	1
19008	System audit for Unix based systems: Ensure passwords in /etc/shadow are hashed with SHA-512 or SHA-256	3	1
19005	SCA summary: System audit for Unix based systems: Score less than 30% (18)	9	1
2501	syslog: User authentication failure.	5	1
501	New wazuh agent connected.	3	1
502	Wazuh server started.	3	1