AKHUWAT College University
مان - احسان - اخلاص - انفاق
KASUR

EBRYX X AKHUWAT

SECURITY PROJECT #02

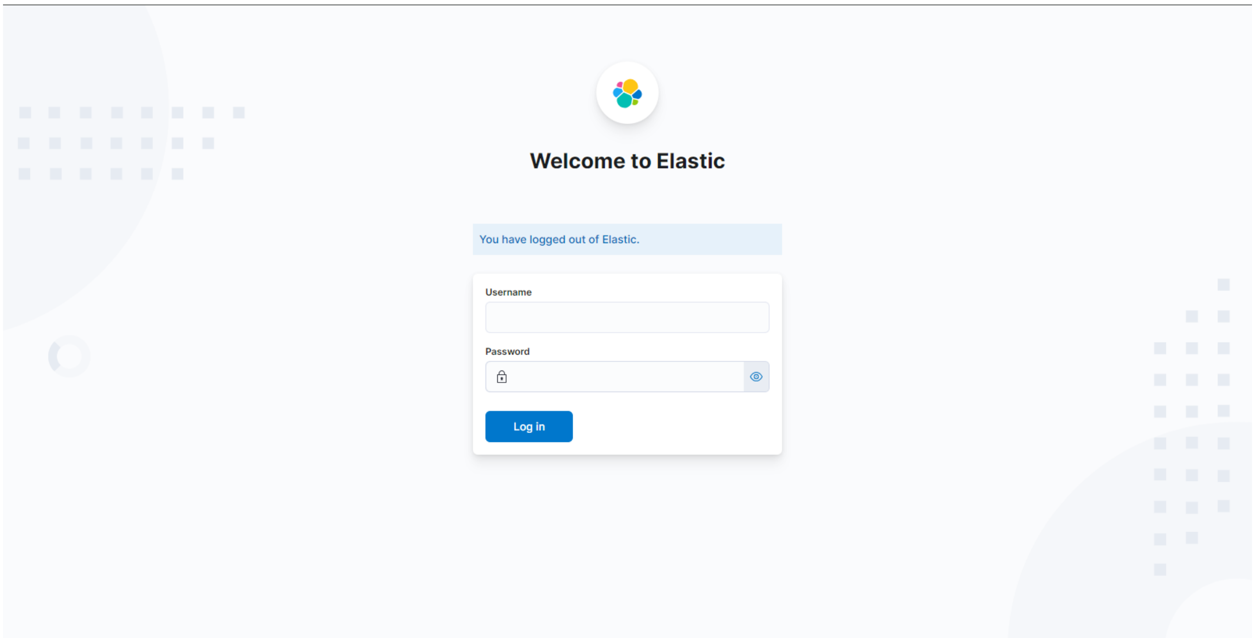
REPORT NO.2

Submitted By: Khalid Hussain
Muhammad Osama

Date of Submission: 08 Oct, 2024

.

Elastic Login Screen: Accessing Elastic in web browser by using username and password that was generated during the installation. **(Fig: 01)**



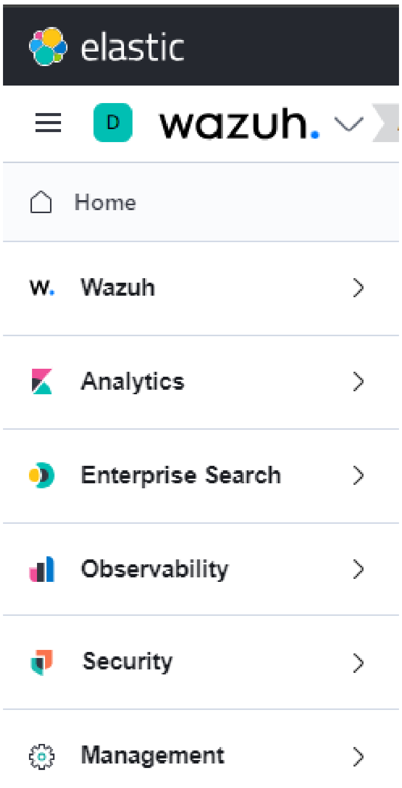
Welcome to Elastic

You have logged out of Elastic.

Username

Password

Fig: 01

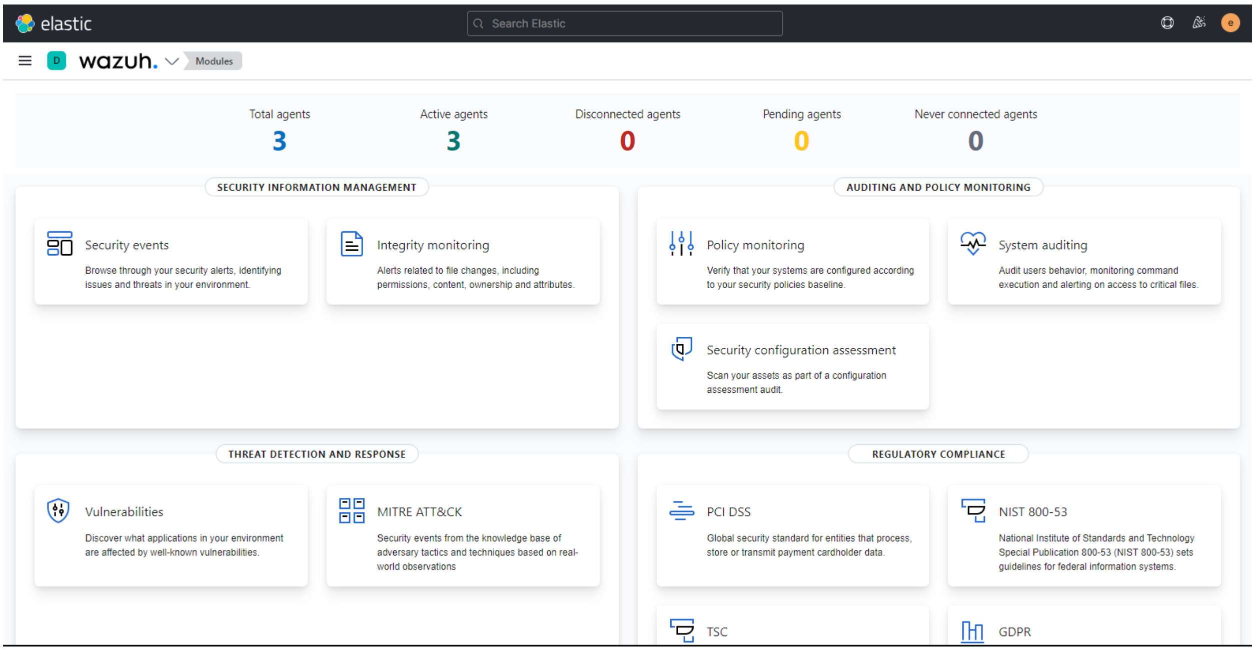


Wazuh Interface in Elastic:

This shows that wazuh is successfully integrated with the ELK stack **(Fig: 02)**

Fig:02

Wazuh Dashboard Overview: Displays agent status, security events, and regulatory compliance monitoring. **(Fig: 03)**



Total agents 3

Active agents 3

Disconnected agents 0

Pending agents 0

Never connected agents 0

SECURITY INFORMATION MANAGEMENT

Security events

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

Integrity monitoring

Alerts related to file changes, including permissions, content, ownership and attributes.

AUDITING AND POLICY MONITORING

Policy monitoring

Verify that your systems are configured according to your security policies baseline.

System auditing

Audit users behavior, monitoring command execution and alerting on access to critical files.

Security configuration assessment

Scan your assets as part of a configuration assessment audit.

THREAT DETECTION AND RESPONSE

Vulnerabilities

Discover what applications in your environment are affected by well-known vulnerabilities.

MITRE ATT&CK

Security events from the knowledge base of adversary tactics and techniques based on real-world observations

REGULATORY COMPLIANCE

PCI DSS

Global security standard for entities that process, store or transmit payment cardholder data.

NIST 800-53

National Institute of Standards and Technology Special Publication 800-53 (NIST 800-53) sets guidelines for federal information systems.

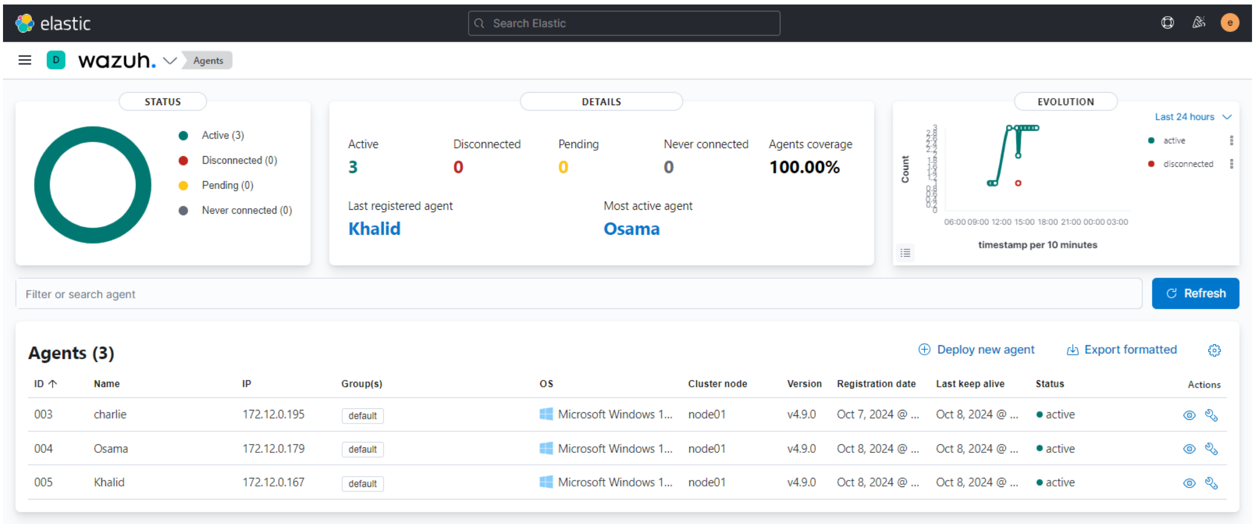
TSC

GDPR

Fig:03

Wazuh Agent Dashboard

This dashboard shows the status, details, and evolution of 3 active Wazuh agents. **(Fig: 04)**



DETAILS

Active	Disconnected	Pending	Never connected	Agents coverage
3	0	0	0	100.00%

Last registered agent **Khalid**

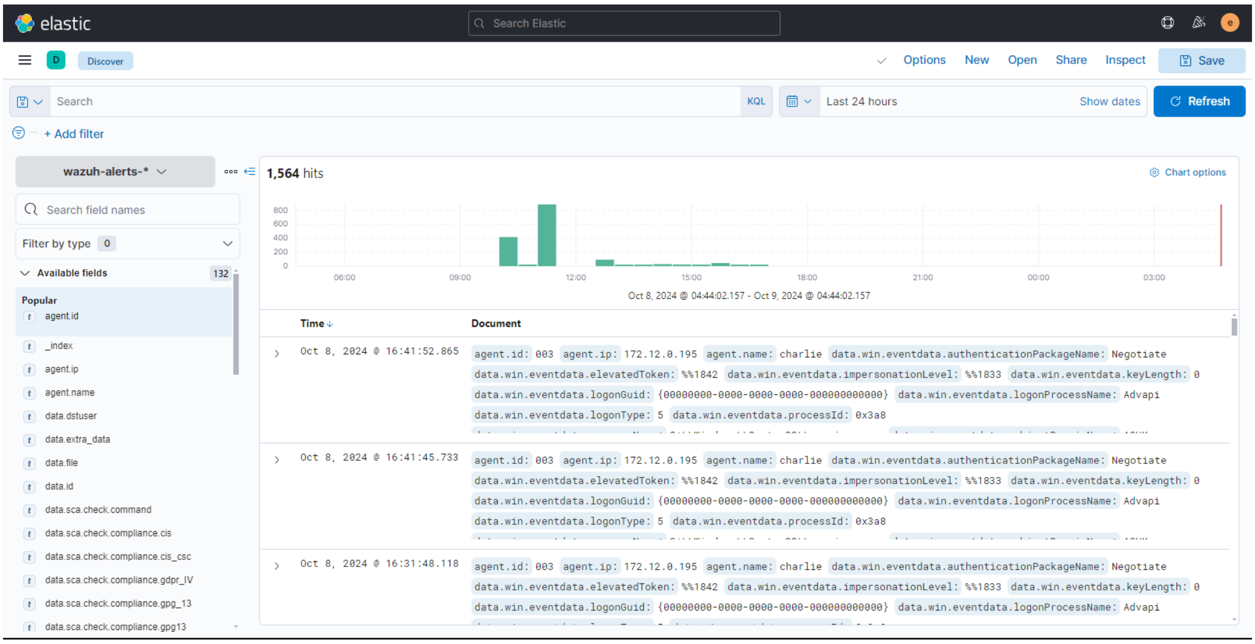
Most active agent **Osama**

Agents (3)

ID ↑	Name	IP	Group(s)	OS	Cluster node	Version	Registration date	Last keep alive	Status	Actions
003	charlie	172.12.0.195	default	Microsoft Windows 1...	node01	v4.9.0	Oct 7, 2024 @ ...	Oct 8, 2024 @ ...	● active	
004	Osama	172.12.0.179	default	Microsoft Windows 1...	node01	v4.9.0	Oct 8, 2024 @ ...	Oct 8, 2024 @ ...	● active	
005	Khalid	172.12.0.167	default	Microsoft Windows 1...	node01	v4.9.0	Oct 8, 2024 @ ...	Oct 8, 2024 @ ...	● active	

Fig:04

Wazuh Alerts Overview: Real-time monitoring of security alerts in Elastic with detailed event logs by using the Kibana . **(Fig: 05)**

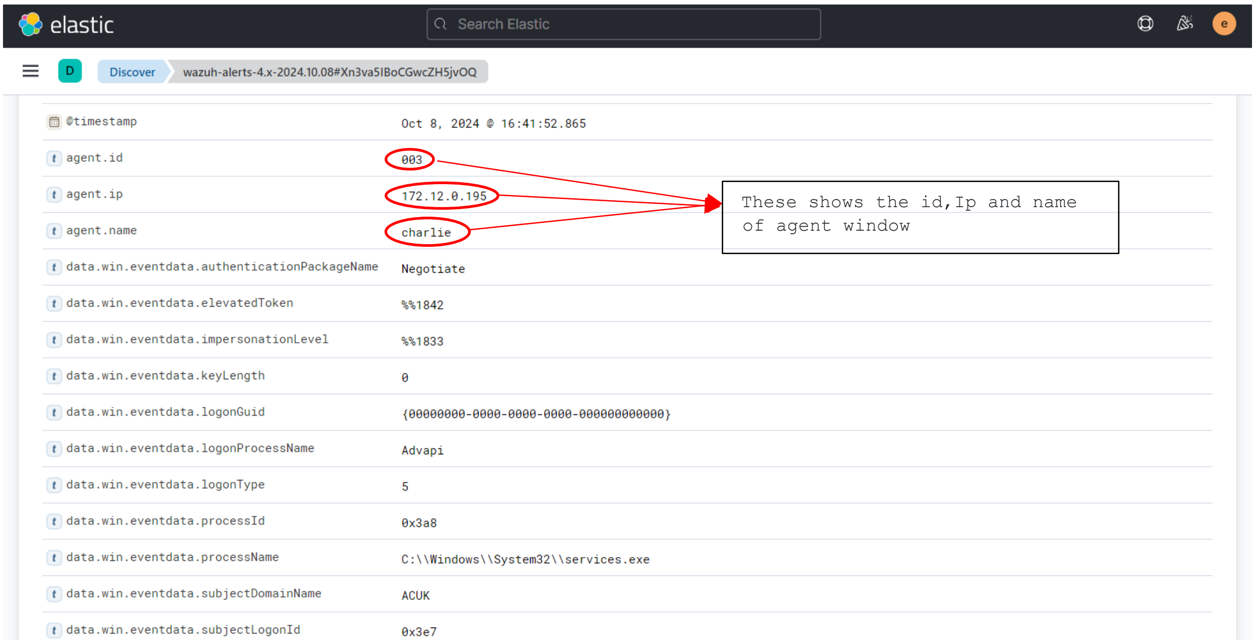


```
Oct 8, 2024 @ 16:41:52.865   agent.id: 003 agent.ip: 172.12.0.195 agent.name: charlie data.win.eventdata.authenticationPackageName: Negotiate
                             data.win.eventdata.elevatedToken: %%1842 data.win.eventdata.impersonationLevel: %%1833 data.win.eventdata.keyLength: 0
                             data.win.eventdata.logonGuid: {00000000-0000-0000-0000-000000000000} data.win.eventdata.logonProcessName: Advapi
                             data.win.eventdata.logonType: 5 data.win.eventdata.processId: 0x3a8

Oct 8, 2024 @ 16:41:45.733   agent.id: 003 agent.ip: 172.12.0.195 agent.name: charlie 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
                             data.win.eventdata.logonType: 5 data.win.eventdata.processId: 0x3a8

Oct 8, 2024 @ 16:31:48.118   agent.id: 003 agent.ip: 172.12.0.195 agent.name: charlie 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
```

Fig 05

Log Detail: this is log data page, featuring a table with various columns and rows containing information about events or activities and details of the logs . **(Fig: 06(a)&(b))**

.

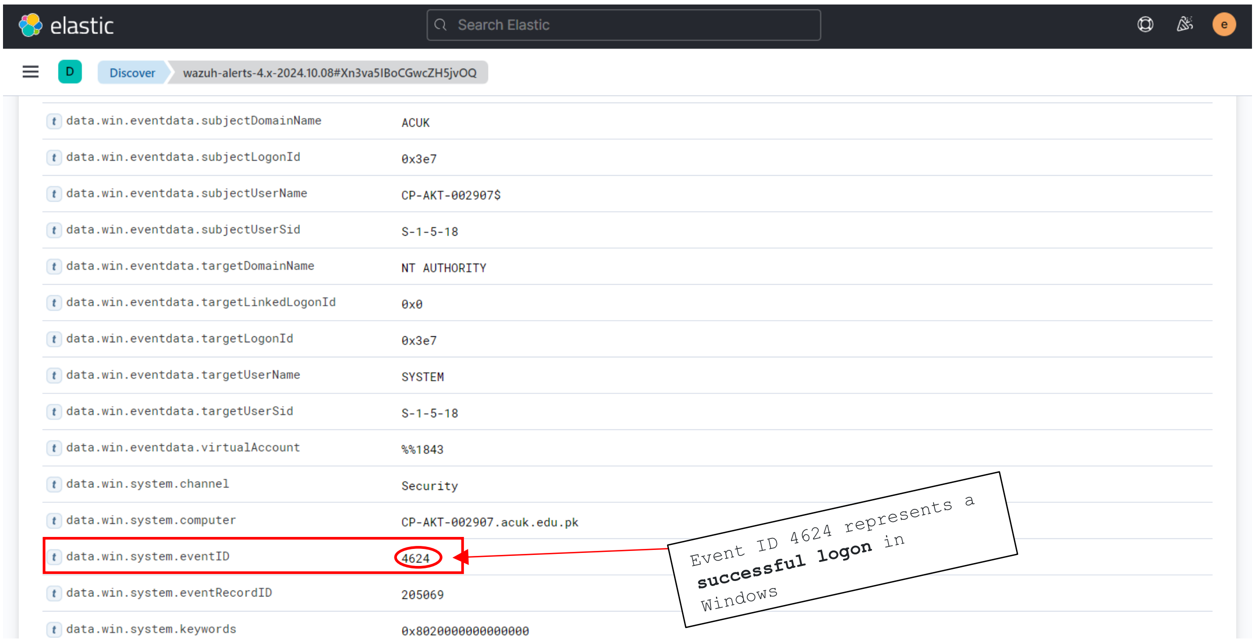


@timestamp	Oct 8, 2024 @ 16:41:52.865
agent.id	003
agent.ip	172.12.0.195
agent.name	charlie
data.win.eventdata.authenticationPackageName	Negotiate
data.win.eventdata.elevatedToken	%%1842
data.win.eventdata.impersonationLevel	%%1833
data.win.eventdata.keyLength	0
data.win.eventdata.logonGuid	{00000000-0000-0000-0000-000000000000}
data.win.eventdata.logonProcessName	Advapi
data.win.eventdata.logonType	5
data.win.eventdata.processId	0x3a8
data.win.eventdata.processName	C:\\Windows\\System32\\services.exe
data.win.eventdata.subjectDomainName	ACUK
data.win.eventdata.subjectLogonId	0x3e7

These shows the id,Ip and name of agent window

Fig: 06 (a)

.



data.win.eventdata.subjectDomainName	ACUK
data.win.eventdata.subjectLogonId	0x3e7
data.win.eventdata.subjectUserName	CP-AKT-002907$
data.win.eventdata.subjectUserSid	S-1-5-18
data.win.eventdata.targetDomainName	NT AUTHORITY
data.win.eventdata.targetLinkedLogonId	0x0
data.win.eventdata.targetLogonId	0x3e7
data.win.eventdata.targetUserName	SYSTEM
data.win.eventdata.targetUserSid	S-1-5-18
data.win.eventdata.virtualAccount	%%1843
data.win.system.channel	Security
data.win.system.computer	CP-AKT-002907.acuk.edu.pk
data.win.system.eventID	4624
data.win.system.eventRecordID	205069
data.win.system.keywords	0x8020000000000000

Event ID 4624 represents a **successful logon** in Windows

Fig: 06 (b)

Data visualization Dashboard: A pie chart visualization data visualization showing the distribution of data points at different hours **(Fig: 07)**

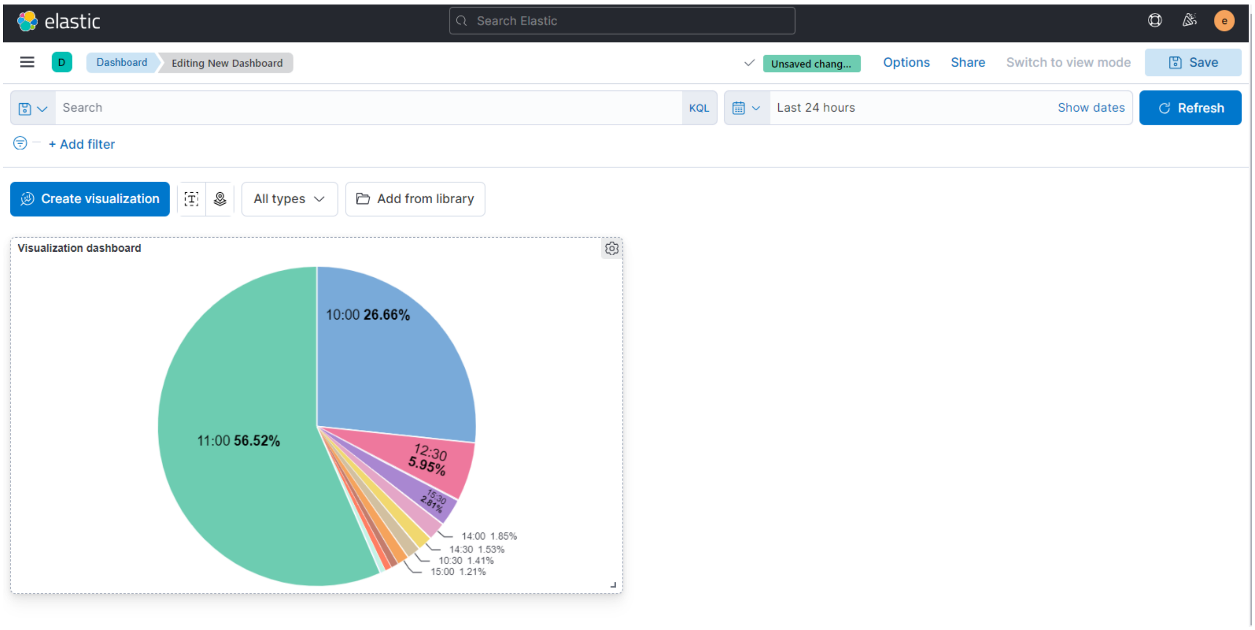


Fig: 07